AWS Arsitektur Referensi Keamanan (AWS SRA) — arsitektur inti

AWS Bimbingan Preskriptif

AWS Bimbingan Preskriptif: AWS Arsitektur Referensi Keamanan (AWS SRA) — arsitektur inti

Table of Contents

AWS Arsitektur Referensi Keamanan (AWS SRA) — arsitektur inti

Tim Keamanan Layanan Global, Amazon Web Services (kontributor)

Desember 2025 (riwayat dokumen)

> Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

Amazon Web Services (AWS) Security Reference Architecture (AWS SRA) adalah seperangkat pedoman holistik untuk menerapkan layanan AWS keamanan lengkap di lingkungan multi-akun. Gunakan untuk membantu merancang, mengimplementasikan, dan mengelola layanan AWS keamanan sehingga selaras dengan praktik yang AWS direkomendasikan. Rekomendasi dibangun di sekitar arsitektur satu halaman yang mencakup layanan AWS keamanan — bagaimana mereka membantu mencapai tujuan keamanan, di mana mereka dapat digunakan dan dikelola dengan baik di Anda Akun AWS, dan bagaimana mereka berinteraksi dengan layanan keamanan lainnya. Panduan arsitektur keseluruhan ini melengkapi rekomendasi terperinci dan spesifik layanan seperti yang ditemukan di situs web Dokumentasi AWS Keamanan.

Arsitektur dan rekomendasi yang menyertainya didasarkan pada pengalaman kolektif kami dengan pelanggan AWS perusahaan. Dokumen ini adalah referensi—seperangkat panduan komprehensif untuk digunakan Layanan AWS untuk mengamankan lingkungan tertentu—dan pola solusi dalam repositori kode AWS SRA dirancang untuk arsitektur spesifik yang diilustrasikan dalam referensi ini. Setiap pelanggan akan memiliki persyaratan yang berbeda. Akibatnya, desain AWS lingkungan Anda mungkin berbeda dari contoh yang diberikan di sini. Anda perlu memodifikasi dan menyesuaikan rekomendasi ini agar sesuai dengan lingkungan pribadi dan kebutuhan keamanan Anda. Sepanjang dokumen, jika sesuai, kami menyarankan opsi untuk skenario alternatif yang sering terlihat.

AWS SRA adalah seperangkat panduan hidup dan diperbarui secara berkala berdasarkan layanan baru dan rilis fitur, umpan balik pelanggan, dan lanskap ancaman yang terus berubah. Setiap pembaruan akan mencakup tanggal revisi dan log perubahan terkait.

Meskipun kami mengandalkan diagram satu halaman sebagai fondasi kami, arsitekturnya lebih dalam dari diagram blok tunggal dan harus dibangun di atas fondasi fundamental dan prinsip-prinsip keamanan yang terstruktur dengan baik. Anda dapat menggunakan dokumen ini dengan

dua cara: sebagai narasi atau sebagai referensi. Topik disusun sebagai cerita, sehingga Anda dapat membacanya dari awal (panduan keamanan dasar) hingga akhir (diskusi tentang contoh kode yang dapat Anda terapkan). Atau, Anda dapat menavigasi dokumen untuk fokus pada prinsip keamanan, layanan, jenis akun, panduan, dan contoh yang paling relevan dengan kebutuhan Anda.

Dokumen ini dibagi menjadi beberapa bagian berikut dan lampiran:

- Tentang perpustakaan AWS SRA memberikan gambaran umum tentang bimbingan teknis dan kode yang termasuk dalam koleksi AWS publikasi SRA.
- Nilai AWS SRA membahas motivasi untuk membangun AWS SRA, menjelaskan bagaimana Anda dapat menggunakannya untuk membantu meningkatkan keamanan Anda, dan mencantumkan takeaways kunci.
- Yayasan keamanan meninjau AWS Cloud Adoption Framework (AWS CAF), AWS Well-Architected Framework, dan AWS Shared Responsibility Model, dan menyoroti elemen-elemen yang sangat relevan dengan SRA. AWS
- AWS Organizations, akun, dan pagar pembatas IAM memperkenalkan AWS Organizations layanan, membahas kemampuan keamanan dasar dan pagar pembatas, dan memberikan gambaran umum tentang strategi multi-akun yang kami rekomendasikan.
- Arsitektur Referensi AWS Keamanan adalah diagram arsitektur satu halaman yang menunjukkan fungsional Akun AWS, dan layanan keamanan serta fitur yang umumnya tersedia.
- AI/ML untuk keamanan menjelaskan bagaimana berbedanya Layanan AWS penggunaan kecerdasan buatan dan pembelajaran mesin (AI/ML) di latar belakang untuk membantu Anda mencapai tujuan keamanan tertentu. Anda dapat memasukkan ini Layanan AWS dalam desain Anda untuk memanfaatkan fitur keamanan canggih.
- Membangun arsitektur keamanan Anda — Pendekatan bertahap memberikan panduan tentang bagaimana Anda dapat membangun arsitektur keamanan Anda sendiri dalam enam fase berulang, berdasarkan referensi yang disediakan oleh SRA. AWS
- AWS Daftar periksa praktik terbaik SRA menyaring rekomendasi yang dibahas di seluruh panduan ke dalam daftar periksa yang dapat Anda ikuti saat Anda membangun versi arsitektur keamanan Anda.
- Sumber daya IAM menyajikan ringkasan dan serangkaian petunjuk untuk panduan AWS Identity and Access Management (IAM) yang penting untuk arsitektur keamanan Anda.
- Repositori kode untuk contoh AWS SRA memberikan gambaran umum tentang GitHub repositori terkait yang akan membantu pengembang dan insinyur menerapkan beberapa panduan dan pola arsitektur yang disajikan dalam dokumen ini. Anda dapat menerapkan sampel dengan

menggunakan AWS CloudFormation atau Terraform oleh. HashiCorp Mereka mendukung AWS Control Tower lingkungan keduanya AWS Control Tower dan bukan.

Lampiran berisi daftar layanan AWS keamanan, identitas, dan kepatuhan individu, dan menyediakan tautan ke informasi lebih lanjut tentang setiap layanan. Bagian Riwayat dokumen menyediakan log perubahan untuk melacak versi dokumen ini. Anda juga dapat berlangganan umpan RSS untuk pemberitahuan perubahan.

Tentang perpustakaan AWS SRA

Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

Panduan ini adalah bagian dari perpustakaan yang menyediakan cetak biru arsitektur dan panduan teknis untuk merancang dan membangun arsitektur keamanan. AWS Pustaka terdiri dari kode implementasi (pustaka kode AWS SRA), alat validasi (Verifikasi SRA), dan dua kategori panduan pelengkap yang mencakup arsitektur inti dan arsitektur penyelaman mendalam.

AWS SRA — arsitektur inti (panduan ini)

Panduan ini merupakan dasar untuk arsitektur AWS keamanan yang direkomendasikan. Ini adalah titik awal yang berlaku untuk semua organisasi, terlepas dari industri mereka, jenis aplikasi, atau pertimbangan lainnya. Fondasi ini membantu Anda membangun arsitektur yang kuat dan terukur AWS dan membantu menciptakan baseline keamanan AWS multi-akun yang kuat yang dapat diskalakan dengan aman seiring pertumbuhan bisnis Anda.

AWS SRA — arsitektur menyelam yang dalam

Panduan arsitektur inti AWS SRA dilengkapi dengan publikasi tambahan yang menyediakan pola arsitektur yang selaras dengan kemampuan keamanan tertentu, jenis aplikasi, dan persyaratan kepatuhan atau peraturan. Pola-pola ini memperluas arsitektur inti dan harus digunakan bersama dengan panduan arsitektur inti AWS SRA.

Panduan berikut memberikan pola arsitektur yang selaras dengan kemampuan keamanan tertentu:

- AWS SRA — manajemen identitas memberikan panduan tentang bagaimana menerapkan solusi manajemen identitas dan akses yang terukur, kuat, dan terpusat. AWS
- AWS SRA — keamanan perimeter membahas pola arsitektur dan Layanan AWS untuk menerapkan keamanan tepi di akun pusat atau di akun individu.
- AWS SRA — forensik cyber menjelaskan cara mengonfigurasi akun AWS Forensik sebagai titik awal untuk mengembangkan kemampuan forensik organisasi Anda dan untuk membantu meningkatkan kesiapsiagaan respons insiden keamanan (IR) Anda.

Panduan berikut memberikan pola arsitektur untuk jenis aplikasi tertentu. Anda mungkin ingin fokus pada hal ini setelah Anda membangun arsitektur keamanan dasar Anda:

- AWS SRA — Keamanan AI memberikan rekomendasi arsitektur keamanan untuk merancang dan membangun aplikasi yang menggabungkan kemampuan AI generatif dengan menggunakan layanan AI AWS generatif.
- AWS SRA — IoT memberikan rekomendasi arsitektur keamanan untuk merancang dan membangun aplikasi IoT. AWS

Selain itu, panduan berikut menjelaskan pola arsitektur yang selaras dengan kepatuhan atau kerangka peraturan tertentu:

- AWS Arsitektur Referensi Privasi (AWS PRA) menyediakan arsitektur keamanan untuk aplikasi yang memproses data pribadi dan harus mendukung persyaratan kepatuhan privasi yang luas seperti Peraturan Perlindungan Data Umum (GDPR), California Consumer Privacy Act (CCPA), atau Undang-Undang Perlindungan Data Umum Brasil (LGPD). AWS PRA menyediakan seperangkat pedoman yang khusus untuk desain dan konfigurasi kontrol privasi di Layanan AWS.

Kami menyarankan Anda memulai dengan panduan arsitektur inti AWS SRA untuk memahami arsitektur dasar dan kemudian berkonsultasi dengan panduan pelengkap untuk memanfaatkan fungsionalitas dan implementasi tingkat lanjut. Untuk informasi selengkapnya tentang kumpulan konten ini, lihat Arsitektur Referensi AWS Keamanan.

Diagram arsitektur

Untuk menyesuaikan diagram arsitektur referensi di perpustakaan AWS SRA berdasarkan kebutuhan bisnis Anda, Anda dapat mengunduh file.zip berikut dan mengekstrak isinya.

Unduh file sumber diagram (PowerPointformat Microsoft)

Nilai AWS SRA

Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

AWS memiliki serangkaian layanan keamanan dan keamanan yang besar (dan terus berkembang). Pelanggan telah menyatakan penghargaan atas informasi terperinci yang tersedia melalui dokumentasi layanan kami, posting blog, tutorial, pertemuan puncak, dan konferensi. Mereka juga memberi tahu kami bahwa mereka ingin lebih memahami gambaran besar dan mendapatkan pandangan strategis tentang layanan AWS keamanan. Ketika kami bekerja dengan pelanggan untuk mendapatkan apresiasi yang lebih dalam atas apa yang mereka butuhkan, tiga prioritas muncul:

- Pelanggan menginginkan informasi lebih lanjut dan pola yang direkomendasikan untuk bagaimana mereka dapat menyebarkan, mengkonfigurasi, dan mengoperasikan layanan AWS keamanan secara holistik. Di akun mana dan ke arah tujuan keamanan mana layanan harus digunakan dan dikelola? Apakah ada satu akun keamanan di mana semua atau sebagian besar layanan harus beroperasi? Bagaimana pilihan lokasi (unit organisasi atau Akun AWS) menginformasikan tujuan keamanan? Trade-off (pertimbangan desain) mana yang harus diperhatikan pelanggan?
- Pelanggan tertarik untuk melihat perspektif yang berbeda untuk secara logis mengatur banyak layanan AWS keamanan. Di luar fungsi utama setiap layanan (misalnya, layanan identitas atau layanan logging), sudut pandang alternatif ini membantu pelanggan merencanakan, merancang, dan mengimplementasikan arsitektur keamanan mereka. Contoh yang dibagikan nanti dalam dokumen ini mengelompokkan layanan berdasarkan lapisan perlindungan yang selaras dengan struktur AWS lingkungan yang direkomendasikan.
- Pelanggan mencari panduan dan contoh untuk mengintegrasikan layanan keamanan dengan cara yang paling efektif. Misalnya, bagaimana cara terbaik mereka menyelaraskan dan terhubung AWS Config dengan layanan lain untuk melakukan pekerjaan berat dalam audit otomatis dan jaringan pipa pemantauan? Pelanggan meminta panduan tentang bagaimana setiap layanan AWS keamanan mengandalkan, atau mendukung, layanan keamanan lainnya.

Kami membahas masing-masing ini di AWS SRA. Prioritas pertama dalam daftar (ke mana perginya) adalah fokus diagram arsitektur utama dan diskusi yang menyertainya dalam dokumen ini. Kami menyediakan AWS Organizations arsitektur yang direkomendasikan dan account-by-account deskripsi layanan mana yang pergi ke mana. Untuk memulai dengan prioritas kedua dalam daftar

(bagaimana memikirkan rangkaian lengkap layanan keamanan), baca bagian, Terapkan layanan keamanan di seluruh AWS organisasi Anda. Bagian ini menjelaskan cara untuk mengelompokkan layanan keamanan sesuai dengan struktur elemen dalam AWS organisasi Anda. Selain itu, ide-ide yang sama tercermin dalam diskusi tentang akun Aplikasi, yang menyoroti bagaimana layanan keamanan dapat dioperasikan untuk fokus pada lapisan akun tertentu: instance Amazon Elastic Compute Cloud (Amazon EC2), Amazon Virtual Private Cloud (Amazon VPC) jaringan, dan akun yang lebih luas. Akhirnya, prioritas ketiga (integrasi layanan) tercermin di seluruh panduan–terutama dalam diskusi layanan individu dalam panduan menyelam mendalam di perpustakaan SRA dan kode dalam repositori kode AWS SRA. AWS

Cara menggunakan AWS SRA

Ada berbagai cara untuk menggunakan AWS SRA tergantung di mana Anda berada dalam perjalanan adopsi cloud Anda. Berikut adalah daftar cara untuk mendapatkan wawasan paling banyak dari aset AWS SRA (diagram arsitektur, panduan tertulis, dan contoh kode).

- Tentukan status target untuk arsitektur keamanan Anda sendiri.

  Apakah Anda baru memulai AWS Cloud perjalanan Anda - menyiapkan set akun pertama Anda - atau berencana untuk meningkatkan AWS lingkungan yang mapan, AWS SRA adalah tempat untuk mulai membangun arsitektur keamanan Anda. Mulailah dengan fondasi komprehensif struktur akun dan layanan keamanan, dan kemudian sesuaikan berdasarkan tumpukan teknologi, keterampilan, tujuan keamanan, dan persyaratan kepatuhan khusus Anda. Jika Anda tahu Anda akan membangun dan meluncurkan lebih banyak beban kerja, Anda dapat mengambil versi AWS SRA yang disesuaikan dan menggunakannya sebagai dasar untuk arsitektur referensi keamanan organisasi Anda. Untuk mengetahui bagaimana Anda dapat mencapai status target yang dijelaskan oleh AWS SRA, lihat bagian Membangun arsitektur keamanan Anda — Pendekatan bertahap.
- Tinjau (dan revisi) desain dan kemampuan yang telah Anda terapkan.

  Jika Anda sudah memiliki desain dan implementasi keamanan, ada baiknya meluangkan waktu untuk membandingkan apa yang Anda miliki dengan AWS SRA. AWS SRA dirancang untuk menjadi komprehensif dan menyediakan dasar diagnostik untuk meninjau keamanan Anda sendiri. Di mana desain keamanan Anda selaras dengan AWS SRA, Anda dapat merasa lebih yakin bahwa Anda mengikuti praktik terbaik saat menggunakan. Layanan AWS Jika desain keamanan Anda berbeda atau bahkan tidak setuju dengan panduan di AWS SRA, ini tidak selalu merupakan tanda bahwa Anda melakukan sesuatu yang salah. Sebaliknya, pengamatan ini memberi Anda

kesempatan untuk meninjau proses keputusan Anda. Ada alasan bisnis dan teknologi yang sah mengapa Anda mungkin menyimpang dari praktik terbaik AWS SRA. Mungkin kepatuhan khusus, peraturan, atau persyaratan keamanan organisasi Anda memerlukan konfigurasi layanan tertentu. Atau, alih-alih menggunakan Layanan AWS, Anda mungkin memiliki preferensi fitur untuk produk dari AWS Partner Network atau aplikasi khusus yang Anda buat dan kelola. Terkadang, selama tinjauan ini, Anda mungkin menemukan bahwa keputusan Anda sebelumnya dibuat berdasarkan teknologi, AWS fitur, atau kendala bisnis lama yang tidak lagi berlaku. Ini adalah kesempatan yang baik untuk meninjau, memprioritaskan pembaruan apa pun, dan menambahkannya ke tempat yang sesuai dari backlog teknik Anda. Apa pun yang Anda temukan saat Anda menilai arsitektur keamanan Anda berdasarkan AWS SRA, Anda akan merasa berharga untuk mendokumentasikan analisis itu. Memiliki catatan sejarah keputusan dan pembenarannya dapat membantu menginformasikan dan memprioritaskan keputusan masa depan.

- Bootstrap implementasi arsitektur keamanan Anda sendiri.

  Modul AWS SRA Infrastructure as code (IAc) menyediakan cara yang cepat dan andal untuk mulai membangun dan menerapkan arsitektur keamanan Anda. Modul-modul ini dijelaskan lebih dalam di bagian repositori kode dan di repositori publik GitHub . Mereka tidak hanya memungkinkan para insinyur untuk membangun contoh pola berkualitas tinggi dalam panduan AWS SRA, tetapi mereka juga menggabungkan kontrol keamanan yang direkomendasikan seperti kebijakan kata sandi IAM, Amazon Simple Storage Service (Amazon S3) memblokir akses publik akun, Amazon EC2 default Amazon Elastic Block Store (Amazon EBS) enkripsi, dan AWS Control Tower integrasi dengan sehingga kontrol diterapkan atau dihapus saat baru sedang aktif papan atau dinonaktifkan. Akun AWS

- Pelajari lebih lanjut tentang layanan dan kemampuan AWS keamanan.

  Panduan dan diskusi dalam AWS SRA mencakup fitur-fitur penting serta pertimbangan penerapan dan manajemen untuk AWS keamanan individu dan layanan terkait keamanan. Salah satu fitur dari AWS SRA adalah bahwa ia memberikan pengenalan tingkat tinggi untuk luasnya layanan AWS keamanan dan bagaimana mereka bekerja sama dalam lingkungan multi-akun. Ini melengkapi penyelaman mendalam ke dalam fitur dan konfigurasi untuk setiap layanan yang ditemukan di sumber lain. Salah satu contohnya adalah diskusi tentang bagaimana AWS Security Hub Cloud Security Posture Management (AWS Security Hub CSPM) menyerap temuan keamanan dari berbagai Layanan AWS, AWS Partner produk, dan bahkan aplikasi Anda sendiri.

- Mendorong diskusi tentang tata kelola organisasi dan tanggung jawab untuk keamanan.

  Elemen penting dalam merancang dan menerapkan arsitektur atau strategi keamanan apa pun adalah memahami siapa di organisasi Anda yang memiliki tanggung jawab terkait keamanan.

Misalnya, pertanyaan tentang di mana mengumpulkan dan memantau temuan keamanan terkait dengan pertanyaan tim mana yang akan bertanggung jawab atas aktivitas tersebut. Apakah semua temuan di seluruh organisasi dipantau oleh tim pusat yang membutuhkan akses ke akun Security Tooling khusus? Atau apakah tim aplikasi individu (atau unit bisnis) bertanggung jawab atas kegiatan pemantauan tertentu dan oleh karena itu memerlukan akses ke alat peringatan dan pemantauan tertentu? Sebagai contoh lain, jika organisasi Anda memiliki grup yang mengelola semua kunci enkripsi secara terpusat, itu akan memengaruhi siapa yang memiliki izin untuk membuat AWS Key Management Service (AWS KMS) kunci dan akun mana kunci tersebut akan dikelola. Memahami karakteristik organisasi Anda — berbagai tim dan tanggung jawab — akan membantu Anda menyesuaikan SRA agar sesuai dengan kebutuhan Anda. AWS Sebaliknya, terkadang diskusi tentang arsitektur keamanan menjadi dorongan untuk membahas tanggung jawab organisasi yang ada dan mempertimbangkan potensi perubahan. AWS merekomendasikan proses pengambilan keputusan yang terdesentralisasi di mana tim beban kerja bertanggung jawab untuk menentukan kontrol keamanan berdasarkan fungsi dan persyaratan beban kerja mereka. Tujuan dari tim keamanan dan tata kelola terpusat adalah untuk membangun sistem yang memungkinkan pemilik beban kerja untuk membuat keputusan berdasarkan informasi dan bagi semua pihak untuk mendapatkan visibilitas konfigurasi, temuan, dan peristiwa. AWS SRA dapat menjadi kendaraan untuk mengidentifikasi dan menginformasikan diskusi ini.

Pedoman implementasi utama AWS SRA

Berikut adalah delapan takeaway utama dari AWS SRA yang perlu diingat saat Anda merancang dan menerapkan keamanan Anda.

- AWS Organizations dan strategi multi-akun yang tepat adalah elemen penting dari arsitektur keamanan Anda. Memisahkan beban kerja, tim, dan fungsi dengan benar memberikan dasar untuk pemisahan tugas dan defense-in-depth strategi. Panduan ini mencakup ini lebih lanjut di bagian selanjutnya.
- Defense-in-depth adalah pertimbangan desain penting untuk memilih kontrol keamanan untuk organisasi Anda. Ini membantu Anda menyuntikkan kontrol keamanan yang sesuai pada lapisan AWS Organizations struktur yang berbeda, yang membantu meminimalkan dampak masalah: Jika ada masalah dengan satu lapisan, ada kontrol di tempat yang mengisolasi sumber daya TI berharga lainnya. AWS SRA menunjukkan bagaimana Layanan AWS fungsi yang berbeda pada lapisan tumpukan AWS teknologi yang berbeda, dan bagaimana menggunakan layanan tersebut dalam kombinasi membantu Anda mencapainya. defense-in-depth defense-in-depthKonsep ini

dibahas AWS lebih lanjut di bagian selanjutnya dengan contoh desain yang ditunjukkan di bawah akun Aplikasi.

- Gunakan berbagai macam blok bangunan keamanan di beberapa fitur Layanan AWS dan untuk membangun infrastruktur cloud yang kuat dan tangguh. Saat menyesuaikan AWS SRA dengan kebutuhan khusus Anda, pertimbangkan tidak hanya fungsi utama Layanan AWS dan fitur (misalnya, otentikasi, enkripsi, pemantauan, kebijakan izin) tetapi juga bagaimana mereka cocok dengan struktur arsitektur Anda. Bagian selanjutnya dalam panduan ini menjelaskan bagaimana beberapa layanan beroperasi di seluruh AWS organisasi Anda. Layanan lain beroperasi paling baik dalam satu akun, dan beberapa dirancang untuk memberikan atau menolak izin kepada kepala sekolah individu. Mempertimbangkan kedua perspektif ini membantu Anda membangun pendekatan keamanan yang lebih fleksibel dan berlapis.
- Jika memungkinkan (seperti yang dijelaskan di bagian selanjutnya), manfaatkan Layanan AWS yang dapat digunakan di setiap akun (didistribusikan alih-alih terpusat) dan buat serangkaian pagar pembatas bersama yang konsisten yang dapat membantu melindungi beban kerja Anda dari penyalahgunaan dan membantu mengurangi dampak peristiwa keamanan. Penggunaan AWS SRA AWS Security Hub CSPM (pemantauan temuan terpusat dan pemeriksaan kepatuhan), Amazon GuardDuty (deteksi ancaman dan deteksi anomali), AWS Config (pemantauan sumber daya dan deteksi perubahan), IAM Access Analyzer (pemantauan akses sumber daya), AWS CloudTrail (aktivitas API layanan pencatatan di seluruh lingkungan Anda), dan Amazon Macie (klasifikasi data) sebagai kumpulan dasar untuk digunakan di setiap lokasi. Layanan AWS Akun AWS
- Manfaatkan fitur administrasi yang didelegasikan AWS Organizations, di mana ia didukung, seperti yang dijelaskan nanti di bagian administrasi yang didelegasikan dari panduan ini. Ini memungkinkan Anda untuk mendaftarkan akun AWS anggota sebagai administrator untuk layanan yang didukung. Administrasi yang didelegasikan memberikan fleksibilitas bagi tim yang berbeda dalam bisnis Anda untuk menggunakan akun terpisah, yang sesuai dengan tanggung jawab mereka, untuk mengelola Layanan AWS seluruh lingkungan. Selain itu, menggunakan administrator yang didelegasikan membantu Anda membatasi akses ke, dan mengelola overhead izin, akun manajemen. AWS Organizations
- Menerapkan pemantauan, manajemen, dan tata kelola terpusat di seluruh organisasi Anda AWS . Dengan menggunakan agregasi multi-akun (dan terkadang Multi-wilayah), bersama dengan fitur administrasi Layanan AWS yang didelegasikan, Anda memberdayakan tim keamanan pusat, jaringan, dan rekayasa cloud Anda untuk memiliki visibilitas dan kontrol yang luas atas konfigurasi keamanan dan pengumpulan data yang sesuai. Selain itu, data dapat diberikan kembali ke tim beban kerja untuk memberdayakan mereka membuat keputusan keamanan yang efektif sebelumnya dalam siklus hidup pengembangan perangkat lunak (SDLC).

- Gunakan AWS Control Tower untuk mengatur dan mengatur AWS lingkungan multi-akun Anda dengan penerapan kontrol keamanan pra-bangun untuk mem-bootstrap build arsitektur referensi keamanan Anda. AWS Control Tower menyediakan cetak biru untuk menyediakan manajemen identitas, akses federasi ke akun, pencatatan terpusat, dan alur kerja yang ditentukan untuk penyediaan akun tambahan. Anda kemudian dapat menggunakan solusi Customizations for AWS Control Tower (CFCT) untuk mendasarkan akun yang dikelola AWS Control Tower dengan kontrol keamanan tambahan, konfigurasi layanan, dan tata kelola, seperti yang ditunjukkan oleh repositori kode SRA. AWS Fitur pabrik akun secara otomatis menyediakan akun baru dengan templat yang dapat dikonfigurasi berdasarkan konfigurasi akun yang disetujui untuk menstandarisasi akun dalam organisasi Anda. AWS Anda juga dapat memperluas tata kelola kepada individu yang ada Akun AWS dengan mendaftarkannya ke unit organisasi (OU) yang sudah diatur oleh. AWS Control Tower
- Contoh kode AWS SRA menunjukkan bagaimana Anda dapat mengotomatiskan implementasi pola dalam panduan AWS SRA dengan menggunakan infrastruktur sebagai kode (IAc). Dengan mengkodifikasi pola, Anda dapat memperlakukan IAc seperti aplikasi lain di organisasi Anda, dan mengotomatiskan pengujian sebelum Anda menerapkan kode. IAc juga membantu memastikan konsistensi dan pengulangan dengan menerapkan pagar pembatas di beberapa lingkungan (misalnya, SDLC atau khusus Wilayah). Contoh kode SRA dapat digunakan di lingkungan AWS Organizations multi-akun dengan atau tanpa. AWS Control Tower Solusi dalam repositori ini yang memerlukan AWS Control Tower telah diterapkan dan diuji di AWS Control Tower lingkungan dengan menggunakan AWS CloudFormation dan Kustomisasi untuk (CFCT). AWS Control Tower Solusi yang tidak memerlukan AWS Control Tower telah diuji di AWS Organizations lingkungan dengan menggunakan AWS CloudFormation. Jika Anda tidak menggunakan AWS Control Tower, Anda dapat menggunakan solusi penyebaran AWS Organizations berbasis.

Fondasi keamanan

Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

AWS SRA sejalan dengan tiga fondasi AWS keamanan: AWS Cloud Adoption Framework (AWS CAF), AWS Well-Architected, dan Shared Responsibility Model. AWS

AWS Layanan Profesional menciptakan AWS CAF untuk membantu perusahaan merancang dan mengikuti jalur yang dipercepat menuju adopsi cloud yang sukses. Panduan dan praktik terbaik yang disediakan oleh kerangka kerja membantu Anda membangun pendekatan komprehensif untuk komputasi awan di seluruh perusahaan Anda dan di seluruh siklus hidup TI Anda. AWS CAF mengatur panduan ke dalam enam bidang fokus, yang disebut perspektif. Setiap perspektif mencakup tanggung jawab berbeda yang dimiliki atau dikelola oleh pemangku kepentingan yang terkait secara fungsional. Secara umum, perspektif bisnis, orang, dan tata kelola fokus pada kemampuan bisnis; sedangkan perspektif platform, keamanan, dan operasi fokus pada kemampuan teknis.

Perspektif keamanan AWS CAF membantu Anda menyusun pemilihan dan implementasi kontrol di seluruh bisnis Anda. Mengikuti AWS rekomendasi saat ini di pilar keamanan dapat membantu Anda memenuhi persyaratan bisnis dan peraturan Anda.

AWS Well-Architected membantu arsitek cloud membangun infrastruktur yang aman, berkinerja tinggi, tangguh, dan efisien untuk aplikasi dan beban kerja mereka. Kerangka kerja ini didasarkan pada enam pilar—keunggulan operasional, keamanan, keandalan, efisiensi kinerja, optimalisasi biaya, dan keberlanjutan—dan memberikan pendekatan yang konsisten bagi AWS pelanggan dan Mitra untuk mengevaluasi arsitektur dan menerapkan desain yang dapat disesuaikan dari waktu ke waktu. Kami meyakini bahwa memiliki beban kerja yang didesain dengan baik akan meningkatkan peluang keberhasilan bisnis.

Pilar keamanan Well-Architected Framework menjelaskan cara memanfaatkan teknologi cloud untuk membantu melindungi data, sistem, dan aset dengan cara yang dapat meningkatkan postur keamanan Anda. Ini akan membantu Anda memenuhi persyaratan bisnis dan peraturan Anda dengan mengikuti AWS rekomendasi saat ini. Ada area fokus Well-Architected Framework tambahan yang menyediakan lebih banyak konteks untuk domain tertentu seperti tata kelola, tanpa server, AI/ML, dan game. Lensa ini dikenal sebagai lensa AWS Well-Architected.

Keamanan dan kepatuhan adalah tanggung jawab bersama antara AWS dan pelanggan. Model bersama ini dapat membantu meringankan beban operasional Anda saat AWS mengoperasikan, mengelola, dan mengontrol komponen dari sistem operasi host dan lapisan virtualisasi hingga keamanan fisik fasilitas tempat layanan beroperasi. Misalnya, Anda memikul tanggung jawab dan pengelolaan sistem operasi tamu (termasuk pembaruan dan patch keamanan), perangkat lunak aplikasi, enkripsi data sisi server, tabel rute lalu lintas jaringan, dan konfigurasi firewall grup keamanan AWS yang disediakan. Untuk layanan abstrak seperti Amazon S3 dan Amazon DynamoDB AWS , mengoperasikan lapisan infrastruktur, sistem operasi, dan platform, dan Anda mengakses titik akhir untuk menyimpan dan mengambil data. Anda bertanggung jawab untuk mengelola data Anda (termasuk opsi enkripsi), mengklasifikasikan aset Anda, dan menggunakan alat IAM untuk menerapkan izin yang sesuai. Model bersama ini sering dijelaskan dengan mengatakan bahwa AWS bertanggung jawab atas keamanan cloud (yaitu, untuk melindungi infrastruktur yang menjalankan semua layanan yang ditawarkan di AWS Cloud), dan Anda bertanggung jawab atas keamanan di cloud (sebagaimana ditentukan oleh AWS Cloud layanan yang Anda pilih).

Dalam panduan yang diberikan oleh dokumen-dokumen dasar ini, dua set konsep sangat relevan dengan desain dan pemahaman AWS SRA: kemampuan keamanan dan prinsip-prinsip desain keamanan.

Kemampuan keamanan

Perspektif keamanan AWS CAF menguraikan sembilan kemampuan yang membantu Anda mencapai kerahasiaan, integritas, dan ketersediaan data dan beban kerja cloud Anda.

- Tata kelola keamanan untuk mengembangkan dan mengkomunikasikan peran, tanggung jawab, kebijakan, proses, dan prosedur keamanan di seluruh AWS lingkungan organisasi Anda.
- Jaminan keamanan untuk memantau, mengevaluasi, mengelola, dan meningkatkan efektivitas program keamanan dan privasi Anda.
- Manajemen identitas dan akses untuk mengelola identitas dan izin dalam skala besar.
- Deteksi ancaman untuk memahami dan mengidentifikasi potensi kesalahan konfigurasi keamanan, ancaman, atau perilaku tak terduga.
- Manajemen kerentanan untuk terus mengidentifikasi, mengklasifikasikan, memulihkan, dan mengurangi kerentanan keamanan.
- Perlindungan infrastruktur untuk membantu memvalidasi bahwa sistem dan layanan dalam beban kerja Anda dilindungi.

- Perlindungan data untuk menjaga visibilitas dan kontrol atas data, dan bagaimana data diakses dan digunakan di organisasi Anda.
- Keamanan aplikasi untuk membantu mendeteksi dan mengatasi kerentanan keamanan selama proses pengembangan perangkat lunak.
- Respon insiden untuk mengurangi potensi bahaya dengan secara efektif menanggapi insiden keamanan.

Prinsip desain keamanan

Pilar keamanan dari Well-Architected Framework menangkap seperangkat tujuh prinsip desain yang mengubah area keamanan tertentu menjadi panduan praktis yang dapat membantu Anda memperkuat keamanan beban kerja Anda. Di mana kemampuan keamanan membingkai strategi keamanan secara keseluruhan, prinsip-prinsip Well-Architected Framework ini menjelaskan apa yang dapat Anda mulai lakukan. Mereka tercermin dengan sangat sengaja dalam AWS SRA ini dan terdiri dari yang berikut:

- Menerapkan fondasi identitas yang kuat - Menerapkan prinsip hak istimewa terkecil, dan menegakkan pemisahan tugas dengan otorisasi yang sesuai untuk setiap interaksi dengan sumber daya Anda. AWS Pusatkan manajemen identitas, dan targetkan untuk tidak bergantung pada kredensial statis jangka panjang.
- Aktifkan ketertelusuran - Pantau, hasilkan peringatan, dan audit tindakan dan perubahan lingkungan Anda secara real time. Integrasikan pengumpulan log dan metrik dengan sistem agar dapat bertindak berdasarkan investigasi yang berjalan otomatis.
- Terapkan keamanan di semua lapisan - Terapkan defense-in-depth pendekatan dengan beberapa kontrol keamanan. Terapkan beberapa jenis kontrol (misalnya, kontrol preventif dan detektif) ke semua lapisan, termasuk edge of network, virtual private cloud (VPC), load balancing, layanan instance dan komputasi, sistem operasi, konfigurasi aplikasi, dan kode.
- Mengotomatiskan praktik terbaik keamanan - Mekanisme keamanan berbasis perangkat lunak otomatis meningkatkan kemampuan Anda untuk menskalakan secara aman lebih cepat dan hemat biaya. Buat arsitektur yang aman, dan terapkan kontrol yang didefinisikan dan dikelola sebagai kode dalam templat yang dikendalikan versi.
- Lindungi data dalam perjalanan dan saat istirahat - Klasifikasi data Anda ke dalam tingkat sensitivitas dan gunakan mekanisme seperti enkripsi, tokenisasi, dan kontrol akses jika sesuai.

- Jauhkan orang dari data — Gunakan mekanisme dan alat untuk mengurangi atau menghilangkan kebutuhan untuk langsung mengakses atau memproses data secara manual. Ini akan mengurangi risiko kekeliruan atau perubahan dan kesalahan manusia dalam penanganan data sensitif.
- Bersiaplah untuk acara keamanan - Mempersiapkan insiden dengan memiliki manajemen insiden dan kebijakan investigasi dan proses yang sesuai dengan kebutuhan organisasi Anda. Jalankan simulasi tanggap-insiden dan gunakan alat dengan otomatisasi untuk mempercepat deteksi, investigasi, dan pemulihan.

Cara menggunakan AWS SRA dengan AWS CAF dan AWS Well-Architected Framework

AWS CAF, AWS Well-Architected Framework, AWS dan SRA adalah kerangka kerja pelengkap yang bekerja sama untuk mendukung upaya migrasi dan modernisasi cloud Anda.

- AWS CAF memanfaatkan AWS pengalaman dan praktik terbaik untuk membantu Anda menyelaraskan nilai-nilai adopsi cloud dengan hasil bisnis yang Anda inginkan. Gunakan AWS CAF untuk mengidentifikasi dan memprioritaskan peluang transformasi, mengevaluasi dan meningkatkan kesiapan cloud, dan secara berulang mengembangkan peta jalan transformasi Anda.
- AWS Well-Architected Framework AWS memberikan rekomendasi untuk membangun infrastruktur yang aman, berkinerja tinggi, tangguh, dan efisien untuk berbagai aplikasi dan beban kerja yang memenuhi hasil bisnis Anda.
- AWS SRA membantu Anda memahami cara menerapkan dan mengatur layanan keamanan dengan cara yang selaras dengan rekomendasi AWS CAF dan Well-Architected Framework. AWS

Misalnya, perspektif keamanan AWS CAF menyarankan agar Anda mengevaluasi cara mengelola identitas tenaga kerja Anda secara terpusat dan otentikasi mereka. AWS Berdasarkan informasi ini, Anda dapat memutuskan untuk menggunakan solusi penyedia identitas perusahaan (iDP) baru atau yang sudah ada seperti Okta, Active Directory, atau Ping Identity untuk tujuan ini. Anda mengikuti panduan dalam AWS Well-Architected Framework dan memutuskan untuk mengintegrasikan IDP Anda dengan untuk memberi karyawan Anda pengalaman masuk tunggal AWS IAM Identity Center yang dapat menyinkronkan keanggotaan dan izin grup mereka. Anda meninjau rekomendasi AWS SRA untuk mengaktifkan Pusat Identitas IAM di akun manajemen AWS organisasi Anda dan mengelolanya melalui akun alat keamanan yang digunakan oleh tim operasi keamanan Anda. Contoh

ini menggambarkan bagaimana AWS CAF membantu Anda membuat keputusan awal tentang postur keamanan yang Anda inginkan, Kerangka Kerja AWS Well-Architected memberikan panduan tentang cara mengevaluasi Layanan AWS yang tersedia untuk memenuhi tujuan itu, dan AWS SRA kemudian memberikan rekomendasi tentang cara menerapkan dan mengatur layanan keamanan yang Anda pilih.

Blok bangunan SRA — AWS Organizations, akun, dan pagar pembatas

Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

AWS Layanan keamanan, kontrol, dan interaksi mereka paling baik digunakan di atas dasar strategi AWS multi-akun dan identitas dan pagar manajemen akses. Pagar pembatas ini menetapkan kemampuan untuk implementasi Anda dengan hak istimewa yang paling sedikit, pemisahan tugas, dan privasi, dan memberikan dukungan untuk keputusan tentang jenis kontrol apa yang diperlukan, di mana setiap layanan keamanan dikelola, dan bagaimana mereka dapat berbagi data dan izin di SRA. AWS

An Akun AWS menyediakan batasan keamanan, akses, dan penagihan untuk AWS sumber daya Anda dan memungkinkan Anda mencapai kemandirian dan isolasi sumber daya. Penggunaan beberapa Akun AWS memainkan peran penting dalam cara Anda memenuhi persyaratan keamanan Anda, seperti yang dibahas dalam Manfaat menggunakan beberapa Akun AWS bagian dari Mengatur AWS lingkungan Anda menggunakan whitepaper beberapa akun. Misalnya, Anda dapat mengatur beban kerja Anda di akun terpisah dan akun grup dalam unit organisasi (OU) berdasarkan fungsi, persyaratan kepatuhan, atau serangkaian kontrol umum alih-alih mencerminkan struktur pelaporan perusahaan Anda. Ingatlah keamanan dan infrastruktur untuk memungkinkan perusahaan Anda menetapkan pagar pembatas umum seiring dengan bertambahnya beban kerja Anda. Pendekatan ini memberikan batasan dan kontrol yang kuat antara beban kerja. Pemisahan tingkat akun, dalam kombinasi dengan AWS Organizations, digunakan untuk mengisolasi lingkungan produksi dari lingkungan pengembangan dan pengujian, atau untuk memberikan batas logis yang kuat antara beban kerja yang memproses data dari klasifikasi yang berbeda seperti Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) atau Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA). Meskipun Anda mungkin memulai AWS perjalanan Anda dengan satu akun, AWS menyarankan agar Anda menyiapkan beberapa akun karena beban kerja Anda bertambah besar dan kompleksitas.

Izin memungkinkan Anda menentukan akses ke AWS sumber daya. Izin diberikan kepada entitas IAM yang dikenal sebagai prinsipal (pengguna, grup, dan peran). Secara default, prinsipal dimulai tanpa izin. Prinsipal IAM tidak dapat melakukan apa pun AWS sampai Anda memberi mereka izin,

dan Anda dapat menyiapkan pagar pembatas yang berlaku seluas seluruh AWS organisasi Anda atau sehalus kombinasi individu dari prinsip, tindakan, sumber daya, dan kondisi.

Menggunakan AWS Organizations untuk keamanan

> Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

AWS Organizationsmembantu Anda mengelola dan mengatur lingkungan Anda secara terpusat saat Anda tumbuh dan meningkatkan sumber daya Anda AWS . Dengan menggunakan AWS Organizations, Anda dapat membuat yang baru secara terprogram Akun AWS, mengalokasikan sumber daya, mengelompokkan akun untuk mengatur beban kerja, dan menerapkan kebijakan ke akun atau grup akun untuk tata kelola. Sebuah AWS organisasi mengkonsolidasikan Anda Akun AWS sehingga Anda dapat mengelolanya sebagai satu unit. Ini memiliki satu akun manajemen bersama dengan nol atau lebih akun anggota. Sebagian besar beban kerja Anda berada di akun anggota, kecuali untuk beberapa proses yang dikelola secara terpusat yang harus berada di akun manajemen atau di akun yang ditetapkan sebagai administrator yang didelegasikan untuk spesifik. Layanan AWS Anda dapat menyediakan alat dan akses dari lokasi pusat untuk tim keamanan Anda untuk mengelola kebutuhan keamanan atas nama AWS organisasi. Anda dapat mengurangi duplikasi sumber daya dengan berbagi sumber daya penting dalam AWS organisasi Anda. Anda dapat mengelompokkan akun ke dalam unit AWS organisasi (OUs), yang dapat mewakili lingkungan yang berbeda berdasarkan persyaratan dan tujuan beban kerja. AWS Organizations juga menyediakan beberapa kebijakan yang memungkinkan Anda menerapkan kontrol keamanan tambahan secara terpusat ke semua akun anggota di organisasi Anda. Bagian ini berfokus pada kebijakan kontrol layanan (SCPs), kebijakan kontrol sumber daya (RCPs), dan kebijakan deklaratif.

Dengan AWS Organizations, Anda dapat menggunakan SCPsdan RCPsmenerapkan pagar pembatas izin di tingkat AWS organisasi, OU, atau akun. SCPs adalah pagar pembatas yang berlaku untuk kepala sekolah dalam akun organisasi, dengan pengecualian akun manajemen (yang merupakan salah satu alasan untuk tidak menjalankan beban kerja di akun ini). Ketika Anda melampirkan SCP ke OU, SCP diwarisi oleh anak OUs dan akun di bawah OU tersebut. SCPs tidak memberikan izin apa pun. Sebagai gantinya, mereka menentukan izin maksimum yang tersedia untuk kepala sekolah Anda di AWS organisasi, OU, atau akun. Anda masih perlu melampirkan kebijakan berbasis identitas atau berbasis sumber daya ke prinsipal atau sumber daya di Anda untuk benar-benar memberikan izin kepada mereka. Akun AWS Misalnya, jika SCP menolak akses ke semua Amazon S3, prinsipal yang terpengaruh oleh SCP tidak akan memiliki akses ke Amazon S3 bahkan

jika mereka secara eksplisit diberikan akses melalui kebijakan IAM. Untuk informasi lebih lanjut tentang bagaimana kebijakan IAM dievaluasi, peran SCPs, dan bagaimana akses akhirnya diberikan atau ditolak, lihat Logika evaluasi kebijakan dalam dokumentasi IAM.

RCPs adalah pagar pembatas yang berlaku untuk sumber daya dalam akun organisasi, terlepas dari apakah sumber daya milik organisasi yang sama. Seperti SCPs, RCPs jangan memengaruhi sumber daya di akun manajemen dan jangan berikan izin apa pun. Ketika Anda melampirkan RCP ke OU, RCP diwarisi oleh anak OUs dan akun di bawah OU. RCPs memberikan kontrol pusat atas izin maksimum yang tersedia untuk sumber daya di organisasi Anda dan saat ini mendukung sebagian dari. Layanan AWS Saat Anda mendesain SCPs untuk Anda OUs, kami sarankan Anda mengevaluasi perubahan dengan menggunakan simulator kebijakan IAM. Anda juga harus meninjau data layanan yang terakhir diakses di IAM dan menggunakannya AWS CloudTrail untuk mencatat penggunaan layanan di tingkat API untuk memahami potensi dampak perubahan SCP.

SCPs dan RCPs merupakan kontrol independen. Anda dapat memilih untuk mengaktifkan saja SCPs atau RCPs, atau menggunakan kedua jenis kebijakan bersama-sama berdasarkan kontrol akses yang ingin Anda terapkan. Misalnya, jika Anda ingin mencegah prinsipal organisasi mengakses sumber daya di luar organisasi, Anda menerapkan kontrol ini dengan menggunakan. SCPs Jika Anda ingin membatasi atau mencegah identitas eksternal mengakses sumber daya Anda, Anda menerapkan kontrol ini dengan menggunakan. RCPs Untuk informasi selengkapnya dan kasus penggunaan untuk RCPs dan SCPs, lihat Menggunakan SCPs dan RCPs dalam AWS Organizations dokumentasi.

Anda dapat menggunakan kebijakan AWS Organizations deklaratif untuk mendeklarasikan dan menerapkan konfigurasi yang Anda inginkan secara terpusat pada skala tertentu Layanan AWS di seluruh organisasi. Misalnya, Anda dapat memblokir akses internet publik ke sumber daya Amazon VPC di seluruh organisasi Anda. Tidak seperti kebijakan otorisasi seperti SCPs dan RCPs, kebijakan deklaratif diberlakukan di bidang kontrol AWS layanan. Kebijakan otorisasi mengatur akses ke APIs, sedangkan kebijakan deklaratif diterapkan langsung di tingkat layanan untuk menegakkan maksud tahan lama. Kebijakan ini membantu memastikan bahwa konfigurasi dasar untuk sebuah selalu Layanan AWS dipertahankan, bahkan ketika layanan memperkenalkan fitur baru atau. APIs Konfigurasi dasar juga dipertahankan ketika akun baru ditambahkan ke organisasi atau ketika prinsip dan sumber daya baru dibuat. Kebijakan deklaratif dapat diterapkan ke seluruh organisasi atau untuk spesifik OUs atau akun.

Setiap Akun AWS memiliki satu pengguna root yang memiliki izin penuh untuk semua AWS sumber daya secara default. Sebagai praktik keamanan terbaik, kami menyarankan Anda untuk tidak menggunakan pengguna root kecuali untuk beberapa tugas yang secara eksplisit memerlukan

pengguna root. Jika Anda mengelola beberapa Akun AWS melalui AWS Organizations, Anda dapat menonaktifkan login root secara terpusat dan kemudian melakukan tindakan hak istimewa root atas nama semua akun anggota. Setelah Anda mengelola akses root untuk akun anggota secara terpusat, Anda dapat menghapus kata sandi pengguna root, kunci akses, dan menandatangani sertifikat, dan menonaktifkan otentikasi multi-faktor (MFA) untuk akun anggota. Akun baru yang dibuat di bawah akses root yang dikelola secara terpusat tidak memiliki kredenal pengguna root secara default. Akun anggota tidak dapat masuk dengan pengguna root mereka atau melakukan pemulihan kata sandi untuk pengguna root mereka.

AWS Control Towermenawarkan cara yang disederhanakan untuk mengatur dan mengatur beberapa akun. Ini mengotomatiskan pengaturan akun di AWS organisasi Anda, mengotomatiskan penyediaan, menerapkan kontrol (yang mencakup kontrol preventif dan detektif), dan memberi Anda dasbor untuk visibilitas. Kebijakan manajemen IAM tambahan, batas izin, dilampirkan ke prinsipal IAM tertentu (pengguna atau peran) dan menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada prinsipal IAM.

AWS Organizations membantu Anda mengonfigurasi Layanan AWSyang berlaku untuk semua akun Anda. Misalnya, Anda dapat mengonfigurasi pencatatan pusat dari semua tindakan yang dilakukan di seluruh AWS organisasi dengan menggunakan CloudTrail, dan mencegah akun anggota menonaktifkan pencatatan. Anda juga dapat menggabungkan data secara terpusat untuk aturan yang telah Anda tetapkan dengan menggunakan AWS Config, sehingga Anda dapat mengaudit beban kerja Anda untuk kepatuhan dan bereaksi cepat terhadap perubahan. Anda dapat menggunakan AWS CloudFormation StackSetsuntuk mengelola CloudFormation tumpukan secara terpusat di seluruh akun dan OUs di AWS organisasi Anda, sehingga Anda dapat secara otomatis menyediakan akun baru untuk memenuhi persyaratan keamanan Anda.

Konfigurasi default AWS Organizations dukungan menggunakan SCPs sebagai daftar penolakan. Dengan menggunakan strategi daftar tolak, administrator akun anggota dapat mendelegasikan semua layanan dan tindakan sampai Anda membuat dan melampirkan SCP yang menolak layanan atau serangkaian tindakan tertentu. Pernyataan penolakan memerlukan pemeliharaan yang lebih sedikit daripada daftar izinkan, karena Anda tidak perlu memperbaruinya saat AWS menambahkan layanan baru. Pernyataan penolakan biasanya lebih pendek dalam panjang karakter, jadi lebih mudah untuk tetap dalam ukuran maksimum untuk SCPs. Dalam pernyataan di mana `Effect` elemen memiliki nilai`Deny`, Anda juga dapat membatasi akses ke sumber daya tertentu, atau menentukan kondisi kapan SCPs berlaku. Sebaliknya, `Allow` pernyataan dalam SCP berlaku untuk semua sumber daya (`"*"`) dan tidak dapat dibatasi oleh kondisi. Untuk informasi dan contoh selengkapnya, lihat Strategi untuk digunakan SCPs dalam AWS Organizations dokumentasi.

Pertimbangan desain

- Atau, untuk digunakan SCPs sebagai daftar izin, Anda harus mengganti `FullAWSAccess` SCP yang dikelola AWS dengan SCP yang secara eksplisit hanya mengizinkan layanan dan tindakan yang ingin Anda izinkan. Agar izin diaktifkan untuk akun tertentu, setiap SCP (dari root melalui setiap OU di jalur langsung ke akun dan bahkan dilampirkan ke akun itu sendiri) harus mengizinkan izin itu. Model ini bersifat lebih ketat dan mungkin cocok untuk beban kerja yang sangat diatur dan sensitif. Pendekatan ini mengharuskan Anda untuk secara eksplisit mengizinkan setiap layanan atau tindakan IAM di jalur dari Akun AWS ke OU.
- Idealnya, Anda akan menggunakan kombinasi daftar tolak dan mengizinkan strategi daftar. Gunakan daftar izinkan untuk menentukan daftar yang diizinkan Layanan AWS disetujui untuk digunakan dalam suatu AWS organisasi dan lampirkan SCP ini di akar AWS organisasi Anda. Jika Anda memiliki serangkaian layanan berbeda yang diizinkan per lingkungan pengembangan Anda, Anda akan melampirkan masing-masing SCPs di setiap OU. Anda kemudian dapat menggunakan daftar penolakan untuk menentukan pagar pembatas perusahaan dengan secara eksplisit menolak tindakan IAM tertentu.
- RCPs berlaku untuk sumber daya untuk subset. Layanan AWS Untuk informasi selengkapnya, lihat Daftar dukungan Layanan AWS tersebut RCPs dalam AWS Organizations dokumentasi. Konfigurasi default AWS Organizations dukungan menggunakan RCPs sebagai daftar penolakan. Ketika Anda mengaktifkan RCPs di organisasi Anda, kebijakan AWS terkelola yang `RCPFullAWSAccess` disebut secara otomatis dilampirkan ke root organisasi, setiap OU, dan setiap akun di organisasi Anda. Anda tidak dapat melepaskan kebijakan ini. RCP default ini memungkinkan semua prinsipal dan tindakan akses untuk melewati evaluasi RCP. Ini berarti bahwa sampai Anda mulai membuat dan melampirkan RCPs, semua izin IAM Anda yang ada terus beroperasi seperti yang mereka lakukan. Kebijakan AWS terkelola ini tidak memberikan akses. Anda kemudian dapat membuat yang baru RCPs sebagai daftar pernyataan penolakan untuk memblokir akses ke sumber daya di organisasi Anda.

Akun manajemen, akses tepercaya, dan administrator yang didelegasikan

Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

Akun manajemen (juga disebut akun Manajemen AWS Organisasi atau akun Manajemen Org) unik dan dibedakan dari setiap akun lainnya di AWS Organizations. Ini adalah akun yang menciptakan AWS organisasi. Dari akun ini, Anda dapat membuat Akun AWS di AWS organisasi, mengundang akun lain yang ada ke AWS organisasi (kedua jenis dianggap sebagai akun anggota), menghapus akun dari AWS organisasi, dan menerapkan kebijakan IAM ke root, OUs, atau akun dalam AWS organisasi.

Akun manajemen menyebarkan pagar keamanan universal melalui SCPs, RCPs, dan penyebaran layanan (seperti CloudTrail) yang akan memengaruhi semua akun anggota dalam organisasi. AWS Untuk lebih membatasi izin di akun manajemen, izin tersebut dapat didelegasikan ke akun lain yang sesuai, seperti akun keamanan, jika memungkinkan.

Akun manajemen memiliki tanggung jawab Akun Pembayar dan bertanggung jawab untuk membayar semua biaya yang diperoleh oleh akun anggota. Anda tidak dapat mengganti akun manajemen AWS organisasi. Seorang Akun AWS dapat menjadi anggota hanya satu AWS organisasi pada satu waktu.

Karena fungsionalitas dan ruang lingkup pengaruh yang dimiliki akun manajemen, kami menyarankan Anda membatasi akses ke akun ini dan memberikan izin hanya untuk peran yang membutuhkannya. Dua fitur yang membantu Anda melakukan ini adalah akses tepercaya dan administrator yang didelegasikan. Anda dapat menggunakan akses tepercaya untuk mengaktifkan Layanan AWS yang Anda tentukan, yang disebut layanan tepercaya, untuk melakukan tugas di AWS organisasi Anda dan akunnya atas nama Anda. Ini melibatkan pemberian izin untuk layanan terpercaya tetapi tidak mempengaruhi izin untuk pengguna atau peran IAM. Anda dapat menggunakan akses tepercaya untuk menentukan setelan dan detail konfigurasi yang ingin disimpan oleh layanan tepercaya di akun AWS organisasi atas nama Anda. Misalnya, bagian akun Manajemen Org di AWS SRA menjelaskan cara memberikan CloudTrail layanan akses tepercaya untuk membuat jejak CloudTrail organisasi di semua akun di AWS organisasi Anda.

Beberapa Layanan AWS mendukung fitur administrator yang didelegasikan di AWS Organizations. Dengan fitur ini, layanan yang kompatibel dapat mendaftarkan akun AWS anggota di AWS organisasi sebagai administrator untuk akun AWS organisasi dalam layanan tersebut. Kemampuan ini

memberikan fleksibilitas bagi tim yang berbeda dalam perusahaan Anda untuk menggunakan akun terpisah, yang sesuai dengan tanggung jawab mereka, untuk mengelola Layanan AWS seluruh lingkungan. Layanan AWS keamanan di AWS SRA yang saat ini mendukung administrator yang didelegasikan termasuk IAM Identity Center,,, AWS Firewall Manager Amazon AWS Config, IAM Access GuardDuty Analyzer, Amazon Macie, Cloud Security Posture Management () AWS Security Hub , Amazon Detective AWS Security Hub CSPM, Amazon Inspector, dan. AWS Audit Manager AWS Systems Manager Penggunaan fitur administrator yang didelegasikan ditekankan dalam AWS SRA sebagai praktik terbaik, dan kami mendelegasikan administrasi layanan terkait keamanan ke akun Security Tooling.

Struktur akun khusus

> Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

An Akun AWS menyediakan batasan keamanan, akses, dan penagihan untuk AWS sumber daya Anda, dan memungkinkan Anda mencapai kemandirian dan isolasi sumber daya. Secara default, tidak ada akses yang diizinkan antar akun.

Saat merancang struktur OU dan akun Anda, mulailah dengan mempertimbangkan keamanan dan infrastruktur. Sebaiknya buat satu set dasar OUs untuk fungsi-fungsi spesifik ini, dibagi menjadi Infrastruktur dan Keamanan OUs. Rekomendasi OU dan akun ini menangkap sebagian dari pedoman kami yang lebih luas AWS Organizations dan lebih komprehensif untuk desain struktur multi-akun. Untuk serangkaian rekomendasi lengkap, lihat Mengatur AWS lingkungan Anda menggunakan beberapa akun dalam AWS dokumentasi dan posting blog Praktik terbaik untuk unit organisasi dengan AWS Organizations.

AWS SRA menggunakan akun berikut untuk mencapai operasi keamanan yang efektif. AWS Akun khusus ini membantu memastikan pemisahan tugas, mendukung kebijakan tata kelola dan akses yang berbeda untuk berbagai aplikasi dan data sensitif, dan membantu mengurangi dampak peristiwa keamanan. Dalam diskusi berikutnya, kami berfokus pada akun produksi (prod) dan beban kerja terkait. Akun siklus hidup pengembangan perangkat lunak (SDLC) (sering disebut akun dev dan pengujian) dimaksudkan untuk pementasan kiriman dan dapat beroperasi di bawah kebijakan keamanan yang berbeda yang ditetapkan dari akun produksi.

Akun	OU	Peran keamanan

Manajemen	—	Tata kelola pusat dan manajemen semua Wilayah AWS dan akun. Akun AWS Yang menjadi tuan rumah akar AWS organisasi.
Perkakas Keamanan	Keamanan	Didedikasikan Akun AWS untuk mengoperasikan layanan keamanan yang berlaku secara luas (seperti GuardDuty, Security Hub CSPM, Audit Manager, Detective, Amazon Inspector, AWS Config dan), Akun AWS memantau, dan mengotoma tiskan peringatan dan respons keamanan. (Dalam AWS Control Tower, nama default untuk akun di bawah Security OU adalah akun Audit.)
Arsip Log	Keamanan	Didedikasikan Akun AWS untuk menelan dan mengarsip kan semua logging dan backup untuk semua dan. Wilayah AWS Akun AWS Ini harus dirancang sebagai penyimpanan yang tidak dapat diubah.

Jaringan	Infrastruktur	Gateway antara aplikasi Anda dan internet yang lebih luas. Akun Jaringan mengisolasi layanan jaringan, konfigura si, dan operasi yang lebih luas dari beban kerja aplikasi individual, keamanan, dan infrastruktur lainnya.
Layanan Bersama	Infrastruktur	Akun ini mendukung layanan yang digunakan beberapa aplikasi dan tim untuk memberikan hasil mereka. Contohnya termasuk layanan direktori Pusat Identitas (Direktori Aktif), layanan pesan, dan layanan metadata.
Aplikasi	Beban kerja	Akun AWS yang menampung aplikasi AWS organisasi dan melakukan beban kerja. (Ini kadang-kadang disebut akun Beban Kerja.) Akun aplikasi harus dibuat untuk mengisola si layanan perangkat lunak alih-alih dipetakan ke tim Anda. Ini membuat aplikasi yang digunakan lebih tahan terhadap perubahan organisas i.

AWS organisasi dan struktur akun AWS SRA

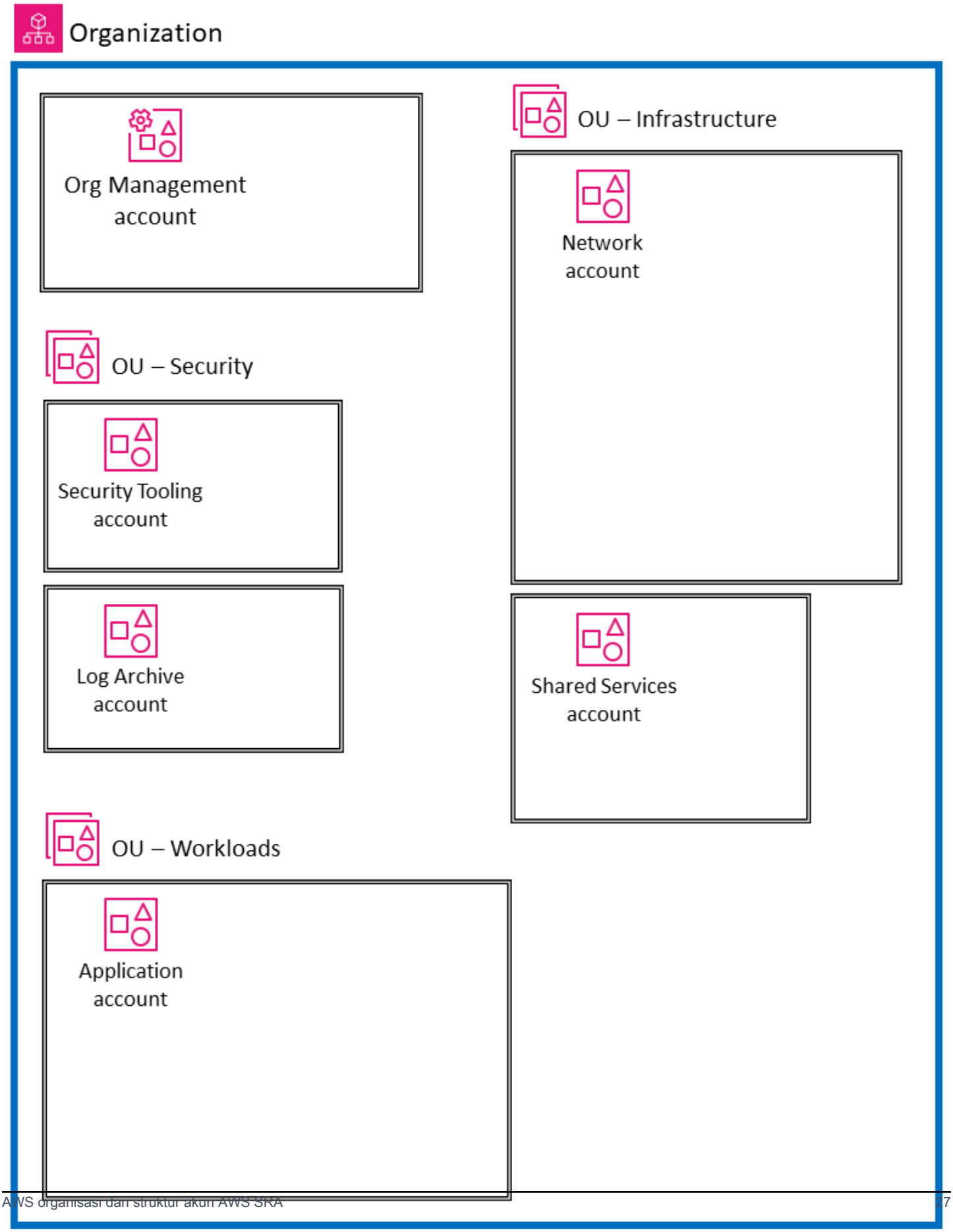
Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

Diagram berikut menangkap struktur tingkat tinggi AWS SRA tanpa menampilkan layanan tertentu. Ini mencerminkan struktur akun khusus yang dibahas di bagian sebelumnya, dan kami menyertakan diagram di sini untuk mengarahkan diskusi seputar komponen utama arsitektur:

- Semua akun yang ditampilkan dalam diagram adalah bagian dari satu AWS organisasi.
- Di kiri atas diagram adalah akun Manajemen Org, yang digunakan untuk membuat AWS organisasi.
- Di bawah akun Manajemen Org adalah OU Keamanan dengan dua akun tertentu: satu untuk Alat Keamanan dan yang lainnya untuk Arsip Log.
- Di sisi kanan adalah Infrastruktur OU dengan akun Jaringan dan akun Layanan Bersama.
- Di bagian bawah diagram adalah Beban Kerja OU, yang dikaitkan dengan akun Aplikasi yang menampung aplikasi perusahaan.

Untuk panduan ini, semua akun dianggap sebagai akun produksi (prod) yang beroperasi dalam satu AWS Region akun. Sebagian besar Layanan AWS (kecuali untuk layanan global) dicakup secara regional, yang berarti bahwa bidang kontrol dan data untuk layanan ada secara independen di masing-masing. AWS Region Untuk alasan ini, Anda harus mereplikasi arsitektur ini di semua Wilayah AWS yang Anda rencanakan untuk digunakan, untuk memastikan cakupan untuk seluruh AWS lanskap Anda. Jika Anda tidak memiliki beban kerja tertentu AWS Region, Anda harus menonaktifkan Wilayah dengan menggunakan SCPsatau dengan menggunakan mekanisme pencatatan dan pemantauan. Anda dapat menggunakan Security Hub CSPM untuk mengumpulkan temuan dan skor keamanan dari beberapa Wilayah AWS ke satu Wilayah agregasi tunggal untuk visibilitas terpusat.

