Membangun program manajemen kerentanan yang dapat diskalakan AWS

AWS Bimbingan Preskriptif

AWS Bimbingan Preskriptif: Membangun program manajemen kerentanan yang dapat diskalakan AWS

Table of Contents

Membangun program manajemen kerentanan yang dapat diskalakan AWS

Anna McAbee dan Megan O'Neil, Amazon Web Services ()AWS

Oktober 2023 (sejarah dokumen)

Bergantung pada teknologi dasar yang Anda gunakan, berbagai alat dan pemindaian dapat menghasilkan temuan keamanan di lingkungan cloud. Tanpa proses untuk menangani temuan ini, mereka dapat mulai menumpuk, seringkali mengarah ke ribuan hingga puluhan ribu temuan dalam waktu singkat. Namun, dengan program manajemen kerentanan terstruktur dan operasionalisasi perkakas Anda yang tepat, organisasi Anda dapat menangani dan melakukan triase sejumlah besar temuan dari beragam sumber.

Manajemen kerentanan berfokus pada menemukan, memprioritaskan, menilai, memulihkan, dan melaporkan kerentanan. Manajemen patch, di sisi lain, berfokus pada menambal atau memperbarui perangkat lunak untuk menghapus atau memulihkan kerentanan keamanan. Manajemen patch hanyalah salah satu aspek dari manajemen kerentanan. Secara umum, kami merekomendasikan untuk membuat patch-in-place proses (juga dikenal sebagai mitigate-in-placeproses) untuk mengatasi skenario kritis, patch-now, dan proses standar yang Anda jalankan pada irama reguler untuk merilis Gambar Mesin Amazon (AMI), kontainer, atau paket perangkat lunak yang ditambal. Proses ini membantu mempersiapkan organisasi Anda untuk merespons kerentanan zero-day dengan cepat. Untuk sistem kritis dalam lingkungan produksi, menggunakan patch-in-place proses bisa lebih cepat dan lebih andal daripada meluncurkan AMI baru di seluruh armada. Untuk patch yang dijadwalkan secara teratur, seperti sistem operasi (OS) dan patch perangkat lunak, kami menyarankan Anda membangun dan menguji menggunakan proses pengembangan standar, seperti halnya perubahan tingkat perangkat lunak. Ini memberikan stabilitas yang lebih baik untuk mode operasi standar. Anda dapat menggunakan Patch Manager, kemampuan AWS Systems Manager, atau produk pihak ketiga lainnya sebagai patch-in-place solusi. Untuk informasi selengkapnya tentang penggunaan Patch Manager, lihat Manajemen patch di AWS Cloud Adoption Framework: Perspektif Operasi. Selain itu, Anda dapat menggunakan EC2 Image Builder untuk mengotomatiskan pembuatan, pengelolaan, dan penyebaran gambar yang disesuaikan up-to-date dan server.

Membangun program manajemen kerentanan yang dapat diskalakan AWS melibatkan pengelolaan perangkat lunak tradisional dan kerentanan jaringan selain risiko konfigurasi cloud. Risiko konfigurasi cloud, seperti bucket Amazon Simple Storage Service (Amazon S3) yang tidak terenkripsi, harus mengikuti proses triase dan remediasi yang serupa dengan kerentanan perangkat lunak. Dalam

kedua kasus ini, tim aplikasi harus memiliki dan bertanggung jawab atas keamanan aplikasi mereka, termasuk infrastruktur yang mendasarinya. Distribusi kepemilikan ini adalah kunci untuk program manajemen kerentanan yang efektif dan terukur.

Panduan ini membahas cara merampingkan identifikasi dan remediasi kerentanan untuk mengurangi risiko secara keseluruhan. Gunakan bagian berikut untuk membangun dan mengulangi program manajemen kerentanan Anda:

1. Siapkan — Persiapkan orang, proses, dan teknologi Anda untuk mengidentifikasi, menilai, dan memulihkan kerentanan di lingkungan Anda.
2. Triase dan remediasi — Rutekan temuan keamanan ke pemangku kepentingan yang relevan, identifikasi tindakan remediasi yang tepat, dan kemudian lakukan tindakan remediasi.
3. Laporkan dan tingkatkan — Gunakan mekanisme pelaporan untuk mengidentifikasi peluang perbaikan, lalu ulangi program manajemen kerentanan Anda.

Membangun program manajemen kerentanan cloud sering kali melibatkan iterasi. Prioritaskan rekomendasi dalam panduan ini dan secara teratur meninjau kembali backlog Anda untuk tetap mengikuti perkembangan teknologi dan persyaratan bisnis Anda.

Audiens yang dituju

Panduan ini ditujukan untuk perusahaan besar yang memiliki tiga tim utama yang bertanggung jawab atas temuan terkait keamanan: tim keamanan, Cloud Center of Excellence (CCoE) atau tim cloud, dan tim aplikasi (atau pengembang). Panduan ini menggunakan model operasi perusahaan yang paling umum dan dibangun di atas model operasi tersebut untuk memungkinkan respons yang lebih efisien terhadap temuan keamanan dan meningkatkan hasil keamanan. Organizations using AWS mungkin memiliki struktur dan model operasi yang berbeda; Namun, Anda dapat memodifikasi banyak konsep dalam panduan ini agar sesuai dengan model operasi yang berbeda dan organisasi yang lebih kecil.

Tujuan

Panduan ini dapat membantu Anda dan organisasi Anda:

- Mengembangkan kebijakan untuk merampingkan manajemen kerentanan dan memastikan akuntabilitas

- Menetapkan mekanisme untuk mendistribusikan tanggung jawab untuk keamanan kepada tim aplikasi
- Konfigurasikan yang relevan AWS layanan sesuai dengan praktik terbaik untuk manajemen kerentanan yang dapat diskalakan
- Mendistribusikan kepemilikan temuan keamanan
- Menetapkan mekanisme untuk melaporkan dan mengulangi program manajemen kerentanan Anda
- Meningkatkan visibilitas pencarian keamanan dan meningkatkan postur keamanan secara keseluruhan

Siapkan program manajemen kerentanan yang dapat diskalakan

Mempersiapkan untuk membangun program manajemen kerentanan yang dapat diskalakan melibatkan mendidik orang, mengembangkan proses, dan menerapkan teknologi yang tepat sesuai dengan praktik terbaik. Orang, proses, dan teknologi sama pentingnya untuk program manajemen kerentanan yang efektif, dan Anda harus mengintegrasikannya dengan erat untuk mengelola kerentanan dalam skala besar.

Bagian panduan ini mengulas tindakan dasar yang dapat Anda ambil untuk mempersiapkan program manajemen kerentanan yang dapat diskalakan. AWS

Topik

Tentukan rencana manajemen kerentanan

Langkah pertama saat menyiapkan program manajemen kerentanan cloud Anda adalah menentukan rencana manajemen kerentanan Anda. Rencana ini mencakup kebijakan dan proses yang diikuti organisasi Anda. Rencana ini harus didokumentasikan dan dapat diakses oleh semua pemangku kepentingan. Rencana manajemen kerentanan adalah dokumen tingkat tinggi yang biasanya mencakup bagian-bagian berikut:

- Tujuan dan ruang lingkup - Garis besar tujuan, fungsi, dan ruang lingkup manajemen kerentanan.
- Peran dan tanggung jawab - Buat daftar pemangku kepentingan manajemen kerentanan dan detail tanggung jawab mereka.
- Tingkat keparahan kerentanan dan definisi prioritas — Tentukan cara mengklasifikasikan tingkat keparahan kerentanan dan cara memprioritaskannya.

- Perjanjian tingkat layanan (SLA) untuk remediasi — Untuk setiap tingkat keparahan, tentukan jumlah waktu maksimum yang dimiliki pemilik remediasi untuk menyelesaikan temuan keamanan. Karena kepatuhan SLA merupakan bagian integral dari memiliki program manajemen kerentanan yang efektif dan dapat diskalakan, pertimbangkan cara melacak apakah Anda memenuhi SLA ini.
- Proses pengecualian - Detail proses pengiriman, persetujuan, dan pembaruan pengecualian. Proses ini harus memastikan bahwa pengecualian sah, terikat waktu, dan dilacak.
- Sumber informasi kerentanan — Daftar sumber atau alat yang menghasilkan temuan keamanan. Untuk informasi lebih lanjut tentang AWS layanan itu bisa menjadi sumber temuan keamanan, lihat Konfigurasikan layanan AWS keamanan di panduan ini.

Meskipun bagian-bagian ini umum di seluruh perusahaan dengan ukuran dan industri yang berbeda, rencana manajemen kerentanan masing-masing organisasi adalah unik. Anda perlu membangun rencana manajemen kerentanan yang paling sesuai untuk organisasi Anda. Berharap untuk mengulangi rencana Anda dari waktu ke waktu untuk menggabungkan pelajaran yang dipetik dan teknologi yang berkembang.

Mendistribusikan kepemilikan keamanan

Model tanggung jawab AWS bersama mendefinisikan bagaimana AWS dan pelanggannya berbagi tanggung jawab atas keamanan dan kepatuhan cloud. Dalam model ini, AWS mengamankan infrastruktur yang menjalankan semua layanan yang ditawarkan di AWS Cloud, dan AWS pelanggan bertanggung jawab untuk mengamankan data dan aplikasi mereka.

