Mencapai kematangan Esential Eight pada AWS

AWS Bimbingan Preskriptif

AWS Bimbingan Preskriptif: Mencapai kematangan Esential Eight pada AWS

Table of Contents

Mencapai kematangan Esential Eight pada AWS: Keamanan dan kepatuhan untuk organisasi Australia

Amazon Web Services (kontributor)

November 2024 (riwayat dokumen)

Direktorat Sinyal Australia (ASD) telah menciptakan dan memprioritaskan strategi untuk membantu organisasi mengurangi risiko ancaman keamanan siber. Delapan dari strategi ini dipilih untuk membentuk kerangka Esential Eight. Banyak organisasi sektor publik dan swasta di Australia diharuskan untuk mencapai kedewasaan di bawah kerangka Essential Eight.

Australian Cyber Security Centre (ACSC) menciptakan kerangka kerja Esential Eight untuk membantu melindungi Microsoftberbasis jaringan internet yang terhubung. Namun, banyak organisasi diharuskan untuk mencapai kematangan Essential Eight untuk semua lingkungan mereka, baik di tempat maupun di cloud.

Kerangka Essential Eight juga mencakup model kematangan yang dirancang untuk membantu organisasi menerapkan kerangka kerja melalui iterasi progresif. Model ini menguraikan tingkat kematangan nol hingga tiga. Tingkat kedewasaan tiga mewakili ketahanan terhadap taktik keamanan siber canggih dan serangan yang sangat bertarget. Panduan ini memberikan panduan spesifik dan berpendirian untuk membantu Anda mencapai kematangan Esential Eight level tiga pada. AWS

Keamanan dan kepatuhan untuk organisasi Australia

Banyak organisasi di Australia menggunakannya AWS Cloud untuk menyimpan data rahasia, memproses transaksi sensitif, dan membangun layanan penting.

Meskipun panduan ini membahas cara mengadaptasi kerangka Essential Eight untuk cloud, AWS juga menyediakan sertifikasi dan model berikut untuk membantu Anda memenuhi persyaratan keamanan dan kepatuhan organisasi Anda:

- Program Asesor Terdaftar Keamanan Informasi
- Kerangka Sertifikasi Hosting
- AWS model tanggung jawab bersama
- AWS Kerangka Well-Architected

Program Asesor Terdaftar Keamanan Informasi

Layanan AWS telah dinilai di bawah Australian Cyber Security Centre (ACSC) Information Security Registered Assesors Program (IRAP) di tingkat PROTECTED. Penilai IRAP bersertifikat Direktorat Sinyal Australia (ASD) independen menyelesaikan penilaian IRAP. AWS Penilaian ini memberikan jaminan bahwa, sehubungan dengan AWS produk dan layanan, kontrol yang berlaku diterapkan untuk beban kerja tingkat PROTECTED.

Paket AWS IRAP PROTECTED tersedia melalui AWS Artifact. Laporan IRAP dikembangkan menggunakan panduan keamanan ACSC Cloud (situs web ACSC). Untuk daftar lengkap Layanan AWS yang ada dalam ruang lingkup, lihat Layanan AWS dalam ruang lingkup: IRAP.

Kerangka Sertifikasi Hosting

Kerangka Sertifikasi Hosting Australia dikembangkan untuk mendukung pengelolaan sistem dan data pemerintah yang aman. Kerangka kerja ini dimaksudkan untuk membantu organisasi mengurangi risiko kepemilikan rantai pasokan dan pusat data. AWS diberikan sertifikasi di tingkat Strategis Bersertifikat. Ini membantu lembaga pemerintah terus berinovasi dengan cepat, mengetahui bahwa AWS memenuhi persyaratan pemerintah.

AWS model tanggung jawab bersama

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. Anda bertanggung jawab untuk mengelola sistem operasi tamu (termasuk pembaruan dan patch keamanan) dan perangkat lunak aplikasi terkait lainnya. Anda juga bertanggung jawab untuk mengonfigurasi firewall grup keamanan yang AWS menyediakan.

Sangat penting bagi Anda untuk memahami model tanggung jawab AWS bersama ketika Anda mendekati kematangan Esential Eight AWS. Tanggung jawab Anda bervariasi tergantung pada layanan yang digunakan, integrasi layanan tersebut ke lingkungan TI Anda, dan hukum dan peraturan yang berlaku.

AWS Kerangka Well-Architected

AWS Well-Architected membantu arsitek cloud membangun infrastruktur yang aman, berkinerja tinggi, tangguh, dan efisien untuk berbagai aplikasi dan beban kerja. The AWS Well-Architected Framework menyediakan praktik terbaik arsitektur yang membantu Anda merancang, membangun, dan mengoperasikan sistem. AWS Kerangka kerja ini dibangun di sekitar enam pilar: keunggulan operasional, keamanan, keandalan, efisiensi kinerja, optimalisasi biaya, dan keberlanjutan.

AWS juga menyediakan layanan untuk meninjau beban kerja Anda. AWS Well-Architected ToolIni membantu Anda meninjau dan menilai arsitektur Anda dengan menggunakan AWS Well-Architected Framework. Ini memberikan rekomendasi untuk membuat beban kerja Anda lebih andal, aman, efisien, dan hemat biaya.

Menafsirkan kembali strategi Esential Eight untuk cloud

Berikut ini adalah strategi mitigasi Essential Eight asli yang dirancang untuk Microsoftjaringan yang terhubung internet berbasis:

- Kontrol aplikasi
- Aplikasi tambalan
- Konfigurasi Microsoft Office pengaturan makro
- Pengerasan aplikasi pengguna
- Batasi hak administratif
- Sistem operasi patch
- Autentikasi multi-faktor
- Pencadangan reguler

Penting untuk ditegaskan kembali bahwa kerangka Essential Eight tidak dirancang untuk lingkungan cloud. Namun, prinsip-prinsip yang mendasarinya berlaku, dan ada tumpang tindih antara strategi Esential Eight dan praktik terbaik AWS Well-Architected Framework.

Berbagai pendekatan cloud-native dapat meningkatkan keamanan dan secara dramatis mengurangi beban kepatuhan Anda. Di lingkungan lokal, Anda bertanggung jawab atas semua aspek keamanan, dan tidak ada kontrol yang diwariskan. Saat menjalankan beban kerja di cloud, AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan layanan kami. Anda juga dapat mengurangi beban kepatuhan Anda dengan menggunakan otomatisasi dan layanan terkelola. Layanan terkelola, juga dikenal sebagai layanan abstrak, yang Layanan AWS 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. Untuk informasi lebih lanjut, lihat Tema 1: Gunakan layanan terkelola bagian dalam panduan ini.

Oleh karena itu, beberapa reinterpretasi diperlukan untuk membuat strategi Esential Eight sesuai untuk beban kerja. AWS Panduan ini mengubah strategi Esential Eight menjadi AWS tema.

Menggunakan tema

Panduan ini dibagi menjadi delapan tema. Setiap strategi Essential Eight dipetakan ke satu atau lebih tema berikut, dan setiap tema dipetakan ke satu atau lebih praktik terbaik dalam Kerangka Well-Architected AWS :

- Tema 1: Gunakan layanan terkelola
- Tema 2: Mengelola infrastruktur yang tidak dapat diubah melalui jaringan pipa yang aman
- Tema 3: Kelola infrastruktur yang bisa berubah dengan otomatisasi
- Tema 4: Mengelola identitas
- Tema 5: Menetapkan perimeter data
- Tema 6: Mengotomatiskan cadangan
- Tema 7: Memusatkan logging dan monitoring
- Tema 8: Menerapkan mekanisme untuk proses manual

Setiap tema mencakup ikhtisar topik, praktik terbaik Kerangka Kerja AWS Well-Architected terkait, dan instruksi tentang cara mencapai kematangan Esential Eight dan memantau kepatuhan. Instruksi memberikan langkah-langkah manual atau membantu Anda mengonfigurasi otomatisasi dengan menggunakan AWS Config aturan. Langkah-langkah manual memerlukan mekanisme untuk memastikan bahwa temuan ditangani. Untuk informasi lebih lanjut, lihatTema 8: Menerapkan mekanisme untuk proses manual. AWS Config aturan memerlukan pengawasan atau otomatisasi serupa untuk memulihkan sumber daya yang tidak patuh. Dengan mengikuti panduan yang selaras dengan tema-tema ini, Anda dapat mencapai kematangan Esential Eight dengan pendekatan yang juga memaksimalkan manfaat cloud.