Saat menghosting AWS organisasi dengan sejumlah besar akun, ada baiknya memiliki lapisan orkestrasi yang memfasilitasi penyebaran akun dan tata kelola akun. AWS Control Tower menawarkan cara mudah untuk mengatur dan mengatur lingkungan multi-akun AWS . Sampel kode AWS SRA di GitHub repositori menunjukkan bagaimana Anda dapat menggunakan solusi Customizations for AWS Control Tower (CFCT) untuk menerapkan struktur yang direkomendasikan SRA. AWS

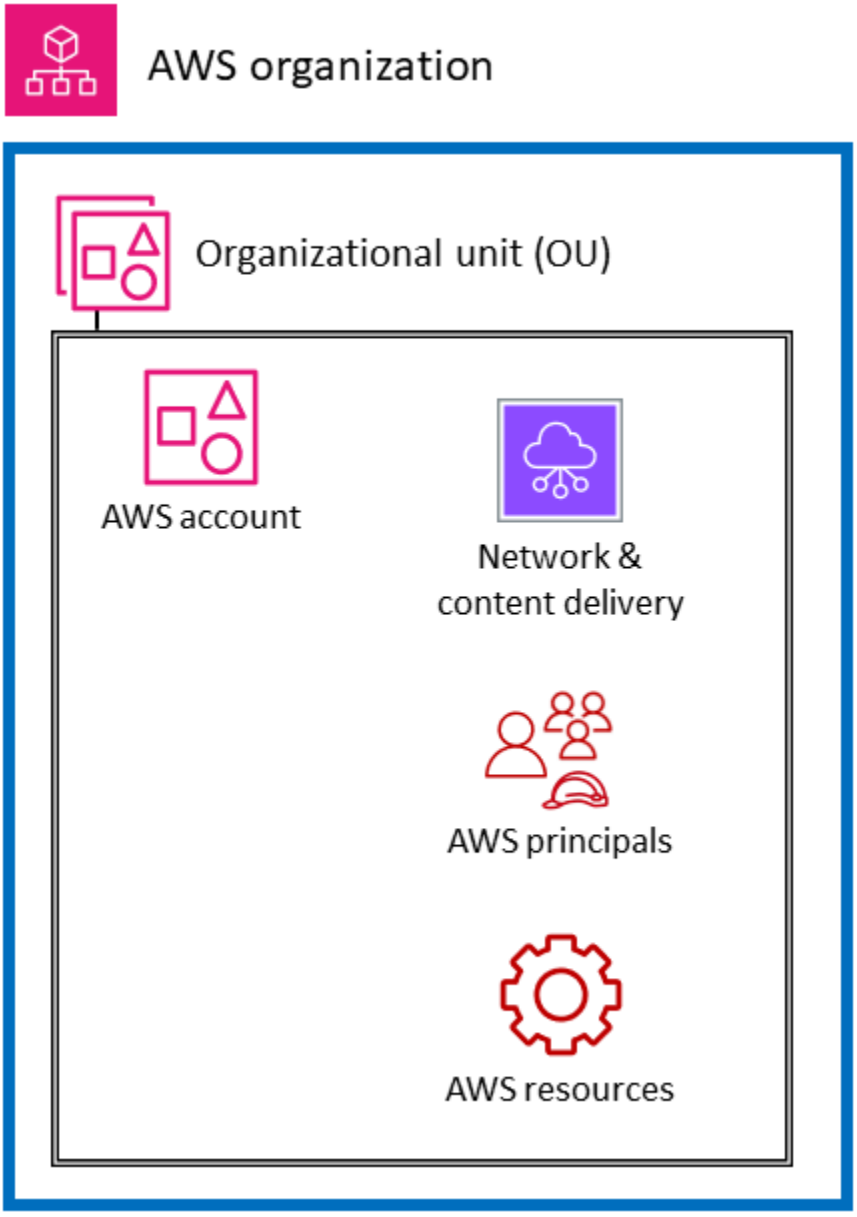

Organization
Org Management account
OU – Infrastructure
Network account
OU – Security
Security Tooling account
Log Archive account
Shared Services account
OU – Workloads
Application account

Terapkan layanan keamanan di seluruh AWS organisasi Anda

Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

Seperti yang dijelaskan di bagian sebelumnya, pelanggan mencari cara tambahan untuk memikirkan dan secara strategis mengatur set lengkap layanan AWS keamanan. Pendekatan organisasi yang paling umum saat ini adalah mengelompokkan layanan keamanan berdasarkan fungsi utama — sesuai dengan apa yang dilakukan masing-masing layanan. Perspektif keamanan AWS CAF mencantumkan sembilan kemampuan fungsional, termasuk manajemen identitas dan akses, perlindungan infrastruktur, perlindungan data, dan deteksi ancaman. Mencocokkan Layanan AWS dengan kemampuan fungsional ini adalah cara praktis untuk membuat keputusan implementasi di setiap bidang. Misalnya, ketika melihat identitas dan manajemen akses, IAM dan IAM Identity Center adalah layanan yang perlu dipertimbangkan. Saat merancang pendekatan deteksi ancaman Anda, GuardDuty mungkin menjadi pertimbangan pertama Anda.

Sebagai pelengkap tampilan fungsional ini, Anda juga dapat melihat keamanan Anda dengan tampilan struktural lintas sektoral. Artinya, selain bertanya, “Mana yang Layanan AWS harus saya gunakan untuk mengontrol dan melindungi identitas saya, akses logis, atau mekanisme deteksi ancaman?” , Anda juga dapat bertanya, “Mana yang Layanan AWS harus saya terapkan di seluruh AWS organisasi saya? Apa lapisan pertahanan yang harus saya lakukan untuk melindungi instans Amazon EC2 di inti aplikasi saya?” Dalam tampilan ini, Anda memetakan Layanan AWS dan fitur ke lapisan di AWS lingkungan Anda. Beberapa layanan dan fitur sangat cocok untuk menerapkan kontrol di seluruh AWS organisasi Anda. Misalnya, memblokir akses publik ke bucket Amazon S3 adalah kontrol khusus pada lapisan ini. Ini sebaiknya dilakukan di organisasi root daripada menjadi bagian dari pengaturan akun individu. Layanan dan fitur lain paling baik digunakan untuk membantu melindungi sumber daya individu dalam file Akun AWS. Menerapkan otoritas sertifikat bawahan (CA) dalam akun yang memerlukan sertifikat TLS pribadi adalah contoh dari kategori ini. Pengelompokan lain yang sama pentingnya terdiri dari layanan yang memiliki efek pada lapisan jaringan virtual AWS infrastruktur Anda. Diagram berikut menunjukkan enam lapisan dalam AWS lingkungan yang khas: AWS organisasi, unit organisasi (OU), akun, infrastruktur jaringan, prinsip, dan sumber daya.



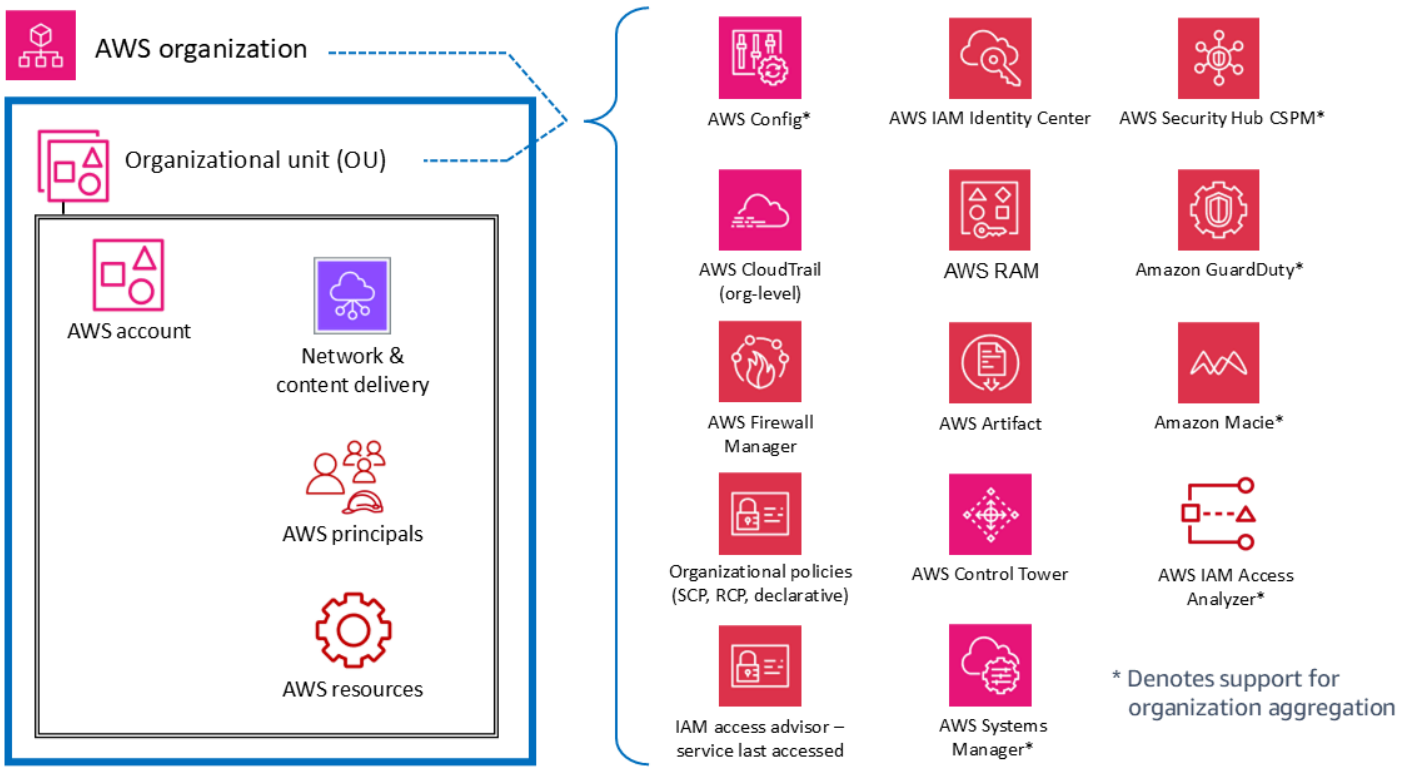
Memahami layanan dalam konteks struktural ini, termasuk kontrol dan perlindungan di setiap lapisan, membantu Anda merencanakan dan menerapkan defense-in-depth strategi di seluruh AWS lingkungan Anda. Dengan perspektif ini, Anda dapat menjawab pertanyaan baik dari atas ke bawah (misalnya, “Layanan mana yang saya gunakan untuk menerapkan kontrol keamanan di seluruh AWS organisasi saya?”) dan dari bawah ke atas (misalnya, “Layanan mana yang mengelola kontrol pada instance EC2 ini?”). Di bagian ini, kami menelusuri elemen AWS lingkungan dan mengidentifikasi layanan dan fitur keamanan terkait. Tentu saja, beberapa Layanan AWS memiliki set fitur yang luas dan mendukung beberapa tujuan keamanan. Layanan ini mungkin mendukung beberapa elemen AWS lingkungan Anda.

Untuk kejelasan, kami memberikan deskripsi singkat tentang bagaimana beberapa layanan sesuai dengan tujuan yang dinyatakan. Bagian selanjutnya memberikan diskusi lebih lanjut tentang layanan individu dalam masing-masing Akun AWS.

Akun di seluruh organisasi atau beberapa

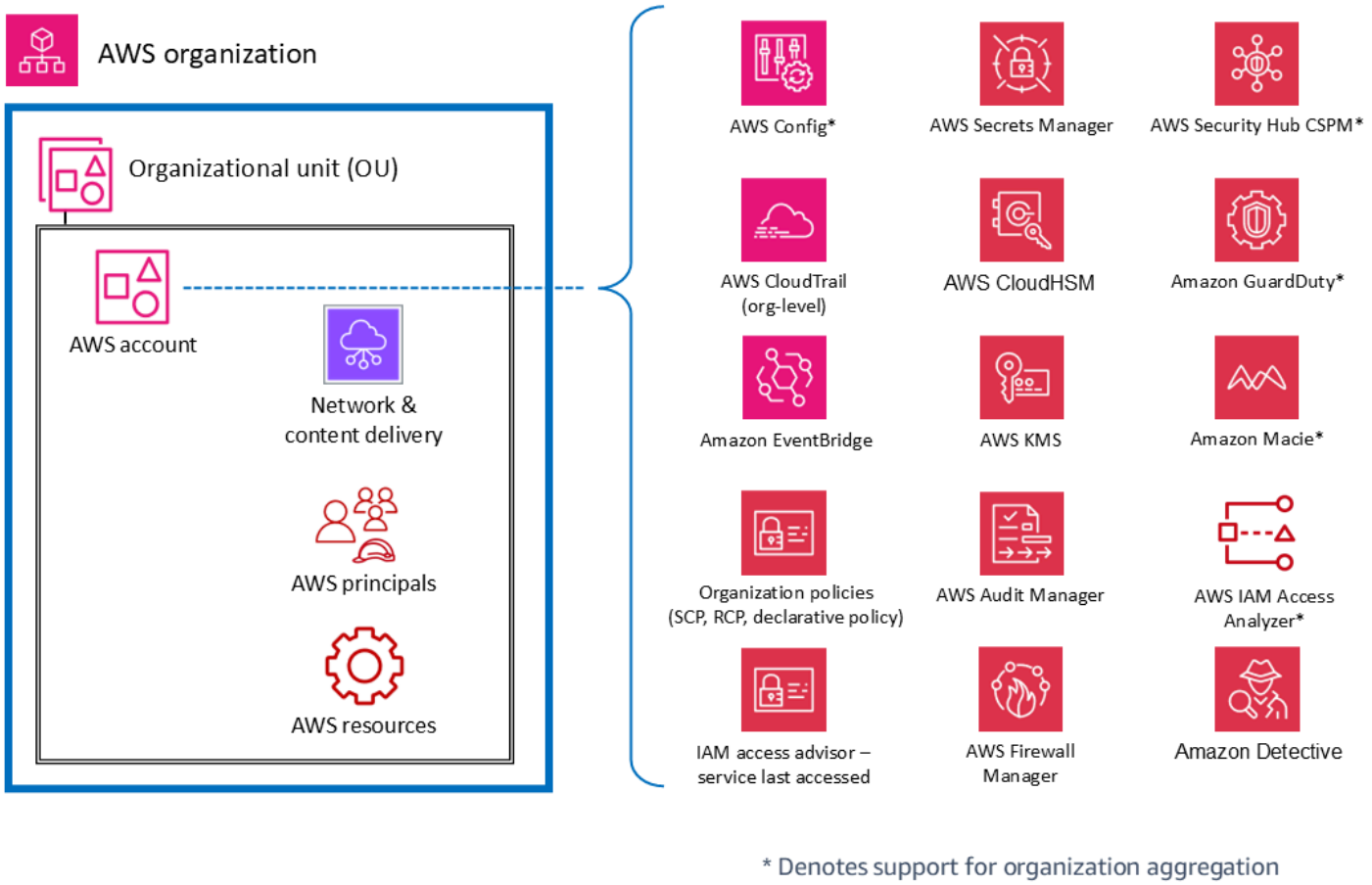
Di tingkat atas, ada Layanan AWS dan fitur yang dirancang untuk menerapkan kemampuan tata kelola dan kontrol atau pagar pembatas di beberapa akun dalam suatu AWS organisasi (termasuk seluruh organisasi atau spesifik). OUs Kebijakan kontrol layanan (SCPs) dan kebijakan kontrol sumber daya (RCPs) adalah contoh yang baik dari fitur IAM yang menyediakan pagar pembatas preventif di seluruh organisasi. AWS AWS Organizations juga menyediakan kebijakan deklaratif yang secara terpusat mendefinisikan dan menegakkan konfigurasi dasar untuk skala besar. Layanan AWS Contoh lain adalah CloudTrail, yang menyediakan pemantauan melalui jejak organisasi yang mencatat semua peristiwa untuk semua Akun AWS di AWS organisasi itu. Jejak komprehensif ini berbeda dari jalur individu yang dapat dibuat di setiap akun. Contoh ketiga adalah AWS Firewall Manager, yang dapat Anda gunakan untuk mengonfigurasi, menerapkan, dan mengelola beberapa sumber daya di semua akun di AWS organisasi Anda: AWS WAF aturan, aturan AWS WAF Klasik, AWS Shield Advanced perlindungan, grup keamanan Amazon Virtual Private Cloud (Amazon VPC) AWS Network Firewall , kebijakan, Amazon Route 53 Resolver dan kebijakan Firewall DNS.

Layanan yang ditandai dengan tanda bintang (*) dalam diagram berikut beroperasi dengan lingkup ganda: seluruh organisasi dan berfokus pada akun. Layanan ini secara fundamental memantau atau membantu mengontrol keamanan dalam akun individu. Namun, mereka juga mendukung kemampuan untuk mengumpulkan hasil mereka dari beberapa akun ke dalam akun di seluruh organisasi untuk visibilitas dan manajemen terpusat. Untuk kejelasan, pertimbangkan SCPs yang berlaku di seluruh OU, Akun AWS, atau AWS organisasi. Sebaliknya, Anda dapat mengonfigurasi dan mengelola GuardDuty keduanya di tingkat akun (di mana temuan individu dihasilkan) dan di tingkat AWS organisasi (dengan menggunakan fitur administrator yang didelegasikan) di mana temuan dapat dilihat dan dikelola secara agregat.



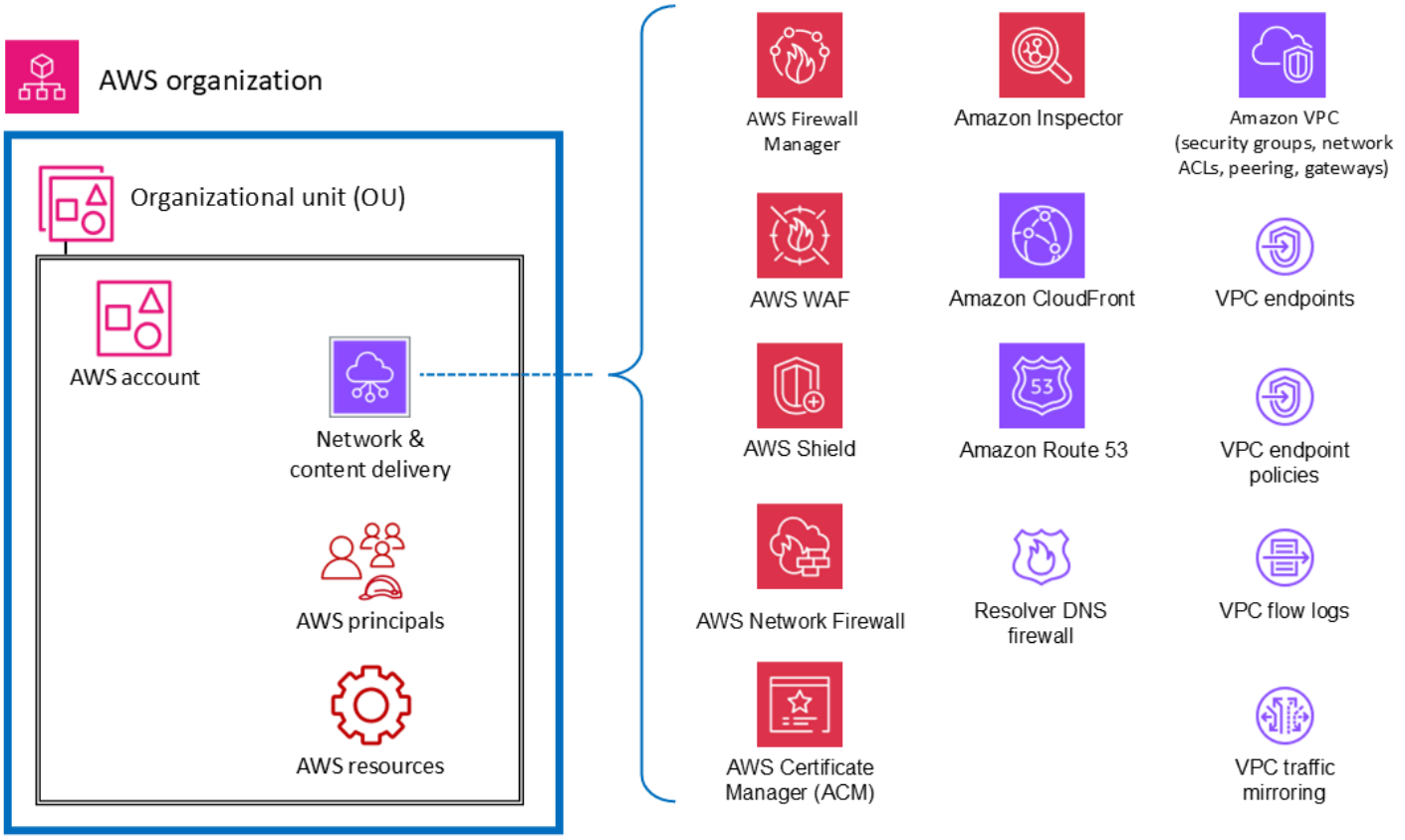
AWS akun

Di dalamnya OUs, ada layanan yang membantu melindungi berbagai jenis elemen dalam file Akun AWS. Misalnya, AWS Secrets Manager biasanya dikelola dari akun tertentu dan melindungi sumber daya (seperti kredensi database atau informasi otentikasi), aplikasi, dan Layanan AWS di akun itu. IAM Access Analyzer dapat dikonfigurasi untuk menghasilkan temuan ketika sumber daya tertentu dapat diakses oleh prinsipal di luar. Akun AWS Seperti disebutkan di bagian sebelumnya, banyak dari layanan ini juga dapat dikonfigurasi dan dikelola di dalamnya AWS Organizations, sehingga dapat dikelola di beberapa akun. Layanan ini ditandai dengan tanda bintang (*) dalam diagram. Mereka juga mempermudah untuk mengumpulkan hasil dari beberapa akun dan mengirimkannya ke satu akun. Ini memberi tim aplikasi individu fleksibilitas dan visibilitas untuk mengelola kebutuhan keamanan yang spesifik untuk beban kerja mereka sementara juga memungkinkan tata kelola dan visibilitas ke tim keamanan terpusat. GuardDuty adalah contoh dari layanan semacam itu. GuardDuty memantau sumber daya dan aktivitas yang terkait dengan satu akun, dan GuardDuty temuan dari beberapa akun anggota (seperti semua akun dalam AWS organisasi) dapat dikumpulkan, dilihat, dan dikelola dari akun administrator yang didelegasikan.



Jaringan virtual, komputasi, dan pengiriman konten

Karena akses jaringan sangat penting dalam keamanan, dan infrastruktur komputasi adalah komponen mendasar dari banyak AWS beban kerja, ada banyak layanan AWS keamanan dan fitur yang didedikasikan untuk sumber daya ini. Misalnya, Amazon Inspector adalah layanan manajemen kerentanan yang terus memindai beban kerja Anda AWS untuk mencari kerentanan. Pemindaian ini mencakup pemeriksaan jangkauan jaringan yang menunjukkan bahwa ada jalur jaringan yang diizinkan ke instans Amazon EC2 di lingkungan Anda. Amazon VPC memungkinkan Anda menentukan jaringan virtual tempat Anda dapat meluncurkan AWS sumber daya. Jaringan virtual ini sangat mirip dengan jaringan tradisional dan mencakup berbagai fitur dan manfaat. Endpoint VPC memungkinkan Anda untuk menghubungkan VPC Anda secara pribadi ke layanan yang didukung Layanan AWS dan ke layanan endpoint yang didukung oleh AWS PrivateLink tanpa memerlukan jalur ke internet. Diagram berikut menggambarkan layanan keamanan yang berfokus pada jaringan, komputasi, dan infrastruktur pengiriman konten.



Prinsipal dan sumber daya

AWS prinsip dan AWS sumber daya (bersama dengan kebijakan IAM) adalah elemen mendasar dalam identitas dan manajemen akses pada. AWS Prinsipal yang diautentikasi AWS dapat melakukan tindakan dan mengakses AWS sumber daya. Prinsipal dapat diautentikasi sebagai pengguna Akun AWS root dan pengguna IAM, atau dengan mengambil peran.

> **Note**
>
> Jangan membuat kunci API persisten yang terkait dengan akun pengguna AWS root. Akses ke akun pengguna root harus dibatasi hanya pada tugas-tugas yang membutuhkan pengguna root, dan kemudian hanya melalui proses pengecualian dan persetujuan yang ketat. Untuk praktik terbaik untuk melindungi pengguna root akun Anda, lihat dokumentasi IAM.

AWS Sumber daya adalah objek yang ada di dalam Layanan AWS yang dapat Anda kerjakan. Contohnya termasuk instans EC2, CloudFormation tumpukan, topik Amazon Simple Notification

Service (Amazon SNS), dan bucket S3. Kebijakan IAM adalah objek yang menentukan izin saat dikaitkan dengan prinsipal IAM (pengguna, grup, atau peran) atau sumber daya. AWS Kebijakan berbasis identitas adalah dokumen kebijakan yang Anda lampirkan ke prinsipal (peran, pengguna, dan grup pengguna) untuk mengontrol tindakan mana yang dapat dilakukan oleh prinsipal, sumber daya mana, dan dalam kondisi apa. Kebijakan berbasis sumber daya adalah dokumen kebijakan yang Anda lampirkan ke sumber daya seperti bucket S3. Kebijakan ini memberikan izin utama yang ditentukan untuk melakukan tindakan spesifik pada sumber daya tersebut dan menentukan kondisi untuk izin tersebut. Kebijakan berbasis sumber daya adalah kebijakan in-line. Bagian sumber daya IAM menyelami lebih dalam jenis kebijakan IAM dan bagaimana mereka digunakan.

Untuk menjaga hal-hal sederhana dalam diskusi ini, kami mencantumkan layanan AWS keamanan dan fitur untuk kepala sekolah IAM yang memiliki tujuan utama untuk mengoperasikan, atau mendaftar ke, kepala sekolah akun. Kami menjaga kesederhanaan itu sambil mengakui fleksibilitas dan luasnya efek kebijakan izin IAM. Sebuah pernyataan tunggal dalam kebijakan dapat memiliki efek pada beberapa jenis AWS entitas. Misalnya, meskipun kebijakan berbasis identitas IAM dikaitkan dengan prinsipal IAM dan mendefinisikan izin (izinkan, tolak) untuk prinsipal tersebut, kebijakan tersebut juga secara implisit mendefinisikan izin untuk tindakan, sumber daya, dan kondisi yang ditentukan. Dengan cara ini, kebijakan berbasis identitas dapat menjadi elemen penting dalam menentukan izin untuk sumber daya.

Diagram berikut menggambarkan layanan AWS keamanan dan fitur untuk AWS kepala sekolah. Kebijakan berbasis identitas terlampir pada pengguna, grup, atau peran IAM. Kebijakan ini memungkinkan Anda menentukan apa yang dapat dilakukan oleh identitas (izinnya). Kebijakan sesi IAM adalah kebijakan izin sebaris yang diteruskan pengguna dalam sesi saat mereka mengambil peran. Anda dapat meneruskan kebijakan sendiri, atau Anda dapat mengonfigurasi pialang identitas Anda untuk memasukkan kebijakan saat identitas Anda bergabung. AWS Ini memungkinkan administrator Anda mengurangi jumlah peran yang harus mereka buat, karena beberapa pengguna dapat mengambil peran yang sama namun memiliki izin sesi yang unik. Layanan IAM Identity Center terintegrasi dengan AWS Organizations dan operasi AWS API, dan membantu Anda mengelola akses SSO dan izin pengguna di seluruh akun Anda. Akun AWS AWS Organizations

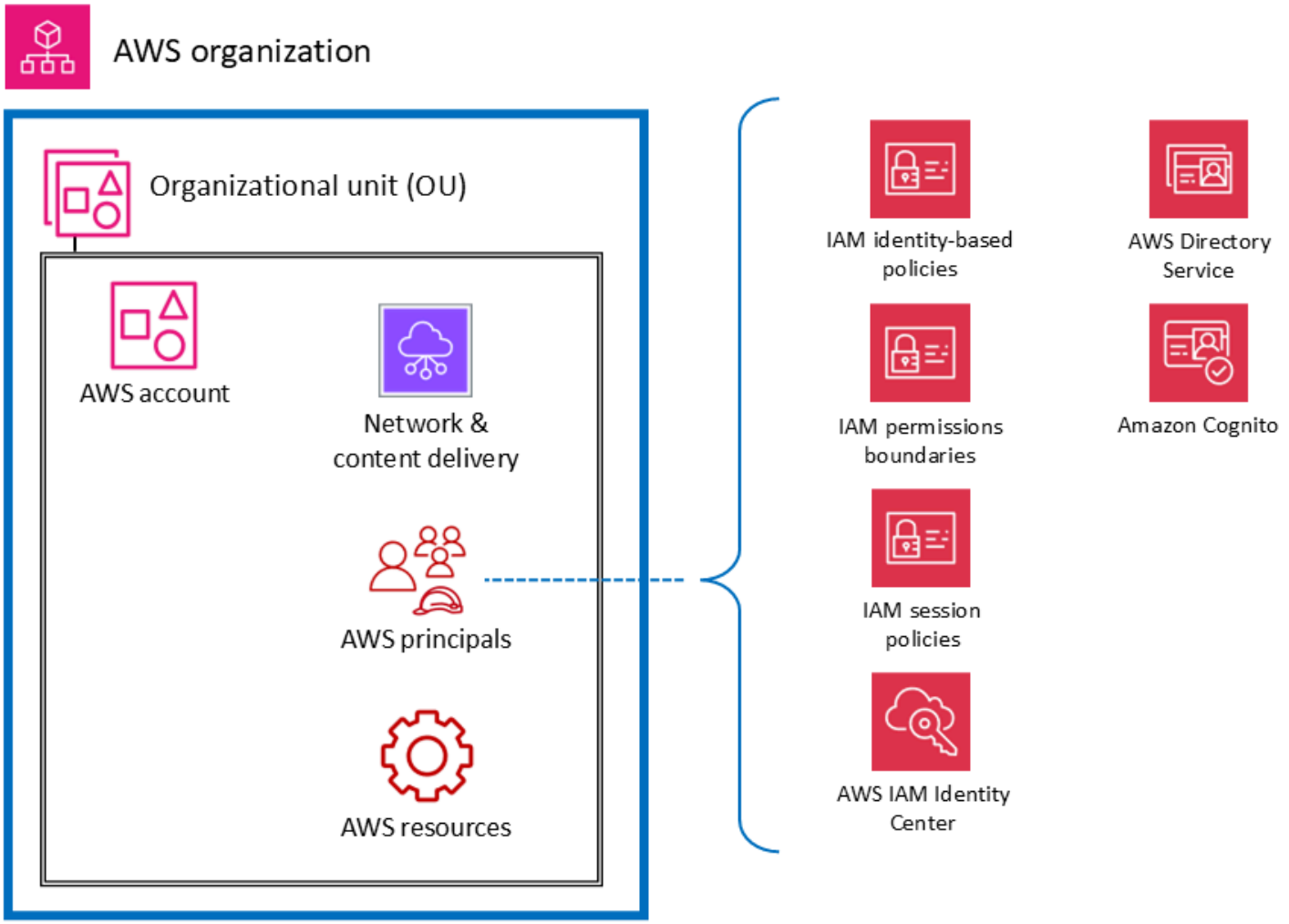
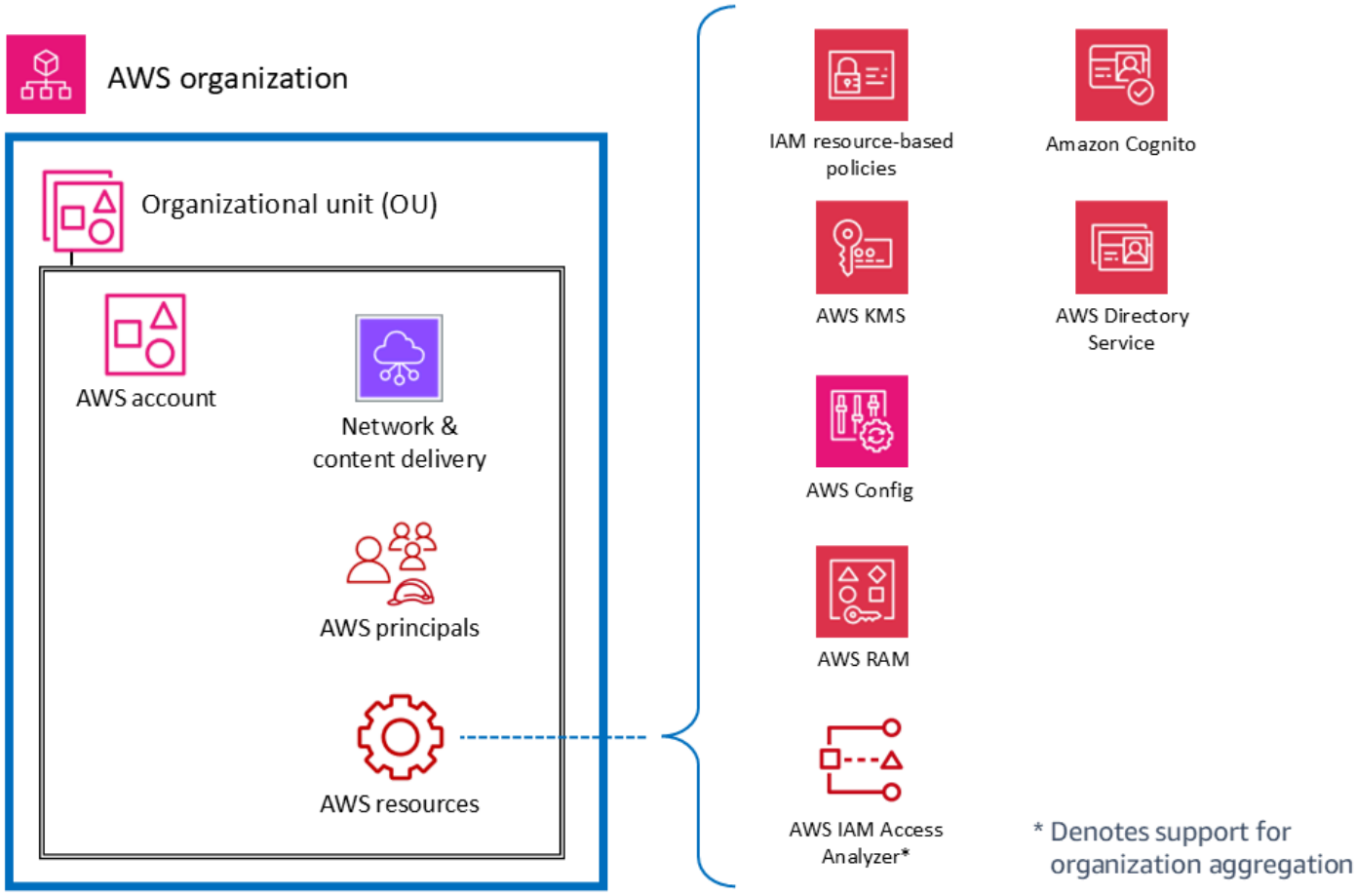


Diagram berikut menggambarkan layanan dan fitur untuk sumber daya akun. Kebijakan berbasis sumber daya dilampirkan pada sumber daya. Misalnya, Anda dapat melampirkan kebijakan berbasis sumber daya ke bucket S3, antrian Amazon Simple Queue Service (Amazon SQS), titik akhir VPC, dan kunci enkripsi. AWS KMS Anda dapat menggunakan kebijakan berbasis sumber daya untuk menentukan siapa yang memiliki akses ke sumber daya dan tindakan apa yang dapat mereka lakukan terhadapnya. Kebijakan bucket S3, kebijakan AWS KMS utama, dan kebijakan titik akhir VPC adalah jenis kebijakan berbasis sumber daya. IAM Access Analyzer membantu Anda mengidentifikasi sumber daya di organisasi dan akun Anda, seperti bucket S3 atau peran IAM, yang dibagikan dengan entitas eksternal. Ini memungkinkan Anda mengidentifikasi akses yang tidak diinginkan ke sumber daya dan data Anda, yang merupakan risiko keamanan. AWS Config memungkinkan Anda untuk menilai, mengaudit, dan mengevaluasi konfigurasi AWS sumber daya yang didukung di Anda Akun AWS. AWS Config terus memantau dan merekam konfigurasi AWS sumber daya, dan secara otomatis mengevaluasi konfigurasi yang direkam terhadap konfigurasi yang diinginkan.


AWS organization
Organizational unit (OU)
AWS account
Network & content delivery
AWS principals
AWS resources
IAM resource-based policies
Amazon Cognito
AWS KMS
AWS Directory Service
AWS Config
AWS RAM
AWS IAM Access Analyzer*
* Denotes support for organization aggregation

Arsitektur Referensi AWS Keamanan

Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

Diagram berikut menggambarkan AWS SRA. Diagram arsitektur ini menyatukan semua layanan AWS terkait keamanan. Ini dibangun di sekitar arsitektur web tiga tingkat sederhana yang dapat ditampung pada satu halaman. Dalam beban kerja seperti itu, ada tingkat web di mana pengguna terhubung dan berinteraksi dengan tingkat aplikasi, yang menangani logika bisnis aplikasi yang sebenarnya: mengambil input dari pengguna, melakukan beberapa perhitungan, dan menghasilkan output. Tingkat aplikasi menyimpan dan mengambil informasi dari tingkat data. Arsitekturnya sengaja modular dan menyediakan abstraksi tingkat tinggi untuk banyak aplikasi web modern.

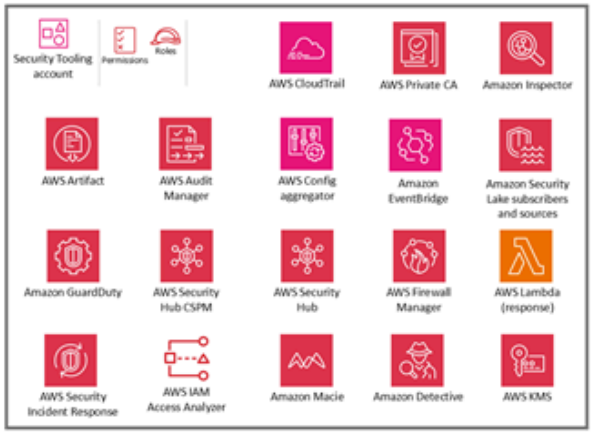
Diagram arsitektur

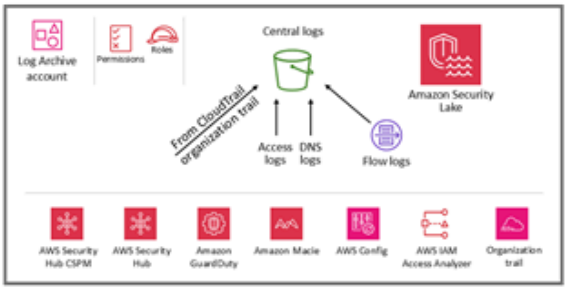
Untuk menyesuaikan diagram arsitektur referensi dalam panduan ini berdasarkan kebutuhan bisnis Anda, Anda dapat mengunduh file.zip berikut dan mengekstrak isinya.

Unduh file sumber diagram (PowerPoint format Microsoft)

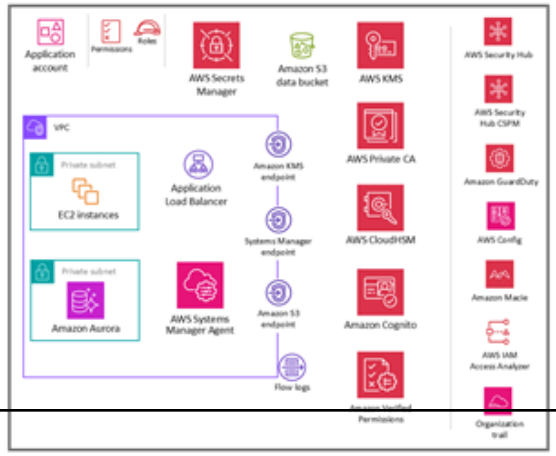
Organization

OU – Security

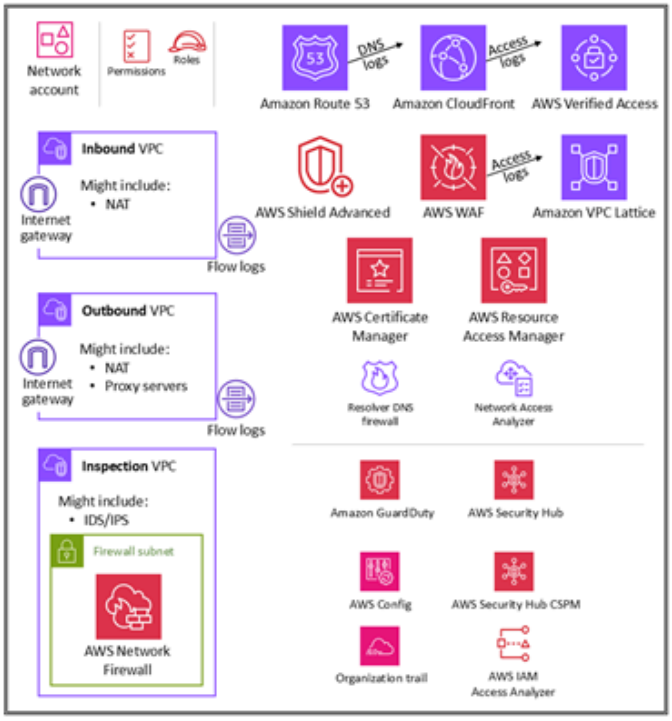


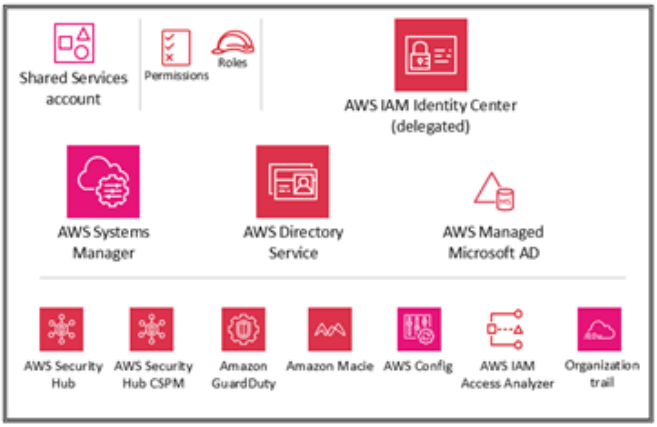


OU – Workloads



OU – Infrastructure





Untuk arsitektur referensi ini, aplikasi web dan tingkat data yang sebenarnya sengaja direpresentasikan sesederhana mungkin, melalui EC2 instance Amazon dan database Amazon Aurora, masing-masing. Sebagian besar diagram arsitektur fokus dan menyelam jauh di web, aplikasi, dan tingkatan data. Untuk keterbacaan, mereka sering menghilangkan kontrol keamanan. Diagram ini membalik penekanan itu untuk menunjukkan keamanan sedapat mungkin, dan menjaga aplikasi dan tingkatan data sesederhana yang diperlukan untuk menunjukkan fitur keamanan secara bermakna.

AWS SRA berisi semua layanan AWS terkait keamanan yang tersedia pada saat publikasi. (Lihat riwayat dokumen.) Namun, tidak setiap beban kerja atau lingkungan, berdasarkan eksposur ancaman yang unik, harus menyebarkan setiap layanan keamanan. Tujuan kami adalah memberikan referensi untuk berbagai opsi, termasuk deskripsi tentang bagaimana layanan ini cocok secara arsitektur, sehingga bisnis Anda dapat membuat keputusan yang paling sesuai untuk kebutuhan infrastruktur, beban kerja, dan keamanan Anda, berdasarkan risiko.

Bagian berikut berjalan melalui setiap OU dan akun untuk memahami tujuannya dan layanan AWS keamanan individu yang terkait dengannya. Untuk setiap elemen (biasanya an Layanan AWS), dokumen ini memberikan informasi berikut:

- Tinjauan singkat tentang elemen dan tujuan keamanannya di AWS SRA. Untuk deskripsi lebih rinci dan informasi teknis tentang layanan individual, lihat lampiran.
- Penempatan yang disarankan untuk mengaktifkan dan mengelola layanan secara efektif. Ini ditangkap dalam diagram arsitektur individu untuk setiap akun dan OU.
- Konfigurasi, manajemen, dan tautan berbagi data ke layanan keamanan lainnya. Bagaimana layanan ini mengandalkan, atau mendukung, layanan keamanan lainnya?
- Pertimbangan desain. Pertama, dokumen menyoroti fitur opsional atau konfigurasi yang memiliki implikasi keamanan penting. Kedua, di mana pengalaman tim kami mencakup variasi umum dalam rekomendasi yang kami buat—biasanya sebagai akibat dari persyaratan atau kendala alternatif—dokumen menjelaskan opsi tersebut.

OUs dan akun

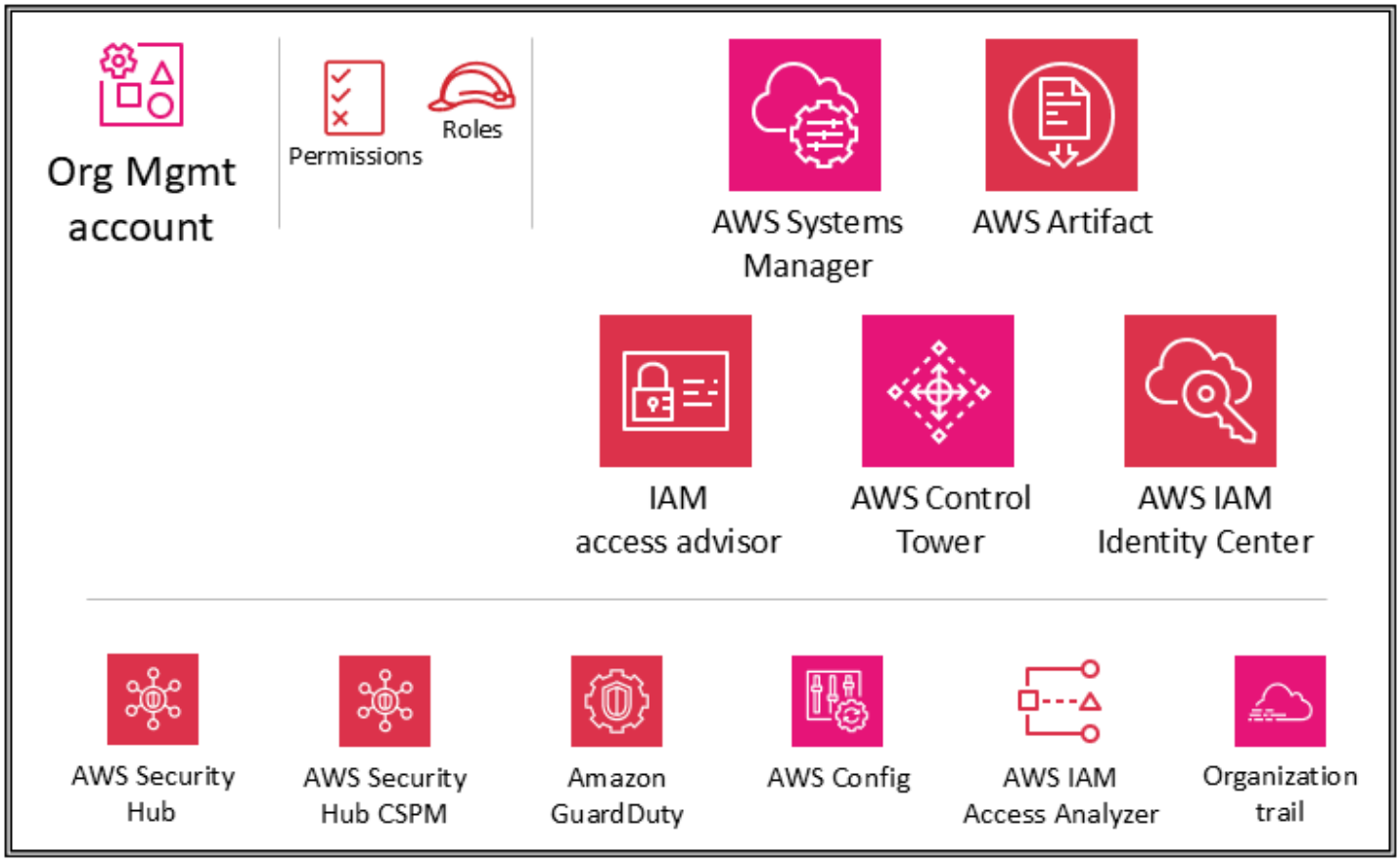
- Akun Manajemen Org
- Security OU - Akun Perkakas Keamanan
- Keamanan OU - Akun Arsip Log
- Infrastruktur OU - Akun jaringan
- Infrastruktur OU - Akun Layanan Bersama

- Beban Kerja OU - Akun aplikasi

Akun Manajemen Org

Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

Diagram berikut menggambarkan layanan AWS keamanan yang dikonfigurasi di akun Manajemen Org.



Bagian Menggunakan AWS Organizations untuk keamanan dan Akun manajemen, akses tepercaya, dan administrator yang didelegasikan sebelumnya dalam panduan ini membahas tujuan dan tujuan keamanan akun Manajemen Org secara mendalam. Ikuti praktik terbaik keamanan untuk akun Manajemen Org Anda. Ini termasuk menggunakan alamat email yang dikelola oleh bisnis Anda, menjaga informasi kontak administratif dan keamanan yang benar (seperti melampirkan nomor telepon ke akun jika AWS perlu menghubungi pemilik akun), mengaktifkan otentikasi multi-faktor

(MFA) untuk semua pengguna, dan secara teratur meninjau siapa yang memiliki akses ke akun Manajemen Org. Layanan yang digunakan di akun Manajemen Organisasi harus dikonfigurasi dengan peran yang sesuai, kebijakan kepercayaan, dan izin lainnya sehingga administrator layanan tersebut (yang harus mengaksesnya di akun Manajemen Org) juga tidak dapat mengakses layanan lain secara tidak tepat.

Kebijakan kontrol layanan

Dengan AWS Organizations, Anda dapat mengelola kebijakan secara terpusat di beberapa Akun AWS. Misalnya, Anda dapat menerapkan kebijakan kontrol layanan (SCPs) di beberapa Akun AWS anggota organisasi. SCPs memungkinkan Anda menentukan mana yang Layanan AWS APIs dapat dan tidak dapat dijalankan oleh prinsipal IAM (seperti pengguna dan peran IAM) di anggota organisasi Anda. Akun AWS SCPs dibuat dan diterapkan dari akun Manajemen Org, yang merupakan akun Akun AWS yang Anda gunakan saat membuat organisasi. Baca lebih lanjut tentang SCPs di bagian Menggunakan AWS Organizations untuk keamanan sebelumnya dalam referensi ini.

Jika Anda menggunakan AWS Control Tower untuk mengelola AWS organisasi Anda, itu akan menggunakan satu set SCPs sebagai pagar pembatas preventif (dikategorikan sebagai wajib, sangat disarankan, atau elektif). Pagar pembatas ini membantu Anda mengatur sumber daya Anda dengan menegakkan kontrol keamanan di seluruh organisasi. Ini SCPs secara otomatis menggunakan aws-control-tower tag yang memiliki nilai managed-by-control-tower.

> **Pertimbangan desain**
>
> SCPs hanya mempengaruhi akun anggota dalam AWS organisasi. Meskipun mereka diterapkan dari akun Manajemen Org, mereka tidak berpengaruh pada pengguna atau peran dalam akun itu. Untuk mempelajari tentang cara kerja logika evaluasi SCP, dan untuk melihat contoh struktur yang direkomendasikan, lihat posting AWS blog Cara menggunakan kebijakan kontrol layanan di AWS Organizations.

Kebijakan pengendalian sumber daya

Kebijakan kontrol sumber daya (RCPs) menawarkan kontrol terpusat atas izin maksimum yang tersedia untuk sumber daya di organisasi Anda. RCP mendefinisikan pagar pembatas izin atau menetapkan batasan pada tindakan yang dapat diambil identitas terhadap sumber daya di organisasi Anda. Anda dapat menggunakan RCPs untuk membatasi siapa yang dapat mengakses sumber daya Anda dan menegakkan persyaratan tentang bagaimana sumber daya Anda dapat diakses di

anggota organisasi Anda. Akun AWS Anda dapat melampirkan RCPs langsung ke akun individu OUs,, atau root organisasi. Untuk penjelasan rinci tentang cara RCPs kerja, lihat evaluasi RCP dalam AWS Organizations dokumentasi. Baca lebih lanjut tentang RCPs di bagian Menggunakan AWS Organizations untuk keamanan sebelumnya dalam referensi ini.

Jika Anda menggunakan AWS Control Tower untuk mengelola AWS organisasi Anda, itu akan menggunakan satu set RCPs sebagai pagar pembatas pencegahan (dikategorikan sebagai wajib, sangat disarankan, atau elektif). Pagar pembatas ini membantu Anda mengatur sumber daya Anda dengan menegakkan kontrol keamanan di seluruh organisasi. Ini SCPs secara otomatis menggunakan `aws-control-tower` tag yang memiliki nilai`managed-by-control-tower`.

Pertimbangan desain

- RCPs hanya mempengaruhi sumber daya di akun anggota dalam organisasi. Mereka tidak berpengaruh pada sumber daya di akun manajemen. Ini juga berarti bahwa RCPs berlaku untuk akun anggota yang ditunjuk sebagai administrator yang didelegasikan.
- RCPs berlaku untuk sumber daya untuk subset. Layanan AWS Untuk informasi selengkapnya, lihat Daftar dukungan Layanan AWS tersebut RCPs dalam AWS Organizations dokumentasi. Anda dapat menggunakan Aturan AWS Configdan AWS Lambda berfungsi untuk memantau dan mengotomatiskan penegakan kontrol keamanan pada sumber daya yang saat ini tidak didukung oleh RCPs.

Kebijakan deklaratif

Kebijakan deklaratif adalah jenis kebijakan AWS Organizations manajemen yang membantu Anda mendeklarasikan dan menegakkan konfigurasi yang Anda inginkan secara terpusat pada skala tertentu Layanan AWS di seluruh organisasi. Kebijakan deklaratif saat ini mendukung layanan Amazon EC2, Amazon VPC, dan Amazon EBS. Atribut layanan yang tersedia termasuk menerapkan Layanan Metadata Instans Versi 2 (IMDSv2), memungkinkan pemecahan masalah melalui konsol serial EC2, memungkinkan pengaturan Amazon Machine Image (AMI), dan memblokir akses publik untuk snapshot Amazon EBS, Amazon EC2, dan sumber daya Amazon VPC. AMIs Untuk layanan dan atribut terbaru yang didukung, lihat Kebijakan deklaratif dalam AWS Organizations dokumentasi.

Anda dapat menerapkan konfigurasi dasar untuk sebuah Layanan AWS dengan membuat beberapa pilihan pada AWS Organizations dan AWS Control Tower konsol atau dengan menggunakan beberapa perintah AWS Command Line Interface ()AWS CLI dan SDK. AWS Kebijakan deklaratif

diberlakukan di bidang kontrol layanan, yang berarti bahwa konfigurasi dasar untuk sebuah selalu Layanan AWS dipertahankan, bahkan ketika layanan memperkenalkan fitur baru atau APIs, ketika akun baru ditambahkan ke organisasi, atau ketika prinsip dan sumber daya baru dibuat. Kebijakan deklaratif dapat diterapkan ke seluruh organisasi atau untuk spesifik OUs atau akun. Kebijakan yang efektif adalah seperangkat aturan yang diwarisi dari akar organisasi dan OUs bersama dengan kebijakan yang langsung dilampirkan ke akun. Jika kebijakan deklaratif terlepas, status atribut akan kembali ke statusnya sebelum kebijakan deklaratif dilampirkan.

Anda dapat menggunakan kebijakan deklaratif untuk membuat pesan kesalahan kustom. Misalnya, jika operasi API gagal karena kebijakan deklaratif, Anda dapat menyetel pesan kesalahan atau memberikan URL kustom–seperti tautan ke wiki internal atau tautan ke pesan yang menjelaskan kegagalan tersebut. Ini membantu memberi pengguna lebih banyak informasi sehingga mereka dapat memecahkan masalah itu sendiri. Anda juga dapat mengaudit proses pembuatan kebijakan deklaratif, memperbarui kebijakan deklaratif, dan menghapus kebijakan deklaratif dengan menggunakan. AWS CloudTrail

Kebijakan deklaratif menyediakan laporan status akun, yang memungkinkan Anda meninjau status saat ini dari semua atribut yang didukung oleh kebijakan deklaratif untuk cakupan akun. Anda dapat memilih akun dan OUs memasukkan dalam lingkup laporan atau memilih seluruh organisasi dengan memilih root. Laporan ini membantu Anda menilai kesiapan dengan memberikan rincian AWS Region dan menentukan apakah status atribut saat ini seragam di seluruh akun (melalui `numberOfMatchedAccounts` nilai) atau tidak konsisten di seluruh akun (melalui nilai). `numberOfUnmatchedAccounts`

> **Pertimbangan desain**
>
> Saat Anda mengonfigurasi atribut layanan menggunakan kebijakan deklaratif, kebijakan tersebut dapat memengaruhi beberapa APIs atribut. Setiap tindakan yang tidak patuh akan gagal. Administrator akun tidak akan dapat mengubah nilai atribut layanan di tingkat akun individu.

Akses root terpusat

Semua akun anggota AWS Organizations memiliki pengguna root mereka sendiri, yang merupakan identitas yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun anggota tersebut. IAM menyediakan manajemen akses root terpusat untuk mengelola akses root di semua akun anggota. Ini membantu mencegah penggunaan pengguna root anggota dan membantu

memberikan pemulihan dalam skala besar. Fitur akses root terpusat memiliki dua kemampuan penting: manajemen kredensial root dan sesi root.

- Kemampuan manajemen kredensial root memungkinkan manajemen pusat dan membantu mengamankan pengguna root di semua akun manajemen. Kemampuan ini mencakup penghapusan kredensi root jangka panjang, pencegahan pemulihan kredenal root oleh akun anggota, dan penyediaan akun anggota baru tanpa kredensi root secara default. Ini juga menyediakan cara mudah untuk menunjukkan kepatuhan. Ketika manajemen pengguna root terpusat, Anda dapat menghapus kata sandi pengguna root, kunci akses, dan sertifikat penandatanganan, dan menonaktifkan otentikasi multi-faktor (MFA) dari semua akun anggota.
- Kemampuan sesi root memungkinkan Anda untuk melakukan tindakan pengguna root istimewa dengan menggunakan kredensi jangka pendek pada akun anggota dari akun Manajemen Org atau dari akun administrator yang didelegasikan. Kemampuan ini membantu Anda mengaktifkan akses root jangka pendek yang mencakup tindakan tertentu, mengikuti prinsip hak istimewa paling sedikit.

Untuk manajemen kredensi root terpusat, Anda perlu mengaktifkan manajemen kredensi root dan kemampuan sesi root di tingkat organisasi dari akun Manajemen Org atau di akun administrator yang didelegasikan. Mengikuti praktik terbaik AWS SRA, kami mendelegasikan kemampuan ini ke akun Security Tooling. Untuk informasi tentang mengkonfigurasi dan menggunakan akses pengguna root terpusat, lihat posting blog AWS Keamanan, Mengelola akses root secara terpusat untuk pelanggan yang menggunakan. AWS Organizations

Pusat Identitas IAM

AWS IAM Identity Centeradalah layanan federasi identitas yang membantu Anda mengelola akses SSO secara terpusat ke semua beban kerja Anda Akun AWS, kepala sekolah, dan cloud. IAM Identity Center juga membantu Anda mengelola akses dan izin ke aplikasi perangkat lunak pihak ketiga sebagai layanan (SaaS) yang umum digunakan. Penyedia identitas terintegrasi dengan IAM Identity Center dengan menggunakan SAMP 2.0. Massal dan just-in-time penyediaan dapat dilakukan dengan menggunakan System for Cross-Domain Identity Management (SCIM). Pusat Identitas IAM juga dapat berintegrasi dengan domain Microsoft Active Directory (AD) lokal atau AWS terkelola sebagai penyedia identitas melalui penggunaan. AWS Directory Service IAM Identity Center mencakup portal pengguna tempat pengguna akhir Anda dapat menemukan dan mengakses Pusat Identitas Akun AWS IAM yang ditetapkan, peran, aplikasi cloud, dan aplikasi khusus mereka di satu tempat.

IAM Identity Center terintegrasi secara native dengan AWS Organizations dan berjalan di akun Manajemen Org secara default. Namun, untuk menggunakan hak istimewa paling sedikit dan mengontrol akses ke akun manajemen dengan ketat, administrasi Pusat Identitas IAM dapat didelegasikan ke akun anggota tertentu. Di AWS SRA, akun Layanan Bersama adalah akun administrator yang didelegasikan untuk Pusat Identitas IAM. Sebelum Anda mengaktifkan administrasi yang didelegasikan untuk IAM Identity Center, tinjau pertimbangan ini. Anda akan menemukan informasi lebih lanjut tentang delegasi di bagian akun Layanan Bersama. Bahkan setelah Anda mengaktifkan delegasi, Pusat Identitas IAM masih perlu dijalankan di akun Manajemen Org untuk melakukan tugas terkait Pusat Identitas IAM tertentu, yang mencakup mengelola set izin yang disediakan di akun Manajemen Org.

Dalam konsol Pusat Identitas IAM, akun ditampilkan oleh OU enkapsulasi mereka. Ini memungkinkan Anda untuk dengan cepat menemukan Akun AWS, menerapkan set izin umum, dan mengelola akses dari lokasi pusat.

IAM Identity Center mencakup toko identitas tempat informasi pengguna tertentu harus disimpan. Namun, IAM Identity Center tidak harus menjadi sumber otoritatif untuk informasi tenaga kerja. Dalam kasus di mana perusahaan Anda sudah memiliki sumber otoritatif, IAM Identity Center mendukung jenis penyedia identitas berikut ()IdPs.

- Toko identitas IAM Identity Center - Pilih opsi ini jika dua opsi berikut tidak tersedia. Pengguna dibuat, penugasan grup dibuat, dan izin ditetapkan di toko identitas. Bahkan jika sumber otoritatif Anda berada di luar Pusat Identitas IAM, salinan atribut utama akan disimpan dengan toko identitas.
- Microsoft Active Directory (AD) — Pilih opsi ini jika Anda ingin terus mengelola pengguna di direktori Anda AWS Directory Service for Microsoft Active Directory atau direktori yang dikelola sendiri di Active Directory.
- Penyedia identitas eksternal - Pilih opsi ini jika Anda lebih suka mengelola pengguna di pihak ketiga eksternal, IDP berbasis SAML.

Anda dapat mengandalkan IDP yang sudah ada yang sudah ada di perusahaan Anda. Ini membuatnya lebih mudah untuk mengelola akses di beberapa aplikasi dan layanan, karena Anda membuat, mengelola, dan mencabut akses dari satu lokasi. Misalnya, jika seseorang meninggalkan tim Anda, Anda dapat mencabut aksesnya ke semua aplikasi dan layanan (termasuk Akun AWS) dari satu lokasi. Ini mengurangi kebutuhan akan banyak kredensil dan memberi Anda kesempatan untuk berintegrasi dengan proses sumber daya manusia (SDM) Anda.

> **Pertimbangan desain**
>
> Gunakan iDP eksternal jika opsi itu tersedia untuk perusahaan Anda. Jika IDP Anda mendukung System for Cross-domain Identity Management (SCIM), manfaatkan kemampuan SCIM di IAM Identity Center untuk mengotomatiskan penyediaan pengguna, grup, dan izin (sinkronisasi). Hal ini memungkinkan AWS akses untuk tetap sinkron dengan alur kerja perusahaan Anda untuk karyawan baru, karyawan yang pindah ke tim lain, dan karyawan yang meninggalkan perusahaan. Pada waktu tertentu, Anda hanya dapat memiliki satu direktori atau satu penyedia identitas SAMP 2.0 yang terhubung ke IAM Identity Center. Namun, Anda dapat beralih ke penyedia identitas lain.

Penasihat akses IAM

Penasihat akses IAM menyediakan data ketertelusuran dalam bentuk layanan informasi yang terakhir diakses untuk Anda dan. Akun AWS OUs Gunakan kontrol detektif ini untuk berkontribusi pada strategi hak istimewa yang paling tidak. Untuk kepala sekolah IAM, Anda dapat melihat dua jenis informasi yang terakhir diakses: informasi yang diizinkan dan Layanan AWS informasi tindakan yang diizinkan. Informasi tersebut meliputi tanggal dan waktu saat percobaan dilakukan.

Akses IAM dalam akun Manajemen Org memungkinkan Anda melihat data layanan yang terakhir diakses untuk akun Manajemen Org, OU, akun anggota, atau kebijakan IAM di organisasi Anda AWS . Informasi ini tersedia di konsol IAM dalam akun manajemen dan juga dapat diperoleh secara terprogram dengan menggunakan penasihat akses IAM APIs di AWS CLI atau klien terprogram. Informasi tersebut menunjukkan penanggung jawab mana dalam suatu organisasi atau akun yang terakhir kali mencoba mengakses layanan dan kapan. Informasi yang diakses terakhir memberikan wawasan untuk penggunaan layanan aktual (lihat contoh skenario), sehingga Anda dapat mengurangi izin IAM hanya untuk layanan yang benar-benar digunakan.

AWS Systems Manager

Quick Setup dan Explorer, yang merupakan kemampuan AWS Systems Manager, keduanya mendukung AWS Organizations dan beroperasi dari akun Manajemen Org.

Quick Setup adalah fitur otomatisasi Systems Manager. Ini memungkinkan akun Manajemen Org untuk dengan mudah menentukan konfigurasi untuk Systems Manager untuk terlibat atas nama Anda di seluruh akun di AWS organisasi Anda. Anda dapat mengaktifkan Pengaturan Cepat di seluruh AWS organisasi Anda atau memilih spesifik OUs. Penyiapan Cepat dapat menjadwalkan AWS

Systems Manager Agen (Agen SSM) untuk menjalankan pembaruan dua mingguan pada instans EC2 Anda dan dapat mengatur pemindaian harian instans tersebut untuk mengidentifikasi tambalan yang hilang.

Explorer adalah dasbor operasi yang dapat disesuaikan yang melaporkan informasi tentang sumber daya Anda AWS . Explorer menampilkan tampilan agregat data operasi untuk AWS akun Anda dan di seluruh Wilayah AWS akun. Ini termasuk data tentang instans EC2 Anda dan detail kepatuhan tambalan. Setelah menyelesaikan Penyiapan Terpadu (yang juga mencakup Systems Manager OpsCenter) di dalamnya AWS Organizations, Anda dapat mengumpulkan data di Explorer oleh OU atau untuk seluruh AWS organisasi. Systems Manager mengumpulkan data ke akun Manajemen AWS Org sebelum menampilkannya di Explorer.

Bagian OU Beban Kerja nanti dalam panduan ini membahas penggunaan Agen SSM pada instans EC2 di akun Aplikasi.