Anda dapat mencerminkan model ini di dalam organisasi Anda dan mendistribusikan tanggung jawab antara cloud dan tim aplikasi Anda. Ini membantu Anda menskalakan program keamanan cloud Anda secara lebih efektif karena tim aplikasi mengambil kepemilikan aspek keamanan tertentu dari aplikasi mereka. Interpretasi paling sederhana dari model tanggung jawab bersama adalah bahwa jika Anda memiliki akses untuk mengonfigurasi sumber daya, maka Anda bertanggung jawab atas keamanan sumber daya itu.

Bagian penting dari mendistribusikan tanggung jawab keamanan kepada tim aplikasi adalah membangun alat keamanan swalayan yang membantu tim aplikasi Anda mengotomatisasi. Awalnya, ini bisa menjadi upaya bersama. Tim keamanan dapat menerjemahkan persyaratan keamanan ke dalam alat pemindaian kode, dan kemudian tim aplikasi dapat menggunakan alat tersebut untuk membangun dan berbagi solusi dengan komunitas pengembang internal mereka. Ini berkontribusi pada efisiensi yang lebih besar di seluruh tim lain yang perlu memenuhi persyaratan keamanan serupa.

Tabel berikut menguraikan langkah-langkah untuk mendistribusikan kepemilikan ke tim aplikasi dan memberikan contoh.

Langkah	Tindakan	Contoh
1	Tentukan persyaratan keamanan Anda — Apa yang ingin Anda capai? Ini mungkin berasal dari standar keamanan atau persyaratan kepatuhan.	Contoh persyaratan keamanan adalah akses hak istimewa paling sedikit untuk identitas aplikasi.
2	Menghitung kontrol untuk persyaratan keamanan — Apa arti persyaratan ini sebenarnya dari perspektif kontrol? Apa yang harus saya lakukan untuk mencapai ini?	Untuk mencapai hak istimewa terkecil untuk identitas aplikasi, berikut ini adalah dua kontrol sampel: • Gunakan AWS Identity and Access Management peran (IAM) • Jangan gunakan wildcard dalam kebijakan IAM
3	Panduan dokumen untuk kontrol — Dengan kontrol ini, panduan apa yang dapat Anda berikan kepada pengembang untuk membantu mereka mematuhi kontrol?	Awalnya, Anda dapat memulai dengan mendokumentasikan kebijakan contoh sederhana, termasuk kebijakan IAM yang aman dan tidak aman serta kebijakan bucket Amazon Simple Storage Service (Amazon S3). Selanjutnya, Anda dapat menyematkan solusi pemindaian kebijakan dalam pipeline integrasi berkelanjutan dan pengiriman berkelanjutan (CI/CD), seperti

Langkah	Tindakan	Contoh
		menggunakan aturan untuk evaluasi proaktif.AWS Config
4	Kembangkan artefak yang dapat digunakan kembali — Dengan panduan ini, dapatkah Anda membuatnya lebih mudah dan mengembangkan artefak yang dapat digunakan kembali untuk pengembang?	Anda dapat membuat infrastruktur sebagai kode (IAc) untuk menerapkan kebijakan IAM yang mengikuti prinsip hak istimewa paling rendah. Anda dapat menyimpan artefak yang dapat digunakan kembali ini dalam repositori kode.

Layanan mandiri mungkin tidak berfungsi untuk semua persyaratan keamanan, tetapi dapat berfungsi untuk skenario standar. Dengan mengikuti langkah-langkah ini, organisasi dapat memberdayakan tim aplikasi mereka untuk menangani lebih banyak tanggung jawab keamanan mereka sendiri dengan cara yang terukur. Secara keseluruhan, model tanggung jawab terdistribusi mengarah pada praktik keamanan yang lebih kolaboratif dalam banyak organisasi.

Mengembangkan program pengungkapan kerentanan

Untuk defense-in-depthpendekatan manajemen kerentanan, buat program pengungkapan kerentanan sehingga orang di dalam atau di luar organisasi Anda dapat melaporkan kerentanan atau risiko keamanan.

Untuk orang-orang di dalam organisasi Anda, buat proses untuk mengirimkan risiko atau kerentanan. Ini dapat dilakukan melalui sistem tiket atau email. Terlepas dari proses yang Anda pilih, penting bagi karyawan Anda untuk mengetahui prosesnya dan dapat dengan mudah mengirimkan kerentanan atau risiko apa pun yang mereka hadapi.

Untuk orang-orang di luar organisasi Anda, buat halaman web eksternal untuk mengirimkan potensi kerentanan keamanan. Sebagai contoh, lihat halaman web Pelaporan AWS Kerentanan. Halaman web ini juga harus berisi pedoman pengungkapan untuk membantu melindungi data dan aset organisasi Anda. Program pengungkapan kerentanan seharusnya tidak mendorong aktivitas yang berpotensi berbahaya, jadi penting bagi Anda untuk memiliki kebijakan yang jelas dengan pedoman. Membangun program pengungkapan yang matang dan bertanggung jawab adalah tujuan yang

harus diperjuangkan saat Anda mematangkan program Anda. Sebagian besar tidak memulai dengan program pengungkapan eksternal, dan butuh waktu untuk melakukannya dengan benar.

Persiapkan AWS lingkungan Anda

Sebelum menerapkan alat manajemen kerentanan apa pun, pastikan AWS lingkungan Anda dirancang untuk mendukung program manajemen kerentanan yang dapat diskalakan. Struktur kebijakan penandaan Anda Akun AWS dan organisasi Anda dapat menyederhanakan proses membangun program manajemen kerentanan yang dapat diskalakan.

Kembangkan Akun AWS struktur

AWS Organizationsmembantu mengelola dan mengatur AWS lingkungan secara terpusat saat bisnis Anda tumbuh dan meningkatkan sumber dayanya AWS . Sebuah organisasi dalam AWS Organizations mengkonsolidasikan Anda Akun AWS ke dalam kelompok logis, atau unit organisasi, sehingga Anda dapat mengelolanya sebagai satu unit. Anda mengelola AWS Organizations dari akun khusus, yang disebut akun manajemen. Untuk informasi lebih lanjut, lihat AWS Organizations terminologi dan konsep.

Kami menyarankan Anda mengelola lingkungan AWS multi-akun Anda di AWS Organizations. Ini membantu membuat inventaris lengkap akun dan sumber daya perusahaan Anda. Inventaris aset lengkap ini merupakan aspek penting dari manajemen kerentanan. Tim aplikasi tidak boleh menggunakan akun yang berada di luar organisasi.

AWS Control Towermembantu Anda mengatur dan mengatur lingkungan AWS multi-akun, mengikuti praktik terbaik preskriptif. Jika Anda belum membangun lingkungan multi-akun, AWS Control Tower adalah titik awal yang baik.

Sebaiknya gunakan struktur akun khusus dan praktik terbaik yang dijelaskan dalam Arsitektur Referensi AWS Keamanan (AWS SRA). Akun Alat Keamanan harus berfungsi sebagai administrator yang didelegasikan untuk layanan keamanan Anda. Informasi lebih lanjut tentang mengonfigurasi alat manajemen kerentanan Anda di akun ini disediakan nanti dalam panduan ini. Host aplikasi di akun khusus di unit organisasi Beban Kerja (OU). Ini menetapkan isolasi tingkat beban kerja yang kuat dan batasan keamanan eksplisit untuk setiap aplikasi. Untuk informasi tentang prinsip desain dan manfaat menggunakan pendekatan multi-akun, lihat Mengatur AWS Lingkungan Anda Menggunakan Beberapa Akun (AWS whitepaper).

Memiliki struktur akun yang disengaja dan mengelola layanan keamanan secara terpusat dari akun khusus adalah aspek penting dari program manajemen kerentanan yang dapat diskalakan.

Mendefinisikan, menerapkan, dan menegakkan tag

Tag adalah pasangan nilai kunci yang bertindak sebagai metadata untuk mengatur sumber daya Anda. AWS Untuk informasi selengkapnya, lihat Menandai AWS sumber daya Anda. Anda dapat menggunakan tag untuk menyediakan konteks bisnis, seperti unit bisnis, pemilik aplikasi, lingkungan, dan pusat biaya. Tabel berikut menunjukkan satu set tag sampel.

Kunci	Nilai
BusinessUnit	HumanResources
CostCenter	CC101
ApplicationTeam	HumanResourcesTechnology
Environment	Produksi

Tag dapat membantu Anda memprioritaskan temuan. Misalnya, ini dapat membantu Anda:

- Identifikasi pemilik sumber daya yang bertanggung jawab untuk menambal kerentanan
- Lacak aplikasi atau unit bisnis mana yang memiliki banyak temuan
- Meningkatkan tingkat keparahan temuan untuk klasifikasi data tertentu, seperti data informasi identifikasi pribadi (PII) atau industri kartu pembayaran (PCI)
- Mengidentifikasi jenis data di lingkungan, seperti data uji di lingkungan pengembangan tingkat rendah atau data produksi

Untuk membantu Anda mencapai penandaan yang efektif dalam skala besar, ikuti petunjuk dalam Membangun strategi penandaan Anda di Praktik Terbaik untuk AWS Sumber Daya Penandaan (AWS whitepaper).

