Merangkak, berjalan, berlari: Mempercepat kematangan keamanan di AWS Cloud

AWS Panduan Preskriptif

AWS Panduan Preskriptif: Merangkak, berjalan, berlari: Mempercepat kematangan keamanan di AWS Cloud

Table of Contents

Merangkak, berjalan, berlari: Mempercepat kematangan keamanan di AWS Cloud

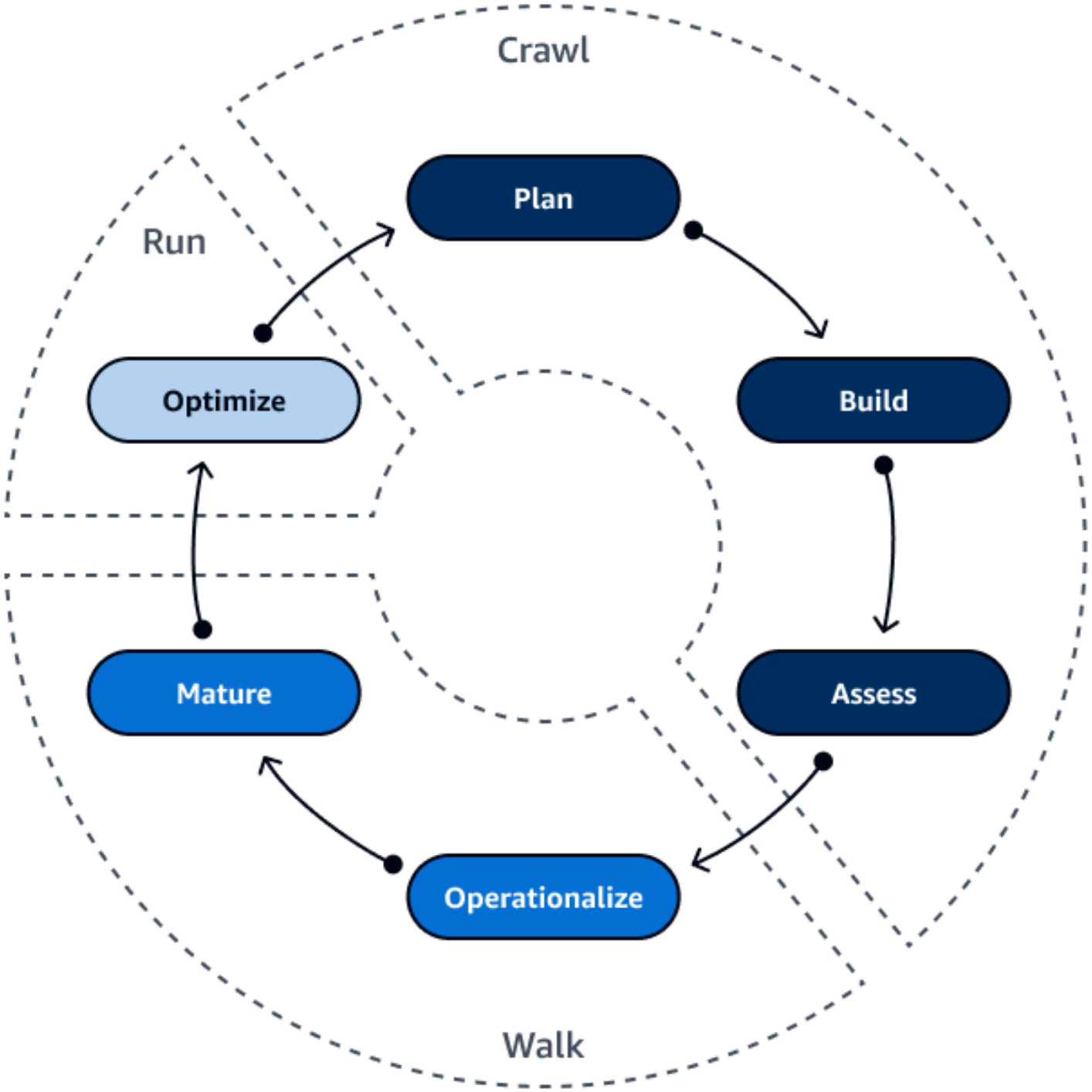
Amazon Web Services (kontributor)

Desember 2023 (riwayat dokumen)

Bagi banyak organisasi, keamanan adalah prioritas dan pertimbangan nomor satu saat bermigrasi ke cloud. Menerapkan kemampuan dan kontrol keamanan cloud bukanlah aktivitas satu kali — ini adalah model berulang. Anda secara bertahap meningkatkan postur keamanan dan kematangan Anda saat Anda meningkatkan operasi cloud. Misalnya, Anda dapat memulai dengan kebijakan AWS terkelola dan kemudian, ketika organisasi Anda siap, Anda dapat menerapkan kebijakan khusus yang mengikuti prinsip hak istimewa paling sedikit.

Panduan ini menyediakan peta jalan untuk menggunakan metodologi crawl, walk, run untuk mempercepat kematangan organisasi Anda dalam keamanan cloud. Ini mendefinisikan step-by-step pendekatan untuk mengotomatiskan kemampuan keamanan. Ini juga secara pragmatis menjelaskan cara mendapatkan fungsionalitas dan fitur maksimal. Layanan AWS Panduan ini membantu Anda memahami tantangan dan peluang di cloud dan cara cepat bergerak maju dan mencapai kesuksesan dengan AWS.

Perjalanan cloud membutuhkan membangun kerangka kerja, mengelola dan mematangkan operasi, dan mengoptimalkan proses. Gambar berikut menunjukkan fase di setiap tahap metodologi crawl, walk, run: merencanakan, membangun, menilai, mengoperasionalkan, matang, dan mengoptimalkan.



Tahap merangkak terdiri dari perencanaan, membangun fondasi, dan menilai postur keamanan Anda saat ini. Dalam tahap berjalan, Anda mengoperasionalkan orang, proses, dan teknologi Anda, dan kemudian Anda mematangkan operasi Anda melalui penyetelan dan pengukuran. Tahap lari terdiri dari pengoptimalan melalui penilaian dan otomatisasi.

Tahap merangkak: Merencanakan, membangun, dan menilai

Tahap merangkak dimulai dengan perencanaan. Perencanaan melibatkan penentuan ruang lingkup keamanan dan memilih model yang paling sesuai dengan organisasi Anda. Setelah Anda membuat rencana, Anda dapat mulai membangun fondasi. Ini diikuti dengan menilai postur keamanan Anda saat ini dan menyiapkan disiplin segera setelah Anda membangun infrastruktur keamanan. Tahap crawl bersifat iteratif. Iterasi di cloud lebih cepat daripada iterasi di lingkungan lokal. Saat Anda mematangkan kemampuan cloud Anda, proses iterasi semakin cepat.

Berikut ini adalah fase dalam tahap merangkak:

- Rencana— Bagaimana Anda mengetahui ruang lingkup Anda dan memilih model?
- Build— Bagaimana Anda akan membangun kerangka kerja?
- Menilai— Apa postur keamanan Anda saat ini?

Rencana: Menetapkan ruang lingkup dan model keamanan Anda

Perencanaan adalah proses berulang saat Anda mematangkan model keamanan Anda. Langkah-langkah kunci dalam proses perencanaan meliputi:

- Memahami ruang lingkup keamanan— Cakupan keamanan bervariasi dan tergantung pada bagaimana cloud digunakan.
- Memilih model keamanan— Identifikasi model keamanan yang paling pas untuk kasus penggunaan keamanan Anda.
- Menciptakan model tujuan bisnisTentukan tujuan dan mekanisme yang jelas untuk mengukur keberhasilan.

Saat Anda mengembangkan rencana Anda, pertimbangkan hal berikut:

- Bersedia untuk mengulangi. Iterasi konstan di cloud. Iterasi membantu Anda mengidentifikasi kesenjangan dalam rencana.
- Jangan mulai dengan layanan. Mulailah dengan rencana Anda alih-alih memilih layanan apa yang Anda butuhkan. Ini membantu mendorong organisasi Anda ke hasil yang diinginkan.

Memahami ruang lingkup keamanan

Model tanggung jawab AWS bersama mendefinisikan bagaimana Anda berbagi tanggung jawab AWS untuk keamanan dan kepatuhan di cloud. AWS mengamankan infrastruktur yang menjalankan semua layanan yang ditawarkan di AWS Cloud, dan Anda bertanggung jawab untuk mengamankan penggunaan layanan tersebut, seperti data dan aplikasi Anda.

Model bersama ini dapat membantu meringankan kepatuhan dan beban operasional Anda karena AWS mengoperasikan, mengelola, dan mengontrol banyak komponen, mulai dari sistem operasi host dan lapisan virtualisasi hingga keamanan fisik fasilitas tempat layanan beroperasi. Layanan terkelola membantu Anda mengurangi kewajiban keamanan dan kepatuhan dengan memungkinkan AWS untuk mengelola beberapa tugas keamanan, seperti patching dan manajemen kerentanan. Menggunakan layanan terkelola adalah praktik terbaik dalam Kerangka AWS Well-Architected. Secara umum, karena infrastruktur dimodernisasi, lebih banyak tanggung jawab dialihkan ke penyedia layanan.

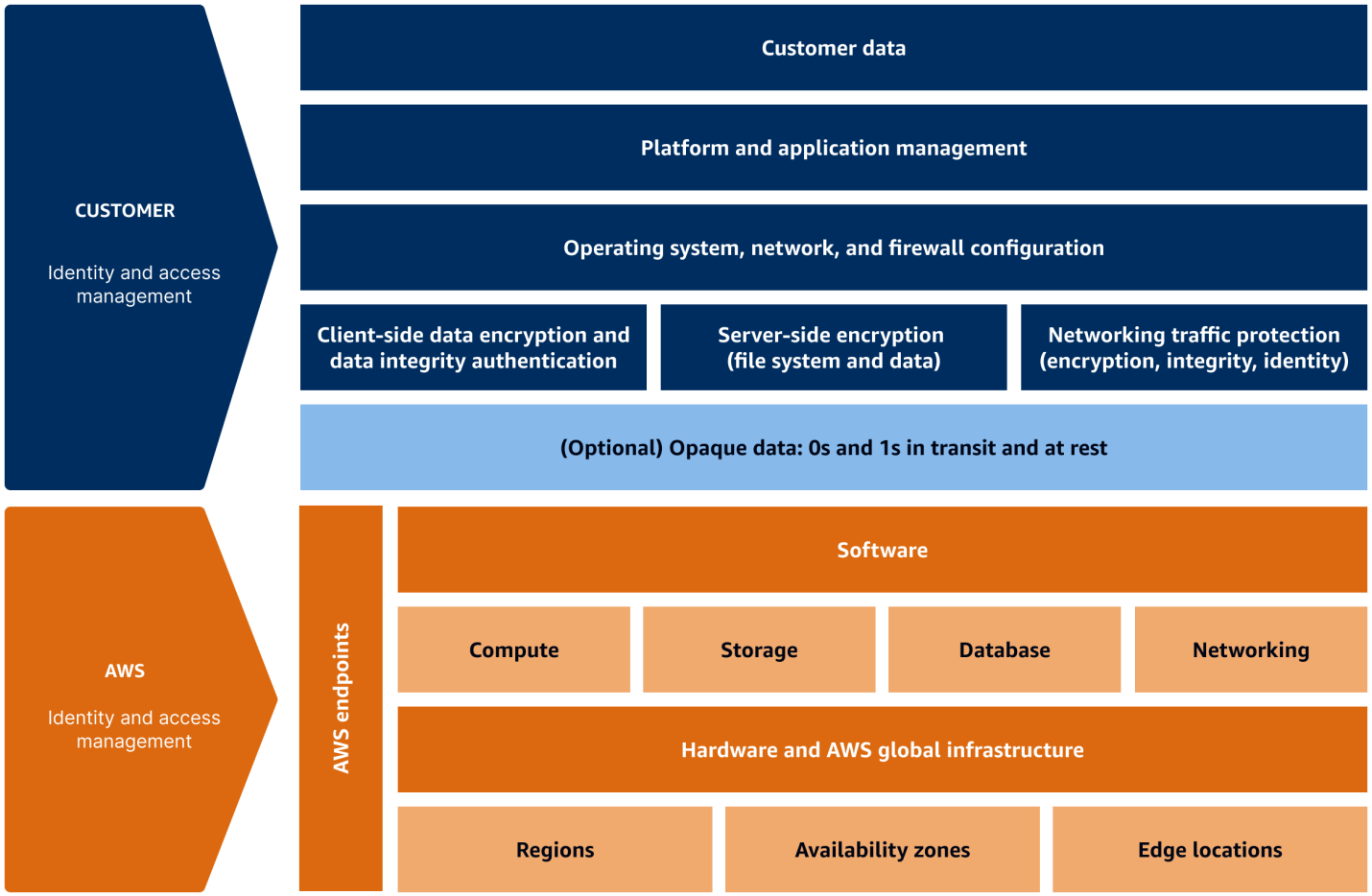
Berikut ini adalah tiga contoh layanan yang berbeda untuk membantu Anda memahami bagaimana cakupan keamanan Anda berubah berdasarkan layanan yang Anda pilih:

- Layanan infrastruktur
- Layanan kontainer
- Layanan tanpa server

Tanggung jawab Anda untuk keamanan tidak statis, dan itu berubah dengan jenis arsitektur yang Anda pilih. Waktu, tenaga, dan biaya Anda dipengaruhi oleh arsitektur cloud yang Anda pilih.