AWS Control Tower

AWS Control Towermenyediakan cara mudah untuk mengatur dan mengatur AWS lingkungan multi-akun yang aman, yang disebut landing zone. AWS Control Tower membuat landing zone Anda dengan menggunakan AWS Organizations, dan menyediakan pengelolaan akun dan tata kelola yang berkelanjutan serta penerapan praktik terbaik. Anda dapat menggunakan AWS Control Tower untuk menyediakan akun baru dalam beberapa langkah sambil memastikan bahwa akun tersebut sesuai dengan kebijakan organisasi Anda. Anda bahkan dapat menambahkan akun yang ada ke AWS Control Tower lingkungan baru.

AWS Control Tower memiliki serangkaian fitur yang luas dan fleksibel. Fitur utamanya adalah kemampuannya untuk mengatur kemampuan beberapa lainnya Layanan AWS, termasuk, dan IAM Identity Center AWS Organizations AWS Service Catalog, untuk membangun landing zone. Misalnya, secara default AWS Control Tower menggunakan AWS CloudFormation untuk menetapkan garis dasar, kebijakan kontrol AWS Organizations layanan (SCPs) untuk mencegah perubahan konfigurasi, dan Aturan AWS Config aturan untuk terus mendeteksi ketidaksesuaian. AWS Control Tower menggunakan cetak biru yang membantu Anda dengan cepat menyelaraskan AWS lingkungan multi-akun Anda dengan prinsip desain fondasi keamanan AWS Well Architected. Di antara fitur tata kelola, AWS Control Tower menawarkan pagar pembatas yang mencegah penyebaran sumber daya yang tidak sesuai dengan kebijakan yang dipilih.

Anda dapat mulai menerapkan panduan AWS SRA dengan AWS Control Tower. Misalnya, AWS Control Tower mendirikan AWS organisasi dengan arsitektur multi-akun yang direkomendasikan. Ini menyediakan cetak biru untuk menyediakan manajemen identitas, menyediakan akses federasi

ke akun, memusatkan logging, membuat audit keamanan lintas akun, menentukan alur kerja untuk penyediaan akun baru, dan menerapkan dasar akun dengan konfigurasi jaringan.

Dalam AWS SRA, AWS Control Tower berada dalam akun Manajemen Org karena AWS Control Tower menggunakan akun ini untuk mengatur AWS organisasi secara otomatis dan menunjuk akun itu sebagai akun manajemen. Akun ini digunakan untuk penagihan di seluruh AWS organisasi Anda. Ini juga digunakan untuk penyediaan akun Account Factory, untuk mengelola OUs, dan mengelola pagar pembatas. Jika Anda meluncurkan AWS Control Tower di AWS organisasi yang ada, Anda dapat menggunakan akun manajemen yang ada. AWS Control Tower akan menggunakan akun itu sebagai akun manajemen yang ditunjuk.

> Pertimbangan desain
>
> Jika Anda ingin melakukan baselining tambahan kontrol dan konfigurasi di seluruh akun Anda, Anda dapat menggunakan Customizations for (CFCT). AWS Control Tower Dengan CFCT, Anda dapat menyesuaikan AWS Control Tower landing zone Anda dengan menggunakan CloudFormation template dan SCPs. Anda dapat menerapkan templat dan kebijakan khusus ke akun individual dan OUs di dalam organisasi Anda. CFCT terintegrasi dengan peristiwa AWS Control Tower siklus hidup untuk memastikan bahwa penerapan sumber daya tetap sinkron dengan landing zone Anda.

AWS Artifact

AWS Artifactmenyediakan akses sesuai permintaan ke laporan AWS keamanan dan kepatuhan dan memilih perjanjian online. Laporan yang tersedia AWS Artifact termasuk laporan Sistem dan Kontrol Organisasi (SOC), laporan Industri Kartu Pembayaran (PCI), dan sertifikasi dari badan akreditasi di seluruh wilayah geografi dan vertikal kepatuhan yang memvalidasi implementasi dan efektivitas operasi kontrol keamanan. AWS AWS Artifact membantu Anda melakukan uji tuntas AWS dengan transparansi yang ditingkatkan ke dalam lingkungan kontrol keamanan kami. Ini juga memungkinkan Anda terus memantau keamanan dan kepatuhan AWS dengan akses langsung ke laporan baru.

AWS Artifact Perjanjian memungkinkan Anda untuk meninjau, menerima, dan melacak status AWS perjanjian seperti Adendum Rekanan Bisnis (BAA) untuk akun individu dan untuk akun yang merupakan bagian dari organisasi Anda. AWS Organizations

Anda dapat memberikan artefak AWS audit kepada auditor atau regulator Anda sebagai bukti kontrol keamanan. AWS Anda juga dapat menggunakan panduan tanggung jawab yang disediakan

oleh beberapa artefak AWS audit untuk merancang arsitektur cloud Anda. Panduan ini membantu menentukan kontrol keamanan tambahan yang dapat Anda lakukan untuk mendukung kasus penggunaan spesifik sistem Anda.

AWS Artifact di-host di akun Manajemen Org untuk menyediakan lokasi pusat tempat Anda dapat meninjau, menerima, dan mengelola perjanjian dengan AWS. Ini karena perjanjian yang diterima di akun manajemen mengalir ke akun anggota.

> **Pertimbangan desain**
>
> Pengguna dalam akun Manajemen Organisasi harus dibatasi untuk hanya menggunakan fitur Perjanjian AWS Artifact dan tidak ada yang lain. Untuk menerapkan pemisahan tugas, AWS Artifact juga di-host di akun Alat Keamanan tempat Anda dapat mendelegasikan izin kepada pemangku kepentingan kepatuhan dan auditor eksternal untuk mengakses artefak audit. Anda dapat menerapkan pemisahan ini dengan mendefinisikan kebijakan izin IAM berbutir halus. Sebagai contoh, lihat Contoh kebijakan IAM dalam AWS dokumentasi.

Pagar pembatas layanan keamanan terdistribusi dan terpusat

Di AWS SRA,,, Amazon AWS Security Hub GuardDuty, AWS Security Hub CSPM, IAM Access Analyzer AWS Config, jalur AWS CloudTrail organisasi, dan seringkali Amazon Macie dikerahkan dengan rangkaian pagar pembatas yang didelegasikan sesuai di seluruh akun dan juga menyediakan pemantauan, manajemen, dan tata kelola terpusat di seluruh organisasi Anda. AWS Anda akan menemukan grup layanan ini di setiap jenis akun yang diwakili dalam AWS SRA. Ini harus menjadi bagian dari Layanan AWS yang harus disediakan sebagai bagian dari proses orientasi dan baselining akun Anda. Repositori GitHub kode menyediakan contoh implementasi layanan yang AWS berfokus pada keamanan di seluruh akun Anda, termasuk akun Manajemen Org. AWS

Selain layanan ini, AWS SRA mencakup dua layanan yang berfokus pada keamanan, Amazon Detective dan AWS Audit Manager, yang mendukung integrasi dan fungsi administrator yang didelegasikan. AWS Organizations Namun, itu tidak termasuk sebagai bagian dari layanan yang direkomendasikan untuk baselining akun. Kami telah melihat bahwa layanan ini paling baik digunakan dalam skenario berikut:

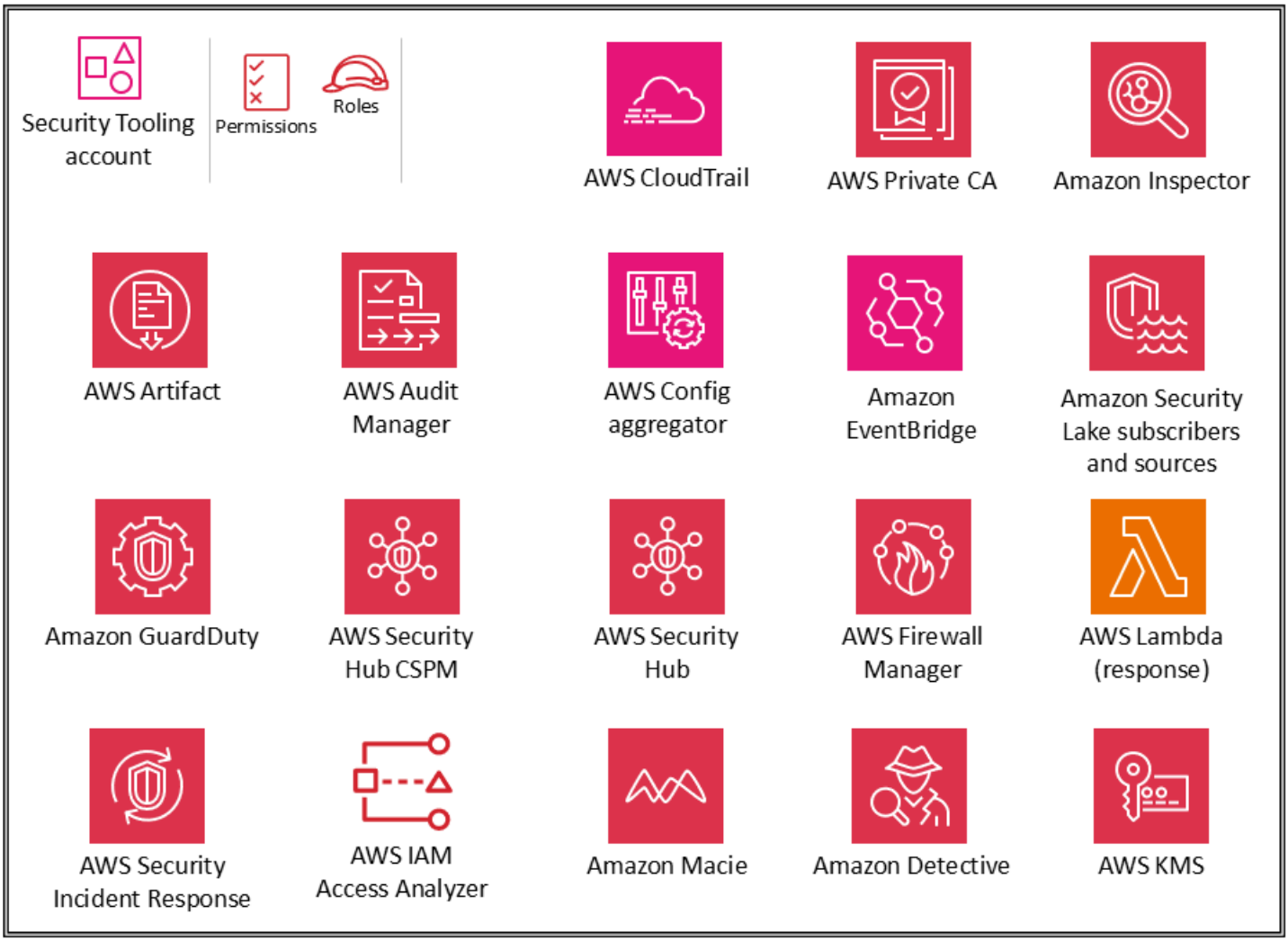
- Anda memiliki tim atau kelompok sumber daya khusus yang menjalankan fungsi forensik digital dan audit TI tersebut. Detective paling baik digunakan oleh tim analis keamanan, dan Audit Manager sangat membantu tim audit atau kepatuhan internal Anda.

- Anda ingin fokus pada seperangkat alat inti seperti AWS Config, Amazon GuardDuty AWS Security Hub, dan AWS Security Hub CSPM pada awal proyek Anda, dan kemudian membangunnya dengan menggunakan layanan yang memberikan kemampuan tambahan.

Security OU - Akun Perkakas Keamanan

Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

Diagram berikut menggambarkan layanan AWS keamanan yang dikonfigurasi di akun Security Tooling.



Akun Security Tooling didedikasikan untuk mengoperasikan layanan keamanan, memantau Akun AWS, dan mengotomatiskan peringatan dan respons keamanan. Tujuan keamanan meliputi:

- Berikan akun khusus dengan akses terkontrol untuk mengelola akses ke pagar pembatas keamanan, pemantauan, dan respons.
- Menjaga infrastruktur keamanan terpusat yang sesuai untuk memantau data operasi keamanan dan menjaga keterlacakan. Deteksi, investigasi, dan respons adalah bagian penting dari siklus hidup keamanan dan dapat digunakan untuk mendukung proses kualitas, kewajiban hukum atau kepatuhan, dan untuk upaya identifikasi dan respons ancaman.
- Lebih lanjut mendukung strategi defense-in-depth organisasi dengan mempertahankan lapisan kontrol lain atas konfigurasi dan operasi keamanan yang sesuai seperti kunci enkripsi dan pengaturan grup keamanan. Ini adalah akun tempat operator keamanan bekerja. Peran baca-hanya/audit untuk melihat informasi di AWS seluruh organisasi adalah tipikal, sedangkan write/modify peran terbatas jumlahnya, dikontrol ketat, dipantau, dan dicatat.

Pertimbangan desain

- AWS Control Tower menamai akun di bawah Keamanan OU Akun Audit secara default. Anda dapat mengganti nama akun selama AWS Control Tower pengaturan.
- Mungkin tepat untuk memiliki lebih dari satu akun Security Tooling. Misalnya, pemantauan dan respons terhadap peristiwa keamanan sering ditugaskan ke tim yang berdedikasi. Keamanan jaringan mungkin menjamin akun dan perannya sendiri bekerja sama dengan infrastruktur cloud atau tim jaringan. Perpecahan semacam itu mempertahankan tujuan memisahkan kantong keamanan terpusat dan lebih lanjut menekankan pemisahan tugas, hak istimewa paling sedikit, dan potensi kesederhanaan tugas tim. Jika Anda menggunakan AWS Control Tower, itu membatasi pembuatan tambahan Akun AWS di bawah Keamanan OU.

Administrator yang didelegasikan untuk layanan keamanan

Akun Security Tooling berfungsi sebagai akun administrator untuk layanan keamanan yang dikelola dalam administrator/member struktur di seluruh file. Akun AWS Seperti disebutkan sebelumnya, ini ditangani melalui fungsi administrator yang AWS Organizations didelegasikan. Layanan di AWS SRA yang saat ini mendukung administrator yang didelegasikan termasuk manajemen akses root terpusat IAM,, AWS Firewall Manager Amazon AWS Config, IAM Access Analyzer GuardDuty, Amazon

Macie,, Amazon Detective AWS Security Hub, Amazon AWS Security Hub CSPM Inspector,, dan. AWS Audit Manager AWS CloudTrail AWS Systems Manager Tim keamanan Anda mengelola fitur keamanan layanan ini dan memantau peristiwa atau temuan khusus keamanan apa pun.

AWS IAM Identity Center mendukung administrasi yang didelegasikan ke akun anggota. AWS SRA menggunakan akun Layanan Bersama sebagai akun administrator yang didelegasikan untuk Pusat Identitas IAM, seperti yang dijelaskan nanti di bagian Pusat Identitas IAM pada akun Layanan Bersama.

Akses root terpusat

Akun Security Tooling adalah akun administrator yang didelegasikan untuk manajemen terpusat IAM dari kemampuan akses root. Kemampuan ini harus diaktifkan di tingkat organisasi dengan mengaktifkan manajemen kredensi dan tindakan root istimewa di akun anggota. Administrator yang didelegasikan harus diberikan `sts:AssumeRoot` izin secara eksplisit untuk dapat mengambil tindakan root istimewa atas nama akun anggota. Izin ini hanya tersedia setelah tindakan root istimewa di akun anggota diaktifkan di Manajemen Org atau akun administrator yang didelegasikan. Dengan izin ini, pengguna dapat melakukan tugas pengguna root istimewa pada akun anggota, secara terpusat dari akun Security Tooling. Setelah meluncurkan sesi istimewa, Anda dapat menghapus kebijakan bucket S3 yang salah dikonfigurasi, menghapus kebijakan antrian SQS yang salah konfigurasi, menghapus kredensyal pengguna root untuk akun anggota, dan mengaktifkan kembali kredensyal pengguna root untuk akun anggota. Anda dapat melakukan tindakan ini dari konsol, dengan menggunakan AWS Command Line Interface (AWS CLI) atau melalui APIs.

AWS CloudTrail

AWS CloudTrailadalah layanan yang mendukung tata kelola, kepatuhan, dan audit aktivitas di Anda. Akun AWS Dengan CloudTrail, Anda dapat log, terus memantau, dan mempertahankan aktivitas akun yang terkait dengan tindakan di seluruh AWS infrastruktur Anda. CloudTrail terintegrasi dengan AWS Organizations, dan integrasi itu dapat digunakan untuk membuat jejak tunggal yang mencatat semua peristiwa untuk semua akun di AWS organisasi. Ini disebut sebagai jejak organisasi. Anda dapat membuat dan mengelola jejak organisasi hanya dari dalam akun manajemen untuk organisasi atau dari akun administrator yang didelegasikan. Saat Anda membuat jejak organisasi, jejak dengan nama yang Anda tentukan dibuat di setiap Akun AWS milik AWS organisasi Anda. Trail mencatat aktivitas untuk semua akun, termasuk akun manajemen, di AWS organisasi dan menyimpan log dalam satu bucket S3. Karena sensitivitas bucket S3 ini, Anda harus mengamankannya dengan mengikuti praktik terbaik yang diuraikan di Amazon S3 sebagai bagian penyimpanan log pusat nanti dalam panduan ini. Semua akun di AWS organisasi dapat melihat jejak organisasi dalam daftar jejak

mereka. Namun, anggota Akun AWS memiliki akses hanya lihat ke jalur ini. Secara default, saat Anda membuat jejak organisasi di CloudTrail konsol, jejak tersebut adalah jejak Multi-wilayah. Untuk praktik terbaik keamanan tambahan, lihat CloudTraildokumentasi.

Di AWS SRA, akun Security Tooling adalah akun administrator yang didelegasikan untuk mengelola. CloudTrail Bucket S3 yang sesuai untuk menyimpan log jejak organisasi dibuat di akun Arsip Log. Ini untuk memisahkan manajemen dan penggunaan hak istimewa CloudTrail log. Untuk informasi tentang cara membuat atau memperbarui bucket S3 untuk menyimpan file log untuk jejak organisasi, lihat CloudTrail dokumentasi. Sebagai praktik terbaik keamanan, tambahkan kunci `aws:SourceArn` kondisi jejak organisasi ke kebijakan sumber daya bucket S3 (dan sumber daya lainnya seperti kunci KMS atau topik SNS). Ini memastikan bahwa bucket S3 hanya menerima data yang terkait dengan jejak tertentu. Jejak dikonfigurasi dengan validasi file log untuk validasi integritas file log. File log dan digest dienkripsi dengan menggunakan SSE-KMS. Jejak organisasi juga terintegrasi dengan grup CloudWatch log di Log untuk mengirim acara untuk retensi jangka panjang.

> **Note**
>
> Anda dapat membuat dan mengelola jejak organisasi dari akun administrator manajemen dan delegasi. Namun, sebagai praktik terbaik, Anda harus membatasi akses ke akun manajemen dan menggunakan fungsionalitas administrator yang didelegasikan jika tersedia.

> **Pertimbangan desain**
>
> - CloudTrail tidak mencatat peristiwa data secara default, karena ini sering merupakan aktivitas volume tinggi. Namun, Anda harus menangkap peristiwa data untuk AWS sumber daya penting tertentu seperti bucket S3, fungsi Lambda, peristiwa log dari luar AWS yang dikirim ke CloudTrail danau, dan topik SNS. Untuk melakukannya, konfigurasikan jejak organisasi Anda untuk menyertakan peristiwa data dari sumber daya tertentu dengan menentukan ARNs masing-masing sumber daya individu.
> - Jika akun anggota memerlukan akses ke file CloudTrail log untuk akunnya sendiri, Anda dapat membagikan file CloudTrail log organisasi secara selektif dari bucket S3 pusat. Namun, jika akun anggota memerlukan grup CloudWatch log Amazon lokal untuk CloudTrail log akun mereka atau ingin mengonfigurasi manajemen log dan peristiwa data (hanya-baca, hanya tulis, peristiwa manajemen, peristiwa data) secara berbeda dari jejak

organisasi, mereka dapat membuat jejak lokal dengan kontrol yang sesuai. Jalur khusus akun lokal dikenakan biaya tambahan.

AWS Security Hub CSPM

AWS Security Hub Cloud Security Posture Management (AWS Security Hub CSPM) AWS Security Hub, yang sebelumnya dikenal sebagai, memberi Anda pandangan komprehensif tentang postur keamanan Anda AWS dan membantu Anda memeriksa lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Security Hub CSPM mengumpulkan data keamanan dari seluruh layanan AWS terintegrasi, produk pihak ketiga yang didukung, dan produk keamanan khusus lainnya yang mungkin Anda gunakan. Ini membantu Anda terus memantau dan menganalisis tren keamanan Anda dan mengidentifikasi masalah keamanan prioritas tertinggi. Selain sumber yang dicerna, Security Hub CSPM menghasilkan temuannya sendiri, yang diwakili oleh kontrol keamanan yang memetakan ke satu atau lebih standar keamanan. Standar ini termasuk Praktik Terbaik Keamanan AWS Dasar (FSBP), Tolok Ukur AWS Yayasan Center for Internet Security (CIS) v1.20 dan v1.4.0, Institut Nasional Standar dan Teknologi (NIST) SP 800-53 Rev. 5, Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS), dan standar yang dikelola layanan. Untuk daftar standar keamanan saat ini dan detail tentang kontrol keamanan tertentu, lihat referensi Standar untuk CSPM Security Hub di dokumentasi CSPM Security Hub.

Security Hub CSPM terintegrasi AWS Organizations untuk menyederhanakan manajemen postur keamanan di semua akun yang ada dan yang akan datang di organisasi Anda. AWS Anda dapat menggunakan fitur konfigurasi pusat CSPM Security Hub dari akun administrator yang didelegasikan (dalam hal ini, Perkakas Keamanan) untuk menentukan bagaimana layanan CSPM Security Hub, standar keamanan, dan kontrol keamanan dikonfigurasi di akun organisasi dan unit organisasi () di seluruh Wilayah. OUs Anda dapat mengonfigurasi pengaturan ini dalam beberapa langkah dari satu Wilayah utama, yang disebut sebagai Wilayah asal. Jika Anda tidak menggunakan konfigurasi pusat, Anda harus mengonfigurasi CSPM Security Hub secara terpisah di setiap akun dan Wilayah. Administrator yang didelegasikan dapat menetapkan akun dan OUs dikelola sendiri, di mana anggota dapat mengonfigurasi pengaturan secara terpisah di setiap Wilayah, atau dikelola secara terpusat, di mana administrator yang didelegasikan dapat mengonfigurasi akun anggota atau OU di seluruh Wilayah. Anda dapat menetapkan semua akun dan OUs di organisasi Anda sebagai dikelola secara terpusat, semua dikelola sendiri, atau kombinasi keduanya. Ini menyederhanakan penegakan konfigurasi yang konsisten sambil memberikan fleksibilitas untuk memodifikasinya untuk setiap OU dan akun.

Akun administrator yang didelegasikan CSPM Security Hub juga dapat melihat temuan, melihat wawasan, dan mengontrol detail dari semua akun anggota. Anda juga dapat menetapkan Wilayah agregasi dalam akun administrator yang didelegasikan untuk memusatkan temuan Anda di seluruh akun dan Wilayah tertaut Anda. Temuan Anda disinkronkan secara terus menerus dan dua arah antara Wilayah agregator dan semua Wilayah lainnya.

Security Hub CSPM mendukung integrasi dengan beberapa. Layanan AWS Amazon GuardDuty AWS Config, Amazon Macie, IAM Access Analyzer, Amazon AWS Firewall Manager Inspector, Amazon Route 53 Resolver DNS Firewall, dan AWS Systems Manager Patch Manager dapat memasukkan temuan ke Security Hub CSPM. Security Hub CSPM memproses temuan dengan menggunakan format standar yang disebut AWS Security Finding Format (ASFF). Security Hub CSPM menghubungkan temuan di seluruh produk terintegrasi untuk memprioritaskan yang paling penting. Anda dapat memperkaya metadata temuan CSPM Security Hub untuk membantu mengontekstualisasikan, memprioritaskan, dan mengambil tindakan yang lebih baik terhadap temuan keamanan. Pengayaan ini menambahkan tag sumber daya, tag AWS aplikasi baru, dan informasi nama akun ke setiap temuan yang dimasukkan ke dalam Security Hub CSPM. Ini membantu Anda menyempurnakan temuan untuk aturan otomatisasi, mencari atau memfilter temuan dan wawasan, dan menilai status postur keamanan berdasarkan aplikasi. Selain itu, Anda dapat menggunakan aturan otomatisasi untuk memperbarui temuan secara otomatis. Karena Security Hub CSPM mencerna temuan, CSPM dapat menerapkan berbagai tindakan aturan, seperti menekan temuan, mengubah tingkat keparahannya, dan menambahkan catatan ke temuan. Tindakan aturan ini berlaku ketika temuan cocok dengan kriteria yang Anda tentukan, seperti sumber daya atau akun IDs yang terkait dengan temuan tersebut, atau judulnya. Anda dapat menggunakan aturan otomatisasi untuk memperbarui bidang pencarian tertentu di ASFF. Aturan berlaku untuk temuan baru dan yang diperbarui.

Selama penyelidikan peristiwa keamanan, Anda dapat menavigasi dari Security Hub CSPM ke Amazon Detective untuk menyelidiki temuan. GuardDuty Security Hub CSPM merekomendasikan untuk menyelaraskan akun administrator yang didelegasikan untuk layanan seperti Detective (di mana mereka ada) untuk integrasi yang lebih lancar. Misalnya, jika Anda tidak menyelaraskan akun administrator antara Detective dan Security Hub CSPM, menavigasi dari temuan ke Detective tidak akan berhasil. Untuk daftar lengkap, lihat Ikhtisar Layanan AWS integrasi dengan Security Hub CSPM di dokumentasi CSPM Security Hub.

Anda dapat menggunakan Security Hub CSPM dengan fitur Network Access Analyzer dari Amazon VPC untuk membantu terus memantau kepatuhan konfigurasi jaringan Anda. AWS Ini akan membantu Anda memblokir akses jaringan yang tidak diinginkan dan membantu mencegah sumber daya penting Anda dari akses eksternal. Untuk detail arsitektur dan implementasi lebih lanjut, lihat

posting AWS blog Verifikasi berkelanjutan kepatuhan jaringan menggunakan Amazon VPC Network Access Analyzer dan. AWS Security Hub CSPM

Selain fitur pemantauannya, Security Hub CSPM mendukung integrasi dengan Amazon EventBridge untuk mengotomatiskan remediasi temuan tertentu. Anda dapat menentukan tindakan kustom yang akan diambil ketika temuan diterima. Misalnya, Anda dapat mengonfigurasi tindakan kustom untuk mengirim temuan ke sistem tiket atau ke sistem remediasi otomatis. Untuk diskusi dan contoh tambahan, lihat posting AWS blog Respons dan remediasi otomatis dengan AWS Security Hub CSPM dan Cara menerapkan AWS solusi untuk respons dan remediasi otomatis CSPM Security Hub.

Security Hub CSPM menggunakan layanan terkait Aturan AWS Config untuk melakukan sebagian besar pemeriksaan keamanannya untuk kontrol. Untuk mendukung kontrol ini, AWS Config harus diaktifkan di semua akun — termasuk akun administrator (atau administrator yang didelegasikan) dan akun anggota — di masing-masing tempat CSPM Security AWS Region Hub diaktifkan.

Pertimbangan desain

- Jika standar kepatuhan, seperti PCI-DSS, sudah ada di Security Hub CSPM, layanan CSPM Security Hub yang dikelola sepenuhnya adalah cara termudah untuk mengoperasionalisasikannya. Namun, jika Anda ingin merakit standar kepatuhan atau keamanan Anda sendiri, yang mungkin mencakup pemeriksaan keamanan, operasional, atau pengoptimalan biaya, paket AWS Config kesesuaian menawarkan proses penyesuaian yang disederhanakan. (Untuk informasi lebih lanjut tentang AWS Config dan paket kesesuaian, lihat bagian AWS Config.)
- Kasus penggunaan umum untuk Security Hub CSPM meliputi:
  - Sebagai dasbor yang memberikan visibilitas bagi pemilik aplikasi ke dalam postur keamanan dan kepatuhan sumber daya mereka AWS
  - Sebagai pandangan sentral dari temuan keamanan yang digunakan oleh operasi keamanan, responden insiden, dan pemburu ancaman untuk melakukan triase dan mengambil tindakan terhadap temuan AWS keamanan dan kepatuhan di seluruh dan Wilayah Akun AWS
  - Untuk menggabungkan dan merutekan temuan keamanan dan kepatuhan dari seluruh Akun AWS wilayah, ke informasi keamanan terpusat dan manajemen peristiwa (SIEM) atau sistem orkestrasi keamanan lainnya

Untuk panduan tambahan tentang kasus penggunaan ini, termasuk cara mengaturnya, lihat posting blog Tiga pola penggunaan CSPM Security Hub berulang dan cara menerapkannya.

Contoh implementasi

Pustaka kode AWS SRA menyediakan contoh implementasi Security Hub CSPM. Ini mencakup pemberdayaan otomatis layanan, administrasi yang didelegasikan ke akun anggota (Security Tooling), dan konfigurasi untuk mengaktifkan Security Hub CSPM untuk semua akun yang ada dan yang akan datang di organisasi. AWS

AWS Security Hub

AWS Security Hubadalah solusi keamanan cloud terpadu yang memprioritaskan ancaman keamanan kritis Anda dan membantu Anda merespons dalam skala besar. Security Hub mendeteksi masalah keamanan dalam waktu dekat dengan secara otomatis menghubungkan dan memperkaya sinyal keamanan dari berbagai sumber, seperti manajemen postur (), manajemen kerentanan (Amazon Inspector AWS Security Hub CSPM), data sensitif (Amazon Macie), dan deteksi ancaman (Amazon). GuardDuty Hal ini memungkinkan tim keamanan untuk memprioritaskan risiko aktif di lingkungan cloud mereka melalui analisis otomatis dan wawasan kontekstual. Security Hub menyediakan representasi visual dari jalur serangan potensial yang dapat dimanfaatkan penyerang untuk mendapatkan akses ke sumber daya yang terkait dengan temuan eksposur. Ini mengubah sinyal keamanan yang kompleks menjadi wawasan yang dapat ditindaklanjuti, sehingga Anda dapat membuat keputusan berdasarkan informasi tentang keamanan Anda dengan cepat.

Security Hub telah didesain ulang secara strategis untuk menyederhanakan pemberdayaan blok bangunan layanan keamanan terkait untuk mencapai hasil keamanan. Dengan mengkorelasikan temuan keamanan dalam matriks ancaman di berbagai sinyal keamanan dalam waktu dekat, Anda dapat memprioritaskan risiko paling kritis terlebih dahulu. Temuan ini berkorelasi untuk mendeteksi paparan yang terkait dengan AWS sumber daya. Eksposur mewakili kelemahan yang lebih luas dalam kontrol keamanan, kesalahan konfigurasi, atau area lain yang dapat dieksploitasi oleh ancaman aktif. Misalnya, eksposur mungkin merupakan instance EC2 yang dapat dijangkau dari internet dan memiliki kerentanan perangkat lunak yang memiliki kemungkinan eksploitasi tinggi.

Security Hub dan Security Hub CSPM adalah layanan pelengkap. Security Hub CSPM memberikan pandangan komprehensif tentang postur keamanan Anda dan membantu Anda mengevaluasi lingkungan cloud Anda terhadap standar industri keamanan dan praktik terbaik. Security Hub memberikan pengalaman terpadu yang membantu Anda memprioritaskan dan menanggapi masalah keamanan kritis. Temuan CSPM Security Hub diarahkan ke Security Hub secara otomatis, di mana mereka berkorelasi dengan temuan dari layanan keamanan lain, seperti Amazon Inspector, untuk menghasilkan eksposur. Ini membantu Anda mengidentifikasi risiko paling kritis di lingkungan Anda.

Security Hub juga menyediakan ringkasan sumber daya di AWS lingkungan Anda berdasarkan jenis dan temuan terkait. Sumber daya diprioritaskan oleh eksposur dan urutan serangan. Saat memilih jenis sumber daya, Anda dapat meninjau semua sumber daya yang terkait dengan jenis sumber daya tersebut.

Untuk pengalaman yang optimal, sebaiknya aktifkan Security Hub dan Security Hub CSPM serta mengaktifkan layanan keamanan lainnya: Amazon, Amazon GuardDuty Inspector, dan Amazon Macie. Anda dapat memperoleh visibilitas apakah layanan dan fitur ini diaktifkan secara seragam di semua akun anggota organisasi Anda dengan menggunakan temuan Cakupan Security Hub.

Di AWS SRA, akun Security Tooling bertindak sebagai administrator yang didelegasikan untuk Security Hub, Security Hub CSPM, dan layanan keamanan lainnya. AWS Dalam akun Security Tooling Anda dapat melihat semua sumber daya yang terkait dengan akun anggota. Anda juga dapat melihat semua sumber daya di rumah Anda AWS Region dari yang ditautkan Wilayah AWS.

> **Catatan implementasi**
>
> Mengaktifkan Security Hub memerlukan tiga langkah, termasuk prosedur yang memperhitungkan apakah sebelumnya Anda telah mengaktifkan Security Hub CSPM. Security Hub terintegrasi secara native AWS Organizations, yang menyederhanakan proses konfigurasi dan implementasi, serta memusatkan dan menggabungkan semua temuan ke dalam satu lokasi. Sesuai dengan praktik terbaik AWS SRA, gunakan akun Security Tooling sebagai akun administrator yang didelegasikan untuk mengelola dan mengonfigurasi Security Hub. Gunakan pengaturan konfigurasi Security Hub untuk mengaktifkan semua Wilayah OUs, dan akun secara otomatis, termasuk Wilayah dan akun future. Anda juga harus mengatur agregasi Lintas wilayah untuk mengumpulkan temuan, sumber daya, dan tren dari beberapa Wilayah AWS ke dalam satu Wilayah asal. Selama konfigurasi, Anda juga dapat mengaktifkan integrasi asli seperti Jira Cloud atau. ServiceNow

Pertimbangan desain

- Temuan Security Hub diformat dalam Open Cybersecurity Schema Framework (OCSF). Security Hub menghasilkan temuan di OCSF dan menerima temuan di OCSF dari Security Hub CSPM dan lainnya. Layanan AWS Temuan OCSF ini dapat dikirim melalui Amazon EventBridge untuk otomatisasi atau disimpan di akun agregasi log pusat untuk melakukan analisis dan retensi log keamanan.
- Akun Manajemen AWS Org tidak dapat menunjuk dirinya sebagai administrator yang didelegasikan di Security Hub. Ini sejalan dengan praktik terbaik AWS SRA untuk menunjuk akun Security Tooling sebagai administrator yang didelegasikan. Perhatikan juga:
  - Akun administrator yang ditunjuk untuk Security Hub CSPM secara otomatis menjadi administrator yang ditunjuk untuk Security Hub.
  - Menghapus administrasi yang didelegasikan melalui Security Hub juga menghapus administrasi yang didelegasikan untuk Security Hub CSPM. Demikian juga, menghapus administrasi yang didelegasikan melalui Security Hub CSPM juga menghapusnya untuk Security Hub.
- Security Hub menyertakan fitur yang secara otomatis memodifikasi dan mengambil tindakan atas temuan berdasarkan spesifikasi Anda, Security Hub mendukung jenis otomatisasi berikut:
  - Aturan otomatisasi, yang secara otomatis memperbarui temuan, menekan temuan, dan mengirim temuan ke alat tiket dalam waktu dekat berdasarkan kriteria yang ditentukan.
  - Respons dan remediasi otomatis, yang membuat EventBridge aturan khusus yang menentukan tindakan otomatis yang harus diambil terhadap temuan dan wawasan tertentu.
- Security Hub dapat mengonfigurasi Amazon Inspector di semua akun anggota dan Wilayah melalui kebijakan, serta dapat mengonfigurasi GuardDuty dan Security Hub CSPM melalui penerapan. Kebijakan menghasilkan AWS Organizations kebijakan untuk akun dan Wilayah. Penerapan adalah tindakan satu kali yang memungkinkan kemampuan keamanan di seluruh akun dan Wilayah yang dipilih. Penerapan tidak berlaku untuk akun yang baru diaktifkan. Sebagai alternatif, Anda dapat mengaktifkan fitur secara otomatis untuk akun anggota baru di GuardDuty dan Security Hub CSPM.

Amazon GuardDuty

Amazon GuardDuty adalah layanan deteksi ancaman yang terus memantau aktivitas berbahaya dan perilaku tidak sah untuk melindungi Anda Akun AWS dan beban kerja. Anda harus selalu menangkap dan menyimpan log yang sesuai untuk tujuan pemantauan dan audit, tetapi GuardDuty menarik aliran data independen langsung dari, log aliran VPC AWS CloudTrail Amazon, dan log DNS. AWS Anda tidak perlu mengelola kebijakan bucket Amazon S3 atau mengubah cara Anda mengumpulkan dan menyimpan log Anda. GuardDutyizin dikelola sebagai peran terkait layanan yang dapat Anda cabut kapan saja dengan menonaktifkannya. GuardDuty Ini memudahkan untuk mengaktifkan layanan tanpa konfigurasi yang rumit, dan menghilangkan risiko bahwa modifikasi izin IAM atau perubahan kebijakan bucket S3 akan memengaruhi pengoperasian layanan.

Selain menyediakan sumber data dasar, GuardDuty menyediakan fitur opsional untuk mengidentifikasi temuan keamanan. Ini termasuk Perlindungan EKS, Perlindungan RDS, Perlindungan S3, Perlindungan Malware, dan Perlindungan Lambda. Untuk detektor baru, fitur opsional ini diaktifkan secara default kecuali untuk Perlindungan EKS, yang harus diaktifkan secara manual.

- Dengan Perlindungan GuardDuty S3, GuardDuty memantau peristiwa data Amazon S3 CloudTrail selain peristiwa manajemen CloudTrail default. Memantau peristiwa data memungkinkan GuardDuty untuk memantau operasi API tingkat objek untuk potensi risiko keamanan terhadap data dalam bucket S3 Anda.
- GuardDuty Perlindungan Malware mendeteksi keberadaan malware di instans Amazon EC2 atau beban kerja kontainer dengan memulai pemindaian tanpa agen pada volume Amazon Elastic Block Store (Amazon EBS) terlampir. GuardDuty juga mendeteksi potensi malware di bucket S3 dengan memindai objek yang baru diunggah atau versi baru dari objek yang ada.
- GuardDuty Perlindungan RDS dirancang untuk memprofilkan dan memantau aktivitas akses ke database Amazon Aurora tanpa memengaruhi kinerja basis data.
- GuardDuty Perlindungan EKS mencakup Pemantauan Log Audit EKS dan Pemantauan Runtime EKS. Dengan EKS Audit Log Monitoring, GuardDuty memantau log audit Kubernetes dari klaster Amazon EKS dan menganalisisnya untuk aktivitas yang berpotensi berbahaya dan mencurigakan. EKS Runtime Monitoring menggunakan agen GuardDuty keamanan (yang merupakan add-on Amazon EKS) untuk memberikan visibilitas runtime ke beban kerja Amazon EKS individual. Agen GuardDuty keamanan membantu mengidentifikasi kontainer tertentu dalam kluster Amazon EKS Anda yang berpotensi dikompromikan. Ini juga dapat mendeteksi upaya untuk meningkatkan hak istimewa dari wadah individu ke host Amazon EC2 yang mendasarinya atau ke lingkungan yang lebih luas. AWS

GuardDuty juga menyediakan fitur yang dikenal sebagai Extended Threat Detection yang secara otomatis mendeteksi serangan multi-tahap yang menjangkau sumber data, berbagai jenis AWS sumber daya, dan waktu dalam file. Akun AWS GuardDutymenghubungkan peristiwa-peristiwa ini, yang disebut sinyal, untuk mengidentifikasi skenario yang menampilkan diri sebagai ancaman potensial terhadap AWS lingkungan Anda, dan kemudian menghasilkan temuan urutan serangan. Ini mencakup skenario ancaman yang melibatkan kompromi yang terkait dengan penyalahgunaan AWS kredensil, dan upaya kompromi data dalam Anda. Akun AWS GuardDuty menganggap semua jenis pencarian urutan serangan sebagai Kritis. Fitur ini diaktifkan secara default, dan tidak ada biaya tambahan yang terkait dengannya.

Di AWS SRA, GuardDuty diaktifkan di semua akun melalui AWS Organizations, dan semua temuan dapat dilihat dan ditindaklanjuti oleh tim keamanan yang sesuai di akun administrator yang GuardDuty didelegasikan (dalam hal ini, akun Perkakas Keamanan). GuardDuty Temuan aktif diekspor ke bucket S3 pusat di akun Log Archive, sehingga Anda dapat menyimpan temuan lebih dari 90 hari. Temuan ini diekspor dari akun administrator yang didelegasikan dan juga mencakup semua temuan dari akun anggota terkait di Wilayah yang sama. Temuan di bucket S3 dienkripsi dengan kunci yang dikelola AWS KMS pelanggan. Kebijakan bucket S3 dan kebijakan kunci KMS dikonfigurasi agar hanya GuardDuty mengizinkan penggunaan sumber daya.

Ketika AWS Security Hub CSPM diaktifkan, GuardDuty temuan secara otomatis mengalir ke Security Hub CSPM dan Security Hub. Ketika Amazon Detective diaktifkan, GuardDuty temuan dimasukkan dalam proses log ingest Detective. GuardDuty dan Detective mendukung alur kerja pengguna lintas layanan, di mana GuardDuty menyediakan tautan dari konsol yang mengarahkan Anda dari temuan yang dipilih ke halaman Detektif yang berisi serangkaian visualisasi yang dikuratori untuk menyelidiki temuan itu. Misalnya, Anda juga dapat berintegrasi GuardDuty dengan Amazon EventBridge untuk mengotomatiskan praktik terbaik GuardDuty, seperti mengotomatiskan tanggapan terhadap temuan baru GuardDuty .

> **Contoh implementasi**
>
> Pustaka kode AWS SRA menyediakan contoh implementasi. GuardDuty Ini mencakup konfigurasi bucket S3 terenkripsi, administrasi yang didelegasikan, dan GuardDuty pemberdayaan untuk semua akun yang ada dan yang akan datang di organisasi. AWS

AWS Config

AWS Configadalah layanan yang memungkinkan Anda menilai, mengaudit, dan mengevaluasi konfigurasi AWS sumber daya yang didukung di Anda Akun AWS. AWS Config terus memantau dan merekam konfigurasi AWS sumber daya, dan secara otomatis mengevaluasi konfigurasi yang direkam terhadap konfigurasi yang diinginkan. Anda juga dapat berintegrasi AWS Config dengan layanan lain untuk melakukan pekerjaan berat dalam jalur audit dan pemantauan otomatis. Misalnya, AWS Config dapat memantau perubahan rahasia individu di AWS Secrets Manager.

Anda dapat mengevaluasi pengaturan konfigurasi AWS sumber daya Anda dengan menggunakan Aturan AWS Config. AWS Config menyediakan pustaka aturan standar yang dapat disesuaikan yang disebut aturan terkelola, atau Anda dapat menulis aturan kustom Anda sendiri. Anda dapat menjalankan Aturan AWS Config dalam mode proaktif (sebelum sumber daya telah digunakan) atau mode detektif (setelah sumber daya telah digunakan). Sumber daya dapat dievaluasi ketika ada perubahan konfigurasi, pada jadwal berkala, atau keduanya.

Paket kesesuaian adalah kumpulan AWS Config aturan dan tindakan remediasi yang dapat digunakan sebagai entitas tunggal di akun dan Wilayah, atau di seluruh organisasi di. AWS Organizations Paket kesesuaian dibuat dengan membuat template YAMM yang berisi daftar aturan AWS Config terkelola atau kustom dan tindakan remediasi. Untuk mulai mengevaluasi AWS lingkungan Anda, gunakan salah satu contoh templat paket kesesuaian.

AWS Config terintegrasi dengan AWS Security Hub CSPM untuk mengirimkan hasil evaluasi aturan AWS Config terkelola dan kustom sebagai temuan ke Security Hub CSPM.

Aturan AWS Config dapat digunakan bersama dengan AWS Systems Manager untuk secara efektif memulihkan sumber daya yang tidak sesuai. Anda menggunakan Systems Manager Explorer untuk mengumpulkan status kepatuhan AWS Config aturan di Akun AWS seluruh wilayah Anda Wilayah AWS dan kemudian menggunakan dokumen Otomasi Systems Manager (runbook) untuk menyelesaikan aturan yang tidak sesuai AWS Config . Untuk detail implementasi, lihat posting blog Memulihkan AWS Config aturan yang tidak sesuai dengan AWS Systems Manager runbook Otomasi.

AWS Config Agregator mengumpulkan data konfigurasi dan kepatuhan di beberapa akun, Wilayah, dan organisasi di. AWS Organizations Dasbor agregator menampilkan data konfigurasi sumber daya agregat. Dasbor inventaris dan kepatuhan menawarkan informasi penting dan terkini tentang konfigurasi AWS sumber daya dan status kepatuhan Anda di seluruh Akun AWS, di seluruh Wilayah AWS, atau di dalam organisasi AWS . Mereka memungkinkan Anda untuk memvisualisasikan dan menilai inventaris AWS sumber daya Anda tanpa perlu menulis kueri AWS Config lanjutan. Anda bisa mendapatkan wawasan penting seperti ringkasan kepatuhan berdasarkan sumber daya, 10 akun

teratas yang memiliki sumber daya yang tidak sesuai, perbandingan instans EC2 yang berjalan dan dihentikan berdasarkan jenis, dan volume EBS berdasarkan jenis dan ukuran volume.

Jika Anda menggunakannya AWS Control Tower untuk mengelola AWS organisasi Anda, itu akan menerapkan seperangkat AWS Config aturan sebagai pagar pembatas detektif (dikategorikan sebagai wajib, sangat disarankan, atau elektif). Pagar pembatas ini membantu Anda mengatur sumber daya dan memantau kepatuhan di seluruh akun di organisasi Anda. AWS AWS Config Aturan ini akan secara otomatis menggunakan `aws-control-tower` tag yang memiliki nilai`managed-by-control-tower`.

AWS Config harus diaktifkan untuk setiap akun anggota di AWS organisasi dan AWS Region yang berisi sumber daya yang ingin Anda lindungi. Anda dapat mengelola AWS Config aturan (misalnya, membuat, memperbarui, dan menghapus) secara terpusat di semua akun dalam AWS organisasi Anda. Dari akun administrator AWS Config yang didelegasikan, Anda dapat menerapkan seperangkat AWS Config aturan umum di semua akun dan menentukan akun di mana AWS Config aturan tidak boleh dibuat. Akun administrator AWS Config yang didelegasikan juga dapat menggabungkan konfigurasi sumber daya dan data kepatuhan dari semua akun anggota untuk memberikan satu tampilan. Gunakan APIs dari akun administrator yang didelegasikan untuk menegakkan tata kelola dengan memastikan bahwa AWS Config aturan dasar tidak dapat diubah oleh akun anggota di organisasi Anda. AWS AWS Config terintegrasi secara native untuk mengirim temuan ke AWS Security Hub CSPM, jika Security Hub CSPM diaktifkan dan setidaknya ada satu aturan AWS Config terkelola atau kustom.

Di AWS SRA, akun administrator yang AWS Config didelegasikan adalah akun Security Tooling. Saluran AWS Config pengiriman dikonfigurasi untuk mengirimkan snapshot konfigurasi sumber daya dalam bucket S3 terpusat di akun Arsip Log. Karena akun Arsip Log adalah penyimpanan repositori log pusat, akun ini digunakan untuk menyimpan konfigurasi sumber daya.

Pertimbangan desain

- AWS Config konfigurasi streaming dan pemberitahuan perubahan kepatuhan ke Amazon EventBridge. Ini berarti Anda dapat menggunakan kemampuan pemfilteran asli EventBridge untuk memfilter AWS Config peristiwa sehingga Anda dapat merutekan jenis pemberitahuan tertentu ke target tertentu. Misalnya, Anda dapat mengirim pemberitahuan kepatuhan untuk aturan atau jenis sumber daya tertentu ke alamat email tertentu, atau merutekan pemberitahuan perubahan konfigurasi ke alat manajemen layanan TI eksternal (ITSM) atau database manajemen konfigurasi (CMDB). Untuk informasi lebih lanjut, lihat praktik AWS Config terbaik posting blog.

- Selain menggunakan evaluasi aturan AWS Config proaktif, Anda dapat menggunakan AWS CloudFormation Guard, yang merupakan alat policy-as-code evaluasi yang secara proaktif memeriksa kepatuhan konfigurasi sumber daya. Antarmuka baris AWS CloudFormation Guard perintah (CLI) memberi Anda deklaratif, bahasa khusus domain (DSL) yang dapat Anda gunakan untuk mengekspresikan kebijakan sebagai kode. Selain itu, Anda dapat menggunakan AWS CLI perintah untuk memvalidasi data terstruktur berformat JSON atau YAML seperti set CloudFormation perubahan, file konfigurasi Terraform berbasis JSON, atau konfigurasi Kubernetes. Anda dapat menjalankan evaluasi secara lokal dengan menggunakan AWS CloudFormation Guard CLI sebagai bagian dari proses penulisan Anda atau menjalankannya dalam pipeline penerapan Anda. Jika Anda memiliki AWS Cloud Development Kit (AWS CDK)aplikasi, Anda dapat menggunakan cdk-nag untuk memeriksa praktik terbaik secara proaktif.

Contoh implementasi

Pustaka kode AWS SRA menyediakan contoh implementasi yang menyebarkan paket AWS Config kesesuaian ke semua Akun AWS dan Wilayah dalam suatu organisasi. AWS Modul AWS Config Aggregator membantu Anda mengonfigurasi AWS Config agregator dengan mendelegasikan administrasi ke akun anggota (Security Tooling) dalam akun Manajemen Org dan kemudian mengonfigurasi AWS Config Aggregator dalam akun administrator yang didelegasikan untuk semua akun yang ada dan yang akan datang di organisasi. AWS Anda dapat menggunakan modul AWS Config Control Tower Management Account untuk mengaktifkan AWS Config dalam akun Manajemen Org–tidak diaktifkan oleh. AWS Control Tower

Amazon Security Lake

Amazon Security Lake adalah layanan danau data keamanan yang dikelola sepenuhnya. Anda dapat menggunakan Security Lake untuk secara otomatis memusatkan data keamanan dari AWS lingkungan, penyedia perangkat lunak sebagai layanan (SaaS), di tempat, dan sumber pihak ketiga. Security Lake membantu Anda membangun sumber data yang dinormalisasi yang menyederhanakan penggunaan alat analitik daripada data keamanan, sehingga Anda bisa mendapatkan pemahaman yang lebih lengkap tentang postur keamanan Anda di seluruh organisasi. Data lake didukung oleh bucket Amazon Simple Storage Service (Amazon S3), dan Anda mempertahankan kepemilikan atas data Anda. Security Lake secara otomatis mengumpulkan log untuk Layanan AWS, termasuk AWS

CloudTrail, Amazon VPC, Amazon Route 53, Amazon S3 AWS Lambda,, AWS Security Hub CSPM log audit Amazon EKS, temuan, dan log. AWS WAF

AWS SRA merekomendasikan agar Anda menggunakan akun Arsip Log sebagai akun administrator yang didelegasikan untuk Security Lake. Untuk informasi selengkapnya tentang menyiapkan akun administrator yang didelegasikan, lihat Amazon Security Lake di bagian Security OU - Log Archive account. Tim keamanan yang ingin mengakses data Security Lake atau memerlukan kemampuan untuk menulis log non-asli ke bucket Security Lake dengan menggunakan fungsi ekstrak, transformasi, dan pemuatan (ETL) kustom harus beroperasi dalam akun Security Tooling.

Security Lake dapat mengumpulkan log dari penyedia cloud yang berbeda, log dari solusi pihak ketiga, atau log khusus lainnya. Kami menyarankan Anda menggunakan akun Security Tooling untuk melakukan fungsi ETL untuk mengonversi log ke format Open Cybersecurity Schema Framework (OCSF) dan mengeluarkan file dalam format Apache Parquet. Security Lake membuat peran lintas akun dengan izin yang tepat untuk akun Security Tooling dan sumber kustom yang didukung oleh fungsi atau AWS Glue crawler Lambda, untuk menulis data ke bucket S3 untuk Security Lake.

Administrator Security Lake harus mengonfigurasi tim keamanan yang menggunakan akun Security Tooling dan memerlukan akses ke log yang dikumpulkan Security Lake sebagai pelanggan. Security Lake mendukung dua jenis akses pelanggan:

- Akses data — Pelanggan dapat langsung mengakses objek Amazon S3 untuk Security Lake. Security Lake mengelola infrastruktur dan izin. Saat Anda mengonfigurasi akun Security Tooling sebagai pelanggan akses data Security Lake, akun akan diberi tahu tentang objek baru di bucket Security Lake melalui Amazon Simple Queue Service (Amazon SQS), dan Security Lake membuat izin untuk mengakses objek baru tersebut.
- Akses kueri — Pelanggan dapat melakukan kueri data sumber dari AWS Lake Formation tabel di bucket S3 Anda dengan menggunakan layanan seperti Amazon Athena. Akses lintas akun diatur secara otomatis untuk akses kueri dengan menggunakan Lake Formation. Saat Anda mengonfigurasi akun Security Tooling sebagai pelanggan akses kueri Security Lake, akun tersebut diberikan akses hanya-baca ke log di akun Security Lake. Saat Anda menggunakan jenis pelanggan ini, Athena AWS Glue dan tabel dibagikan dari akun Security Lake Log Archive dengan akun Security Tooling melalui (). AWS Resource Access Manager AWS RAM Untuk mengaktifkan kemampuan ini, Anda harus memperbarui pengaturan berbagi data lintas akun ke versi 3.

Untuk informasi selengkapnya tentang membuat pelanggan, lihat Manajemen pelanggan di dokumentasi Security Lake.

Untuk praktik terbaik untuk menyerap sumber kustom, lihat Mengumpulkan data dari sumber kustom dalam dokumentasi Security Lake.

Anda dapat menggunakan Amazon Quick Sight, Amazon OpenSearch Service, dan Amazon SageMaker untuk menyiapkan analitik terhadap data keamanan yang Anda simpan di Security Lake.

> **Pertimbangan desain**
>
> Jika tim aplikasi memerlukan akses kueri ke data Security Lake untuk memenuhi persyaratan bisnis, administrator Security Lake harus mengonfigurasi akun Aplikasi tersebut sebagai pelanggan.

Amazon Macie

Amazon Macie adalah layanan keamanan data dan privasi data yang dikelola sepenuhnya yang menggunakan pembelajaran mesin dan pencocokan pola untuk menemukan dan membantu melindungi data sensitif Anda. AWS Anda perlu mengidentifikasi jenis dan klasifikasi data yang sedang diproses oleh beban kerja Anda untuk memastikan bahwa kontrol yang tepat diberlakukan. Anda dapat menggunakan Macie untuk mengotomatiskan penemuan dan pelaporan data sensitif dengan dua cara: dengan melakukan penemuan data sensitif otomatis dan dengan membuat dan menjalankan pekerjaan penemuan data sensitif. Dengan penemuan data sensitif otomatis, Macie mengevaluasi inventaris bucket S3 Anda setiap hari dan menggunakan teknik pengambilan sampel untuk mengidentifikasi dan memilih objek S3 yang representatif dari bucket Anda. Macie kemudian mengambil dan menganalisis objek yang dipilih, memeriksanya untuk data sensitif. Pekerjaan penemuan data sensitif memberikan analisis yang lebih dalam dan lebih bertarget. Dengan opsi ini, Anda menentukan luas dan kedalaman analisis, termasuk bucket S3 untuk dianalisis, kedalaman pengambilan sampel, dan kriteria khusus yang berasal dari properti objek S3. Jika Macie mendeteksi potensi masalah dengan keamanan atau privasi ember, itu menciptakan temuan kebijakan untuk Anda. Penemuan data otomatis diaktifkan secara default untuk semua pelanggan Macie baru, dan pelanggan Macie yang ada dapat mengaktifkannya dengan satu klik.

Macie diaktifkan di semua akun melalui AWS Organizations. Prinsipal yang memiliki izin yang sesuai di akun administrator yang didelegasikan (dalam hal ini, akun Alat Keamanan) dapat mengaktifkan atau menangguhkan Macie di akun apa pun, membuat pekerjaan penemuan data sensitif untuk bucket yang dimiliki oleh akun anggota, dan melihat semua temuan kebijakan untuk semua akun anggota. Temuan data sensitif hanya dapat dilihat oleh akun yang menciptakan pekerjaan temuan

sensitif. Untuk informasi selengkapnya, lihat Mengelola beberapa akun Macie sebagai organisasi dalam dokumentasi Macie.

Temuan Macie mengalir ke AWS Security Hub CSPM untuk ditinjau dan dianalisis. Macie juga terintegrasi dengan Amazon EventBridge untuk memfasilitasi respons otomatis terhadap temuan seperti peringatan, umpan ke sistem informasi keamanan dan manajemen peristiwa (SIEM), dan remediasi otomatis.

Pertimbangan desain

- Jika objek S3 dienkripsi dengan kunci AWS Key Management Service (AWS KMS) yang Anda kelola, Anda dapat menambahkan peran terkait layanan Macie sebagai pengguna kunci ke kunci KMS tersebut untuk memungkinkan Macie memindai data.
- Macie dioptimalkan untuk memindai objek di Amazon S3. Akibatnya, semua jenis objek yang didukung MACIE yang dapat ditempatkan di Amazon S3 (secara permanen atau sementara) dapat dipindai untuk data sensitif. Ini berarti bahwa data dari sumber lain—misalnya, ekspor snapshot berkala dari Amazon Relational Database Service (Amazon RDS) atau database Amazon Aurora, tabel Amazon DynamoDB yang diekspor, atau file teks yang diekstraksi dari aplikasi asli atau pihak ketiga—dapat dipindahkan ke Amazon S3 dan dievaluasi oleh Macie.

Contoh implementasi

Pustaka kode AWS SRA menyediakan contoh implementasi Amazon Macie. Ini termasuk mendelegasikan administrasi ke akun anggota dan mengonfigurasi Macie dalam akun administrator yang didelegasikan untuk semua akun yang ada dan yang akan datang di organisasi. AWS Macie juga dikonfigurasi untuk mengirim temuan ke bucket S3 pusat yang dienkripsi dengan kunci yang dikelola pelanggan. AWS KMS

IAM Access Analyzer

Saat Anda mempercepat perjalanan AWS Cloud adopsi dan terus berinovasi, sangat penting untuk mempertahankan kontrol ketat atas akses berbutir halus (izin), berisi proliferasi akses, dan memastikan bahwa izin digunakan secara efektif. Akses yang berlebihan dan tidak terpakai menghadirkan tantangan keamanan dan mempersulit perusahaan untuk menegakkan prinsip

hak istimewa yang paling rendah. Prinsip ini merupakan pilar arsitektur keamanan penting yang melibatkan izin IAM ukuran yang tepat secara terus-menerus untuk menyeimbangkan persyaratan keamanan dengan persyaratan pengembangan operasional dan aplikasi. Upaya ini melibatkan beberapa persona pemangku kepentingan, termasuk keamanan pusat dan tim Cloud Center of Excellence (CCoE) serta tim pengembangan yang terdesentralisasi.

AWS Identity and Access Management Access Analyzer menyediakan alat untuk secara efisien mengatur izin halus, memverifikasi izin yang dimaksudkan, dan menyempurnakan izin dengan menghapus akses yang tidak digunakan untuk membantu Anda memenuhi standar keamanan perusahaan Anda. Ini memberi Anda visibilitas ke akses eksternal dan internal ke AWS sumber daya dan temuan akses yang tidak terpakai melalui dasbor dan. AWS Security Hub CSPM Selain itu, ia mendukung Amazon EventBridge untuk pemberitahuan kustom berbasis acara dan alur kerja remediasi.

Fitur temuan penganalisis akses eksternal IAM Access Analyzer membantu Anda mengidentifikasi sumber daya di AWS organisasi dan akun Anda, seperti bucket Amazon S3 atau peran IAM, yang dibagikan dengan entitas eksternal. AWS Organisasi atau akun yang Anda pilih dikenal sebagai zona kepercayaan. Penganalisis menggunakan penalaran otomatis untuk menganalisis semua sumber daya yang didukung dalam zona kepercayaan, dan menghasilkan temuan untuk prinsipal yang dapat mengakses sumber daya dari luar zona kepercayaan. Temuan ini membantu mengidentifikasi sumber daya yang dibagikan dengan entitas eksternal dan membantu Anda melihat pratinjau bagaimana kebijakan memengaruhi akses publik dan lintas akun ke sumber daya Anda sebelum menerapkan izin sumber daya. Ini tersedia tanpa biaya tambahan.

Demikian pula, fitur pencarian penganalisis akses internal IAM Access Analyzer membantu Anda mengidentifikasi sumber daya di AWS organisasi dan akun yang dibagikan dengan kepala sekolah secara internal dalam organisasi atau akun Anda. Analisis ini mendukung prinsip hak istimewa terkecil dengan memastikan bahwa sumber daya yang Anda tentukan hanya dapat diakses oleh prinsipal yang dituju dalam organisasi Anda. Ini adalah fitur berbayar dan memerlukan konfigurasi sumber daya eksplisit untuk diperiksa. Gunakan fitur ini dengan bijaksana untuk memantau sumber daya sensitif tertentu yang, menurut desain, perlu dikunci bahkan secara internal.

Temuan IAM Access Analyzer juga membantu Anda mengidentifikasi akses yang tidak terpakai yang diberikan di AWS organisasi dan akun Anda, termasuk:

- Peran IAM yang tidak digunakan — Peran yang tidak memiliki aktivitas akses dalam jendela penggunaan yang ditentukan.

- Pengguna IAM yang tidak digunakan, kredensil, dan kunci akses — Kredensil yang dimiliki oleh pengguna IAM dan digunakan untuk mengakses dan sumber daya. Layanan AWS
- Kebijakan dan izin IAM yang tidak digunakan — Izin tingkat layanan dan tingkat tindakan yang tidak digunakan oleh peran dalam jendela penggunaan tertentu. IAM Access Analyzer menggunakan kebijakan berbasis identitas yang dilampirkan pada peran untuk menentukan layanan dan tindakan yang dapat diakses oleh peran tersebut. Analyzer memberikan tinjauan izin yang tidak digunakan untuk semua izin tingkat layanan.

Anda dapat menggunakan temuan yang dihasilkan dari IAM Access Analyzer untuk mendapatkan visibilitas ke, dan memulihkan, akses yang tidak diinginkan atau tidak digunakan berdasarkan kebijakan dan standar keamanan organisasi Anda. Setelah remediasi, temuan ini ditandai sebagai diselesaikan saat penganalisis berjalan berikutnya. Jika temuan ini disengaja, Anda dapat menandainya sebagai diarsipkan dalam IAM Access Analyzer dan memprioritaskan temuan lain yang menghadirkan risiko keamanan yang lebih besar. Selain itu, Anda dapat mengatur aturan arsip untuk mengarsipkan temuan tertentu secara otomatis. Misalnya, Anda dapat membuat aturan arsip untuk secara otomatis mengarsipkan temuan apa pun untuk bucket Amazon S3 tertentu yang dapat Anda akses secara teratur.

Sebagai pembangun, Anda dapat menggunakan IAM Access Analyzer untuk melakukan pemeriksaan kebijakan IAM otomatis sebelumnya dalam proses pengembangan dan penerapan (CI/CD) Anda untuk mematuhi standar keamanan perusahaan Anda. Anda dapat mengintegrasikan pemeriksaan kebijakan kustom IAM Access Analyzer dan tinjauan kebijakan AWS CloudFormation untuk mengotomatiskan tinjauan kebijakan sebagai bagian dari pipeline tim pengembangan Anda. CI/CD Hal ini mencakup:

- Validasi kebijakan IAM - IAM Access Analyzer memvalidasi kebijakan Anda terhadap tata bahasa kebijakan IAM dan praktik terbaik. AWS Anda dapat melihat temuan untuk pemeriksaan validasi kebijakan, termasuk peringatan keamanan, kesalahan, peringatan umum, dan saran untuk kebijakan Anda. Lebih dari 100 pemeriksaan validasi kebijakan saat ini tersedia dan dapat diotomatisasi dengan menggunakan AWS Command Line Interface (AWS CLI) dan APIs.
- Pemeriksaan kebijakan khusus IAM — Pemeriksaan kebijakan khusus IAM Access Analyzer memvalidasi kebijakan Anda terhadap standar keamanan yang Anda tentukan. Pemeriksaan kebijakan khusus menggunakan penalaran otomatis untuk memberikan tingkat jaminan yang lebih tinggi dalam memenuhi standar keamanan perusahaan Anda. Jenis pemeriksaan kebijakan khusus meliputi:

- Periksa kebijakan referensi: Saat mengedit kebijakan, Anda dapat membandingkannya dengan kebijakan referensi, seperti versi kebijakan yang ada, untuk memeriksa apakah pembaruan memberikan akses baru. CheckNoNewAccessAPI membandingkan dua kebijakan (kebijakan yang diperbarui dan kebijakan referensi) untuk menentukan apakah kebijakan yang diperbarui memperkenalkan akses baru ke kebijakan referensi, dan mengembalikan respons lulus atau gagal.
- Periksa daftar tindakan IAM: Anda dapat menggunakan CheckAccessNotGrantedAPI untuk memastikan bahwa kebijakan tidak memberikan akses ke daftar tindakan penting yang ditentukan dalam standar keamanan Anda. API ini mengambil kebijakan dan daftar hingga 100 tindakan IAM untuk memeriksa apakah kebijakan mengizinkan setidaknya satu tindakan, dan mengembalikan respons lulus atau gagal.

Tim keamanan dan penulis kebijakan IAM lainnya dapat menggunakan IAM Access Analyzer untuk membuat kebijakan yang sesuai dengan tata bahasa kebijakan IAM dan standar keamanan. Menulis kebijakan berukuran tepat secara manual dapat rawan kesalahan dan memakan waktu. Fitur pembuatan kebijakan IAM Access Analyzer membantu dalam membuat kebijakan IAM yang didasarkan pada aktivitas akses prinsipal. IAM Access Analyzer meninjau AWS CloudTrail log untuk layanan yang didukung dan menghasilkan templat kebijakan yang berisi izin yang digunakan oleh prinsipal dalam rentang tanggal yang ditentukan. Anda kemudian dapat menggunakan templat ini untuk membuat kebijakan dengan izin berbutir halus yang hanya memberikan izin yang diperlukan.