Pantau buletin AWS keamanan

Kami sangat menyarankan pemantauan buletin AWS keamanan secara teratur dan sering. Buletin keamanan dapat memberi tahu Anda tentang kerentanan terkait keamanan baru, layanan yang terpengaruh, dan pembaruan yang berlaku. Anda juga dapat berlangganan umpan RSS untuk buletin keamanan dan membangun proses untuk menelan dan menangani buletin ini sebagai bagian dari program manajemen kerentanan Anda.

Konfigurasikan layanan AWS keamanan

AWS menawarkan berbagai layanan keamanan yang dirancang untuk membantu melindungi AWS lingkungan Anda. Untuk program manajemen kerentanan Anda, kami sarankan Anda mengaktifkan yang berikut AWS layanan di setiap akun:

- Amazon GuardDuty membantu mendeteksi ancaman aktif di lingkungan Anda. GuardDutyTemuan dapat membantu Anda mengidentifikasi kerentanan yang tidak diketahui yang dieksploitasi di lingkungan Anda. Ini juga dapat membantu Anda memahami efek dari kerentanan yang belum ditambal.
- AWS Healthmemberikan visibilitas berkelanjutan ke kinerja sumber daya Anda dan ketersediaan akun Anda AWS layanan .
- AWS Identity and Access Management Access Analyzermenganalisis kebijakan berbasis sumber daya di AWS lingkungan Anda untuk mengidentifikasi sumber daya yang dibagikan dengan entitas eksternal. Ini dapat membantu Anda mengidentifikasi kerentanan yang terkait dengan akses yang tidak diinginkan ke sumber daya dan data Anda. Untuk setiap instance sumber daya yang dibagikan di luar akun Anda, IAM Access Analyzer menghasilkan temuan.
- Amazon Inspector adalah layanan manajemen kerentanan yang terus memindai AWS beban kerja Anda untuk kerentanan perangkat lunak dan paparan jaringan yang tidak diinginkan.
- AWS Security Hubmembantu Anda memeriksa AWS lingkungan Anda terhadap standar industri keamanan dan dapat mengidentifikasi risiko konfigurasi cloud. Ini juga memberikan pandangan komprehensif tentang keadaan AWS keamanan Anda dengan menggabungkan temuan dari layanan AWS keamanan lain dan alat keamanan pihak ketiga.

Bagian ini membahas cara mengaktifkan dan mengonfigurasi Amazon Inspector dan Security Hub untuk membantu Anda membuat program manajemen kerentanan yang dapat diskalakan.

Menggunakan Amazon Inspector dalam program manajemen kerentanan Anda

Amazon Inspector adalah layanan manajemen kerentanan yang terus-menerus memindai image wadah Amazon Elastic Compute Cloud (Amazon EC2), instans Amazon Elastic Container Registry (Amazon ECR), dan berfungsi untuk kerentanan perangkat lunak dan eksposur jaringan yang tidak diinginkan. AWS Lambda Anda dapat menggunakan Amazon Inspector untuk mendapatkan visibilitas dan memprioritaskan resolusi kerentanan perangkat lunak di seluruh lingkungan Anda. AWS

Amazon Inspector terus menilai lingkungan Anda sepanjang siklus hidup sumber daya Anda. Ini secara otomatis memindai kembali sumber daya sebagai respons terhadap perubahan yang dapat memperkenalkan kerentanan baru. Misalnya, ini memindai ulang saat Anda menginstal paket baru pada instans EC2, saat Anda menginstal tambalan, atau ketika kerentanan dan eksposur umum baru (CVE) yang memengaruhi sumber daya dipublikasikan. Ketika Amazon Inspector mengidentifikasi kerentanan atau jalur jaringan terbuka, Amazon Inspector menghasilkan temuan yang dapat Anda selidiki. Temuan ini memberikan informasi komprehensif tentang kerentanan, termasuk yang berikut:

- Skor risiko Amazon Inspector
- Skor Common Vulnerability Scoring System (CVSS)
- Sumber daya yang terpengaruh
- Data intelijen kerentanan tentang CVE dari Amazon,, dan Recorded FutureCybersecurity and Infrastructure Security Agency (CISA)
- Rekomendasi remediasi

Untuk petunjuk cara menyiapkan Amazon Inspector, lihat Memulai Amazon Inspector. Langkah Activate Amazon Inspector dalam tutorial ini menyediakan dua opsi konfigurasi: lingkungan akun mandiri dan lingkungan multi-akun. Sebaiknya gunakan opsi lingkungan multi-akun jika Anda ingin memantau beberapa Akun AWS anggota organisasi. AWS Organizations

Saat menyiapkan Amazon Inspector untuk lingkungan multi-akun, Anda menetapkan akun di organisasi untuk menjadi administrator yang didelegasikan Amazon Inspector. Administrator yang didelegasikan dapat mengelola temuan dan beberapa pengaturan untuk anggota organisasi. Misalnya, administrator yang didelegasikan dapat melihat detail temuan agregat untuk semua akun anggota, mengaktifkan atau menonaktifkan pemindaian untuk akun anggota, dan meninjau sumber daya yang dipindai. AWS SRA merekomendasikan agar Anda membuat akun Security Tooling dan menggunakannya sebagai administrator yang didelegasikan Amazon Inspector.

Menggunakan AWS Security Hub dalam program manajemen kerentanan Anda

Membangun program manajemen kerentanan yang dapat diskalakan AWS melibatkan pengelolaan perangkat lunak tradisional dan kerentanan jaringan selain risiko konfigurasi cloud. AWS Security Hubmembantu Anda memeriksa AWS lingkungan Anda terhadap standar industri keamanan dan dapat mengidentifikasi risiko konfigurasi cloud. Security Hub juga memberikan pandangan

komprehensif tentang status keamanan Anda AWS dengan menggabungkan temuan keamanan dari layanan keamanan lain dan AWS alat keamanan pihak ketiga.

Di bagian berikut, kami memberikan praktik dan rekomendasi terbaik untuk menyiapkan Security Hub guna mendukung program manajemen kerentanan Anda:

- Menyiapkan Security Hub
- Mengaktifkan standar Security Hub
- Mengelola temuan Security Hub
- Menggabungkan temuan dari layanan dan alat keamanan lainnya

Menyiapkan Security Hub

Untuk petunjuk penyiapan, lihat Menyiapkan AWS Security Hub. Untuk menggunakan Security Hub, Anda harus mengaktifkan AWS Config. Untuk informasi selengkapnya, lihat Mengaktifkan dan mengonfigurasi AWS Config dalam dokumentasi Security Hub.

Jika Anda terintegrasi dengan AWS Organizations, dari akun manajemen organisasi, Anda menetapkan akun untuk menjadi administrator yang didelegasikan Security Hub. Untuk petunjuknya, lihat Menunjuk administrator yang didelegasikan Security Hub. AWS SRA merekomendasikan agar Anda membuat akun Security Tooling dan menggunakannya sebagai administrator yang didelegasikan Security Hub.

Administrator yang didelegasikan secara otomatis memiliki akses untuk mengonfigurasi Security Hub untuk semua akun anggota di organisasi dan untuk melihat temuan yang terkait dengan akun tersebut. Kami menyarankan Anda mengaktifkan AWS Config Security Hub di semua Wilayah AWS dan semua milik Anda Akun AWS. Anda dapat mengonfigurasi Security Hub untuk secara otomatis memperlakukan akun organisasi baru sebagai akun anggota Security Hub. Untuk petunjuk, lihat Mengelola akun anggota milik organisasi.

Mengaktifkan standar Security Hub

Security Hub menghasilkan temuan dengan menjalankan pemeriksaan keamanan otomatis dan berkelanjutan terhadap kontrol keamanan. Kontrol dikaitkan dengan satu atau lebih standar keamanan. Kontrol membantu Anda menentukan apakah persyaratan dalam suatu standar terpenuhi.

Saat Anda mengaktifkan standar di Security Hub, Security Hub secara otomatis mengaktifkan kontrol yang berlaku untuk standar. Security Hub menggunakan AWS Config aturan untuk melakukan sebagian besar pemeriksaan keamanannya untuk kontrol. Anda dapat mengaktifkan

atau menonaktifkan standar Security Hub kapan saja. Untuk informasi selengkapnya, lihat Kontrol dan standar keamanan di AWS Security Hub. Untuk daftar lengkap standar, lihat Referensi standar Security Hub.

Jika organisasi Anda belum memiliki standar keamanan pilihan, sebaiknya gunakan standar AWS Foundational Security Best Practices (FSBP). Standar ini dirancang untuk mendeteksi kapan Akun AWS dan sumber daya menyimpang dari praktik terbaik keamanan. AWS mengkurasi standar ini dan memperbaruinya secara teratur untuk mencakup fitur dan layanan baru. Setelah memuji temuan FSBP, pertimbangkan untuk mengaktifkan standar lain.

Mengelola temuan Security Hub

Security Hub menyediakan beberapa fitur yang membantu Anda mengatasi sejumlah besar temuan dari seluruh organisasi Anda dan memahami keadaan keamanan AWS lingkungan Anda. Untuk membantu Anda mengelola temuan, sebaiknya aktifkan dua fitur Security Hub berikut:

- Gunakan agregasi lintas wilayah untuk mengumpulkan temuan, menemukan pembaruan, wawasan, mengontrol status kepatuhan, dan skor keamanan dari beberapa Wilayah AWS ke satu Wilayah agregasi.
- Gunakan temuan kontrol terkonsolidasi untuk mengurangi kebisingan temuan dengan menghapus temuan duplikat. Ketika temuan kontrol konsolidasi diaktifkan di akun Anda, Security Hub menghasilkan satu temuan baru atau menemukan pembaruan untuk setiap pemeriksaan keamanan kontrol, bahkan jika kontrol berlaku untuk beberapa standar yang diaktifkan.