Menafsirkan kembali strategi Esential Eight untuk cloud

Karena kerangka Essential Eight tidak dirancang untuk lingkungan cloud, penting untuk mengambil pendekatan cloud-native saat menangani prinsip-prinsip dasar dari setiap strategi Essential Eight. Pendekatannya bervariasi tergantung pada dua pertanyaan kunci.

Layanan apa yang Anda gunakan?

AWS model tanggung jawab bersamaDapat membantu meringankan kepatuhan dan beban operasional Anda. Layanan terkelola mengalihkan lebih banyak tanggung jawab AWS untuk menjaga

ketersediaan, kinerja, dan pengoptimalan keamanan layanan yang diterapkan. Layanan yang dikelola juga menghilangkan beban operasional dan administrasi dalam mempertahankan layanan, memberikan lebih banyak waktu untuk fokus pada inovasi.

Layanan terkelola mencakup layanan tanpa server, seperti Amazon API Gateway AWS Lambda, dan DynamoDB. Database di Amazon Relational Database Service (Amazon RDS) memerlukan tanggung jawab operasional yang lebih sedikit daripada database di Amazon Elastic Compute Cloud (Amazon). EC2

Misalnya, jika Anda mengadaptasi strategi sistem operasi Patch Essential Eight untuk cloud, Anda perlu mempertimbangkan layanan mana yang Anda gunakan dan apakah Anda bertanggung jawab untuk menambal sumber daya tersebut. AWS bertanggung jawab untuk menambal layanan yang dikelola sepenuhnya, seperti Lambda dan DynamoDB. Untuk layanan lain, seperti Amazon RDS atau Amazon Redshift, Anda mungkin perlu mengelola tambalan selama jendela pemeliharaan.

Model penerapan apa yang Anda gunakan?

Apakah organisasi Anda menggunakan pendekatan infrastruktur yang dapat berubah atau tidak dapat diubah?

Model infrastruktur yang dapat berubah memperbarui dan memodifikasi infrastruktur yang ada untuk beban kerja produksi. Ini adalah metode penerapan standar sebelum cloud, ketika mengganti infrastruktur server sangat mahal dan memakan waktu sehingga pendekatan yang paling praktis adalah menerapkan perubahan pada server yang sudah dalam produksi. Contoh pendekatan yang bisa berubah di cloud adalah menyebarkan perubahan aplikasi secara langsung ke EC2 instance yang berjalan, baik secara manual atau dengan menggunakan layanan penyebaran perangkat lunak, seperti AWS Systems Manager Run Command atau. AWS CodeDeploy

Model infrastruktur yang tidak dapat diubah menyebarkan infrastruktur baru untuk beban kerja produksi alih-alih memperbarui, menambal, atau memodifikasi infrastruktur yang ada. Contoh pendekatan yang tidak dapat diubah adalah mendefinisikan tumpukan aplikasi di atau. AWS CloudFormationAWS Cloud Development Kit (AWS CDK) Anda dapat menggunakan layanan ini untuk menyebarkan tumpukan aplikasi melalui pipeline continuous integration dan continuous delivery (CI/CD). Pendekatan ini menggunakan metode penerapan seperti rolling atau biru/hijau. Untuk informasi lebih lanjut tentang pendekatan ini, lihat praktik terbaik Deploy using immutable infrastructure in the AWS Well-Architected Framework.

Misalnya, jika Anda mengadaptasi strategi sistem operasi Patch Essential Eight untuk cloud, Anda perlu mempertimbangkan bagaimana patching berlaku untuk model penerapan. Untuk infrastruktur

yang dapat berubah, Anda dapat menambal sumber daya secara manual atau dapat meningkatkan efisiensi operasional melalui otomatisasi. Jika Anda menggunakan infrastruktur yang tidak dapat diubah, maka Anda akan menggunakan pipa CI/CD untuk menyebarkan infrastruktur baru dengan versi terbaru dari sistem operasi. Bahkan, istilah patching adalah keliru di bawah model ini karena infrastruktur akan diganti daripada ditambal.

Tema 1: Gunakan layanan terkelola

Esensi Delapan strategi tercakup

Patch aplikasi, batasi hak administratif, patch sistem operasi

Layanan terkelola membantu Anda mengurangi kewajiban kepatuhan dengan mengizinkan AWS untuk mengelola beberapa tugas keamanan, seperti patching dan manajemen kerentanan.

Seperti yang dibahas di AWS model tanggung jawab bersama bagian ini, Anda berbagi tanggung jawab AWS untuk keamanan dan kepatuhan cloud. Hal ini dapat mengurangi beban operasional Anda karena AWS mengoperasikan, mengelola, dan mengendalikan komponen, dari sistem operasi host dan lapisan virtualisasi hingga keamanan fisik fasilitas di mana layanan beroperasi.

Tanggung jawab Anda mungkin termasuk mengelola jendela pemeliharaan untuk layanan terkelola, seperti Amazon Relational Database Service (Amazon RDS) atau Amazon Redshift, dan memindai kerentanan AWS Lambda dalam gambar kode atau kontainer. Seperti semua tema dalam panduan ini, Anda juga bertanggung jawab untuk pemantauan dan pelaporan kepatuhan. Anda dapat menggunakan Amazon Inspector untuk melaporkan kerentanan di semua kerentanan Anda. Akun AWS Anda dapat menggunakan aturan AWS Config untuk memastikan bahwa layanan, seperti Amazon RDS dan Amazon Redshift, mengaktifkan pembaruan kecil dan jendela pemeliharaan.

Misalnya, jika Anda menjalankan EC2 instans Amazon, tanggung jawab Anda meliputi yang berikut:

- Kontrol aplikasi
- Aplikasi penambalan
- Membatasi hak administratif untuk bidang EC2 kontrol Amazon dan sistem operasi (OS)
- Menambal OS
- Menegakkan otentikasi multi-faktor (MFA) untuk mengakses bidang kontrol dan AWS OS
- Mencadangkan data dan konfigurasi

Sedangkan jika Anda menjalankan fungsi Lambda, maka tanggung jawab Anda berkurang dan termasuk yang berikut:

- Kontrol aplikasi

- Mengkonfirmasikan bahwa perpustakaan adalah up-to-date
- Membatasi hak administratif untuk pesawat kontrol Lambda
- Menegakkan MFA untuk mengakses pesawat kontrol AWS
- Mencadangkan kode fungsi dan konfigurasi Lambda

Praktik terbaik terkait dalam Kerangka AWS Well-Architected

- SEC01-BP05 Mengurangi ruang lingkup manajemen keamanan

Menerapkan tema ini

Aktifkan penambalan

- Terapkan pembaruan Amazon RDS
- Aktifkan pembaruan terkelola di AWS Elastic Beanstalk
- Waspadai jendela pemeliharaan cluster Amazon Redshift

Pindai kerentanan

- Pindai gambar wadah Amazon Elastic Container Registry (Amazon ECR) dengan Amazon Inspector
- Pindai fungsi Lambda dengan Amazon Inspector

Memantau tema ini

Melaksanakan pemeriksaan tata kelola

- Aktifkan Praktik Terbaik Operasional untuk paket kesesuaian ACSC Essential 8 di AWS Config

Pantau Amazon Inspector

- Menilai cakupan tingkat akun
- Kelola beberapa akun

Menerapkan AWS Config aturan berikut

- RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED
- REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK
- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK
- EKS_CLUSTER_SUPPORTED_VERSION

Tema 2: Mengelola infrastruktur yang tidak dapat diubah melalui jaringan pipa yang aman

Esensi Delapan strategi tercakup

Kontrol aplikasi, aplikasi patch, sistem operasi patch

Untuk infrastruktur yang tidak dapat diubah, Anda harus mengamankan pipeline penyebaran untuk perubahan sistem. AWS Insinyur Terhormat, Colm MacCárthaigh, menjelaskan prinsip ini dalam Operasi Tanpa Hak Istimewa: Menjalankan Layanan Tanpa Akses ke Data (YouTube video) presentasi pada konferensi AWS re:Invent 2022.

Dengan membatasi akses langsung untuk mengonfigurasi AWS sumber daya, Anda dapat meminta agar semua sumber daya disebarkan atau diubah melalui jalur pipa yang disetujui, aman, dan otomatis. Biasanya, Anda membuat kebijakan AWS Identity and Access Management (IAM) yang memungkinkan pengguna mengakses hanya akun yang menghosting pipeline penerapan. Anda juga mengonfigurasi kebijakan IAM yang memungkinkan akses break-glass untuk sejumlah pengguna terbatas. Untuk mencegah perubahan manual, Anda dapat menggunakan grup keamanan untuk memblokir SSH dan Windows akses protokol desktop jarak jauh (RDP) ke server. Session Manager, kemampuan AWS Systems Manager, dapat menyediakan akses ke instance tanpa perlu membuka port masuk atau memelihara host bastion.