- Anda harus mengaktifkan CloudTrail jejak untuk akun Anda untuk membuat kebijakan berdasarkan aktivitas akses.
- IAM Access Analyzer tidak mengidentifikasi aktivitas tingkat tindakan untuk peristiwa data, seperti peristiwa data Amazon S3, dalam kebijakan yang dihasilkan.
- `iam:PassRole`Tindakan tidak dilacak oleh CloudTrail dan tidak disertakan dalam kebijakan yang dihasilkan.

IAM Access Analyzer digunakan di akun Security Tooling melalui fungsionalitas administrator yang didelegasikan di. AWS Organizations Administrator yang didelegasikan memiliki izin untuk membuat dan mengelola penganalisis dengan AWS organisasi sebagai zona kepercayaan.

> **Pertimbangan desain**
>
> Untuk mendapatkan temuan cakupan akun (di mana akun berfungsi sebagai batas tepercaya), Anda membuat penganalisis cakupan akun di setiap akun anggota. Ini dapat

dilakukan sebagai bagian dari pipeline akun. Temuan cakupan akun mengalir ke Security Hub CSPM di tingkat akun anggota. Dari sana, mereka mengalir ke akun administrator yang didelegasikan CSPM Security Hub (Security Tooling).

Contoh implementasi

- Pustaka kode AWS SRA menyediakan contoh implementasi IAM Access Analyzer. Ini menunjukkan cara mengkonfigurasi penganalisis tingkat organisasi dalam akun administrator yang didelegasikan dan penganalisis tingkat akun dalam setiap akun.
- Untuk informasi tentang cara mengintegrasikan pemeriksaan kebijakan kustom ke dalam alur kerja builder, lihat posting AWS blog Memperkenalkan pemeriksaan kebijakan kustom IAM Access Analyzer.

AWS Firewall Manager

AWS Firewall Managermembantu melindungi jaringan Anda dengan menyederhanakan tugas administrasi dan pemeliharaan Anda untuk AWS WAF AWS Shield Advanced, grup keamanan Amazon VPC AWS Network Firewall, Amazon Route 53 Resolver dan DNS Firewall di beberapa akun dan sumber daya. Dengan Firewall Manager, Anda mengatur aturan AWS WAF firewall, perlindungan Shield Advanced, grup keamanan Amazon VPC, firewall Network Firewall, dan asosiasi grup aturan DNS Firewall hanya sekali. Layanan ini secara otomatis menerapkan aturan dan perlindungan di seluruh akun dan sumber daya Anda, bahkan saat Anda menambahkan sumber daya baru.

Firewall Manager sangat berguna ketika Anda ingin melindungi seluruh AWS organisasi Anda alih-alih sejumlah kecil akun dan sumber daya tertentu, atau jika Anda sering menambahkan sumber daya baru yang ingin Anda lindungi. Firewall Manager menggunakan kebijakan keamanan untuk memungkinkan Anda menentukan serangkaian konfigurasi, termasuk aturan, perlindungan, dan tindakan yang relevan yang harus diterapkan serta akun dan sumber daya (ditunjukkan oleh tag) untuk disertakan atau dikecualikan. Anda dapat membuat konfigurasi granular dan fleksibel sambil tetap dapat menskalakan kontrol ke sejumlah besar akun dan. VPCs Kebijakan ini secara otomatis dan konsisten menerapkan aturan yang Anda konfigurasikan bahkan ketika akun dan sumber daya baru dibuat. Firewall Manager diaktifkan di semua akun melalui AWS Organizations, dan konfigurasi dan manajemen dilakukan oleh tim keamanan yang sesuai di akun administrator yang didelegasikan Firewall Manager (dalam hal ini, akun Security Tooling).

Anda harus mengaktifkan AWS Config untuk setiap AWS Region yang berisi sumber daya yang ingin Anda lindungi. Jika Anda tidak ingin mengaktifkan AWS Config semua sumber daya, Anda harus mengaktifkannya untuk sumber daya yang terkait dengan jenis kebijakan Firewall Manager yang Anda gunakan. Saat Anda menggunakan keduanya AWS Security Hub CSPM dan Firewall Manager, Firewall Manager secara otomatis mengirimkan temuan Anda ke Security Hub CSPM. Firewall Manager membuat temuan untuk sumber daya yang tidak sesuai dan untuk serangan yang dideteksi, dan mengirimkan temuan ke Security Hub CSPM. Saat menyiapkan kebijakan Firewall Manager AWS WAF, Anda dapat mengaktifkan pencatatan pada daftar kontrol akses web (web ACLs) secara terpusat untuk semua akun dalam lingkup dan memusatkan log di bawah satu akun.

Dengan Firewall Manager Anda dapat memiliki satu atau beberapa administrator yang dapat mengelola sumber daya firewall organisasi Anda. Saat menetapkan beberapa administrator, Anda dapat menerapkan kondisi lingkup administratif yang membatasi untuk menentukan sumber daya (akun,, Wilayah OUs, jenis kebijakan) yang dapat dikelola oleh setiap administrator. Ini memberi Anda fleksibilitas untuk memiliki peran administrator yang berbeda dalam organisasi Anda, dan membantu Anda mempertahankan prinsip akses yang paling tidak istimewa. AWS SRA menggunakan satu administrator dengan lingkup administratif penuh yang didelegasikan ke akun Security Tooling.

> **Pertimbangan desain**
>
> Manajer akun akun anggota individu dalam AWS organisasi dapat mengonfigurasi kontrol tambahan (seperti AWS WAF aturan dan grup keamanan Amazon VPC) di layanan yang dikelola Manajer Firewall sesuai dengan kebutuhan khusus mereka.

> **Contoh implementasi**
>
> Pustaka kode AWS SRA menyediakan contoh implementasi Firewall Manager. Ini menunjukkan administrasi yang didelegasikan (Security Tooling), menyebarkan grup keamanan maksimum yang diizinkan, mengonfigurasi kebijakan grup keamanan, dan mengonfigurasi beberapa kebijakan. AWS WAF

Amazon EventBridge

Amazon EventBridge adalah layanan bus acara tanpa server yang membuatnya mudah untuk menghubungkan aplikasi Anda dengan data dari berbagai sumber. Ini sering digunakan dalam

otomatisasi keamanan. Anda dapat mengatur aturan perutean untuk menentukan ke mana harus mengirim data Anda untuk membangun arsitektur aplikasi yang bereaksi secara real time ke semua sumber data Anda. Anda dapat membuat bus acara khusus untuk menerima acara dari aplikasi khusus Anda, selain menggunakan bus acara default di setiap akun. Anda dapat membuat bus acara di akun Security Tooling yang dapat menerima peristiwa khusus keamanan dari akun lain di organisasi. AWS Misalnya, dengan menautkan Aturan AWS Config, Amazon GuardDuty, dan AWS Security Hub CSPM dengan EventBridge, Anda membuat pipeline otomatis yang fleksibel untuk merutekan data keamanan, meningkatkan peringatan, dan mengelola tindakan untuk menyelesaikan masalah.

Pertimbangan desain

- EventBridge mampu merutekan peristiwa ke sejumlah target yang berbeda. Salah satu pola berharga untuk mengotomatiskan tindakan keamanan adalah menghubungkan peristiwa tertentu ke AWS Lambda responden individu, yang mengambil tindakan yang tepat. Misalnya, dalam keadaan tertentu, Anda mungkin ingin menggunakannya EventBridge untuk merutekan pencarian bucket S3 publik ke responden Lambda yang mengoreksi kebijakan bucket dan menghapus izin publik. Responden ini dapat diintegrasikan ke dalam buku pedoman investigasi dan buku runbook Anda untuk mengoordinasikan aktivitas respons.
- Praktik terbaik untuk tim operasi keamanan yang sukses adalah mengintegrasikan aliran peristiwa keamanan dan temuan ke dalam sistem notifikasi dan alur kerja seperti sistem tiket, sistem, atau sistem informasi keamanan dan manajemen acara (SIEM) lainnya. bug/issue Ini menghilangkan alur kerja dari email dan laporan statis, dan membantu Anda merutekan, meningkatkan, dan mengelola peristiwa atau temuan. Kemampuan routing yang fleksibel di dalamnya EventBridge adalah enabler yang kuat untuk integrasi ini.

Amazon Detective

Amazon Detective mendukung strategi kontrol keamanan responsif Anda dengan membuatnya mudah untuk menganalisis, menyelidiki, dan mengidentifikasi dengan cepat akar penyebab temuan keamanan atau aktivitas mencurigakan bagi analis keamanan Anda. Detective secara otomatis mengekstrak peristiwa berbasis waktu seperti upaya login, panggilan API, dan lalu lintas jaringan dari log AWS CloudTrail dan log aliran VPC Amazon. Detective menggunakan peristiwa ini dengan menggunakan aliran log independen dan log aliran CloudTrail VPC Amazon. Anda dapat menggunakan Detektif untuk mengakses data peristiwa historis hingga satu tahun. Detektif

menggunakan pembelajaran mesin dan visualisasi untuk menciptakan pandangan interaktif yang terpadu tentang perilaku sumber daya Anda dan interaksi di antara mereka dari waktu ke waktu — ini disebut grafik perilaku. Anda dapat menjelajahi grafik perilaku untuk memeriksa tindakan yang berbeda seperti upaya masuk yang gagal atau panggilan API yang mencurigakan.

Detective terintegrasi dengan Amazon Security Lake untuk memungkinkan analis keamanan melakukan kueri dan mengambil log yang disimpan di Security Lake. Anda dapat menggunakan integrasi ini untuk mendapatkan informasi tambahan dari CloudTrail log dan log aliran VPC Amazon yang disimpan di Security Lake saat melakukan investigasi keamanan di Detective.

Detective juga mencerna temuan yang terdeteksi oleh Amazon GuardDuty, termasuk ancaman yang terdeteksi oleh GuardDuty Runtime Monitoring. Ketika sebuah akun mengaktifkan Detektif, itu menjadi akun administrator untuk grafik perilaku. Sebelum Anda mencoba mengaktifkan Detektif, pastikan akun Anda telah terdaftar setidaknya GuardDuty selama 48 jam. Jika Anda tidak memenuhi persyaratan ini, Anda tidak dapat mengaktifkan DetectiveDetective.

Sumber data opsional tambahan untuk Detektif termasuk log audit Amazon EKS dan. AWS Security Hub CSPM Sumber data log audit Amazon EKS meningkatkan informasi yang diberikan tentang jenis entitas berikut: klaster Amazon EKS, pod Kubernetes, gambar kontainer, dan subjek Kubernetes. Sumber data Security Hub adalah bagian dari temuan AWS keamanan, di mana ia mengkorelasikan temuan di seluruh produk ke Security Hub dan menyerapnya ke Detektif.

Detektif secara otomatis mengelompokkan beberapa temuan yang terkait dengan satu peristiwa kompromi keamanan ke dalam kelompok pencarian. Aktor ancaman biasanya melakukan serangkaian tindakan yang mengarah pada beberapa temuan keamanan yang tersebar di seluruh waktu dan sumber daya. Oleh karena itu, menemukan kelompok harus menjadi titik awal untuk investigasi yang melibatkan banyak entitas dan temuan. Detective juga menyediakan ringkasan grup pencarian dengan menggunakan AI generatif yang secara otomatis menganalisis grup pencarian dan memberikan wawasan dalam bahasa alami untuk membantu Anda mempercepat penyelidikan keamanan.

Detektif terintegrasi dengan. AWS Organizations Akun Manajemen Org mendelegasikan akun anggota sebagai akun administrator Detektif. Di AWS SRA, ini adalah akun Security Tooling. Akun administrator Detektif memiliki kemampuan untuk secara otomatis mengaktifkan semua akun anggota saat ini di organisasi sebagai akun anggota Detektif, dan juga menambahkan akun anggota baru saat ditambahkan ke organisasi. AWS Akun administrator Detektif juga memiliki kemampuan untuk mengundang akun anggota yang saat ini tidak berada di AWS organisasi, tetapi berada dalam Wilayah yang sama, untuk menyumbangkan data mereka ke grafik perilaku akun utama. Ketika akun

anggota menerima undangan dan diaktifkan, Detektif mulai menyerap dan mengekstrak data akun anggota ke dalam grafik perilaku tersebut.

> **Pertimbangan desain**
>
> Anda dapat menavigasi ke Detective menemukan profil dari GuardDuty dan AWS Security Hub CSPM konsol. Tautan ini dapat membantu merampingkan proses investigasi. Akun Anda harus merupakan akun administratif untuk Detektif dan layanan yang Anda putar (atau Security GuardDuty Hub CSPM). Jika akun utama sama untuk layanan, tautan integrasi bekerja dengan mulus.

AWS Audit Manager

AWS Audit Managermembantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola audit dan kepatuhan terhadap peraturan dan standar industri. Ini memungkinkan Anda untuk beralih dari mengumpulkan, meninjau, dan mengelola bukti secara manual ke solusi yang mengotomatiskan pengumpulan bukti, menyediakan cara sederhana untuk melacak sumber bukti audit, memungkinkan kolaborasi kerja tim, dan membantu mengelola keamanan dan integritas bukti. Saat tiba waktunya untuk audit, Audit Manager membantu Anda mengelola tinjauan pemangku kepentingan atas kontrol Anda.

Dengan Audit Manager, Anda dapat mengaudit kerangka kerja bawaan seperti benchmark Center for Internet Security (CIS), Tolok Ukur AWS Yayasan CIS, Kontrol Sistem dan Organisasi 2 (SOC 2), dan Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS). Ini juga memberi Anda kemampuan untuk membuat kerangka kerja Anda sendiri dengan kontrol standar atau kustom berdasarkan persyaratan spesifik Anda untuk audit internal.

Audit Manager mengumpulkan empat jenis bukti. Tiga jenis bukti otomatis: bukti pemeriksaan kepatuhan dari AWS Config dan AWS Security Hub CSPM, bukti peristiwa manajemen dari AWS CloudTrail, dan bukti konfigurasi dari panggilan AWS service-to-service API. Untuk bukti yang tidak dapat diotomatisasi, Audit Manager memungkinkan Anda mengunggah bukti manual.

Secara default, data Anda di Audit Manager dienkripsi menggunakan kunci AWS terkelola. AWS SRA menggunakan kunci yang dikelola pelanggan untuk enkripsi untuk memberikan kontrol yang lebih besar atas akses logis. Anda juga harus mengonfigurasi bucket S3 di AWS Region tempat Audit Manager menerbitkan laporan penilaian. Bucket ini harus dienkripsi dengan kunci yang dikelola pelanggan dan memiliki kebijakan bucket yang dikonfigurasi agar hanya mengizinkan Audit Manager yang mempublikasikan laporan.

> **Note**
>
> Audit Manager membantu mengumpulkan bukti yang relevan untuk memverifikasi kepatuhan terhadap standar dan peraturan kepatuhan tertentu. Namun, itu tidak menilai kepatuhan Anda. Oleh karena itu, bukti yang dikumpulkan melalui Audit Manager mungkin tidak mencakup rincian proses operasional Anda yang diperlukan untuk audit. Audit Manager bukan pengganti penasihat hukum atau pakar kepatuhan. Kami menyarankan Anda untuk menggunakan layanan dari penilai pihak ketiga yang disertifikasi untuk kerangka kepatuhan yang Anda evaluasi.

Penilaian Audit Manager dapat dijalankan di beberapa akun di AWS organisasi Anda. Audit Manager mengumpulkan dan mengkonsolidasikan bukti ke dalam akun administrator yang didelegasikan di. AWS Organizations Fungsionalitas audit ini terutama digunakan oleh tim kepatuhan dan audit internal, dan hanya memerlukan akses baca ke Anda Akun AWS.

> **Pertimbangan desain**
>
> - Audit Manager melengkapi layanan AWS keamanan lainnya seperti AWS Security Hub CSPM, AWS Security Hub, dan AWS Config untuk membantu menerapkan kerangka kerja manajemen risiko. Audit Manager menyediakan fungsionalitas jaminan risiko independen, sedangkan Security Hub CSPM membantu Anda mengawasi risiko dan paket AWS Config kesesuaian membantu mengelola risiko Anda. Profesional audit yang akrab dengan Model Tiga Garis yang dikembangkan oleh Institute of Internal Auditors (IIA) harus mencatat bahwa kombinasi ini Layanan AWS membantu Anda mencakup tiga garis pertahanan. Untuk informasi lebih lanjut, lihat seri blog dua bagian di blog AWS Cloud Operasi & Migrasi.
> - Agar Audit Manager mengumpulkan bukti CSPM Security Hub, akun administrator yang didelegasikan untuk kedua layanan harus sama. Akun AWS Untuk alasan ini, di AWS SRA, akun Security Tooling adalah administrator yang didelegasikan untuk Audit Manager.

AWS Artifact

AWS Artifactdi-host dalam akun Security Tooling untuk memisahkan fungsionalitas manajemen artefak kepatuhan dari akun Manajemen AWS Org. Pemisahan tugas ini penting karena kami menyarankan Anda menghindari penggunaan akun Manajemen AWS Org untuk penerapan

kecuali benar-benar diperlukan. Sebagai gantinya, teruskan penerapan ke akun anggota. Karena manajemen artefak audit dapat dilakukan dari akun anggota dan fungsinya selaras dengan tim keamanan dan kepatuhan, akun Perkakas Keamanan ditetapkan sebagai akun administrator. AWS Artifact Anda dapat menggunakan AWS Artifact laporan untuk mengunduh dokumen AWS keamanan dan kepatuhan, seperti sertifikasi AWS ISO, Industri Kartu Pembayaran (PCI), dan laporan Kontrol Sistem dan Organisasi (SOC).

AWS Artifact tidak mendukung fitur administrasi yang didelegasikan. Sebagai gantinya, Anda dapat membatasi kemampuan ini hanya untuk peran IAM di akun Alat Keamanan yang berkaitan dengan tim audit dan kepatuhan Anda, sehingga mereka dapat mengunduh, meninjau, dan memberikan laporan tersebut kepada auditor eksternal sesuai kebutuhan. Anda juga dapat membatasi peran IAM tertentu agar hanya memiliki akses ke AWS Artifact laporan tertentu melalui kebijakan IAM. Untuk contoh kebijakan IAM, lihat AWS Artifact dokumentasi.

> **Pertimbangan desain**
>
> Jika Anda memilih untuk memiliki tim khusus Akun AWS audit dan kepatuhan, Anda dapat menghosting AWS Artifact di akun audit keamanan, yang terpisah dari akun Perkakas Keamanan. AWS Artifact Laporan memberikan bukti yang menunjukkan bahwa suatu organisasi mengikuti proses yang terdokumentasi atau memenuhi persyaratan tertentu. Artefak audit dikumpulkan dan diarsipkan di seluruh siklus pengembangan sistem dan dapat digunakan sebagai bukti dalam audit dan penilaian internal atau eksternal.

AWS KMS

AWS Key Management Service(AWS KMS) membantu Anda membuat dan mengelola kunci kriptografi dan mengontrol penggunaannya di berbagai Layanan AWS dan dalam aplikasi Anda. AWS KMS adalah layanan yang aman dan tangguh yang menggunakan modul keamanan perangkat keras untuk melindungi kunci kriptografi. Ini mengikuti proses siklus hidup standar industri untuk bahan utama, seperti penyimpanan, rotasi, dan kontrol akses kunci. AWS KMS dapat membantu melindungi data Anda dengan enkripsi dan kunci penandatanganan, dan dapat digunakan untuk enkripsi sisi server dan enkripsi sisi klien melalui Enkripsi SDK.AWS Untuk perlindungan dan fleksibilitas, AWS KMS mendukung tiga jenis kunci: kunci yang dikelola pelanggan, kunci AWS terkelola, dan kunci yang AWS dimiliki. Kunci yang dikelola pelanggan adalah AWS KMS kunci Akun AWS yang Anda buat, miliki, dan kelola. AWS kunci terkelola adalah AWS KMS kunci di akun Anda yang dibuat, dikelola, dan digunakan atas nama Anda oleh Layanan AWS yang terintegrasi dengan AWS KMS. AWS kunci yang dimiliki adalah kumpulan AWS KMS kunci yang Layanan AWS dimiliki dan dikelola

untuk digunakan dalam beberapa Akun AWS. Untuk informasi selengkapnya tentang penggunaan AWS KMS kunci, lihat AWS KMS dokumentasi dan detail AWS KMS kriptografi.

Salah satu opsi penerapan adalah memusatkan tanggung jawab manajemen AWS KMS kunci ke satu akun sambil mendelegasikan kemampuan untuk menggunakan kunci di akun Aplikasi dengan sumber daya aplikasi dengan menggunakan kombinasi kebijakan kunci dan IAM. Pendekatan ini aman dan mudah dikelola, tetapi Anda dapat menghadapi rintangan karena batas AWS KMS pembatasan, batas layanan akun, dan tim keamanan dibanjiri tugas manajemen kunci operasional. Opsi penyebaran lainnya adalah memiliki model terdesentralisasi di mana Anda mengizinkan AWS KMS untuk tinggal di beberapa akun, dan Anda mengizinkan mereka yang bertanggung jawab atas infrastruktur dan beban kerja di akun tertentu untuk mengelola kunci mereka sendiri. Model ini memberi tim beban kerja Anda lebih banyak kontrol, fleksibilitas, dan kelincahan atas penggunaan kunci enkripsi. Ini juga membantu menghindari batasan API, membatasi ruang lingkup dampak Akun AWS hanya untuk satu, dan menyederhanakan pelaporan, audit, dan tugas terkait kepatuhan lainnya. Dalam model terdesentralisasi, penting untuk menerapkan dan menegakkan pagar pembatas sehingga kunci yang terdesentralisasi dikelola dengan cara yang sama dan penggunaan kunci diaudit sesuai dengan praktik dan kebijakan terbaik yang AWS KMS ditetapkan. Untuk informasi selengkapnya, lihat whitepaper Praktik AWS Key Management Service Terbaik. AWS SRA merekomendasikan model manajemen kunci terdistribusi di mana AWS KMS kunci berada secara lokal di dalam akun tempat mereka digunakan. Kami menyarankan Anda menghindari penggunaan satu kunci dalam satu akun untuk semua fungsi kriptografi. Kunci dapat dibuat berdasarkan fungsi dan persyaratan perlindungan data, dan untuk menegakkan prinsip hak istimewa paling sedikit. Dalam beberapa kasus, izin enkripsi akan disimpan terpisah dari izin dekripsi, dan administrator akan mengelola fungsi siklus hidup tetapi tidak akan dapat mengenkripsi atau mendekripsi data dengan kunci yang mereka kelola.

Dalam akun Security Tooling, AWS KMS digunakan untuk mengelola enkripsi layanan keamanan terpusat seperti jejak AWS CloudTrail organisasi yang dikelola oleh organisasi. AWS

AWS Private CA

AWS Private Certificate Authority(AWS Private CA) adalah layanan CA pribadi terkelola yang membantu Anda mengelola siklus hidup sertifikat TLS entitas akhir pribadi Anda dengan aman untuk instans EC2, kontainer, perangkat IoT, dan sumber daya lokal. Ini memungkinkan komunikasi TLS terenkripsi untuk menjalankan aplikasi. Dengan AWS Private CA, Anda dapat membuat hierarki CA Anda sendiri (CA root, melalui bawahan CAs, hingga sertifikat entitas akhir) dan mengeluarkan sertifikat dengannya untuk mengautentikasi pengguna internal, komputer, aplikasi, layanan, server,

dan perangkat lain, dan untuk menandatangani kode komputer. Sertifikat yang dikeluarkan oleh CA pribadi hanya dipercaya dalam AWS organisasi Anda, bukan di internet.

Infrastruktur kunci publik (PKI) atau tim keamanan dapat bertanggung jawab untuk mengelola seluruh infrastruktur PKI. Ini termasuk manajemen dan pembuatan CA pribadi. Namun, harus ada ketentuan yang memungkinkan tim beban kerja untuk melayani sendiri persyaratan sertifikat mereka. AWS SRA menggambarkan hierarki CA terpusat di mana root CA di-host dalam akun Security Tooling. Hal ini memungkinkan tim keamanan untuk menegakkan kontrol keamanan yang ketat, karena akar CA adalah dasar dari seluruh PKI. Namun, pembuatan sertifikat pribadi dari CA pribadi didelegasikan ke tim pengembangan aplikasi dengan membagikan CA ke akun Aplikasi dengan menggunakan AWS Resource Access Manager (AWS RAM). AWS RAM mengelola izin yang diperlukan untuk berbagi lintas akun. Ini menghilangkan kebutuhan akan CA pribadi di setiap akun dan menyediakan cara penyebaran yang lebih hemat biaya. Untuk informasi selengkapnya tentang alur kerja dan implementasi, lihat posting blog Cara menggunakan AWS RAM untuk berbagi AWS Private CA lintas akun Anda.

> **Note**
>
> AWS Certificate Manager (ACM) juga membantu Anda menyediakan, mengelola, dan menyebarkan sertifikat TLS publik untuk digunakan. Layanan AWS Untuk mendukung fungsi ini, ACM harus berada di Akun AWS yang akan menggunakan sertifikat publik. Ini akan dibahas nanti dalam panduan ini, di bagian Akun aplikasi.

> **Pertimbangan desain**
>
> - Dengan AWS Private CA, Anda dapat membuat hierarki otoritas sertifikat hingga lima level. Anda juga dapat membuat beberapa hierarki, masing-masing dengan akarnya sendiri. AWS Private CA Hirarki harus mematuhi desain PKI organisasi Anda. Namun, perlu diingat bahwa meningkatkan hierarki CA meningkatkan jumlah sertifikat di jalur sertifikasi, yang, pada gilirannya, meningkatkan waktu validasi sertifikat entitas akhir. Hirarki CA yang terdefinisi dengan baik memberikan manfaat yang mencakup kontrol keamanan granular yang sesuai untuk setiap CA, delegasi CA bawahan ke aplikasi yang berbeda, yang mengarah pada pembagian tugas administratif, penggunaan CA dengan kepercayaan terbatas yang dapat dibatalkan, kemampuan untuk menentukan periode validitas yang berbeda, dan kemampuan untuk menegakkan batas jalur. Idealnya, root dan bawahan CAs Anda terpisah Akun AWS. Untuk informasi selengkapnya tentang perencanaan hierarki CA

dengan menggunakan AWS Private CA, lihat AWS Private CA dokumentasi dan posting blog Cara mengamankan AWS Private CA hierarki skala perusahaan untuk otomotif dan manufaktur.

- AWS Private CA dapat berintegrasi dengan hierarki CA yang ada, yang memungkinkan Anda menggunakan otomatisasi dan kemampuan AWS integrasi asli ACM bersama dengan akar kepercayaan yang ada yang Anda gunakan saat ini. Anda dapat membuat CA bawahan yang AWS Private CA didukung oleh CA induk di tempat. Untuk informasi selengkapnya tentang implementasi, lihat Menginstal sertifikat CA bawahan yang ditandatangani oleh CA induk eksternal dalam AWS Private CA dokumentasi.

Amazon Inspector

Amazon Inspector adalah layanan manajemen kerentanan otomatis yang secara otomatis menemukan dan memindai instans Amazon EC2, gambar kontainer di Amazon Elastic Container Registry (Amazon ECR), fungsi, dan repositori kode dalam pengelola kode sumber Anda untuk mengetahui kerentanan AWS Lambda perangkat lunak yang diketahui dan paparan jaringan yang tidak diinginkan.

Amazon Inspector terus menilai lingkungan Anda sepanjang siklus hidup sumber daya Anda dengan memindai sumber daya secara otomatis setiap kali Anda membuat perubahan padanya. Peristiwa yang memulai recanning sumber daya termasuk menginstal paket baru pada instans EC2, menginstal tambalan, dan publikasi laporan kerentanan dan eksposur umum baru (CVE) yang memengaruhi sumber daya. Amazon Inspector mendukung penilaian Benchmark Center of Internet Security (CIS) untuk sistem operasi dalam instans EC2.

Amazon Inspector terintegrasi dengan alat pengembang seperti Jenkins dan TeamCity untuk penilaian gambar kontainer. Anda dapat menilai gambar kontainer Anda untuk kerentanan perangkat lunak dalam integrasi berkelanjutan dan pengiriman berkelanjutan (dasbor CI/CD) tools, and push security to an earlier point in the software development lifecycle. Assessment findings are available in the CI/CD alat, sehingga Anda dapat melakukan tindakan otomatis sebagai respons terhadap masalah keamanan penting seperti build yang diblokir atau dorongan gambar ke pendaftar kontainer. Jika sudah aktif Akun AWS, Anda dapat menginstal plugin Amazon Inspector dari marketplace CI/CD alat dan menambahkan pemindaian Amazon Inspector di pipeline build Anda tanpa perlu mengaktifkan layanan Amazon Inspector. Fitur ini bekerja dengan CI/CD alat yang dihosting di mana saja—di tempat AWS, atau di cloud hibrid–sehingga Anda dapat secara konsisten menggunakan satu solusi di semua pipeline pengembangan Anda. Saat Amazon Inspector diaktifkan, Amazon

Inspector secara otomatis akan menemukan semua instans EC2 Anda, gambar kontainer di Amazon ECR dan alat CI/CD , dan fungsi Lambda dalam skala besar, dan terus memantau kerentanan yang diketahui.

Temuan jangkauan jaringan Amazon Inspector menilai aksesibilitas instans EC2 Anda ke atau dari tepi VPC seperti gateway internet, koneksi peering VPC, atau jaringan pribadi virtual () melalui gateway virtual. VPNs Aturan ini membantu mengotomatiskan pemantauan AWS jaringan Anda dan mengidentifikasi di mana akses jaringan ke instans EC2 Anda mungkin salah dikonfigurasi melalui grup keamanan yang salah kelola, daftar kontrol akses (ACLs), gateway internet, dan sebagainya. Untuk informasi selengkapnya, lihat dokumentasi Amazon Inspector.

Saat Amazon Inspector mengidentifikasi kerentanan atau jalur jaringan terbuka, Amazon Inspector menghasilkan temuan yang dapat Anda selidiki. Temuan ini mencakup rincian komprehensif tentang kerentanan, termasuk skor risiko, sumber daya yang terpengaruh, dan rekomendasi remediasi. Skor risiko secara khusus disesuaikan dengan lingkungan Anda dan dihitung dengan menghubungkan informasi up-to-date CVE dengan faktor temporal dan lingkungan seperti aksesibilitas jaringan dan informasi eksploitasi untuk memberikan temuan kontekstual.

Amazon Inspector Code Security memindai kode sumber aplikasi pihak pertama, dependensi aplikasi pihak ketiga, dan infrastruktur sebagai kode (IAc) untuk mencari kerentanan. Setelah Anda mengaktifkan Keamanan Kode, Anda dapat membuat dan menerapkan konfigurasi pemindaian ke repositori kode Anda untuk menentukan frekuensi, jenis pemindaian, dan repositori yang akan dipindai. Kode Keamanan mendukung pengujian keamanan aplikasi statis (SAST), analisis komposisi perangkat lunak (SCA), dan pemindaian IAc. Untuk mengonfigurasi frekuensi, Anda dapat menentukan pemindaian sesuai permintaan, perubahan kode, atau secara berkala. Pemindaian kode menangkap cuplikan kode untuk menyoroti kerentanan yang terdeteksi. Cuplikan kode disimpan dienkripsi dengan kunci KMS. Administrator yang didelegasikan untuk organisasi tidak dapat melihat cuplikan kode milik akun anggota. Setelah Anda mengintegrasikan manajer kode sumber (SCMs) dengan Kode Keamanan, semua repositori kode terdaftar sebagai proyek di konsol Amazon Inspector. Code Security hanya memonitor cabang default dari setiap repositori. Amazon Inspector merampingkan remediasi keamanan dengan memberikan rekomendasi perbaikan kode spesifik secara langsung di tempat pengembang bekerja. Integrasi dua arah dengan SCM Anda secara otomatis menyarankan perbaikan sebagai komentar dalam pull requests (PRs) dan merge requests (MRs) untuk temuan kritis dan tinggi, dan memberi tahu pengembang tentang kerentanan paling penting untuk ditangani tanpa mengganggu alur kerja mereka.

Untuk memindai kerentanan, instans EC2 harus dikelola AWS Systems Manager dengan menggunakan AWS Systems Manager Agen (SSMagent). Tidak ada agen yang diperlukan untuk

jangkauan jaringan instans EC2 atau pemindaian kerentanan gambar kontainer dalam fungsi Amazon ECR atau Lambda.

Amazon Inspector terintegrasi dengan AWS Organizations dan mendukung administrasi yang didelegasikan. Di AWS SRA, akun Security Tooling dibuat akun administrator yang didelegasikan untuk Amazon Inspector. Akun administrator yang didelegasikan Amazon Inspector dapat mengelola data temuan dan pengaturan tertentu untuk anggota organisasi. AWS Ini termasuk melihat rincian temuan agregat untuk semua akun anggota, mengaktifkan atau menonaktifkan pemindaian untuk akun anggota, dan meninjau sumber daya yang dipindai dalam organisasi. AWS

Pertimbangan desain

- Amazon Inspector terintegrasi dengan dan Security AWS Security Hub CSPM Hub secara otomatis saat kedua layanan diaktifkan. Anda dapat menggunakan integrasi ini untuk mengirim semua temuan dari Amazon Inspector ke Security Hub CSPM, yang kemudian akan menyertakan temuan tersebut dalam analisisnya tentang postur keamanan Anda.
- Amazon Inspector secara otomatis mengekspor peristiwa untuk temuan, perubahan cakupan sumber daya, dan pemindaian awal sumber daya individu ke Amazon EventBridge, dan, secara opsional, ke bucket Amazon Simple Storage Service (Amazon S3). Untuk mengekspor temuan aktif ke bucket S3, Anda memerlukan AWS KMS kunci yang dapat digunakan Amazon Inspector untuk mengenkripsi temuan, dan bucket S3 dengan izin yang memungkinkan Amazon Inspector mengunggah objek. EventBridgeintegrasi memungkinkan Anda untuk memantau dan memproses temuan dalam waktu dekat sebagai bagian dari alur kerja keamanan dan kepatuhan yang ada. EventBridge acara dipublikasikan ke akun administrator yang didelegasikan Amazon Inspector selain akun anggota dari mana mereka berasal.
- Integrasi Amazon Inspector Code Security dengan GitHub SaaS, GitHub Enterprise Cloud, dan GitHub Enterprise Server memerlukan akses internet publik.

Contoh implementasi

Pustaka kode AWS SRA menyediakan contoh implementasi Amazon Inspector. Ini menunjukkan administrasi yang didelegasikan (Security Tooling) dan mengonfigurasi Amazon Inspector untuk semua akun yang ada dan yang akan datang di organisasi. AWS

Respons Insiden Keamanan AWS

Respons Insiden Keamanan AWSadalah layanan yang membantu Anda mempersiapkan, dan menanggapi, insiden keamanan di AWS lingkungan Anda. Ini melakukan triase temuan, meningkatkan peristiwa keamanan, dan mengelola kasus-kasus yang membutuhkan perhatian segera Anda. Selain itu, ini memberi Anda akses ke Tim Respons Insiden AWS Pelanggan (CIRT), yang menyelidiki sumber daya yang terkena dampak. Respons Insiden Keamanan AWS Juga menyediakan kemampuan respons dan remediasi otomatis melalui AWS Systems Manager dokumen (dokumen SSM), yang membantu tim keamanan merespons, dan memulihkan dari, insiden keamanan secara lebih efisien. Respons Insiden Keamanan AWS terintegrasi dengan Amazon GuardDuty dan AWS Security Hub CSPM untuk menerima temuan keamanan dan mengatur respons otomatis.

Di AWS SRA, Respons Insiden Keamanan AWS digunakan di akun Security Tooling sebagai akun administrator yang didelegasikan. Akun Security Tooling dipilih karena sejalan dengan tujuan akun untuk mengoperasikan layanan keamanan dan mengotomatiskan peringatan dan respons keamanan. Akun Security Tooling juga bertindak sebagai akun administrator yang didelegasikan untuk Security Hub CSPM dan GuardDuty, yang, bersama dengan Respons Insiden Keamanan AWS, membantu menyederhanakan manajemen alur kerja. Respons Insiden Keamanan AWS dikonfigurasi agar berfungsi AWS Organizations, sehingga Anda dapat mengelola respons insiden di seluruh akun organisasi Anda dari akun Alat Keamanan.

Respons Insiden Keamanan AWS membantu Anda menerapkan tahap-tahap berikut dari siklus hidup respons insiden:

- Persiapan: Membuat dan memelihara rencana respons dan dokumen SSM untuk tindakan penahanan.
- Deteksi dan analisis: Secara otomatis menganalisis temuan keamanan dan menentukan tingkat keparahan insiden.
- Deteksi dan analisis: Buka kasus yang didukung layanan dan libatkan dengan AWS CIRT untuk bantuan tambahan. CIRT adalah sekelompok individu yang memberikan dukungan selama acara keamanan aktif.
- Penahanan dan pemberantasan: Jalankan tindakan penahanan otomatis melalui dokumen SSM.
- Aktivitas pasca-insiden: Dokumentasikan detail insiden dan lakukan analisis pasca-insiden.

Anda juga dapat menggunakan Respons Insiden Keamanan AWS untuk membuat kasus yang dikelola sendiri. Respons Insiden Keamanan AWS dapat membuat pemberitahuan atau kasus keluar

ketika Anda perlu mengetahui, atau menindaklanjuti, sesuatu yang mungkin memengaruhi akun atau sumber daya Anda. Fitur ini hanya tersedia jika Anda mengaktifkan respons proaktif dan alur kerja triaging peringatan sebagai bagian dari langganan Anda.

Pertimbangan desain

- Saat Anda menerapkan Respons Insiden Keamanan AWS, tinjau dan uji tindakan respons otomatis dengan cermat sebelum Anda mengaktifkannya dalam produksi. Otomatisasi dapat mempercepat respons insiden, tetapi tindakan otomatis yang tidak dikonfigurasi dengan benar dapat memengaruhi beban kerja yang sah.
- Pertimbangkan untuk menggunakan dokumen SSM Respons Insiden Keamanan AWS untuk menerapkan prosedur penahanan khusus organisasi sambil mempertahankan praktik terbaik bawaan layanan untuk jenis insiden umum.
- Jika Anda berencana untuk menggunakan Respons Insiden Keamanan AWS dalam VPC, pastikan Anda memiliki titik akhir VPC yang sesuai yang dikonfigurasi untuk Systems Manager dan layanan terintegrasi lainnya untuk mengaktifkan tindakan penahanan di subnet pribadi.

Menyebarkan layanan keamanan umum dalam semua Akun AWS

Bagian Terapkan layanan keamanan di seluruh AWS organisasi Anda sebelumnya dalam referensi ini menyoroti layanan keamanan yang melindungi Akun AWS, dan mencatat bahwa banyak dari layanan ini juga dapat dikonfigurasi dan dikelola di dalamnya AWS Organizations. Beberapa layanan ini harus digunakan di semua akun, dan Anda akan melihatnya di AWS SRA. Ini memungkinkan serangkaian pagar pembatas yang konsisten dan menyediakan pemantauan, manajemen, dan tata kelola terpusat di seluruh organisasi Anda. AWS

Security Hub CSPM,, GuardDuty AWS Config, IAM Access Analyzer, dan jejak CloudTrail organisasi muncul di semua akun. Tiga yang pertama mendukung fitur administrator yang didelegasikan yang dibahas sebelumnya di bagian Akun manajemen, akses tepercaya, dan administrator yang didelegasikan. CloudTrail saat ini menggunakan mekanisme agregasi yang berbeda.

Repositori GitHub kode AWS SRA menyediakan contoh implementasi untuk mengaktifkan jalur CSPM GuardDuty,,, AWS Config, CloudTrail dan organisasi Security Hub di semua akun Anda AWS Firewall Manager, termasuk akun Manajemen Org. AWS

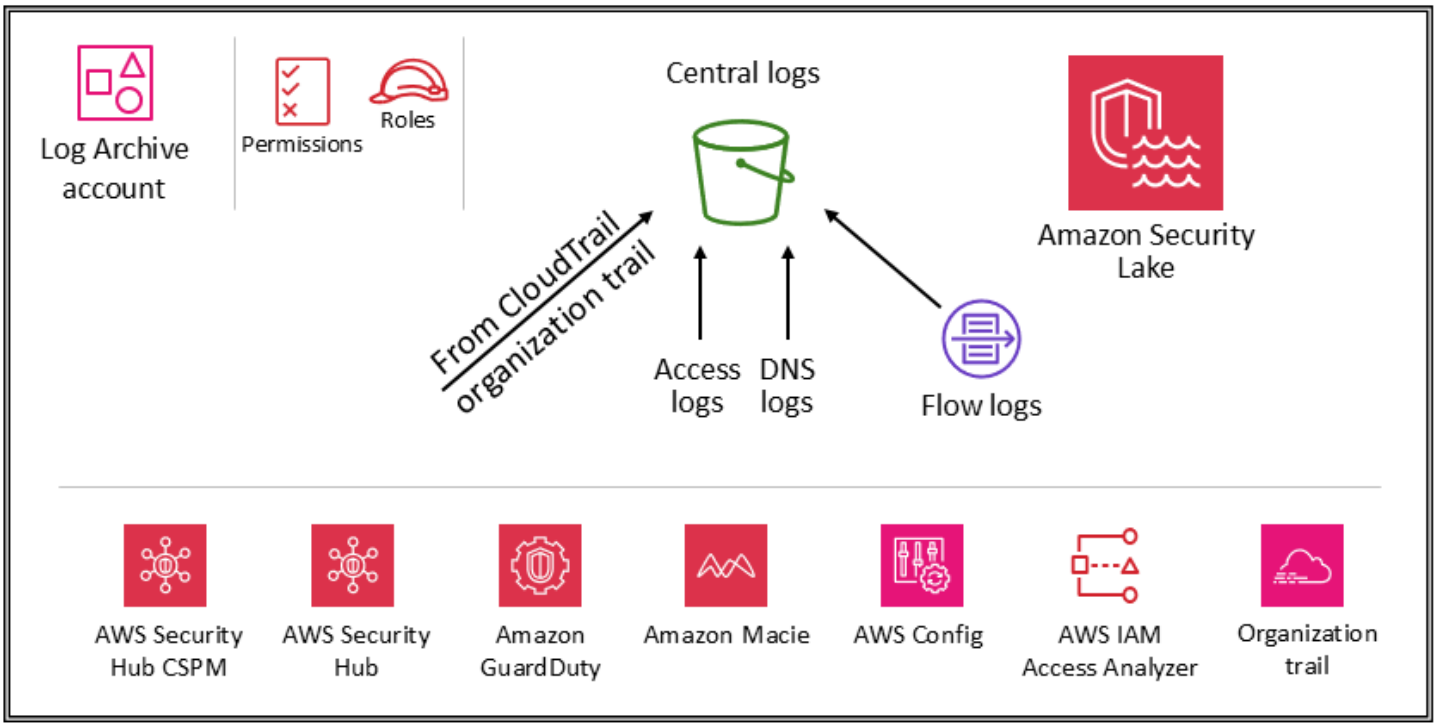
Pertimbangan desain

- Konfigurasi akun tertentu mungkin memerlukan layanan keamanan tambahan. Misalnya, akun yang mengelola bucket S3 (akun Aplikasi dan Arsip Log) juga harus menyertakan Amazon Macie, dan pertimbangkan untuk mengaktifkan pencatatan peristiwa data S3 CloudTrail di layanan keamanan umum ini. (Macie mendukung administrasi yang didelegasikan dengan konfigurasi dan pemantauan terpusat.) Contoh lain adalah Amazon Inspector, yang hanya berlaku untuk akun yang menghosting instans EC2 atau gambar Amazon ECR.
- Selain layanan yang dijelaskan sebelumnya di bagian ini, AWS SRA mencakup dua layanan yang berfokus pada keamanan, Amazon Detective dan AWS Audit Manager, yang mendukung AWS Organizations integrasi dan fungsionalitas administrator yang didelegasikan. Namun, itu tidak termasuk sebagai bagian dari layanan yang direkomendasikan untuk baselining akun, karena kami telah melihat bahwa layanan ini paling baik digunakan dalam skenario berikut:
  - Anda memiliki tim khusus atau kelompok sumber daya yang menjalankan fungsi-fungsi ini. Detective paling baik digunakan oleh tim analis keamanan dan Audit Manager sangat membantu tim audit atau kepatuhan internal Anda.
  - Anda ingin fokus pada seperangkat alat inti seperti GuardDuty dan Security Hub CSPM di awal proyek Anda, dan kemudian membangunnya dengan menggunakan layanan yang memberikan kemampuan tambahan.

Keamanan OU - Akun Arsip Log

Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

Diagram berikut menggambarkan layanan AWS keamanan yang dikonfigurasi di akun Arsip Log.



Akun Arsip Log didedikasikan untuk menelan dan mengarsipkan semua log dan cadangan terkait keamanan. Dengan log terpusat, Anda dapat memantau, mengaudit, dan memberi tahu akses objek Amazon S3, aktivitas tidak sah berdasarkan identitas, perubahan kebijakan IAM, dan aktivitas penting lainnya yang dilakukan pada sumber daya sensitif. Tujuan keamanan sangat mudah: Ini harus penyimpanan yang tidak dapat diubah, diakses hanya dengan mekanisme yang dikontrol, otomatis, dan dipantau, dan dibangun untuk daya tahan (misalnya, dengan menggunakan proses replikasi dan arsip yang sesuai). Kontrol dapat diimplementasikan secara mendalam untuk melindungi integritas dan ketersediaan log dan proses manajemen log. Selain kontrol preventif, seperti menetapkan peran hak istimewa paling sedikit untuk digunakan untuk mengakses dan mengenkripsi log dengan AWS KMS kunci terkontrol, gunakan kontrol detektif seperti AWS Config untuk memantau (dan memperingatkan dan memulihkan) kumpulan izin ini untuk perubahan yang tidak terduga.

Pertimbangan desain

Data log operasional yang digunakan oleh tim infrastruktur, operasi, dan beban kerja Anda sering tumpang tindih dengan data log yang digunakan oleh tim keamanan, audit, dan kepatuhan. Kami menyarankan Anda untuk mengkonsolidasikan data log operasional Anda ke akun Arsip Log. Berdasarkan persyaratan keamanan dan tata kelola spesifik Anda, Anda mungkin perlu memfilter data log operasional yang disimpan ke akun ini. Anda mungkin juga perlu menentukan siapa yang memiliki akses ke data log operasional di akun Arsip Log.

Jenis log

Log utama yang ditampilkan di AWS SRA termasuk AWS CloudTrail (jejak organisasi), log aliran VPC Amazon, log akses dari Amazon AWS WAF dan, dan log DNS dari CloudFront Amazon Route 53. Log ini menyediakan audit atas tindakan yang diambil (atau dicoba) oleh pengguna, peran Layanan AWS, atau entitas jaringan (diidentifikasi, misalnya, oleh alamat IP). Jenis log lainnya (misalnya, log aplikasi atau log database) dapat ditangkap dan diarsipkan juga. Untuk informasi selengkapnya tentang sumber log dan praktik terbaik pencatatan, lihat dokumentasi keamanan untuk setiap layanan.

Amazon S3 sebagai toko log pusat

Banyak informasi Layanan AWS log di Amazon S3 — baik secara default atau eksklusif. AWS CloudTrail, Amazon VPC Flow Logs, Elastic Load Balancing, GuardDuty AWS Config Amazon AWS WAF , dan beberapa contoh layanan yang mencatat informasi di Amazon S3. Ini berarti bahwa integritas log dicapai melalui integritas objek S3; kerahasiaan log dicapai melalui kontrol akses objek S3; dan ketersediaan log dicapai melalui S3 Object Lock, versi objek S3, dan aturan Siklus Hidup S3. Dengan mencatat informasi di bucket S3 khusus dan terpusat yang berada di akun khusus, Anda dapat mengelola log ini hanya dalam beberapa bucket dan menerapkan kontrol keamanan, akses, dan pemisahan tugas yang ketat.

Di AWS SRA, log utama yang disimpan di Amazon S3 CloudTrail berasal, jadi bagian ini menjelaskan cara melindungi objek tersebut. Panduan ini juga berlaku untuk objek S3 lainnya yang dibuat baik oleh aplikasi Anda sendiri atau oleh orang lain Layanan AWS. Terapkan pola ini setiap kali Anda memiliki data di Amazon S3 yang membutuhkan integritas tinggi, kontrol akses yang kuat, serta retensi atau penghancuran otomatis.

Semua objek baru (termasuk CloudTrail log) yang diunggah ke bucket S3 dienkripsi secara default dengan menggunakan enkripsi sisi server Amazon dengan kunci enkripsi yang dikelola Amazon S3 (SSE-S3). Ini membantu melindungi data saat istirahat, tetapi kontrol akses dikendalikan secara eksklusif oleh kebijakan IAM. Untuk menyediakan lapisan keamanan terkelola tambahan, Anda dapat menggunakan enkripsi sisi server dengan AWS KMS kunci yang Anda kelola (SSE-KMS) di semua bucket S3 keamanan. Ini menambahkan kontrol akses tingkat kedua. Untuk membaca file log, pengguna harus memiliki izin baca Amazon S3 untuk objek S3 dan kebijakan atau peran IAM yang diterapkan yang memungkinkan mereka untuk mendekripsi oleh kebijakan kunci terkait.

Dua opsi membantu Anda melindungi atau memverifikasi integritas objek CloudTrail log yang disimpan di Amazon S3. CloudTrail menyediakan validasi integritas file log untuk menentukan apakah file log diubah atau dihapus setelah CloudTrail dikirimkan. Pilihan lainnya adalah S3 Object Lock.

Selain melindungi bucket S3 itu sendiri, Anda dapat mematuhi prinsip hak istimewa paling sedikit untuk layanan logging (misalnya, CloudTrail) dan akun Arsip Log. Misalnya, pengguna dengan izin yang diberikan oleh kebijakan IAM AWS terkelola `AWSCloudTrail_FullAccess` dapat menonaktifkan atau mengkonfigurasi ulang fungsi audit yang paling sensitif dan penting di dalamnya. Akun AWS Batasi penerapan kebijakan IAM ini kepada sesedikit mungkin individu.

Gunakan kontrol detektif, seperti yang disampaikan oleh AWS Config dan IAM Access Analyzer, untuk memantau (dan memperingatkan dan memulihkan) kumpulan kontrol pencegahan yang lebih luas ini untuk perubahan yang tidak terduga.

Untuk diskusi lebih dalam tentang praktik terbaik keamanan untuk bucket S3, lihat dokumentasi Amazon S3, pembicaraan teknologi online, dan posting blog 10 praktik terbaik keamanan teratas untuk mengamankan data di Amazon S3.

> **Contoh implementasi**
>
> Pustaka kode AWS SRA menyediakan contoh implementasi akses publik akun blok Amazon S3. Modul ini memblokir akses publik Amazon S3 untuk semua akun yang ada dan yang akan datang di organisasi. AWS

Amazon Security Lake

AWS SRA merekomendasikan agar Anda menggunakan akun Arsip Log sebagai akun administrator yang didelegasikan untuk Amazon Security Lake. Saat Anda melakukan ini, Security Lake mengumpulkan log yang didukung di bucket S3 khusus di akun yang sama dengan log keamanan yang direkomendasikan SRA lainnya.

Untuk melindungi ketersediaan log dan proses manajemen log, bucket S3 untuk Security Lake harus diakses hanya oleh layanan Security Lake atau oleh peran IAM yang dikelola oleh Security Lake untuk sumber atau pelanggan. Selain menggunakan kontrol preventif–seperti menetapkan peran hak istimewa paling rendah untuk akses, dan mengenkripsi log dengan AWS KMS kunci terkontrol–gunakan kontrol detektif seperti untuk memantau (dan memperingatkan dan memulihkan) kumpulan izin ini AWS Config untuk perubahan yang tidak terduga.

Administrator Security Lake dapat mengaktifkan pengumpulan log di seluruh AWS organisasi Anda. Log ini disimpan dalam bucket S3 regional di akun Arsip Log. Selain itu, untuk memusatkan log dan memfasilitasi penyimpanan dan analisis yang lebih mudah, administrator Security Lake dapat memilih satu atau lebih Wilayah rollup di mana log dari semua bucket S3 regional dikonsolidasikan

dan disimpan. Log dari Layanan AWS yang didukung secara otomatis diubah menjadi skema sumber terbuka standar yang disebut Open Cybersecurity Schema Framework (OCSF) dan disimpan dalam format Apache Parquet di bucket Security Lake S3. Dengan dukungan OCSF, Security Lake secara efisien menormalkan dan mengkonsolidasikan data keamanan dari AWS dan sumber keamanan perusahaan lainnya untuk membuat repositori informasi terkait keamanan yang terpadu dan andal.

Security Lake dapat mengumpulkan log yang terkait dengan peristiwa AWS CloudTrail manajemen dan peristiwa CloudTrail data untuk Amazon S3 dan. AWS Lambda Untuk mengumpulkan acara CloudTrail manajemen di Security Lake, Anda harus memiliki setidaknya satu jejak organisasi CloudTrail Multi-wilayah yang mengumpulkan acara CloudTrail manajemen baca dan tulis. Logging harus diaktifkan untuk jejak. Jejak multi-wilayah mengirimkan file log dari beberapa Wilayah ke satu bucket S3 untuk satu. Akun AWS Jika Wilayah berada di negara yang berbeda, pertimbangkan persyaratan ekspor data untuk menentukan apakah jalur Multi-wilayah dapat diaktifkan.

AWS Security Hub CSPM adalah sumber data asli yang didukung di Security Lake, dan Anda harus menambahkan temuan CSPM Security Hub ke Security Lake. Security Hub CSPM menghasilkan temuan dari banyak integrasi yang berbeda Layanan AWS dan pihak ketiga. Temuan ini membantu Anda mendapatkan gambaran umum tentang postur kepatuhan Anda dan apakah Anda mengikuti rekomendasi AWS dan AWS Partner solusi keamanan.

Untuk mendapatkan visibilitas dan wawasan yang dapat ditindaklanjuti dari log dan peristiwa, Anda dapat melakukan kueri data dengan menggunakan alat seperti Amazon Athena, Amazon Service OpenSearch , Amazon Quick, dan solusi pihak ketiga. Pengguna yang memerlukan akses ke data log Security Lake tidak boleh mengakses akun Arsip Log secara langsung. Mereka harus mengakses data hanya dari akun Security Tooling. Atau mereka dapat menggunakan lokasi lain Akun AWS atau lokal yang menyediakan alat analisis seperti OpenSearch Layanan, Cepat, atau alat pihak ketiga seperti informasi keamanan dan alat manajemen peristiwa (SIEM). Untuk menyediakan akses ke data, administrator harus mengkonfigurasi pelanggan Security Lake di akun Arsip Log dan mengkonfigurasi akun yang memerlukan akses ke data sebagai pelanggan akses kueri. Untuk informasi selengkapnya, lihat Amazon Security Lake di bagian Security OU - Security Tooling account dari panduan ini.

Security Lake menyediakan kebijakan AWS terkelola untuk membantu Anda mengelola akses administrator ke layanan. Untuk informasi selengkapnya, lihat Panduan Pengguna Security Lake. Sebagai praktik terbaik, kami menyarankan Anda membatasi konfigurasi Security Lake melalui pipeline pengembangan dan mencegah perubahan konfigurasi melalui AWS konsol atau (). AWS Command Line Interface AWS CLI Selain itu, Anda harus menyiapkan kebijakan IAM yang ketat dan kebijakan kontrol layanan (SCPs) untuk memberikan hanya izin yang diperlukan untuk mengelola

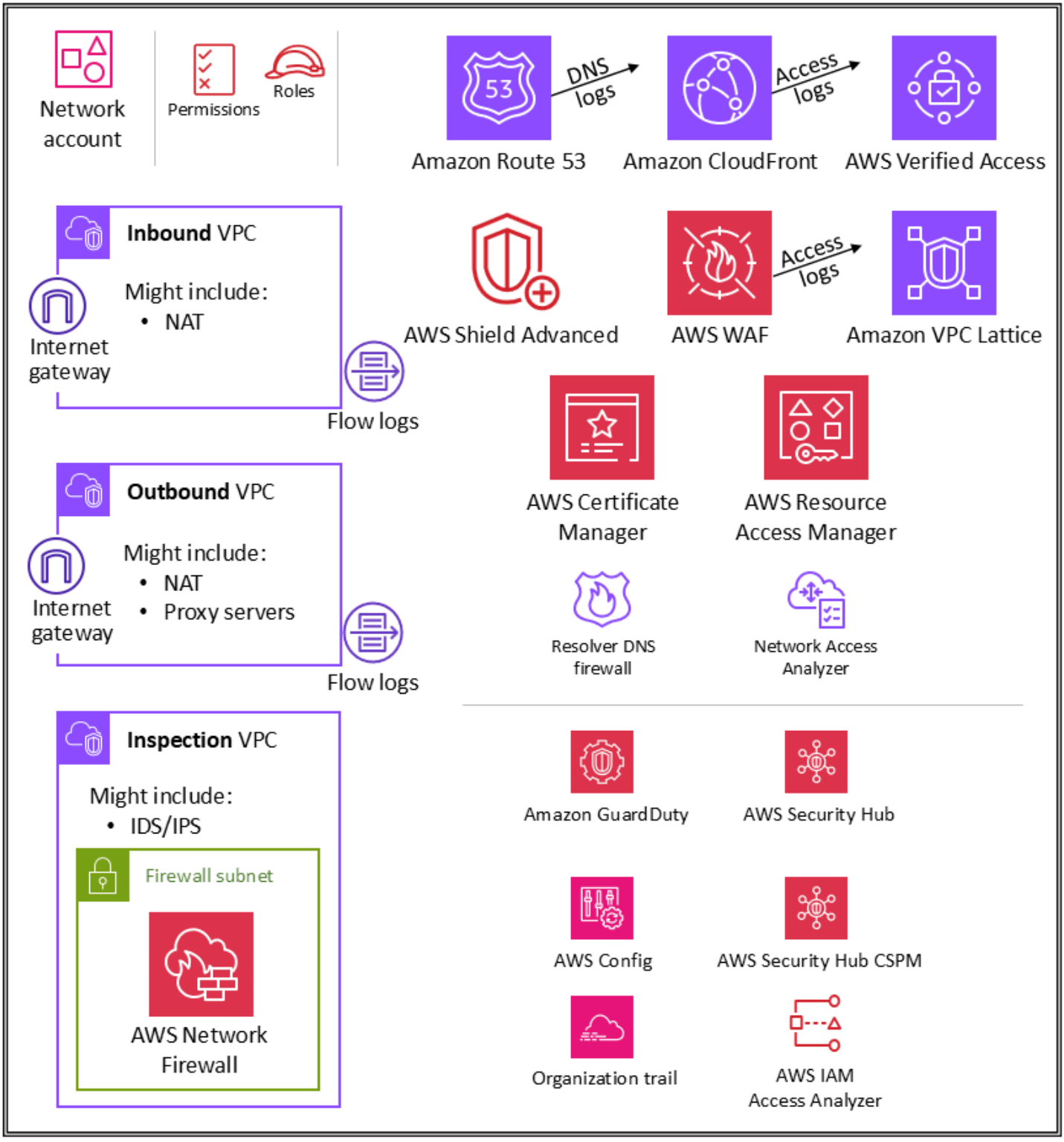
Security Lake. Anda dapat mengonfigurasi notifikasi untuk mendeteksi akses langsung ke bucket S3 ini.

> **Pertimbangan desain**
>
> Ketika Anda mengaktifkan acara CloudTrail manajemen di Security Lake, mereka mengakibatkan biaya Security Lake. Kumpulan acara CloudTrail manajemen di Security Lake membutuhkan jejak organisasi CloudTrail Multi-wilayah yang mengumpulkan acara CloudTrail manajemen baca dan tulis. Jalur pertama ini tersedia tanpa biaya untuk Anda. CloudTrail Acara manajemen biasanya membentuk persentase kecil (sekitar 5%) dari total CloudTrail peristiwa. Ini berlaku untuk pelanggan yang menggunakan AWS Control Tower atau memiliki CloudTrail log terpusat di akun Arsip Log.

Infrastruktur OU - Akun jaringan

Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

Diagram berikut menggambarkan layanan AWS keamanan yang dikonfigurasi di akun Jaringan.



Akun Jaringan mengelola gateway antara aplikasi Anda dan internet yang lebih luas. Penting untuk melindungi antarmuka dua arah itu. Akun Jaringan mengisolasi layanan jaringan, konfigurasi, dan operasi dari beban kerja aplikasi individu, keamanan, dan infrastruktur lainnya. Pengaturan ini tidak

hanya membatasi konektivitas, izin, dan aliran data, tetapi juga mendukung pemisahan tugas dan hak istimewa paling sedikit bagi tim yang perlu beroperasi di akun ini. Dengan membagi aliran jaringan menjadi cloud pribadi virtual inbound dan outbound yang terpisah (VPCs), Anda dapat melindungi infrastruktur dan lalu lintas sensitif dari akses yang tidak diinginkan. Jaringan inbound umumnya dianggap berisiko lebih tinggi dan layak mendapatkan perutean, pemantauan, dan potensi mitigasi masalah yang tepat. Akun infrastruktur ini akan mewarisi pagar pembatas izin dari akun Manajemen Org dan Infrastruktur OU. Tim jaringan (dan keamanan) mengelola sebagian besar infrastruktur di akun ini.

Arsitektur jaringan

Meskipun desain jaringan dan spesifikasi berada di luar cakupan dokumen ini, kami merekomendasikan tiga opsi ini untuk konektivitas jaringan antara berbagai akun: VPC peering AWS PrivateLink,, dan. AWS Transit Gateway Pertimbangan penting dalam memilih di antaranya adalah norma operasional, anggaran, dan kebutuhan bandwidth tertentu.

- VPC peering - Cara paling sederhana untuk menghubungkan dua VPCs adalah dengan menggunakan VPC peering. Koneksi memungkinkan konektivitas dua arah penuh antara. VPCs VPCs yang berada di akun terpisah dan juga Wilayah AWS dapat diintip bersama. Pada skala besar, ketika Anda memiliki puluhan hingga ratusan VPCs, menghubungkannya dengan pengintipan menghasilkan jaring ratusan hingga ribuan koneksi pengintipan, yang dapat menjadi tantangan untuk dikelola dan ditingkatkan. Peering VPC paling baik digunakan ketika sumber daya dalam satu VPC harus berkomunikasi dengan sumber daya di VPC lain, lingkungan keduanya VPCs dikendalikan dan diamankan, dan jumlah yang akan dihubungkan kurang dari 10 (VPCs untuk memungkinkan manajemen individu dari setiap koneksi).
- AWS PrivateLink- PrivateLink menyediakan konektivitas pribadi antara VPCs, layanan, dan aplikasi. Anda dapat membuat aplikasi Anda sendiri di VPC Anda dan mengkonfigurasinya sebagai layanan PrivateLink bertenaga (disebut sebagai layanan endpoint). AWS Prinsipal lain dapat membuat koneksi dari VPC mereka ke layanan endpoint Anda dengan menggunakan titik akhir VPC antarmuka atau titik akhir Load Balancer Gateway, tergantung pada jenis layanannya. Saat Anda menggunakan PrivateLink, lalu lintas layanan tidak melewati jaringan yang dapat dirutekan secara publik. Gunakan PrivateLink saat Anda memiliki pengaturan client-server di mana Anda ingin memberikan satu atau lebih akses VPCs searah konsumen ke layanan tertentu atau serangkaian instance di VPC penyedia layanan. Ini juga merupakan pilihan yang baik ketika klien dan server di keduanya VPCs memiliki alamat IP yang tumpang tindih, karena PrivateLink menggunakan antarmuka jaringan elastis dalam VPC klien sehingga tidak ada konflik IP dengan penyedia layanan.

- AWS Transit GatewayTransit Gateway menyediakan hub-and-spoke desain untuk menghubungkan VPCs dan jaringan lokal sebagai layanan yang dikelola sepenuhnya tanpa mengharuskan Anda menyediakan peralatan virtual. AWS mengelola ketersediaan dan skalabilitas tinggi. Transit gateway adalah sumber daya regional dan dapat menghubungkan ribuan orang di VPCs dalamnya AWS Region. Anda dapat melampirkan konektivitas hybrid Anda (VPN dan AWS Direct Connect koneksi) ke gateway transit tunggal, sehingga mengkonsolidasikan dan mengendalikan seluruh konfigurasi perutean AWS organisasi Anda di satu tempat. Gateway transit memecahkan kompleksitas yang terlibat dengan membuat dan mengelola beberapa koneksi peering VPC dalam skala besar. Ini adalah default untuk sebagian besar arsitektur jaringan, tetapi kebutuhan spesifik seputar biaya, bandwidth, dan latensi mungkin membuat VPC mengintip lebih cocok untuk kebutuhan Anda.

Masuk (masuknya) VPC

VPC inbound dimaksudkan untuk menerima, memeriksa, dan merutekan koneksi jaringan yang dimulai dari luar aplikasi. Tergantung pada spesifikasi aplikasi, Anda dapat mengharapkan untuk melihat beberapa terjemahan alamat jaringan (NAT) di VPC ini. Log aliran dari VPC ini ditangkap dan disimpan di akun Arsip Log.

Keluar (jalan keluar) VPC

VPC keluar dimaksudkan untuk menangani koneksi jaringan yang dimulai dari dalam aplikasi. Bergantung pada spesifikasi aplikasi, Anda dapat melihat NAT lalu lintas, titik akhir VPC Layanan AWS spesifik, dan hosting titik akhir API eksternal di VPC ini. Log aliran dari VPC ini ditangkap dan disimpan di akun Arsip Log.

Inspeksi VPC

VPC inspeksi khusus menyediakan pendekatan yang disederhanakan dan sentral untuk mengelola inspeksi antara VPCs (dalam hal yang sama atau berbeda Wilayah AWS), internet, dan jaringan lokal. Untuk AWS SRA, pastikan bahwa semua lalu lintas antar VPCs melewati VPC inspeksi, dan hindari menggunakan VPC inspeksi untuk beban kerja lainnya.

AWS Network Firewall

AWS Network Firewalladalah layanan firewall jaringan terkelola yang sangat tersedia untuk VPC Anda. Ini memungkinkan Anda untuk dengan mudah menyebarkan dan mengelola inspeksi stateful,

pencegahan dan deteksi intrusi, dan penyaringan web untuk membantu melindungi jaringan virtual Anda. AWS Anda dapat menggunakan Network Firewall untuk mendekripsi sesi TLS dan memeriksa lalu lintas masuk dan keluar. Untuk informasi selengkapnya tentang mengonfigurasi Network Firewall, lihat posting blog AWS Network Firewall — Layanan Firewall Terkelola Baru di VPC.