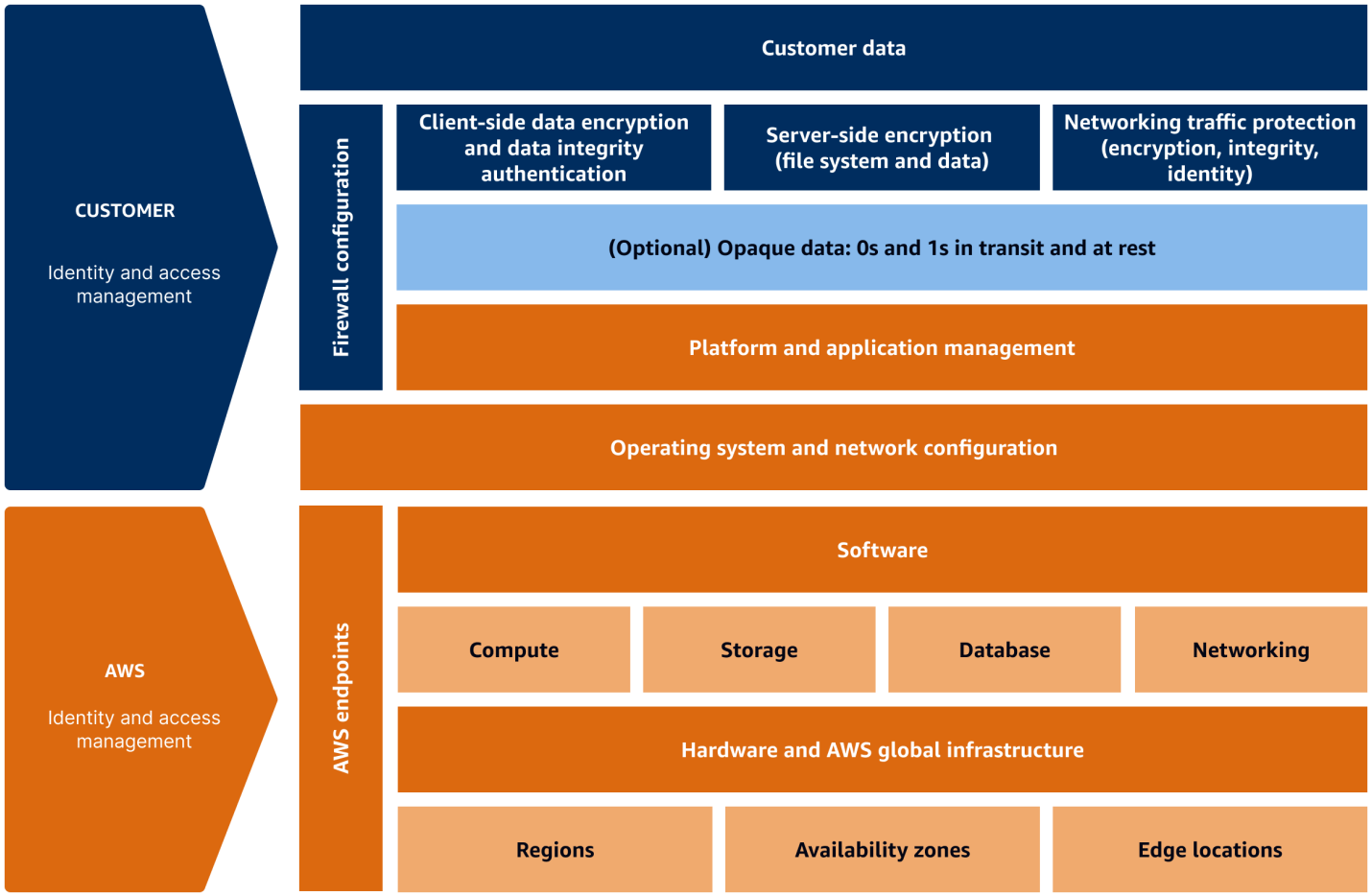
Layanan infrastruktur

Untuk layanan infrastruktur, AWS berfokus pada pengamanan infrastruktur yang mendasarinya. Dalam layanan infrastruktur, cakupannya lebih besar bagi pelanggan karena mereka perlu mengatasi keamanan platform, patch OS, dan manajemen aplikasi, dibandingkan dengan model lainnya. Amazon Elastic Compute Cloud (Amazon EC2) adalah contoh layanan infrastruktur umum.



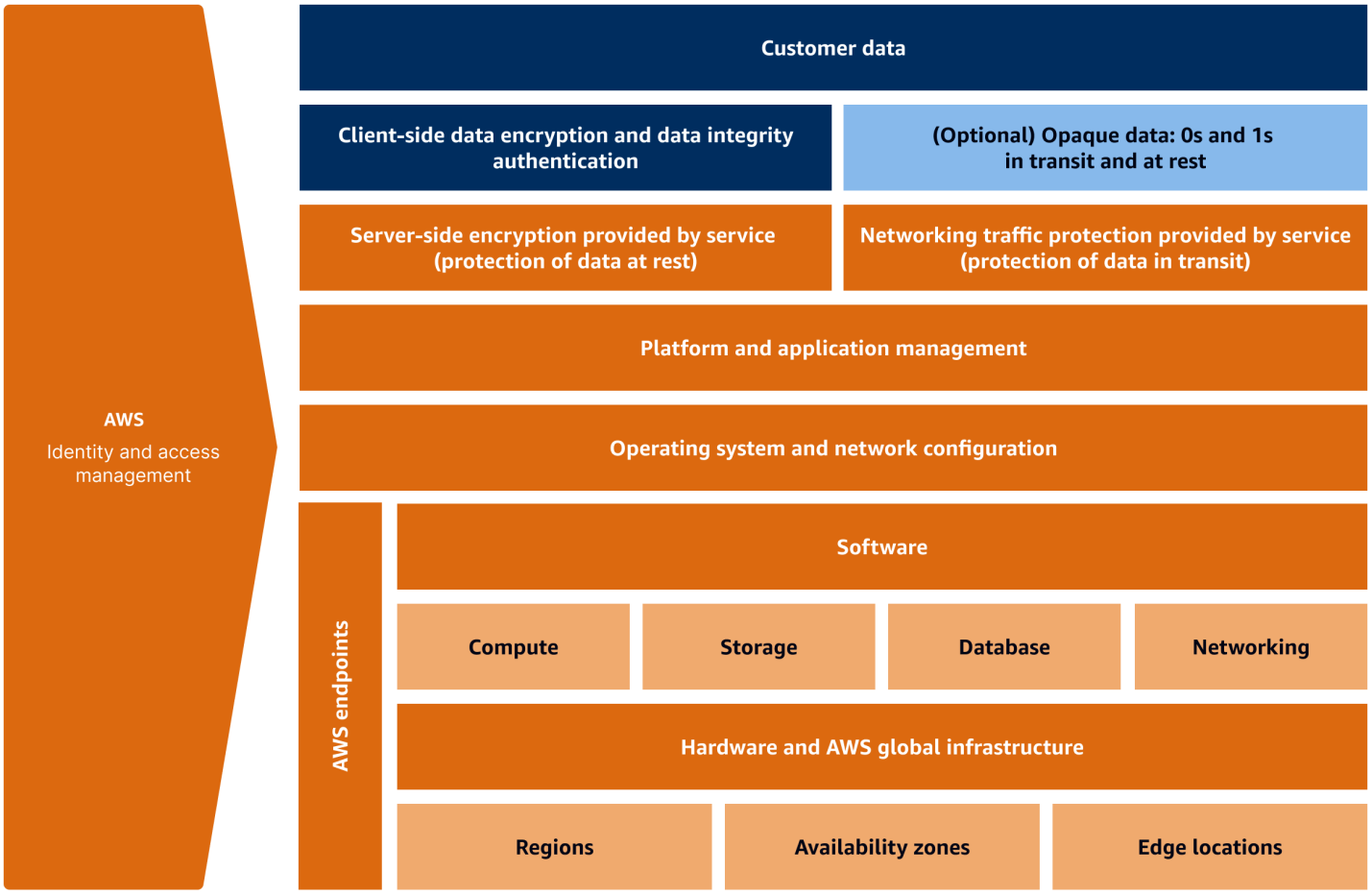
Layanan kontainer

Ketika infrastruktur menjadi lebih abstrak dan dimodernisasi, jejak menjadi lebih kecil. Ruang lingkup Anda menyusut karena tanggung jawab untuk beberapa elemen keamanan bergeser ke. AWS Layanan kontainer adalah contoh di mana beberapa tanggung jawab backend beralih kembali ke. AWS Misalnya, bertanggung AWS jawab atas konfigurasi sistem operasi (OS), konfigurasi jaringan, manajemen platform, dan manajemen aplikasi. Contoh layanan kontainer umum termasuk Amazon Elastic Kubernetes Service (Amazon EKS), Amazon Elastic Container Registry (Amazon ECR), Amazon Elastic Container Service (Amazon ECS), dan. AWS Fargate



Layanan tanpa server

Saat menggunakan layanan tanpa server, hampir semua tanggung jawab atas keamanan adalah milik. AWS Ruang lingkup tanggung jawab Anda minimal. Misalnya, database tanpa server yang dikelola (DB) menghilangkan kebutuhan bagi Anda untuk mengamankan jaringan, perangkat keras, dan sistem operasi. Semua patch OS dan DB ditutupi oleh AWS. Satu-satunya perhatian Anda adalah mengamankan akses ke data melalui enkripsi dan otentikasi.



Memilih model keamanan

Anda dapat memilih dari berbagai model atau pendekatan keamanan untuk AWS. Pilihan pendekatan dan model yang paling pas tergantung pada audiens Anda, target hasil bisnis, dan keseluruhan proses bisnis. Dimungkinkan untuk menggunakan campuran beberapa model.

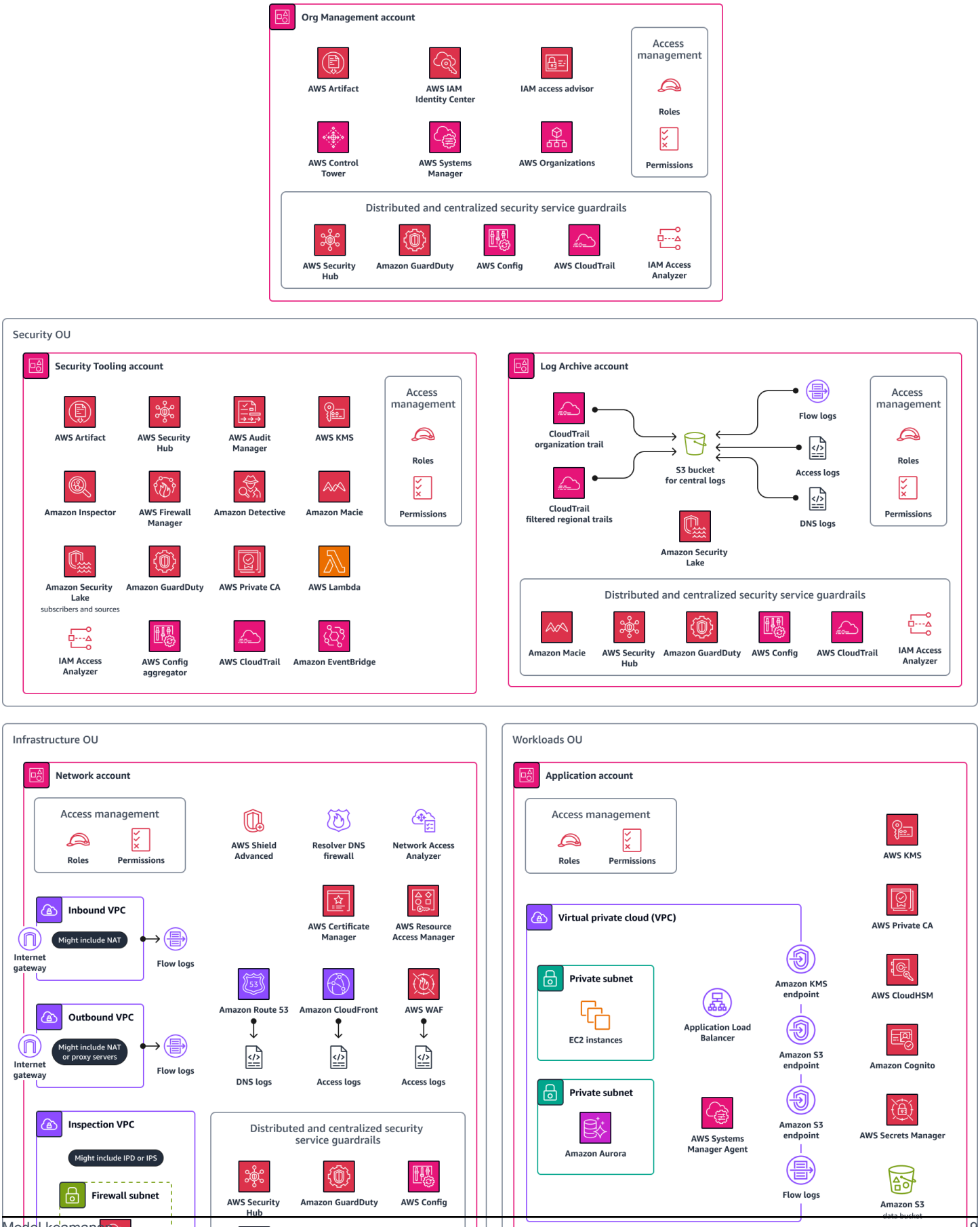
Berikut ini adalah beberapa model umum:

- Model arsitektur
- Model kedewasaan
- Model tata kelola

Setiap model memiliki kelebihan dan kekurangannya sendiri. Penting untuk mempertimbangkan pendekatan mana yang paling cocok untuk organisasi Anda. Libatkan profesional keamanan di awal proses memodernisasi infrastruktur Anda dan mengadopsi strategi cloud. Model yang Anda pilih memiliki dampak signifikan pada peran dan tanggung jawab dalam organisasi Anda.

Model arsitektur

Gambar berikut menunjukkan Arsitektur Referensi AWS Keamanan. Pendekatan arsitektur ini menyediakan cetak biru untuk model keamanan. Pendekatan ini paling cocok ketika Anda terlibat dengan tim teknis dalam organisasi Anda. Ini membantu menetapkan tujuan negara masa depan yang ideal. Ini juga sejalan dengan banyak kepatuhan dan AWS kerangka kerja.