Amazon Machine Images (AMIs) dan gambar kontainer harus dibuat dengan aman dan berulang. Untuk EC2 instans Amazon, Anda dapat menggunakan EC2 Image Builder untuk membangun AMIs yang memiliki fitur keamanan bawaan, seperti penemuan instance, kontrol aplikasi, dan pencatatan. Untuk informasi selengkapnya tentang kontrol aplikasi, lihat Menerapkan Kontrol Aplikasi di situs web ACSC. Anda juga dapat menggunakan Image Builder untuk membuat gambar kontainer, dan Anda dapat menggunakan Amazon Elastic Container Registry (Amazon ECR) Registry (Amazon ECR) untuk berbagi gambar tersebut di seluruh akun. Tim keamanan pusat dapat menyetujui proses otomatis untuk membuat gambar ini AMIs dan kontainer sehingga AMI atau gambar kontainer yang dihasilkan disetujui untuk digunakan oleh tim aplikasi.

Aplikasi harus didefinisikan dalam infrastruktur sebagai kode (IAc), dengan menggunakan layanan seperti AWS CloudFormationatau AWS Cloud Development Kit (AWS CDK). Alat analisis kode, seperti, cfn-nag AWS CloudFormation Guard, atau cdk-nag, dapat secara otomatis menguji kode terhadap praktik terbaik keamanan di pipeline Anda yang disetujui.

Seperti halnyaTema 1: Gunakan layanan terkelola, Amazon Inspector dapat melaporkan kerentanan di seluruh Anda. Akun AWS Tim cloud dan keamanan terpusat dapat menggunakan informasi ini untuk memverifikasi bahwa tim aplikasi memenuhi persyaratan keamanan dan kepatuhan.

Untuk memantau dan melaporkan kepatuhan, lakukan tinjauan berkelanjutan terhadap sumber daya dan log IAM. Gunakan AWS Config aturan untuk memastikan bahwa hanya disetujui yang AMIs digunakan, dan pastikan Amazon Inspector dikonfigurasi untuk memindai sumber daya Amazon ECR dari kerentanan.

Praktik terbaik terkait dalam Kerangka AWS Well-Architected

- OPS05-BP04 Menggunakan sistem manajemen build dan deployment
- REL08-BP04 Melakukan deployment dengan menggunakan infrastruktur yang tidak bisa diubah
- SEC06-BP03 Kurangi manajemen manual dan akses interaktif

Menerapkan tema ini

Menerapkan AMI dan pipeline pembuatan kontainer

- Gunakan EC2 Image Builder dan buat yang berikut ini ke dalam AMIs:
  - AWS Systems Manager Agen (SSM Agent), yang digunakan misalnya penemuan dan manajemen
  - Alat keamanan untuk kontrol aplikasi, seperti Security Enhanced Linux (SELinux) (GitHub), Daemon Kebijakan Akses File (fapolicyd) (), atau OpenSCAP GitHub
  - Amazon CloudWatch Agent, yang digunakan untuk logging
- Untuk semua EC2 instance, sertakan `AmazonSSMManagedInstanceCore` kebijakan `CloudWatchAgentServerPolicy` dan dalam profil instans atau peran IAM yang digunakan Systems Manager untuk mengakses instans Anda
- Berbagi AMIs dengan seluruh organisasi
- Bagikan sumber daya EC2 Image Builder
- Pastikan bahwa tim aplikasi mereferensikan yang terbaru AMIs
- Gunakan pipeline AMI Anda untuk manajemen tambalan
- Menerapkan pipa pembuatan kontainer:

  - Buat pipeline gambar kontainer menggunakan wizard konsol EC2 Image Builder
  - Buat pipeline pengiriman berkelanjutan untuk gambar kontainer Anda dengan menggunakan Amazon ECR sebagai sumber (posting AWS blog)
- Bagikan gambar kontainer ECR di seluruh organisasi Anda melalui arsitektur multi-akun dan Multi-wilayah

Menerapkan pipeline build aplikasi yang aman

- Menerapkan pipeline build untuk IAc, seperti dengan menggunakan EC2 Image Builder dan AWS CodePipeline (AWS posting blog)
- Gunakan alat analisis kode, seperti AWS CloudFormation Guard, cfn-nag (GitHub), atau cdk-nag (GitHub), dalam saluran CI/CD untuk membantu mendeteksi pelanggaran praktik terbaik, seperti:
  - Kebijakan IAM yang terlalu permisif, seperti yang menggunakan wildcard
  - Aturan grup keamanan yang terlalu permisif, seperti yang menggunakan wildcard atau mengizinkan akses SSH
  - Akses log yang tidak diaktifkan
  - Enkripsi yang tidak diaktifkan
  - Literal kata sandi
- Menerapkan alat pemindaian di saluran pipa (posting AWS blog)
- Gunakan AWS Identity and Access Management Access Analyzer dalam pipeline (posting AWS blog) untuk memvalidasi kebijakan IAM yang didefinisikan dalam template CloudFormation
- Konfigurasikan kebijakan IAM dan kebijakan kontrol layanan untuk akses dengan hak istimewa paling sedikit untuk menggunakan pipeline atau melakukan modifikasi apa pun

Menerapkan pemindaian kerentanan

- Aktifkan Amazon Inspector di semua akun di organisasi Anda
- Gunakan Amazon Inspector untuk memindai AMIs di pipeline build AMI Anda:
  - Mengelola siklus hidup AMIs di EC2 Image Builder () GitHub
- Konfigurasikan pemindaian yang disempurnakan untuk repositori Amazon ECR dengan menggunakan Amazon Inspector
- Membangun program manajemen kerentanan untuk melakukan triase dan memulihkan temuan keamanan

Memantau tema ini

Memantau IAM dan log secara berkelanjutan

- Tinjau kebijakan IAM Anda secara berkala untuk memastikan bahwa:
  - Hanya pipeline penyebaran yang memiliki akses langsung ke sumber daya
  - Hanya layanan yang disetujui yang memiliki akses langsung ke data
  - Pengguna tidak memiliki akses langsung ke sumber daya atau data
- Pantau AWS CloudTrail log untuk mengonfirmasi bahwa pengguna memodifikasi sumber daya melalui saluran pipa dan tidak secara langsung memodifikasi sumber daya atau mengakses data
- Tinjau secara berkala temuan IAM Access Analyzer
- Siapkan peringatan untuk memberi tahu Anda jika kredensi pengguna root untuk sebuah digunakan Akun AWS

Menerapkan AWS Config aturan berikut

- `APPROVED_AMIS_BY_ID`
- `APPROVED_AMIS_BY_TAG`
- `ECR_PRIVATE_IMAGE_SCANNING_ENABLED`

Tema 3: Kelola infrastruktur yang bisa berubah dengan otomatisasi

Esensi Delapan strategi tercakup

Kontrol aplikasi, aplikasi patch, sistem operasi patch

Mirip dengan infrastruktur yang tidak dapat diubah, Anda mengelola infrastruktur yang dapat berubah sebagai IAc, dan Anda memodifikasi atau memperbarui infrastruktur ini melalui proses otomatis. Banyak langkah implementasi untuk infrastruktur yang tidak dapat diubah juga berlaku untuk infrastruktur yang dapat berubah. Namun, untuk infrastruktur yang dapat berubah, Anda juga harus menerapkan kontrol manual untuk memastikan bahwa beban kerja yang dimodifikasi tetap mengikuti praktik terbaik.

Untuk infrastruktur yang bisa berubah, Anda dapat mengotomatiskan manajemen tambalan dengan menggunakan Patch Manager, kemampuan. AWS Systems Manager Aktifkan Patch Manager di semua akun di AWS organisasi Anda.

Mencegah akses SSH dan RDP langsung dan mengharuskan pengguna untuk menggunakan Session Manager atau Run Command, yang juga merupakan kemampuan Systems Manager. Tidak seperti SSH dan RDP, kemampuan ini dapat mencatat akses dan perubahan sistem.

Untuk memantau dan melaporkan kepatuhan, Anda harus melakukan tinjauan kepatuhan patch yang sedang berlangsung. Anda dapat menggunakan AWS Config aturan untuk memastikan bahwa semua EC2 instans Amazon dikelola oleh Systems Manager, memiliki izin yang diperlukan dan aplikasi yang diinstal, serta dalam kepatuhan patch.