Menggabungkan temuan dari layanan dan alat keamanan lainnya

Selain menghasilkan temuan keamanan, Anda dapat menggunakan Security Hub untuk mengumpulkan data pencarian dari beberapa AWS layanan solusi keamanan pihak ketiga yang didukung. Bagian ini berfokus pada pengiriman temuan keamanan ke Security Hub. Bagian selanjutnyaBersiaplah untuk menetapkan temuan keamanan, membahas bagaimana Anda dapat mengintegrasikan Security Hub dengan produk yang dapat menerima temuan dari Security Hub.

Ada banyak produk pihak ketiga AWS layanan, dan solusi sumber terbuka yang dapat Anda integrasikan dengan Security Hub. Jika Anda baru memulai, kami sarankan untuk melakukan hal berikut:

1. Aktifkan terintegrasi AWS layanan — Sebagian besar AWS layanan integrasi yang mengirim temuan ke Security Hub diaktifkan secara otomatis setelah Anda mengaktifkan Security Hub dan

layanan terintegrasi. Untuk program manajemen kerentanan Anda, sebaiknya aktifkan Amazon Inspector, GuardDuty AWS Health Amazon, dan IAM Access Analyzer di setiap akun. Layanan ini secara otomatis mengirimkan temuan mereka ke Security Hub. Untuk daftar lengkap AWS layanan integrasi yang didukung, lihat AWS layanan yang mengirimkan temuan ke Security Hub.

> **Note**
>
> AWS Health mengirimkan temuan ke Security Hub jika salah satu dari kondisi berikut terpenuhi:
>
> - Temuan ini terkait dengan layanan AWS keamanan
> - Typecode temuan berisi kata-kata`security`,, `abuse` atau `certificate`
> - AWS Health Layanan pencarian adalah `risk` atau `abuse`

2. Menyiapkan integrasi pihak ketiga — Untuk daftar integrasi yang saat ini didukung, lihat Integrasi produk mitra pihak ketiga yang tersedia. Pilih alat tambahan yang dapat mengirim temuan ke atau menerima temuan dari Security Hub. Anda mungkin sudah memiliki beberapa alat pihak ketiga ini. Ikuti petunjuk produk untuk mengonfigurasi integrasi dengan Security Hub.

Bersiaplah untuk menetapkan temuan keamanan

Di bagian ini, Anda menyiapkan alat yang digunakan tim Anda untuk mengelola dan menetapkan temuan keamanan. Bagian ini mencakup opsi berikut:

- Kelola temuan di alat dan alur kerja yang ada— Opsi ini terintegrasi AWS Security Hub dengan sistem yang ada yang digunakan tim Anda untuk mengelola tugas sehari-hari mereka, seperti backlog produk. Opsi ini direkomendasikan untuk tim yang telah membuat alat untuk mengelola alur kerja mereka.
- Mengelola temuan di Security Hub— Opsi ini mengonfigurasi pemberitahuan untuk peristiwa Security Hub sehingga tim yang sesuai menerima peringatan dan dapat mengatasi temuan di Security Hub.

Tentukan alur kerja mana yang paling cocok untuk tim Anda, dan pastikan bahwa temuan keamanan dapat membuatnya segera kepada pemiliknya masing-masing.

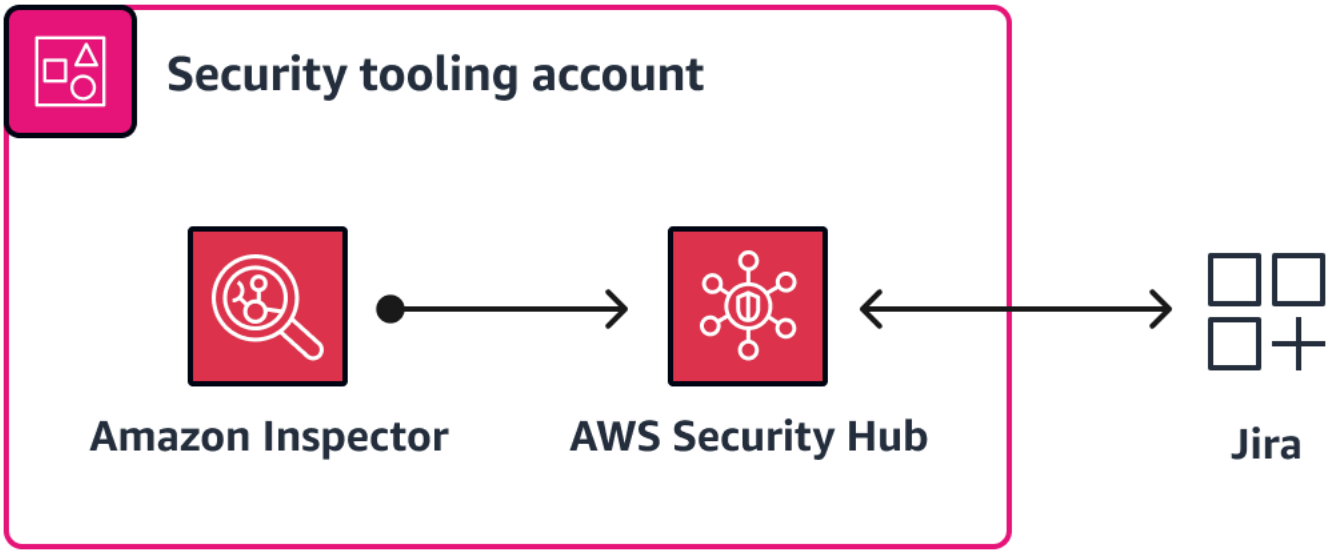
Kelola temuan di alat dan alur kerja yang ada

Kami merekomendasikan integrasi Security Hub tambahan untuk organisasi perusahaan yang telah membuat alat yang digunakan tim untuk mengelola atau melakukan tugas sehari-hari mereka. Anda dapat mengimpor data pencarian Security Hub ke beberapa platform teknologi. Contohnya termasuk:

- Sistem informasi keamanan dan manajemen acara (SIEM) membantu tim keamanan melakukan triase peristiwa keamanan operasional. Sistem SIEM menyediakan analisis real-time dari peringatan keamanan yang dihasilkan oleh aplikasi dan perangkat keras jaringan.
- Sistem tata kelola, risiko, dan kepatuhan (GRC) membantu tim kepatuhan dan tata kelola memantau dan melaporkan data manajemen risiko. Alat GRC adalah aplikasi perangkat lunak yang dapat digunakan bisnis untuk mengelola kebijakan, menilai risiko, mengontrol akses pengguna, dan merampingkan kepatuhan. Anda dapat menggunakan alat GRC untuk mengintegrasikan proses bisnis, mengurangi biaya, dan meningkatkan efisiensi.
- Sistem backlog dan tiket produk membantu tim aplikasi dan cloud mengelola fitur dan memprioritaskan tugas pengembangan. Atlassian Jiradan Microsoft Azure DevOpsmerupakan contoh dari sistem ini.

Mengintegrasikan temuan Security Hub secara langsung dengan sistem perusahaan yang ada ini dapat meningkatkan mean time to recovery (MTTR) dan hasil keamanan karena alur kerja operasional harian tidak harus berubah. Tim dapat merespons dan belajar dari temuan keamanan lebih cepat karena mereka tidak harus menggunakan alur kerja dan alat yang terpisah. Integrasi menjadikan pengalamatan temuan keamanan sebagai bagian dari alur kerja standar yang normal.

Security Hub terintegrasi dengan beberapa produk mitra pihak ketiga. Untuk daftar lengkap dan petunjuk, lihat Integrasi produk mitra pihak ketiga yang tersedia di dokumentasi Security Hub. Integrasi umum termasuk Atlassian - Jira Service Management, terintegrasi dua arah AWS Security Hub dengan Jira perangkat lunak, dan. ServiceNow – ITSM Diagram berikut menunjukkan bagaimana Anda dapat mengonfigurasi Amazon Inspector untuk mengirim temuan ke Security Hub dan kemudian mengonfigurasi Security Hub untuk mengirim semua temuan. Jira



Mengelola temuan di Security Hub

Anda dapat membuat sistem notifikasi berbasis cloud untuk temuan Security Hub dengan menggunakan EventBridge aturan Amazon dan topik Amazon Simple Notification Service (Amazon SNS). Sistem ini memberi tahu tim yang sesuai tentang temuan saat dibuat. Untuk pendekatan ini, strategi multi-akun yang dijelaskan dalam Kembangkan Akun AWS struktur sangat penting karena aplikasi dipisahkan menjadi akun khusus. Ini membantu Anda memberi tahu tim yang tepat untuk setiap temuan.