Org Management account
AWS Artifact
AWS IAM Identity Center
IAM access advisor
Access management
Roles
Permissions
AWS Control Tower
AWS Systems Manager
AWS Organizations
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Security OU
Security Tooling account
AWS Artifact
AWS Security Hub
AWS Audit Manager
AWS KMS
Access management
Roles
Permissions
Amazon Inspector
AWS Firewall Manager
Amazon Detective
Amazon Macie
Amazon Security Lake
subscribers and sources
Amazon GuardDuty
AWS Private CA
AWS Lambda
IAM Access Analyzer
AWS Config aggregator
AWS CloudTrail
Amazon EventBridge
Log Archive account
CloudTrail organization trail
CloudTrail filtered regional trails
S3 bucket for central logs
Flow logs
Access logs
DNS logs
Amazon Security Lake
Access management
Roles
Permissions
Distributed and centralized security service guardrails
Amazon Macie
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Infrastructure OU
Network account
Access management
Roles
Permissions
AWS Shield Advanced
Resolver DNS firewall
Network Access Analyzer
AWS Certificate Manager
AWS Resource Access Manager
Inbound VPC
Might include NAT
Internet gateway
Flow logs
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
Amazon Route 53
Amazon CloudFront
AWS WAF
DNS logs
Access logs
Access logs
Inspection VPC
Might include IPD or IPS
Firewall subnet
AWS Network Firewall
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Workloads OU
Application account
Access management
Roles
Permissions
AWS KMS
AWS Private CA
AWS CloudHSM
Amazon Cognito
AWS Secrets Manager
Amazon S3
Virtual private cloud (VPC)
Private subnet
EC2 instances
Private subnet
Amazon Aurora
Application Load Balancer
AWS Systems Manager Agent
Amazon KMS endpoint
Amazon S3 endpoint
Amazon S3 endpoint
Flow logs
Distributed and centralized security service guardrails
Amazon Macie
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer

Keuntungan dari model arsitektur:

- Sejajar dengan persyaratan Health Insurance Portability and Accountability Act (HIPAA) dan Health Information Trust Alliance Common Security Framework (HITRUST CSF)
- Memberikan perspektif arsitektur
- Sejajar dengan strategi cloud dan panduan untuk perusahaan besar
- Sejajar dengan AWS Cloud Adoption Framework (AWS CAF)
- Selaras dengan Kerangka AWS Well-Architected

Kerugian dari model arsitektur:

- Berfokus pada teknologi daripada berfokus pada bisnis

Model kedewasaan

Pendekatan AWS Security Maturity Model berfokus pada pengelolaan dan pengurangan risiko dengan memprioritaskan penerapan langkah-langkah keamanan. Pendekatan ini sangat cocok untuk direktur keamanan dan CISOs, tetapi tidak berfokus pada bisnis.

Keuntungan dari model kematangan:

- Apakah keamanan terfokus
- Merupakan model yang berfokus pada penggunaan pendekatan implementasi berbasis agile
- Membantu Anda mengurangi risiko dengan cepat
- Sejajar dengan AWS Cloud Adoption Framework (AWS CAF)

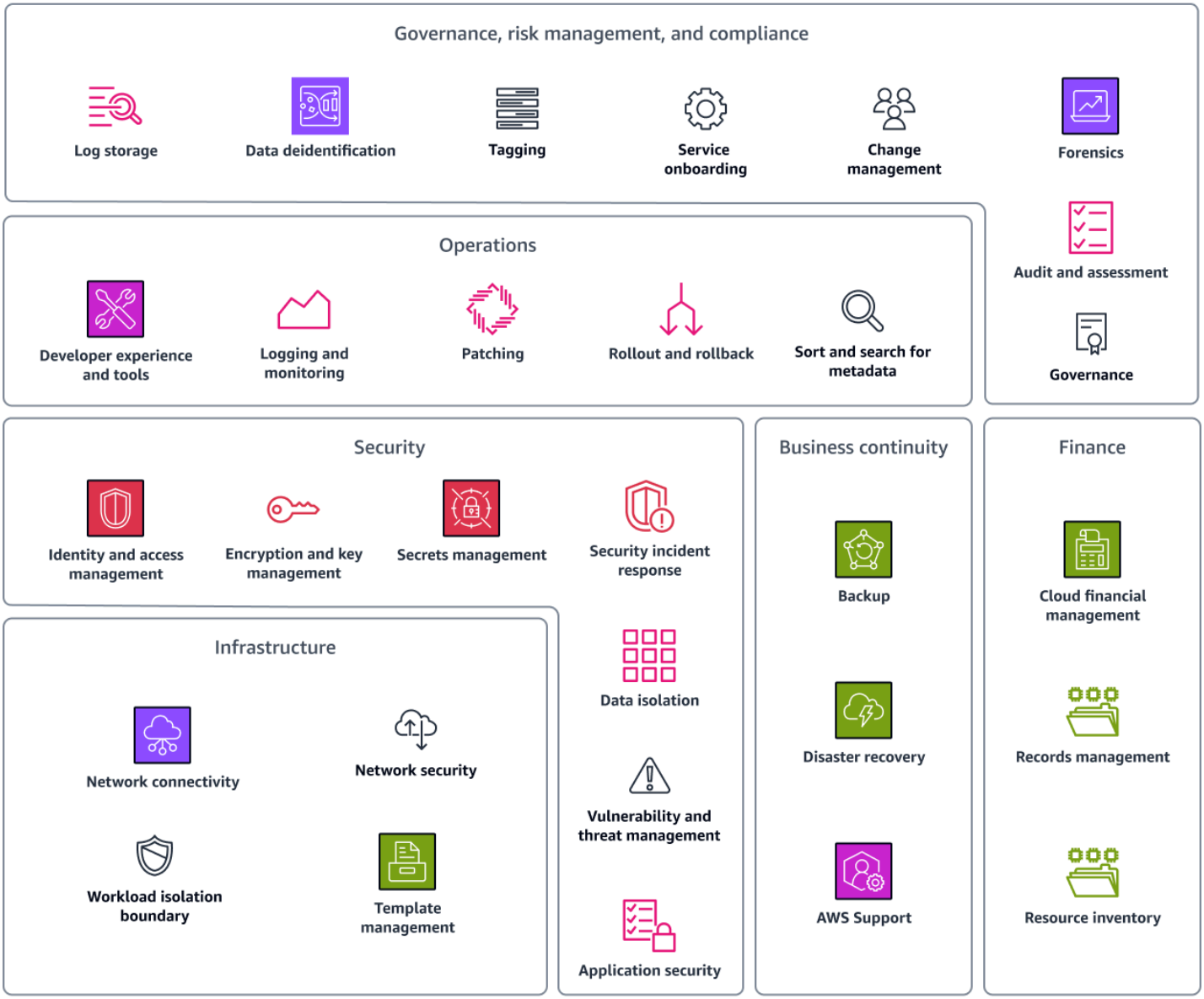
Kerugian dari model kematangan:

- Berfokus pada teknologi daripada berfokus pada bisnis

Model tata kelola

Cloud Foundation on AWS model menggunakan pendekatan tata kelola, manajemen risiko, dan kepatuhan (GRC) untuk membantu organisasi memenuhi persyaratan keamanan dan kepatuhan. Ini mendefinisikan kebijakan keseluruhan yang harus diikuti oleh lingkungan cloud Anda. Kemampuan

dalam model ini membantu Anda menentukan item tindakan, menentukan selera risiko, dan menyelaraskan kebijakan internal.



Model Cloud Foundation adalah panduan kemampuan dan tata kelola yang membantu Anda membangun dan mengembangkan lingkungan Anda AWS Cloud . Ini didasarkan pada serangkaian definisi, skenario, panduan, dan otomatisasi. Panduan ini mencakup aspek orang, proses, dan teknologi untuk membangun AWS Cloud lingkungan. Ini mencakup enam kategori kemampuan yang penting untuk fondasi cloud:

- Tata kelola, manajemen risiko, dan kepatuhan
- Operasi

- Keamanan
- Kelanjutan bisnis
- Keuangan
- Infrastruktur

Panduan ini juga memberikan contoh, jadwal, dan bacaan lebih lanjut untuk setiap kemampuan.

Keuntungan dari model tata kelola:

- Memiliki fokus teknologi yang luas
- Dirancang untuk keandalan
- Menggunakan pendekatan operasional

Kerugian dari model tata kelola:

- Berfokus pada teknologi daripada berfokus pada bisnis

Menciptakan model tujuan bisnis

Model tujuan bisnis melibatkan mendefinisikan hasil bisnis. Ini mirip dengan AWS Cloud Adoption Framework dan AWS Well-Architected Framework. Pendekatan ini berfokus pada apa yang diminati bisnis dengan menafsirkan hasil bisnis target. Nilai dari pendekatan ini adalah mudah untuk mengikat tujuan bisnis dengan tujuan keamanan. Contoh dari tujuan bisnis adalah “Aktifkan koneksi eksternal yang aman dan percepatan penyediaan pengguna dan lingkungan baru, dengan mengotomatiskan visibilitas dan pengukuran terhadap praktik terbaik untuk terus menurunkan risiko.” Anda menetapkan tujuan teknologi yang membantu Anda memenuhi hasil bisnis yang sesuai. Model tujuan bisnis terkait kembali ke tujuan keamanan, seperti menjaga visibilitas. Anda kemudian menerapkan tujuan teknis, seperti praktik terbaik keamanan AWS Identity and Access Management (IAM), untuk mengurangi risiko keamanan.

Keuntungan dari pendekatan objektif bisnis:

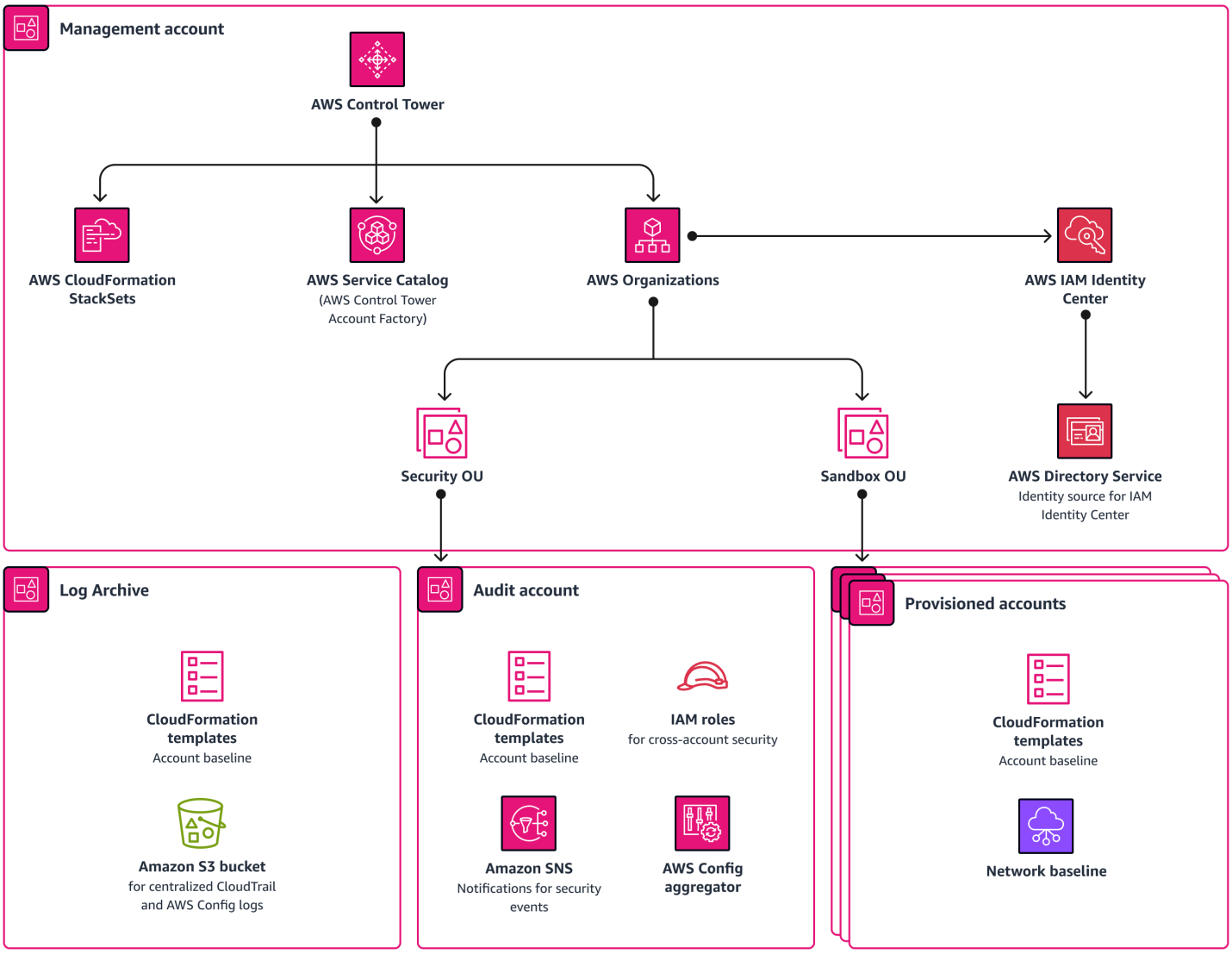
- Termasuk pembenaran biaya
- Memberikan arah keamanan yang jelas dan selaras dengan bisnis
- Mendefinisikan ukuran keberhasilan melalui pencapaian target hasil bisnis

Kerugian dari pendekatan objektif bisnis:

- Dapat memakan waktu karena Anda harus mencari tahu apa yang diinginkan bisnis
- Berfokus pada bisnis daripada berfokus pada teknologi

Membangun: Meletakkan dasar untuk fondasi keamanan cloud yang kuat

Sekarang setelah Anda memiliki rencana, langkah selanjutnya adalah meletakkan dasar. Langkah ini menunjukkan cara membangun fondasi cloud awal AWS yang aman, tangguh, terukur, dan otomatis di beberapa akun. Meletakkan dasar dapat dirancang dan disesuaikan secara khusus sesuai dengan tujuan bisnis Anda. Anda dapat menyesuaikan kontrol ke landing zone baru, atau Anda dapat memasukkannya ke dalam landing zone yang ada. Otomatisasi di AWS Control Towerdapat membantu Anda meletakkan dasar keamanan di. AWS Cloud Gambar berikut menunjukkan landing zone yang diatur melalui AWS Control Tower.