Anda menggunakan firewall berdasarkan Per-Availability Zone di VPC Anda. Untuk setiap Availability Zone, Anda memilih subnet untuk meng-host endpoint firewall yang memfilter lalu lintas Anda. Titik akhir firewall di Availability Zone dapat melindungi semua subnet di dalam zona kecuali subnet di mana ia berada. Tergantung pada kasus penggunaan dan model penerapan, subnet firewall dapat bersifat publik atau pribadi. Firewall benar-benar transparan terhadap arus lalu lintas dan tidak melakukan terjemahan alamat jaringan (NAT). Ini mempertahankan sumber dan alamat tujuan. Dalam arsitektur referensi ini, titik akhir firewall di-host dalam VPC inspeksi. Semua lalu lintas dari VPC masuk dan ke VPC keluar dirutekan melalui subnet firewall ini untuk diperiksa.

Network Firewall membuat aktivitas firewall terlihat secara real time melalui CloudWatch metrik Amazon, dan menawarkan peningkatan visibilitas lalu lintas jaringan dengan mengirimkan log ke Amazon Simple Storage Service (Amazon S3) CloudWatch, dan Amazon Data Firehose. Network Firewall dapat dioperasikan dengan pendekatan keamanan yang ada, termasuk teknologi dari AWS Mitra. Anda juga dapat mengimpor aturan Suricata yang ada, yang mungkin telah ditulis secara internal atau bersumber secara eksternal dari vendor pihak ketiga atau platform sumber terbuka.

Dalam AWS SRA, Network Firewall digunakan dalam akun jaringan karena fungsi layanan yang berfokus pada kontrol jaringan selaras dengan maksud akun.

Pertimbangan desain

- AWS Firewall Manager mendukung Network Firewall, sehingga Anda dapat mengonfigurasi dan menerapkan aturan Network Firewall secara terpusat di seluruh organisasi Anda. (Untuk detailnya, lihat Menggunakan AWS Network Firewall kebijakan di Firewall Manager dalam AWS dokumentasi.) Ketika Anda mengkonfigurasi Firewall Manager, secara otomatis membuat firewall dengan set aturan di akun dan VPCs yang Anda tentukan. Ini juga menyebarkan titik akhir di subnet khusus untuk setiap Availability Zone yang berisi subnet publik. Pada saat yang sama, setiap perubahan pada seperangkat aturan yang dikonfigurasi secara terpusat secara otomatis diperbarui ke hilir pada firewall Network Firewall yang digunakan.
- Ada beberapa model penyebaran yang tersedia dengan Network Firewall. Model yang tepat tergantung pada kasus penggunaan dan persyaratan Anda. Contohnya meliputi hal berikut:

    - Model penyebaran terdistribusi di mana Network Firewall dikerahkan ke individu. VPCs
    - Model penyebaran terpusat di mana Network Firewall dikerahkan ke dalam VPC terpusat untuk lalu lintas timur-barat (VPC-to-VPC) atau utara-selatan (internet egress and ingress, on-premise).
    - Model penyebaran gabungan di mana Network Firewall dikerahkan ke dalam VPC terpusat untuk timur-barat dan subset lalu lintas utara-selatan.
- Sebagai praktik terbaik, jangan gunakan subnet Network Firewall untuk menyebarkan layanan lainnya. Ini karena Network Firewall tidak dapat memeriksa lalu lintas dari sumber atau tujuan dalam subnet firewall.

Penganalisis Akses Jaringan

Network Access Analyzer adalah fitur Amazon VPC yang mengidentifikasi akses jaringan yang tidak diinginkan ke sumber daya Anda. Anda dapat menggunakan Network Access Analyzer untuk memvalidasi segmentasi jaringan, mengidentifikasi sumber daya yang dapat diakses dari internet atau hanya dapat diakses dari rentang alamat IP tepercaya, dan memvalidasi bahwa Anda memiliki kontrol jaringan yang sesuai di semua jalur jaringan.

Network Access Analyzer menggunakan algoritma penalaran otomatis untuk menganalisis jalur jaringan yang dapat diambil paket antara sumber daya dalam AWS jaringan, dan menghasilkan temuan untuk jalur yang sesuai dengan Lingkup Akses Jaringan yang Anda tentukan. Network Access Analyzer melakukan analisis statis dari konfigurasi jaringan, yang berarti bahwa tidak ada paket yang ditransmisikan dalam jaringan sebagai bagian dari analisis ini.

Aturan Amazon Inspector Network Reachability menyediakan fitur terkait. Temuan yang dihasilkan oleh aturan ini digunakan dalam akun Aplikasi. Baik Network Access Analyzer dan Network Reachability menggunakan teknologi terbaru dari inisiatif keamanan yang AWS dapat dibuktikan, dan mereka menerapkan teknologi ini dengan area fokus yang berbeda. Paket Network Reachability berfokus secara khusus pada EC2 instance dan aksesibilitas internetnya.

Akun Jaringan mendefinisikan infrastruktur jaringan penting yang mengontrol lalu lintas masuk dan keluar dari AWS lingkungan Anda. Lalu lintas ini perlu dipantau dengan ketat. Dalam AWS SRA, Network Access Analyzer digunakan dalam akun Jaringan untuk membantu mengidentifikasi akses jaringan yang tidak diinginkan, mengidentifikasi sumber daya yang dapat diakses internet melalui gateway internet, dan memverifikasi bahwa kontrol jaringan yang sesuai seperti firewall jaringan dan gateway NAT hadir di semua jalur jaringan antara sumber daya dan gateway internet.

Pertimbangan desain

Network Access Analyzer adalah fitur Amazon VPC, dan dapat digunakan di Akun AWS semua yang memiliki VPC. Administrator jaringan bisa mendapatkan peran IAM lintas akun dengan cakupan ketat untuk memvalidasi bahwa jalur jaringan yang disetujui diberlakukan di masing-masing. Akun AWS

AWS RAM

AWS Resource Access Manager(AWS RAM) membantu Anda berbagi AWS sumber daya yang Anda buat dengan aman Akun AWS dengan yang lain Akun AWS.AWS RAM menyediakan tempat sentral untuk mengelola berbagi sumber daya dan untuk membakukan pengalaman ini di seluruh akun. Ini membuatnya lebih mudah untuk mengelola sumber daya sambil memanfaatkan isolasi administratif dan penagihan, dan mengurangi ruang lingkup manfaat penahanan dampak yang diberikan oleh strategi multi-akun. Jika akun Anda dikelola oleh AWS Organizations, AWS RAM memungkinkan Anda berbagi sumber daya dengan semua akun di organisasi, atau hanya dengan akun dalam satu atau beberapa unit organisasi tertentu (OUs). Anda juga dapat berbagi dengan ID akun tertentu Akun AWS , terlepas dari apakah akun tersebut merupakan bagian dari organisasi. Anda juga dapat membagikan beberapa jenis sumber daya yang didukung dengan peran dan pengguna IAM tertentu.

AWS RAM memungkinkan Anda berbagi sumber daya yang tidak mendukung kebijakan berbasis sumber daya IAM, seperti subnet VPC dan aturan Route 53. Selanjutnya, dengan AWS RAM, pemilik sumber daya dapat melihat kepala sekolah mana yang memiliki akses ke sumber daya individu yang telah mereka bagikan. Prinsipal IAM dapat mengambil daftar sumber daya yang dibagikan dengan mereka secara langsung, yang tidak dapat mereka lakukan dengan sumber daya yang dibagikan oleh kebijakan sumber daya IAM. Jika AWS RAM digunakan untuk berbagi sumber daya di luar AWS organisasi Anda, proses undangan dimulai. Penerima harus menerima undangan sebelum akses ke sumber daya diberikan. Ini memberikan pemeriksaan dan saldo tambahan.

AWS RAM dipanggil dan dikelola oleh pemilik sumber daya, di akun tempat sumber daya bersama digunakan. Salah satu kasus penggunaan umum untuk AWS RAM diilustrasikan dalam AWS SRA adalah untuk administrator jaringan untuk berbagi subnet VPC dan gateway transit dengan seluruh organisasi. AWS Ini memberikan kemampuan untuk memisahkan Akun AWS dan fungsi manajemen jaringan dan membantu mencapai pemisahan tugas. Untuk informasi selengkapnya tentang berbagi VPC, lihat AWS posting blog Berbagi VPC: Pendekatan baru untuk beberapa akun dan manajemen VPC dan whitepaper infrastruktur jaringan.AWS

Pertimbangan desain

Meskipun AWS RAM sebagai layanan hanya digunakan dalam akun Jaringan di AWS SRA, biasanya akan digunakan di lebih dari satu akun. Misalnya, Anda dapat memusatkan manajemen data lake Anda ke satu akun data lake, lalu membagikan sumber daya katalog AWS Lake Formation data (database dan tabel) dengan akun lain di organisasi Anda AWS . Untuk informasi selengkapnya, lihat AWS Lake Formation dokumentasi dan posting AWS blog Bagikan data Anda dengan aman di seluruh Akun AWS penggunaan AWS Lake Formation. Selain itu, administrator keamanan dapat menggunakan AWS RAM untuk mengikuti praktik terbaik ketika mereka membangun AWS Private Certificate Authority hierarki. CAs dapat dibagikan dengan pihak ketiga eksternal, yang dapat menerbitkan sertifikat tanpa memiliki akses ke hierarki CA. Hal ini memungkinkan organisasi originasi untuk membatasi dan mencabut akses pihak ketiga.

Akses Terverifikasi AWS

Akses Terverifikasi AWSmenyediakan akses aman ke aplikasi dan sumber daya perusahaan tanpa VPN. Ini meningkatkan postur keamanan dan membantu menerapkan akses tanpa kepercayaan dengan mengevaluasi setiap permintaan akses secara real time terhadap persyaratan yang telah ditentukan. Anda dapat menentukan kebijakan akses unik untuk setiap aplikasi dengan kondisi berdasarkan data identitas dan postur perangkat. Verified Access menyediakan akses aman ke aplikasi HTTP (S), seperti aplikasi berbasis browser, dan aplikasi non-HTTP (S) melalui protokol TCP, SSH, dan RDP untuk aplikasi seperti repositori Git, database, dan grup instance. EC2 Ini dapat diakses dengan menggunakan terminal baris perintah atau dari aplikasi desktop. Akses Terverifikasi juga menyederhanakan operasi keamanan dengan membantu administrator mengatur dan memantau kebijakan akses secara efisien. Ini membebaskan waktu untuk memperbarui kebijakan, menanggapi insiden keamanan dan konektivitas, dan mengaudit standar kepatuhan. Verified Access juga mendukung integrasi AWS WAF untuk membantu Anda menyaring ancaman umum seperti injeksi SQL dan cross-site scripting (XSS). Akses Terverifikasi terintegrasi dengan mulus AWS IAM Identity Center, yang memungkinkan pengguna untuk mengautentikasi dengan penyedia identitas pihak ketiga berbasis SAMP (). IdPs Jika Anda sudah memiliki solusi iDP kustom yang kompatibel dengan OpenID Connect (OIDC), Verified Access juga dapat mengautentikasi pengguna dengan langsung terhubung dengan IDP Anda. Akses Terverifikasi mencatat setiap upaya akses sehingga Anda dapat dengan cepat menanggapi insiden keamanan dan permintaan audit. Akses Terverifikasi mendukung pengiriman log ini ke Amazon Simple Storage Service (Amazon S3), Amazon Logs, dan CloudWatch Amazon Data Firehose.

Verified Access mendukung dua pola aplikasi perusahaan yang umum: internal dan internet-facing. Verified Access terintegrasi dengan aplikasi dengan menggunakan Application Load Balancers atau antarmuka jaringan elastis. Jika Anda menggunakan Application Load Balancer, Akses Terverifikasi memerlukan penyeimbang beban internal. Karena Verified Access mendukung AWS WAF pada tingkat instans, aplikasi yang sudah ada yang memiliki AWS WAF integrasi dengan Application Load Balancer dapat memindahkan kebijakan dari penyeimbang beban ke instance Akses Terverifikasi. Aplikasi perusahaan direpresentasikan sebagai titik akhir Akses Terverifikasi. Setiap titik akhir dikaitkan dengan grup Akses Terverifikasi dan mewarisi kebijakan akses untuk grup. Grup Akses Terverifikasi adalah kumpulan titik akhir Akses Terverifikasi dan kebijakan Akses Terverifikasi tingkat grup. Grup menyederhanakan manajemen kebijakan dan memungkinkan administrator TI untuk menyiapkan kriteria dasar. Pemilik aplikasi dapat lebih lanjut menentukan kebijakan terperinci tergantung pada sensitivitas aplikasi.

Di AWS SRA, Akses Terverifikasi di-host dalam akun Jaringan. Tim TI pusat menyiapkan konfigurasi yang dikelola secara terpusat. Misalnya, mereka mungkin menghubungkan penyedia kepercayaan seperti penyedia identitas (misalnya, Okta) dan penyedia kepercayaan perangkat (misalnya, Jamf), membuat grup, dan menentukan kebijakan tingkat grup. Konfigurasi ini kemudian dapat dibagikan dengan puluhan, ratusan, atau ribuan akun beban kerja dengan menggunakan. AWS RAM Hal ini memungkinkan tim aplikasi untuk mengelola endpoint dasar yang mengelola aplikasi mereka tanpa overhead dari tim lain. AWS RAM menyediakan cara yang dapat diskalakan untuk memanfaatkan Akses Terverifikasi untuk aplikasi perusahaan yang di-host di berbagai akun beban kerja.

> **Pertimbangan desain**
>
> Anda dapat mengelompokkan titik akhir untuk aplikasi yang memiliki persyaratan keamanan serupa untuk menyederhanakan administrasi kebijakan, dan kemudian berbagi grup dengan akun aplikasi. Semua aplikasi dalam grup berbagi kebijakan grup. Jika aplikasi dalam grup memerlukan kebijakan khusus karena kasus tepi, Anda dapat menerapkan kebijakan tingkat aplikasi untuk aplikasi tersebut.

Kisi VPC Amazon

Amazon VPC Lattice adalah layanan jaringan aplikasi yang menghubungkan, memantau, dan mengamankan komunikasi. service-to-service Layanan, sering disebut layanan mikro, adalah unit perangkat lunak yang dapat digunakan secara independen yang memberikan tugas tertentu. VPC Lattice secara otomatis mengelola konektivitas jaringan dan perutean lapisan aplikasi antara layanan di seluruh VPCs dan Akun AWS tanpa mengharuskan Anda mengelola konektivitas jaringan

yang mendasarinya, penyeimbang beban frontend, atau proxy sespan. Ini menyediakan proxy lapisan aplikasi yang dikelola sepenuhnya yang menyediakan perutean tingkat aplikasi berdasarkan karakteristik permintaan seperti jalur dan header. VPC Lattice dibangun ke dalam infrastruktur VPC, sehingga memberikan pendekatan yang konsisten di berbagai jenis komputasi seperti Amazon Elastic Compute Cloud (Amazon), Amazon Elastic Kubernetes Service (Amazon EC2 EKS), dan. AWS Lambda VPC Lattice juga mendukung perutean tertimbang untuk dan penerapan gaya kenari. blue/green Anda dapat menggunakan VPC Lattice untuk membuat jaringan layanan dengan batas logis yang secara otomatis mengimplementasikan penemuan layanan dan konektivitas. VPC Lattice terintegrasi dengan IAM untuk service-to-service otentikasi dan otorisasi menggunakan kebijakan autentikasi.

VPC Lattice terintegrasi dengan AWS RAM untuk memungkinkan berbagi layanan dan jaringan layanan. AWS SRA menggambarkan arsitektur terdistribusi di mana pengembang atau pemilik layanan membuat layanan VPC Lattice di akun Aplikasi mereka. Pemilik layanan menentukan pendengar, aturan perutean, dan grup target bersama dengan kebijakan autentikasi. Mereka kemudian berbagi layanan dengan akun lain, dan mengaitkan layanan dengan jaringan layanan VPC Lattice. Jaringan ini dibuat oleh administrator jaringan di akun Jaringan dan dibagikan dengan akun Aplikasi. Administrator jaringan mengonfigurasi kebijakan dan pemantauan autentikasi tingkat jaringan layanan. Administrator mengaitkan VPCs dan layanan VPC Lattice dengan satu atau lebih jaringan layanan. Untuk panduan mendetail tentang arsitektur terdistribusi ini, lihat posting AWS blog Membangun konektivitas multi-VPC multi-akun yang aman untuk aplikasi Anda dengan Amazon VPC Lattice

Pertimbangan desain

- Bergantung pada model operasi layanan atau visibilitas jaringan layanan organisasi Anda, administrator jaringan dapat berbagi jaringan layanan mereka dan dapat memberikan pemilik layanan kontrol untuk mengaitkan layanan mereka dan VPCs dengan jaringan layanan ini. Atau, pemilik layanan dapat berbagi layanan mereka, dan administrator jaringan dapat mengaitkan layanan dengan jaringan layanan.
- Klien dapat mengirim permintaan ke layanan yang terkait dengan jaringan layanan hanya jika klien berada dalam VPC yang terkait dengan jaringan layanan yang sama. Lalu lintas klien yang melintasi koneksi peering VPC atau gateway transit ditolak.

Keamanan tepi

Keamanan tepi umumnya mencakup tiga jenis perlindungan: pengiriman konten yang aman, perlindungan lapisan jaringan dan aplikasi, dan mitigasi penolakan layanan (S) terdistribusi. DDo Konten seperti data, video, aplikasi, dan APIs harus dikirimkan dengan cepat dan aman, menggunakan versi TLS yang direkomendasikan untuk mengenkripsi komunikasi antar titik akhir. Konten juga harus memiliki batasan akses melalui cookie yang ditandatangani URLs, ditandatangani, dan otentikasi token. Keamanan tingkat aplikasi harus dirancang untuk mengontrol lalu lintas bot, memblokir pola serangan umum seperti injeksi SQL atau cross-site scripting (XSS), dan memberikan visibilitas lalu lintas web. Di ujungnya, mitigasi DDo S menyediakan lapisan pertahanan penting yang memastikan ketersediaan operasi dan layanan bisnis yang sangat penting. Aplikasi dan APIs harus dilindungi dari banjir SYN, banjir UDP, atau serangan refleksi lainnya, dan memiliki mitigasi inline untuk menghentikan serangan lapisan jaringan dasar.

AWS menawarkan beberapa layanan untuk membantu menyediakan lingkungan yang aman, dari cloud inti hingga tepi AWS jaringan. Amazon CloudFront, AWS Certificate Manager (ACM),, AWS Shield AWS WAF, dan Amazon Route 53 bekerja sama untuk membantu menciptakan perimeter keamanan yang fleksibel dan berlapis. Dengan CloudFront, konten APIs, atau aplikasi dapat dikirimkan melalui HTTPS dengan TLSv1 menggunakan.3 untuk mengenkripsi dan mengamankan komunikasi antara klien penampil dan klien. CloudFront Anda dapat menggunakan ACM untuk membuat sertifikat SSL khusus dan menyebarkannya ke CloudFront distribusi secara gratis. ACM secara otomatis menangani perpanjangan sertifikat. Shield adalah layanan perlindungan DDo S terkelola yang membantu melindungi aplikasi yang berjalan. AWS Ini menyediakan deteksi dinamis dan mitigasi inline otomatis yang meminimalkan waktu henti dan latensi aplikasi. AWS WAF memungkinkan Anda membuat aturan untuk memfilter lalu lintas web berdasarkan kondisi tertentu (alamat IP, header dan badan HTTP, atau kustom URIs), serangan web umum, dan bot yang meresap. Route 53 adalah layanan web DNS yang sangat tersedia dan dapat diskalakan. Route 53 menghubungkan permintaan pengguna ke aplikasi internet yang berjalan di AWS atau di tempat. AWS SRA mengadopsi arsitektur ingress jaringan terpusat dengan menggunakan AWS Transit Gateway, di-host dalam akun Jaringan, sehingga infrastruktur keamanan edge juga terpusat di akun ini.

Amazon CloudFront

Amazon CloudFront adalah jaringan pengiriman konten aman (CDN) yang memberikan perlindungan inheren terhadap lapisan jaringan umum dan upaya transport DDo S. Anda dapat mengirimkan konten, APIs, atau aplikasi Anda dengan menggunakan sertifikat TLS, dan fitur TLS lanjutan diaktifkan secara otomatis. Anda dapat menggunakan AWS Certificate Manager (ACM) untuk

membuat sertifikat TLS kustom dan menerapkan komunikasi HTTPS antara pemirsa dan CloudFront, seperti yang dijelaskan nanti di bagian ACM. Anda juga dapat mengharuskan komunikasi antara CloudFront dan asal kustom Anda menerapkan end-to-end enkripsi dalam perjalanan. Untuk skenario ini, Anda harus menginstal sertifikat TLS di server asal Anda. Jika asal Anda adalah penyeimbang beban elastis, Anda dapat menggunakan sertifikat yang dihasilkan oleh ACM atau sertifikat yang divalidasi oleh otoritas sertifikat pihak ketiga (CA) dan diimpor ke ACM. Jika titik akhir situs web bucket S3 berfungsi sebagai asal CloudFront, Anda tidak dapat mengonfigurasi CloudFront untuk menggunakan HTTPS dengan asal Anda, karena Amazon S3 tidak mendukung HTTPS untuk titik akhir situs web. (Namun, Anda masih dapat meminta HTTPS antara pemirsa dan CloudFront.) Untuk semua asal lain yang mendukung pemasangan sertifikat HTTPS, Anda harus menggunakan sertifikat yang ditandatangani oleh CA pihak ketiga tepercaya.

CloudFront menyediakan beberapa opsi untuk mengamankan dan membatasi akses ke konten Anda. Misalnya, dapat membatasi akses ke asal Amazon S3 Anda dengan menggunakan cookie yang URLs ditandatangani dan ditandatangani. Untuk informasi selengkapnya, lihat Mengkonfigurasi akses aman dan membatasi akses ke konten dalam CloudFront dokumentasi.

AWS SRA menggambarkan CloudFront distribusi terpusat di akun Jaringan karena mereka selaras dengan pola jaringan terpusat yang diimplementasikan dengan menggunakan. AWS Transit Gateway Dengan menerapkan dan mengelola CloudFront distribusi di akun Jaringan, Anda mendapatkan manfaat dari kontrol terpusat. Anda dapat mengelola semua CloudFront distribusi di satu tempat, yang membuatnya lebih mudah untuk mengontrol akses, mengonfigurasi pengaturan, dan memantau penggunaan di semua akun. Selain itu, Anda dapat mengelola sertifikat ACM, catatan DNS, dan CloudFront pencatatan dari satu akun terpusat.

Dasbor CloudFront keamanan menyediakan AWS WAF visibilitas dan kontrol langsung dalam CloudFront distribusi Anda. Anda mendapatkan visibilitas ke tren keamanan teratas aplikasi Anda, lalu lintas yang diizinkan dan diblokir, dan aktivitas bot. Anda dapat menggunakan alat investigasi seperti penganalisis log visual dan kontrol pemblokiran bawaan untuk mengisolasi pola lalu lintas dan memblokir lalu lintas tanpa menanyakan log atau menulis aturan keamanan.

Pertimbangan desain

- Atau, Anda dapat menyebarkan CloudFront sebagai bagian dari aplikasi di akun Aplikasi. Dalam skenario ini, tim aplikasi membuat keputusan seperti bagaimana CloudFront distribusi dikerahkan, menentukan kebijakan cache yang sesuai, dan bertanggung jawab atas tata kelola, audit, dan pemantauan distribusi. CloudFront Dengan menyebarkan CloudFront distribusi di beberapa akun, Anda bisa mendapatkan keuntungan dari

kuota layanan tambahan. Sebagai manfaat lain, Anda dapat menggunakan CloudFront konfigurasi identitas akses asal (OAI) dan kontrol akses asal (OAC) yang melekat dan otomatis untuk membatasi akses ke asal Amazon S3.

- Ketika Anda mengirimkan konten web melalui CDN seperti CloudFront, Anda harus mencegah pemirsa melewati CDN dan mengakses konten asal Anda secara langsung. Untuk mencapai pembatasan akses asal ini, Anda dapat menggunakan CloudFront dan AWS WAF menambahkan header khusus dan memverifikasi header sebelum meneruskan permintaan ke asal kustom Anda. Untuk penjelasan rinci tentang solusi ini, lihat posting blog AWS keamanan Cara meningkatkan keamanan CloudFront asal Amazon dengan AWS WAF dan AWS Secrets Manager. Metode alternatif adalah membatasi hanya daftar CloudFront awalan dalam grup keamanan yang terkait dengan Application Load Balancer. Ini akan membantu memastikan bahwa hanya CloudFront distribusi yang dapat mengakses penyeimbang beban.

AWS WAF

AWS WAFadalah firewall aplikasi web yang membantu melindungi aplikasi web Anda dari eksploitasi web seperti kerentanan umum dan bot yang dapat memengaruhi ketersediaan aplikasi, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan. Ini dapat diintegrasikan dengan CloudFront distribusi Amazon, API REST Amazon API Gateway, Application Load Balancer, API GraphQL AWS AppSync , kumpulan pengguna Amazon Cognito, dan layanan. AWS App Runner

AWS WAF menggunakan daftar kontrol akses web (ACLs) untuk melindungi sekumpulan AWS sumber daya. ACL web adalah seperangkat aturan yang mendefinisikan kriteria inspeksi, dan tindakan terkait yang harus diambil (memblokir, mengizinkan, menghitung, atau menjalankan kontrol bot) jika permintaan web memenuhi kriteria. AWS WAF menyediakan seperangkat aturan terkelola yang memberikan perlindungan terhadap kerentanan aplikasi umum. Aturan-aturan ini dikuratori dan dikelola oleh AWS dan AWS Mitra. AWS WAF juga menawarkan bahasa aturan yang kuat untuk membuat aturan khusus. Anda dapat menggunakan aturan khusus untuk menulis kriteria inspeksi yang sesuai dengan kebutuhan khusus Anda. Contohnya termasuk pembatasan IP, batasan geografis, dan versi aturan terkelola yang disesuaikan yang lebih sesuai dengan perilaku aplikasi spesifik Anda.

AWS WAF menyediakan seperangkat aturan terkelola tingkat cerdas untuk bot umum dan bertarget serta perlindungan pengambilalihan akun (ATP). Anda dikenakan biaya berlangganan dan biaya

inspeksi lalu lintas saat Anda menggunakan kontrol bot dan grup aturan ATP. Oleh karena itu, kami menyarankan Anda memantau lalu lintas Anda terlebih dahulu dan kemudian memutuskan apa yang akan digunakan. Anda dapat menggunakan dasbor manajemen bot dan pengambilalihan akun yang tersedia secara gratis di AWS WAF konsol untuk memantau aktivitas ini dan kemudian memutuskan apakah Anda memerlukan grup AWS WAF aturan tingkat cerdas.

Dalam AWS SRA, AWS WAF terintegrasi dengan CloudFront dalam akun Jaringan. Dalam konfigurasi ini, pemrosesan AWS WAF aturan terjadi di lokasi tepi alih-alih di dalam VPC. Ini memungkinkan pemfilteran lalu lintas berbahaya lebih dekat ke pengguna akhir yang meminta konten, dan membantu membatasi lalu lintas berbahaya memasuki jaringan inti Anda.

Anda dapat mengirim AWS WAF log lengkap ke bucket S3 di akun Arsip Log dengan mengonfigurasi akses lintas akun ke bucket S3. Untuk informasi lebih lanjut, lihat artikel AWS re:Post tentang topik ini.

Pertimbangan desain

- Sebagai alternatif untuk menyebarkan AWS WAF secara terpusat di akun Jaringan, beberapa kasus penggunaan lebih baik dipenuhi dengan menerapkan AWS WAF di akun Aplikasi. Misalnya, Anda dapat memilih opsi ini saat menerapkan CloudFront distribusi di akun Aplikasi atau memiliki Application Load Balancer yang menghadap publik, atau jika Anda menggunakan API Gateway di depan aplikasi web Anda. Jika Anda memutuskan untuk menerapkan AWS WAF di setiap akun Aplikasi, gunakan AWS Firewall Manager untuk mengelola AWS WAF aturan di akun ini dari akun Security Tooling terpusat.
- Anda juga dapat menambahkan AWS WAF aturan umum di CloudFront lapisan dan AWS WAF aturan khusus aplikasi tambahan di sumber daya Regional seperti Application Load Balancer atau gateway API.

AWS Shield

AWS Shieldadalah layanan perlindungan DDo S terkelola yang melindungi aplikasi yang berjalan. AWS Ada dua tingkatan Shield: Shield Standarddan Shield Advanced. Shield Standard memberi semua AWS pelanggan perlindungan terhadap kejadian infrastruktur (lapisan 3 dan 4) yang paling umum tanpa biaya tambahan. Shield Advanced menyediakan mitigasi otomatis yang lebih canggih untuk peristiwa tidak sah yang menargetkan aplikasi di Amazon yang dilindungi, Elastic Load EC2 Balancing (Elastic Load Balancing) CloudFront,,, AWS Global Accelerator dan zona host Route 53.

Jika Anda memiliki situs web dengan visibilitas tinggi atau rentan terhadap serangan DDo S yang sering, Anda dapat mempertimbangkan fitur tambahan yang disediakan Shield Advanced.

Anda dapat menggunakan fitur mitigasi lapisan DDo S aplikasi otomatis Shield Advanced untuk mengonfigurasi Shield Advanced untuk merespons secara otomatis untuk mengurangi serangan lapisan aplikasi (lapisan 7) terhadap CloudFront distribusi yang dilindungi, penyeimbang beban Elastic Load Balancing (Elastic Load Balancing) (Aplikasi, Jaringan, dan Klasik), zona yang dihosting Amazon Route 53, alamat IP Amazon Elastic, dan akselerator standar. EC2 AWS Global Accelerator Saat Anda mengaktifkan fitur ini, Shield Advanced secara otomatis menghasilkan AWS WAF aturan khusus untuk mengurangi serangan DDo S. Shield Advanced juga memberi Anda akses ke AWS Shield Response Team (SRT). Anda dapat menghubungi SRT kapan saja untuk membuat dan mengelola mitigasi khusus untuk aplikasi Anda atau selama serangan S aktif. DDo Jika Anda ingin SRT secara proaktif memantau sumber daya yang dilindungi dan menghubungi Anda selama upaya DDo S, pertimbangkan untuk mengaktifkan fitur keterlibatan proaktif.

Pertimbangan desain

- Jika Anda memiliki beban kerja yang dihadapkan oleh sumber daya yang menghadap ke internet di akun Aplikasi, seperti Application Load Balancer CloudFront, atau Network Load Balancer, konfigurasikan Shield Advanced di akun Aplikasi dan tambahkan sumber daya tersebut ke perlindungan Shield. Anda dapat menggunakan AWS Firewall Manager untuk mengonfigurasi opsi ini dalam skala besar.
- Jika Anda memiliki beberapa sumber daya dalam aliran data, seperti CloudFront distribusi di depan Application Load Balancer, gunakan hanya sumber daya entry-point sebagai sumber daya yang dilindungi. Ini akan memastikan bahwa Anda tidak membayar biaya Shield Data Transfer Out (DTO) dua kali untuk dua sumber daya.
- Shield Advanced merekam metrik yang dapat Anda pantau di Amazon CloudWatch. (Untuk informasi selengkapnya, lihat Memantau dengan Amazon CloudWatch di AWS dokumentasi.) Siapkan CloudWatch alarm untuk menerima pemberitahuan SNS ke pusat keamanan Anda saat peristiwa DDo S terdeteksi. Dalam peristiwa DDo S yang dicurigai, hubungi tim AWS Enterprise Support dengan mengajukan tiket dukungan dan menetapkannya sebagai prioritas tertinggi. Tim Enterprise Support akan menyertakan Shield Response Team (SRT) saat menangani acara. Selain itu, Anda dapat mengkonfigurasi ulang fungsi Lambda AWS Shield keterlibatan untuk membuat tiket dukungan dan mengirim email ke tim SRT.

AWS Certificate Manager (ACM)

AWS Certificate Manager(ACM) memungkinkan Anda menyediakan, mengelola, dan menyebarkan sertifikat TLS publik dan pribadi untuk digunakan dengan Layanan AWS dan sumber daya internal Anda yang terhubung. Dengan ACM, Anda dapat meminta sertifikat dengan cepat, menerapkannya pada AWS sumber daya yang terintegrasi dengan ACM, seperti penyeimbang beban Elastic Load Balancing, distribusi, CloudFront dan di Amazon APIs API Gateway, dan membiarkan ACM menangani perpanjangan sertifikat. Saat Anda meminta sertifikat publik ACM, Anda tidak perlu membuat key pair atau permintaan penandatanganan sertifikat (CSR), mengirimkan CSR ke otoritas sertifikat (CA), atau mengunggah dan menginstal sertifikat saat diterima. ACM juga menyediakan opsi untuk mengimpor sertifikat TLS yang dikeluarkan oleh pihak ketiga CAs dan menyebarkannya dengan layanan terintegrasi ACM. Saat Anda menggunakan ACM untuk mengelola sertifikat, kunci privat sertifikat dilindungi dan disimpan dengan aman menggunakan enkripsi yang kuat dan praktik terbaik manajemen kunci. Dengan ACM tidak ada biaya tambahan untuk penyediaan sertifikat publik, dan ACM mengelola proses perpanjangan.

ACM digunakan dalam akun Jaringan untuk menghasilkan sertifikat TLS publik, yang, pada gilirannya, digunakan oleh CloudFront distribusi untuk membuat koneksi HTTPS antara pemirsa dan. CloudFront Lihat informasi yang lebih lengkap dalam dokumentasi CloudFront .

> **Pertimbangan desain**
>
> Untuk sertifikat yang dihadapi secara eksternal, ACM harus berada di akun yang sama dengan sumber daya yang diberikannya sertifikat. Sertifikat tidak dapat dibagikan di seluruh akun.

Amazon Route 53

Amazon Route 53 adalah layanan web DNS yang sangat tersedia dan dapat diskalakan. Anda dapat menggunakan Route 53 untuk melakukan tiga fungsi utama: pendaftaran domain, perutean DNS, dan pemeriksaan kesehatan.

Anda dapat menggunakan Route 53 sebagai layanan DNS untuk memetakan nama domain ke EC2 instans, bucket S3, CloudFront distribusi, dan sumber daya lainnya. AWS Sifat terdistribusi dari server AWS DNS membantu memastikan bahwa pengguna akhir Anda diarahkan ke aplikasi Anda secara konsisten. Fitur seperti arus lalu lintas Route 53 dan kontrol perutean membantu Anda meningkatkan keandalan. Jika titik akhir aplikasi utama Anda tidak tersedia, Anda dapat

mengonfigurasi failover untuk mengalihkan pengguna ke lokasi alternatif. Route 53 Resolver menyediakan DNS rekursif untuk VPC dan jaringan lokal Anda melalui atau VPN terkelola. AWS Direct Connect AWS

Dengan menggunakan layanan IAM dengan Route 53, Anda mendapatkan kontrol halus atas siapa yang dapat memperbarui data DNS Anda. Anda dapat mengaktifkan penandatanganan DNS Security Extensions (DNSSEC) agar resolver DNS memvalidasi bahwa respons DNS berasal dari Route 53 dan belum dirusak.

Route 53 Resolver DNS Firewall memberikan perlindungan untuk permintaan DNS keluar dari Anda. VPCs Permintaan ini melalui Route 53 Resolver untuk resolusi nama domain. Penggunaan utama perlindungan DNS Firewall adalah untuk membantu mencegah eksfiltrasi DNS data Anda. Dengan DNS Firewall, Anda dapat memantau dan mengontrol domain yang dapat dimintai oleh aplikasi Anda. Anda dapat menolak akses ke domain yang Anda tahu buruk, dan mengizinkan semua pertanyaan lain melewatinya. Sebagai alternatif, Anda dapat menolak akses ke semua domain kecuali domain yang Anda percayai secara eksplisit. Anda juga dapat menggunakan DNS Firewall untuk memblokir permintaan resolusi ke sumber daya di zona host pribadi (bersama atau lokal), termasuk nama titik akhir VPC. Hal ini juga dapat memblokir permintaan untuk nama EC2 instans publik atau pribadi.

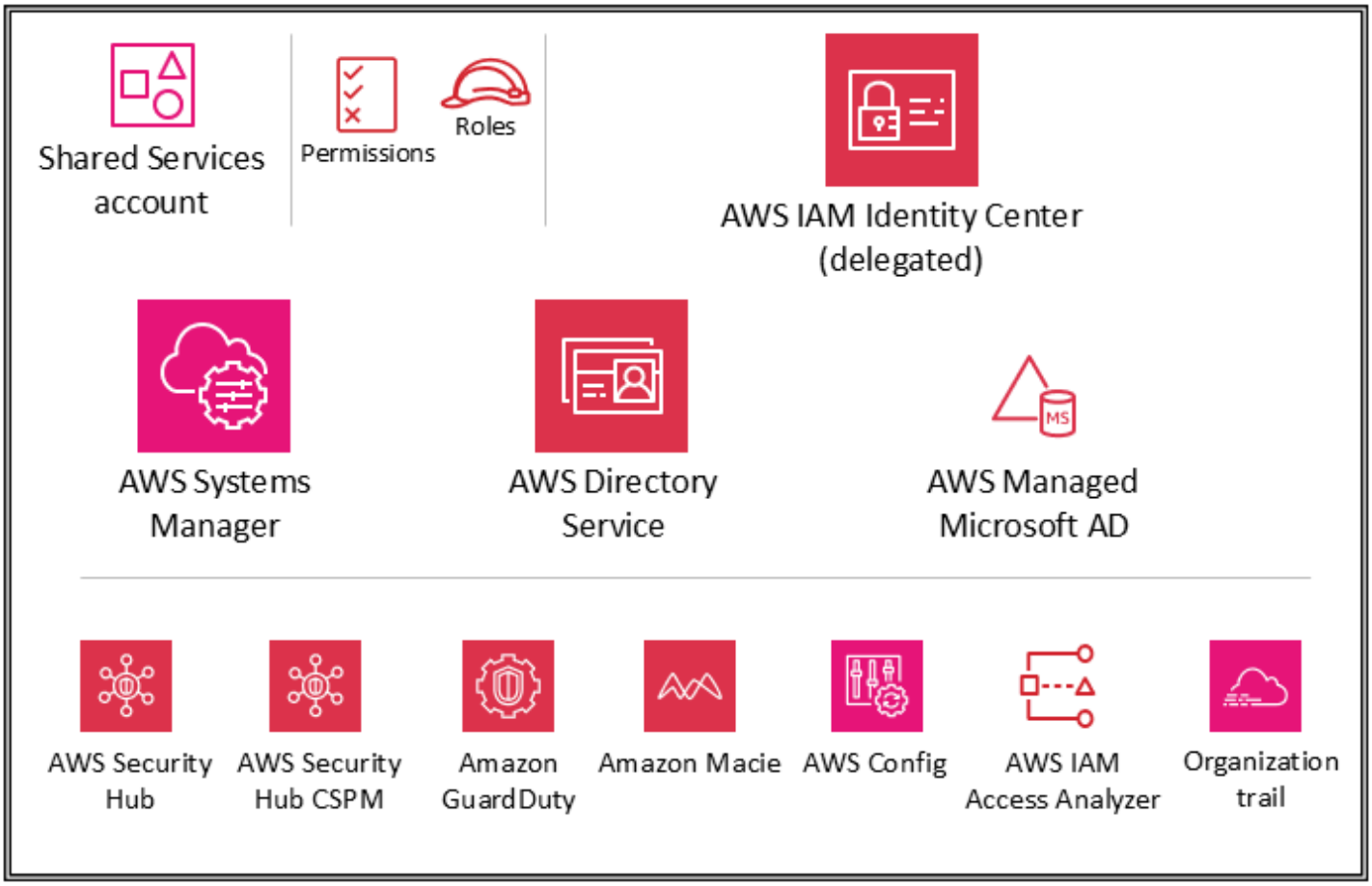
Resolver Route 53 dibuat secara default sebagai bagian dari setiap VPC. Dalam AWS SRA, Route 53 digunakan dalam akun Jaringan terutama untuk kemampuan DNS Firewall.

> **Pertimbangan desain**
>
> DNS Firewall dan AWS Network Firewall keduanya menawarkan pemfilteran nama domain, tetapi untuk berbagai jenis lalu lintas. Anda dapat menggunakan DNS Firewall dan Network Firewall bersama-sama untuk mengonfigurasi pemfilteran berbasis domain untuk lalu lintas lapisan aplikasi melalui dua jalur jaringan yang berbeda:
>
> - DNS Firewall menyediakan pemfilteran untuk kueri DNS keluar yang melewati Resolver Route 53 dari aplikasi di dalam Anda. VPCs Anda juga dapat mengonfigurasi DNS Firewall untuk mengirim respons kustom untuk permintaan ke nama domain yang diblokir.
> - Network Firewall menyediakan pemfilteran untuk lalu lintas lapisan jaringan dan lapisan aplikasi, tetapi tidak memiliki visibilitas ke dalam kueri yang dibuat oleh Route 53 Resolver.

Infrastruktur OU - Akun Layanan Bersama

Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

Diagram berikut menggambarkan layanan AWS keamanan yang dikonfigurasi di akun Layanan Bersama.



Akun Layanan Bersama adalah bagian dari Infrastruktur OU, dan tujuannya adalah untuk mendukung layanan yang digunakan beberapa aplikasi dan tim untuk memberikan hasil mereka. Misalnya, layanan direktori (Active Directory), layanan pesan, dan layanan metadata berada dalam kategori ini. AWS SRA menyoroti layanan bersama yang mendukung kontrol keamanan. Meskipun akun Jaringan juga merupakan bagian dari Infrastruktur OU, mereka dihapus dari akun Layanan Bersama untuk mendukung pemisahan tugas. Tim yang akan mengelola layanan ini tidak memerlukan izin atau akses ke akun Jaringan.

AWS Systems Manager

AWS Systems Manager(yang juga termasuk dalam akun Manajemen Org dan di akun Aplikasi) menyediakan kumpulan kemampuan yang memungkinkan visibilitas dan kontrol AWS sumber daya Anda. Salah satu kemampuan ini, Systems Manager Explorer, adalah dasbor operasi yang dapat disesuaikan yang melaporkan informasi tentang sumber daya Anda AWS . Anda dapat menyinkronkan data operasi di semua akun di AWS organisasi Anda dengan menggunakan AWS Organizations dan Systems Manager Explorer. Systems Manager digunakan di akun Shared Services melalui fungsionalitas administrator yang didelegasikan di. AWS Organizations

Systems Manager membantu Anda bekerja untuk menjaga keamanan dan kepatuhan dengan memindai instans dan pelaporan terkelola Anda (atau mengambil tindakan korektif) pada setiap pelanggaran kebijakan yang terdeteksi. Dengan memasangkan Systems Manager dengan penerapan yang sesuai di masing-masing anggota Akun AWS (misalnya, akun Aplikasi), Anda dapat mengoordinasikan pengumpulan data inventaris instans dan memusatkan otomatisasi seperti patch dan pembaruan keamanan.

AWS Managed Microsoft AD

AWS Directory Service for Microsoft Active Directory, juga dikenal sebagai AWS Managed Microsoft AD, memungkinkan beban kerja dan AWS sumber daya yang sadar direktori Anda untuk menggunakan Direktori Aktif terkelola. AWS Anda dapat menggunakan AWS Managed Microsoft AD untuk bergabung dengan Amazon EC2 untuk Windows Server, Amazon EC2 untuk Linux, dan Amazon RDS for SQL Server instance ke domain Anda, dan AWS menggunakan layanan komputasi pengguna akhir (EUC), seperti WorkSpacesAmazon, dengan pengguna dan grup Active Directory.

AWS Managed Microsoft AD membantu Anda memperluas Direktori Aktif yang ada ke AWS dan menggunakan kredensyal pengguna lokal yang ada untuk mengakses sumber daya cloud. Anda juga dapat mengelola pengguna, grup, aplikasi, dan sistem lokal tanpa kerumitan menjalankan dan memelihara Active Directory lokal yang sangat tersedia. Anda dapat bergabung dengan komputer, laptop, dan printer yang ada ke AWS Managed Microsoft AD domain.

AWS Managed Microsoft AD dibangun di Microsoft Active Directory dan tidak mengharuskan Anda untuk menyinkronkan atau mereplikasi data dari Active Directory yang ada ke cloud. Anda dapat menggunakan alat dan fitur administrasi Direktori Aktif yang sudah dikenal, seperti Objek Kebijakan Grup (GPOs), kepercayaan domain, kebijakan kata sandi berbutir halus, grup Akun Layanan Terkelola (gMSAs), ekstensi skema, dan sistem masuk tunggal berbasis Kerberos. Anda juga dapat mendelegasikan tugas administratif dan mengotorisasi akses menggunakan grup keamanan Active Directory.

Replikasi Multi-Region memungkinkan Anda untuk menyebarkan dan menggunakan satu AWS Managed Microsoft AD direktori di beberapa. Wilayah AWS Ini membuatnya lebih mudah dan lebih hemat biaya bagi Anda untuk menyebarkan dan mengelola beban kerja Microsoft Windows dan Linux Anda secara global. Saat Anda menggunakan kemampuan replikasi Multi-wilayah otomatis, Anda mendapatkan ketahanan yang lebih tinggi saat aplikasi Anda menggunakan direktori lokal untuk kinerja yang optimal.

AWS Managed Microsoft AD mendukung Lightweight Directory Access Protocol (LDAP) melalui SSL/TLS, juga dikenal sebagai LDAPS, baik dalam peran klien dan server. Saat bertindak sebagai server, AWS Managed Microsoft AD mendukung LDAPS melalui port 636 (SSL) dan 389 (TLS). Anda mengaktifkan komunikasi LDAPS sisi server dengan memasang sertifikat pada pengontrol AWS Managed Microsoft AD domain Anda dari otoritas sertifikat Active Directory Certificate Services (AD CS) AWS berbasis (CA). Saat bertindak sebagai klien, AWS Managed Microsoft AD mendukung LDAPS melalui port 636 (SSL). Anda dapat mengaktifkan komunikasi LDAPS sisi klien dengan mendaftarkan sertifikat CA dari penerbit sertifikat server Anda AWS, lalu mengaktifkan LDAPS di direktori Anda.

Di AWS SRA, Directory Service digunakan dalam akun Layanan Bersama untuk menyediakan layanan domain untuk beban kerja yang sadar Microsoft di beberapa akun anggota. AWS

> **Pertimbangan desain**
>
> Anda dapat memberikan akses kepada pengguna Active Directory lokal untuk masuk ke Konsol Manajemen AWS dan AWS Command Line Interface (AWS CLI) dengan kredensyal Active Directory yang ada dengan menggunakan IAM Identity Center dan memilih AWS Managed Microsoft AD sebagai sumber identitas. Hal ini memungkinkan pengguna Anda untuk mengambil salah satu peran yang ditetapkan saat login, dan untuk mengakses dan mengambil tindakan pada sumber daya sesuai dengan izin yang ditentukan untuk peran tersebut. Opsi alternatif adalah menggunakan AWS Managed Microsoft AD untuk memungkinkan pengguna Anda mengambil peran IAM.

Pusat Identitas IAM

AWS SRA menggunakan fitur administrator yang didelegasikan yang didukung oleh AWS IAM Identity Center untuk mendelegasikan sebagian besar administrasi Pusat Identitas IAM ke akun Layanan Bersama. Ini membantu membatasi jumlah pengguna yang memerlukan akses ke akun Manajemen Org. Pusat Identitas IAM masih perlu diaktifkan di akun Manajemen Org untuk

melakukan tugas-tugas tertentu, termasuk pengelolaan set izin yang disediakan dalam akun Manajemen Org.

Alasan utama untuk menggunakan akun Layanan Bersama sebagai administrator yang didelegasikan untuk Pusat Identitas IAM adalah lokasi Direktori Aktif. Jika Anda berencana untuk menggunakan Active Directory sebagai sumber identitas Pusat Identitas IAM Anda, Anda harus menemukan direktori di akun anggota yang telah Anda tetapkan sebagai akun administrator yang didelegasikan IAM Identity Center Anda. Di AWS SRA, akun Layanan Bersama dihosting AWS Managed Microsoft AD, sehingga akun tersebut dijadikan administrator yang didelegasikan untuk IAM Identity Center.

IAM Identity Center mendukung pendaftaran akun anggota tunggal sebagai administrator yang didelegasikan pada satu waktu. Anda dapat mendaftarkan akun anggota hanya ketika Anda masuk dengan kredensyal dari akun manajemen. Untuk mengaktifkan delegasi, Anda harus mempertimbangkan prasyarat yang tercantum dalam dokumentasi IAM Identity Center. Akun administrator yang didelegasikan dapat melakukan sebagian besar tugas manajemen Pusat Identitas IAM, tetapi dengan beberapa batasan, yang tercantum dalam dokumentasi Pusat Identitas IAM. Akses ke akun administrator yang didelegasikan untuk IAM Identity Center harus dikontrol dengan ketat.

Pertimbangan desain

- Jika Anda memutuskan untuk mengubah sumber identitas IAM Identity Center dari sumber lain ke Active Directory, atau mengubahnya dari Active Directory ke sumber lain, direktori harus berada di (dimiliki oleh) akun anggota administrator yang didelegasikan IAM Identity Center, jika ada; jika tidak, itu harus berada di akun manajemen.
- Anda dapat meng-host Anda AWS Managed Microsoft AD dalam VPC khusus di akun yang berbeda dan kemudian menggunakan AWS Resource Access Manager (AWS RAM) untuk berbagi subnet dari akun lain ini ke akun administrator yang didelegasikan. Dengan begitu, AWS Managed Microsoft AD instance dikontrol di akun administrator yang didelegasikan, tetapi dari perspektif jaringan ia bertindak seolah-olah digunakan di VPC akun lain. Ini sangat membantu ketika Anda memiliki beberapa AWS Managed Microsoft AD instance dan Anda ingin menerapkannya secara lokal ke tempat beban kerja Anda berjalan tetapi mengelolanya secara terpusat melalui satu akun.
- Jika Anda memiliki tim identitas khusus yang melakukan aktivitas manajemen identitas dan akses reguler atau memiliki persyaratan keamanan yang ketat untuk memisahkan fungsi manajemen identitas dari fungsi layanan bersama lainnya, Anda dapat meng-host yang didedikasikan Akun AWS untuk manajemen identitas. Dalam skenario ini, Anda

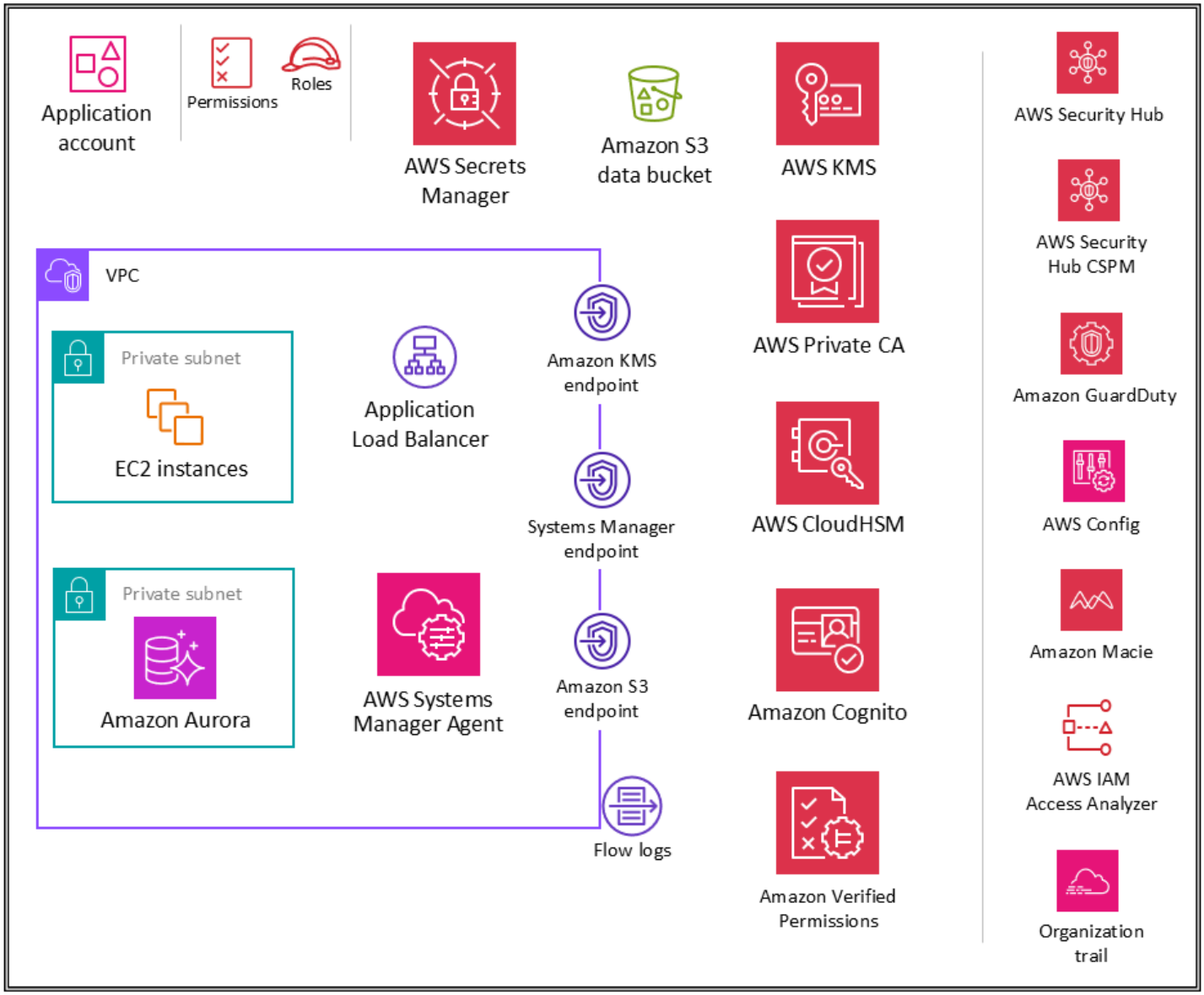
menetapkan akun ini sebagai administrator yang didelegasikan untuk IAM Identity Center, dan juga meng-host direktori Anda. AWS Managed Microsoft AD Anda dapat mencapai tingkat isolasi logis yang sama antara beban kerja manajemen identitas dan beban kerja layanan bersama lainnya dengan menggunakan izin IAM berbutir halus dalam satu akun layanan bersama.

- Pusat Identitas IAM saat ini tidak menyediakan dukungan Multi-wilayah. (Untuk mengaktifkan Pusat Identitas IAM di Wilayah yang berbeda, Anda harus terlebih dahulu menghapus konfigurasi Pusat Identitas IAM Anda saat ini.) Selain itu, ini tidak mendukung penggunaan sumber identitas yang berbeda untuk kumpulan akun yang berbeda atau memungkinkan Anda mendelegasikan manajemen izin ke berbagai bagian organisasi Anda (yaitu, beberapa administrator yang didelegasikan) atau ke grup administrator yang berbeda. Jika Anda memerlukan salah satu fitur ini, Anda dapat menggunakan federasi IAM untuk mengelola identitas pengguna Anda dalam penyedia identitas (iDP) di luar AWS dan memberikan izin identitas pengguna eksternal ini untuk menggunakan AWS sumber daya di akun Anda. Dukungan IAM IdPs yang kompatibel dengan OpenID Connect (OIDC) atau SAMP 2.0. Sebagai praktik terbaik, gunakan federasi SAMP 2.0 dengan penyedia identitas pihak ketiga seperti Active Directory Federation Service (AD FS), Okta, Azure Active Directory (Azure AD), atau Ping Identity untuk memberikan kemampuan masuk tunggal bagi pengguna untuk masuk ke atau memanggil operasi API. Konsol Manajemen AWS AWS Untuk informasi lebih lanjut tentang federasi IAM dan penyedia identitas, lihat Tentang federasi berbasis SAMP 2.0 dalam dokumentasi IAM.

Beban Kerja OU - Akun aplikasi

Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

Diagram berikut menggambarkan layanan AWS keamanan yang dikonfigurasi di akun Aplikasi (bersama dengan aplikasi itu sendiri).



Akun Aplikasi menghosting infrastruktur dan layanan utama untuk menjalankan dan memelihara aplikasi perusahaan. Akun Aplikasi dan Beban Kerja OU melayani beberapa tujuan keamanan utama. Pertama, Anda membuat akun terpisah untuk setiap aplikasi untuk memberikan batasan dan kontrol antar beban kerja sehingga Anda dapat menghindari masalah peran, izin, data, dan kunci enkripsi yang akan datang. Anda ingin menyediakan wadah akun terpisah di mana tim aplikasi dapat diberikan hak luas untuk mengelola infrastruktur mereka sendiri tanpa mempengaruhi orang lain. Selanjutnya, Anda menambahkan lapisan perlindungan dengan menyediakan mekanisme bagi tim operasi keamanan untuk memantau dan mengumpulkan data keamanan. Mempekerjakan jejak organisasi dan penyebaran lokal layanan keamanan akun (Amazon GuardDuty,,, AWS Security Hub CSPM Amazon AWS Config, IAM Access Analyzer) EventBridge, yang dikonfigurasi dan dipantau oleh tim keamanan. Terakhir, Anda memungkinkan perusahaan Anda untuk mengatur kontrol

secara terpusat. Anda menyelaraskan akun aplikasi ke struktur keamanan yang lebih luas dengan menjadikannya anggota Workloads OU yang melaluinya mewarisi izin layanan, kendala, dan pagar pembatas yang sesuai.

> **Pertimbangan desain**
>
> Di organisasi Anda, Anda cenderung memiliki lebih dari satu aplikasi bisnis. Beban Kerja OU dimaksudkan untuk menampung sebagian besar beban kerja spesifik bisnis Anda, termasuk lingkungan produksi dan non-produksi. Beban kerja ini dapat berupa campuran aplikasi komersial off-the-shelf (COTS) dan aplikasi kustom dan layanan data Anda sendiri yang dikembangkan secara internal. Ada beberapa pola untuk mengatur aplikasi bisnis yang berbeda bersama dengan lingkungan pengembangannya. Salah satu pola adalah memiliki banyak anak OUs berdasarkan lingkungan perkembangan Anda, seperti produksi, pementasan, tes, dan pengembangan, dan menggunakan anak terpisah Akun AWS di bawah OUs yang berkaitan dengan aplikasi yang berbeda. Pola umum lainnya adalah memiliki anak terpisah OUs per aplikasi dan kemudian menggunakan anak terpisah Akun AWS untuk lingkungan perkembangan individu. Struktur OU dan akun yang tepat tergantung pada desain aplikasi Anda dan tim yang mengelola aplikasi tersebut. Pertimbangkan kontrol keamanan yang ingin Anda terapkan, apakah itu khusus lingkungan atau khusus aplikasi, karena lebih mudah untuk menerapkan kontrol tersebut seperti pada. SCPs OUs Untuk pertimbangan lebih lanjut tentang mengatur berorientasi beban kerja OUs, lihat OUs bagian Aplikasi pada AWS whitepaper Mengatur lingkungan Anda menggunakan beberapa akun. AWS

Aplikasi VPC

Virtual private cloud (VPC) di akun Aplikasi membutuhkan akses masuk (untuk layanan web sederhana yang Anda modelkan) dan akses keluar (untuk kebutuhan atau kebutuhan aplikasi). Layanan AWS Secara default, sumber daya di dalam VPC dapat dirutekan satu sama lain. Ada dua subnet pribadi: satu untuk meng-host EC2 instance (lapisan aplikasi) dan yang lainnya untuk Amazon Aurora (lapisan basis data). Segmentasi jaringan antara tingkatan yang berbeda, seperti tingkat aplikasi dan tingkat basis data, dilakukan melalui grup keamanan VPC, yang membatasi lalu lintas di tingkat instans. Untuk ketahanan, beban kerja mencakup dua atau lebih Availability Zone dan menggunakan dua subnet per zona.

Pertimbangan desain

Anda dapat menggunakan Traffic Mirroring untuk menyalin lalu lintas jaringan dari elastic network interface EC2 instance. Anda kemudian dapat mengirim lalu lintas ke peralatan out-of-band keamanan dan pemantauan untuk pemeriksaan konten, pemantauan ancaman, atau pemecahan masalah. Misalnya, Anda mungkin ingin memantau lalu lintas yang meninggalkan VPC Anda atau lalu lintas yang sumbernya berada di luar VPC Anda. Dalam hal ini, Anda akan mencerminkan semua lalu lintas kecuali lalu lintas yang lewat dalam VPC Anda dan mengirimkannya ke satu alat pemantauan. Log aliran VPC Amazon tidak menangkap lalu lintas cermin; mereka umumnya menangkap informasi dari header paket saja. Traffic Mirroring memberikan wawasan yang lebih dalam tentang lalu lintas jaringan dengan memungkinkan Anda menganalisis konten lalu lintas aktual, termasuk payload. Aktifkan Pencerminan Lalu Lintas hanya untuk antarmuka elastis network EC2 instance yang mungkin beroperasi sebagai bagian dari beban kerja sensitif atau yang Anda harapkan memerlukan diagnostik terperinci jika terjadi masalah.

Titik akhir VPC

Titik akhir VPC menyediakan lapisan kontrol keamanan lain serta skalabilitas dan keandalan. Gunakan ini untuk menghubungkan VPC aplikasi Anda ke yang lain. Layanan AWS(Di akun Aplikasi, AWS SRA menggunakan titik akhir VPC untuk,, AWS KMS dan AWS Systems Manager Amazon S3.) Endpoint adalah perangkat virtual. Mereka merupakan komponen VPC skala horizontal, redundan, dan sangat tersedia. Mereka memungkinkan komunikasi antara instance di VPC dan layanan Anda tanpa memaksakan risiko ketersediaan atau kendala bandwidth pada lalu lintas jaringan Anda. Anda dapat menggunakan titik akhir VPC untuk menghubungkan VPC Anda secara pribadi ke layanan endpoint yang didukung Layanan AWS dan VPC yang AWS PrivateLink didukung tanpa memerlukan gateway internet, perangkat NAT, koneksi VPN, atau koneksi. AWS Direct Connect Instans di VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi dengan orang lain. Layanan AWS Lalu lintas antara VPC Anda dan yang lainnya Layanan AWS tidak meninggalkan jaringan Amazon.

Manfaat lain menggunakan titik akhir VPC adalah mengaktifkan konfigurasi kebijakan titik akhir. Kebijakan titik akhir VPC adalah kebijakan sumber daya IAM yang Anda lampirkan ke titik akhir ketika membuat atau mengubah titik akhir. Jika Anda tidak melampirkan kebijakan IAM saat membuat titik akhir, AWS melampirkan kebijakan IAM default untuk Anda yang memungkinkan akses penuh ke layanan. Kebijakan endpoint tidak mengesampingkan atau mengganti kebijakan pengguna IAM atau kebijakan khusus layanan (seperti kebijakan bucket S3). Ini adalah kebijakan IAM terpisah untuk

mengontrol akses dari titik akhir ke layanan yang ditentukan. Dengan cara ini, ia menambahkan lapisan kontrol lain di mana AWS prinsipal dapat berkomunikasi dengan sumber daya atau layanan.

Amazon EC2

EC2Instans Amazon yang menyusun aplikasi kami menggunakan versi 2 dari Layanan Metadata Instans (). IMDSv2 IMDSv2 menambahkan perlindungan untuk empat jenis kerentanan yang dapat digunakan untuk mencoba mengakses IMDS: firewall aplikasi situs web, proxy terbalik terbuka, kerentanan pemalsuan permintaan sisi server (SSRF), firewall lapisan 3 terbuka, dan. NATs Untuk informasi selengkapnya, lihat posting blog Tambahkan pertahanan secara mendalam terhadap firewall terbuka, proxy terbalik, dan kerentanan SSRF dengan penyempurnaan pada Layanan Metadata Instans. EC2

Gunakan terpisah VPCs (sebagai bagian dari batas akun) untuk mengisolasi infrastruktur berdasarkan segmen beban kerja. Gunakan subnet untuk melakukan isolasi terhadap jenjang-jenjang aplikasi Anda (misalnya web, aplikasi, dan basis data) dalam satu VPC. Gunakan subnet privat untuk instans Anda jika instan tersebut tidak dapat diakses secara langsung dari internet. Untuk memanggil Amazon EC2 API dari subnet pribadi Anda tanpa menggunakan gateway internet, gunakan AWS PrivateLink. Batasi akses ke instans Anda dengan menggunakan grup keamanan. Gunakan VPC Flow Logs untuk memantau lalu lintas yang mencapai instans Anda. Gunakan Session Manager, kemampuan AWS Systems Manager, untuk mengakses instans Anda dari jarak jauh alih-alih membuka port SSH masuk dan mengelola kunci SSH. Gunakan volume Amazon Elastic Block Store (Amazon EBS) terpisah untuk sistem operasi dan data Anda. Anda dapat mengonfigurasi Akun AWS untuk menerapkan enkripsi volume EBS baru dan salinan snapshot yang Anda buat.

> **Contoh implementasi**
>
> Pustaka kode AWS SRA menyediakan contoh implementasi enkripsi Amazon EBS default di Amazon. EC2 Ini menunjukkan bagaimana Anda dapat mengaktifkan enkripsi Amazon EBS default tingkat akun dalam masing-masing Akun AWS dan AWS Region di organisasi. AWS

AWS Enklaf Nitro

AWS Nitro Enclave adalah EC2 fitur Amazon yang memungkinkan Anda membuat lingkungan eksekusi terisolasi, yang disebut kantong, dari instance. EC2 Enklave adalah mesin virtual yang terpisah, mengeras, dan sangat dibatasi. CPU dan memori dari EC2 instance induk tunggal dipartisi menjadi kantong terisolasi. Setiap enclave menjalankan kernel independen. Enklave hanya

menyediakan konektivitas soket lokal yang aman dengan instance induknya. Mereka tidak memiliki penyimpanan persisten, akses interaktif, atau jaringan eksternal. Pengguna tidak dapat SSH ke dalam enclave, dan data dan aplikasi di dalam enclave tidak dapat diakses oleh proses, aplikasi, atau pengguna (root atau administrator) dari instance induk. Anda dapat mengamankan data Anda yang paling sensitif, seperti informasi identitas pribadi (PII), layanan kesehatan, keuangan, dan data kekayaan intelektual, dalam beberapa kasus. EC2 Nitro Enclave memungkinkan Anda untuk fokus pada aplikasi Anda alih-alih mengkhawatirkan integrasi dengan layanan eksternal. Nitro Enclave mencakup pengesahan kriptografi untuk perangkat lunak Anda sehingga Anda dapat yakin bahwa hanya kode resmi yang berjalan, dan integrasi dengan AWS KMS sehingga hanya kantong Anda yang dapat mengakses materi sensitif. Ini membantu mengurangi area permukaan serangan untuk aplikasi pemrosesan data Anda yang paling sensitif. Tidak ada biaya tambahan untuk menggunakan Nitro Enclave.