Praktik terbaik terkait dalam Kerangka AWS Well-Architected

- SEC06-BP03 Kurangi manajemen manual dan akses interaktif
- SEC06-BP05 Mengotomatiskan perlindungan komputasi

Menerapkan tema ini

Otomatiskan penambalan

- Terapkan langkah-langkah di Aktifkan Patch Manager di semua akun di AWS organisasi Anda
- Untuk semua EC2 instance, sertakan `CloudWatchAgentServerPolicy` dan `AmazonSSMManagedInstanceCore` dalam profil instans atau peran IAM yang digunakan Systems Manager untuk mengakses instans Anda

Gunakan otomatisasi daripada proses manual

- Menerapkan panduan dalam Implementasikan AMI dan pipeline build container di Tema 2: Mengelola infrastruktur yang tidak dapat diubah melalui jaringan pipa yang aman
- Gunakan Session Manager atau Run Command alih-alih akses SSH atau RDP langsung

Gunakan otomatisasi untuk menginstal yang berikut ini pada EC2 instance

- AWS Systems Manager Agen (SSM Agent), yang digunakan misalnya penemuan dan manajemen
- Alat keamanan untuk kontrol aplikasi, seperti Security Enhanced Linux (SELinux) (GitHub), Daemon Kebijakan Akses File (fapolicyd) (), atau OpenSCAP GitHub
- Amazon CloudWatch Agent, yang digunakan untuk logging

Gunakan peer review sebelum rilis apa pun untuk memastikan bahwa perubahan memenuhi praktik terbaik

- Kebijakan IAM yang terlalu permisif, seperti yang menggunakan wildcard
- Aturan grup keamanan yang terlalu permisif, seperti yang menggunakan wildcard atau mengizinkan akses SSH
- Akses log yang tidak diaktifkan
- Enkripsi yang tidak diaktifkan
- Literal kata sandi
- Kebijakan IAM yang aman

Gunakan kontrol tingkat identitas

- Untuk mengharuskan pengguna memodifikasi sumber daya melalui proses otomatis dan mencegah konfigurasi manual, izinkan izin hanya-baca untuk peran yang dapat diasumsikan pengguna
- Berikan izin untuk mengubah sumber daya hanya untuk peran layanan, seperti peran yang digunakan oleh Systems Manager

Menerapkan pemindaian kerentanan

- Menerapkan panduan dalam Menerapkan pemindaian kerentanan di Tema 2: Mengelola infrastruktur yang tidak dapat diubah melalui jaringan pipa yang aman
- Pindai EC2 instans Anda dengan menggunakan Amazon Inspector

Memantau tema ini

Memantau kepatuhan patch secara berkelanjutan

- Laporkan kepatuhan patch dengan menggunakan otomatisasi dan dasbor
- Menerapkan mekanisme untuk meninjau dasbor untuk kepatuhan tambalan

Memantau IAM dan log secara berkelanjutan

- Tinjau kebijakan IAM Anda secara berkala untuk memastikan bahwa:
  - Hanya pipeline penyebaran yang memiliki akses langsung ke sumber daya
  - Hanya layanan yang disetujui yang memiliki akses langsung ke data
  - Pengguna tidak memiliki akses langsung ke sumber daya atau data
- Pantau AWS CloudTrail log untuk memastikan bahwa pengguna memodifikasi sumber daya melalui saluran pipa dan tidak secara langsung memodifikasi sumber daya atau mengakses data
- Tinjau AWS Identity and Access Management Access Analyzer temuan secara berkala
- Siapkan peringatan untuk memberi tahu Anda jika kredensi pengguna root untuk sebuah digunakan Akun AWS

Menerapkan AWS Config aturan berikut

- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK
- EC2_INSTANCE_MANAGED_BY_SSM
- EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED - SELinux/fapolicyd/OpenSCAP, CW Agent
- EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED - any unsupported apps
- IAM_ROLE_MANAGED_POLICY_CHECK - CW Logs, SSM
- EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK
- REQUIRED_TAGS
- RESTRICTED_INCOMING_TRAFFIC - 22, 3389

Tema 4: Mengelola identitas

Esensi Delapan strategi tercakup

Batasi hak administratif, otentikasi multi-faktor

Manajemen identitas dan izin yang kuat adalah aspek penting dalam mengelola keamanan di cloud. Praktik identitas yang kuat menyeimbangkan akses yang diperlukan dan hak istimewa yang paling sedikit. Ini membantu tim pengembangan bergerak cepat tanpa mengorbankan keamanan.

Gunakan federasi identitas untuk memusatkan manajemen identitas. Ini membuatnya lebih mudah untuk mengelola akses di beberapa aplikasi dan layanan karena Anda mengelola akses dari satu lokasi. Ini juga membantu Anda menerapkan izin sementara dan otentikasi multi-faktor (MFA).

Berikan pengguna hanya izin yang mereka perlukan untuk melakukan tugas mereka. AWS Identity and Access Management Access Analyzer dapat memvalidasi kebijakan dan memverifikasi akses publik dan lintas akun. Fitur seperti kebijakan kontrol AWS Organizations layanan (SCPs), kondisi kebijakan IAM, batas izin IAM, dan set AWS IAM Identity Center izin dapat membantu Anda mengonfigurasi kontrol akses berbutir halus (FGAC).

Saat melakukan jenis otentikasi apa pun, yang terbaik adalah menggunakan kredensil sementara untuk mengurangi atau menghilangkan risiko — seperti kredensil yang secara tidak sengaja diungkapkan, dibagikan, atau dicuri. Gunakan peran IAM alih-alih pengguna IAM.

Gunakan mekanisme masuk yang kuat, seperti MFA, untuk mengurangi risiko di mana kredensi masuk telah diungkapkan secara tidak sengaja atau mudah ditebak. Memerlukan MFA untuk pengguna root, dan Anda juga dapat memerlukannya di tingkat federasi. Jika penggunaan pengguna IAM tidak dapat dihindari, terapkan MFA.

Untuk memantau dan melaporkan kepatuhan, Anda harus terus bekerja untuk mengurangi izin, memantau temuan dari IAM Access Analyzer, dan menghapus sumber daya IAM yang tidak digunakan. Gunakan AWS Config aturan untuk memastikan bahwa mekanisme masuk yang kuat ditegakkan, kredensialnya berumur pendek, dan sumber daya IAM sedang digunakan.

Praktik terbaik terkait dalam Kerangka AWS Well-Architected

- SEC02-BP01 Gunakan mekanisme masuk yang kuat

- SEC02-BP02 Menggunakan kredensial sementara
- SEC02-BP03 Menyimpan dan menggunakan rahasia secara aman
- SEC02-BP04 Mengandalkan penyedia identitas tersentralisasi
- SEC02-BP05 Melakukan audit dan rotasi kredensial secara berkala
- SEC02-BP06 Manfaatkan grup dan atribut pengguna
- SEC03-BP01 Menetapkan persyaratan akses
- SEC03-BP02 Memberikan hak akses paling rendah
- SEC03-BP03 Menetapkan proses akses darurat
- SEC03-BP04 Mengurangi izin secara terus-menerus
- SEC03-BP05 Tentukan pagar pembatas izin untuk organisasi Anda
- SEC03-BP06 Mengelola akses berdasarkan siklus hidup
- SEC03-BP07 Menganalisis akses publik dan lintas akun
- SEC03-BP08 Membagikan sumber daya secara aman dalam organisasi Anda

Menerapkan tema ini

Melaksanakan federasi identitas

- Mewajibkan pengguna manusia untuk berfederasi dengan penyedia identitas untuk mengakses AWS dengan menggunakan kredensi sementara
- Menerapkan akses sementara yang ditinggikan ke AWS lingkungan Anda

Terapkan izin hak istimewa paling sedikit

- Lindungi kredensil pengguna root Anda dan jangan menggunakannya untuk tugas sehari-hari
- Gunakan IAM Access Analyzer untuk menghasilkan kebijakan hak istimewa paling sedikit berdasarkan aktivitas akses
- Verifikasi akses publik dan lintas akun ke sumber daya dengan IAM Access Analyzer
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk izin yang aman dan fungsional
- Menetapkan pagar pembatas izin di beberapa akun

- Gunakan batas izin untuk menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas
- Gunakan ketentuan dalam kebijakan IAM untuk membatasi akses lebih lanjut
- Secara teratur meninjau dan menghapus pengguna, peran, izin, kebijakan, dan kredensil yang tidak digunakan
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit
- Gunakan fitur set izin di IAM Identity Center