AWS Control Tower mengatur beberapa Layanan AWS atas nama Anda, seperti AWS Organizations,, dan. AWS Service Catalog AWS IAM Identity Center Anda dapat mengatur landing zone baru dalam waktu satu jam, dan landing zone tersebut dirancang untuk memenuhi persyaratan keamanan dan kepatuhan Anda. AWS Control Tower mengatur landing zone Anda sesuai dengan praktik terbaik keamanan preskriptif. AWS Control Tower membantu Anda mengelola penyediaan cloud dengan meningkatkan visibilitas dan kontrol atas akun dan pengguna akhir. Ini membantu administrator mengalokasikan dan mengawasi sumber daya komputasi secara efisien, menerapkan kontrol akses berbasis peran, memantau kinerja melalui alat pencatatan dan pemantauan, mengelola biaya secara efektif, mengotomatiskan proses penyebaran, menegakkan langkah-langkah keamanan, dan memastikan kepatuhan terhadap standar industri.

AWS Control Tower adalah cara tercepat untuk mengatur dan mengatur AWS lingkungan multi-akun yang aman, patuh, berdasarkan praktik terbaik. Untuk informasi lebih lanjut tentang bekerja dengan AWS Control Tower dan praktik terbaik yang diuraikan dalam strategi AWS multi-akun, lihat strategi AWS multi-akun: Panduan praktik terbaik.

Meskipun AWS Control Tower merupakan pendekatan tercepat, itu bukan satu-satunya. Bagian yang penting adalah Anda mengatur landing zone yang, setidaknya, menyediakan yang berikut:

- Manajemen multi-akun
- Identitas dan manajemen akses federasi
- Arsip terpusat untuk log
- Akses audit lintas akun
- Penyediaan akun pengguna akhir
- Pemantauan dan pemberitahuan terpusat

Menilai: Mengevaluasi postur keamanan cloud Anda saat ini

Sebelum Anda menyebarkan apa pun ke landing zone, nilai landing zone Anda untuk memastikannya memenuhi persyaratan Anda dan untuk menetapkan garis dasar. Praktik ini disebut penilaian postur awan. Ini membantu Anda mengidentifikasi dan memulihkan risiko di seluruh infrastruktur cloud Anda. Menilai postur keamanan cloud Anda memberikan visibilitas kontrol keamanan yang relevan di lingkungan cloud.

Berikut ini adalah manfaat dari penilaian postur cloud:

- Ini membantu Anda memahami postur keamanan Anda saat ini dan mendapatkan rekomendasi untuk mengurangi profil risiko Anda, memulihkan kerentanan yang ada, atau memperbaiki kesalahan konfigurasi.
- Ini membantu Anda mengidentifikasi praktik terbaik keamanan sehingga Anda dapat menghindari kesalahan langkah dan mengurangi risiko bisnis.
- Ini menyediakan metrik yang membantu Anda melacak peningkatan dan mengukur keberhasilan.

Bagian ini mengulas layanan dan alat, AWS Security Hub CSPM danProwler, yang dapat Anda gunakan untuk melakukan penilaian postur cloud di lingkungan Anda.

Prowler

Prowleradalah alat baris perintah open source yang membantu Anda menilai, mengaudit, dan memantau akun Anda untuk kepatuhan terhadap praktik terbaik AWS keamanan dan kerangka kerja dan standar keamanan lainnya. Ini memeriksa konfigurasi Anda dan mengidentifikasi masalah keamanan. Anda dapat menggunakannya Prowler di lingkungan multi-akun, dan vendor pihak ketiga juga dapat menggunakannya untuk menilai keamanan lingkungan Anda. AWS

Berikut ini adalah manfaat dariProwler:

- Ini gratis dan open source.
- Ini memiliki opsi penerapan yang fleksibel dan dapat diskalakan.
- Ini menjalankan pemeriksaan kepatuhan, seperti untuk Center for Internet Security (CIS) Benchmark for AWS, General Data Protection Regulation (GDPR), dan HIPAA.
- Ini membantu Anda membuat snapshot dan baseline.

AWS Security Hub CSPM

AWS Security Hub CSPMmemberikan pandangan komprehensif tentang keadaan keamanan Anda di AWS. Ini juga membantu Anda memeriksa lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Ini terintegrasi dengan AWS Control Tower sehingga Anda dapat mengkonfigurasi kontrol detektif Security Hub CSPM melalui layanan. AWS Control Tower Tujuan mempercepat kematangan keamanan adalah untuk mematangkan proses penilaian dari snapshot satu kali menjadi proses berkelanjutan untuk memantau kemajuan.

Berikut ini adalah manfaat dari Security Hub CSPM:

- Ini menyediakan dasbor terpadu yang menunjukkan status lingkungan saat ini dan membantu Anda mengidentifikasi dan memperbaiki masalah.
- Ini melakukan penilaian berkelanjutan dengan pemeriksaan otomatis.

Panggung berjalan: Operasionalisasi dan pematangan

Panggung berjalan berfokus pada operasionalisasi. Selama tahap ini, organisasi Anda perlu mengevaluasi model operasinya saat ini, menentukan bagaimana model tersebut harus disesuaikan untuk cloud, menerapkan perubahan tersebut, dan kemudian mengukur kemajuan. Ini termasuk menangani keterampilan, proses operasi, dan teknologi. Menyetel penyebaran cloud dan mengukur kemajuan sangat penting di seluruh tahap berjalan untuk memvalidasi kesuksesan.

Berikut ini adalah fase dalam tahap berjalan:

- Mengoperasionalkan— Bagaimana Anda mempersiapkan orang, teknologi, dan proses Anda untuk cloud?
- DewasaBagaimana Anda mengukur kemajuan dan kesuksesan?

Operasionalisasi: Mempersiapkan organisasi Anda untuk postur keamanan cloud yang matang

Untuk bergerak maju dengan proses penyebaran beban operasional ke cloud, penting untuk fokus pada penyelarasan orang, proses, dan teknologi. Hal ini sangat penting dalam lingkungan cloud karena proses dan keterampilan mungkin berbeda dari operasi lokal. Di bagian ini, Anda menggunakan kerangka kerja untuk menyelaraskan karyawan, proses, dan teknologi Anda, dan kemudian Anda mengonfirmasi bahwa kerangka kerja telah membantu Anda mencapai hasil yang Anda harapkan.

AWS Kerangka Adopsi Cloud

AWS Cloud Adoption Framework (AWS CAF) membantu Anda mempercepat hasil bisnis Anda melalui penggunaan Layanan AWS dan fitur inovatif. AWS CAF mengidentifikasi enam perspektif organisasi spesifik yang mendukung transformasi cloud yang sukses: Bisnis, Orang, Tata Kelola,

Platform, Keamanan, dan Operasi. Setiap perspektif berisi kemampuan yang dapat meningkatkan kesiapan cloud Anda dan membantu Anda mempercepat perjalanan transformasi cloud Anda.

Gambar berikut menunjukkan enam perspektif dalam AWS CAF dan kemampuan di setiap perspektif. Untuk informasi selengkapnya, lihat Kemampuan dasar dalam Ikhtisar Kerangka Adopsi AWS Cloud.

Hasil yang diharapkan

Saat Anda menggunakan AWS CAF untuk menyelaraskan karyawan, proses, dan teknologi Anda, Anda dapat mengharapkan untuk mencapai hasil berikut:

- DevSecOps pipeline and process — Menerapkan DevOps pipeline dengan alat keamanan terintegrasi dapat membantu Anda menerapkan infrastruktur sebagai kode (IAc) dengan lebih aman. Anda dapat menerapkan pemindaian kode dan pemeriksaan keamanan dalam proses pipeline, seperti cfn_nag (GitHub), yang merupakan penganalisis kode statis open source.
- Penandaan dan manajemen aset — Tag dapat membantu Anda mengelola sumber daya secara lebih efisien dan konsisten di cloud. Untuk informasi selengkapnya, lihat Menandai sumber daya AWS. Sangat penting untuk mengembangkan strategi manajemen aset dinamis yang dapat beradaptasi dengan sifat cloud yang terus berubah. AWS Systems Manager Inventaris membantu Anda menetapkan tag sehingga Anda dapat dengan cepat mencari, mengelola, dan mengidentifikasi sumber daya Anda.
- Pemantauan dan integrasi detektif — Sangat penting untuk menetapkan metode untuk mengirim peringatan dari cloud ke pusat operasi keamanan lokal (SOCs) dan sistem informasi keamanan dan manajemen peristiwa (SIEM). Amazon GuardDuty adalah layanan pemantauan keamanan berkelanjutan yang menganalisis dan memproses log untuk mengidentifikasi aktivitas tak terduga dan berpotensi tidak sah di lingkungan Anda AWS . Ini juga terintegrasi dengan banyak alat pihak ketiga.
- Rencana dan program respons insiden cloud — Penting untuk memastikan bahwa personel yang bertanggung jawab menangani peringatan cloud terbiasa dengan proses menelan peringatan tersebut dan mengetahui cara merespons peringatan cloud, dibandingkan dengan peringatan lokal. Untuk meningkatkan kemampuan respons insiden, latih personel untuk menggunakan Detektif Amazon untuk analisis log. Amazon Detective membantu Anda menganalisis, menyelidiki, dan mengidentifikasi akar penyebab temuan keamanan atau aktivitas mencurigakan. Amazon Detective harus menjadi bagian dari rencana respons insiden.
- Manajemen kerentanan cloud — Proses mengelola kerentanan di cloud berbeda dari lingkungan lokal. Selain manajemen kerentanan tradisional, Anda juga harus menilai lapisan kode infrastruktur. Amazon Inspector adalah layanan manajemen kerentanan otomatis yang terus-menerus mengevaluasi sumber daya Anda untuk kerentanan dan paparan jaringan yang tidak diinginkan.
- Manajemen postur cloud — Manajemen postur cloud, seperti yang dijelaskan di bagian Penilaian, merupakan aspek penting dari keamanan cloud. Anda dapat menggunakannya AWS Security Hub CSPM untuk mengotomatiskan pemeriksaan praktik terbaik keamanan dan mengevaluasi keseluruhan postur cloud Anda di semua area Anda Akun AWS.
- Pelatihan keamanan cloud — Sangat penting untuk memberikan pelatihan yang tepat kepada karyawan sehingga mereka menjadi mahir dalam keamanan cloud. Ini termasuk menyediakan akses ke sumber daya dan mengalokasikan waktu bagi karyawan untuk memperoleh pengetahuan

dan keterampilan yang diperlukan. AWS menyediakan banyak sumber pelatihan untuk meningkatkan keterampilan dan mendidik, seperti AWS Skill Builder.

Dewasa: Proses penyetelan dan pengukuran, alat, dan risiko

Pada fase matang model keamanan cloud, fokusnya adalah menyelaraskan tim keamanan dengan kemampuan keamanan AWS Cloud Adoption Framework (AWS CAF) dan melembagakan proses tangkas. Penyelarasan ini membantu tim khusus mempercepat inovasi dalam sprint pendek sambil juga menggabungkan peta jalan dan perencanaan jarak jauh. Fase matang menekankan kolaborasi dengan operasi TI dan meningkatkan keterampilan cloud khusus yang mendalam. Setiap kemampuan keamanan menerapkan alat dan proses utama untuk meningkatkan efisiensi dan dampak, disertai dengan pengembangan metrik dan mekanisme pelaporan untuk mengukur perubahan bertahap dan dampak keseluruhan.