Tim keamanan atau cloud mungkin memilih untuk menerima acara dari semua Akun AWS. Dalam hal ini, buat EventBridge aturan dalam akun administrator yang didelegasikan Security Hub dan berlangganan topik Amazon SNS yang memberi tahu tim ini. Untuk tim aplikasi, konfigurasikan EventBridge aturan dan topik SNS dalam akun aplikasi masing-masing. Ketika temuan Security Hub terjadi dalam akun aplikasi, tim yang bertanggung jawab akan diberitahu tentang temuan tersebut.

Security Hub sudah secara otomatis mengirimkan semua temuan baru dan semua pembaruan temuan yang ada ke EventBridge sebagai Temuan Security Hub - Acara yang diimpor. Setiap Temuan Security Hub - Acara yang diimpor berisi satu temuan. Anda dapat menerapkan filter pada EventBridge aturan sehingga temuan memulai aturan hanya jika temuan cocok dengan filter. Untuk petunjuk, lihat Mengonfigurasi EventBridge aturan untuk temuan yang dikirim secara otomatis. Untuk informasi selengkapnya tentang membuat dan berlangganan topik Amazon SNS, lihat Mengonfigurasi Amazon SNS.

Pertimbangkan hal berikut saat menggunakan pendekatan ini:

- Untuk tim aplikasi, buat EventBridge aturan di masing-masing Akun AWS dan Wilayah AWS di mana aplikasi di-host.
- Untuk tim keamanan dan cloud, buat EventBridge aturan di akun administrator yang didelegasikan Security Hub. Ini memberi tahu tim tentang semua temuan di akun anggota.
- Amazon SNS mengirimkan pemberitahuan setiap hari jika status temuan keamanan adalah. `NEW` Jika Anda ingin mematikan notifikasi harian, Anda dapat membuat AWS Lambda fungsi khusus yang mengubah status temuan dari `NEW` menjadi `NOTIFIED` setelah pelanggan Amazon SNS menerima notifikasi.

Triase dan remediasi temuan keamanan di lingkungan Anda AWS

Triaging temuan keamanan melibatkan routing temuan ke pemangku kepentingan yang tepat, menilai dan memprioritaskan temuan, kemudian memulihkannya. Bagian ini meninjau setiap langkah ini secara rinci dan memberikan rekomendasi untuk skalabilitas dan efisiensi. Ini juga mencakup contoh untuk membantu menggambarkan proses triase dan remediasi.

Topik

Mendefinisikan kepemilikan temuan keamanan

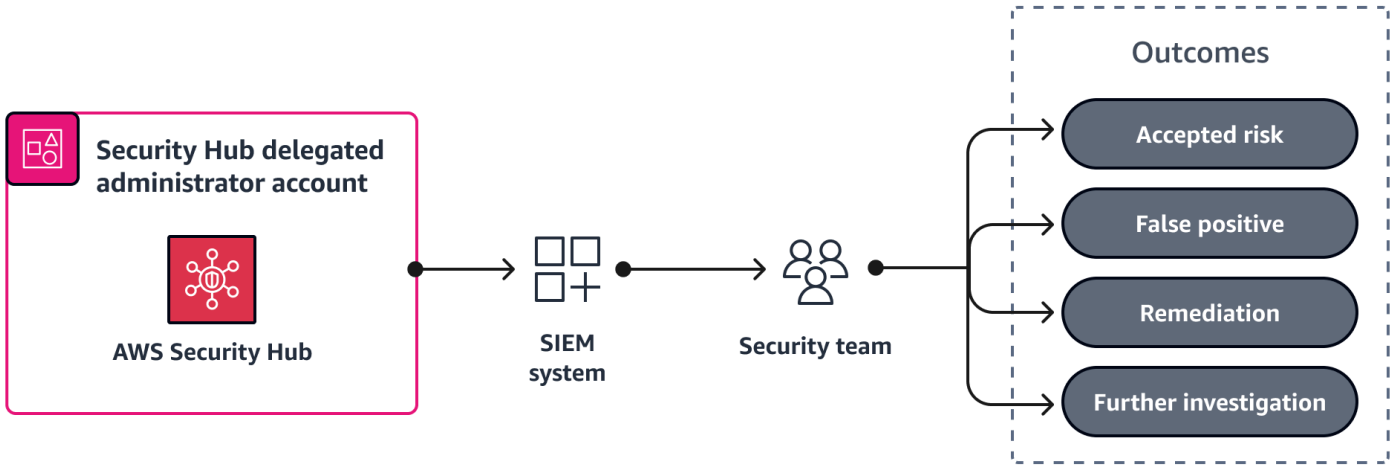
Mendefinisikan model kepemilikan untuk triase temuan keamanan bisa menjadi tantangan, tetapi tidak harus demikian. Lanskap keamanan berubah secara konstan, dan praktisi harus fleksibel untuk beradaptasi dengan perubahan ini. Mengadopsi pendekatan fleksibel untuk mengembangkan model kepemilikan Anda untuk temuan keamanan. Model awal Anda harus memungkinkan tim Anda untuk segera bertindak. Kami merekomendasikan memulai dengan logika kepemilikan dasar dan menyempurnakan logika itu dari waktu ke waktu. Jika Anda menunda untuk menentukan kriteria kepemilikan yang sempurna, jumlah temuan keamanan akan terus bertambah.

Untuk memfasilitasi penugasan temuan ke tim dan sumber daya yang sesuai, kami sarankan untuk mengintegrasikan AWS Security Hub dengan sistem yang ada yang digunakan tim Anda untuk mengelola tugas sehari-hari mereka. Misalnya, Anda dapat mengintegrasikan Security Hub dengan sistem informasi keamanan dan manajemen acara (SIEM) atau sistem backlog dan tiket produk. Untuk informasi selengkapnya, lihat Bersiaplah untuk menetapkan temuan keamanan dalam panduan ini.

Berikut ini adalah contoh model kepemilikan yang dapat Anda gunakan sebagai titik awal:

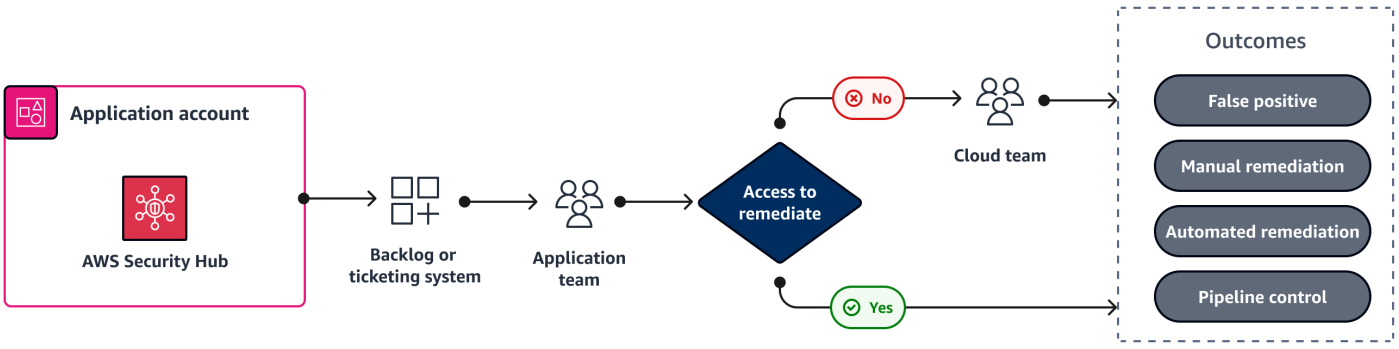
- Tim keamanan meninjau ancaman yang berpotensi aktif dan membantu menilai dan memprioritaskan temuan keamanan. Tim keamanan memiliki keahlian dan alat untuk mengevaluasi konteks dengan benar. Mereka memahami data terkait keamanan tambahan yang membantu

mereka menilai dan memprioritaskan kerentanan dan menyelidiki peristiwa deteksi ancaman. Jika menemukan tingkat keparahan atau penyetelan tambahan diperlukan, lihat Menilai dan memprioritaskan temuan keamanan bagian dalam panduan ini. Sebagai contoh, lihat Contoh tim keamanan di panduan ini.



- Mendistribusikan temuan keamanan antara tim cloud dan aplikasi — Seperti yang dibahas di Mendistribusikan kepemilikan keamanan bagian ini, tim yang memiliki akses untuk mengonfigurasi sumber daya bertanggung jawab atas konfigurasi amannya. Tim aplikasi bertanggung jawab atas temuan keamanan yang terkait dengan sumber daya yang mereka bangun dan konfigurasikan, dan tim cloud bertanggung jawab atas temuan keamanan yang terkait dengan konfigurasi yang luas. Dalam kebanyakan kasus, tim aplikasi tidak memiliki akses untuk mengubah konfigurasi jangkauan luas dan AWS layanan, seperti, kebijakan kontrol layanan (SCP) di AWS Control Tower, konfigurasi VPC AWS Organizations terkait jaringan, dan Pusat Identitas IAM.AWS

  Untuk lingkungan multi-akun yang memisahkan aplikasi ke dalam akun khusus, Anda biasanya dapat mengintegrasikan temuan terkait keamanan untuk akun ke dalam sistem backlog atau tiket aplikasi. Dari sistem itu, tim cloud atau tim aplikasi dapat mengatasi temuan tersebut. Sebagai contoh, lihat Contoh tim cloud atau Contoh tim aplikasi dalam panduan ini.