Putar kredensil

- Memerlukan beban kerja untuk menggunakan peran IAM untuk mengakses AWS
- Mengotomatiskan penghapusan peran IAM yang tidak digunakan
- Putar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensil jangka panjang

Menegakkan MFA

- Memerlukan MFA untuk pengguna root
- Memerlukan MFA melalui IAM Identity Center
- Pertimbangkan untuk mewajibkan MFA untuk melakukan tindakan API khusus layanan

Memantau tema ini

Pantau akses hak istimewa paling sedikit

- Kirim temuan IAM Access Analyzer ke AWS Security Hub
- Pertimbangkan untuk menyiapkan pemberitahuan untuk temuan Pusat Identitas IAM yang kritis
- Secara teratur meninjau laporan kredensi untuk Anda Akun AWS

Menerapkan AWS Config aturan berikut

- `ACCESS_KEYS_ROTATED`
- `IAM_ROOT_ACCESS_KEY_CHECK`

- IAM_USER_MFA_ENABLED
- IAM_USER_UNUSED_CREDENTIALS_CHECK
- IAM_PASSWORD_POLICY
- ROOT_ACCOUNT_HARDWARE_MFA_ENABLED

Tema 5: Menetapkan perimeter data

Esensi Delapan strategi tercakup

Batasi hak administratif

Perimeter data adalah seperangkat pagar pembatas pencegahan di AWS lingkungan Anda yang membantu memastikan bahwa hanya identitas tepercaya yang mengakses sumber daya tepercaya dari jaringan yang diharapkan. Pagar pembatas ini berfungsi sebagai batas yang selalu aktif yang membantu melindungi data Anda di seluruh rangkaian dan sumber daya yang luas. Akun AWS Pagar pembatas di seluruh organisasi ini tidak menggantikan kontrol akses berbutir halus yang ada. Sebaliknya, mereka membantu meningkatkan strategi keamanan Anda dengan memastikan bahwa semua pengguna, peran, dan sumber daya AWS Identity and Access Management (IAM) mematuhi seperangkat standar keamanan yang ditetapkan.

Anda dapat membuat perimeter data dengan menggunakan kebijakan yang mencegah akses dari luar batas organisasi, yang biasanya dibuat. AWS Organizations Tiga kondisi otorisasi perimeter utama yang digunakan untuk membuat perimeter data adalah:

- Identitas tepercaya — Kepala Sekolah (peran atau pengguna IAM) dalam diri Anda Akun AWS, atau Layanan AWS bertindak atas nama Anda.
- Sumber daya tepercaya — Sumber daya yang ada di Anda Akun AWS atau dikelola dengan Layanan AWS bertindak atas nama Anda.
- Jaringan yang diharapkan — Pusat data lokal Anda dan awan pribadi virtual (VPCs), atau jaringan yang Layanan AWS bertindak atas nama Anda.

Pertimbangkan untuk menerapkan batas data antara lingkungan dengan klasifikasi data yang berbeda, seperti `OFFICIAL:SENSITIVE` atau`PROTECTED`, atau tingkat risiko yang berbeda, seperti pengembangan, pengujian, atau produksi. Untuk informasi selengkapnya, lihat Membangun perimeter data pada AWS (AWS whitepaper) dan Membuat perimeter data pada AWS: Ikhtisar (posting AWS blog).

Praktik terbaik terkait dalam Kerangka AWS Well-Architected

- SEC03-BP05 Tentukan pagar pembatas izin untuk organisasi Anda

- SEC07-BP02 Menerapkan kontrol perlindungan data berdasarkan sensitivitas data

Menerapkan tema ini

Menerapkan kontrol identitas

- Izinkan hanya identitas tepercaya untuk mengakses sumber daya Anda — Gunakan kebijakan berbasis sumber daya dengan kunci kondisi dan. `aws:PrincipalOrgID` `aws:PrincipalIsAWSService` Ini hanya memungkinkan prinsipal dari AWS organisasi Anda dan dari AWS untuk mengakses sumber daya Anda.
- Izinkan identitas tepercaya hanya dari jaringan Anda — Gunakan kebijakan titik akhir VPC dengan kunci kondisi dan. `aws:PrincipalOrgID` `aws:PrincipalIsAWSService` Ini hanya memungkinkan prinsipal dari AWS organisasi Anda dan dari AWS untuk mengakses layanan melalui titik akhir VPC.

Menerapkan kontrol sumber daya

- Izinkan identitas Anda hanya mengakses sumber daya tepercaya — Gunakan kebijakan kontrol layanan (SCPs) dengan kunci `aws:ResourceOrgID` kondisi. Ini memungkinkan identitas Anda hanya mengakses sumber daya di AWS organisasi Anda.
- Izinkan akses ke sumber daya tepercaya hanya dari jaringan Anda — Gunakan kebijakan titik akhir VPC dengan kunci kondisi. `aws:ResourceOrgID` Ini memungkinkan identitas Anda untuk mengakses layanan hanya melalui titik akhir VPC yang merupakan bagian dari organisasi Anda. AWS

Menerapkan kontrol jaringan

- Izinkan identitas mengakses sumber daya hanya dari jaringan yang diharapkan — Gunakan SCPs dengan tombol kondisi`aws:SourceIp`,, `aws:SourceVpc``aws:SourceVpce`, dan`aws:ViaAWSService`. Ini memungkinkan identitas Anda untuk mengakses sumber daya hanya dari alamat IP yang diharapkan, VPCs, dan titik akhir VPC, dan melalui. Layanan AWS
- Izinkan akses ke sumber daya Anda hanya dari jaringan yang diharapkan — Gunakan kebijakan berbasis sumber daya dengan kunci kondisi`aws:SourceIp`,,,`aws:SourceVpc`, `aws:SourceVpce` dan. `aws:ViaAWSService` `aws:PrincipalIsAWSService` Ini memungkinkan akses ke sumber daya Anda hanya dari yang diharapkan IPs, dari yang diharapkan

VPCs, dari titik akhir VPC yang diharapkan, melalui Layanan AWS, atau ketika identitas panggilan adalah file. Layanan AWS

Memantau tema ini

Pantau kebijakan

- Menerapkan mekanisme untuk meninjau SCPs, kebijakan IAM, dan kebijakan titik akhir VPC

Menerapkan AWS Config aturan berikut

- `SERVICE_VPC_ENDPOINT_ENABLED`

Tema 6: Mengotomatiskan cadangan

Esensi Delapan strategi tercakup

Pencadangan reguler

“Kegagalan diberikan dan semuanya pada akhirnya akan gagal seiring waktu: dari router ke hard disk, dari sistem operasi ke unit memori yang merusak paket TCP, dari kesalahan sementara hingga kegagalan permanen. Ini diberikan, apakah Anda menggunakan perangkat keras berkualitas tinggi atau komponen dengan biaya terendah.” —Werner Vogels, CTO, Amazon, Semua Hal Didistribusikan

Pencadangan dan pemulihan data adalah bagian penting dari keandalan suatu sistem. AWS dirancang untuk membuatnya lebih mudah untuk membuat cadangan, menjaga daya tahan data yang dicadangkan, dan memastikan bahwa data yang dicadangkan tetap dapat dipulihkan.

AWS Backupadalah layanan yang dikelola sepenuhnya yang memusatkan dan mengotomatiskan pencadangan data di seluruh. Layanan AWS Ini mendukung beberapa jenis AWS sumber daya dan membantu Anda menerapkan dan memelihara strategi cadangan untuk beban kerja yang menggunakan banyak AWS sumber daya yang harus dicadangkan secara kolektif. AWS Backup juga membantu Anda untuk secara kolektif memantau operasi pencadangan dan pemulihan beberapa sumber AWS daya.

AWS Backup Vault Lock adalah fitur opsional dari brankas cadangan, dan dapat memberikan keamanan dan kontrol tambahan. Ketika kunci aktif dalam mode Kepatuhan dan waktu tenggang berakhir, konfigurasi vault tidak dapat diubah atau dihapus oleh pengguna, akun atau pemilik data, atau. AWS Setiap lemari besi dapat memiliki satu kunci brankas di tempatnya. Ini menyediakan konfigurasi write-once, read-many (WORM) dan penegakan periode retensi.

Jika Anda mengikuti panduan konfigurasi saat ini, AWS Backup dapat memberikan daya tahan tahunan 99,999999999%, juga dikenal sebagai 11 sembilan. Ini menggunakan infrastruktur AWS global untuk mereplikasi cadangan Anda di beberapa Availability Zone. Untuk informasi selengkapnya, lihat Ketahanan di AWS Backup.