Pengesahan kriptografi adalah proses yang digunakan untuk membuktikan identitas sebuah kantong. Proses pengesahan dilakukan melalui Nitro Hypervisor, yang menghasilkan dokumen pengesahan yang ditandatangani untuk kantong untuk membuktikan identitasnya kepada pihak ketiga atau layanan lain. Dokumen pengesahan berisi rincian kunci enklave seperti kunci publik enklave, hash gambar dan aplikasi enclave, dan banyak lagi.

Dengan AWS Certificate Manager (ACM) untuk Nitro Enclave, Anda dapat menggunakan sertifikat publik dan pribadi. SSL/TLS certificates with your web applications and web servers running on EC2 instances with Nitro Enclaves. SSL/TLS certificates are used to secure network communications and to establish the identity of websites over the internet and resources on private networks. ACM for Nitro Enclaves removes the time-consuming and error-prone manual process of purchasing, uploading, and renewing SSL/TLS ACM untuk Nitro Enclave membuat kunci pribadi yang aman, mendistribusikan sertifikat dan kunci pribadinya ke kantong Anda, dan mengelola perpanjangan sertifikat. Dengan ACM untuk Nitro Enclave, kunci pribadi sertifikat tetap terisolasi di enklave, yang mencegah instance dan penggunanya mengaksesnya. Untuk informasi lebih lanjut, lihat AWS Certificate Manager untuk Nitro Enclave dalam dokumentasi Nitro Enclave.

Application Load Balancer

Application Load Balancer mendistribusikan lalu lintas aplikasi yang masuk di beberapa target, seperti EC2 instance, di beberapa Availability Zone. Dalam AWS SRA, kelompok target untuk penyeimbang beban adalah instance aplikasi EC2 . AWS SRA menggunakan pendengar HTTPS untuk memastikan bahwa saluran komunikasi dienkripsi. Application Load Balancer menggunakan sertifikat server untuk mengakhiri koneksi front-end, dan kemudian mendekripsi permintaan dari klien sebelum mengirimnya ke target.

AWS Certificate Manager (ACM) terintegrasi secara native dengan Application Load Balancers, dan AWS SRA menggunakan ACM untuk menghasilkan dan mengelola sertifikat publik X.509 (server TLS) yang diperlukan. Anda dapat menerapkan TLS 1.2 dan cipher yang kuat untuk koneksi front-end melalui kebijakan keamanan Application Load Balancer. Untuk informasi lebih lanjut, lihat Dokumentasi Penyeimbangan Beban Elastis.

Pertimbangan desain

- Untuk skenario umum seperti aplikasi internal ketat yang memerlukan sertifikat TLS pribadi pada Application Load Balancer, Anda dapat menggunakan ACM dalam akun ini untuk menghasilkan sertifikat pribadi dari. AWS Private CADi AWS SRA, ACM root private CA dihosting di akun Security Tooling dan dapat dibagikan dengan seluruh AWS organisasi atau dengan khusus Akun AWS untuk mengeluarkan sertifikat entitas akhir, seperti yang dijelaskan sebelumnya di bagian akun Security Tooling.
- Untuk sertifikat publik, Anda dapat menggunakan ACM untuk menghasilkan sertifikat tersebut dan mengelolanya, termasuk rotasi otomatis. Atau, Anda dapat membuat sertifikat Anda sendiri dengan menggunakan SSL/TLS alat untuk membuat permintaan penandatanganan sertifikat (CSR), mendapatkan CSR yang ditandatangani oleh otoritas sertifikat (CA) untuk menghasilkan sertifikat, dan kemudian mengimpor sertifikat ke ACM atau mengunggah sertifikat ke IAM untuk digunakan dengan Application Load Balancer. Jika Anda mengimpor sertifikat ke ACM, Anda harus memantau tanggal kedaluwarsa sertifikat dan memperbaruinya sebelum kedaluwarsa.
- Untuk lapisan pertahanan tambahan, Anda dapat menerapkan AWS WAF kebijakan untuk melindungi Application Load Balancer. Memiliki kebijakan tepi, kebijakan aplikasi, dan bahkan lapisan penegakan kebijakan pribadi atau internal menambah visibilitas permintaan komunikasi dan menyediakan penegakan kebijakan terpadu. Untuk informasi lebih lanjut, lihat posting blog Menyebarkan pertahanan secara mendalam menggunakan Peraturan yang Dikelola AWS for AWS WAF.

AWS Private CA

AWS Private Certificate Authority(AWS Private CA) digunakan dalam akun Aplikasi untuk menghasilkan sertifikat pribadi yang akan digunakan dengan Application Load Balancer. Ini adalah skenario umum untuk Application Load Balancers untuk menyajikan konten aman melalui TLS. Ini

membutuhkan sertifikat TLS untuk diinstal pada Application Load Balancer. Untuk aplikasi yang benar-benar internal, sertifikat TLS pribadi dapat menyediakan saluran aman.

Di AWS SRA, AWS Private CA di-host di akun Security Tooling dan dibagikan ke akun Aplikasi dengan menggunakan. AWS RAM Hal ini memungkinkan pengembang di akun Aplikasi untuk meminta sertifikat dari CA pribadi bersama. Berbagi CAs di seluruh organisasi Anda atau di seluruh Akun AWS membantu mengurangi biaya dan kompleksitas membuat dan mengelola duplikat CAs di semua bisnis Anda Akun AWS. Saat Anda menggunakan ACM untuk menerbitkan sertifikat pribadi dari CA bersama, sertifikat dibuat secara lokal di akun yang meminta, dan ACM menyediakan manajemen dan perpanjangan siklus hidup penuh.

Amazon Inspector

AWS SRA menggunakan Amazon Inspector untuk secara otomatis menemukan dan EC2 memindai instance dan gambar kontainer yang berada di Amazon Elastic Container Registry (Amazon ECR) untuk mencari kerentanan perangkat lunak dan paparan jaringan yang tidak diinginkan.

Amazon Inspector ditempatkan di akun Aplikasi, karena menyediakan layanan manajemen kerentanan untuk EC2 instance di akun ini. Selain itu, Amazon Inspector melaporkan jalur jaringan yang tidak diinginkan ke dan dari EC2 instance.

Amazon Inspector di akun anggota dikelola secara terpusat oleh akun administrator yang didelegasikan. Di AWS SRA, akun Security Tooling adalah akun administrator yang didelegasikan. Akun administrator yang didelegasikan dapat mengelola data temuan dan pengaturan tertentu untuk anggota organisasi. Ini termasuk melihat rincian temuan agregat untuk semua akun anggota, mengaktifkan atau menonaktifkan pemindaian untuk akun anggota, dan meninjau sumber daya yang dipindai dalam organisasi. AWS

> **Pertimbangan desain**
>
> Anda dapat menggunakan Patch Manager, kemampuan AWS Systems Manager, untuk memicu patching sesuai permintaan guna memulihkan Amazon Inspector zero-day atau kerentanan keamanan kritis lainnya. Patch Manager membantu Anda menambal kerentanan tersebut tanpa harus menunggu jadwal patching normal Anda. Remediasi dilakukan dengan menggunakan runbook Systems Manager Automation. Untuk informasi selengkapnya, lihat seri blog dua bagian Mengotomatiskan manajemen kerentanan dan remediasi dalam menggunakan Amazon AWS Inspector dan. AWS Systems Manager

AWS Systems Manager

AWS Systems Manageradalah Layanan AWS yang dapat Anda gunakan untuk melihat data operasional dari beberapa Layanan AWS dan mengotomatiskan tugas operasional di seluruh AWS sumber daya Anda. Dengan alur kerja dan runbook persetujuan otomatis, Anda dapat bekerja untuk mengurangi kesalahan manusia dan menyederhanakan tugas pemeliharaan dan penerapan pada sumber daya. AWS

Selain kemampuan otomatisasi umum ini, Systems Manager mendukung sejumlah fitur keamanan preventif, detektif, dan responsif. AWS Systems Manager Agen (Agen SSM) adalah perangkat lunak Amazon yang dapat diinstal dan dikonfigurasi pada EC2 instans, server lokal, atau mesin virtual (VM). SSM Agent memungkinkan Systems Manager untuk memperbarui, mengelola, dan mengonfigurasi sumber daya ini. Systems Manager membantu Anda menjaga keamanan dan kepatuhan dengan memindai instans dan pelaporan terkelola ini (atau mengambil tindakan korektif) pada setiap pelanggaran yang terdeteksi dalam patch, konfigurasi, dan kebijakan kustom Anda.

AWS SRA menggunakan Session Manager, kemampuan Systems Manager, untuk memberikan pengalaman CLI dan shell berbasis browser yang interaktif. Ini menyediakan manajemen instans yang aman dan dapat diaudit tanpa perlu membuka port masuk, memelihara host bastion, atau mengelola kunci SSH. AWS SRA menggunakan Patch Manager, kemampuan Systems Manager, untuk menerapkan patch ke EC2 instance untuk sistem operasi dan aplikasi.

AWS SRA juga menggunakan Automation, kemampuan Systems Manager, untuk menyederhanakan tugas pemeliharaan dan penyebaran umum EC2 instans Amazon dan sumber daya lainnya. AWS Otomatisasi dapat menyederhanakan tugas-tugas TI umum seperti mengubah status satu atau lebih node (menggunakan otomatisasi persetujuan) dan mengelola status node sesuai dengan jadwal. Systems Manager menyertakan fitur yang membantu Anda menargetkan grup besar instance dengan menggunakan tag, dan kontrol kecepatan yang membantu Anda meluncurkan perubahan sesuai dengan batas yang Anda tentukan. Automation menawarkan otomatisasi sekali klik untuk menyederhanakan tugas-tugas kompleks seperti membuat Amazon Machine Images (AMIs) emas dan memulihkan instans yang tidak terjangkau. EC2 Selain itu, Anda dapat meningkatkan keamanan operasional dengan memberikan akses peran IAM ke runbook tertentu untuk menjalankan fungsi tertentu, tanpa secara langsung memberikan izin ke peran tersebut. Misalnya, jika Anda ingin peran IAM memiliki izin untuk memulai ulang EC2 instance tertentu setelah pembaruan tambalan, tetapi Anda tidak ingin memberikan izin langsung ke peran itu, Anda dapat membuat runbook Otomasi dan memberikan izin peran untuk hanya menjalankan runbook.

Pertimbangan desain

- Systems Manager mengandalkan metadata EC2 instance agar berfungsi dengan benar. Systems Manager dapat mengakses metadata instans dengan menggunakan versi 1 atau versi 2 dari Layanan Metadata Instance (dan). IMDSv1 IMDSv2
- Agen SSM harus berkomunikasi dengan berbagai Layanan AWS sumber daya seperti EC2 pesan Amazon, Systems Manager, dan Amazon S3. Agar komunikasi ini terjadi, subnet memerlukan konektivitas internet keluar atau penyediaan titik akhir VPC yang sesuai. AWS SRA menggunakan titik akhir VPC untuk Agen SSM untuk membuat jalur jaringan pribadi ke berbagai. Layanan AWS
- Dengan menggunakan otomatisasi, Anda dapat berbagi praktik terbaik dengan seluruh organisasi Anda. Anda dapat membuat praktik terbaik untuk pengelolaan sumber daya di runbook dan membagikan runbook di seluruh Wilayah AWS dan grup. Anda juga dapat membatasi nilai yang diizinkan untuk parameter runbook. Untuk kasus penggunaan ini, Anda mungkin harus membuat runbook Otomasi di akun pusat seperti Perkakas Keamanan atau Layanan Bersama dan membagikannya dengan organisasi lainnya. AWS Kasus penggunaan umum termasuk kemampuan untuk menerapkan patching dan pembaruan keamanan secara terpusat, memulihkan penyimpangan pada konfigurasi VPC atau kebijakan bucket S3, dan mengelola instance dalam skala besar. EC2 Untuk detail implementasi, lihat dokumentasi Systems Manager.

Amazon Aurora

Di AWS SRA, Amazon Aurora dan Amazon S3 membentuk tingkat data logis. Aurora adalah mesin basis data relasional yang dikelola sepenuhnya dan kompatibel dengan MySQL dan PostgreSQL. Aplikasi yang berjalan pada EC2 instance berkomunikasi dengan Aurora dan Amazon S3 sesuai kebutuhan. Aurora dikonfigurasi dengan cluster database di dalam grup subnet DB.

Pertimbangan desain

Seperti dalam banyak layanan database, keamanan untuk Aurora dikelola pada tiga tingkatan. Untuk mengontrol siapa yang dapat melakukan tindakan pengelolaan Amazon Relational Database Service (Amazon RDS) pada cluster DB Aurora dan instans DB, Anda menggunakan IAM. Untuk mengontrol perangkat dan EC2 instance mana yang dapat membuka koneksi ke titik akhir cluster dan port instans DB untuk cluster Aurora DB di VPC,

Anda menggunakan grup keamanan VPC. Untuk mengautentikasi login dan izin untuk cluster Aurora DB, Anda dapat mengambil pendekatan yang sama seperti dengan instance DB MySQL atau PostgreSQL yang berdiri sendiri, atau Anda dapat menggunakan otentikasi database IAM untuk Aurora MySQL Edisi yang kompatibel dengan MySQL. Dengan pendekatan terakhir ini, Anda mengautentikasi ke cluster DB yang kompatibel dengan Aurora MySQL Anda dengan menggunakan peran IAM dan token otentikasi.

Amazon S3

Amazon S3 adalah layanan penyimpanan objek yang menawarkan skalabilitas, ketersediaan data, keamanan, dan kinerja terdepan di industri. Ini adalah tulang punggung data dari banyak aplikasi yang dibangun AWS, dan izin serta kontrol keamanan yang sesuai sangat penting untuk melindungi data sensitif. Untuk praktik terbaik keamanan yang direkomendasikan untuk Amazon S3, lihat dokumentasi, pembicaraan teknologi online, dan penyelaman lebih dalam di posting blog. Praktik terbaik yang paling penting adalah memblokir akses yang terlalu permisif (terutama akses publik) ke bucket S3.

AWS KMS

AWS SRA menggambarkan model distribusi yang direkomendasikan untuk manajemen kunci, di mana AWS KMS key berada dalam Akun AWS sama dengan sumber daya yang akan dienkripsi. Untuk alasan ini, AWS KMS digunakan dalam akun Aplikasi selain dimasukkan dalam akun Perkakas Keamanan. Di akun Aplikasi, AWS KMS digunakan untuk mengelola kunci yang khusus untuk sumber daya aplikasi. Anda dapat menerapkan pemisahan tugas dengan menggunakan kebijakan utama untuk memberikan izin penggunaan kunci ke peran aplikasi lokal dan untuk membatasi izin pengelolaan dan pemantauan kepada kustodian utama Anda.

Pertimbangan desain

Dalam model terdistribusi, tanggung jawab manajemen AWS KMS kunci berada pada tim aplikasi. Namun, tim keamanan pusat Anda dapat bertanggung jawab atas tata kelola dan pemantauan peristiwa kriptografi penting seperti berikut ini:

- Materi kunci yang diimpor dalam kunci KMS mendekati tanggal kedaluwarsanya.
- Materi kunci dalam kunci KMS diputar secara otomatis.
- Kunci AKMS telah dihapus.

- Ada tingkat kegagalan dekripsi yang tinggi.

AWS CloudHSM

AWS CloudHSMmenyediakan modul keamanan perangkat keras terkelola (HSMs) di AWS Cloud. Ini memungkinkan Anda untuk menghasilkan dan menggunakan kunci enkripsi Anda sendiri AWS dengan menggunakan FIPS 140-2 level 3 yang divalidasi HSMs yang Anda kendalikan aksesnya. Anda dapat menggunakan AWS CloudHSM untuk membongkar SSL/TLS pemrosesan untuk server web Anda. Ini mengurangi beban pada server web dan memberikan keamanan ekstra dengan menyimpan kunci pribadi server web AWS CloudHSM. Anda juga dapat menyebarkan HSM dari VPC masuk AWS CloudHSM di akun Jaringan untuk menyimpan kunci pribadi Anda dan menandatangani permintaan sertifikat jika Anda perlu bertindak sebagai otoritas sertifikat penerbit.

Pertimbangan desain

Jika Anda memiliki persyaratan sulit untuk FIPS 140-2 level 3, Anda juga dapat memilih untuk mengonfigurasi AWS KMS untuk menggunakan AWS CloudHSM cluster sebagai penyimpanan kunci khusus daripada menggunakan toko kunci KMS asli. Dengan melakukan ini, Anda mendapat manfaat dari integrasi antara AWS KMS dan Layanan AWS yang mengenkripsi data Anda, sambil bertanggung jawab atas HSMs yang melindungi kunci KMS Anda. Ini menggabungkan penyewa tunggal HSMs di bawah kendali Anda dengan kemudahan penggunaan dan integrasi. AWS KMS Untuk mengelola AWS CloudHSM infrastruktur Anda, Anda harus menggunakan infrastruktur kunci publik (PKI) dan memiliki tim yang memiliki pengalaman mengelola. HSMs

AWS Secrets Manager

AWS Secrets Managermembantu Anda melindungi kredensi (rahasia) yang Anda butuhkan untuk mengakses aplikasi, layanan, dan sumber daya TI Anda. Layanan ini memungkinkan Anda untuk secara efisien memutar, mengelola, dan mengambil kredenal database, kunci API, dan rahasia lainnya sepanjang siklus hidupnya. Anda dapat mengganti kredensi hardcode dalam kode Anda dengan panggilan API ke Secrets Manager untuk mengambil rahasia secara terprogram. Ini membantu memastikan bahwa rahasia tidak dapat dikompromikan oleh seseorang yang memeriksa kode Anda, karena rahasia tidak lagi ada dalam kode. Selain itu, Secrets Manager membantu Anda memindahkan aplikasi antar lingkungan (pengembangan, pra-produksi, produksi). Alih-alih

mengubah kode, Anda dapat memastikan bahwa rahasia yang diberi nama dan direferensikan dengan tepat tersedia di lingkungan. Ini mempromosikan konsistensi dan kegunaan kembali kode aplikasi di lingkungan yang berbeda, sementara membutuhkan lebih sedikit perubahan dan interaksi manusia setelah kode diuji.

Dengan Secrets Manager, Anda dapat mengelola akses ke rahasia dengan menggunakan kebijakan IAM berbutir halus dan kebijakan berbasis sumber daya. Anda dapat membantu mengamankan rahasia dengan mengenkripsi mereka dengan kunci enkripsi yang Anda kelola dengan menggunakan. AWS KMS Secrets Manager juga terintegrasi dengan layanan AWS pencatatan dan pemantauan untuk audit terpusat.

Secrets Manager menggunakan enkripsi amplop dengan AWS KMS keys dan kunci data untuk melindungi setiap nilai rahasia. Saat membuat rahasia, Anda dapat memilih kunci yang dikelola pelanggan simetris di Akun AWS dan Wilayah, atau Anda dapat menggunakan kunci AWS terkelola untuk Secrets Manager.

Sebagai praktik terbaik, Anda dapat memantau rahasia Anda untuk mencatat perubahan apa pun padanya. Ini membantu Anda memastikan bahwa penggunaan atau perubahan yang tidak terduga dapat diselidiki. Perubahan yang tidak diinginkan dapat digulung kembali. Secrets Manager saat ini mendukung dua Layanan AWS yang memungkinkan Anda memantau organisasi dan aktivitas Anda: AWS CloudTrail dan AWS Config. CloudTrail menangkap semua panggilan API untuk Secrets Manager sebagai peristiwa, termasuk panggilan dari konsol Secrets Manager dan dari panggilan kode ke Secrets Manager APIs. Selain itu, CloudTrail menangkap peristiwa terkait (non-API) lainnya yang mungkin memiliki dampak keamanan atau kepatuhan pada Anda Akun AWS atau mungkin membantu Anda memecahkan masalah operasional. Ini termasuk peristiwa rotasi rahasia tertentu dan penghapusan versi rahasia. AWS Config dapat memberikan kontrol detektif dengan melacak dan memantau perubahan rahasia di Secrets Manager. Perubahan ini termasuk deskripsi rahasia, konfigurasi rotasi, tag, dan hubungan dengan AWS sumber lain seperti kunci enkripsi KMS atau AWS Lambda fungsi yang digunakan untuk rotasi rahasia. Anda juga dapat mengonfigurasi Amazon EventBridge, yang menerima pemberitahuan perubahan konfigurasi dan kepatuhan dari AWS Config, untuk merutekan peristiwa rahasia tertentu untuk tindakan pemberitahuan atau perbaikan.

Di AWS SRA, Secrets Manager terletak di akun Aplikasi untuk mendukung kasus penggunaan aplikasi lokal dan untuk mengelola rahasia yang dekat dengan penggunaannya. Di sini, profil instance dilampirkan ke EC2 instance di akun Aplikasi. Rahasia terpisah kemudian dapat dikonfigurasi di Secrets Manager untuk memungkinkan profil instans tersebut mengambil rahasia —misalnya, untuk bergabung dengan Active Directory atau domain LDAP yang sesuai dan untuk mengakses database Aurora. Secrets Manager terintegrasi dengan Amazon RDS untuk mengelola

kredensyal pengguna saat Anda membuat, memodifikasi, atau memulihkan instans Amazon RDS DB atau cluster DB multi-AZ. Ini membantu Anda mengelola pembuatan dan rotasi kunci dan mengganti kredensi hardcode dalam kode Anda dengan panggilan API terprogram ke Secrets Manager.

> **Pertimbangan desain**
>
> Secara umum, konfigurasikan dan kelola Secrets Manager di akun yang paling dekat dengan tempat rahasia akan digunakan. Pendekatan ini memanfaatkan pengetahuan lokal tentang kasus penggunaan dan memberikan kecepatan dan fleksibilitas kepada tim pengembangan aplikasi. Untuk informasi yang dikontrol ketat di mana lapisan kontrol tambahan mungkin sesuai, rahasia dapat dikelola secara terpusat oleh Secrets Manager di akun Security Tooling.

Amazon Cognito

Amazon Cognito memungkinkan Anda menambahkan pendaftaran pengguna, masuk, dan kontrol akses ke web dan aplikasi seluler Anda dengan cepat dan efisien. Amazon Cognito menskalakan jutaan pengguna dan mendukung proses masuk dengan penyedia identitas sosial, seperti Apple, Facebook, Google, dan Amazon, serta penyedia identitas perusahaan melalui SAMP 2.0 dan OpenID Connect. Dua komponen utama Amazon Cognito adalah kumpulan pengguna dan kumpulan identitas. Kumpulan pengguna adalah direktori pengguna yang menyediakan opsi pendaftaran dan masuk untuk pengguna aplikasi Anda. Identity pool memungkinkan Anda untuk memberikan pengguna Anda akses ke orang lain Layanan AWS. Anda dapat menggunakan kolam identitas dan kolam pengguna secara terpisah atau bersama-sama. Untuk skenario penggunaan umum, lihat dokumentasi Amazon Cognito.

Amazon Cognito menyediakan UI bawaan dan dapat disesuaikan untuk pendaftaran dan masuk pengguna. Anda dapat menggunakan Android, iOS, dan JavaScript SDKs Amazon Cognito untuk menambahkan halaman pendaftaran dan login pengguna ke aplikasi Anda. Amazon Cognito Sync adalah pustaka Layanan AWS dan klien yang memungkinkan sinkronisasi lintas perangkat data pengguna terkait aplikasi.

Amazon Cognito mendukung otentikasi multi-faktor dan enkripsi data saat istirahat dan data dalam perjalanan. Kumpulan pengguna Amazon Cognito menyediakan fitur keamanan canggih untuk membantu melindungi akses ke akun pengguna di aplikasi Anda. Fitur keamanan canggih ini memberikan otentikasi adaptif berbasis risiko dan perlindungan dari penggunaan kredensi yang dikompromikan.

Pertimbangan desain

- Anda dapat membuat AWS Lambda fungsi dan kemudian memicu fungsi tersebut selama operasi kumpulan pengguna seperti pendaftaran pengguna, konfirmasi, dan login (otentikasi) dengan pemicu Lambda. Anda dapat menambahkan tantangan autentikasi, memigrasikan pengguna, dan menyesuaikan pesan verifikasi. Untuk operasi umum dan alur pengguna, lihat dokumentasi Amazon Cognito. Amazon Cognito memanggil fungsi Lambda secara sinkron.
- Anda dapat menggunakan kumpulan pengguna Amazon Cognito untuk mengamankan aplikasi kecil multi-penyewa. Kasus penggunaan umum desain multi-tenant adalah menjalankan beban kerja untuk mendukung pengujian beberapa versi aplikasi. Desain multi-penyewa juga berguna untuk menguji aplikasi tunggal dengan set data yang berbeda, yang memungkinkan penggunaan penuh sumber daya klaster Anda. Namun, pastikan bahwa jumlah penyewa dan volume yang diharapkan selaras dengan kuota layanan Amazon Cognito terkait. Kuota ini dibagi di semua penyewa di dalam aplikasi Anda.

Izin Terverifikasi Amazon

Izin Terverifikasi Amazon adalah manajemen izin yang dapat diskalakan dan layanan otorisasi berbutir halus untuk aplikasi yang Anda buat. Pengembang dan administrator dapat menggunakan Cedar, bahasa kebijakan sumber terbuka yang dibuat khusus dan mengutamakan keamanan, dengan peran dan atribut untuk menentukan kontrol akses berbasis kebijakan yang lebih terperinci, sadar konteks, dan berbasis kebijakan. Pengembang dapat membangun aplikasi yang lebih aman lebih cepat dengan mengeksternalisasi otorisasi dan memusatkan manajemen dan administrasi kebijakan. Izin Terverifikasi mencakup definisi skema, tata bahasa pernyataan kebijakan, dan penalaran otomatis yang menskalakan jutaan izin, sehingga Anda dapat menerapkan prinsip penolakan default dan hak istimewa paling sedikit. Layanan ini juga mencakup alat simulator evaluasi untuk membantu Anda menguji keputusan otorisasi dan kebijakan penulis Anda. Fitur-fitur ini memfasilitasi penerapan model otorisasi yang mendalam dan berbutir halus untuk mendukung tujuan zero-trust Anda. Izin Terverifikasi memusatkan izin di toko kebijakan dan membantu pengembang menggunakan izin tersebut untuk mengotorisasi tindakan pengguna dalam aplikasi mereka.

Anda dapat menghubungkan aplikasi Anda ke layanan melalui API untuk mengotorisasi permintaan akses pengguna. Untuk setiap permintaan otorisasi, layanan mengambil kebijakan yang relevan dan mengevaluasi kebijakan tersebut untuk menentukan apakah pengguna diizinkan untuk mengambil tindakan pada sumber daya, berdasarkan masukan konteks seperti pengguna, peran, keanggotaan

grup, dan atribut. Anda dapat mengonfigurasi dan menghubungkan Izin Terverifikasi untuk mengirim log manajemen kebijakan dan otorisasi. AWS CloudTrail Jika Anda menggunakan Amazon Cognito sebagai penyimpanan identitas, Anda dapat mengintegrasikan dengan Izin Terverifikasi dan menggunakan ID dan token akses yang dikembalikan Amazon Cognito dalam keputusan otorisasi dalam aplikasi Anda. Anda memberikan token Amazon Cognito ke Izin Terverifikasi, yang menggunakan atribut yang terkandung dalam token untuk mewakili prinsipal dan mengidentifikasi hak prinsipal. Untuk informasi lebih lanjut tentang integrasi ini, lihat posting AWS blog Menyederhanakan otorisasi halus dengan Izin Terverifikasi Amazon dan Amazon Cognito.

Izin Terverifikasi membantu Anda menentukan kontrol akses berbasis kebijakan (PBAC). PBAC adalah model kontrol akses yang menggunakan izin yang dinyatakan sebagai kebijakan untuk menentukan siapa yang dapat mengakses sumber daya dalam aplikasi. PBAC menyatukan kontrol akses berbasis peran (RBAC) dan kontrol akses berbasis atribut (ABAC), menghasilkan model kontrol akses yang lebih kuat dan fleksibel. Untuk mempelajari lebih lanjut tentang PBAC dan cara mendesain model otorisasi menggunakan Izin Terverifikasi, lihat posting AWS blog Kontrol akses berbasis kebijakan dalam pengembangan aplikasi dengan Izin Terverifikasi Amazon.

Di AWS SRA, Izin Terverifikasi terletak di akun Aplikasi untuk mendukung manajemen izin untuk aplikasi melalui integrasinya dengan Amazon Cognito.

Pertahanan berlapis

Akun Aplikasi memberikan kesempatan untuk mengilustrasikan prinsip-prinsip pertahanan berlapis yang memungkinkan. AWS Pertimbangkan keamanan EC2 instance yang membentuk inti dari aplikasi contoh sederhana yang diwakili dalam AWS SRA dan Anda dapat melihat cara Layanan AWS bekerja sama dalam pertahanan berlapis. Pendekatan ini sejalan dengan pandangan struktural layanan AWS keamanan, seperti yang dijelaskan di bagian Menerapkan layanan keamanan di seluruh AWS organisasi Anda sebelumnya dalam panduan ini.

- Lapisan terdalam adalah instance. EC2 Seperti disebutkan sebelumnya, EC2 instance mencakup banyak fitur keamanan asli baik secara default atau sebagai opsi. Contohnya termasuk IMDSv2, sistem Nitro, dan enkripsi penyimpanan Amazon EBS.
- Lapisan perlindungan kedua berfokus pada sistem operasi dan perangkat lunak yang berjalan pada EC2 instance. Layanan seperti Amazon Inspector dan AWS Systems Managermemungkinkan Anda memantau, melaporkan, dan mengambil tindakan korektif pada konfigurasi ini. Amazon Inspector memantau kerentanan perangkat lunak Anda dan Systems Manager membantu Anda menjaga keamanan dan kepatuhan dengan memindai instans terkelola

untuk status patch dan konfigurasi mereka, lalu melaporkan dan mengambil tindakan korektif apa pun yang Anda tentukan.

- Instans, dan perangkat lunak yang berjalan pada contoh ini, duduk dengan infrastruktur AWS jaringan Anda. Selain menggunakan fitur keamanan Amazon VPC, AWS SRA juga memanfaatkan titik akhir VPC untuk menyediakan konektivitas pribadi antara VPC dan yang didukung Layanan AWS, dan untuk menyediakan mekanisme untuk menempatkan kebijakan akses pada batas jaringan.
- Aktivitas dan konfigurasi EC2 instans, perangkat lunak, jaringan, dan peran dan sumber daya IAM dipantau lebih lanjut oleh layanan yang Akun AWS berfokus seperti,, Amazon,, AWS Security Hub CSPM, IAM Access GuardDuty Analyzer AWS CloudTrail AWS Config, dan AWS Security Hub Amazon Macie.
- Terakhir, di luar akun Aplikasi, AWS RAM membantu mengontrol sumber daya mana yang dibagikan dengan akun lain, dan kebijakan kontrol layanan IAM membantu Anda menerapkan izin yang konsisten di seluruh organisasi. AWS

AI/ML untuk keamanan

Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

Kecerdasan buatan dan pembelajaran mesin (AI/ML) is transforming businesses. AI/MLtelah menjadi fokus Amazon selama lebih dari 20 tahun, dan banyak dari kemampuan yang digunakan pelanggan AWS, termasuk layanan keamanan, didorong oleh AI/ML. Ini menciptakan nilai terdiferensiasi bawaan, karena Anda dapat membangun dengan aman AWS tanpa memerlukan tim keamanan atau pengembangan aplikasi Anda untuk memiliki keahlian dalam AI/ML.

AI adalah teknologi canggih yang memungkinkan mesin dan sistem untuk mendapatkan kecerdasan dan kemampuan prediksi. Sistem AI belajar dari pengalaman masa lalu melalui data yang dikonsumsi atau dilatih. ML adalah salah satu aspek terpenting dari AI. ML adalah kemampuan komputer untuk belajar dari data tanpa diprogram secara eksplisit. Dalam pemrograman tradisional, programmer menulis aturan yang menentukan bagaimana program harus bekerja pada komputer atau mesin. Dalam ML, model mempelajari aturan dari data. Model ML dapat menemukan pola tersembunyi dalam data atau membuat prediksi akurat pada data baru yang tidak digunakan selama pelatihan. Layanan AWS Penggunaan ganda AI/ML untuk belajar dari kumpulan data besar dan membuat kesimpulan keamanan.

- Amazon Macie adalah layanan keamanan data yang menggunakan ML dan pencocokan pola untuk menemukan dan membantu melindungi data sensitif Anda. Macie secara otomatis mendeteksi daftar tipe data sensitif yang besar dan terus bertambah, termasuk informasi identitas pribadi (PII) seperti nama, alamat, dan informasi keuangan seperti nomor kartu kredit. Ini juga memberi Anda visibilitas konstan ke data Anda yang disimpan di Amazon Simple Storage Service (Amazon S3). Macie menggunakan Natural Language Processing (NLP) dan model ML yang dilatih pada berbagai jenis dataset untuk memahami data yang ada dan untuk menetapkan nilai bisnis untuk memprioritaskan data penting bisnis. Macie kemudian menghasilkan temuan data sensitif.
- Amazon GuardDuty adalah layanan deteksi ancaman yang menggunakan ML, deteksi anomali, dan intelijen ancaman terintegrasi untuk terus memantau aktivitas berbahaya dan perilaku tidak sah untuk membantu melindungi beban kerja, pengguna, database Akun AWS, dan penyimpanan Anda, instans, tanpa server dan kontainer. GuardDuty menggabungkan teknik ML yang sangat efektif dalam membedakan aktivitas pengguna yang berpotensi berbahaya dari perilaku operasional anomali tetapi jinak di dalamnya. Akun AWS Kemampuan ini terus

memodelkan pemanggilan API dalam akun dan menggabungkan prediksi probabilistik untuk mengisolasi dan memperingatkan perilaku pengguna yang sangat mencurigakan secara lebih akurat. Pendekatan ini membantu mengidentifikasi aktivitas jahat yang terkait dengan taktik ancaman yang diketahui, termasuk penemuan, akses awal, ketekunan, eskalasi hak istimewa, penghindaran pertahanan, akses kredenal, dampak, dan eksfiltrasi data. Untuk mempelajari lebih lanjut tentang cara GuardDuty menggunakan pembelajaran mesin, lihat sesi breakout AWS re: Inforce 2023 Mengembangkan temuan baru menggunakan pembelajaran mesin di Amazon (0). GuardDuty TDR31

Keamanan yang dapat dibuktikan

AWS mengembangkan alat penalaran otomatis yang menggunakan logika matematika untuk menjawab pertanyaan kritis tentang infrastruktur Anda dan untuk mendeteksi kesalahan konfigurasi yang berpotensi mengekspos data Anda. Kemampuan ini disebut keamanan yang dapat dibuktikan karena memberikan jaminan yang lebih tinggi dalam keamanan cloud dan cloud. Keamanan yang dapat dibuktikan menggunakan penalaran otomatis, yang merupakan disiplin khusus AI yang menerapkan pengurangan logis ke sistem komputer. Misalnya, alat penalaran otomatis dapat menganalisis kebijakan dan konfigurasi arsitektur jaringan, dan membuktikan tidak adanya konfigurasi yang tidak diinginkan yang berpotensi mengekspos data yang rentan. Pendekatan ini memberikan tingkat jaminan tertinggi yang mungkin untuk karakteristik keamanan kritis cloud. Untuk informasi selengkapnya, lihat Sumber Daya Keamanan yang Dapat Dibuktikan di AWS situs web. Berikut Layanan AWS dan fitur saat ini menggunakan penalaran otomatis untuk membantu Anda mencapai keamanan yang dapat dibuktikan untuk aplikasi Anda:

- Izin Terverifikasi Amazon adalah manajemen izin yang dapat diskalakan dan layanan otorisasi berbutir halus untuk aplikasi yang Anda buat. Izin Terverifikasi menggunakan Cedar, yang merupakan bahasa sumber terbuka untuk kontrol akses yang dibangun dengan menggunakan penalaran otomatis dan pengujian diferensial. Cedar adalah bahasa untuk mendefinisikan izin sebagai kebijakan yang menjelaskan siapa yang harus memiliki akses ke sumber daya mana. Ini juga merupakan spesifikasi untuk mengevaluasi kebijakan tersebut. Gunakan kebijakan Cedar untuk mengontrol apa yang diizinkan dilakukan oleh setiap pengguna aplikasi Anda dan sumber daya mana yang dapat mereka akses. Kebijakan Cedar adalah pernyataan izin atau larangan yang menentukan apakah pengguna dapat bertindak berdasarkan sumber daya. Kebijakan dikaitkan dengan sumber daya, dan Anda dapat melampirkan beberapa kebijakan ke sumber daya. Melarang kebijakan mengesampingkan kebijakan izin. Ketika pengguna aplikasi Anda mencoba melakukan tindakan pada sumber daya, aplikasi Anda membuat permintaan otorisasi ke mesin

kebijakan Cedar. Cedar mengevaluasi kebijakan yang berlaku dan mengembalikan keputusan `ALLOW` atau`DENY`. Cedar mendukung aturan otorisasi untuk semua jenis prinsipal dan sumber daya, memungkinkan kontrol akses berbasis peran dan atribut, dan mendukung analisis melalui alat penalaran otomatis yang dapat membantu mengoptimalkan kebijakan Anda dan memvalidasi model keamanan Anda.

- AWS Identity and Access Management Access Analyzermembantu Anda merampingkan manajemen izin. Anda dapat menggunakan fitur ini untuk mengatur izin berbutir halus, memverifikasi izin yang dimaksudkan, dan memperbaiki izin dengan menghapus akses yang tidak digunakan. IAM Access Analyzer menghasilkan kebijakan berbutir halus berdasarkan aktivitas akses yang ditangkap di log Anda. Ini juga menyediakan lebih dari 100 pemeriksaan kebijakan untuk membantu Anda membuat dan memvalidasi kebijakan Anda. IAM Access Analyzer menggunakan keamanan yang dapat dibuktikan untuk menganalisis jalur akses dan memberikan temuan komprehensif untuk akses publik dan lintas akun ke sumber daya Anda. Alat ini dibangun di atas Zelkova, yang menerjemahkan kebijakan IAM ke dalam pernyataan logis yang setara dan menjalankan serangkaian pemecah logis tujuan umum dan khusus (teori modulo kepuasan) terhadap masalah tersebut. IAM Access Analyzer menerapkan Zelkova berulang kali pada kebijakan dengan kueri yang semakin spesifik untuk mengkarakterisasi kelas perilaku yang diizinkan kebijakan, berdasarkan konten kebijakan. Analyzer tidak memeriksa log akses untuk menentukan apakah entitas eksternal mengakses sumber daya dalam zona kepercayaan Anda. Ini menghasilkan temuan ketika kebijakan berbasis sumber daya memungkinkan akses ke sumber daya, bahkan jika sumber daya tidak diakses oleh entitas eksternal. Untuk mempelajari lebih lanjut tentang teori modulo kepuasan, lihat Teori Modulo Kepuasan dalam Buku Pegangan Kepuasan. *
- Amazon S3 Block Public Access adalah fitur Amazon S3 yang memungkinkan Anda memblokir kemungkinan kesalahan konfigurasi yang dapat menyebabkan akses publik ke ember dan objek Anda. Anda dapat mengaktifkan Amazon S3 Blokir Akses Publik untuk titik akses, bucket, akun, dan AWS organisasi (yang memengaruhi bucket yang ada dan baru di akun). Akses publik diberikan ke bucket dan objek melalui daftar kontrol akses (ACLs), kebijakan bucket, atau keduanya. Penentuan apakah kebijakan tertentu atau ACL dianggap publik dilakukan dengan menggunakan sistem penalaran otomatis Zelkova. Amazon S3 menggunakan Zelkova untuk memeriksa setiap kebijakan bucket dan memperingatkan Anda jika pengguna yang tidak sah dapat membaca atau menulis ke bucket Anda. Jika bucket ditandai sebagai publik, beberapa permintaan publik diizinkan untuk mengakses bucket. Jika bucket ditandai sebagai tidak publik, semua permintaan publik ditolak. Zelkova mampu membuat penentuan seperti itu karena memiliki representasi matematis yang tepat dari kebijakan IAM. Ini menciptakan formula untuk setiap kebijakan dan membuktikan teorema tentang rumus itu.

- Amazon VPC Network Access Analyzer adalah fitur Amazon VPC yang membantu Anda memahami jalur jaringan potensial ke sumber daya Anda, dan mengidentifikasi potensi akses jaringan yang tidak diinginkan. Network Access Analyzer membantu Anda memverifikasi segmentasi jaringan, mengidentifikasi aksesibilitas internet, dan memverifikasi jalur jaringan dan akses jaringan tepercaya. Fitur ini menggunakan algoritma penalaran otomatis untuk menganalisis jalur jaringan yang dapat diambil paket antara sumber daya dalam jaringan. AWS Kemudian menghasilkan temuan untuk jalur yang sesuai dengan Lingkup Akses Jaringan Anda, yang menentukan pola lalu lintas keluar dan masuk. Network Access Analyzer melakukan analisis statis dari konfigurasi jaringan, yang berarti bahwa tidak ada paket yang ditransmisikan dalam jaringan sebagai bagian dari analisis ini.
- Amazon VPC Reachability Analyzer adalah fitur Amazon VPC yang memungkinkan Anda men-debug, memahami, dan memvisualisasikan konektivitas di jaringan Anda. AWS Reachability Analyzer adalah alat analisis konfigurasi yang memungkinkan Anda melakukan pengujian konektivitas antara sumber daya sumber dan sumber daya tujuan di cloud pribadi virtual Anda (). VPCs Ketika tujuan dapat dijangkau, Reachability hop-by-hop Analyzer menghasilkan rincian jalur jaringan virtual antara sumber dan tujuan. Ketika tujuan tidak dapat dijangkau, Reachability Analyzer mengidentifikasi komponen pemblokiran. Reachability Analyzer menggunakan penalaran otomatis untuk mengidentifikasi jalur yang layak dengan membangun model konfigurasi jaringan antara sumber dan tujuan. Kemudian memeriksa jangkauan berdasarkan konfigurasi. Itu tidak mengirim paket atau menganalisis pesawat data.

[*] Biere, A.M. Heule, H. van Maaren, dan T. Walsh. 2009. Buku Pegangan Kepuasan. Pers IOS, NLD.

Membangun arsitektur keamanan Anda — pendekatan bertahap

Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

Arsitektur keamanan multi-akun yang direkomendasikan oleh AWS SRA adalah arsitektur dasar untuk membantu Anda menyuntikkan keamanan lebih awal ke dalam proses desain Anda. Perjalanan cloud setiap organisasi adalah unik. Agar berhasil mengembangkan arsitektur keamanan cloud Anda, Anda perlu membayangkan status target yang Anda inginkan, memahami kesiapan cloud Anda saat ini, dan mengadopsi pendekatan tangkas untuk menutup celah apa pun. AWS SRA menyediakan status target referensi untuk arsitektur keamanan Anda. Transformasi secara bertahap memungkinkan Anda untuk menunjukkan nilai dengan cepat sambil meminimalkan kebutuhan untuk membuat prediksi yang luas.

AWS Cloud Adoption Framework (AWS CAF) merekomendasikan empat fase transformasi cloud berulang dan bertahap: membayangkan, menyelaraskan, meluncurkan, dan skala. Ketika Anda memasuki fase peluncuran dan fokus pada memberikan inisiatif percontohan dalam produksi, Anda harus fokus pada membangun arsitektur keamanan yang kuat sebagai dasar untuk fase skala sehingga Anda memiliki kemampuan teknis untuk bermigrasi dan mengoperasikan beban kerja bisnis Anda yang paling kritis dengan percaya diri. Pendekatan bertahap ini berlaku jika Anda seorang startup, perusahaan kecil atau menengah yang ingin memperluas bisnis mereka, atau perusahaan yang mengakuisisi unit bisnis baru atau menjalani merger dan akuisisi. AWS SRA membantu Anda mencapai arsitektur dasar keamanan sehingga Anda dapat menerapkan kontrol keamanan secara seragam di seluruh organisasi Anda yang sedang berkembang. AWS Organizations Arsitektur dasar terdiri dari beberapa Akun AWS dan layanan. Perencanaan dan implementasi harus menjadi proses multi-fase sehingga Anda dapat mengulangi tonggak yang lebih kecil untuk mencapai tujuan yang lebih besar dalam menyiapkan arsitektur keamanan dasar Anda. Bagian ini menjelaskan fase khas perjalanan cloud Anda berdasarkan pendekatan terstruktur. Fase-fase ini selaras dengan prinsip-prinsip desain keamanan AWS Well-Architected Framework.

Fase 1: Bangun struktur OU dan akun Anda

Prasyarat untuk fondasi keamanan yang kuat adalah AWS organisasi dan struktur akun yang dirancang dengan baik. Seperti yang dijelaskan sebelumnya di bagian blok bangunan SRA dari panduan ini, memiliki banyak Akun AWS membantu Anda mengisolasi fungsi bisnis dan keamanan yang berbeda berdasarkan desain. Ini mungkin tampak seperti pekerjaan yang tidak perlu pada awalnya, tetapi ini adalah investasi untuk membantu Anda meningkatkan skala dengan cepat dan aman. Bagian itu juga menjelaskan bagaimana Anda dapat menggunakan AWS Organizations untuk mengelola beberapa Akun AWS, dan cara menggunakan akses tepercaya dan fitur administrator yang didelegasikan untuk mengelola secara terpusat Layanan AWS di beberapa akun ini.

Anda dapat menggunakan AWS Control Towerseperti yang diuraikan sebelumnya dalam panduan ini untuk mengatur landing zone Anda. Jika saat ini Anda menggunakan satu akun Akun AWS, lihat Akun AWS panduan Transisi ke beberapa untuk bermigrasi ke beberapa akun sedini mungkin. Misalnya, jika perusahaan startup Anda saat ini sedang merancang dan membuat prototipe produk Anda dalam satu Akun AWS, Anda harus berpikir tentang mengadopsi strategi multi-akun sebelum Anda meluncurkan produk Anda di pasar. Demikian pula, organisasi kecil, menengah, dan perusahaan harus mulai membangun strategi multi-akun mereka segera setelah mereka merencanakan beban kerja produksi awal mereka. Mulailah dengan yayasan Anda OUs dan Akun AWS, lalu tambahkan akun dan terkait beban kerja OUs Anda.

Untuk Akun AWS rekomendasi struktur OU di luar apa yang disediakan di AWS SRA, lihat strategi Multi-akun untuk posting blog usaha kecil dan menengah. Saat Anda menyelesaikan OU dan struktur akun Anda, pertimbangkan kontrol keamanan tingkat tinggi di seluruh organisasi yang ingin Anda terapkan dengan menggunakan kebijakan kontrol layanan (), kebijakan kontrol sumber daya (SCPs), dan kebijakan deklaratifRCPs.

> **Pertimbangan desain**
>
> Jangan mereplikasi struktur pelaporan perusahaan Anda saat Anda mendesain OU dan struktur akun Anda. Anda OUs harus didasarkan pada fungsi beban kerja dan serangkaian kontrol keamanan umum yang berlaku untuk beban kerja. Jangan mencoba mendesain struktur akun lengkap Anda dari awal. Fokus pada dasar OUs, dan kemudian tambahkan beban kerja OUs saat Anda membutuhkannya. Anda dapat memindahkan akun OUs untuk bereksperimen dengan pendekatan alternatif selama tahap awal desain Anda. Namun, ini mungkin mengakibatkan beberapa overhead seputar pengelolaan izin logis, tergantung pada SCPs,, kebijakan deklaratif RCPs, dan kondisi IAM yang didasarkan pada jalur OU dan akun.

Contoh implementasi

Pustaka kode AWS SRA menyediakan contoh implementasi Kontak Alternatif Akun. Solusi ini menetapkan kontak alternatif penagihan, operasi, dan keamanan untuk semua akun dalam suatu organisasi.

Tahap 2: Menerapkan fondasi identitas yang kuat

Segera setelah Anda membuat beberapa Akun AWS, Anda harus memberi tim Anda akses ke AWS sumber daya dalam akun tersebut. Ada dua kategori umum manajemen identitas: identitas tenaga kerja dan manajemen akses dan identitas pelanggan dan manajemen akses (CIAM). Workforce IAM adalah untuk organisasi di mana karyawan dan beban kerja otomatis perlu masuk AWS untuk melakukan pekerjaan mereka. CIAM digunakan ketika sebuah organisasi membutuhkan cara untuk mengautentikasi pengguna untuk menyediakan akses ke aplikasi organisasi. Anda memerlukan strategi IAM tenaga kerja terlebih dahulu, sehingga tim Anda dapat membangun dan memigrasi aplikasi. Anda harus selalu menggunakan peran IAM alih-alih pengguna IAM untuk menyediakan akses ke pengguna manusia atau mesin. Ikuti panduan AWS SRA tentang cara menggunakan AWS IAM Identity Center akun Manajemen Organisasi dan Layanan Bersama untuk mengelola akses masuk tunggal (SSO) secara terpusat ke akun Anda. Akun AWS Panduan ini juga memberikan pertimbangan desain untuk menggunakan federasi IAM ketika Anda tidak dapat menggunakan IAM Identity Center.

Saat Anda bekerja dengan peran IAM untuk menyediakan akses pengguna ke AWS sumber daya, Anda harus menggunakan IAM Access Analyzer dan penasihat akses IAM sebagaimana diuraikan dalam bagian Perkakas Keamanan dan Manajemen Org dari panduan ini. Layanan ini membantu Anda mencapai hak istimewa paling sedikit, yang merupakan kontrol pencegahan penting yang membantu Anda membangun postur keamanan yang baik.

Pertimbangan desain

Untuk mencapai hak istimewa paling sedikit, rancang proses untuk secara teratur meninjau dan memahami hubungan antara identitas Anda dan izin yang mereka perlukan untuk berfungsi dengan baik. Saat Anda belajar, sesuaikan izin tersebut dan secara bertahap pangkas hingga izin sekecil mungkin. Untuk skalabilitas, ini harus menjadi tanggung jawab bersama antara tim keamanan dan aplikasi pusat Anda. Gunakan fitur seperti kebijakan

berbasis sumber daya, batas izin, kontrol akses berbasis atribut, dan kebijakan sesi untuk membantu pemilik aplikasi menentukan kontrol akses berbutir halus.

Contoh implementasi

Pustaka kode AWS SRA menyediakan dua contoh implementasi yang berlaku untuk fase ini:

- Kebijakan Kata Sandi IAM menetapkan kebijakan kata sandi akun agar pengguna selaras dengan standar kepatuhan umum.
- Access Analyzer mengonfigurasi penganalisis tingkat organisasi dalam akun administrator yang didelegasikan dan penganalisis tingkat akun dalam setiap akun.

Fase 3: Pertahankan ketertelusuran

Ketika pengguna Anda memiliki akses ke AWS dan mulai membangun, Anda akan ingin tahu siapa yang melakukan apa, kapan, dan dari mana. Anda juga akan menginginkan visibilitas ke potensi kesalahan konfigurasi keamanan, ancaman, atau perilaku tak terduga. Pemahaman yang lebih baik tentang ancaman keamanan memungkinkan Anda memprioritaskan kontrol keamanan yang sesuai. Untuk memantau AWS aktivitas, ikuti rekomendasi AWS SRA untuk menyiapkan jejak organisasi dengan menggunakan AWS CloudTraildan memusatkan log Anda dalam akun Arsip Log. Untuk pemantauan peristiwa keamanan, gunakan, Amazon AWS Security Hub CSPM GuardDuty AWS Config, dan Amazon Security Lake sebagaimana diuraikan di bagian akun Security Tooling.

Pertimbangan desain

Saat Anda mulai menggunakan new Layanan AWS, pastikan untuk mengaktifkan log khusus layanan untuk layanan dan menyimpannya sebagai bagian dari repositori log pusat Anda.

Contoh implementasi

Pustaka kode AWS SRA menyediakan contoh implementasi berikut yang berlaku untuk fase ini:

- Organisasi CloudTrail membuat jejak organisasi dan menetapkan default untuk mengonfigurasi peristiwa data (misalnya, di Amazon S3 dan AWS Lambda) untuk

mengurangi duplikat yang dikonfigurasi oleh. CloudTrail AWS Control Tower Solusi ini menyediakan opsi untuk mengonfigurasi acara manajemen.

- AWS Config Control Tower Management Account memungkinkan AWS Config di akun Manajemen untuk memantau kepatuhan sumber daya.
- Aturan Organisasi Paket Kesesuaian menerapkan paket kesesuaian ke akun dan Wilayah tertentu dalam organisasi.
- AWS Config Aggregator menyebarkan agregator dengan mendelegasikan administrasi ke akun anggota selain akun Audit.
- Organisasi CSPM Security Hub mengonfigurasi CSPM Security Hub dalam akun administrator yang didelegasikan untuk akun dan Wilayah yang diatur dalam organisasi.
- GuardDuty Organisasi mengonfigurasi GuardDuty dalam akun administrator yang didelegasikan untuk akun dalam organisasi.

Fase 4: Terapkan keamanan di semua lapisan

Pada titik ini, Anda harus memiliki:

- Kontrol keamanan yang tepat untuk Anda Akun AWS.
- Akun dan struktur OU yang terdefinisi dengan baik dengan kontrol preventif yang didefinisikan melalui SCPs, RCPs, kebijakan deklaratif, dan peran dan kebijakan IAM yang paling tidak istimewa.
- Kemampuan untuk mencatat AWS aktivitas dengan menggunakan AWS CloudTrail; untuk mendeteksi peristiwa keamanan dengan menggunakan AWS Security Hub CSPM, Amazon GuardDuty, dan AWS Config; dan untuk melakukan analitik lanjutan pada data lake yang dibuat khusus untuk keamanan dengan menggunakan Amazon Security Lake.

Pada fase ini, rencanakan untuk menerapkan keamanan di lapisan lain AWS organisasi Anda, seperti yang dijelaskan di bagian, Terapkan layanan keamanan di seluruh AWS organisasi Anda. Anda dapat membangun kontrol keamanan untuk lapisan jaringan Anda dengan menggunakan layanan seperti AWS WAF,,, AWS Shield AWS Firewall Manager, AWS Certificate Manager (ACM) AWS Network Firewall, Amazon, Amazon CloudFront Route 53, dan Amazon VPC, sebagaimana diuraikan di bagian akun Jaringan. Saat Anda memindahkan tumpukan teknologi Anda, terapkan kontrol keamanan yang spesifik untuk beban kerja atau tumpukan aplikasi Anda. Gunakan titik akhir

VPC, Amazon Inspector,,, AWS Systems Manager dan AWS Secrets Manager Amazon Cognito sebagaimana diuraikan di bagian Akun aplikasi.

Pertimbangan desain

Saat Anda merancang kontrol keamanan pertahanan Anda secara mendalam (DiD), pertimbangkan faktor penskalaan. Tim keamanan pusat Anda tidak akan memiliki bandwidth atau pemahaman penuh tentang bagaimana setiap aplikasi berperilaku di lingkungan Anda. Berdayakan tim aplikasi Anda untuk bertanggung jawab dan bertanggung jawab dalam mengidentifikasi dan merancang kontrol keamanan yang tepat untuk aplikasi mereka. Tim keamanan pusat harus fokus pada penyediaan alat dan konsultasi yang tepat untuk memungkinkan tim aplikasi. Untuk memahami mekanisme penskalaan yang AWS digunakan untuk mengadopsi pendekatan keamanan yang lebih bergeser ke kiri, lihat posting blog Bagaimana AWS membangun program Penjaga Keamanan, sebuah mekanisme untuk mendistribusikan kepemilikan keamanan.

Contoh implementasi

Pustaka kode AWS SRA menyediakan contoh implementasi berikut yang berlaku untuk fase ini:

- Enkripsi EBS Default EC2 mengonfigurasi enkripsi Amazon EBS default di Amazon EC2 untuk menggunakan default dalam yang disediakan. AWS KMS key Wilayah AWS
- Akses Publik Akun Blok S3 mengonfigurasi pengaturan Blokir Akses Publik (BPA) tingkat akun di Amazon S3 untuk akun dalam organisasi.
- Firewall Manager menunjukkan cara mengonfigurasi kebijakan dan AWS WAF kebijakan grup keamanan untuk akun dalam organisasi.
- Inspector Organization mengonfigurasi Amazon Inspector dalam akun administrator yang didelegasikan untuk akun dan Wilayah yang diatur dalam organisasi.

Tahap 5: Lindungi data dalam perjalanan dan saat istirahat

Data bisnis dan pelanggan Anda adalah aset berharga yang perlu Anda lindungi. AWS menyediakan berbagai layanan dan fitur keamanan untuk melindungi data yang bergerak dan saat istirahat. Gunakan Amazon CloudFront dengan AWS Certificate Manager, seperti yang diuraikan di bagian

Akun Jaringan, untuk melindungi data yang bergerak yang dikumpulkan melalui internet. Untuk data yang bergerak dalam jaringan internal, gunakan Application Load Balancer dengan AWS Private Certificate Authority, seperti yang dijelaskan di bagian Akun aplikasi. AWS KMS dan AWS CloudHSM membantu Anda menyediakan manajemen kunci kriptografi untuk melindungi data saat istirahat.

Tahap 6: Mempersiapkan acara keamanan

Saat Anda mengoperasikan lingkungan TI Anda, Anda akan menghadapi peristiwa keamanan, yang merupakan perubahan dalam operasi sehari-hari lingkungan TI Anda yang menunjukkan kemungkinan pelanggaran kebijakan keamanan atau kegagalan kontrol keamanan. Keterlacakan yang tepat sangat penting sehingga Anda mengetahui peristiwa keamanan secepat mungkin. Sama pentingnya untuk bersiap melakukan triase dan menanggapi peristiwa keamanan semacam itu sehingga Anda dapat mengambil tindakan yang tepat sebelum acara keamanan meningkat. Persiapan membantu Anda melakukan triase acara keamanan dengan cepat untuk memahami potensi dampaknya.

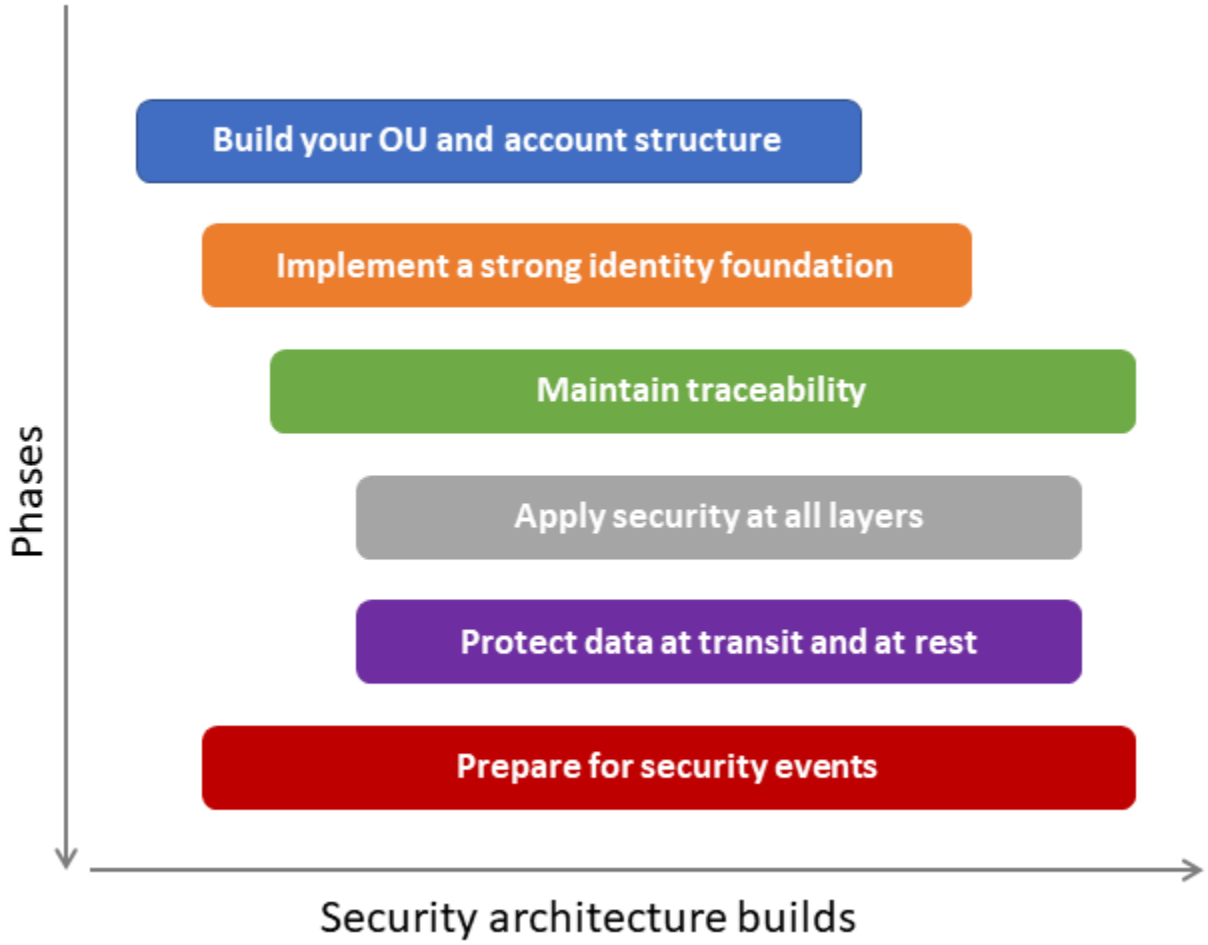
AWS SRA, melalui desain akun Security Tooling dan penyebaran layanan keamanan umum dalam semua Akun AWS, memberi Anda kemampuan untuk mendeteksi peristiwa keamanan di seluruh organisasi Anda. AWS Amazon Detective dalam akun Security Tooling membantu Anda melakukan triase peristiwa keamanan dan mengidentifikasi akar penyebabnya. Selama penyelidikan keamanan, Anda harus dapat meninjau log yang relevan untuk mencatat dan memahami ruang lingkup dan garis waktu penuh insiden tersebut. Log juga diperlukan untuk pembuatan peringatan ketika tindakan tertentu yang menarik terjadi. AWS SRA merekomendasikan akun Arsip Log pusat untuk penyimpanan yang tidak dapat diubah dari semua log keamanan dan operasional. Anda dapat melakukan kueri log dengan menggunakan Wawasan CloudWatch Log untuk data yang disimpan di grup CloudWatch log, serta Amazon Athena dan OpenSearch Amazon Service untuk data yang disimpan di Amazon S3. Gunakan Amazon Security Lake untuk secara otomatis memusatkan data keamanan dari AWS lingkungan, penyedia perangkat lunak sebagai layanan (SaaS), di tempat, dan penyedia cloud lainnya. Siapkan pelanggan di akun Security Tooling atau akun khusus apa pun, sebagaimana diuraikan oleh AWS SRA, untuk menanyakan log tersebut untuk diselidiki.

Respons Insiden Keamanan AWSmembantu Anda mengotomatiskan respons insiden keamanan, investigasi, dan remediasi. Ini menyediakan buku pedoman dan alur kerja pra-bangun untuk membantu Anda merespons peristiwa keamanan dengan cepat dan konsisten. Ketika fitur respons proaktif diaktifkan, Security Incident Response terintegrasi dengan Security Hub CSPM dan GuardDuty secara otomatis memicu alur kerja respons saat temuan keamanan terdeteksi. Layanan ini membantu Anda menstandarisasi dan mengotomatiskan proses respons insiden di seluruh

organisasi Anda. AWS Jika Anda memerlukan bantuan tambahan, Anda dapat membuka kasus yang didukung layanan untuk terlibat dengan Tim Respons Insiden AWS Pelanggan (CIRT).

Pertimbangan desain

- Anda harus mulai bersiap untuk mendeteksi dan menanggapi peristiwa keamanan sejak awal perjalanan cloud Anda. Untuk memanfaatkan sumber daya yang terbatas dengan lebih baik, tetapkan data dan kekritisan bisnis ke AWS sumber daya Anda sehingga ketika Anda mendeteksi peristiwa keamanan, Anda dapat memprioritaskan triase dan respons berdasarkan kekritisan sumber daya yang terlibat.
- Fase untuk membangun arsitektur keamanan cloud Anda, seperti yang dibahas di bagian ini, bersifat berurutan. Namun, Anda tidak perlu menunggu penyelesaian penuh dari satu fase sebelum memulai fase berikutnya. Kami menyarankan Anda mengadopsi pendekatan berulang, di mana Anda mulai mengerjakan beberapa fase secara paralel dan mengembangkan setiap fase saat Anda mengembangkan postur keamanan cloud Anda. Saat Anda melewati fase yang berbeda, desain Anda akan berkembang. Pertimbangkan untuk menyesuaikan urutan yang disarankan yang ditunjukkan pada diagram berikut dengan kebutuhan khusus Anda.



Contoh implementasi

Pustaka kode AWS SRA menyediakan contoh implementasi Organisasi Detektif, yang secara otomatis mengaktifkan Amazon Detective dengan mendelegasikan administrasi ke akun (misalnya, Audit atau Alat Keamanan) dan mengonfigurasi Detektif untuk akun yang ada dan yang akan datang. AWS Organizations

AWS Daftar periksa praktik terbaik SRA

Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

Bagian ini menyaring praktik terbaik AWS SRA yang dirinci di seluruh panduan ini ke dalam daftar periksa yang dapat Anda ikuti saat Anda membangun versi arsitektur keamanan Anda. AWS Gunakan daftar ini sebagai titik referensi dan bukan sebagai pengganti untuk meninjau panduan. Daftar periksa dikelompokkan berdasarkan. Layanan AWSJika Anda ingin memvalidasi AWS lingkungan yang ada secara terprogram terhadap daftar periksa praktik terbaik AWS SRA, Anda dapat menggunakan Verifikasi SRA.