- Tetapkan temuan yang tersisa dan belum terselesaikan ke tim cloud — Temuan sisa mungkin terkait dengan pengaturan default atau konfigurasi jangkauan luas yang dapat ditangani oleh tim cloud. Tim ini kemungkinan memiliki pengetahuan dan akses paling historis untuk menyelesaikan temuan tersebut. Secara keseluruhan, ini biasanya merupakan bagian yang jauh lebih kecil dari total temuan.

Menilai dan memprioritaskan temuan keamanan

Komponen penting dari program manajemen kerentanan yang efektif adalah kemampuan untuk menilai dan memprioritaskan temuan keamanan. Di sinilah menarik konteks, sejarah organisasi, dan sistem deteksi tuning terjadi. Prioritas temuan keamanan membantu menetapkan kecepatan yang tepat untuk tingkat respons.

Untuk Amazon Inspector, AWS Security Hub, dan Amazon GuardDuty, temuan mengandung label atau skor keparahan. Kami merekomendasikan untuk memprioritaskan penyelidikan semua temuan kritis dan tingkat keparahan tinggi di Security Hub, termasuk temuan yang terkait dengan standar Foundational Security Best Practices (FSBP), Amazon Inspector, dan. GuardDuty Menemukan label keparahan adalah skor ditentukan sebagai berikut:

- Skor Amazon Inspector adalah skor yang sangat kontekstual untuk setiap temuan. Ini dihitung dengan mengkorelasikan informasi skor dasar Common Vulnerability Scoring System (CVSS) dengan hasil jangkauan jaringan dan data eksploitabilitas. Dengan menggunakan skor ini, Anda dapat memprioritaskan temuan untuk fokus pada temuan paling kritis dan sumber daya yang rentan. Selain skor, Amazon Inspector juga menyediakan kecerdasan kerentanan yang ditingkatkan tentang Common Vulnerabilities and Exposures (CVE). Ini adalah ringkasan intelijen yang tersedia tentang CVE dari Amazon serta sumber intelijen keamanan standar industri, seperti Recorded Future dan Cybersecurity and Infrastructure Security Agency (CISA). Misalnya, Amazon Inspector dapat memberikan nama-nama kit malware yang dikenal yang digunakan untuk mengeksploitasi kerentanan. Untuk informasi selengkapnya, lihat Intelijen Kerentanan.
- Setiap GuardDuty temuan memiliki tingkat keparahan dan nilai yang ditetapkan yang mencerminkan potensi risiko temuan terhadap lingkungan Anda. Tingkat dan nilai ini ditentukan oleh insinyur AWS keamanan. Misalnya, tingkat `High` keparahan menunjukkan bahwa sumber daya dikompromikan dan secara aktif digunakan untuk tujuan yang tidak sah. Kami menyarankan Anda memperlakukan GuardDuty temuan `High` tingkat keparahan sebagai prioritas dan segera memulihkan untuk mencegah penggunaan yang tidak sah lebih lanjut.

- Tingkat keparahan temuan kontrol Security Hub ditentukan oleh kesulitan untuk mengeksploitasi dan kemungkinan kompromi. Kesulitan ditentukan oleh jumlah kecanggihan atau kompleksitas yang diperlukan untuk menggunakan kelemahan untuk melakukan skenario ancaman. Kemungkinan kompromi menunjukkan seberapa besar kemungkinan skenario ancaman akan mengakibatkan gangguan atau pelanggaran sumber daya Anda AWS layanan atau sumber daya.

Untuk menyetel temuan, Anda dapat menekan atau mengarsipkan temuan tertentu secara langsung di konsol layanan masing-masing atau dengan menggunakan API layanan. Selain itu, Anda dapat membuat perubahan pada temuan di Security Hub dengan menggunakan aturan otomatisasi. GuardDuty dan temuan Amazon Inspector secara otomatis dikirim ke Security Hub. Anda dapat menggunakan aturan otomatisasi untuk memperbarui secara otomatis (seperti mengubah tingkat keparahan) atau menekan temuan dalam waktu dekat, berdasarkan kriteria yang Anda tentukan. Saat Anda membuat aturan otomatisasi, sebaiknya tambahkan konteks ke deskripsi aturan, seperti tanggal pembuatan atau modifikasi, siapa yang membuatnya, dan mengapa aturan tersebut diperlukan. Informasi ini sering bermanfaat untuk referensi future.

Memulihkan temuan keamanan

Setelah menilai dan memprioritaskan temuan, tindakan selanjutnya adalah memulihkan temuan tersebut. Ada banyak tindakan berbeda yang dapat Anda ambil untuk memulihkan temuan. Untuk kerentanan perangkat lunak, Anda dapat memperbarui sistem operasi atau menerapkan tambalan. Untuk temuan konfigurasi cloud, Anda dapat memperbarui konfigurasi sumber daya. Secara umum, tindakan yang Anda ambil untuk memulihkan dapat dikelompokkan ke dalam salah satu hasil berikut:

- Remediasi manual — Anda secara manual memberikan perbaikan terhadap kerentanan, seperti memodifikasi properti AWS sumber daya untuk mengaktifkan enkripsi. Jika temuan ini berasal dari satu pemeriksaan terkelola di Security Hub, maka temuan tersebut menyertakan tautan ke instruksi untuk memulihkan temuan secara manual.
- Artefak yang dapat digunakan kembali — Anda memperbarui infrastruktur sebagai kode (IAc) untuk memperbaiki kerentanan dan mengetahui bahwa orang lain dapat memperoleh manfaat dari solusi serupa. Pertimbangkan untuk mengunggah IAc yang diperbarui dan ringkasan singkat resolusi ke repositori kode bersama internal.
- Remediasi otomatis — Kerentanan secara otomatis diperbaiki melalui mekanisme yang Anda buat.
- Kontrol pipa - Anda menerapkan kontrol dalam pipeline integrasi berkelanjutan dan pengiriman berkelanjutan (CI/CD) yang mencegah penyebaran jika ada kerentanan.

- Risiko yang diterima — Anda tidak mengambil tindakan atau menerapkan kontrol kompensasi, dan Anda menerima risiko yang ditimbulkan oleh kerentanan tersebut. Lacak risiko yang diterima di lokasi khusus, seperti registri risiko.
- Positif palsu — Anda tidak mengambil tindakan karena Anda telah menentukan temuan itu tidak mengidentifikasi kerentanan dengan benar.

Daftar lengkap berbagai tindakan yang dapat Anda ambil dan alat yang dapat Anda gunakan untuk memulihkan kerentanan berada di luar cakupan panduan ini. Namun, ada beberapa layanan dan alat yang dapat membantu Anda memulihkan kerentanan dalam skala yang perlu diperhatikan, termasuk:

- Patch Manager, kemampuan AWS Systems Manager, mengotomatiskan proses menambal node terkelola dengan pembaruan terkait keamanan dan jenis pembaruan lainnya. Anda dapat menggunakan Patch Manager untuk menerapkan patch untuk kedua sistem operasi dan aplikasi.
- AWS Firewall Managermembantu Anda mengonfigurasi dan mengelola aturan firewall secara terpusat di seluruh akun dan aplikasi Anda. AWS Organizations Saat aplikasi baru dibuat, Firewall Manager membuatnya lebih mudah untuk membawa aplikasi dan sumber daya baru ke dalam kepatuhan dengan menegakkan seperangkat aturan keamanan umum.
- Automated Security Response on AWS adalah AWS Solusi yang bekerja dengan Security Hub dan memberikan respons dan tindakan remediasi yang telah ditentukan berdasarkan standar kepatuhan industri dan praktik terbaik untuk ancaman keamanan.

Contoh triaging dan remediasi temuan keamanan

Bagian ini memberikan contoh proses triase untuk tim keamanan, cloud, dan aplikasi. Ini membahas jenis temuan yang biasanya ditangani oleh setiap tim dan memberikan contoh bagaimana merespons. Panduan remediasi tingkat tinggi juga disertakan.

Contoh-contoh berikut disertakan dalam bagian ini:

- Contoh tim keamanan: Membuat aturan otomatisasi Security Hub
- Contoh tim cloud: Mengubah konfigurasi VPC
- Contoh tim aplikasi: Membuat AWS Config aturan

Contoh tim keamanan: Membuat aturan otomatisasi Security Hub

Tim keamanan menerima temuan terkait deteksi ancaman, termasuk GuardDuty temuan Amazon. Untuk daftar lengkap jenis GuardDuty pencarian yang dikategorikan berdasarkan jenis AWS sumber daya, lihat Menemukan jenis dalam GuardDuty dokumentasi. Tim keamanan harus terbiasa dengan semua jenis temuan ini.

Untuk contoh ini, tim keamanan menerima tingkat risiko terkait untuk temuan keamanan Akun AWS yang digunakan secara ketat untuk tujuan pembelajaran dan tidak menyertakan data penting atau sensitif. Nama akun ini adalah`sandbox`, dan ID akun adalah`123456789012`. Tim keamanan dapat membuat aturan AWS Security Hub otomatisasi yang menekan semua GuardDuty temuan dari akun ini. Mereka dapat membuat aturan dari template, yang mencakup banyak kasus penggunaan umum, atau mereka dapat membuat aturan khusus. Di Security Hub, sebaiknya pratinjau hasil kriteria untuk mengonfirmasi bahwa aturan mengembalikan temuan yang dimaksud.