AWS Backup membantu Anda mengotomatiskan pemulihan dan pengujian data cadangan untuk memverifikasi integritas dan proses cadangan.

Praktik terbaik terkait dalam Kerangka AWS Well-Architected

- SEC09-BP01 Menerapkan manajemen kunci dan sertifikat yang aman
- SEC09-BP02 Menerapkan enkripsi data bergerak
- SEC09-BP03 Mengautentikasi komunikasi jaringan

Menerapkan tema ini

Mengotomatiskan pencadangan dan pemulihan data

- Menerapkan cadangan data pada AWS
- Mengotomatiskan cadangan data dalam skala (posting AWS blog)
- Mengotomatiskan validasi pemulihan data dengan AWS Backup (AWS posting blog)

Menerapkan tata kelola di seluruh hasil Anda AWS Backup

- 10 praktik terbaik keamanan teratas untuk mengamankan cadangan di AWS (AWS posting blog)
- Gunakan AWS Backup Vault Lock untuk meningkatkan keamanan brankas cadangan Anda
- Gunakan AWS Backup Audit Manager untuk mengaudit kepatuhan AWS Backup kebijakan Anda

Memantau tema ini

Menerapkan AWS Config aturan berikut

- `RDS_IN_BACKUP_PLAN`
- `RDS_LAST_BACKUP_RECOVERY_POINT_CREATED`
- `RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN`
- `REDSHIFT_BACKUP_ENABLED`
- `AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED`
- `AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN`
- `BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK`
- `BACKUP_RECOVERY_POINT_ENCRYPTED`

- BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
- BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
- DB_INSTANCE_BACKUP_ENABLED
- DYNAMODB_IN_BACKUP_PLAN
- DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED
- DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EBS_IN_BACKUP_PLAN
- EBS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EC2_LAST_BACKUP_RECOVERY_POINT_CREATED
- S3_LAST_BACKUP_RECOVERY_POINT_CREATED
- S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED
- STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED
- VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tema 7: Memusatkan logging dan monitoring

Esensi Delapan strategi tercakup

Kontrol aplikasi, aplikasi tambalan, batasi hak administratif, otentikasi multi-faktor

AWS menyediakan alat dan fitur yang memungkinkan Anda untuk melihat apa yang terjadi di AWS lingkungan Anda. Ini termasuk:

- AWS CloudTrailmembantu Anda memantau AWS penerapan Anda dengan membuat jejak historis panggilan AWS API untuk akun Anda, termasuk panggilan API yang dilakukan melalui AWS Management Console, AWS SDKs, dan alat baris perintah. Untuk layanan yang mendukung CloudTrail, Anda juga dapat mengidentifikasi pengguna dan akun mana yang disebut API layanan, alamat IP sumber tempat panggilan dibuat, dan kapan panggilan terjadi.
- Amazon CloudWatch membantu Anda memantau metrik sumber AWS daya Anda dan aplikasi yang Anda jalankan AWS secara real time.
- Amazon CloudWatch Logs membantu Anda memusatkan log dari semua sistem, aplikasi, Layanan AWS sehingga Anda dapat memantau dan mengarsipkannya dengan aman.
- 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 . GuardDuty terintegrasi dengan Amazon EventBridge untuk memulai respons otomatis atau memberi tahu manusia.
- AWS Security Hubmemberikan pandangan komprehensif tentang keadaan keamanan Anda di AWS. Ini juga membantu Anda memeriksa AWS lingkungan Anda terhadap standar industri keamanan dan praktik terbaik.

Alat dan fitur ini dirancang untuk meningkatkan visibilitas dan membantu Anda mengatasi masalah sebelum berdampak negatif pada lingkungan Anda. Ini membantu Anda meningkatkan postur keamanan organisasi Anda di cloud dan mengurangi profil risiko lingkungan Anda.

Praktik terbaik terkait dalam Kerangka AWS Well-Architected

- SEC04-BP01 Mengonfigurasi pencatatan log layanan dan aplikasi
- SEC04-BP02 Tangkap log, temuan, dan metrik di lokasi standar

Menerapkan tema ini

Mengaktifkan pencatatan

- Gunakan CloudWatch agen untuk mempublikasikan log tingkat sistem ke Log CloudWatch
- Siapkan peringatan untuk temuan GuardDuty
- Buat jejak organisasi di CloudTrail

Menerapkan praktik terbaik keamanan logging

- Menerapkan praktik terbaik CloudTrail keamanan
- Gunakan SCPs untuk mencegah pengguna menonaktifkan layanan keamanan (AWS posting blog)
- Enkripsi data log di CloudWatch Log dengan menggunakan AWS Key Management Service

Memusatkan log

- Menerima CloudTrail log dari beberapa akun
- Kirim log ke akun arsip log
- Sentralisasi CloudWatch Log dalam akun untuk audit dan analisis (AWS posting blog)
- Memusatkan manajemen Amazon Inspector
- Buat agregator seluruh organisasi di AWS Config(posting blog)AWS
- Memusatkan manajemen Security Hub
- Memusatkan manajemen GuardDuty
- Pertimbangkan untuk menggunakan Amazon Security Lake

Memantau tema ini

Menerapkan mekanisme

- Menetapkan mekanisme untuk meninjau temuan log
- Menetapkan mekanisme untuk meninjau temuan Security Hub
- Menetapkan mekanisme untuk menanggapi GuardDuty temuan

Menerapkan AWS Config aturan berikut

- `CLOUDTRAIL_SECURITY_TRAIL_ENABLED`
- `GUARDDUTY_ENABLED_CENTRALIZED`
- `SECURITYHUB_ENABLED`
- `ACCOUNT_PART_OF_ORGANIZATIONS`

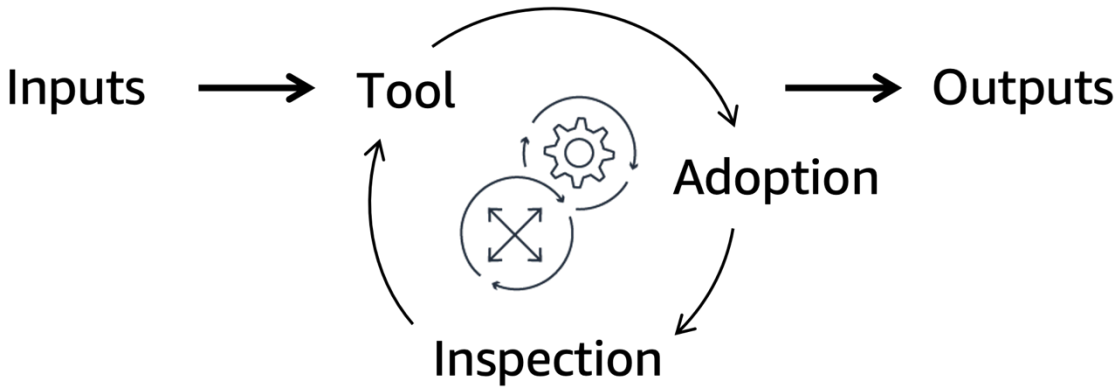
Tema 8: Menerapkan mekanisme untuk proses manual

Esensi Delapan strategi tercakup

Kontrol aplikasi, aplikasi tambalan

Di Amazon, kami memiliki pepatah: Niat baik tidak berfungsi—mekanisme berhasil (AWS posting blog). Ini berarti Anda harus mengganti upaya terbaik dengan proses dan alat yang otomatis, berulang, dan dapat diskalakan untuk mencapai hasil yang diinginkan.

Seperti yang ditunjukkan pada diagram berikut, mekanisme adalah proses lengkap di mana Anda membuat alat, mendorong adopsi alat, dan kemudian memeriksa hasilnya untuk penyesuaian. Ini adalah siklus yang memperkuat dan meningkatkan dirinya sendiri saat beroperasi. Dibutuhkan input yang dapat dikontrol dan mengubahnya menjadi output berkelanjutan untuk mengatasi tantangan bisnis yang berulang. Untuk informasi lebih lanjut, lihat Membangun mekanisme di AWS Well-Architected Framework.