Pada fase ini, Anda:

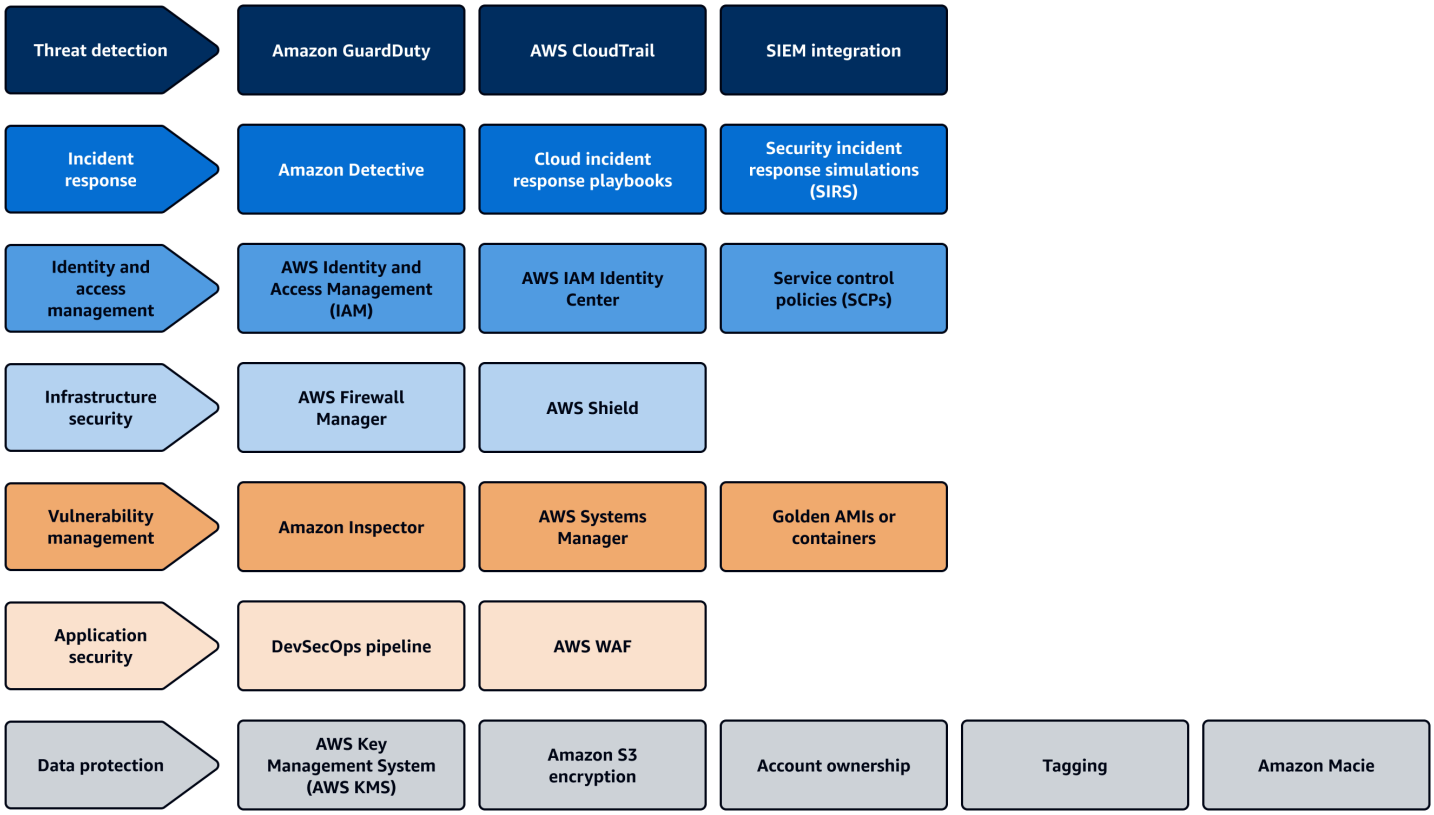
- Menyetel dan mengukur proses
- Menyetel dan mengukur alat
- Menyetel dan mengukur risiko
- Tinjau contoh kasus penggunaan pada fase matang

Menyetel dan mengukur proses

Pendekatan tangkas memberikan lebih banyak fleksibilitas dan inovasi, dan dapat membantu Anda dengan cepat menguji dan menerapkan ide-ide baru. Bagilah tim keamanan Anda menjadi peran khusus, seperti responden insiden dan manajer kerentanan. Peran harus selaras dengan kategori dalam gambar berikut, yang sesuai dengan kemampuan dalam AWS Cloud Adoption Framework (AWS CAF). Pendekatan tangkas mendorong tim untuk berpikir besar, menciptakan, menyederhanakan, dan mengidentifikasi potensi kesenjangan dalam keamanan. Ini menghasilkan pembuatan backlog cerita pengguna atau peta jalan untuk perbaikan di masa depan.

Proses tangkas memungkinkan solusi yang lebih dinamis dan adaptif, daripada hanya mengandalkan kemampuan alat tertentu. Gagal cepat adalah filosofi yang menggunakan pengujian yang sering dan bertahap untuk mengurangi siklus hidup pengembangan, dan ini adalah bagian penting dari pendekatan tangkas. Buat perubahan, uji, dan kemudian putuskan apakah akan melanjutkan pendekatan saat ini atau beralih ke pendekatan alternatif. Jika tim bekerja dalam siklus ini, ini

membantu organisasi Anda tetap terkini dengan sifat cloud yang serba cepat. Pelatihan terfokus juga penting, dan Anda harus memberikan pelatihan yang khusus untuk domain keamanan cloud tertentu.



> **Note**
>
> Gambar ini tidak berisi jaminan keamanan dan kemampuan tata kelola keamanan di CAF. AWS Panduan ini berfokus pada operasi keamanan, dan jaminan keamanan dan tata kelola berada di luar cakupan panduan ini. Untuk informasi selengkapnya tentang jaminan keamanan, lihat AWS re:Inforce 2023 - Scaling compliance with on. AWS Control Tower YouTube

Dalam organisasi Anda, gunakan pendekatan tangkas yang membantu organisasi Anda mengikuti perkembangan pesat dan perubahan di cloud. Berikut ini adalah beberapa cara untuk mulai bereksperimen dan iterasi di lingkungan cloud Anda:

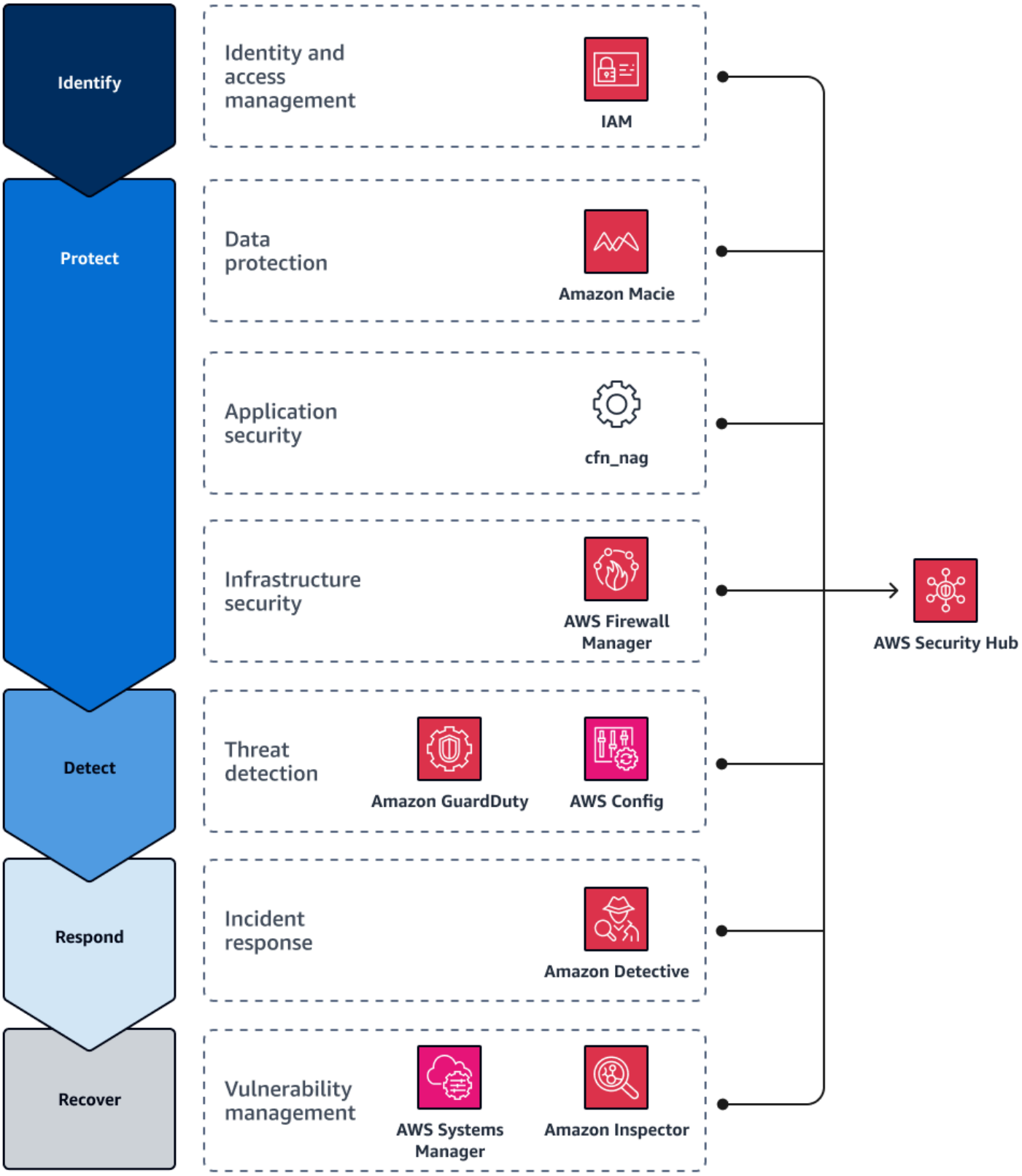
- Spesialisasi pada kategori yang ditentukan dalam AWS CAF, seperti yang ditunjukkan pada gambar sebelumnya.
- Agar lebih dinamis, fokuslah pada inovasi daripada operasi.

- Bergerak cepat dalam sprint dengan memungkinkan orang untuk menguji, gagal cepat, dan menerapkan dengan cepat dan melanjutkan siklus ini untuk mengikuti bisnis.
- Untuk mendukung operasi berkelanjutan, jika memungkinkan, menyelaraskan proses untuk lingkungan berbasis Internet dan lokal.
- Untuk membantu individu menelusuri dan fokus pada satu area, berikan pelatihan yang terfokus alih-alih pelatihan luas.
- Dorong orang untuk berpikir besar, menyelidiki “bagaimana jika,” dan membuat backlog (seperti peta jalan atau celah).

Menyetel dan mengukur alat

Setelah Anda membentuk tim khusus untuk domain keamanan yang berbeda, selaraskan tim satu sama lain. AWS Security Hub CSPMdapat membantu Anda mencapai ini. Security Hub CSPM menyediakan dasbor terpusat dan terpadu untuk memantau kemajuan terhadap kerangka kerja. Ini juga terintegrasi dengan layanan AWS keamanan banyak alat pihak ketiga.

Kerangka Keamanan Siber Institut Standar dan Teknologi Nasional (NIST) di situs web NIST terdiri dari lima fungsi: mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan. Gambar berikut menunjukkan bagaimana Anda dapat menggunakan yang berbeda Layanan AWS selama setiap fungsi dan kemudian mengonfigurasi layanan tersebut untuk mengirimkan temuannya ke Security Hub CSPM untuk pelaporan terkonsolidasi. Jika Anda memilih untuk menggunakan alat lain, Anda dapat menggunakan Security Hub CSPM API, AWS Command Line Interface (AWS CLI), dan AWS Security Finding Format (ASFF) untuk membuat integrasi kustom. Untuk informasi selengkapnya tentang integrasi CSPM Security Hub dengan layanan lain, lihat Integrasi produk dalam dokumentasi CSPM AWS Security Hub CSPM Security Hub.



Security Hub CSPM terintegrasi dengan semua layanan dan alat ini dan menyediakan hal-hal berikut:

- Menyediakan dasbor terpadu yang menampilkan pembaruan dan membantu tim untuk melakukan iterasi
- Terintegrasi secara otomatis dengan layanan AWS keamanan, seperti Amazon Macie, Amazon, dan _GuardDutyAmazon Detective
- Mendukung integrasi dengan alat pihak ketiga, seperti Prowlerdan cfn_nag
- Mendukung integrasi kustom dengan alat, seperti Security Hub CSPM API AWS CLI, dan AWS Security Finding Format (ASFF)

Menyetel dan mengukur risiko

Selama fase matang dari tahap berjalan, Anda dapat menggunakannya AWS Security Hub CSPM untuk terus menyesuaikan dan mengukur risiko keamanan. Security Hub CSPM terus menilai postur keamanan organisasi dan mengambil tindakan untuk memulihkan masalah yang teridentifikasi. Security Hub CSPM memusatkan dan memprioritaskan temuan keamanan dari seluruh layanan Akun AWS, dan mitra pihak ketiga yang didukung. Ini membantu Anda menganalisis tren keamanan dan mengidentifikasi masalah keamanan prioritas tinggi.

Security Hub CSPM melakukan ratusan pemeriksaan keamanan dan mengklasifikasikannya berdasarkan risiko terhadap lingkungan Anda. AWS Anda dapat melihat skor Anda terhadap kontrol keamanan di dasbor terpadu di konsol CSPM Security Hub. Untuk informasi selengkapnya, lihat Menentukan skor keamanan dalam dokumentasi CSPM Security Hub. Melalui dasbor ini, DevSecOps fungsi dapat dengan cepat mengidentifikasi pemeriksaan apa pun yang gagal, tingkat keparahan masalah keamanan, Wilayah AWS dan sumber daya mana yang terpengaruh. Setelah diidentifikasi, DevSecOps tim dapat memprioritaskan dan memulihkan masalah. Saat masalah diperbaiki, Security Hub CSPM secara otomatis memperbarui status.

Tinjau contoh kasus penggunaan pada fase matang

Berikut ini adalah contoh fase matang. Contoh-contoh ini menyelam lebih dalam ke dalam model, alat, dan proses untuk tujuan bisnis yang berbeda, pada tingkat praktis.