> **Note**
>
> Contoh ini menyoroti fungsionalitas aturan otomatisasi. Kami tidak menyarankan untuk menekan semua GuardDuty temuan untuk sebuah akun. Konteks penting, dan setiap organisasi harus memilih temuan mana yang akan ditekan berdasarkan tipe data, klasifikasi, dan kontrol mitigasi.

Berikut ini adalah parameter yang digunakan untuk membuat aturan otomatisasi ini:

- Aturan:
  - Nama aturan adalah `Suppress findings from Sandbox account`
  - Deskripsi aturan adalah `Date: 06/25/23 Authored by: John Doe Reason: Suppress GuardDuty findings from the sandbox account`
- Kriteria:
  - `AwsAccountId` = `123456789012`
  - `ProductName` = `GuardDuty`
  - `WorkflowStatus` = `NEW`
  - `RecordState` = `ACTIVE`
- Tindakan otomatis:
  - `Workflow.status`adalah `SUPPRESSED`

Untuk informasi selengkapnya, lihat Aturan otomatisasi di dokumentasi Security Hub. Tim keamanan memiliki banyak pilihan untuk menyelidiki dan memulihkan temuan untuk ancaman yang terdeteksi. Untuk panduan ekstensif, lihat Panduan Respons Insiden AWS Keamanan. Kami merekomendasikan untuk meninjau panduan ini untuk mengonfirmasi bahwa Anda telah menetapkan proses respons insiden yang kuat.

Contoh tim cloud: Mengubah konfigurasi VPC

Tim cloud bertanggung jawab untuk melakukan triaging dan remediasi temuan keamanan yang memiliki tren umum, seperti perubahan pada pengaturan AWS default yang mungkin tidak sesuai dengan kasus penggunaan Anda. Temuan ini cenderung mempengaruhi banyak Akun AWS atau sumber daya, seperti konfigurasi VPC, atau mereka termasuk pembatasan yang harus ditempatkan di seluruh lingkungan. Sebagian besar, tim cloud membuat perubahan manual satu kali, seperti menambahkan atau memperbarui kebijakan.

Setelah organisasi Anda menggunakan AWS lingkungan untuk beberapa waktu, Anda mungkin menemukan serangkaian anti-pola yang berkembang. Anti-pola adalah solusi yang sering digunakan untuk masalah berulang di mana solusinya kontra-produktif, tidak efektif, atau kurang efektif daripada alternatif. Sebagai alternatif dari anti-pola ini, organisasi Anda dapat menggunakan pembatasan lingkungan yang lebih efektif, seperti kebijakan kontrol AWS Organizations layanan (SCP) atau kumpulan izin Pusat Identitas IAM. SCP dan set izin dapat memberikan batasan tambahan untuk jenis sumber daya, seperti mencegah pengguna mengonfigurasi bucket Amazon Simple Storage Service (Amazon S3) publik. Meskipun mungkin tergoda untuk membatasi setiap konfigurasi keamanan yang mungkin, ada batasan ukuran kebijakan untuk SCP dan set izin. Kami merekomendasikan pendekatan yang seimbang untuk kontrol preventif dan detektif.

Berikut ini adalah beberapa kontrol dari standar AWS Security Hub Foundational Security Best Practices (FSBP) yang mungkin menjadi tanggung jawab tim cloud:

- [EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk dan keluar
- [EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis
- [Config.1] AWS Config harus diaktifkan

Untuk contoh ini, tim cloud menangani temuan untuk kontrol FSBP EC2.2. Dokumentasi untuk kontrol ini merekomendasikan untuk tidak menggunakan grup keamanan default karena memungkinkan akses luas melalui aturan masuk dan keluar default. Karena grup keamanan default tidak dapat dihapus, rekomendasinya adalah mengubah pengaturan aturan untuk membatasi lalu lintas masuk dan keluar. Untuk mengatasi masalah ini secara efisien, tim cloud harus menggunakan mekanisme yang telah ditetapkan untuk memodifikasi aturan grup keamanan untuk semua VPC karena setiap VPC memiliki grup keamanan default ini. Dalam kebanyakan kasus, tim cloud mengelola konfigurasi VPC dengan menggunakan AWS Control Towerkustomisasi atau alat infrastruktur sebagai kode (IAc), seperti atau. HashiCorp TerraformAWS CloudFormation

Contoh tim aplikasi: Membuat AWS Config aturan

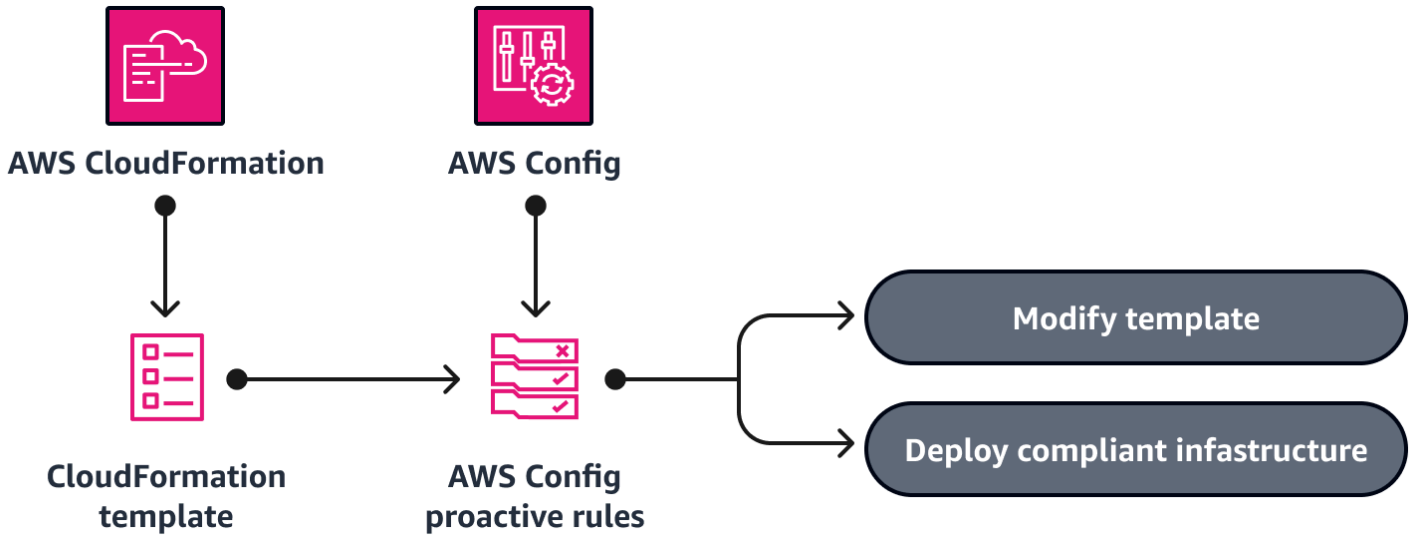
Berikut ini adalah beberapa kontrol dari standar keamanan Security Hub Foundational Security Best Practices (FSBP) Security Hub yang mungkin bertanggung jawab atas aplikasi atau tim pengembangan:

- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [EC2.19] Grup keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi
- [CodeBuild.1] CodeBuild GitHub atau URL repositori sumber Bitbucket harus menggunakan OAuth
- [ECS.4] Kontainer ECS harus berjalan sebagai non-hak istimewa
- [ELB.1] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS

Untuk contoh ini, tim aplikasi menangani temuan untuk kontrol FSBP EC2.19. Kontrol ini memeriksa apakah lalu lintas masuk yang tidak terbatas untuk grup keamanan dapat diakses ke port tertentu yang memiliki risiko tertinggi. Kontrol ini gagal jika ada aturan dalam grup keamanan yang mengizinkan lalu lintas masuk dari `0.0.0.0/0` atau `::/0` untuk port tersebut. Dokumentasi untuk kontrol ini merekomendasikan untuk menghapus aturan yang memungkinkan lalu lintas ini.

Selain menangani aturan kelompok keamanan individu, ini adalah contoh bagus dari temuan yang seharusnya menghasilkan AWS Config aturan baru. Dengan menggunakan mode evaluasi proaktif, Anda dapat membantu mencegah penerapan aturan grup keamanan berisiko di masa mendatang. Mode proaktif mengevaluasi sumber daya sebelum digunakan sehingga Anda dapat mencegah sumber daya yang salah konfigurasi dan temuan keamanan terkait. Saat menerapkan layanan baru atau fungsionalitas baru, tim aplikasi dapat menjalankan aturan dalam mode proaktif sebagai bagian dari pipeline continuous integration and continuous delivery (CI/CD) untuk mengidentifikasi sumber daya yang tidak sesuai. Gambar berikut menunjukkan bagaimana Anda dapat menggunakan

AWS Config aturan proaktif untuk mengonfirmasi bahwa infrastruktur yang ditentukan dalam AWS CloudFormation template sesuai.



Efisiensi penting lainnya dapat diperoleh dalam contoh ini. Ketika tim aplikasi membuat AWS Config aturan proaktif, mereka dapat membagikannya dalam repositori kode umum sehingga tim aplikasi lain dapat menggunakannya.

Setiap temuan yang terkait dengan kontrol Security Hub berisi detail tentang temuan dan tautan ke instruksi untuk memulihkan masalah. Meskipun tim cloud mungkin menemukan temuan yang memerlukan remediasi manual satu kali, bila perlu, kami merekomendasikan untuk membuat pemeriksaan proaktif yang mengidentifikasi masalah sedini mungkin dalam proses pengembangan.