SRA Verify adalah alat penilaian keamanan yang membantu Anda menilai keselarasan organisasi Anda dengan AWS SRA di beberapa Akun AWS dan Wilayah. Ini langsung memetakan ke rekomendasi AWS SRA dengan memberikan pemeriksaan otomatis yang memvalidasi implementasi Anda terhadap panduan AWS SRA. Alat ini membantu Anda memverifikasi bahwa layanan keamanan Anda dikonfigurasi dengan benar sesuai dengan arsitektur referensi. Ini memberikan temuan terperinci dan langkah-langkah perbaikan yang dapat ditindaklanjuti untuk membantu memastikan bahwa AWS lingkungan Anda mengikuti praktik terbaik keamanan. Verifikasi SRA dirancang untuk berjalan AWS CodeBuild di akun audit organisasi (Security Tooling). Anda juga dapat menjalankannya secara lokal atau memperluasnya dengan menggunakan pustaka Verifikasi SRA.

> **Note**
>
> Verifikasi SRA berisi pemeriksaan untuk beberapa layanan, tetapi mungkin tidak berisi cek untuk setiap pertimbangan AWS SRA. Untuk informasi lebih lanjut, tinjau panduan di perpustakaan AWS SRA.

AWS Organizations

- AWS Organizations diaktifkan dengan semua fitur.
- Kebijakan kontrol layanan (SCPs) digunakan untuk menentukan pedoman kontrol akses untuk prinsipal IAM.

- Kebijakan kontrol sumber daya (RCPs) digunakan untuk menentukan pedoman kontrol akses untuk AWS sumber daya.
- Kebijakan deklaratif digunakan untuk mendeklarasikan dan menerapkan konfigurasi yang Anda inginkan secara terpusat pada skala tertentu Layanan AWS di seluruh organisasi Anda.
- Tiga dasar OUs dibuat (Keamanan, Infrastruktur, dan Beban Kerja) ke akun anggota grup yang menyediakan layanan dasar.
- Akun Security Tooling dibuat di bawah Security OU. Akun ini menyediakan manajemen terpusat layanan AWS keamanan dan alat keamanan pihak ketiga lainnya.
- Akun Arsip Log dibuat di bawah Keamanan OU. Akun ini menyediakan repositori log pusat Layanan AWS dan log aplikasi yang dikontrol ketat.
- Akun Jaringan dibuat di bawah Infrastruktur OU. Akun ini mengelola gateway antara aplikasi Anda dan internet yang lebih luas. Ini mengisolasi layanan jaringan, konfigurasi, dan operasi dari beban kerja aplikasi individu, keamanan, dan infrastruktur lainnya.
- Akun Layanan Bersama dibuat di bawah Infrastruktur OU. Akun ini mendukung layanan yang digunakan beberapa aplikasi dan tim untuk memberikan hasil mereka.
- Akun Aplikasi dibuat di bawah Workloads OU. Akun ini menampung infrastruktur dan layanan utama untuk menjalankan dan memelihara aplikasi perusahaan. Panduan ini memberikan representasi, tetapi di dunia nyata akan ada beberapa akun OUs dan anggota yang dipisahkan oleh aplikasi, lingkungan pengembangan, dan pertimbangan keamanan lainnya.
- Informasi kontak alternatif untuk penagihan, operasi, dan keamanan untuk semua akun anggota dikonfigurasi.

AWS CloudTrail

- Jejak organisasi dikonfigurasi yang memungkinkan pengiriman acara CloudTrail manajemen di akun manajemen dan semua akun anggota dalam suatu AWS organisasi.
- Jejak organisasi dikonfigurasi sebagai jejak Multi-wilayah.
- Jejak organisasi dikonfigurasi untuk menangkap peristiwa dari sumber daya global.
- Jalur tambahan untuk menangkap peristiwa data tertentu dikonfigurasi seperlunya untuk memantau aktivitas AWS sumber daya yang sensitif.
- Akun Security Tooling ditetapkan sebagai administrator yang didelegasikan dari jejak organisasi.
- Jejak organisasi dikonfigurasi agar diaktifkan secara otomatis untuk semua akun anggota baru.

- Jejak organisasi dikonfigurasi untuk mempublikasikan log ke bucket S3 terpusat yang di-host di akun Arsip Log.
- Jejak organisasi memiliki validasi file log yang diaktifkan untuk memverifikasi integritas file log.
- Jejak organisasi terintegrasi dengan CloudWatch Log untuk penyimpanan log.
- Jejak organisasi dienkripsi dengan menggunakan kunci yang dikelola pelanggan.
- Bucket S3 pusat yang digunakan untuk repositori log di akun Arsip Log dienkripsi dengan kunci yang dikelola pelanggan.
- Bucket S3 pusat yang digunakan untuk repositori log di akun Log Archive dikonfigurasi dengan S3 Object Lock untuk kekekalan.
- Pembuatan versi diaktifkan untuk bucket S3 pusat yang digunakan untuk repositori log di akun Arsip Log.
- Bucket S3 pusat yang digunakan untuk repositori log di akun Arsip Log memiliki kebijakan sumber daya yang ditetapkan yang membatasi unggahan objek hanya berdasarkan jejak organisasi melalui sumber daya Amazon Resource Name (ARN).

AWS Security Hub CSPM

- Security Hub CSPM diaktifkan untuk semua akun anggota dan akun manajemen.
- AWS Config diaktifkan untuk semua akun anggota sebagai prasyarat untuk Security Hub CSPM.
- Akun Security Tooling ditetapkan sebagai administrator yang didelegasikan dari Security Hub CSPM.
- Amazon GuardDuty dan Amazon Detective memiliki akun administrator yang didelegasikan sama dengan Security Hub CSPM untuk integrasi layanan yang lancar.
- Konfigurasi pusat digunakan untuk mengatur dan mengelola CSPM Security Hub di beberapa Akun AWS dan. Wilayah AWS
- Semua akun OU dan anggota ditetapkan sebagai dikelola secara terpusat oleh administrator yang didelegasikan dari Security Hub CSPM.
- Security Hub CSPM diaktifkan secara otomatis untuk semua akun anggota baru.
- Security Hub CSPM secara otomatis diaktifkan untuk konfigurasi standar baru.
- Temuan CSPM Security Hub dari semua Wilayah dikumpulkan ke satu Wilayah asal.
- Temuan CSPM Security Hub dari semua akun anggota dikumpulkan dalam akun Security Tooling.
- Standar AWS Foundational Best Practices (FSBP) di Security Hub CSPM diaktifkan untuk semua akun anggota.

- Standar CIS AWS Foundation Benchmark di Security Hub CSPM diaktifkan untuk semua akun anggota.
- Standar CSPM Security Hub lainnya diaktifkan sebagaimana berlaku.
- Aturan otomatisasi CSPM Security Hub digunakan untuk memperkaya temuan dengan konteks sumber daya.
- Fitur respons dan remediasi otomatis Security Hub CSPM digunakan untuk membuat EventBridge aturan khusus untuk mengambil tindakan otomatis terhadap temuan tertentu.

AWS Config

- AWS Config Perekam diaktifkan untuk semua akun anggota dan akun manajemen.
- AWS Config Perekam diaktifkan untuk semua Wilayah.
- Bucket saluran AWS Config pengiriman S3 terpusat di akun Arsip Log.
- Akun administrator AWS Config yang didelegasikan diatur ke akun Security Tooling.
- AWS Config memiliki agregator organisasi yang disiapkan. Agregator mencakup semua Wilayah.
- AWS Config paket kesesuaian disebarkan secara seragam ke semua akun anggota dari akun administrator yang didelegasikan.
- AWS Config Temuan aturan secara otomatis dikirim ke Security Hub CSPM.

Amazon GuardDuty

- GuardDuty detektor diaktifkan untuk semua akun anggota dan akun manajemen.
- GuardDuty detektor diaktifkan untuk semua Wilayah.
- GuardDuty detektor diaktifkan secara otomatis untuk semua akun anggota baru.
- GuardDuty administrasi yang didelegasikan diatur ke akun Security Tooling.
- GuardDuty Sumber data dasar seperti peristiwa CloudTrail manajemen, log aliran VPC, dan log kueri DNS Route 53 Resolver diaktifkan.
- GuardDuty Perlindungan S3 diaktifkan.
- GuardDuty Perlindungan Malware untuk volume EBS diaktifkan.
- GuardDuty Perlindungan Malware untuk S3 diaktifkan.
- GuardDuty Perlindungan RDS diaktifkan.
- GuardDuty Perlindungan Lambda diaktifkan.

- GuardDuty Perlindungan EKS diaktifkan.
- GuardDuty EKS Runtime Monitoring diaktifkan.
- GuardDuty Deteksi Ancaman Diperpanjang diaktifkan.
- GuardDuty temuan diekspor ke bucket S3 pusat di akun Log Archive untuk retensi.

IAM

- Pengguna IAM tidak digunakan.
- Manajemen terpusat akses root untuk akun anggota diberlakukan.
- Tugas pengguna root istimewa terpusat untuk akun manajemen diberlakukan dari administrator yang didelegasikan.
- Manajemen akses root terpusat didelegasikan ke akun Security Tooling.
- Semua kredensi root akun anggota dihapus.
- Semua kebijakan Akun AWS kata sandi anggota dan manajemen ditetapkan sesuai dengan standar keamanan organisasi.
- Penasihat akses IAM digunakan untuk meninjau informasi yang terakhir digunakan untuk grup, pengguna, peran, dan kebijakan IAM.
- Batas izin digunakan untuk membatasi izin maksimum yang mungkin untuk peran IAM.

IAM Access Analyzer

- IAM Access Analyzer diaktifkan untuk semua akun anggota dan akun manajemen.
- Administrator yang didelegasikan IAM Access Analyzer diatur ke akun Security Tooling.
- Penganalisis akses eksternal IAM Access Analyzer dikonfigurasi dengan zona kepercayaan organisasi di setiap Wilayah.
- Penganalisis akses eksternal IAM Access Analyzer dikonfigurasi dengan zona kepercayaan akun di setiap Wilayah.
- Penganalisis akses internal IAM Access Analyzer dikonfigurasi dengan zona kepercayaan organisasi di setiap Wilayah.
- Penganalisis akses internal IAM Access Analyzer dikonfigurasi dengan zona kepercayaan akun di setiap Wilayah.
- IAM Access Analyzer penganalisis akses yang tidak digunakan untuk akun saat ini dibuat.

- IAM Access Analyzer penganalisis akses yang tidak digunakan untuk organisasi saat ini dibuat.

Amazon Detective

- Detektif diaktifkan untuk semua akun anggota.
- Detektif diaktifkan secara otomatis untuk semua akun anggota baru.
- Detektif diaktifkan untuk semua Wilayah.
- Administrator yang didelegasikan Detektif diatur ke akun Security Tooling.
- Administrator delegasi Detektif GuardDuty, dan Security Hub CSPM diatur ke akun Security Tooling yang sama.
- Detective terintegrasi dengan Security Lake untuk penyimpanan dan analisis log mentah.
- Detektif terintegrasi dengan GuardDuty untuk menelan temuan.
- Detective menelan log audit Amazon EKS untuk analisis.
- Detective menelan log CSPM Security Hub untuk analisis.

AWS Firewall Manager

- Kebijakan keamanan Firewall Manager ditetapkan.
- Administrator yang didelegasikan oleh Firewall Manager diatur ke akun Security Tooling.
- AWS Config diaktifkan sebagai prasyarat.
- Beberapa administrator Firewall Manager diatur dengan cakupan terbatas per OU, akun, dan Wilayah.
- Kebijakan AWS WAF keamanan Firewall Manager didefinisikan.
- Kebijakan logging AWS WAF terpusat Firewall Manager didefinisikan.
- Kebijakan keamanan lanjutan Firewall Manager Shield ditentukan.
- Kebijakan keamanan grup keamanan Firewall Manager didefinisikan.

Amazon Inspector

- Amazon Inspector diaktifkan untuk semua akun anggota.
- Amazon Inspector diaktifkan secara otomatis untuk setiap akun anggota baru.
- Administrator yang didelegasikan Amazon Inspector disetel ke akun Security Tooling.

- Pemindaian EC2 kerentanan Amazon Inspector diaktifkan.
- Pemindaian kerentanan gambar Amazon Inspector ECR diaktifkan.
- Fungsi Amazon Inspector Lambda dan pemindaian kerentanan lapisan diaktifkan.
- Pemindaian kode Amazon Inspector Lambda diaktifkan.
- Pemindaian keamanan kode Amazon Inspector diaktifkan.

Amazon Macie

- Macie diaktifkan untuk akun anggota yang berlaku.
- Macie diaktifkan secara otomatis untuk akun anggota baru yang berlaku.
- Administrator yang didelegasikan Macie diatur ke akun Security Tooling.
- Temuan Macie diekspor ke bucket S3 pusat di akun Arsip log.
- Bucket S3 yang menyimpan temuan Macie dienkripsi dengan kunci yang dikelola pelanggan.
- Kebijakan dan kebijakan klasifikasi Macie dipublikasikan ke Security Hub CSPM.

Amazon Security Lake

- Konfigurasi organisasi Security Lake diaktifkan.
- Administrator yang didelegasikan Security Lake diatur ke akun Security Tooling.
- Konfigurasi organisasi Security Lake diaktifkan untuk akun anggota baru.
- Akun Security Tooling diatur sebagai pelanggan akses data untuk melakukan analisis log.
- Akun Security Tooling diatur sebagai pelanggan kueri data untuk melakukan analisis log.
- Sumber log CloudTrail manajemen diaktifkan untuk Security Lake di semua atau akun anggota aktif tertentu.
- Sumber log aliran VPC diaktifkan untuk Security Lake di semua atau akun anggota aktif yang ditentukan.
- Sumber log Route 53 diaktifkan untuk Security Lake di semua atau akun anggota aktif yang ditentukan.
- CloudTrail peristiwa data untuk sumber log S3 diaktifkan untuk Security Lake di semua atau akun anggota aktif tertentu.
- Sumber log eksekusi Lambda diaktifkan untuk Security Lake di semua atau akun anggota aktif tertentu.

- Sumber log audit Amazon EKS diaktifkan untuk Security Lake di semua atau akun anggota aktif yang ditentukan.
- Sumber log temuan Security Hub diaktifkan untuk Security Lake di semua atau akun anggota aktif yang ditentukan.
- Sumber AWS WAF log diaktifkan untuk Security Lake di semua atau akun anggota aktif yang ditentukan.
- Antrian Security Lake SQS di akun administrator yang didelegasikan dienkripsi dengan kunci yang dikelola pelanggan.
- Antrian surat mati Security Lake SQS di akun administrator yang didelegasikan dienkripsi dengan kunci yang dikelola pelanggan.
- Bucket Security Lake S3 dienkripsi dengan kunci yang dikelola pelanggan.
- Bucket Security Lake S3 memiliki kebijakan sumber daya yang membatasi akses langsung hanya oleh Security Lake.

AWS WAF

- Semua CloudFront distribusi terkait dengan AWS WAF.
- Semua Amazon API Gateway REST APIs dikaitkan dengan AWS WAF.
- Semua Application Load Balancers terkait dengan. AWS WAF
- Semua AWS AppSync APIs GraphQL terkait dengan. AWS WAF
- Semua kumpulan pengguna Amazon Cognito dikaitkan dengan. AWS WAF
- Semua AWS App Runner layanan terkait dengan AWS WAF.
- Semua Akses Terverifikasi AWS contoh terkait dengan AWS WAF.
- Semua AWS Amplify aplikasi terkait dengan AWS WAF.
- AWS WAF logging diaktifkan.
- AWS WAF log dipusatkan dalam bucket S3 di akun Arsip Log.

AWS Shield Advanced

- Langganan Shield Advanced diaktifkan dan diatur untuk perpanjangan otomatis untuk semua akun aplikasi yang memiliki sumber daya yang menghadap publik.
- Shield Advanced dikonfigurasi untuk semua CloudFront distribusi.

- Shield Advanced dikonfigurasi untuk semua Application Load Balancer.
- Shield Advanced dikonfigurasi untuk semua Network Load Balancer.
- Shield Advanced dikonfigurasi untuk semua zona yang dihosting Route 53.
- Shield Advanced dikonfigurasi untuk semua alamat IP Elastis.
- Shield Advanced dikonfigurasi untuk semua Akselerator Global.
- CloudWatch alarm dikonfigurasi untuk CloudFront dan sumber daya Route 53 yang dilindungi oleh Shield Advanced.
- Akses Shield Response Team (SRT) dikonfigurasi.
- Keterlibatan proaktif Shield Advanced diaktifkan.
- Kontak keterlibatan proaktif Shield Advanced dikonfigurasi.
- Sumber daya yang dilindungi Shield Advanced memiliki AWS WAF aturan khusus yang dikonfigurasi.
- Sumber daya yang dilindungi Shield Advanced mengaktifkan mitigasi lapisan aplikasi DDo S otomatis.

AWS Respon Insiden Keamanan

- AWS Security Incident Response diaktifkan untuk seluruh AWS organisasi.
- Administrator yang didelegasikan AWS Security Incident Response disetel ke akun Security Tooling.
- Respons proaktif dan alur kerja triaging peringatan diaktifkan.
- AWS Tindakan penahanan Customer Incident Response Team (CIRT) diotorisasi.

AWS Audit Manager

- Audit Manager diaktifkan untuk semua akun anggota.
- Audit Manager diaktifkan secara otomatis untuk akun anggota baru.
- Administrator yang didelegasikan Audit Manager diatur ke akun Security Tooling.
- AWS Config diaktifkan sebagai prasyarat untuk Audit Manager.
- Kunci yang dikelola pelanggan digunakan untuk data yang disimpan di Audit Manager.
- Tujuan laporan penilaian default dikonfigurasi.

Sumber daya IAM

Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

Meskipun AWS Identity and Access Management (IAM) bukan layanan yang termasuk dalam diagram arsitektur tradisional, ia menyentuh setiap aspek AWS organisasi, Akun AWS, dan. Layanan AWS Anda tidak dapat menerapkan apa pun Layanan AWS tanpa membuat entitas IAM dan memberikan izin terlebih dahulu. Penjelasan lengkap tentang IAM berada di luar cakupan dokumen ini, tetapi bagian ini memberikan ringkasan penting dari rekomendasi praktik terbaik dan petunjuk ke sumber daya tambahan.

- Untuk praktik terbaik IAM, lihat Praktik terbaik keamanan di IAM dalam AWS dokumentasi, artikel IAM di blog AWS Keamanan, dan AWS presentasi RE:Invent.
- Pilar keamanan Well-Architected menguraikan langkah-langkah kunci dalam proses manajemen izin: menentukan pagar pembatas izin, memberikan akses hak istimewa paling sedikit, menganalisis akses publik dan lintas akun, berbagi sumber daya dengan aman, mengurangi izin terus menerus, dan membuat proses akses darurat. AWS
- Tabel berikut dan catatan yang menyertainya memberikan gambaran tingkat tinggi tentang panduan yang direkomendasikan tentang jenis kebijakan izin IAM yang tersedia dan cara menggunakannya dalam arsitektur keamanan Anda. Untuk mempelajari lebih lanjut, lihat video AWS re:Invent 2020 tentang memilih campuran kebijakan IAM yang tepat.

Kasus penggunaan atau kebijakan	Efek	Dikelola oleh	Tujuan	Berkaitan dengan	Mempengaruhi	Dikerahkan di
Kebijakan kontrol layanan (SCPs)	Membatasi	Tim pusat, seperti platform atau tim keamanan [1]	Pagar pembatas, tata kelola	Organisasi, OU, akun	Semua kepala sekolah di Organisasi, OU, dan akun	Akun Manajemen Org [2]

Kebijakan kontrol sumber daya (RCPs)	Membatasi	Tim pusat, seperti platform atau tim keamanan [1]	Pagar pembatas, tata kelola	Organisasi, OU, akun	Sumber daya di akun anggota [12]	Akun Manajemen Org [2]
Kebijakan otomatisasi akun dasar (peran IAM yang digunakan oleh platform untuk mengoperasikan akun)	Hibah dan batasi	Tim pusat, seperti platform, keamanan, atau tim IAM [1]	Izin untuk peran otomatisasi non-beban kerja (dasar) [3]	Akun tunggal [4]	Prinsipal yang digunakan oleh otomatisasi dalam akun anggota	Akun anggota
Kebijakan manusia dasar (peran IAM yang memberikan izin kepada pengguna untuk melakukan pekerjaan mereka)	Hibah dan batasi	Tim pusat, seperti platform, keamanan, atau tim IAM [1]	Izin untuk peran manusia [5]	Akun tunggal [4]	Prinsipal federasi [5] dan pengguna IAM [6]	Akun anggota

Batas izin (izin maksimum yang dapat ditetapkan oleh pengembang yang diberdayakan ke prinsipal lain)	Membatasi	Tim pusat, seperti platform, keamanan, atau tim IAM [1]	Pagar pembatas untuk peran aplikasi (harus diterapkan)	Akun tunggal [4]	Peran individu untuk aplikasi atau beban kerja di akun ini [7]	Akun anggota
Kebijakan peran mesin untuk aplikasi (peran yang melekat pada infrastruktur yang digunakan oleh pengembang)	Hibah dan batasi	Delegasikan ke pengembang [8]	Izin untuk aplikasi atau beban kerja [9]	Akun tunggal	Prinsipal dalam akun ini	Akun anggota
Kebijakan sumber daya	Hibah dan batasi	Delegasikan ke pengembang [8,10]	Izin untuk sumber daya	Akun tunggal	Seorang kepala sekolah dalam sebuah akun [11]	Akun anggota

Manajemen pengguna root pusat	Hibah dan batasi	Tim pusat, seperti platform, keamanan, atau tim IAM [1]	Kelola pengguna root akun anggota secara terpusat dalam skala besar	Organisasi	Semua pengguna root di akun anggota	Akun manajemen organisasi, akun administrator yang didelegasikan

Catatan dari tabel:

1. Perusahaan memiliki banyak tim terpusat (seperti platform cloud, operasi keamanan, atau tim manajemen identitas dan akses) yang membagi tanggung jawab kontrol independen ini, dan peer review kebijakan satu sama lain. Contoh dalam tabel adalah placeholder. Anda perlu menentukan pemisahan tugas yang paling efektif untuk perusahaan Anda.
2. Untuk menggunakannya SCPs, Anda harus mengaktifkan semua fitur di dalamnya AWS Organizations.
3. Peran dan kebijakan dasar umum umumnya diperlukan untuk mengaktifkan otomatisasi, seperti izin untuk pipeline, alat penyebaran, alat pemantauan (misalnya, AWS Lambda dan Aturan AWS Config), dan izin lainnya. Konfigurasi ini biasanya dikirimkan saat akun disediakan.
4. Meskipun ini berkaitan dengan sumber daya (seperti peran atau kebijakan) dalam satu akun, mereka dapat direplikasi atau digunakan ke beberapa akun dengan menggunakan. AWS CloudFormation StackSets
5. Tentukan seperangkat inti peran manusia dasar dan kebijakan yang diterapkan ke semua akun anggota oleh tim pusat (seringkali selama penyediaan akun). Contohnya termasuk pengembang di tim platform, tim IAM, dan tim audit keamanan.
6. Gunakan federasi identitas (bukan pengguna IAM lokal) bila memungkinkan.
7. Batas izin digunakan oleh administrator yang didelegasikan. Kebijakan IAM ini menentukan izin maksimum dan mengesampingkan kebijakan lain (termasuk `"*:*"` kebijakan yang mengizinkan semua tindakan pada sumber daya). Batas izin harus diperlukan dalam kebijakan dasar manusia sebagai syarat untuk membuat peran (seperti peran kinerja beban kerja) dan untuk melampirkan kebijakan. Konfigurasi tambahan seperti SCPs menegakkan lampiran batas izin.
8. Ini mengasumsikan bahwa pagar pembatas yang cukup (misalnya, SCPs dan batas izin) telah diterapkan.

9. Kebijakan opsional ini dapat disampaikan selama penyediaan akun atau sebagai bagian dari proses pengembangan aplikasi. Izin untuk membuat dan melampirkan kebijakan ini akan diatur oleh izin pengembang aplikasi sendiri.
10. Selain izin akun lokal, tim terpusat (seperti tim platform cloud atau tim operasi keamanan) sering mengelola beberapa kebijakan berbasis sumber daya untuk mengaktifkan akses lintas akun untuk mengoperasikan akun (misalnya, untuk menyediakan akses ke bucket S3 untuk pencatatan).
11. Kebijakan IAM berbasis sumber daya dapat merujuk pada prinsipal apa pun di akun apa pun untuk mengizinkan atau menolak akses ke sumber dayanya. Bahkan dapat merujuk ke kepala sekolah anonim untuk mengaktifkan akses publik.
12. RCPs berlaku untuk sumber daya untuk subset. Layanan AWS Untuk informasi selengkapnya, lihat Daftar dukungan Layanan AWS tersebut RCPs dalam AWS Organizations dokumentasi.

Memastikan bahwa identitas IAM hanya memiliki izin yang diperlukan untuk serangkaian tugas yang digambarkan dengan baik sangat penting untuk mengurangi risiko penyalahgunaan izin yang berbahaya atau tidak disengaja. Membangun dan mempertahankan model hak istimewa terkecil membutuhkan rencana yang disengaja untuk terus memperbarui, mengevaluasi, dan mengurangi kelebihan hak istimewa. Berikut adalah beberapa rekomendasi tambahan untuk rencana itu:

- Gunakan model tata kelola organisasi Anda dan selera risiko yang ditetapkan untuk menetapkan pagar pembatas dan batas izin tertentu.
- Menerapkan hak istimewa terkecil melalui proses berulang yang terus-menerus. Ini bukan latihan satu kali.
- Gunakan SCPs untuk mengurangi risiko yang dapat ditindaklanjuti. Ini dimaksudkan untuk menjadi pagar pembatas yang luas, bukan kontrol yang ditargetkan secara sempit.
- Gunakan batas izin untuk mendelegasikan administrasi IAM dengan cara yang lebih aman.
  - Pastikan bahwa administrator yang didelegasikan melampirkan kebijakan batas IAM yang sesuai ke peran dan pengguna yang mereka buat.
- Sebagai defense-in-depth pendekatan (dalam hubungannya dengan kebijakan berbasis identitas), gunakan kebijakan IAM berbasis sumber daya untuk menolak akses luas ke sumber daya.
- Gunakan penasihat akses IAM, AWS CloudTrail, IAM Access Analyzer, dan perkakas terkait untuk secara teratur menganalisis penggunaan historis dan izin yang diberikan. Segera pulihkan izin berlebih yang jelas.
- Cakupan tindakan luas ke sumber daya tertentu jika berlaku alih-alih menggunakan tanda bintang sebagai wildcard untuk menunjukkan semua sumber daya.

- Menerapkan mekanisme untuk mengidentifikasi, meninjau, dan menyetujui pengecualian kebijakan IAM dengan cepat berdasarkan permintaan.

Repositori kode untuk AWS contoh SRA

Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

Untuk membantu Anda mulai membangun dan menerapkan panduan di AWS SRA, repositori infrastruktur sebagai kode (IAc) di https://github.com/aws-samples/aws-security-reference-architecture-examples menyertai panduan ini. Repositori ini berisi kode untuk membantu pengembang dan insinyur menyebarkan beberapa panduan dan pola arsitektur yang disajikan dalam dokumen ini. Kode ini diambil dari pengalaman langsung konsultan Layanan AWS Profesional dengan pelanggan. Template bersifat umum–tujuannya adalah untuk mengilustrasikan pola implementasi daripada memberikan solusi lengkap. Layanan AWS Konfigurasi dan penyebaran sumber daya sengaja sangat membatasi. Anda mungkin perlu memodifikasi dan menyesuaikan solusi ini agar sesuai dengan kebutuhan lingkungan dan keamanan Anda.

Repositori kode AWS SRA menyediakan contoh kode dengan keduanya AWS CloudFormation dan opsi penerapan Terraform. Pola solusi mendukung dua lingkungan: satu membutuhkan AWS Control Tower dan yang lainnya menggunakan AWS Organizations tanpa AWS Control Tower. Solusi dalam repositori ini yang membutuhkan AWS Control Tower telah diterapkan dan diuji dalam AWS Control Tower lingkungan dengan menggunakan AWS CloudFormation dan Kustomisasi untuk (CFCT). AWS Control Tower Solusi yang tidak memerlukan AWS Control Tower telah diuji dalam AWS Organizations lingkungan dengan menggunakan AWS CloudFormation. Solusi CFCT membantu pelanggan dengan cepat mengatur AWS lingkungan multi-akun yang aman berdasarkan praktik AWS terbaik. Ini membantu menghemat waktu dengan mengotomatiskan pengaturan lingkungan untuk menjalankan beban kerja yang aman dan terukur sambil menerapkan dasar keamanan awal melalui pembuatan akun dan sumber daya. AWS Control Tower juga menyediakan lingkungan dasar untuk memulai dengan arsitektur multi-akun, identitas dan manajemen akses, tata kelola, keamanan data, desain jaringan, dan logging. Solusi dalam repositori AWS SRA menyediakan konfigurasi keamanan tambahan untuk mengimplementasikan pola yang dijelaskan dalam dokumen ini.

Berikut adalah ringkasan solusi dalam repositori AWS SRA. Setiap solusi menyertakan `README.md` file dengan detail.

- Solusi CloudTrail Organisasi membuat jejak organisasi dalam akun Manajemen Org dan mendelegasikan administrasi ke akun anggota seperti akun Audit atau Perkakas Keamanan. Jejak ini dienkripsi dengan kunci terkelola pelanggan yang dibuat di akun Security Tooling dan

mengirimkan log ke bucket S3 di akun Arsip Log. Secara opsional, peristiwa data dapat diaktifkan untuk Amazon S3 AWS Lambda dan fungsi. Jejak organisasi mencatat peristiwa untuk semua orang Akun AWS di AWS organisasi sambil mencegah akun anggota memodifikasi konfigurasi.

- Solusi GuardDuty Organisasi memungkinkan Amazon GuardDuty dengan mendelegasikan administrasi ke akun Security Tooling. Ini mengkonfigurasi GuardDuty dalam akun Security Tooling untuk semua akun AWS organisasi yang ada dan yang akan datang. GuardDuty Temuan ini juga dienkripsi dengan kunci KMS dan dikirim ke bucket S3 di akun Log Archive.
- Solusi Organisasi CSPM Security Hub mengonfigurasi CSPM Security Hub dengan mendelegasikan administrasi ke akun Security Tooling. Ini mengonfigurasi CSPM Security Hub dalam akun Security Tooling untuk semua akun organisasi yang ada dan yang akan datang. AWS Solusi ini juga menyediakan parameter untuk menyinkronkan standar keamanan yang diaktifkan di semua akun dan Wilayah serta mengonfigurasi agregator Wilayah dalam akun Security Tooling. Sentralisasi Security Hub CSPM dalam akun Security Tooling memberikan pandangan lintas akun tentang kepatuhan standar keamanan dan temuan dari integrasi kedua dan pihak ketiga. Layanan AWS AWS Partner
- Solusi Inspector mengonfigurasi Amazon Inspector dalam akun administrator yang didelegasikan (Perkakas Keamanan) untuk semua akun dan Wilayah yang diatur di bawah organisasi. AWS
- Solusi Firewall Manager mengonfigurasi kebijakan AWS Firewall Manager keamanan dengan mendelegasikan administrasi ke akun Security Tooling dan mengonfigurasi Firewall Manager dengan kebijakan grup keamanan dan beberapa kebijakan. AWS WAF Kebijakan grup keamanan memerlukan grup keamanan maksimum yang diizinkan dalam VPC (ada atau dibuat oleh solusi), yang digunakan oleh solusi.
- Solusi Organisasi Macie memungkinkan Amazon Macie dengan mendelegasikan administrasi ke akun Security Tooling. Ini mengonfigurasi Macie dalam akun Security Tooling untuk semua akun organisasi yang ada dan yang akan datang AWS . Macie selanjutnya dikonfigurasi untuk mengirim hasil penemuannya ke bucket S3 pusat yang dienkripsi dengan kunci KMS.
- AWS Config:
  - Solusi Config Aggregator mengonfigurasi AWS Config agregator dengan mendelegasikan administrasi ke akun Security Tooling. Solusi tersebut kemudian mengonfigurasi AWS Config agregator dalam akun Security Tooling untuk semua akun yang ada dan yang akan datang di organisasi. AWS
  - Solusi Aturan Organisasi Paket Kesesuaian diterapkan Aturan AWS Config dengan mendelegasikan administrasi ke akun Security Tooling. Kemudian membuat paket kesesuaian organisasi dalam akun administrator yang didelegasikan untuk semua akun yang ada dan yang

akan datang di organisasi. AWS Solusinya dikonfigurasi untuk menerapkan templat sampel paket kesesuaian Praktik Terbaik Operasional untuk Enkripsi dan Manajemen Kunci.

  - Solusi AWS Config Control Tower Management Account memungkinkan AWS Config di akun AWS Control Tower manajemen dan memperbarui AWS Config agregator dalam akun Security Tooling yang sesuai. Solusinya menggunakan AWS Control Tower CloudFormation template untuk memungkinkan AWS Config sebagai referensi untuk memastikan konsistensi dengan akun lain dalam AWS organisasi.
- IAM:
  - Solusi Access Analyzer memungkinkan IAM Access Analyzer dengan mendelegasikan administrasi ke akun Security Tooling. Kemudian mengkonfigurasi IAM Access Analyzer tingkat organisasi dalam akun Security Tooling untuk semua akun yang ada dan yang akan datang di organisasi. AWS Solusi ini juga menerapkan IAM Access Analyzer ke semua akun anggota dan Wilayah untuk mendukung analisis izin tingkat akun.
  - Solusi Kebijakan Kata Sandi IAM memperbarui kebijakan Akun AWS kata sandi dalam semua akun dalam suatu AWS organisasi. Solusi ini menyediakan parameter untuk mengonfigurasi pengaturan kebijakan kata sandi untuk membantu Anda menyelaraskan dengan standar kepatuhan industri.
- Solusi Enkripsi EBS EC2 Default memungkinkan enkripsi Amazon EBS default tingkat akun di masing-masing Akun AWS dan AWS Region di organisasi. AWS Ini memberlakukan enkripsi volume dan snapshot EBS baru yang Anda buat. Misalnya, Amazon EBS mengenkripsi volume EBS yang dibuat saat Anda meluncurkan instance dan snapshot yang Anda salin dari snapshot yang tidak terenkripsi.
- Solusi Akses Publik Akun Blok S3 memungkinkan pengaturan tingkat akun Amazon S3 dalam Akun AWS masing-masing di organisasi. AWS Fitur Blokir Akses Publik Amazon S3 menyediakan pengaturan untuk titik akses, bucket, dan akun untuk membantu Anda mengelola akses publik ke sumber daya Amazon S3. Secara bawaan, bucket baru, titik akses, dan objek baru tidak mengizinkan akses publik. Namun, pengguna dapat memodifikasi kebijakan bucket, kebijakan titik akses, atau izin objek untuk memungkinkan akses publik. Amazon S3 Blokir Pengaturan Akses Publik mengesampingkan kebijakan dan izin ini sehingga Anda dapat membatasi akses publik ke sumber daya ini.
- Solusi Organisasi Detektif mengotomatiskan mengaktifkan Amazon Detective dengan mendelegasikan administrasi ke akun (seperti akun Audit atau Security Tooling) dan mengonfigurasi Detective untuk semua akun yang ada dan yang akan datang. AWS Organizations
- Solusi Shield Advanced mengotomatiskan penerapan AWS Shield Advanced untuk memberikan perlindungan DDo S yang ditingkatkan untuk aplikasi Anda. AWS

- Solusi AMI Bakery Organization membantu mengotomatiskan proses pembuatan dan pengelolaan gambar Amazon Machine Image (AMI) standar yang diperkeras. Ini memastikan konsistensi dan keamanan di seluruh AWS instans Anda, dan menyederhanakan tugas penerapan dan pemeliharaan.
- Solusi Patch Manager membantu merampingkan manajemen patch di beberapa Akun AWS. Anda dapat menggunakan solusi ini untuk memperbarui AWS Systems Manager Agen (Agen SSM) pada semua instans yang dikelola, dan untuk memindai dan menginstal patch keamanan penting dan penting serta perbaikan bug pada instance yang ditandai Windows dan Linux. Solusi ini juga mengonfigurasi pengaturan Konfigurasi Manajemen Host Default untuk mendeteksi pembuatan baru Akun AWS dan secara otomatis menerapkan solusi ke akun tersebut.

Kontributor

Penulis utama:

- Avik Mukherjie, Keamanan Senior SA AWS

Kontributor:

- Jason Hurst, Penyelidik Keamanan AWS Senior CIRT
- Abhishek Panday, Manajer Produk AWS Utama — Tech
- Itay Meller, Spesialis AWS Senior SA
- Jonathan VanKim, AWS Principal Security SA
- Josh Du Lac, Ahli Strategi Keamanan AWS Perusahaan
- James Thompson, Arsitek Solusi Senior AWS
- Jeremy Girven, Spesialis SA AWS
- Rodney Underkoffler, Spesialis Senior SA AWS
- Farhan Farooq, Arsitek Solusi Senior AWS
- Prashob Krishnan, Manajer Akun Teknis AWS
- Meg Peddada, Konsultan Keamanan Senior AWS
- Ashwin Phadke, Arsitek Solusi Senior AWS
- Sowjanya Rajavaram, Keamanan Senior SA AWS
- Tomek Jakubowski, Konsultan Senior AWS
- Arun Thomas, Arsitek Solusi AWS Senior
- Ross Warren, Arsitek Solusi AWS Produk
- Scott Conklin, Konsultan Senior AWS
- Ilya Epshteyn, Manajer AWS Senior, Solusi Identitas
- Michael Haken, Ahli Teknologi AWS Utama
- Mehial Mendrin, Konsultan Senior AWS
- Christopher Evensen, Manajer Akun Teknis AWS Senior

Meninjau:

- Eric Rose, Keamanan AWS Utama SA
- Manoj Kumar, Konsultan Pengiriman AWS

Penulisan teknis:

- Handan Selamoglu, Penulis Teknis Senior AWS

Lampiran: AWS keamanan, identitas, dan layanan kepatuhan

Mempengaruhi masa depan AWS Security Reference Architecture (AWS SRA) dengan mengambil survei singkat.

Untuk pengenalan atau penyegaran, lihat Keamanan, identitas, dan kepatuhan AWS di AWS situs web untuk daftar Layanan AWS yang membantu Anda mengamankan beban kerja dan aplikasi di cloud. Layanan ini dikelompokkan menjadi lima kategori: perlindungan data, manajemen identitas & akses, perlindungan jaringan & aplikasi, deteksi ancaman & pemantauan berkelanjutan, dan kepatuhan & privasi data.

Perlindungan data — AWS menyediakan layanan yang membantu Anda melindungi data, akun, dan beban kerja Anda dari akses yang tidak sah.

- Amazon Macie — Temukan, klasifikasikan, dan lindungi data sensitif dengan fitur keamanan yang didukung pembelajaran mesin.
- AWS KMS— Buat dan kendalikan kunci yang digunakan untuk mengenkripsi data Anda.
- AWS CloudHSM— Kelola modul keamanan perangkat keras Anda (HSMs) di AWS Cloud.
- AWS Certificate Manager— Menyediakan, mengelola, dan menyebarkan SSL/TLS sertifikat untuk digunakan dengan Layanan AWS.
- AWS Secrets Manager— Putar, kelola, dan ambil kredenal basis data, kunci API, dan rahasia lainnya melalui siklus hidupnya.

Manajemen identitas & akses — layanan AWS identitas memungkinkan Anda mengelola identitas, sumber daya, dan izin dengan aman dalam skala besar.

- IAM - Kontrol akses Layanan AWS dan sumber daya dengan aman.
- IAM Identity Center - Mengelola akses SSO secara terpusat ke beberapa aplikasi bisnis Akun AWS .
- Amazon Cognito — Tambahkan pendaftaran pengguna, masuk, dan kontrol akses ke web dan aplikasi seluler Anda.
- AWS Directory Service— Gunakan Microsoft Active Directory yang dikelola di AWS Cloud.

- AWS RAM— Bagikan AWS sumber daya secara sederhana dan aman.
- AWS Organizations— Menerapkan manajemen berbasis kebijakan untuk beberapa. Akun AWS
- Izin Terverifikasi Amazon — Kelola izin dan otorisasi yang dapat diskalakan dan berbutir halus di aplikasi kustom Anda.

Perlindungan jaringan & aplikasi — Kategori layanan ini memungkinkan Anda untuk menegakkan kebijakan keamanan berbutir halus di titik-titik kontrol jaringan di seluruh organisasi Anda. Layanan AWS membantu Anda memeriksa dan memfilter lalu lintas untuk membantu mencegah akses sumber daya yang tidak sah di batas tingkat host, tingkat jaringan, dan tingkat aplikasi.

- AWS Shield— Lindungi aplikasi web Anda yang berjalan AWS dengan perlindungan S terkelola DDo.
- AWS WAF— Lindungi aplikasi web Anda dari eksploitasi web umum, dan pastikan ketersediaan dan keamanan.
- AWS Firewall Manager— Konfigurasikan dan kelola AWS WAF aturan di seluruh Akun AWS dan aplikasi dari lokasi pusat.
- AWS Systems Manager— Konfigurasikan dan kelola Amazon EC2 dan sistem lokal untuk menerapkan patch OS, membuat gambar sistem yang aman, dan mengonfigurasi sistem operasi yang aman.
- Amazon VPC - Menyediakan bagian yang terisolasi secara logis AWS di mana Anda dapat meluncurkan AWS sumber daya di jaringan virtual yang Anda tentukan.
- AWS Network Firewall— Menyebarkan perlindungan jaringan penting untuk Anda. VPCs
- Amazon Route 53 DNS Firewall — Lindungi permintaan DNS keluar Anda dari Anda. VPCs
- Akses Terverifikasi AWS— Menyediakan akses aman ke aplikasi Anda tanpa memerlukan jaringan pribadi virtual (VPNs).
- Amazon VPC Lattice — Sederhanakan service-to-service konektivitas, keamanan, dan pemantauan.

Deteksi ancaman & pemantauan berkelanjutan — layanan AWS pemantauan dan deteksi memberikan panduan untuk membantu mengidentifikasi potensi insiden keamanan di AWS lingkungan Anda.

- AWS Security Hub CSPM— Lihat dan kelola peringatan keamanan dan otomatiskan pemeriksaan kepatuhan dari lokasi pusat.

- AWS Security HubMengkorelasikan dan memperkaya temuan keamanan untuk memprioritaskan masalah keamanan kritis di seluruh akun Anda dan. Wilayah AWS
- Amazon GuardDuty — Lindungi Akun AWS beban kerja Anda dengan deteksi ancaman cerdas dan pemantauan berkelanjutan.
- Amazon Inspector — Mengotomatiskan penilaian keamanan untuk membantu meningkatkan keamanan dan kepatuhan aplikasi yang digunakan. AWS
- AWS Config— Rekam dan evaluasi konfigurasi AWS sumber daya Anda untuk memungkinkan audit kepatuhan, pelacakan perubahan sumber daya, dan analisis keamanan.
- Aturan AWS ConfigBuat aturan yang secara otomatis mengambil tindakan sebagai respons terhadap perubahan di lingkungan Anda, seperti mengisolasi sumber daya, memperkaya peristiwa dengan data tambahan, atau memulihkan konfigurasi ke keadaan baik yang diketahui.
- Respons Insiden Keamanan AWS— Otomatiskan respons insiden keamanan, investigasi, dan remediasi dengan buku pedoman dan alur kerja yang sudah dibuat sebelumnya.
- AWS CloudTrail— Lacak aktivitas pengguna dan penggunaan API untuk memungkinkan tata kelola dan audit operasional dan risiko Anda. Akun AWS
- Amazon Detective — Menganalisis dan memvisualisasikan data keamanan untuk dengan cepat sampai ke akar penyebab masalah keamanan potensial.
- AWS LambdaJalankan kode tanpa menyediakan atau mengelola server sehingga Anda dapat menskalakan respons terprogram dan otomatis terhadap insiden.

Kepatuhan & privasi data — AWS memberi Anda pandangan komprehensif tentang status kepatuhan Anda dan terus memantau lingkungan Anda dengan menggunakan pemeriksaan kepatuhan otomatis berdasarkan praktik AWS terbaik dan standar industri yang diikuti bisnis Anda.

- AWS Artifact— Gunakan portal swalayan tanpa biaya untuk mendapatkan akses sesuai permintaan ke laporan AWS keamanan dan kepatuhan dan pilih perjanjian online.
- AWS Audit Manager— Terus audit AWS penggunaan Anda untuk menyederhanakan cara Anda menilai risiko dan kepatuhan terhadap peraturan dan standar industri.

Riwayat dokumen

Tabel berikut menjelaskan perubahan signifikan pada panduan ini. Jika Anda ingin diberi tahu tentang pembaruan masa depan, Anda dapat berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Merestrukturisasi dan pembaruan konten	• Menambahkan panduan untuk Security Hub dan AWS Nitro Enclave. • Merestrukturisasi AWS SRA untuk fokus pada arsitektur inti dan memindahkan bagian penyelaman mendalam ke panduan terpisah untuk manajemen identitas, keamanan perimeter, forensik cyber, AI generatif, dan IoT. • Panduan yang ada diperbarui untuk menyertakan detail tambahan untuk AWS CloudTrail, AWS Config, Detektif Amazon, AWS Firewall Manager Amazon, IAM Access Analyzer GuardDuty, Amazon Security Lake AWS Shield Advanced, dan. AWS Audit Manager	Desember 22, 2025
Pembaruan besar	• Menambahkan informasi tentang manajemen akses pengguna root terpusat IAM baru, kebijakan kontrol	Agustus 29, 2025

sumber daya (RCPs), dan kebijakandeklaratif.

- Referensi CSPM Security Hub yang diperbarui ke CSPM Security Hub baru.
- Termasuk fitur layanan baru untuk Amazon GuardDuty dan Security Hub CSPM.
- Menambahkan panduan Respons Insiden Keamanan AWS layanan.
- Panduan penyelama n mendalam IAM yang diperbarui untuk menyertak an VPC Lattice machine-to-machine untuk manajemen identitas.
- Menambahkan panduan menyelam mendalam baru: SRA untuk IoT.

Penambahan dan klarifikasi	• Di bagian akun Security Tooling, perbarui AWS KMS panduan. • Di bagian Manajemen identitas Pelanggan, memperluas informasi tentang otorisasi API Gateway. • Memperbarui bagian Generative AI untuk menambahkan pertimbangan desain untuk OU dan desain akun. • Di bagian repositori kode AWS SRA, menambahkan informasi tentang solusi Manajemen Patch baru.	September 12, 2024

Pembaruan besar	• Menambahkan dua bagian untuk panduan arsitektur deep dive: Generative AI menggunakan Amazon Bedrock dan manajemen Identity. • Memperbarui AWS Identity and Access Management Access Analyzer, Amazon Detective, Amazon Inspector, AWS Artifact, AWS Config, Amazon Security Lake AWS Security Hub CSPM,, dan bagian CloudFrontAmazon dengan fitur layanan baru. • Memperbarui bagian repositori kode AWS SRA untuk menyertakan opsi penerapan Terraform baru dan penambahan dan solusi AMI Bakery. AWS Shield Advanced	Juni 7, 2024

Pembaruan besar	• Memperbarui bagian Akun Jaringan dan akun Aplikasi untuk menambahkan panduan arsitektur untuk Izin Terverifikasi Amazon, Akses Terverifikasi AWS, dan Amazon VPC Lattice. • Menambahkan panduan arsitektur menyelam mendalam berdasarkan fungsionalitas keamanan. • Menambahkan panduan baru tentang bagaimana Layanan AWS penggunaan AI/ML untuk memberikan hasil keamanan yang lebih baik. • Menambahkan panduan tentang bagaimana merencanakan arsitektur keamanan Anda secara bertahap.	November 4, 2023
Penambahan Danau Keamanan	Memperbarui akun Perkakas Keamanan dan bagian akun Arsip Log untuk menambahkan panduan desain yang terkait dengan Amazon Security Lake.	September 22, 2023

Pembaruan kecil	• Panduan yang ada diperbarui untuk mencermin kan Layanan AWS fitur baru dan praktik terbaik. • Panduan arsitektur yang diperbarui untuk AWS CloudTrail, AWS IAM Identity Center, dan keamanan tepi.	10 Mei 2023
Survei	Menambahkan survei singkat untuk mendapatkan pemahaman yang lebih baik tentang bagaimana Anda menggunakan AWS SRA di organisasi Anda.	14 Desember 2022
File sumber untuk diagram arsitektur referensi	Di bagian Arsitektur Referensi AWS Keamanan, tambahkan file unduhan yang menyediak an diagram arsitektur untuk panduan ini dalam format yang dapat diedit PowerPoint .	17 November 2022
Pembaruan untuk bagian Yayasan Keamanan	Di bagian Yayasan Keamanan, memperbar ui informasi tentang pilar Well-Architected Framework dan prinsip-prinsip desain keamanan.	September 27, 2022

Penambahan dan pembaruan utama	• Menambahkan informasi tentang cara menggunakan AWS SRA dan pedoman implementasi utama. • Menambahkan panduan arsitektur untuk tambahan Layanan AWS seperti AWS Artifact, Amazon Inspector ,, AWS RAM Amazon Route 53,,, AWS Control Tower, Amazon Cognito AWS Audit Manager Directory Service, dan Network Access Analyzer. • Panduan yang ada diperbarui untuk mencerminkan Layanan AWS fitur baru dan praktik terbaik.	25 Juli 2022
—	Publikasi awal	23 Juni 2021

AWS Glosarium Panduan Preskriptif

Berikut ini adalah istilah yang umum digunakan dalam strategi, panduan, dan pola yang disediakan oleh Panduan AWS Preskriptif. Untuk menyarankan entri, silakan gunakan tautan Berikan umpan balik di akhir glosarium.

Nomor

7 Rs

Tujuh strategi migrasi umum untuk memindahkan aplikasi ke cloud. Strategi ini dibangun di atas 5 Rs yang diidentifikasi Gartner pada tahun 2011 dan terdiri dari yang berikut:

- Refactor/Re-Architect — Memindahkan aplikasi dan memodifikasi arsitekturnya dengan memanfaatkan sepenuhnya fitur cloud-native untuk meningkatkan kelincahan, kinerja, dan skalabilitas. Ini biasanya melibatkan porting sistem operasi dan database. Contoh: Migrasikan database Oracle lokal Anda ke Amazon Aurora PostgreSQL Compatible Edition.
- Replatform (angkat dan bentuk ulang) — Pindahkan aplikasi ke cloud, dan perkenalkan beberapa tingkat pengoptimalan untuk memanfaatkan kemampuan cloud. Contoh: Migrasikan database Oracle lokal Anda ke Amazon Relational Database Service (Amazon RDS) untuk Oracle di. AWS Cloud
- Pembelian kembali (drop and shop) - Beralih ke produk yang berbeda, biasanya dengan beralih dari lisensi tradisional ke model SaaS. Contoh: Migrasikan sistem manajemen hubungan pelanggan (CRM) Anda ke Salesforce.com.
- Rehost (lift dan shift) — Pindahkan aplikasi ke cloud tanpa membuat perubahan apa pun untuk memanfaatkan kemampuan cloud. Contoh: Migrasikan database Oracle lokal Anda ke Oracle pada instans EC2 di. AWS Cloud
- Relokasi (hypervisor-level lift and shift) — Pindahkan infrastruktur ke cloud tanpa membeli perangkat keras baru, menulis ulang aplikasi, atau memodifikasi operasi yang ada. Anda memigrasikan server dari platform lokal ke layanan cloud untuk platform yang sama. Contoh: Migrasikan Microsoft Hyper-V aplikasi ke AWS.
- Pertahankan (kunjungi kembali) - Simpan aplikasi di lingkungan sumber Anda. Ini mungkin termasuk aplikasi yang memerlukan refactoring besar, dan Anda ingin menunda pekerjaan itu sampai nanti, dan aplikasi lama yang ingin Anda pertahankan, karena tidak ada pembenaran bisnis untuk memigrasikannya.

- Pensiun — Menonaktifkan atau menghapus aplikasi yang tidak lagi diperlukan di lingkungan sumber Anda.

A

ABAC

Lihat kontrol akses berbasis atribut.

layanan abstrak

Lihat layanan terkelola.

ASAM

Lihat atomisitas, konsistensi, isolasi, daya tahan.

migrasi aktif-aktif

Metode migrasi database di mana database sumber dan target tetap sinkron (dengan menggunakan alat replikasi dua arah atau operasi penulisan ganda), dan kedua database menangani transaksi dari menghubungkan aplikasi selama migrasi. Metode ini mendukung migrasi dalam batch kecil yang terkontrol alih-alih memerlukan pemotongan satu kali. Ini lebih fleksibel tetapi membutuhkan lebih banyak pekerjaan daripada migrasi aktif-pasif.

migrasi aktif-pasif

Metode migrasi database di mana database sumber dan target disimpan dalam sinkron, tetapi hanya database sumber yang menangani transaksi dari menghubungkan aplikasi sementara data direplikasi ke database target. Basis data target tidak menerima transaksi apa pun selama migrasi.

fungsi agregat

Fungsi SQL yang beroperasi pada sekelompok baris dan menghitung nilai pengembalian tunggal untuk grup. Contoh fungsi agregat meliputi `SUM` dan`MAX`.

AI

Lihat kecerdasan buatan.

AIOps

Lihat operasi kecerdasan buatan.

anonimisasi

Proses menghapus informasi pribadi secara permanen dalam kumpulan data. Anonimisasi dapat membantu melindungi privasi pribadi. Data anonim tidak lagi dianggap sebagai data pribadi.

anti-pola

Solusi yang sering digunakan untuk masalah berulang di mana solusinya kontra-produktif, tidak efektif, atau kurang efektif daripada alternatif.

kontrol aplikasi

Pendekatan keamanan yang memungkinkan penggunaan hanya aplikasi yang disetujui untuk membantu melindungi sistem dari malware.

portofolio aplikasi

Kumpulan informasi rinci tentang setiap aplikasi yang digunakan oleh organisasi, termasuk biaya untuk membangun dan memelihara aplikasi, dan nilai bisnisnya. Informasi ini adalah kunci untuk penemuan portofolio dan proses analisis dan membantu mengidentifikasi dan memprioritaskan aplikasi yang akan dimigrasi, dimodernisasi, dan dioptimalkan.

kecerdasan buatan (AI)

Bidang ilmu komputer yang didedikasikan untuk menggunakan teknologi komputasi untuk melakukan fungsi kognitif yang biasanya terkait dengan manusia, seperti belajar, memecahkan masalah, dan mengenali pola. Untuk informasi lebih lanjut, lihat Apa itu Kecerdasan Buatan?

operasi kecerdasan buatan (AIOps)

Proses menggunakan teknik pembelajaran mesin untuk memecahkan masalah operasional, mengurangi insiden operasional dan intervensi manusia, dan meningkatkan kualitas layanan. Untuk informasi selengkapnya tentang cara AIOps digunakan dalam strategi AWS migrasi, lihat panduan integrasi operasi.

enkripsi asimetris

Algoritma enkripsi yang menggunakan sepasang kunci, kunci publik untuk enkripsi dan kunci pribadi untuk dekripsi. Anda dapat berbagi kunci publik karena tidak digunakan untuk dekripsi, tetapi akses ke kunci pribadi harus sangat dibatasi.

atomisitas, konsistensi, isolasi, daya tahan (ACID)

Satu set properti perangkat lunak yang menjamin validitas data dan keandalan operasional database, bahkan dalam kasus kesalahan, kegagalan daya, atau masalah lainnya.

kontrol akses berbasis atribut (ABAC)

Praktik membuat izin berbutir halus berdasarkan atribut pengguna, seperti departemen, peran pekerjaan, dan nama tim. Untuk informasi selengkapnya, lihat ABAC untuk AWS dokumentasi AWS Identity and Access Management (IAM).

sumber data otoritatif

Lokasi di mana Anda menyimpan versi utama data, yang dianggap sebagai sumber informasi yang paling dapat diandalkan. Anda dapat menyalin data dari sumber data otoritatif ke lokasi lain untuk tujuan memproses atau memodifikasi data, seperti menganonimkan, menyunting, atau membuat nama samaran.

Zona Ketersediaan

Lokasi berbeda di dalam AWS Region yang terisolasi dari kegagalan di Availability Zone lainnya dan menyediakan konektivitas jaringan latensi rendah yang murah ke Availability Zone lainnya di Wilayah yang sama.

AWS Kerangka Adopsi Cloud (AWS CAF)

Kerangka pedoman dan praktik terbaik AWS untuk membantu organisasi mengembangkan rencana yang efisien dan efektif untuk bergerak dengan sukses ke cloud. AWS CAF mengatur panduan ke dalam enam area fokus yang disebut perspektif: bisnis, orang, tata kelola, platform, keamanan, dan operasi. Perspektif bisnis, orang, dan tata kelola fokus pada keterampilan dan proses bisnis; perspektif platform, keamanan, dan operasi fokus pada keterampilan dan proses teknis. Misalnya, perspektif masyarakat menargetkan pemangku kepentingan yang menangani sumber daya manusia (SDM), fungsi kepegawaian, dan manajemen orang. Untuk perspektif ini, AWS CAF memberikan panduan untuk pengembangan, pelatihan, dan komunikasi orang untuk membantu mempersiapkan organisasi untuk adopsi cloud yang sukses. Untuk informasi lebih lanjut, lihat situs web AWS CAF dan whitepaper AWS CAF.

AWS Kerangka Kualifikasi Beban Kerja (AWS WQF)

Alat yang mengevaluasi beban kerja migrasi database, merekomendasikan strategi migrasi, dan memberikan perkiraan kerja. AWS WQF disertakan dengan AWS Schema Conversion Tool ()AWS SCT. Ini menganalisis skema database dan objek kode, kode aplikasi, dependensi, dan karakteristik kinerja, dan memberikan laporan penilaian.

B

bot buruk

Bot yang dimaksudkan untuk mengganggu atau menyebabkan kerugian bagi individu atau organisasi.

BCP

Lihat perencanaan kontinuitas bisnis.

grafik perilaku

Pandangan interaktif yang terpadu tentang perilaku dan interaksi sumber daya dari waktu ke waktu. Anda dapat menggunakan grafik perilaku dengan Amazon Detective untuk memeriksa upaya logon yang gagal, panggilan API yang mencurigakan, dan tindakan serupa. Untuk informasi selengkapnya, lihat Data dalam grafik perilaku di dokumentasi Detektif.

sistem big-endian

Sistem yang menyimpan byte paling signifikan terlebih dahulu. Lihat juga endianness.

klasifikasi biner

Sebuah proses yang memprediksi hasil biner (salah satu dari dua kelas yang mungkin). Misalnya, model ML Anda mungkin perlu memprediksi masalah seperti “Apakah email ini spam atau bukan spam?” atau “Apakah produk ini buku atau mobil?”

filter mekar

Struktur data probabilistik dan efisien memori yang digunakan untuk menguji apakah suatu elemen adalah anggota dari suatu himpunan.

deployment biru/hijau

Strategi penyebaran tempat Anda membuat dua lingkungan yang terpisah namun identik. Anda menjalankan versi aplikasi saat ini di satu lingkungan (biru) dan versi aplikasi baru di lingkungan lain (hijau). Strategi ini membantu Anda dengan cepat memutar kembali dengan dampak minimal.

bot

Aplikasi perangkat lunak yang menjalankan tugas otomatis melalui internet dan mensimulasikan aktivitas atau interaksi manusia. Beberapa bot berguna atau bermanfaat, seperti perayap web yang mengindeks informasi di internet. Beberapa bot lain, yang dikenal sebagai bot buruk, dimaksudkan untuk mengganggu atau membahayakan individu atau organisasi.

botnet

Jaringan bot yang terinfeksi oleh malware dan berada di bawah kendali satu pihak, yang dikenal sebagai bot herder atau operator bot. Botnet adalah mekanisme paling terkenal untuk skala bot dan dampaknya.

cabang

Area berisi repositori kode. Cabang pertama yang dibuat dalam repositori adalah cabang utama. Anda dapat membuat cabang baru dari cabang yang ada, dan Anda kemudian dapat mengembangkan fitur atau memperbaiki bug di cabang baru. Cabang yang Anda buat untuk membangun fitur biasanya disebut sebagai cabang fitur. Saat fitur siap dirilis, Anda menggabungkan cabang fitur kembali ke cabang utama. Untuk informasi selengkapnya, lihat Tentang cabang (GitHub dokumentasi).

akses break-glass

Dalam keadaan luar biasa dan melalui proses yang disetujui, cara cepat bagi pengguna untuk mendapatkan akses ke Akun AWS yang biasanya tidak memiliki izin untuk mengaksesnya. Untuk informasi lebih lanjut, lihat indikator Implementasikan prosedur break-glass dalam panduan Well-Architected AWS .

strategi brownfield

Infrastruktur yang ada di lingkungan Anda. Saat mengadopsi strategi brownfield untuk arsitektur sistem, Anda merancang arsitektur di sekitar kendala sistem dan infrastruktur saat ini. Jika Anda memperluas infrastruktur yang ada, Anda dapat memadukan strategi brownfield dan greenfield.

cache penyangga

Area memori tempat data yang paling sering diakses disimpan.

kemampuan bisnis

Apa yang dilakukan bisnis untuk menghasilkan nilai (misalnya, penjualan, layanan pelanggan, atau pemasaran). Arsitektur layanan mikro dan keputusan pengembangan dapat didorong oleh kemampuan bisnis. Untuk informasi selengkapnya, lihat bagian Terorganisir di sekitar kemampuan bisnis dari Menjalankan layanan mikro kontainer di whitepaper. AWS

perencanaan kelangsungan bisnis (BCP)

Rencana yang membahas dampak potensial dari peristiwa yang mengganggu, seperti migrasi skala besar, pada operasi dan memungkinkan bisnis untuk melanjutkan operasi dengan cepat.

C

KAFE

Lihat Kerangka Adopsi AWS Cloud.

penyebaran kenari

Rilis versi yang lambat dan bertahap untuk pengguna akhir. Ketika Anda yakin, Anda menyebarkan versi baru dan mengganti versi saat ini secara keseluruhan.

CCoE

Lihat Cloud Center of Excellence.

CDC

Lihat mengubah pengambilan data.

ubah pengambilan data (CDC)

Proses melacak perubahan ke sumber data, seperti tabel database, dan merekam metadata tentang perubahan tersebut. Anda dapat menggunakan CDC untuk berbagai tujuan, seperti mengaudit atau mereplikasi perubahan dalam sistem target untuk mempertahankan sinkronisasi.

rekayasa kekacauan

Sengaja memperkenalkan kegagalan atau peristiwa yang mengganggu untuk menguji ketahanan sistem. Anda dapat menggunakan AWS Fault Injection Service (AWS FIS) untuk melakukan eksperimen yang menekankan AWS beban kerja Anda dan mengevaluasi responsnya.

CI/CD

Lihat integrasi berkelanjutan dan pengiriman berkelanjutan.

klasifikasi

Proses kategorisasi yang membantu menghasilkan prediksi. Model ML untuk masalah klasifikasi memprediksi nilai diskrit. Nilai diskrit selalu berbeda satu sama lain. Misalnya, model mungkin perlu mengevaluasi apakah ada mobil dalam gambar atau tidak.

Enkripsi sisi klien

Enkripsi data secara lokal, sebelum target Layanan AWS menerimanya.

Pusat Keunggulan Cloud (CCoE)

Tim multi-disiplin yang mendorong upaya adopsi cloud di seluruh organisasi, termasuk mengembangkan praktik terbaik cloud, memobilisasi sumber daya, menetapkan jadwal migrasi, dan memimpin organisasi melalui transformasi skala besar. Untuk informasi selengkapnya, lihat posting CCo E di Blog Strategi AWS Cloud Perusahaan.

komputasi cloud

Teknologi cloud yang biasanya digunakan untuk penyimpanan data jarak jauh dan manajemen perangkat IoT. Cloud computing umumnya terhubung ke teknologi edge computing.

model operasi cloud

Dalam organisasi TI, model operasi yang digunakan untuk membangun, mematangkan, dan mengoptimalkan satu atau lebih lingkungan cloud. Untuk informasi selengkapnya, lihat Membangun Model Operasi Cloud Anda.

tahap adopsi cloud

Empat fase yang biasanya dilalui organisasi ketika mereka bermigrasi ke AWS Cloud:

- Proyek — Menjalankan beberapa proyek terkait cloud untuk bukti konsep dan tujuan pembelajaran
- Foundation — Melakukan investasi dasar untuk meningkatkan adopsi cloud Anda (misalnya, membuat landing zone, mendefinisikan CCo E, membuat model operasi)
- Migrasi — Migrasi aplikasi individual
- Re-invention — Mengoptimalkan produk dan layanan, dan berinovasi di cloud

Tahapan ini didefinisikan oleh Stephen Orban dalam posting blog The Journey Toward Cloud-First & the Stages of Adoption di blog Strategi Perusahaan. AWS Cloud Untuk informasi tentang bagaimana kaitannya dengan strategi AWS migrasi, lihat panduan kesiapan migrasi.