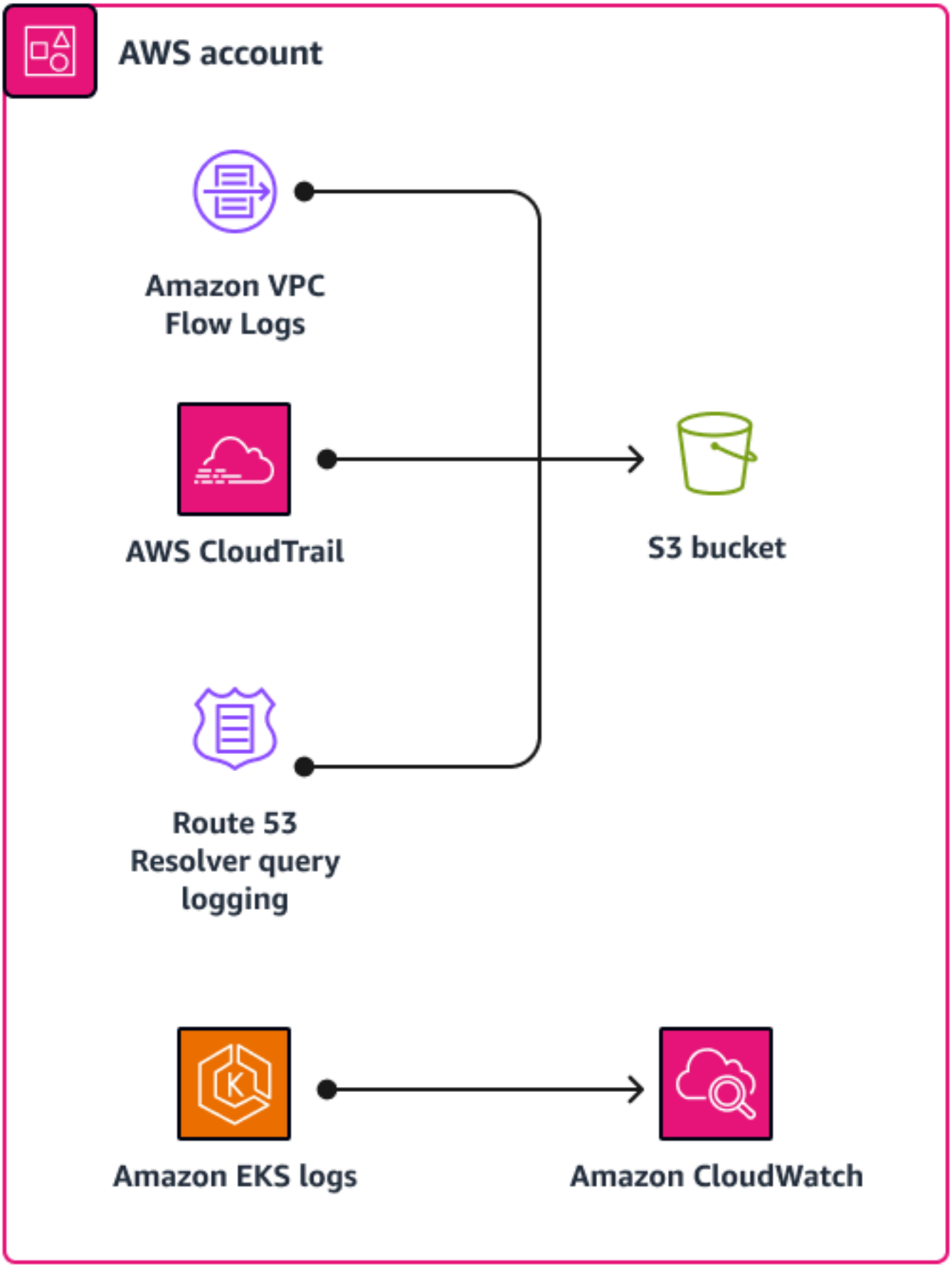
Dewasa: Contoh deteksi ancaman

Hasil bisnis untuk kontrol detektif: Meningkatkan visibilitas dan kecepatan deteksi insiden cloud untuk menurunkan risiko dan memungkinkan penggunaan dan pengembangan sumber daya cloud yang dipercepat.

Tool: Assisted Log Enabler for AWS(GitHub) adalah alat open source yang membantu Anda mengaktifkan logging di tengah insiden keamanan. Ini dapat dengan cepat meningkatkan visibilitas Anda ke dalam suatu insiden.

Contoh kasus penggunaan: Pertimbangkan kasus penggunaan akun tunggal yang digambarkan dalam diagram berikut. Ada peristiwa yang membutuhkan penyelidikan lebih lanjut. Anda tidak yakin apakah logging diaktifkan. Dalam hal ini, tindakan terbaik adalah melakukan dry run dengan melihat layanan mana yang diaktifkan atau dinonaktifkan. Assisted Log Enabler Assisted Log Enablermemeriksa AWS CloudTrail jejak, log kueri DNS, log aliran VPC, dan log lainnya. Jika mereka tidak diaktifkan, Assisted Log Enabler aktifkan mereka. Assisted Log Enablerdapat memeriksa dan mengaktifkan logging di semua Wilayah AWS.

Anda juga bisa melakukan throttle Assisted Log Enabler ke atas atau ke bawah. Setelah Anda menyelesaikan dry run, menutup acara, dan menyelesaikan masalah, Anda menyadari bahwa Anda tidak lagi membutuhkan tingkat logging ini. Anda dapat dengan cepat membersihkan penyebaran untuk menghentikan logging. Fitur ini memungkinkan Anda untuk digunakan Assisted Log Enabler sebagai alat triase.


AWS account
Amazon VPC Flow Logs
AWS CloudTrail
S3 bucket
Route 53 Resolver query logging
Amazon EKS logs
Amazon CloudWatch

Berikut ini adalah fitur utama dariAssisted Log Enabler for AWS:

- Anda dapat menjalankannya di lingkungan satu akun atau multi-akun.
- Anda dapat menggunakannya untuk menetapkan garis dasar untuk masuk ke lingkungan Anda.
- Anda dapat menggunakan fitur dry run untuk memeriksa status saat ini dan menentukan layanan mana yang mengaktifkan logging.
- Anda dapat memilih layanan mana yang ingin Anda aktifkan pencatatan.
- Anda dapat melakukan throttle ke Assisted Log Enabler atas atau ke bawah, untuk kasus penggunaan Anda.

Dewasa: Contoh IAM

Hasil bisnis IAM: Mengotomatiskan visibilitas dan pengukuran terhadap praktik terbaik untuk terus mengurangi risiko, untuk memungkinkan koneksi eksternal yang aman, dan untuk menyediakan pengguna dan lingkungan baru dengan cepat

Alat:AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) membantu Anda mengidentifikasi sumber daya yang dibagikan dengan entitas eksternal, memvalidasi kebijakan IAM terhadap tata bahasa kebijakan dan praktik terbaik, dan menghasilkan kebijakan IAM berdasarkan aktivitas akses historis. Kami sangat menyarankan Anda mengaktifkan IAM Access Analyzer di tingkat akun dan organisasi.

Manfaat layanan: IAM Access Analyzer menyediakan banyak temuan berwawasan luas. Ini dapat mengidentifikasi sumber daya dan akun organisasi Anda yang dibagikan dengan entitas eksternal. Ini dapat mendeteksi sumber daya seperti bucket S3 publik, AWS KMS key berbagi dengan akun lain, atau peran yang dibagikan dengan akun eksternal, memberi Anda visibilitas yang sangat baik untuk mengidentifikasi sumber daya yang tidak berada di bawah kendali organisasi Anda. Ini tidak hanya memvalidasi kebijakan IAM tetapi juga dapat menghasilkannya untuk Anda.

Jalankan tahap: Mengoptimalkan operasi keamanan cloud Anda

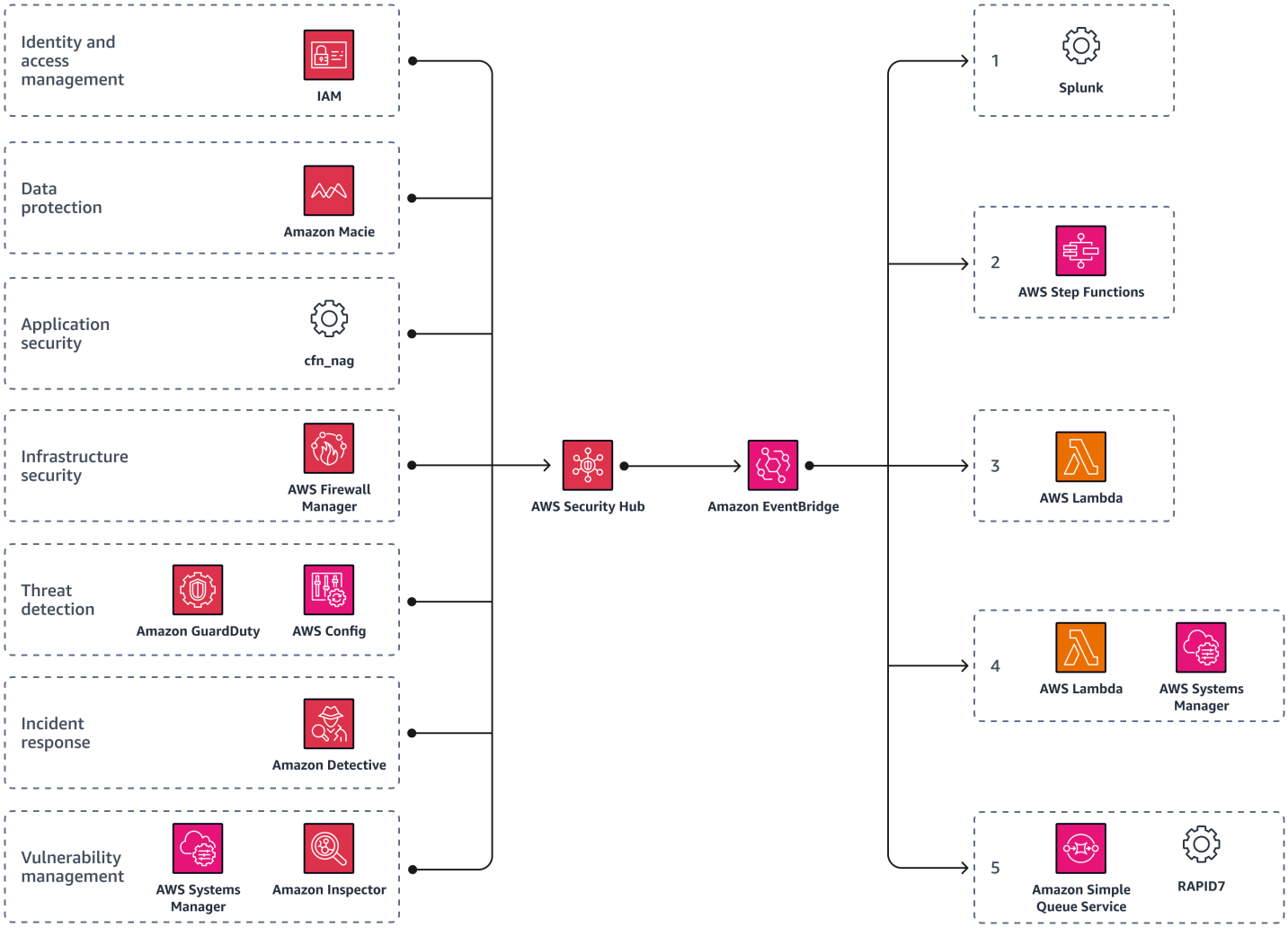
Setelah Anda menerapkan baseline di tahap berjalan, organisasi Anda maju ke tahap lari. Tahap ini difokuskan untuk menunjukkan kemampuan keamanan siber yang tersedia di cloud, banyak di antaranya tidak mungkin atau sangat sulit diterapkan dengan solusi lokal. Tahap ini menyatukan berbagai komponen keamanan dan mengotomatiskan proses. Otomatisasi membebaskan sumber daya Anda sehingga mereka dapat fokus pada pekerjaan bernilai tinggi.

Berikut ini adalah satu-satunya fase dalam tahap lari:

- Pengoptimalan— Bagaimana cara meningkatkan proses ini dan menambahkan otomatisasi?

Optimalkan: Otomatiskan dan ulangi operasi keamanan cloud Anda

Pada fase optimasi, Anda mengotomatiskan operasi keamanan Anda. Seperti tahapan crawl dan walk, Anda dapat menggunakan AWS Security Hub CSPM selama tahap run untuk mencapai otomatisasi dan iterasi. Gambar berikut menunjukkan cara CSPM Security Hub dapat memicu EventBridge aturan Amazon khusus yang menentukan tindakan otomatis yang harus diambil terhadap temuan dan wawasan tertentu. Untuk informasi selengkapnya, lihat Otomatisasi di dokumentasi CSPM Security Hub.



Dengan menggunakan Security Hub CSPM sebagai pusat otomatisasi pusat, Anda juga dapat meneruskan aktivitas ke. Splunk Splunkkemudian dapat mendeteksi yang anomali dan memicu tindakan yang sesuai di. EventBridge Ini membantu Anda mengotomatiskan tugas berulang dan menyediakan lebih banyak waktu bagi anggota tim yang terampil untuk fokus pada aktivitas bernilai lebih tinggi. Anda juga dapat menggunakannya AWS Step Functionsuntuk mengumpulkan log, mengambil foto forensik, mengkarantina server yang disusupi, dan menggantinya dengan gambar emas. Selain itu, Anda dapat menggunakan AWS Lambdafungsi yang digunakan AWS Systems Manageruntuk memulihkan kerentanan di seluruh lingkungan dan menggunakan fungsi Amazon Simple Queue Service (Amazon SQS) untuk memvalidasi keamanan sistem. Dengan mengambil pendekatan ini, dimungkinkan untuk dengan cepat menahan dan memulihkan insiden keamanan dengan dampak minimal terhadap operasi bisnis normal.