Laporkan dan tingkatkan program manajemen kerentanan Anda

Pelaporan yang efektif untuk manajemen kerentanan melibatkan peninjauan data, memantau tren, dan berbagi pengetahuan. Ini memberikan visibilitas dan membantu tim meningkatkan postur keamanan organisasi mereka di. AWS Cloud

Melakukan rapat operasi keamanan bulanan

Pertemuan operasi keamanan bulanan adalah mekanisme yang efektif untuk mempromosikan kepemilikan, akuntabilitas, dan penyelarasan berkelanjutan di seluruh tim. Dalam pertemuan tersebut, para pemangku kepentingan dari tim keamanan, cloud, dan aplikasi meninjau data untuk temuan keamanan yang luar biasa, temuan di luar perjanjian tingkat layanan (SLA), dan tim yang memiliki temuan terbanyak.

Rapat ini membantu tim Anda mengidentifikasi anti-pola, seperti peluang untuk menambahkan lebih banyak batasan. Kontrol pencegahan dan peluang otomatisasi juga dapat ditemukan dan dibagikan. Rapat juga membantu mengidentifikasi apa yang berhasil dan tidak berfungsi dengan baik dalam program manajemen kerentanan sehingga Anda dapat melakukan perbaikan.

Dengan meninjau data, mengidentifikasi anti-pola dan masalah, dan berbagi informasi tentang kontrol dan otomatisasi, tim dapat memperoleh wawasan berharga dan membuat penyempurnaan berkelanjutan yang dapat memperkuat postur keamanan mereka dan mengurangi SLA terkait keamanan mereka.

Gunakan wawasan Security Hub untuk mengidentifikasi anti-pola

AWS Security Hub wawasan juga dapat membantu Anda mengidentifikasi anti-pola dan melacak kemajuan Anda dalam memulihkan temuan. Wawasan Security Hub adalah kumpulan temuan terkait. Ini mengidentifikasi area keamanan yang membutuhkan perhatian dan intervensi. Wawasan Security Hub dapat membantu Anda mengidentifikasi persyaratan spesifik dan mengembangkan laporan. Security Hub menawarkan beberapa wawasan terkelola bawaan. Untuk melacak masalah keamanan yang unik untuk AWS lingkungan dan penggunaan Anda, Anda dapat membuat wawasan khusus.

Kesimpulan dan langkah selanjutnya

Singkatnya, program manajemen kerentanan yang efektif memerlukan persiapan menyeluruh dan mengharuskan Anda mengaktifkan alat dan integrasi yang tepat, menyempurnakan alat-alat tersebut, masalah triase yang efisien, dan terus melaporkan dan meningkatkan. Dengan mengikuti praktik terbaik dalam panduan ini, organisasi dapat membangun program manajemen kerentanan yang dapat diskalakan AWS untuk membantu mengamankan lingkungan cloud mereka.

Anda dapat memperluas program ini untuk menyertakan kerentanan dan temuan terkait keamanan tambahan, seperti kerentanan keamanan aplikasi. AWS Security Hub mendukung integrasi produk kustom. Pertimbangkan untuk menggunakan Security Hub sebagai titik integrasi untuk alat dan produk keamanan tambahan. Integrasi ini memungkinkan Anda untuk memanfaatkan proses dan alur kerja yang telah Anda buat dalam program manajemen kerentanan Anda, seperti integrasi langsung dengan backlog produk dan rapat tinjauan keamanan bulanan.

Tabel berikut merangkum fase dan item tindakan yang dijelaskan dalam panduan ini.

Fase	Item tindakan
Siapkan	• Tentukan rencana manajemen kerentanan. • Mendistribusikan kepemilikan temuan. • Mengembangkan program pengungkapan kerentanan. • Kembangkan Akun AWS struktur. • Mendefinisikan, menerapkan, dan menegakkan tag. • Pantau buletin AWS keamanan. • Aktifkan Amazon Inspector dengan administrator yang didelegasikan. • Aktifkan Security Hub dengan administrator yang didelegasikan. • Aktifkan standar Security Hub. • Siapkan agregasi lintas wilayah Security Hub.

Fase	Item tindakan
	• Aktifkan temuan kontrol terkonsolidasi di Security Hub. • Mengatur dan mengelola integrasi Security Hub, termasuk integrasi hilir yang berlaku dengan SIEM, GRC, atau backlog produk atau sistem tiket
Triase dan remediasi	• Rute temuan berdasarkan strategi multi-aku n. • Rutekan temuan ke tim keamanan, cloud, dan aplikasi atau pengembang. • Sesuaikan temuan keamanan untuk memastikan bahwa mereka dapat ditindakl anjuti untuk lingkungan spesifik Anda. • Kembangkan mekanisme remediasi otomatis, bila memungkinkan. • Menerapkan kontrol pipa CI/CD atau pagar pembatas lain yang membantu mencegah temuan keamanan, jika memungkinkan. • Gunakan aturan otomatisasi Security Hub untuk meningkatkan atau menekan temuan.
Laporkan dan tingkatkan	• Mengadakan pertemuan operasi keamanan bulanan. • Gunakan wawasan Security Hub untuk mengidentifikasi anti-pola.

Sumber daya

AWS dokumentasi layanan

- Integrasi produk ()AWS Security Hub
- Mengintegrasikan AWS Security Hub dalam Jira Service Management Cloud ()AWS Security Hub
- Aturan otomatisasi (AWS Security Hub)
- Aturan evaluasi proaktif ()AWS Config
- Manajer Patch (AWS Systems Manager)

AWS Sumber daya lainnya

- Praktik terbaik untuk menandai AWS sumber daya (AWS whitepaper)
- Respon Keamanan Otomatis pada AWS (Perpustakaan AWS Solusi)
- AWS Panduan Respons Insiden Keamanan (Panduan AWS Teknis)
- AWS buletin keamanan

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
Publikasi awal	—	12 Oktober 2023

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 Wilayah AWS 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 AWS layanan menerimanya.

Cloud Center of Excellence (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 CCoE 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 CCoE, 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. AWS CodeCommit 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, AWS Panorama menawarkan perangkat yang menambahkan CV ke jaringan kamera lokal, dan Amazon SageMaker menyediakan algoritme 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 umumnya 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 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 database.

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.

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.

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 pengguna akhir dapat mengakses. Dalam pipa CI/CD, 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, Wilayah AWS, 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.

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.

G

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.

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 (OU). 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, 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.

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 VPC masuk, keluar, dan inspeksi 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 selengkapnya, 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 VPC (dalam hal yang sama atau berbeda Wilayah AWS), internet, dan jaringan lokal. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan VPC masuk, keluar, dan inspeksi 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 selengkapnya, 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.

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.

lingkungan yang lebih rendah

Lihat lingkungan.

M

pembelajaran mesin (ML)

Jenis kecerdasan buatan yang menggunakan algoritma dan teknik untuk pengenalan pola dan pembelajaran. 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

AWS layanan 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 melalui API yang terdefinisi dengan baik 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 API ringan. 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 terbaik dan pelajaran yang dipetik 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 file. 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 VPC masuk, keluar, dan inspeksi 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 kebijakanberbasis sumber daya), atau menentukan izin maksimum untuk semua akun dalam organisasi di (lihat kebijakan kontrol layanan). AWS Organizations

persistensi 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. Untuk informasi selengkapnya, lihat Mengaktifkan persistensi data di layanan mikro.

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 oleh Desain

Pendekatan dalam rekayasa sistem yang memperhitungkan privasi di seluruh proses rekayasa.

zona host pribadi

Container yang menyimpan informasi tentang bagaimana Anda ingin Amazon Route 53 merespons kueri DNS untuk domain dan subdomainnya dalam satu atau beberapa VPC. 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.

pseudonimisasi

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

terbitkan/berlangganan (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).

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 hilangnya 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.

Wilayah

Kumpulan AWS sumber daya di wilayah geografis. Masing-masing Wilayah AWS 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 prinsip 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). Jenis 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.

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 AWS Management Console 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.

PENIPUAN

Lihat kontrol pengawasan dan akuisisi data.

SCP

Lihat kebijakan kontrol layanan.

Rahasia

Dalam AWS Secrets Manager, informasi rahasia atau terbatas, seperti kata sandi atau kredensi 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.

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 AWS layanan yang menerimanya.

kebijakan kontrol layanan (SCP)

Kebijakan yang menyediakan kontrol terpusat atas izin untuk semua akun di organisasi. AWS Organizations SCP menentukan pagar pembatas atau menetapkan batasan pada tindakan yang dapat didelegasikan oleh administrator kepada pengguna atau peran. Anda dapat menggunakan SCP sebagai 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 AWS layanan. Anda dapat menggunakan endpoint untuk terhubung secara terprogram ke layanan target. Untuk informasi selengkapnya, lihat AWS layanan 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.

T

tag

Pasangan nilai kunci yang bertindak sebagai metadata untuk mengatur sumber daya Anda. AWS Tanda dapat 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 VPC dan jaringan lokal Anda. 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 VPC yang memungkinkan Anda 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 Kerangka Kualifikasi Beban Kerja AWS.

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.

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.