Praktik terbaik terkait dalam Kerangka AWS Well-Architected

- OPS02-BP01 Sumber daya memiliki pemilik teridentifikasi
- OPS02-BP02 Proses dan Prosedur memiliki pemilik teridentifikasi
- OPS02-BP03 Aktivitas operasi memiliki pemilik teridentifikasi yang bertanggung jawab atas kinerjanya
- OPS02-BP04 Mekanisme tersedia untuk mengelola tanggung jawab dan kepemilikan
- OPS03-BP01 Memberikan sponsor eksekutif

- OPS03-BP03 Tim didorong untuk membawa masalah ke tingkat yang lebih tinggi

Menerapkan tema ini

- Menetapkan mekanisme untuk meninjau dan mengatasi kesenjangan kepatuhan
- Menetapkan mekanisme untuk memperbarui kebijakan keamanan
- Hapus aplikasi yang tidak didukung dan kemudian tambahkan ke daftar AWS Config penolakan aturan
- Validasi kebijakan akses dengan AWS Identity and Access Management Access Analyzer
- Aktifkan Amazon Inspector, yang secara otomatis menyimpan register kerentanan up-to-date
- Minimal, tinjau aturan kontrol aplikasi yang ditetapkan setiap tahun
- Pertimbangkan untuk menerapkan otomatisasi, seperti AWS Config aturan, untuk mengurangi beban proses manual
- Pertimbangkan untuk menggunakan AWS Systems Manager Inventaris untuk mendapatkan visibilitas ke instans mana yang menjalankan perangkat lunak yang diperlukan oleh kebijakan perangkat lunak Anda

Memantau tema ini

- Menetapkan pengawasan untuk sponsor eksekutif yang dapat melacak kemajuan menuju tujuan — termasuk kepatuhan, inspeksi kesenjangan, dan evaluasi mekanisme.

Studi kasus indikatif untuk mencapai kematangan Esential Eight pada AWS

Bab ini menyajikan studi kasus indikatif untuk lembaga pemerintah yang menargetkan kematangan Esential Eight pada. AWS

Bagian dalam Bab ini:

Ikhtisar skenario dan arsitektur

Lembaga pemerintah memiliki tiga beban kerja di AWS Cloud:

- Data lake tanpa server yang menggunakan Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) untuk penyimpanan AWS Lambda dan untuk operasi ekstrak, transformasi, dan pemuatan (ETL)
- Layanan web kontainer yang berjalan di Amazon Elastic Container Service (Amazon ECS) dan menggunakan database di Amazon Relational Database Service (Amazon RDS)
- Perangkat lunak komersial off-the-shelf (COTS) yang berjalan di Amazon EC2

Tim cloud menyediakan platform terpusat untuk organisasi, menjalankan layanan inti untuk AWS lingkungan. Tim cloud menyediakan layanan inti untuk AWS lingkungan. Setiap beban kerja dimiliki oleh tim aplikasi yang berbeda, juga dikenal sebagai tim pengembang atau tim pengiriman.

Arsitektur inti

Tim cloud telah menetapkan kemampuan berikut di AWS Cloud:

- Federasi identitas terhubung AWS IAM Identity Center ke mereka Microsoft Entra ID (sebelumnya Azure Active Directory) misalnya. Federasi memberlakukan MFA, kedaluwarsa otomatis akun pengguna, dan penggunaan AWS Identity and Access Management kredensil berumur pendek melalui peran (IAM).

- Pipeline AMI terpusat digunakan untuk menambal OSs dan aplikasi inti dengan EC2 Image Builder.
- Amazon Inspector diaktifkan untuk mengidentifikasi kerentanan, dan semua temuan keamanan dikirim ke Amazon GuardDuty untuk pengelolaan terpusat.
- Mekanisme yang ditetapkan digunakan untuk memperbarui aturan kontrol aplikasi, menanggapi peristiwa keamanan cyber, dan meninjau kesenjangan kepatuhan.
- AWS CloudTrail digunakan untuk logging dan monitoring.
- Peristiwa keamanan, seperti login pengguna root, memulai peringatan.
- SCPs dan kebijakan titik akhir VPC menetapkan batas data untuk lingkungan Anda. AWS
- SCPs mencegah tim aplikasi menonaktifkan layanan keamanan dan pencatatan, seperti CloudTrail dan. AWS Config
- AWS Config Temuan dikumpulkan dari seluruh AWS organisasi menjadi satu Akun AWS untuk keamanan.
- Paket kesesuaian AWS Config ACSC Essential 8 diaktifkan di semua Akun AWS organisasi Anda.

Contoh beban kerja: Data lake tanpa server

Beban kerja ini adalah contoh dari. Tema 1: Gunakan layanan terkelola

Danau data menggunakan Amazon S3 untuk penyimpanan dan AWS Lambda untuk ETL. Sumber daya ini didefinisikan dalam AWS Cloud Development Kit (AWS CDK) aplikasi. Perubahan pada sistem diterapkan melalui AWS CodePipeline. Pipeline ini dibatasi untuk tim aplikasi. Ketika tim aplikasi membuat permintaan tarik untuk repositori kode, aturan dua orang digunakan.

Untuk beban kerja ini, tim aplikasi mengambil tindakan berikut untuk mengatasi strategi Esential Eight.

Kontrol aplikasi

- Tim aplikasi memungkinkan Lambda Protection in dan GuardDuty Lambda scanning di Amazon Inspector.
- Tim aplikasi menerapkan mekanisme untuk memeriksa dan mengelola temuan Amazon Inspector.

Aplikasi tambalan

- Tim aplikasi mengaktifkan pemindaian Lambda di Amazon Inspector dan mengonfigurasi peringatan untuk pustaka yang tidak digunakan lagi atau rentan.

- Tim aplikasi memungkinkan AWS Config untuk melacak AWS sumber daya untuk penemuan aset.

Batasi hak administratif

- Seperti yang dijelaskan di Arsitektur inti bagian ini, tim aplikasi sudah membatasi akses ke penerapan produksi melalui aturan persetujuan pada pipeline penerapan mereka.
- Tim aplikasi bergantung pada federasi identitas terpusat dan solusi logging terpusat yang dijelaskan di bagian ini. Arsitektur inti
- Tim aplikasi membuat AWS CloudTrail jejak dan CloudWatch filter Amazon.
- Tim aplikasi menyiapkan peringatan Amazon Simple Notification Service (Amazon SNS) CodePipeline untuk penerapan dan penghapusan tumpukan. AWS CloudFormation

Sistem operasi patch

- Tim aplikasi mengaktifkan pemindaian Lambda di Amazon Inspector dan mengonfigurasi peringatan untuk pustaka yang tidak digunakan lagi atau rentan.

Otentikasi multi-faktor

- Tim aplikasi bergantung pada solusi federasi identitas terpusat yang dijelaskan di bagian ini. Arsitektur inti Solusi ini memberlakukan MFA, otentikasi log, dan peringatan pada atau secara otomatis merespons peristiwa MFA yang mencurigakan.

Pencadangan reguler

- Tim aplikasi menyimpan kode, seperti AWS CDK aplikasi dan fungsi dan konfigurasi Lambda, dalam repositori kode.
- Tim aplikasi memungkinkan pembuatan versi dan Amazon S3 Object Lock untuk membantu mencegah objek dihapus atau dimodifikasi.
- Tim aplikasi mengandalkan daya tahan Amazon S3 bawaan daripada mereplikasi seluruh dataset mereka ke yang lain. Wilayah AWS
- Tim aplikasi menjalankan salinan beban kerja di tempat lain Wilayah AWS yang memenuhi persyaratan kedaulatan data mereka. Mereka menggunakan tabel global Amazon DynamoDB dan Replikasi Lintas Wilayah Amazon S3 untuk mereplikasi data secara otomatis dari Wilayah primer ke Wilayah sekunder.

Contoh beban kerja: Layanan web kontainer

Beban kerja ini adalah contoh dari. Tema 2: Mengelola infrastruktur yang tidak dapat diubah melalui jaringan pipa yang aman

Layanan web berjalan di Amazon ECS dan menggunakan database di Amazon RDS. Tim aplikasi mendefinisikan sumber daya ini dalam AWS CloudFormation template. Wadah dibuat dengan EC2 Image Builder dan disimpan di Amazon ECR. Tim aplikasi menyebarkan perubahan ke sistem melalui AWS CodePipeline. Pipeline ini dibatasi untuk tim aplikasi. Ketika tim aplikasi membuat permintaan tarik untuk repositori kode, aturan dua orang digunakan.

Untuk beban kerja ini, tim aplikasi mengambil tindakan berikut untuk mengatasi strategi Esential Eight.