CMDB

Lihat database manajemen konfigurasi.

repositori kode

Lokasi di mana kode sumber dan aset lainnya, seperti dokumentasi, sampel, dan skrip, disimpan dan diperbarui melalui proses kontrol versi. Repositori cloud umum termasuk GitHub atau. Bitbucket Cloud Setiap versi kode disebut cabang. Dalam struktur layanan mikro, setiap repositori

dikhususkan untuk satu bagian fungsionalitas. Pipa CI/CD tunggal dapat menggunakan beberapa repositori.

cache dingin

Cache buffer yang kosong, tidak terisi dengan baik, atau berisi data basi atau tidak relevan. Ini mempengaruhi kinerja karena instance database harus membaca dari memori utama atau disk, yang lebih lambat daripada membaca dari cache buffer.

data dingin

Data yang jarang diakses dan biasanya historis. Saat menanyakan jenis data ini, kueri lambat biasanya dapat diterima. Memindahkan data ini ke tingkat penyimpanan atau kelas yang berkinerja lebih rendah dan lebih murah dapat mengurangi biaya.

visi komputer (CV)

Bidang AI yang menggunakan pembelajaran mesin untuk menganalisis dan mengekstrak informasi dari format visual seperti gambar dan video digital. Misalnya, Amazon SageMaker AI menyediakan algoritma pemrosesan gambar untuk CV.

konfigurasi drift

Untuk beban kerja, konfigurasi berubah dari status yang diharapkan. Ini dapat menyebabkan beban kerja menjadi tidak patuh, dan biasanya bertahap dan tidak disengaja.

database manajemen konfigurasi (CMDB)

Repositori yang menyimpan dan mengelola informasi tentang database dan lingkungan TI, termasuk komponen perangkat keras dan perangkat lunak dan konfigurasinya. Anda biasanya menggunakan data dari CMDB dalam penemuan portofolio dan tahap analisis migrasi.

paket kesesuaian

Kumpulan AWS Config aturan dan tindakan remediasi yang dapat Anda kumpulkan untuk menyesuaikan kepatuhan dan pemeriksaan keamanan Anda. Anda dapat menerapkan paket kesesuaian sebagai entitas tunggal di Akun AWS dan Wilayah, atau di seluruh organisasi, dengan menggunakan templat YAMM. Untuk informasi selengkapnya, lihat Paket kesesuaian dalam dokumentasi. AWS Config

integrasi berkelanjutan dan pengiriman berkelanjutan (CI/CD)

Proses mengotomatiskan sumber, membangun, menguji, pementasan, dan tahap produksi dari proses rilis perangkat lunak. CI/CD biasanya digambarkan sebagai pipa. CI/CD dapat membantu

Anda mengotomatiskan proses, meningkatkan produktivitas, meningkatkan kualitas kode, dan memberikan lebih cepat. Untuk informasi lebih lanjut, lihat Manfaat pengiriman berkelanjutan. CD juga dapat berarti penerapan berkelanjutan. Untuk informasi selengkapnya, lihat Continuous Delivery vs Continuous Deployment.

CV

Lihat visi komputer.

D

data saat istirahat

Data yang stasioner di jaringan Anda, seperti data yang ada di penyimpanan.

klasifikasi data

Proses untuk mengidentifikasi dan mengkategorikan data dalam jaringan Anda berdasarkan kekritisan dan sensitivitasnya. Ini adalah komponen penting dari setiap strategi manajemen risiko keamanan siber karena membantu Anda menentukan perlindungan dan kontrol retensi yang tepat untuk data. Klasifikasi data adalah komponen pilar keamanan dalam AWS Well-Architected Framework. Untuk informasi selengkapnya, lihat Klasifikasi data.

penyimpangan data

Variasi yang berarti antara data produksi dan data yang digunakan untuk melatih model ML, atau perubahan yang berarti dalam data input dari waktu ke waktu. Penyimpangan data dapat mengurangi kualitas, akurasi, dan keadilan keseluruhan dalam prediksi model ML.

data dalam transit

Data yang aktif bergerak melalui jaringan Anda, seperti antara sumber daya jaringan.

jala data

Kerangka arsitektur yang menyediakan kepemilikan data terdistribusi dan terdesentralisasi dengan manajemen dan tata kelola terpusat.

minimalisasi data

Prinsip pengumpulan dan pemrosesan hanya data yang sangat diperlukan. Mempraktikkan minimalisasi data di dalamnya AWS Cloud dapat mengurangi risiko privasi, biaya, dan jejak karbon analitik Anda.

perimeter data

Satu set pagar pembatas pencegahan di AWS lingkungan Anda yang membantu memastikan bahwa hanya identitas tepercaya yang mengakses sumber daya tepercaya dari jaringan yang diharapkan. Untuk informasi selengkapnya, lihat Membangun perimeter data pada AWS.

prapemrosesan data

Untuk mengubah data mentah menjadi format yang mudah diuraikan oleh model ML Anda. Preprocessing data dapat berarti menghapus kolom atau baris tertentu dan menangani nilai yang hilang, tidak konsisten, atau duplikat.

asal data

Proses melacak asal dan riwayat data sepanjang siklus hidupnya, seperti bagaimana data dihasilkan, ditransmisikan, dan disimpan.

subjek data

Individu yang datanya dikumpulkan dan diproses.

gudang data

Sistem manajemen data yang mendukung intelijen bisnis, seperti analitik. Gudang data biasanya berisi sejumlah besar data historis, dan biasanya digunakan untuk kueri dan analisis.

bahasa definisi database (DDL)

Pernyataan atau perintah untuk membuat atau memodifikasi struktur tabel dan objek dalam database.

bahasa manipulasi basis data (DHTML)

Pernyataan atau perintah untuk memodifikasi (memasukkan, memperbarui, dan menghapus) informasi dalam database.

DDL

Lihat bahasa definisi database.

ansambel yang dalam

Untuk menggabungkan beberapa model pembelajaran mendalam untuk prediksi. Anda dapat menggunakan ansambel dalam untuk mendapatkan prediksi yang lebih akurat atau untuk memperkirakan ketidakpastian dalam prediksi.

pembelajaran mendalam

Subbidang ML yang menggunakan beberapa lapisan jaringan saraf tiruan untuk mengidentifikasi pemetaan antara data input dan variabel target yang diinginkan.

defense-in-depth

Pendekatan keamanan informasi di mana serangkaian mekanisme dan kontrol keamanan dilapisi dengan cermat di seluruh jaringan komputer untuk melindungi kerahasiaan, integritas, dan ketersediaan jaringan dan data di dalamnya. Saat Anda mengadopsi strategi ini AWS, Anda menambahkan beberapa kontrol pada lapisan AWS Organizations struktur yang berbeda untuk membantu mengamankan sumber daya. Misalnya, defense-in-depth pendekatan mungkin menggabungkan otentikasi multi-faktor, segmentasi jaringan, dan enkripsi.

administrator yang didelegasikan

Di AWS Organizations, layanan yang kompatibel dapat mendaftarkan akun AWS anggota untuk mengelola akun organisasi dan mengelola izin untuk layanan tersebut. Akun ini disebut administrator yang didelegasikan untuk layanan itu. Untuk informasi selengkapnya dan daftar layanan yang kompatibel, lihat Layanan yang berfungsi dengan AWS Organizations AWS Organizations dokumentasi.

deployment

Proses pembuatan aplikasi, fitur baru, atau perbaikan kode tersedia di lingkungan target. Deployment melibatkan penerapan perubahan dalam basis kode dan kemudian membangun dan menjalankan basis kode itu di lingkungan aplikasi.

lingkungan pengembangan

Lihat lingkungan.

kontrol detektif

Kontrol keamanan yang dirancang untuk mendeteksi, mencatat, dan memperingatkan setelah suatu peristiwa terjadi. Kontrol ini adalah garis pertahanan kedua, memperingatkan Anda tentang peristiwa keamanan yang melewati kontrol pencegahan yang ada. Untuk informasi selengkapnya, lihat Kontrol Detektif dalam Menerapkan kontrol keamanan pada. AWS

pemetaan aliran nilai pengembangan (DVSM)

Sebuah proses yang digunakan untuk mengidentifikasi dan memprioritaskan kendala yang mempengaruhi kecepatan dan kualitas dalam siklus hidup pengembangan perangkat lunak. DVSM memperluas proses pemetaan aliran nilai yang awalnya dirancang untuk praktik

manufaktur ramping. Ini berfokus pada langkah-langkah dan tim yang diperlukan untuk menciptakan dan memindahkan nilai melalui proses pengembangan perangkat lunak.

kembar digital

Representasi virtual dari sistem dunia nyata, seperti bangunan, pabrik, peralatan industri, atau jalur produksi. Kembar digital mendukung pemeliharaan prediktif, pemantauan jarak jauh, dan optimalisasi produksi.

tabel dimensi

Dalam skema bintang, tabel yang lebih kecil yang berisi atribut data tentang data kuantitatif dalam tabel fakta. Atribut tabel dimensi biasanya bidang teks atau angka diskrit yang berperilaku seperti teks. Atribut ini biasanya digunakan untuk pembatasan kueri, pemfilteran, dan pelabelan set hasil.

musibah

Peristiwa yang mencegah beban kerja atau sistem memenuhi tujuan bisnisnya di lokasi utama yang digunakan. Peristiwa ini dapat berupa bencana alam, kegagalan teknis, atau akibat dari tindakan manusia, seperti kesalahan konfigurasi yang tidak disengaja atau serangan malware.

pemulihan bencana (DR)

Strategi dan proses yang Anda gunakan untuk meminimalkan downtime dan kehilangan data yang disebabkan oleh bencana. Untuk informasi selengkapnya, lihat Disaster Recovery of Workloads on AWS: Recovery in the Cloud in the AWS Well-Architected Framework.

DML~

Lihat bahasa manipulasi basis data.

desain berbasis domain

Pendekatan untuk mengembangkan sistem perangkat lunak yang kompleks dengan menghubungkan komponennya ke domain yang berkembang, atau tujuan bisnis inti, yang dilayani oleh setiap komponen. Konsep ini diperkenalkan oleh Eric Evans dalam bukunya, Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003). Untuk informasi tentang cara menggunakan desain berbasis domain dengan pola gambar pencekik, lihat Memodernisasi layanan web Microsoft ASP.NET (ASMX) lama secara bertahap menggunakan container dan Amazon API Gateway.

DR

Lihat pemulihan bencana.

deteksi drift

Melacak penyimpangan dari konfigurasi dasar. Misalnya, Anda dapat menggunakan AWS CloudFormation untuk mendeteksi penyimpangan dalam sumber daya sistem, atau Anda dapat menggunakannya AWS Control Tower untuk mendeteksi perubahan di landing zone yang mungkin memengaruhi kepatuhan terhadap persyaratan tata kelola.

DVSM

Lihat pemetaan aliran nilai pengembangan.

E

EDA

Lihat analisis data eksplorasi.

EDI

Lihat pertukaran data elektronik.

komputasi tepi

Teknologi yang meningkatkan daya komputasi untuk perangkat pintar di tepi jaringan IoT. Jika dibandingkan dengan komputasi awan, komputasi tepi dapat mengurangi latensi komunikasi dan meningkatkan waktu respons.

pertukaran data elektronik (EDI)

Pertukaran otomatis dokumen bisnis antar organisasi. Untuk informasi selengkapnya, lihat Apa itu Pertukaran Data Elektronik.

enkripsi

Proses komputasi yang mengubah data plaintext, yang dapat dibaca manusia, menjadi ciphertext.

kunci enkripsi

String kriptografi dari bit acak yang dihasilkan oleh algoritma enkripsi. Panjang kunci dapat bervariasi, dan setiap kunci dirancang agar tidak dapat diprediksi dan unik.

endianness

Urutan byte disimpan dalam memori komputer. Sistem big-endian menyimpan byte paling signifikan terlebih dahulu. Sistem little-endian menyimpan byte paling tidak signifikan terlebih dahulu.

titik akhir

Lihat titik akhir layanan.

layanan endpoint

Layanan yang dapat Anda host di cloud pribadi virtual (VPC) untuk dibagikan dengan pengguna lain. Anda dapat membuat layanan endpoint dengan AWS PrivateLink dan memberikan izin kepada prinsipal lain Akun AWS atau ke AWS Identity and Access Management (IAM). Akun atau prinsipal ini dapat terhubung ke layanan endpoint Anda secara pribadi dengan membuat titik akhir VPC antarmuka. Untuk informasi selengkapnya, lihat Membuat layanan titik akhir di dokumentasi Amazon Virtual Private Cloud (Amazon VPC).

perencanaan sumber daya perusahaan (ERP)

Sistem yang mengotomatiskan dan mengelola proses bisnis utama (seperti akuntansi, MES, dan manajemen proyek) untuk suatu perusahaan.

enkripsi amplop

Proses mengenkripsi kunci enkripsi dengan kunci enkripsi lain. Untuk informasi selengkapnya, lihat Enkripsi amplop dalam dokumentasi AWS Key Management Service (AWS KMS).

lingkungan

Sebuah contoh dari aplikasi yang sedang berjalan. Berikut ini adalah jenis lingkungan yang umum dalam komputasi awan:

- Development Environment — Sebuah contoh dari aplikasi yang berjalan yang hanya tersedia untuk tim inti yang bertanggung jawab untuk memelihara aplikasi. Lingkungan pengembangan digunakan untuk menguji perubahan sebelum mempromosikannya ke lingkungan atas. Jenis lingkungan ini kadang-kadang disebut sebagai lingkungan pengujian.
- lingkungan yang lebih rendah — Semua lingkungan pengembangan untuk aplikasi, seperti yang digunakan untuk build awal dan pengujian.
- lingkungan produksi — Sebuah contoh dari aplikasi yang berjalan yang dapat diakses oleh pengguna akhir. Dalam sebuah CI/CD pipeline, lingkungan produksi adalah lingkungan penyebaran terakhir.
- lingkungan atas — Semua lingkungan yang dapat diakses oleh pengguna selain tim pengembangan inti. Ini dapat mencakup lingkungan produksi, lingkungan praproduksi, dan lingkungan untuk pengujian penerimaan pengguna.

epik

Dalam metodologi tangkas, kategori fungsional yang membantu mengatur dan memprioritaskan pekerjaan Anda. Epik memberikan deskripsi tingkat tinggi tentang persyaratan dan tugas implementasi. Misalnya, epos keamanan AWS CAF mencakup manajemen identitas dan akses, kontrol detektif, keamanan infrastruktur, perlindungan data, dan respons insiden. Untuk informasi selengkapnya tentang epos dalam strategi AWS migrasi, lihat panduan implementasi program.

ERP

Lihat perencanaan sumber daya perusahaan.

analisis data eksplorasi (EDA)

Proses menganalisis dataset untuk memahami karakteristik utamanya. Anda mengumpulkan atau mengumpulkan data dan kemudian melakukan penyelidikan awal untuk menemukan pola, mendeteksi anomali, dan memeriksa asumsi. EDA dilakukan dengan menghitung statistik ringkasan dan membuat visualisasi data.

F

tabel fakta

Tabel tengah dalam skema bintang. Ini menyimpan data kuantitatif tentang operasi bisnis. Biasanya, tabel fakta berisi dua jenis kolom: kolom yang berisi ukuran dan yang berisi kunci asing ke tabel dimensi.

gagal cepat

Filosofi yang menggunakan pengujian yang sering dan bertahap untuk mengurangi siklus hidup pengembangan. Ini adalah bagian penting dari pendekatan tangkas.

batas isolasi kesalahan

Dalam AWS Cloud, batas seperti Availability Zone, AWS Region, control plane, atau data plane yang membatasi efek kegagalan dan membantu meningkatkan ketahanan beban kerja. Untuk informasi selengkapnya, lihat Batas Isolasi AWS Kesalahan.

cabang fitur

Lihat cabang.

fitur

Data input yang Anda gunakan untuk membuat prediksi. Misalnya, dalam konteks manufaktur, fitur bisa berupa gambar yang diambil secara berkala dari lini manufaktur.

pentingnya fitur

Seberapa signifikan fitur untuk prediksi model. Ini biasanya dinyatakan sebagai skor numerik yang dapat dihitung melalui berbagai teknik, seperti Shapley Additive Explanations (SHAP) dan gradien terintegrasi. Untuk informasi lebih lanjut, lihat Interpretabilitas model pembelajaran mesin dengan. AWS

transformasi fitur

Untuk mengoptimalkan data untuk proses ML, termasuk memperkaya data dengan sumber tambahan, menskalakan nilai, atau mengekstrak beberapa set informasi dari satu bidang data. Hal ini memungkinkan model ML untuk mendapatkan keuntungan dari data. Misalnya, jika Anda memecah tanggal “2021-05-27 00:15:37" menjadi “2021", “Mei”, “Kamis”, dan “15", Anda dapat membantu algoritme pembelajaran mempelajari pola bernuansa yang terkait dengan komponen data yang berbeda.

beberapa tembakan mendorong

Menyediakan LLM dengan sejumlah kecil contoh yang menunjukkan tugas dan output yang diinginkan sebelum memintanya untuk melakukan tugas serupa. Teknik ini adalah aplikasi pembelajaran dalam konteks, di mana model belajar dari contoh (bidikan) yang tertanam dalam petunjuk. Beberapa bidikan dapat efektif untuk tugas-tugas yang memerlukan pemformatan, penalaran, atau pengetahuan domain tertentu. Lihat juga bidikan nol.

FGAC

Lihat kontrol akses berbutir halus.

kontrol akses berbutir halus (FGAC)

Penggunaan beberapa kondisi untuk mengizinkan atau menolak permintaan akses.

migrasi flash-cut

Metode migrasi database yang menggunakan replikasi data berkelanjutan melalui pengambilan data perubahan untuk memigrasikan data dalam waktu sesingkat mungkin, alih-alih menggunakan pendekatan bertahap. Tujuannya adalah untuk menjaga downtime seminimal mungkin.

FM

Lihat model pondasi.

model pondasi (FM)

Jaringan saraf pembelajaran mendalam yang besar yang telah melatih kumpulan data besar-besaran data umum dan tidak berlabel. FMs mampu melakukan berbagai tugas umum, seperti memahami bahasa, menghasilkan teks dan gambar, dan berbicara dalam bahasa alami. Untuk informasi selengkapnya, lihat Apa itu Model Foundation.

G

AI generatif

Subset model AI yang telah dilatih pada sejumlah besar data dan yang dapat menggunakan prompt teks sederhana untuk membuat konten dan artefak baru, seperti gambar, video, teks, dan audio. Untuk informasi lebih lanjut, lihat Apa itu AI Generatif.

pemblokiran geografis

Lihat pembatasan geografis.

pembatasan geografis (pemblokiran geografis)

Di Amazon CloudFront, opsi untuk mencegah pengguna di negara tertentu mengakses distribusi konten. Anda dapat menggunakan daftar izinkan atau daftar blokir untuk menentukan negara yang disetujui dan dilarang. Untuk informasi selengkapnya, lihat Membatasi distribusi geografis konten Anda dalam dokumentasi. CloudFront

Alur kerja Gitflow

Pendekatan di mana lingkungan bawah dan atas menggunakan cabang yang berbeda dalam repositori kode sumber. Alur kerja Gitflow dianggap warisan, dan alur kerja berbasis batang adalah pendekatan modern yang lebih disukai.

gambar emas

Sebuah snapshot dari sistem atau perangkat lunak yang digunakan sebagai template untuk menyebarkan instance baru dari sistem atau perangkat lunak itu. Misalnya, di bidang manufaktur, gambar emas dapat digunakan untuk menyediakan perangkat lunak pada beberapa perangkat dan membantu meningkatkan kecepatan, skalabilitas, dan produktivitas dalam operasi manufaktur perangkat.

strategi greenfield

Tidak adanya infrastruktur yang ada di lingkungan baru. Saat mengadopsi strategi greenfield untuk arsitektur sistem, Anda dapat memilih semua teknologi baru tanpa batasan kompatibilitas dengan infrastruktur yang ada, juga dikenal sebagai brownfield. Jika Anda memperluas infrastruktur yang ada, Anda dapat memadukan strategi brownfield dan greenfield.

pagar pembatas

Aturan tingkat tinggi yang membantu mengatur sumber daya, kebijakan, dan kepatuhan di seluruh unit organisasi ()OUs. Pagar pembatas preventif menegakkan kebijakan untuk memastikan keselarasan dengan standar kepatuhan. Mereka diimplementasikan dengan menggunakan kebijakan kontrol layanan dan batas izin IAM. Detective guardrails mendeteksi pelanggaran kebijakan dan masalah kepatuhan, dan menghasilkan peringatan untuk remediasi. Mereka diimplementasikan dengan menggunakan AWS Config, AWS Security Hub CSPM, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector, dan pemeriksaan khusus AWS Lambda .

H

HA

Lihat ketersediaan tinggi.

migrasi database heterogen

Memigrasi database sumber Anda ke database target yang menggunakan mesin database yang berbeda (misalnya, Oracle ke Amazon Aurora). Migrasi heterogen biasanya merupakan bagian dari upaya arsitektur ulang, dan mengubah skema dapat menjadi tugas yang kompleks. AWS menyediakan AWS SCT yang membantu dengan konversi skema.

ketersediaan tinggi (HA)

Kemampuan beban kerja untuk beroperasi terus menerus, tanpa intervensi, jika terjadi tantangan atau bencana. Sistem HA dirancang untuk gagal secara otomatis, secara konsisten memberikan kinerja berkualitas tinggi, dan menangani beban dan kegagalan yang berbeda dengan dampak kinerja minimal.

modernisasi sejarawan

Pendekatan yang digunakan untuk memodernisasi dan meningkatkan sistem teknologi operasional (OT) untuk melayani kebutuhan industri manufaktur dengan lebih baik. Sejarawan

adalah jenis database yang digunakan untuk mengumpulkan dan menyimpan data dari berbagai sumber di pabrik.

data penahanan

Sebagian dari data historis berlabel yang ditahan dari kumpulan data yang digunakan untuk melatih model pembelajaran mesin. Anda dapat menggunakan data penahanan untuk mengevaluasi kinerja model dengan membandingkan prediksi model dengan data penahanan.

migrasi database homogen

Memigrasi database sumber Anda ke database target yang berbagi mesin database yang sama (misalnya, Microsoft SQL Server ke Amazon RDS for SQL Server). Migrasi homogen biasanya merupakan bagian dari upaya rehosting atau replatforming. Anda dapat menggunakan utilitas database asli untuk memigrasi skema.

data panas

Data yang sering diakses, seperti data real-time atau data translasi terbaru. Data ini biasanya memerlukan tingkat atau kelas penyimpanan berkinerja tinggi untuk memberikan respons kueri yang cepat.

perbaikan terbaru

Perbaikan mendesak untuk masalah kritis dalam lingkungan produksi. Karena urgensinya, perbaikan terbaru biasanya dibuat di luar alur kerja DevOps rilis biasa.

periode hypercare

Segera setelah cutover, periode waktu ketika tim migrasi mengelola dan memantau aplikasi yang dimigrasi di cloud untuk mengatasi masalah apa pun. Biasanya, periode ini panjangnya 1-4 hari. Pada akhir periode hypercare, tim migrasi biasanya mentransfer tanggung jawab untuk aplikasi ke tim operasi cloud.

I

IAc

Lihat infrastruktur sebagai kode.

kebijakan berbasis identitas

Kebijakan yang dilampirkan pada satu atau beberapa prinsip IAM yang mendefinisikan izin mereka dalam lingkungan. AWS Cloud

aplikasi idle

Aplikasi yang memiliki penggunaan CPU dan memori rata-rata antara 5 dan 20 persen selama periode 90 hari. Dalam proyek migrasi, adalah umum untuk menghentikan aplikasi ini atau mempertahankannya di tempat.

IIoT

Lihat Internet of Things industri.

infrastruktur yang tidak dapat diubah

Model yang menyebarkan infrastruktur baru untuk beban kerja produksi alih-alih memperbarui, menambal, atau memodifikasi infrastruktur yang ada. Infrastruktur yang tidak dapat diubah secara inheren lebih konsisten, andal, dan dapat diprediksi daripada infrastruktur yang dapat berubah. Untuk informasi selengkapnya, lihat praktik terbaik Deploy using immutable infrastructure di AWS Well-Architected Framework.

masuk (masuknya) VPC

Dalam arsitektur AWS multi-akun, VPC yang menerima, memeriksa, dan merutekan koneksi jaringan dari luar aplikasi. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan inbound, outbound, dan inspeksi VPCs untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

migrasi inkremental

Strategi cutover di mana Anda memigrasikan aplikasi Anda dalam bagian-bagian kecil alih-alih melakukan satu cutover penuh. Misalnya, Anda mungkin hanya memindahkan beberapa layanan mikro atau pengguna ke sistem baru pada awalnya. Setelah Anda memverifikasi bahwa semuanya berfungsi dengan baik, Anda dapat secara bertahap memindahkan layanan mikro atau pengguna tambahan hingga Anda dapat menonaktifkan sistem lama Anda. Strategi ini mengurangi risiko yang terkait dengan migrasi besar.

Industri 4.0

Sebuah istilah yang diperkenalkan oleh Klaus Schwab pada tahun 2016 untuk merujuk pada modernisasi proses manufaktur melalui kemajuan dalam konektivitas, data real-time, otomatisasi, analitik, dan AI/ML.

infrastruktur

Semua sumber daya dan aset yang terkandung dalam lingkungan aplikasi.

infrastruktur sebagai kode (IAc)

Proses penyediaan dan pengelolaan infrastruktur aplikasi melalui satu set file konfigurasi. IAc dirancang untuk membantu Anda memusatkan manajemen infrastruktur, menstandarisasi sumber daya, dan menskalakan dengan cepat sehingga lingkungan baru dapat diulang, andal, dan konsisten.

Internet of Things industri (IIoT)

Penggunaan sensor dan perangkat yang terhubung ke internet di sektor industri, seperti manufaktur, energi, otomotif, perawatan kesehatan, ilmu kehidupan, dan pertanian. Untuk informasi lebih lanjut, lihat Membangun strategi transformasi digital Internet of Things (IIoT) industri.

inspeksi VPC

Dalam arsitektur AWS multi-akun, VPC terpusat yang mengelola inspeksi lalu lintas jaringan antara VPCs (dalam yang sama atau berbeda Wilayah AWS), internet, dan jaringan lokal. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan inbound, outbound, dan inspeksi VPCs untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

Internet of Things (IoT)

Jaringan objek fisik yang terhubung dengan sensor atau prosesor tertanam yang berkomunikasi dengan perangkat dan sistem lain melalui internet atau melalui jaringan komunikasi lokal. Untuk informasi selengkapnya, lihat Apa itu IoT?

interpretabilitas

Karakteristik model pembelajaran mesin yang menggambarkan sejauh mana manusia dapat memahami bagaimana prediksi model bergantung pada inputnya. Untuk informasi lebih lanjut, lihat Interpretabilitas model pembelajaran mesin dengan. AWS

IoT

Lihat Internet of Things.

Perpustakaan informasi TI (ITIL)

Serangkaian praktik terbaik untuk memberikan layanan TI dan menyelaraskan layanan ini dengan persyaratan bisnis. ITIL menyediakan dasar untuk ITSM.

Manajemen layanan TI (ITSM)

Kegiatan yang terkait dengan merancang, menerapkan, mengelola, dan mendukung layanan TI untuk suatu organisasi. Untuk informasi tentang mengintegrasikan operasi cloud dengan alat ITSM, lihat panduan integrasi operasi.

ITIL

Lihat perpustakaan informasi TI.

ITSM

Lihat manajemen layanan TI.

L

kontrol akses berbasis label (LBAC)

Implementasi kontrol akses wajib (MAC) di mana pengguna dan data itu sendiri masing-masing secara eksplisit diberi nilai label keamanan. Persimpangan antara label keamanan pengguna dan label keamanan data menentukan baris dan kolom mana yang dapat dilihat oleh pengguna.

landing zone

Landing zone adalah AWS lingkungan multi-akun yang dirancang dengan baik yang dapat diskalakan dan aman. Ini adalah titik awal dari mana organisasi Anda dapat dengan cepat meluncurkan dan menyebarkan beban kerja dan aplikasi dengan percaya diri dalam lingkungan keamanan dan infrastruktur mereka. Untuk informasi selengkapnya tentang zona pendaratan, lihat Menyiapkan lingkungan multi-akun AWS yang aman dan dapat diskalakan.

model bahasa besar (LLM)

Model AI pembelajaran mendalam yang dilatih sebelumnya pada sejumlah besar data. LLM dapat melakukan beberapa tugas, seperti menjawab pertanyaan, meringkas dokumen, menerjemahkan teks ke dalam bahasa lain, dan menyelesaikan kalimat. Untuk informasi lebih lanjut, lihat Apa itu LLMs.

migrasi besar

Migrasi 300 atau lebih server.

LBAC

Lihat kontrol akses berbasis label.

hak istimewa paling sedikit

Praktik keamanan terbaik untuk memberikan izin minimum yang diperlukan untuk melakukan tugas. Untuk informasi selengkapnya, lihat Menerapkan izin hak istimewa terkecil dalam dokumentasi IAM.

angkat dan geser

Lihat 7 Rs.

sistem endian kecil

Sebuah sistem yang menyimpan byte paling tidak signifikan terlebih dahulu. Lihat juga endianness.

LLM

Lihat model bahasa besar.

lingkungan yang lebih rendah

Lihat lingkungan.

M

pembelajaran mesin (ML)

Jenis kecerdasan buatan yang menggunakan algoritma dan teknik untuk pengenalan dan pembelajaran pola. ML menganalisis dan belajar dari data yang direkam, seperti data Internet of Things (IoT), untuk menghasilkan model statistik berdasarkan pola. Untuk informasi selengkapnya, lihat Machine Learning.

cabang utama

Lihat cabang.

malware

Perangkat lunak yang dirancang untuk membahayakan keamanan atau privasi komputer. Malware dapat mengganggu sistem komputer, membocorkan informasi sensitif, atau mendapatkan akses yang tidak sah. Contoh malware termasuk virus, worm, ransomware, Trojan horse, spyware, dan keyloggers.

layanan terkelola

Layanan AWS yang AWS mengoperasikan lapisan infrastruktur, sistem operasi, dan platform, dan Anda mengakses titik akhir untuk menyimpan dan mengambil data. Amazon Simple Storage Service (Amazon S3) dan Amazon DynamoDB adalah contoh layanan terkelola. Ini juga dikenal sebagai layanan abstrak.

sistem eksekusi manufaktur (MES)

Sistem perangkat lunak untuk melacak, memantau, mendokumentasikan, dan mengendalikan proses produksi yang mengubah bahan baku menjadi produk jadi di lantai toko.

PETA

Lihat Program Percepatan Migrasi.

mekanisme

Proses lengkap di mana Anda membuat alat, mendorong adopsi alat, dan kemudian memeriksa hasilnya untuk melakukan penyesuaian. Mekanisme adalah siklus yang memperkuat dan meningkatkan dirinya sendiri saat beroperasi. Untuk informasi lebih lanjut, lihat Membangun mekanisme di AWS Well-Architected Framework.

akun anggota

Semua Akun AWS selain akun manajemen yang merupakan bagian dari organisasi di AWS Organizations. Akun dapat menjadi anggota dari hanya satu organisasi pada suatu waktu.

MES

Lihat sistem eksekusi manufaktur.

Transportasi Telemetri Antrian Pesan (MQTT)

Protokol komunikasi ringan machine-to-machine (M2M), berdasarkan pola terbitkan/berlangganan, untuk perangkat IoT yang dibatasi sumber daya.

layanan mikro

Layanan kecil dan independen yang berkomunikasi dengan jelas APIs dan biasanya dimiliki oleh tim kecil yang mandiri. Misalnya, sistem asuransi mungkin mencakup layanan mikro yang memetakan kemampuan bisnis, seperti penjualan atau pemasaran, atau subdomain, seperti pembelian, klaim, atau analitik. Manfaat layanan mikro termasuk kelincahan, penskalaan yang fleksibel, penyebaran yang mudah, kode yang dapat digunakan kembali, dan ketahanan. Untuk

informasi selengkapnya, lihat Mengintegrasikan layanan mikro dengan menggunakan layanan tanpa AWS server.

arsitektur microservices

Pendekatan untuk membangun aplikasi dengan komponen independen yang menjalankan setiap proses aplikasi sebagai layanan mikro. Layanan mikro ini berkomunikasi melalui antarmuka yang terdefinisi dengan baik dengan menggunakan ringan. APIs Setiap layanan mikro dalam arsitektur ini dapat diperbarui, digunakan, dan diskalakan untuk memenuhi permintaan fungsi tertentu dari suatu aplikasi. Untuk informasi selengkapnya, lihat Menerapkan layanan mikro di AWS.

Program Percepatan Migrasi (MAP)

AWS Program yang menyediakan dukungan konsultasi, pelatihan, dan layanan untuk membantu organisasi membangun fondasi operasional yang kuat untuk pindah ke cloud, dan untuk membantu mengimbangi biaya awal migrasi. MAP mencakup metodologi migrasi untuk mengeksekusi migrasi lama dengan cara metodis dan seperangkat alat untuk mengotomatisasi dan mempercepat skenario migrasi umum.

migrasi dalam skala

Proses memindahkan sebagian besar portofolio aplikasi ke cloud dalam gelombang, dengan lebih banyak aplikasi bergerak pada tingkat yang lebih cepat di setiap gelombang. Fase ini menggunakan praktik dan pelajaran terbaik dari fase sebelumnya untuk mengimplementasikan pabrik migrasi tim, alat, dan proses untuk merampingkan migrasi beban kerja melalui otomatisasi dan pengiriman tangkas. Ini adalah fase ketiga dari strategi AWS migrasi.

pabrik migrasi

Tim lintas fungsi yang merampingkan migrasi beban kerja melalui pendekatan otomatis dan gesit. Tim pabrik migrasi biasanya mencakup operasi, analis dan pemilik bisnis, insinyur migrasi, pengembang, dan DevOps profesional yang bekerja di sprint. Antara 20 dan 50 persen portofolio aplikasi perusahaan terdiri dari pola berulang yang dapat dioptimalkan dengan pendekatan pabrik. Untuk informasi selengkapnya, lihat diskusi tentang pabrik migrasi dan panduan Pabrik Migrasi Cloud di kumpulan konten ini.

metadata migrasi

Informasi tentang aplikasi dan server yang diperlukan untuk menyelesaikan migrasi. Setiap pola migrasi memerlukan satu set metadata migrasi yang berbeda. Contoh metadata migrasi termasuk subnet target, grup keamanan, dan akun. AWS

pola migrasi

Tugas migrasi berulang yang merinci strategi migrasi, tujuan migrasi, dan aplikasi atau layanan migrasi yang digunakan. Contoh: Rehost migrasi ke Amazon EC2 AWS dengan Layanan Migrasi Aplikasi.

Penilaian Portofolio Migrasi (MPA)

Alat online yang menyediakan informasi untuk memvalidasi kasus bisnis untuk bermigrasi ke. AWS Cloud MPA menyediakan penilaian portofolio terperinci (ukuran kanan server, harga, perbandingan TCO, analisis biaya migrasi) serta perencanaan migrasi (analisis data aplikasi dan pengumpulan data, pengelompokan aplikasi, prioritas migrasi, dan perencanaan gelombang). Alat MPA (memerlukan login) tersedia gratis untuk semua AWS konsultan dan konsultan APN Partner.

Penilaian Kesiapan Migrasi (MRA)

Proses mendapatkan wawasan tentang status kesiapan cloud organisasi, mengidentifikasi kekuatan dan kelemahan, dan membangun rencana aksi untuk menutup kesenjangan yang diidentifikasi, menggunakan CAF. AWS Untuk informasi selengkapnya, lihat panduan kesiapan migrasi. MRA adalah tahap pertama dari strategi AWS migrasi.

strategi migrasi

Pendekatan yang digunakan untuk memigrasikan beban kerja ke. AWS Cloud Untuk informasi lebih lanjut, lihat entri 7 Rs di glosarium ini dan lihat Memobilisasi organisasi Anda untuk mempercepat migrasi skala besar.

ML

Lihat pembelajaran mesin.

modernisasi

Mengubah aplikasi usang (warisan atau monolitik) dan infrastrukturnya menjadi sistem yang gesit, elastis, dan sangat tersedia di cloud untuk mengurangi biaya, mendapatkan efisiensi, dan memanfaatkan inovasi. Untuk informasi selengkapnya, lihat Strategi untuk memodernisasi aplikasi di. AWS Cloud

penilaian kesiapan modernisasi

Evaluasi yang membantu menentukan kesiapan modernisasi aplikasi organisasi; mengidentifikasi manfaat, risiko, dan dependensi; dan menentukan seberapa baik organisasi dapat mendukung keadaan masa depan aplikasi tersebut. Hasil penilaian adalah cetak biru arsitektur target, peta

jalan yang merinci fase pengembangan dan tonggak untuk proses modernisasi, dan rencana aksi untuk mengatasi kesenjangan yang diidentifikasi. Untuk informasi lebih lanjut, lihat Mengevaluasi kesiapan modernisasi untuk aplikasi di. AWS Cloud

aplikasi monolitik (monolit)

Aplikasi yang berjalan sebagai layanan tunggal dengan proses yang digabungkan secara ketat. Aplikasi monolitik memiliki beberapa kelemahan. Jika satu fitur aplikasi mengalami lonjakan permintaan, seluruh arsitektur harus diskalakan. Menambahkan atau meningkatkan fitur aplikasi monolitik juga menjadi lebih kompleks ketika basis kode tumbuh. Untuk mengatasi masalah ini, Anda dapat menggunakan arsitektur microservices. Untuk informasi lebih lanjut, lihat Mengurai monolit menjadi layanan mikro.

MPA

Lihat Penilaian Portofolio Migrasi.

MQTT

Lihat Transportasi Telemetri Antrian Pesan.

klasifikasi multiclass

Sebuah proses yang membantu menghasilkan prediksi untuk beberapa kelas (memprediksi satu dari lebih dari dua hasil). Misalnya, model ML mungkin bertanya “Apakah produk ini buku, mobil, atau telepon?” atau “Kategori produk mana yang paling menarik bagi pelanggan ini?”

infrastruktur yang bisa berubah

Model yang memperbarui dan memodifikasi infrastruktur yang ada untuk beban kerja produksi. Untuk meningkatkan konsistensi, keandalan, dan prediktabilitas, AWS Well-Architected Framework merekomendasikan penggunaan infrastruktur yang tidak dapat diubah sebagai praktik terbaik.

O

OAC

Lihat kontrol akses asal.

OAI

Lihat identitas akses asal.

OCM

Lihat manajemen perubahan organisasi.

migrasi offline

Metode migrasi di mana beban kerja sumber diturunkan selama proses migrasi. Metode ini melibatkan waktu henti yang diperpanjang dan biasanya digunakan untuk beban kerja kecil dan tidak kritis.

OI

Lihat integrasi operasi.

OLA

Lihat perjanjian tingkat operasional.

migrasi online

Metode migrasi di mana beban kerja sumber disalin ke sistem target tanpa diambil offline. Aplikasi yang terhubung ke beban kerja dapat terus berfungsi selama migrasi. Metode ini melibatkan waktu henti nol hingga minimal dan biasanya digunakan untuk beban kerja produksi yang kritis.

OPC-UA

Lihat Komunikasi Proses Terbuka - Arsitektur Terpadu.

Komunikasi Proses Terbuka - Arsitektur Terpadu (OPC-UA)

Protokol komunikasi machine-to-machine (M2M) untuk otomasi industri. OPC-UA menyediakan standar interoperabilitas dengan enkripsi data, otentikasi, dan skema otorisasi.

perjanjian tingkat operasional (OLA)

Perjanjian yang menjelaskan apa yang dijanjikan kelompok TI fungsional untuk diberikan satu sama lain, untuk mendukung perjanjian tingkat layanan (SLA).

Tinjauan Kesiapan Operasional (ORR)

Daftar pertanyaan dan praktik terbaik terkait yang membantu Anda memahami, mengevaluasi, mencegah, atau mengurangi ruang lingkup insiden dan kemungkinan kegagalan. Untuk informasi lebih lanjut, lihat Ulasan Kesiapan Operasional (ORR) dalam Kerangka Kerja Well-Architected AWS .

teknologi operasional (OT)

Sistem perangkat keras dan perangkat lunak yang bekerja dengan lingkungan fisik untuk mengendalikan operasi industri, peralatan, dan infrastruktur. Di bidang manufaktur, integrasi sistem OT dan teknologi informasi (TI) adalah fokus utama untuk transformasi Industri 4.0.

integrasi operasi (OI)

Proses modernisasi operasi di cloud, yang melibatkan perencanaan kesiapan, otomatisasi, dan integrasi. Untuk informasi selengkapnya, lihat panduan integrasi operasi.

jejak organisasi

Jejak yang dibuat oleh AWS CloudTrail itu mencatat semua peristiwa untuk semua Akun AWS dalam organisasi di AWS Organizations. Jejak ini dibuat di setiap Akun AWS bagian organisasi dan melacak aktivitas di setiap akun. Untuk informasi selengkapnya, lihat Membuat jejak untuk organisasi dalam CloudTrail dokumentasi.

manajemen perubahan organisasi (OCM)

Kerangka kerja untuk mengelola transformasi bisnis utama yang mengganggu dari perspektif orang, budaya, dan kepemimpinan. OCM membantu organisasi mempersiapkan, dan transisi ke, sistem dan strategi baru dengan mempercepat adopsi perubahan, mengatasi masalah transisi, dan mendorong perubahan budaya dan organisasi. Dalam strategi AWS migrasi, kerangka kerja ini disebut percepatan orang, karena kecepatan perubahan yang diperlukan dalam proyek adopsi cloud. Untuk informasi lebih lanjut, lihat panduan OCM.

kontrol akses asal (OAC)

Di CloudFront, opsi yang disempurnakan untuk membatasi akses untuk mengamankan konten Amazon Simple Storage Service (Amazon S3) Anda. OAC mendukung semua bucket S3 di semua Wilayah AWS, enkripsi sisi server dengan AWS KMS (SSE-KMS), dan dinamis dan permintaan ke bucket S3. `PUT` `DELETE`

identitas akses asal (OAI)

Di CloudFront, opsi untuk membatasi akses untuk mengamankan konten Amazon S3 Anda. Saat Anda menggunakan OAI, CloudFront buat prinsipal yang dapat diautentikasi oleh Amazon S3. Prinsipal yang diautentikasi dapat mengakses konten dalam bucket S3 hanya melalui distribusi tertentu. CloudFront Lihat juga OAC, yang menyediakan kontrol akses yang lebih terperinci dan ditingkatkan.

ORR

Lihat tinjauan kesiapan operasional.

OT

Lihat teknologi operasional.

keluar (jalan keluar) VPC

Dalam arsitektur AWS multi-akun, VPC yang menangani koneksi jaringan yang dimulai dari dalam aplikasi. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan inbound, outbound, dan inspeksi VPCs untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

P

batas izin

Kebijakan manajemen IAM yang dilampirkan pada prinsipal IAM untuk menetapkan izin maksimum yang dapat dimiliki pengguna atau peran. Untuk informasi selengkapnya, lihat Batas izin dalam dokumentasi IAM.

Informasi Identifikasi Pribadi (PII)

Informasi yang, jika dilihat secara langsung atau dipasangkan dengan data terkait lainnya, dapat digunakan untuk menyimpulkan identitas individu secara wajar. Contoh PII termasuk nama, alamat, dan informasi kontak.

PII

Lihat informasi yang dapat diidentifikasi secara pribadi.

buku pedoman

Serangkaian langkah yang telah ditentukan sebelumnya yang menangkap pekerjaan yang terkait dengan migrasi, seperti mengirimkan fungsi operasi inti di cloud. Buku pedoman dapat berupa skrip, runbook otomatis, atau ringkasan proses atau langkah-langkah yang diperlukan untuk mengoperasikan lingkungan modern Anda.

PLC

Lihat pengontrol logika yang dapat diprogram.

PLM

Lihat manajemen siklus hidup produk.

kebijakan

Objek yang dapat menentukan izin (lihat kebijakan berbasis identitas), menentukan kondisi akses (lihat kebijakan berbasis sumber daya), atau menentukan izin maksimum untuk semua akun di organisasi (lihat kebijakan kontrol layanan). AWS Organizations

ketekunan poliglot

Secara independen memilih teknologi penyimpanan data microservice berdasarkan pola akses data dan persyaratan lainnya. Jika layanan mikro Anda memiliki teknologi penyimpanan data yang sama, mereka dapat menghadapi tantangan implementasi atau mengalami kinerja yang buruk. Layanan mikro lebih mudah diimplementasikan dan mencapai kinerja dan skalabilitas yang lebih baik jika mereka menggunakan penyimpanan data yang paling sesuai dengan kebutuhan mereka.

penilaian portofolio

Proses menemukan, menganalisis, dan memprioritaskan portofolio aplikasi untuk merencanakan migrasi. Untuk informasi selengkapnya, lihat Mengevaluasi kesiapan migrasi.

predikat

Kondisi kueri yang mengembalikan `true` atau`false`, biasanya terletak di `WHERE` klausa.

predikat pushdown

Teknik pengoptimalan kueri database yang menyaring data dalam kueri sebelum transfer. Ini mengurangi jumlah data yang harus diambil dan diproses dari database relasional, dan meningkatkan kinerja kueri.

kontrol preventif

Kontrol keamanan yang dirancang untuk mencegah suatu peristiwa terjadi. Kontrol ini adalah garis pertahanan pertama untuk membantu mencegah akses tidak sah atau perubahan yang tidak diinginkan ke jaringan Anda. Untuk informasi selengkapnya, lihat Kontrol pencegahan dalam Menerapkan kontrol keamanan pada. AWS

principal

Entitas AWS yang dapat melakukan tindakan dan mengakses sumber daya. Entitas ini biasanya merupakan pengguna root untuk Akun AWS, peran IAM, atau pengguna. Untuk informasi selengkapnya, lihat Prinsip dalam istilah dan konsep Peran dalam dokumentasi IAM.

privasi berdasarkan desain

Pendekatan rekayasa sistem yang memperhitungkan privasi melalui seluruh proses pengembangan.

zona yang dihosting pribadi

Container yang menyimpan informasi tentang bagaimana Anda ingin Amazon Route 53 merespons kueri DNS untuk domain dan subdomainnya dalam satu atau lebih. VPCs Untuk informasi selengkapnya, lihat Bekerja dengan zona yang dihosting pribadi di dokumentasi Route 53.

kontrol proaktif

Kontrol keamanan yang dirancang untuk mencegah penyebaran sumber daya yang tidak sesuai. Kontrol ini memindai sumber daya sebelum disediakan. Jika sumber daya tidak sesuai dengan kontrol, maka itu tidak disediakan. Untuk informasi selengkapnya, lihat panduan referensi Kontrol dalam AWS Control Tower dokumentasi dan lihat Kontrol proaktif dalam Menerapkan kontrol keamanan pada AWS.

manajemen siklus hidup produk (PLM)

Manajemen data dan proses untuk suatu produk di seluruh siklus hidupnya, mulai dari desain, pengembangan, dan peluncuran, melalui pertumbuhan dan kematangan, hingga penurunan dan penghapusan.

lingkungan produksi

Lihat lingkungan.

pengontrol logika yang dapat diprogram (PLC)

Di bidang manufaktur, komputer yang sangat andal dan mudah beradaptasi yang memantau mesin dan mengotomatiskan proses manufaktur.

rantai cepat

Menggunakan output dari satu prompt LLM sebagai input untuk prompt berikutnya untuk menghasilkan respons yang lebih baik. Teknik ini digunakan untuk memecah tugas yang kompleks menjadi subtugas, atau untuk secara iteratif memperbaiki atau memperluas respons awal. Ini membantu meningkatkan akurasi dan relevansi respons model dan memungkinkan hasil yang lebih terperinci dan dipersonalisasi.

pseudonimisasi

Proses penggantian pengidentifikasi pribadi dalam kumpulan data dengan nilai placeholder. Pseudonimisasi dapat membantu melindungi privasi pribadi. Data pseudonim masih dianggap sebagai data pribadi.

publish/subscribe (pub/sub)

Pola yang memungkinkan komunikasi asinkron antara layanan mikro untuk meningkatkan skalabilitas dan daya tanggap. Misalnya, dalam MES berbasis layanan mikro, layanan mikro dapat mempublikasikan pesan peristiwa ke saluran yang dapat berlangganan layanan mikro lainnya. Sistem dapat menambahkan layanan mikro baru tanpa mengubah layanan penerbitan.

Q

rencana kueri

Serangkaian langkah, seperti instruksi, yang digunakan untuk mengakses data dalam sistem database relasional SQL.

regresi rencana kueri

Ketika pengoptimal layanan database memilih rencana yang kurang optimal daripada sebelum perubahan yang diberikan ke lingkungan database. Hal ini dapat disebabkan oleh perubahan statistik, kendala, pengaturan lingkungan, pengikatan parameter kueri, dan pembaruan ke mesin database.

R

Matriks RACI

Lihat bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan (RACI).

LAP

Lihat Retrieval Augmented Generation.

ransomware

Perangkat lunak berbahaya yang dirancang untuk memblokir akses ke sistem komputer atau data sampai pembayaran dilakukan.

Matriks RASCI

Lihat bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan (RACI).

RCAC

Lihat kontrol akses baris dan kolom.

replika baca

Salinan database yang digunakan untuk tujuan read-only. Anda dapat merutekan kueri ke replika baca untuk mengurangi beban pada database utama Anda.

arsitek ulang

Lihat 7 Rs.

tujuan titik pemulihan (RPO)

Jumlah waktu maksimum yang dapat diterima sejak titik pemulihan data terakhir. Ini menentukan apa yang dianggap sebagai kehilangan data yang dapat diterima antara titik pemulihan terakhir dan gangguan layanan.

tujuan waktu pemulihan (RTO)

Penundaan maksimum yang dapat diterima antara gangguan layanan dan pemulihan layanan.

refactor

Lihat 7 Rs.

Region

Kumpulan AWS sumber daya di wilayah geografis. Masing-masing AWS Region terisolasi dan independen dari yang lain untuk memberikan toleransi kesalahan, stabilitas, dan ketahanan. Untuk informasi selengkapnya, lihat Menentukan Wilayah AWS akun yang dapat digunakan.

regresi

Teknik ML yang memprediksi nilai numerik. Misalnya, untuk memecahkan masalah “Berapa harga rumah ini akan dijual?” Model ML dapat menggunakan model regresi linier untuk memprediksi harga jual rumah berdasarkan fakta yang diketahui tentang rumah (misalnya, luas persegi).

rehost

Lihat 7 Rs.

melepaskan

Dalam proses penyebaran, tindakan mempromosikan perubahan pada lingkungan produksi.

memindahkan

Lihat 7 Rs.

memplatform ulang

Lihat 7 Rs.

pembelian kembali

Lihat 7 Rs.

ketahanan

Kemampuan aplikasi untuk melawan atau pulih dari gangguan. Ketersediaan tinggi dan pemulihan bencana adalah pertimbangan umum ketika merencanakan ketahanan di. AWS Cloud Untuk informasi lebih lanjut, lihat AWS Cloud Ketahanan.

kebijakan berbasis sumber daya

Kebijakan yang dilampirkan ke sumber daya, seperti bucket Amazon S3, titik akhir, atau kunci enkripsi. Jenis kebijakan ini menentukan prinsipal mana yang diizinkan mengakses, tindakan yang didukung, dan kondisi lain yang harus dipenuhi.

matriks yang bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan (RACI)

Matriks yang mendefinisikan peran dan tanggung jawab untuk semua pihak yang terlibat dalam kegiatan migrasi dan operasi cloud. Nama matriks berasal dari jenis tanggung jawab yang didefinisikan dalam matriks: bertanggung jawab (R), akuntabel (A), dikonsultasikan (C), dan diinformasikan (I). Tipe dukungan (S) adalah opsional. Jika Anda menyertakan dukungan, matriks disebut matriks RASCI, dan jika Anda mengecualikannya, itu disebut matriks RACI.

kontrol responsif

Kontrol keamanan yang dirancang untuk mendorong remediasi efek samping atau penyimpangan dari garis dasar keamanan Anda. Untuk informasi selengkapnya, lihat Kontrol responsif dalam Menerapkan kontrol keamanan pada AWS.

melestarikan

Lihat 7 Rs.

pensiun

Lihat 7 Rs.

Retrieval Augmented Generation (RAG)

Teknologi AI generatif di mana LLM merujuk sumber data otoritatif yang berada di luar sumber data pelatihannya sebelum menghasilkan respons. Misalnya, model RAG mungkin melakukan

pencarian semantik dari basis pengetahuan organisasi atau data kustom. Untuk informasi lebih lanjut, lihat Apa itu RAG.

rotasi

Proses memperbarui rahasia secara berkala untuk membuatnya lebih sulit bagi penyerang untuk mengakses kredensil.

kontrol akses baris dan kolom (RCAC)

Penggunaan ekspresi SQL dasar dan fleksibel yang telah menetapkan aturan akses. RCAC terdiri dari izin baris dan topeng kolom.

RPO

Lihat tujuan titik pemulihan.

RTO

Lihat tujuan waktu pemulihan.

buku runbook

Satu set prosedur manual atau otomatis yang diperlukan untuk melakukan tugas tertentu. Ini biasanya dibangun untuk merampingkan operasi berulang atau prosedur dengan tingkat kesalahan yang tinggi.

D

SAML 2.0

Standar terbuka yang digunakan oleh banyak penyedia identitas (IdPs). Fitur ini memungkinkan sistem masuk tunggal gabungan (SSO), sehingga pengguna dapat masuk ke Konsol Manajemen AWS atau memanggil operasi AWS API tanpa Anda harus membuat pengguna di IAM untuk semua orang di organisasi Anda. Untuk informasi lebih lanjut tentang federasi berbasis SAMP 2.0, lihat Tentang federasi berbasis SAMP 2.0 dalam dokumentasi IAM.

SCADA

Lihat kontrol pengawasan dan akuisisi data.

SCP

Lihat kebijakan kontrol layanan.

Rahasia

Dalam AWS Secrets Manager, informasi rahasia atau terbatas, seperti kata sandi atau kredensil pengguna, yang Anda simpan dalam bentuk terenkripsi. Ini terdiri dari nilai rahasia dan metadata-nya. Nilai rahasia dapat berupa biner, string tunggal, atau beberapa string. Untuk informasi selengkapnya, lihat Apa yang ada di rahasia Secrets Manager? dalam dokumentasi Secrets Manager.

keamanan dengan desain

Pendekatan rekayasa sistem yang memperhitungkan keamanan melalui seluruh proses pengembangan.

kontrol keamanan

Pagar pembatas teknis atau administratif yang mencegah, mendeteksi, atau mengurangi kemampuan pelaku ancaman untuk mengeksploitasi kerentanan keamanan. Ada empat jenis kontrol keamanan utama: preventif, detektif, responsif, dan proaktif.

pengerasan keamanan

Proses mengurangi permukaan serangan untuk membuatnya lebih tahan terhadap serangan. Ini dapat mencakup tindakan seperti menghapus sumber daya yang tidak lagi diperlukan, menerapkan praktik keamanan terbaik untuk memberikan hak istimewa paling sedikit, atau menonaktifkan fitur yang tidak perlu dalam file konfigurasi.

sistem informasi keamanan dan manajemen acara (SIEM)

Alat dan layanan yang menggabungkan sistem manajemen informasi keamanan (SIM) dan manajemen acara keamanan (SEM). Sistem SIEM mengumpulkan, memantau, dan menganalisis data dari server, jaringan, perangkat, dan sumber lain untuk mendeteksi ancaman dan pelanggaran keamanan, dan untuk menghasilkan peringatan.

otomatisasi respons keamanan

Tindakan yang telah ditentukan dan diprogram yang dirancang untuk secara otomatis merespons atau memulihkan peristiwa keamanan. Otomatisasi ini berfungsi sebagai kontrol keamanan detektif atau responsif yang membantu Anda menerapkan praktik terbaik AWS keamanan. Contoh tindakan respons otomatis termasuk memodifikasi grup keamanan VPC, menambal instans Amazon EC2, atau memutar kredensil.

enkripsi sisi server

Enkripsi data di tujuannya, oleh Layanan AWS yang menerimanya.

kebijakan kontrol layanan (SCP)

Kebijakan yang menyediakan kontrol terpusat atas izin untuk semua akun di organisasi. AWS Organizations SCPs menentukan pagar pembatas atau menetapkan batasan pada tindakan yang dapat didelegasikan oleh administrator kepada pengguna atau peran. Anda dapat menggunakan SCPs daftar izin atau daftar penolakan, untuk menentukan layanan atau tindakan mana yang diizinkan atau dilarang. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan dalam AWS Organizations dokumentasi.

titik akhir layanan

URL titik masuk untuk file Layanan AWS. Anda dapat menggunakan endpoint untuk terhubung secara terprogram ke layanan target. Untuk informasi selengkapnya, lihat Layanan AWS titik akhir di Referensi Umum AWS.

perjanjian tingkat layanan (SLA)

Perjanjian yang menjelaskan apa yang dijanjikan tim TI untuk diberikan kepada pelanggan mereka, seperti waktu kerja dan kinerja layanan.

indikator tingkat layanan (SLI)

Pengukuran aspek kinerja layanan, seperti tingkat kesalahan, ketersediaan, atau throughputnya.

tujuan tingkat layanan (SLO)

Metrik target yang mewakili kesehatan layanan, yang diukur dengan indikator tingkat layanan.

model tanggung jawab bersama

Model yang menjelaskan tanggung jawab yang Anda bagikan AWS untuk keamanan dan kepatuhan cloud. AWS bertanggung jawab atas keamanan cloud, sedangkan Anda bertanggung jawab atas keamanan di cloud. Untuk informasi selengkapnya, lihat Model tanggung jawab bersama.

SIEM

Lihat informasi keamanan dan sistem manajemen acara.

titik kegagalan tunggal (SPOF)

Kegagalan dalam satu komponen penting dari aplikasi yang dapat mengganggu sistem.

SLA

Lihat perjanjian tingkat layanan.

SLI

Lihat indikator tingkat layanan.

SLO

Lihat tujuan tingkat layanan.

split-and-seed model

Pola untuk menskalakan dan mempercepat proyek modernisasi. Ketika fitur baru dan rilis produk didefinisikan, tim inti berpisah untuk membuat tim produk baru. Ini membantu meningkatkan kemampuan dan layanan organisasi Anda, meningkatkan produktivitas pengembang, dan mendukung inovasi yang cepat. Untuk informasi lebih lanjut, lihat Pendekatan bertahap untuk memodernisasi aplikasi di. AWS Cloud

SPOF

Lihat satu titik kegagalan.

skema bintang

Struktur organisasi database yang menggunakan satu tabel fakta besar untuk menyimpan data transaksional atau terukur dan menggunakan satu atau lebih tabel dimensi yang lebih kecil untuk menyimpan atribut data. Struktur ini dirancang untuk digunakan dalam gudang data atau untuk tujuan intelijen bisnis.

pola ara pencekik

Pendekatan untuk memodernisasi sistem monolitik dengan menulis ulang secara bertahap dan mengganti fungsionalitas sistem sampai sistem warisan dapat dinonaktifkan. Pola ini menggunakan analogi pohon ara yang tumbuh menjadi pohon yang sudah mapan dan akhirnya mengatasi dan menggantikan inangnya. Pola ini diperkenalkan oleh Martin Fowler sebagai cara untuk mengelola risiko saat menulis ulang sistem monolitik. Untuk contoh cara menerapkan pola ini, lihat Memodernisasi layanan web Microsoft ASP.NET (ASMX) lama secara bertahap menggunakan container dan Amazon API Gateway.

subnet

Rentang alamat IP dalam VPC Anda. Subnet harus berada di Availability Zone tunggal.

kontrol pengawasan dan akuisisi data (SCADA)

Di bidang manufaktur, sistem yang menggunakan perangkat keras dan perangkat lunak untuk memantau aset fisik dan operasi produksi.

enkripsi simetris

Algoritma enkripsi yang menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data.

pengujian sintetis

Menguji sistem dengan cara yang mensimulasikan interaksi pengguna untuk mendeteksi potensi masalah atau untuk memantau kinerja. Anda dapat menggunakan Amazon CloudWatch Synthetics untuk membuat tes ini.

sistem prompt

Teknik untuk memberikan konteks, instruksi, atau pedoman ke LLM untuk mengarahkan perilakunya. Permintaan sistem membantu mengatur konteks dan menetapkan aturan untuk interaksi dengan pengguna.

T

tag

Pasangan nilai kunci yang bertindak sebagai metadata untuk mengatur sumber daya Anda. AWS Tanda membantu Anda mengelola, mengidentifikasi, mengatur, dan memfilter sumber daya. Untuk informasi selengkapnya, lihat Menandai AWS sumber daya Anda.

variabel target

Nilai yang Anda coba prediksi dalam ML yang diawasi. Ini juga disebut sebagai variabel hasil. Misalnya, dalam pengaturan manufaktur, variabel target bisa menjadi cacat produk.

daftar tugas

Alat yang digunakan untuk melacak kemajuan melalui runbook. Daftar tugas berisi ikhtisar runbook dan daftar tugas umum yang harus diselesaikan. Untuk setiap tugas umum, itu termasuk perkiraan jumlah waktu yang dibutuhkan, pemilik, dan kemajuan.

lingkungan uji

Lihat lingkungan.

pelatihan

Untuk menyediakan data bagi model ML Anda untuk dipelajari. Data pelatihan harus berisi jawaban yang benar. Algoritma pembelajaran menemukan pola dalam data pelatihan yang

memetakan atribut data input ke target (jawaban yang ingin Anda prediksi). Ini menghasilkan model ML yang menangkap pola-pola ini. Anda kemudian dapat menggunakan model ML untuk membuat prediksi pada data baru yang Anda tidak tahu targetnya.

gerbang transit

Hub transit jaringan yang dapat Anda gunakan untuk menghubungkan jaringan Anda VPCs dan lokal. Untuk informasi selengkapnya, lihat Apa itu gateway transit dalam AWS Transit Gateway dokumentasi.

alur kerja berbasis batang

Pendekatan di mana pengembang membangun dan menguji fitur secara lokal di cabang fitur dan kemudian menggabungkan perubahan tersebut ke cabang utama. Cabang utama kemudian dibangun untuk pengembangan, praproduksi, dan lingkungan produksi, secara berurutan.

akses tepercaya

Memberikan izin ke layanan yang Anda tentukan untuk melakukan tugas di organisasi Anda di dalam AWS Organizations dan di akunnya atas nama Anda. Layanan tepercaya menciptakan peran terkait layanan di setiap akun, ketika peran itu diperlukan, untuk melakukan tugas manajemen untuk Anda. Untuk informasi selengkapnya, lihat Menggunakan AWS Organizations dengan AWS layanan lain dalam AWS Organizations dokumentasi.

penyetelan

Untuk mengubah aspek proses pelatihan Anda untuk meningkatkan akurasi model ML. Misalnya, Anda dapat melatih model ML dengan membuat set pelabelan, menambahkan label, dan kemudian mengulangi langkah-langkah ini beberapa kali di bawah pengaturan yang berbeda untuk mengoptimalkan model.

tim dua pizza

Sebuah DevOps tim kecil yang bisa Anda beri makan dengan dua pizza. Ukuran tim dua pizza memastikan peluang terbaik untuk berkolaborasi dalam pengembangan perangkat lunak.

U

waswas

Sebuah konsep yang mengacu pada informasi yang tidak tepat, tidak lengkap, atau tidak diketahui yang dapat merusak keandalan model ML prediktif. Ada dua jenis ketidakpastian: ketidakpastian epistemik disebabkan oleh data yang terbatas dan tidak lengkap, sedangkan

ketidakpastian aleatorik disebabkan oleh kebisingan dan keacakan yang melekat dalam data. Untuk informasi lebih lanjut, lihat panduan Mengukur ketidakpastian dalam sistem pembelajaran mendalam.

tugas yang tidak terdiferensiasi

Juga dikenal sebagai angkat berat, pekerjaan yang diperlukan untuk membuat dan mengoperasikan aplikasi tetapi itu tidak memberikan nilai langsung kepada pengguna akhir atau memberikan keunggulan kompetitif. Contoh tugas yang tidak terdiferensiasi termasuk pengadaan, pemeliharaan, dan perencanaan kapasitas.

lingkungan atas

Lihat lingkungan.

V

menyedot debu

Operasi pemeliharaan database yang melibatkan pembersihan setelah pembaruan tambahan untuk merebut kembali penyimpanan dan meningkatkan kinerja.

kendali versi

Proses dan alat yang melacak perubahan, seperti perubahan kode sumber dalam repositori.

Peering VPC

Koneksi antara dua VPCs yang memungkinkan Anda untuk merutekan lalu lintas dengan menggunakan alamat IP pribadi. Untuk informasi selengkapnya, lihat Apa itu peering VPC di dokumentasi VPC Amazon.

kerentanan

Kelemahan perangkat lunak atau perangkat keras yang membahayakan keamanan sistem.

W

cache hangat

Cache buffer yang berisi data terkini dan relevan yang sering diakses. Instance database dapat membaca dari cache buffer, yang lebih cepat daripada membaca dari memori utama atau disk.

data hangat

Data yang jarang diakses. Saat menanyakan jenis data ini, kueri yang cukup lambat biasanya dapat diterima.

fungsi jendela

Fungsi SQL yang melakukan perhitungan pada sekelompok baris yang berhubungan dengan catatan saat ini. Fungsi jendela berguna untuk memproses tugas, seperti menghitung rata-rata bergerak atau mengakses nilai baris berdasarkan posisi relatif dari baris saat ini.

beban kerja

Kumpulan sumber daya dan kode yang memberikan nilai bisnis, seperti aplikasi yang dihadapi pelanggan atau proses backend.

aliran kerja

Grup fungsional dalam proyek migrasi yang bertanggung jawab atas serangkaian tugas tertentu. Setiap alur kerja independen tetapi mendukung alur kerja lain dalam proyek. Misalnya, alur kerja portofolio bertanggung jawab untuk memprioritaskan aplikasi, perencanaan gelombang, dan mengumpulkan metadata migrasi. Alur kerja portofolio mengirimkan aset ini ke alur kerja migrasi, yang kemudian memigrasikan server dan aplikasi.

CACING

Lihat menulis sekali, baca banyak.

WQF

Lihat AWS Kerangka Kualifikasi Beban Kerja.

tulis sekali, baca banyak (WORM)

Model penyimpanan yang menulis data satu kali dan mencegah data dihapus atau dimodifikasi. Pengguna yang berwenang dapat membaca data sebanyak yang diperlukan, tetapi mereka tidak dapat mengubahnya. Infrastruktur penyimpanan data ini dianggap tidak dapat diubah.

Z

eksploitasi zero-day

Serangan, biasanya malware, yang memanfaatkan kerentanan zero-day.

kerentanan zero-day

Cacat atau kerentanan yang tak tanggung-tanggung dalam sistem produksi. Aktor ancaman dapat menggunakan jenis kerentanan ini untuk menyerang sistem. Pengembang sering menyadari kerentanan sebagai akibat dari serangan tersebut.

bisikan zero-shot

Memberikan LLM dengan instruksi untuk melakukan tugas tetapi tidak ada contoh (tembakan) yang dapat membantu membimbingnya. LLM harus menggunakan pengetahuan pra-terlatih untuk menangani tugas. Efektivitas bidikan nol tergantung pada kompleksitas tugas dan kualitas prompt. Lihat juga beberapa bidikan yang diminta.

aplikasi zombie

Aplikasi yang memiliki CPU rata-rata dan penggunaan memori di bawah 5 persen. Dalam proyek migrasi, adalah umum untuk menghentikan aplikasi ini.

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.