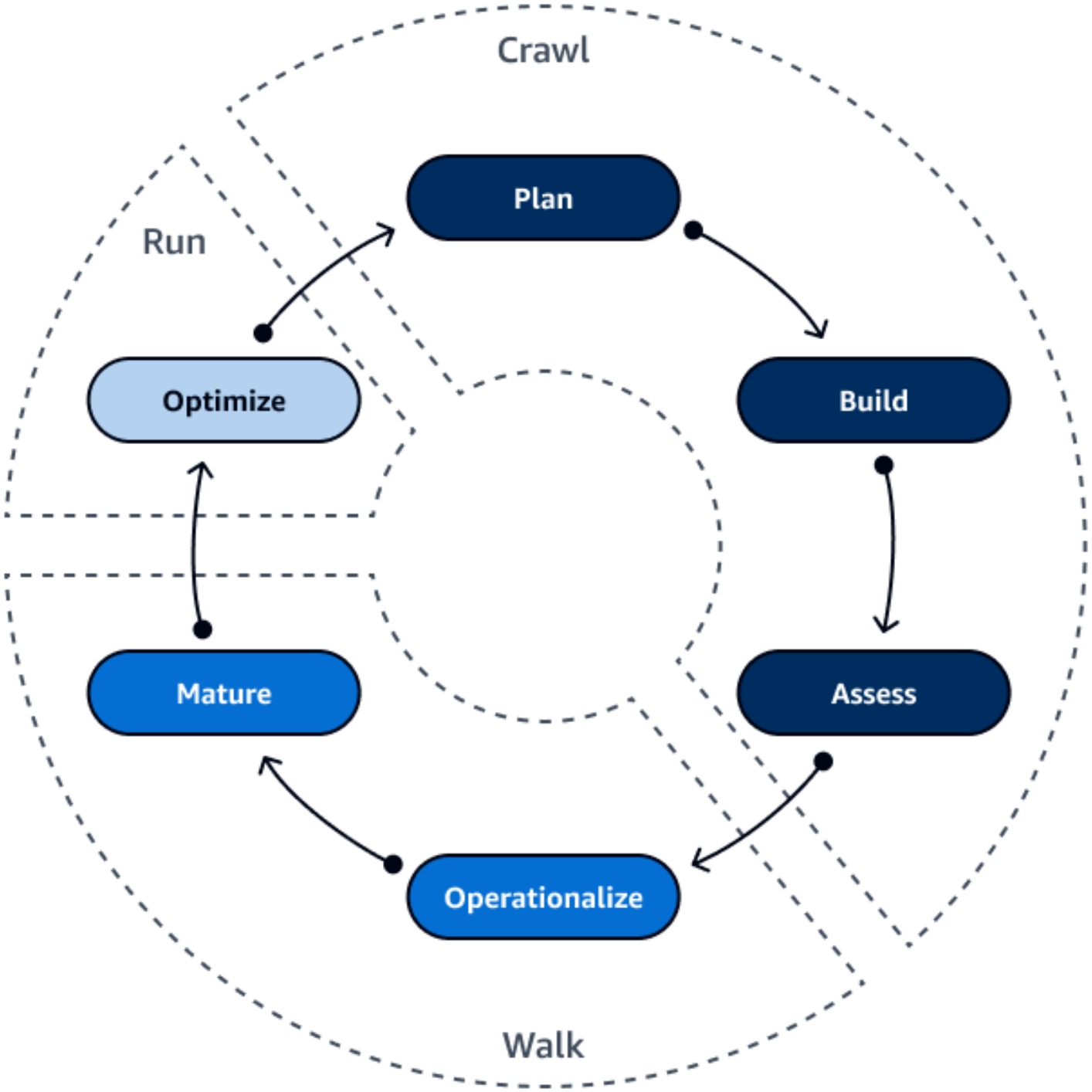
Berikut ini adalah contoh tindakan otomatis berulang, seperti yang ditunjukkan pada gambar sebelumnya:

1. Gunakan Splunk untuk mendeteksi aktivitas yang dipertanyakan.
2. Gunakan Step Functions untuk mengumpulkan log, mencabut akses, karantina, dan mengambil snapshot forensik.
3. Gunakan EventBridge aturan untuk memulai fungsi Lambda yang mengkarantina, mengambil foto forensik, dan mengganti server yang disusupi dengan gambar emas.
4. Mulai fungsi Lambda yang menggunakan Systems Manager untuk memulihkan dan menerapkan tambalan di seluruh lingkungan lainnya.
5. Mulai pesan Amazon SQS yang menggunakan pemindai Rapid7 untuk memindai dan memvalidasi apakah sumber daya aman. AWS

Untuk informasi selengkapnya, lihat Cara mengotomatiskan respons insiden di instans AWS Cloud untuk EC2 di Blog Keamanan. AWS

Kesimpulan: Merangkak, berjalan, lari, lalu terbang!

Singkatnya, model crawl, walk, run adalah kerangka kerja yang membantu Anda secara bertahap meningkatkan postur keamanan Anda dan mengadopsi praktik terbaik untuk mengamankan infrastruktur AWS . Proses ini terus berkembang seiring dengan munculnya teknologi dan kebutuhan bisnis baru. Dengan mengikuti kerangka kerja ini dan menggunakan sumber daya yang disediakan oleh AWS, Anda dapat membangun fondasi yang kuat untuk keamanan cloud, mengelola risiko keamanan secara efektif, mempercepat kematangan keamanan, dan mendorong inovasi.



Pada tahap merangkak, Anda mengatur fondasi. Anda menentukan apa rencana keamanan Anda, menggunakan arsitektur praktik terbaik keamanan yang ditentukan, dan mendorong penilaian berkelanjutan terhadap tujuan bisnis organisasi Anda.

Di panggung berjalan, Anda mengambil langkah pertama. Anda melihat kebijakan, membangun buku pedoman, melatih orang, dan menyelaraskan strategi. Tahap ini membantu Anda memahami cara memanfaatkan inovasi untuk mengikuti teknologi di cloud.

Di tahap lari, Anda berpikir besar. Anda menggunakan otomatisasi dan menempatkan orang-orang terampil Anda secara strategis di tempat yang tepat. Anda menerapkan otomatisasi untuk mendorong penilaian berkelanjutan terhadap tujuan bisnis organisasi Anda.

Sekarang, saatnya Anda terbang. Gunakan rekomendasi dalam panduan ini untuk mempercepat kematangan keamanan Anda di AWS Cloud.

Sumber daya

Kerangka kerja dan model

- AWS Kerangka Adopsi Cloud (AWS CAF)
- AWS Kerangka Well-Architected
- AWS Arsitektur Referensi Keamanan (AWS SRA)
- AWS Model Kematangan Keamanan
- Arsitektur Referensi HIPAA
- Arsitektur Referensi HITRUST

Layanan AWS

- AWS Control Tower
- AWS Identity and Access Management Access Analyzer
- AWS Security Hub CSPM

AWS Sumber daya lainnya

- Respon Keamanan Otomatis AWS aktif di Perpustakaan AWS Solusi
- Otomatiskan Operasi TI Anda Menggunakan AWS Step Functions dan CloudWatch Acara Amazon di Blog AWS Komputasi
- Cara mengotomatiskan respons insiden di AWS Cloud for EC2 instance di Blog Keamanan AWS
- Cara melakukan respons insiden otomatis di lingkungan multi-akun di Blog AWS Keamanan
- AWS Re: Inforce 2022 - Merangkak, berjalan, berlari: Mempercepat video kematangan keamanan aktif YouTube
- AWS Re: Inforce 2022 - Merangkak, berjalan, berlari: Mempercepat presentasi kematangan keamanan (Lampiran) PowerPoint

Kontributor

Individu berikut berkontribusi pada panduan ini.

Mengotorisasi

- Chad Lorenc, Manajer Praktik Keamanan, AWS
- Ivy Gin, Konsultan Jaminan Keamanan, AWS
- Sayali Paseband, Konsultan Keamanan, AWS

Meninjau

- Deeps Baisya, Arsitek Keamanan Senior, AWS
- Mike LaRue, Konsultan Keamanan Senior, AWS
- Raul Radu, Insinyur Keamanan Senior, AWS

Penulisan teknis

- Lilly AbouHarb, Penulis Teknis Senior, AWS

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	—	20 Desember 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 — Pindahkan aplikasi dan modifikasi 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 Edition. PostgreSQL-Compatible
- Replatform (angkat dan bentuk ulang) — Pindahkan aplikasi ke cloud, dan perkenalkan beberapa tingkat pengoptimalan untuk memanfaatkan kemampuan cloud. Contoh: Memigrasikan 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

A2A () Agent-to-Agent

Protokol stateful untuk kolaborasi agen-ke-agen yang mendukung delegasi tugas dan transfer negara.

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.

Agen

Sistem AI yang dapat secara mandiri bernalar, merencanakan, dan mengambil tindakan menggunakan alat untuk mencapai tujuan.

Agen Ops

Praktik operasional untuk membangun, menguji, menyebarkan, dan menjalankan agen AI dalam produksi dalam skala besar.

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.

blue/green penyebaran

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. AWS Well-Architected

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.

Pengembang Warga

Pengguna bisnis yang membuat aplikasi AI menggunakan platform tanpa code/low kode tanpa keterampilan teknis khusus.

Enkripsi sisi klien

Enkripsi data secara lokal, sebelum target Layanan AWS 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 AWS Cloud Perusahaan. Untuk informasi tentang bagaimana kaitannya dengan strategi AWS migrasi, lihat panduan kesiapan migrasi.

CMDB

Lihat database manajemen konfigurasi.

repositori kode

Lokasi di mana kode sumber dan aset lainnya, seperti dokumentasi, sampel, dan skrip, disimpan dan diperbarui melalui proses kontrol versi. Repositori cloud umum termasuk GitHub atau. Bitbucket Cloud Setiap versi kode disebut cabang. Dalam struktur layanan mikro, setiap repositori dikhususkan untuk satu bagian fungsionalitas. Satu CI/CD pipa dapat menggunakan beberapa repositori.

cache dingin

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

data dingin

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

visi komputer (CV)

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

konfigurasi drift

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

database manajemen konfigurasi (CMDB)

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

paket kesesuaian

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

integrasi berkelanjutan dan pengiriman berkelanjutan (CI/CD)

Proses mengotomatiskan sumber, membangun, menguji, pementasan, dan tahap produksi dari proses rilis perangkat lunak. CI/CD biasanya digambarkan sebagai pipa. CI/CD dapat membantu Anda mengotomatiskan proses, meningkatkan produktivitas, meningkatkan kualitas kode, dan memberikan lebih cepat. Untuk informasi lebih lanjut, lihat Manfaat pengiriman berkelanjutan. CD juga dapat berarti penerapan berkelanjutan. Untuk informasi selengkapnya, lihat Continuous Delivery vs Continuous Deployment.

CV

Lihat visi komputer.

D

data saat istirahat

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

klasifikasi data

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

penyimpangan data

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

data dalam transit

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

jala data

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

minimalisasi data

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

perimeter data

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

prapemrosesan data

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

asal data

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

subjek data

Individu yang datanya dikumpulkan dan diproses.

gudang data

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

bahasa definisi database (DDL)

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

bahasa manipulasi basis data (DHTML)

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

DDL

Lihat bahasa definisi database.

ansambel yang dalam

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

pembelajaran mendalam

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

pertahanan-mendalam

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, pendekatan defense-in-depth 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 setiap komponen. Konsep ini diperkenalkan oleh Eric Evans dalam bukunya, Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003). Untuk informasi tentang cara menggunakan desain berbasis domain dengan pola gambar pencekik, lihat Memodernisasi layanan web Microsoft ASP.NET (ASMX) lama secara bertahap menggunakan container dan Amazon API Gateway.

DR

Lihat pemulihan bencana.

deteksi drift

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

DVSM

Lihat pemetaan aliran nilai pengembangan.

E

EDA

Lihat analisis data eksplorasi.

EDI

Lihat pertukaran data elektronik.

komputasi tepi

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

pertukaran data elektronik (EDI)

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

enkripsi

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

kunci enkripsi

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

endianness

Urutan byte disimpan dalam memori komputer. Big-endian sistem menyimpan byte paling signifikan terlebih dahulu. Little-endian sistem menyimpan byte paling tidak signifikan terlebih dahulu.

titik akhir

Lihat titik akhir layanan.

layanan endpoint

Layanan yang dapat Anda host di cloud pribadi virtual (VPC) untuk dibagikan dengan pengguna lain. Anda dapat membuat layanan endpoint dengan AWS PrivateLink dan memberikan izin

kepada prinsipal lain Akun AWS atau ke AWS Identity and Access Management (IAM). Akun atau prinsipal ini dapat terhubung ke layanan endpoint Anda secara pribadi dengan membuat titik akhir VPC antarmuka. Untuk informasi selengkapnya, lihat Membuat layanan titik akhir di dokumentasi Amazon Virtual Private Cloud (Amazon VPC).

perencanaan sumber daya perusahaan (ERP)

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

enkripsi amplop

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

lingkungan

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

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

epik

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

ERP

Lihat perencanaan sumber daya perusahaan.

analisis data eksplorasi (EDA)

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

F

tabel fakta

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

gagal cepat

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

batas isolasi kesalahan

Dalam AWS Cloud, batas seperti Availability Zone, 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.

beberapa tembakan mendorong

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

FGAC

Lihat kontrol akses berbutir halus.

kontrol akses berbutir halus (FGAC)

Penggunaan beberapa kondisi untuk mengizinkan atau menolak permintaan akses.

migrasi flash-cut

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

FM

Lihat model pondasi.

model pondasi (FM)

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

Gerbang FM

Perantara terpusat yang mengontrol dan menormalkan akses ke model pondasi. Juga dikenal sebagai gateway LLM.

G

AI generatif

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

pemblokiran geografis

Lihat pembatasan geografis.

pembatasan geografis (pemblokiran geografis)

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

Alur kerja Gitflow

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

gambar emas

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

strategi greenfield

Tidak adanya infrastruktur yang ada di lingkungan baru. Saat mengadopsi strategi greenfield untuk arsitektur sistem, Anda dapat memilih semua teknologi baru tanpa batasan kompatibilitas

dengan infrastruktur yang ada, juga dikenal sebagai brownfield. Jika Anda memperluas infrastruktur yang ada, Anda dapat memadukan strategi brownfield dan greenfield.

pagar pembatas

Aturan tingkat tinggi yang membantu mengatur sumber daya, kebijakan, dan kepatuhan di seluruh unit organisasi (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 CSPM, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector, dan pemeriksaan khusus AWS Lambda .

pagar pembatas (AI)

Mekanisme keamanan yang menyaring, memvalidasi, dan membatasi input dan output agen untuk membantu memastikan perilaku AI yang bertanggung jawab dan aman.

H

HA

Lihat ketersediaan tinggi.

migrasi database heterogen

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

ketersediaan tinggi (HA)

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

modernisasi sejarawan

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

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

data penahanan

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

manusia-dalam-lingkaran (HiTL)

Pola alur kerja di mana eksekusi agen berhenti untuk peninjauan dan persetujuan manusia pada titik keputusan kritis.

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 in the Framework. AWS Well-Architected

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 lebih lanjut, lihat Interpretabilitas model pembelajaran mesin dengan. AWS

IoT

Lihat Internet of Things.

Perpustakaan informasi TI (ITIL)

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

Manajemen layanan TI (ITSM)

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

ITIL

Lihat perpustakaan informasi TI.

ITSM

Lihat manajemen layanan TI.

L

kontrol akses berbasis label (LBAC)

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

landing zone

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

model bahasa besar (LLM)

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

migrasi besar

Migrasi 300 atau lebih server.

LBAC

Lihat kontrol akses berbasis label.

hak istimewa paling sedikit

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

angkat dan geser

Lihat 7 Rs.

sistem endian kecil

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

LLM

Lihat model bahasa besar.

lingkungan yang lebih rendah

Lihat lingkungan.

M

pembelajaran mesin (ML)

Jenis kecerdasan buatan yang menggunakan algoritma dan teknik untuk pengenalan 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

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

sistem eksekusi manufaktur (MES)

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

PETA

Lihat Program Percepatan Migrasi.

MCP

Lihat Protokol Konteks Model.

Protokol Konteks Model (MCP)

Protokol stateless untuk komunikasi agen -to- alat.

Server MCP

Layanan yang mengekspos satu atau lebih alat melalui Protokol Konteks Model.

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 selengkapnya, lihat Membangun mekanisme dalam AWS Well-Architected Kerangka Kerja.

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 mesin-ke-mesin (M2M) yang ringan, berdasarkan pola publish/subscribe, 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

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

metadata migrasi

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

pola migrasi

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

Penilaian Portofolio Migrasi (MPA)

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

Penilaian Kesiapan Migrasi (MRA)

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

strategi migrasi

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

ML

Lihat pembelajaran mesin.

modernisasi

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

penilaian kesiapan modernisasi

Evaluasi yang membantu menentukan kesiapan modernisasi aplikasi organisasi; mengidentifikasi manfaat, risiko, dan dependensi; dan menentukan seberapa baik organisasi dapat mendukung keadaan masa depan aplikasi tersebut. Hasil penilaian adalah cetak biru arsitektur target, peta jalan yang merinci fase pengembangan dan tonggak untuk proses modernisasi, dan rencana aksi untuk mengatasi kesenjangan yang diidentifikasi. Untuk informasi lebih lanjut, lihat Mengevaluasi kesiapan modernisasi untuk aplikasi di. AWS Cloud

aplikasi monolitik (monolit)

Aplikasi yang berjalan sebagai layanan tunggal dengan proses yang digabungkan secara ketat. Aplikasi monolitik memiliki beberapa kelemahan. Jika satu fitur aplikasi mengalami lonjakan permintaan, seluruh arsitektur harus diskalakan. Menambahkan atau meningkatkan fitur aplikasi monolitik juga menjadi lebih kompleks ketika basis kode tumbuh. Untuk mengatasi masalah ini, Anda dapat menggunakan arsitektur microservices. Untuk informasi lebih lanjut, lihat Menguraikan 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 mesin-ke-mesin (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 selengkapnya, lihat Ulasan Kesiapan Operasional (ORR) dalam Kerangka Kerja. AWS Well-Architected

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 PUT dan DELETE permintaan ke bucket S3.

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.

penilaian portofolio

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

predikat

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

predikat pushdown

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

kontrol preventif

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

principal

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

privasi berdasarkan desain

Pendekatan rekayasa sistem yang memperhitungkan privasi melalui seluruh proses pengembangan.

zona 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.

rantai cepat

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

pseudonimisasi

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

publish/subscribe (pub/sub)

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

Q

rencana kueri

Serangkaian langkah, seperti instruksi, yang digunakan untuk mengakses data dalam sistem database relasional SQL.

regresi rencana kueri

Ketika pengoptimal layanan database memilih rencana yang kurang optimal daripada sebelum perubahan yang diberikan ke lingkungan database. Hal ini dapat disebabkan oleh perubahan statistik, kendala, pengaturan lingkungan, pengikatan parameter kueri, dan pembaruan ke mesin database.

R

Matriks RACI

Lihat bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan (RACI).

LAP

Lihat Retrieval Augmented Generation.

ransomware

Perangkat lunak berbahaya yang dirancang untuk memblokir akses ke sistem komputer atau data sampai pembayaran dilakukan.

Matriks RASCI

Lihat bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan (RACI).

RCAC

Lihat kontrol akses baris dan kolom.

replika baca

Salinan database yang digunakan untuk tujuan read-only. Anda dapat merutekan kueri ke replika baca untuk mengurangi beban pada database utama Anda.

arsitek ulang

Lihat 7 Rs.

tujuan titik pemulihan (RPO)

Jumlah waktu maksimum yang dapat diterima sejak titik pemulihan data terakhir. Ini menentukan apa yang dianggap sebagai kehilangan data yang dapat diterima antara titik pemulihan terakhir dan gangguan layanan.

tujuan waktu pemulihan (RTO)

Penundaan maksimum yang dapat diterima antara gangguan layanan dan pemulihan layanan.

refactor

Lihat 7 Rs.

Region

Kumpulan AWS sumber daya di wilayah geografis. Masing-masing 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 prinsipal mana yang diizinkan mengakses, tindakan yang didukung, dan kondisi lain yang harus dipenuhi.

matriks yang bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan (RACI)

Matriks yang mendefinisikan peran dan tanggung jawab untuk semua pihak yang terlibat dalam kegiatan migrasi dan operasi cloud. Nama matriks berasal dari jenis tanggung jawab yang

didefinisikan dalam matriks: bertanggung jawab (R), akuntabel (A), dikonsultasikan (C), dan diinformasikan (I). 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.

Retrieval Augmented Generation (RAG)

Teknologi AI generatif di mana LLM mereferensikan sumber data otoritatif yang berada di luar sumber data pelatihannya sebelum menghasilkan respons. Misalnya, model RAG mungkin melakukan pencarian semantik dari basis pengetahuan organisasi atau data kustom. Untuk informasi lebih lanjut, lihat Apa itu RAG.

rotasi

Proses memperbarui rahasia secara berkala untuk membuatnya lebih sulit bagi penyerang untuk mengakses kredensil.

kontrol akses baris dan kolom (RCAC)

Penggunaan ekspresi SQL dasar dan fleksibel yang telah menetapkan aturan akses. RCAC terdiri dari izin baris dan topeng kolom.

RPO

Lihat tujuan titik pemulihan.

RTO

Lihat tujuan waktu pemulihan.

buku runbook

Satu set prosedur manual atau otomatis yang diperlukan untuk melakukan tugas tertentu. Ini biasanya dibangun untuk merampingkan operasi berulang atau prosedur dengan tingkat kesalahan yang tinggi.

D

SAML 2.0

Standar terbuka yang digunakan oleh banyak penyedia identitas (IdPs). Fitur ini memungkinkan sistem masuk tunggal gabungan (SSO), sehingga pengguna dapat masuk ke Konsol Manajemen AWS atau memanggil operasi AWS API tanpa Anda harus membuat pengguna di IAM untuk semua orang di organisasi Anda. Untuk informasi lebih lanjut tentang federasi berbasis SAMP 2.0, lihat Tentang federasi berbasis SAMP 2.0 dalam dokumentasi IAM.

SCADA

Lihat kontrol pengawasan dan akuisisi data.

SCP

Lihat kebijakan kontrol layanan.

Rahasia

Dalam AWS Secrets Manager, informasi rahasia atau terbatas, seperti kata sandi atau kredensil pengguna, yang Anda simpan dalam bentuk terenkripsi. Ini terdiri dari nilai rahasia dan metadata-nya. Nilai rahasia dapat berupa biner, string tunggal, atau beberapa string. Untuk informasi selengkapnya, lihat Apa yang ada di rahasia Secrets Manager? dalam dokumentasi Secrets Manager.

keamanan dengan desain

Pendekatan rekayasa sistem yang memperhitungkan keamanan melalui seluruh proses pengembangan.

kontrol keamanan

Pagar pembatas teknis atau administratif yang mencegah, mendeteksi, atau mengurangi kemampuan pelaku ancaman untuk mengeksploitasi kerentanan keamanan. Ada empat jenis kontrol keamanan utama: preventif, detektif, responsif, dan proaktif.

pengerasan keamanan

Proses mengurangi permukaan serangan untuk membuatnya lebih tahan terhadap serangan. Ini dapat mencakup tindakan seperti menghapus sumber daya yang tidak lagi diperlukan, menerapkan praktik keamanan terbaik untuk memberikan hak istimewa paling sedikit, atau menonaktifkan fitur yang tidak perlu dalam file konfigurasi.

sistem informasi keamanan dan manajemen acara (SIEM)

Alat dan layanan yang menggabungkan sistem manajemen informasi keamanan (SIM) dan manajemen acara keamanan (SEM). Sistem SIEM mengumpulkan, memantau, dan menganalisis data dari server, jaringan, perangkat, dan sumber lain untuk mendeteksi ancaman dan pelanggaran keamanan, dan untuk menghasilkan peringatan.

otomatisasi respons keamanan

Tindakan yang telah ditentukan dan diprogram yang dirancang untuk secara otomatis merespons atau memulihkan peristiwa keamanan. Otomatisasi ini berfungsi sebagai kontrol keamanan detektif atau responsif yang membantu Anda menerapkan praktik terbaik AWS keamanan. Contoh tindakan respons otomatis termasuk memodifikasi grup keamanan VPC, menambal instans Amazon EC2, atau memutar kredensil.

enkripsi sisi server

Enkripsi data di tujuannya, oleh Layanan AWS yang menerimanya.

kebijakan kontrol layanan (SCP)

Kebijakan yang menyediakan kontrol terpusat atas izin untuk semua akun di organisasi. AWS Organizations 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 Layanan AWS. Anda dapat menggunakan endpoint untuk terhubung secara terprogram ke layanan target. Untuk informasi selengkapnya, lihat Layanan AWS titik akhir di Referensi Umum AWS.

perjanjian tingkat layanan (SLA)

Perjanjian yang menjelaskan apa yang dijanjikan tim TI untuk diberikan kepada pelanggan mereka, seperti waktu kerja dan kinerja layanan.

indikator tingkat layanan (SLI)

Pengukuran aspek kinerja layanan, seperti tingkat kesalahan, ketersediaan, atau throughputnya.

tujuan tingkat layanan (SLO)

Metrik target yang mewakili kesehatan layanan, yang diukur dengan indikator tingkat layanan.

model tanggung jawab bersama

Model yang menjelaskan tanggung jawab yang Anda bagikan AWS untuk keamanan dan kepatuhan cloud. AWS bertanggung jawab atas keamanan cloud, sedangkan Anda bertanggung jawab atas keamanan di cloud. Untuk informasi selengkapnya, lihat Model tanggung jawab bersama.

Bayangan AI

Aplikasi AI yang tidak sah dibuat atau digunakan di luar saluran yang diatur dalam suatu organisasi.

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.

model split-and-seed

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 ASP.NET Microsoft (ASMX) lama secara bertahap menggunakan container dan Amazon API Gateway.

subnet

Rentang alamat IP dalam VPC Anda. Subnet harus berada di Availability Zone tunggal.

kontrol pengawasan dan akuisisi data (SCADA)

Di bidang manufaktur, sistem yang menggunakan perangkat keras dan perangkat lunak untuk memantau aset fisik dan operasi produksi.

enkripsi simetris

Algoritma enkripsi yang menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data.

pengujian sintetis

Menguji sistem dengan cara yang mensimulasikan interaksi pengguna untuk mendeteksi potensi masalah atau untuk memantau kinerja. Anda dapat menggunakan Amazon CloudWatch Synthetics untuk membuat tes ini.

sistem prompt

Teknik untuk memberikan konteks, instruksi, atau pedoman ke LLM untuk mengarahkan perilakunya. Permintaan sistem membantu mengatur konteks dan menetapkan aturan untuk interaksi dengan pengguna.

T

tag

Key-value pasangan yang bertindak sebagai metadata untuk mengatur sumber daya Anda AWS . Tag membantu Anda mengelola, mengidentifikasi, mengatur, dan memfilter sumber daya. Untuk informasi selengkapnya, lihat Menandai sumber daya AWS.

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.

alat

Fungsi atau API yang dapat dipanggil agen untuk melakukan operasi di sistem eksternal.

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.

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 AWS Kerangka Kualifikasi Beban Kerja.

tulis sekali, baca banyak (WORM)

Model penyimpanan yang menulis data satu kali dan mencegah data dihapus atau dimodifikasi. Pengguna yang berwenang dapat membaca data sebanyak yang diperlukan, tetapi mereka tidak dapat mengubahnya. Infrastruktur penyimpanan data ini dianggap tidak dapat diubah.

Z

eksploitasi zero-day

Serangan, biasanya malware, yang memanfaatkan kerentanan zero-day.

kerentanan zero-day

Cacat atau kerentanan yang tak tanggung-tanggung dalam sistem produksi. Aktor ancaman dapat menggunakan jenis kerentanan ini untuk menyerang sistem. Pengembang sering menyadari kerentanan sebagai akibat dari serangan tersebut.

bisikan zero-shot

Memberikan LLM dengan instruksi untuk melakukan tugas tetapi tidak ada contoh (tembakan) yang dapat membantu membimbingnya. LLM harus menggunakan pengetahuan pra-terlatih untuk menangani tugas. Efektivitas bidikan nol tergantung pada kompleksitas tugas dan kualitas prompt. Lihat juga beberapa bidikan yang diminta.

aplikasi zombie

Aplikasi yang memiliki CPU rata-rata dan penggunaan memori di bawah 5 persen. Dalam proyek migrasi, adalah umum untuk menghentikan aplikasi ini.

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.