Kontrol aplikasi

- Tim aplikasi memungkinkan pemindaian gambar kontainer Amazon ECR di Amazon Inspector.
- Tim aplikasi membangun alat keamanan File Access Policy Daemon (fapolicyd) ke dalam pipeline Image Builder. EC2 Untuk informasi selengkapnya, lihat Menerapkan Kontrol Aplikasi di situs web ACSC.
- Tim aplikasi mengonfigurasi definisi tugas Amazon ECS untuk mencatat output ke Amazon CloudWatch Logs.
- Tim aplikasi menerapkan mekanisme untuk memeriksa dan mengelola temuan Amazon Inspector.

Aplikasi tambalan

- Tim aplikasi memungkinkan pemindaian gambar kontainer Amazon ECR di Amazon Inspector dan mengonfigurasi peringatan untuk pustaka yang tidak digunakan lagi atau rentan.
- Tim aplikasi mengotomatiskan tanggapan mereka terhadap temuan Amazon Inspector. Temuan baru memulai pipeline penyebaran mereka melalui EventBridge pemicu Amazon, dan CodePipeline merupakan targetnya.
- Tim aplikasi memungkinkan AWS Config untuk melacak AWS sumber daya untuk penemuan aset.

Batasi hak administratif

- Tim aplikasi sudah membatasi akses ke penerapan produksi melalui aturan persetujuan pada pipeline penerapan mereka.

- Tim aplikasi mengandalkan federasi identitas tim cloud terpusat untuk rotasi kredensil dan pencatatan terpusat.
- Tim aplikasi membuat CloudTrail jejak dan CloudWatch filter.
- Tim aplikasi menyiapkan peringatan Amazon SNS untuk CodePipeline penerapan dan penghapusan tumpukan. CloudFormation

Sistem operasi patch

- Tim aplikasi memungkinkan pemindaian gambar kontainer Amazon ECR di Amazon Inspector dan mengonfigurasi peringatan untuk pembaruan patch OS.
- Tim aplikasi mengotomatiskan tanggapan mereka terhadap temuan Amazon Inspector. Temuan baru memulai pipa penyebaran mereka melalui EventBridge pemicu, dan CodePipeline merupakan targetnya.
- Tim aplikasi berlangganan pemberitahuan acara Amazon RDS sehingga mereka diberi tahu tentang pembaruan. Mereka membuat keputusan berbasis risiko dengan pemilik bisnis mereka tentang apakah akan menerapkan pembaruan ini secara manual atau membiarkan Amazon RDS menerapkannya secara otomatis.
- Tim aplikasi mengonfigurasi instans Amazon RDS menjadi klaster Zona Ketersediaan Multi untuk mengurangi dampak peristiwa pemeliharaan.

Otentikasi multi-faktor

- Tim aplikasi bergantung pada solusi federasi identitas terpusat yang dijelaskan di bagian ini. Arsitektur inti Solusi ini memberlakukan MFA, otentikasi log, dan peringatan pada atau secara otomatis merespons peristiwa MFA yang mencurigakan.

Pencadangan reguler

- Tim aplikasi mengonfigurasi AWS Backup untuk mengotomatiskan cadangan data cluster Amazon RDS mereka.
- Tim aplikasi menyimpan CloudFormation template dalam repositori kode.
- Tim aplikasi mengembangkan pipeline otomatis untuk membuat salinan beban kerja mereka di Wilayah lain dan menjalankan pengujian otomatis (posting AWS blog). Setelah pengujian otomatis berjalan, pipa menghancurkan tumpukan. Pipeline ini secara otomatis berjalan sebulan sekali dan memvalidasi efektivitas prosedur pemulihan.

Contoh beban kerja: Perangkat lunak COTS di Amazon EC2

Beban kerja ini adalah contoh dari. Tema 3: Kelola infrastruktur yang bisa berubah dengan otomatisasi

Beban kerja yang berjalan di Amazon EC2 dibuat secara manual dengan menggunakan file. AWS Management Console Pengembang memperbarui sistem secara manual dengan masuk ke EC2 instance dan memperbarui perangkat lunak.

Untuk beban kerja ini, tim cloud dan aplikasi mengambil tindakan berikut untuk mengatasi strategi Esential Eight.

Kontrol aplikasi

- Tim cloud mengonfigurasi pipeline AMI terpusat mereka untuk menginstal dan mengonfigurasi AWS Systems Manager Agen (Agen SSM), CloudWatch agen, dan. SELinux Mereka membagikan AMI yang dihasilkan di semua akun di organisasi.
- Tim cloud menggunakan AWS Config aturan untuk mengonfirmasi bahwa semua EC2 instans yang berjalan dikelola oleh Systems Manager dan memiliki Agen SSM, CloudWatch agen, dan SELinux diinstal.
- Tim cloud mengirimkan output Amazon CloudWatch Logs ke solusi manajemen informasi dan peristiwa keamanan terpusat (SIEM) yang berjalan di Amazon OpenSearch Service.
- Tim aplikasi menerapkan mekanisme untuk memeriksa dan mengelola temuan dari AWS Config, GuardDuty, dan Amazon Inspector. Tim cloud mengimplementasikan mekanisme mereka sendiri untuk menangkap temuan apa pun yang terlewatkan oleh tim aplikasi. Untuk panduan selengkapnya tentang membuat program manajemen kerentanan untuk mengatasi temuan, lihat Membangun program manajemen kerentanan yang dapat diskalakan. AWS

Aplikasi tambalan

- Tim aplikasi menambal instance berdasarkan temuan Amazon Inspector.
- Tim cloud menambal AMI dasar, dan tim aplikasi menerima peringatan ketika AMI itu berubah.
- Tim aplikasi membatasi akses langsung ke EC2 instance mereka dengan mengonfigurasi aturan grup keamanan untuk mengizinkan lalu lintas hanya pada port yang dibutuhkan beban kerja.
- Tim aplikasi menggunakan Patch Manager untuk menambal instance alih-alih masuk ke instance individual.

- Untuk menjalankan perintah arbitrer pada grup EC2 instance, tim aplikasi menggunakan Run Command.
- Pada kesempatan langka ketika tim aplikasi membutuhkan akses langsung ke sebuah instance, mereka menggunakan Session Manager. Pendekatan akses ini menggunakan identitas federasi dan mencatat aktivitas sesi apa pun untuk tujuan audit.

Batasi hak administratif

- Tim aplikasi mengonfigurasi aturan grup keamanan untuk mengizinkan lalu lintas hanya pada port yang dibutuhkan beban kerja. Ini membatasi akses langsung ke EC2 instans Amazon dan mengharuskan pengguna mengakses EC2 instans melalui Session Manager.
- Tim aplikasi mengandalkan federasi identitas tim cloud terpusat untuk rotasi kredensil dan pencatatan terpusat.
- Tim aplikasi membuat CloudTrail jejak dan CloudWatch filter.
- Tim aplikasi menyiapkan peringatan Amazon SNS untuk CodePipeline penerapan dan penghapusan tumpukan. CloudFormation

Sistem operasi patch

- Tim cloud menambal AMI dasar, dan tim aplikasi menerima peringatan ketika AMI itu berubah. Tim aplikasi menyebarkan instance baru dengan menggunakan AMI ini, dan kemudian mereka menggunakan State Manager, kemampuan Systems Manager, untuk menginstal perangkat lunak yang diperlukan.
- Tim aplikasi menggunakan Patch Manager untuk menambal instance, instance login ke instance individual.
- Untuk menjalankan perintah arbitrer pada grup EC2 instance, tim aplikasi menggunakan Run Command.
- Pada kesempatan langka ketika tim aplikasi membutuhkan akses langsung, mereka menggunakan Session Manager.

Otentikasi multi-faktor

- Tim aplikasi bergantung pada solusi federasi identitas terpusat yang dijelaskan di bagian ini. Arsitektur inti Solusi ini memberlakukan MFA, otentikasi log, dan peringatan pada atau secara otomatis merespons peristiwa MFA yang mencurigakan.

Pencadangan reguler

- Tim aplikasi membuat AWS Backup rencana untuk EC2 instance-nya dan volume Amazon Elastic Block Store (Amazon EBS).
- Tim aplikasi menerapkan mekanisme untuk melakukan restorasi cadangan secara manual setiap bulan.

Sumber daya

AWS dokumentasi

- AWS Arsitektur Referensi Keamanan (AWS SRA)
- AWS dokumentasi keamanan
- Pilar keamanan dari AWS Well-Architected Framework

AWS Sumber daya lainnya

- AWS Keamanan Cloud
- AWS Kerangka Adopsi Cloud (Perspektif keamanan)

Sumber daya Pusat Keamanan Cyber Australia

- Esential Eight Dijelaskan
- Model Kedewasaan Delapan Esensi
- Panduan Proses Penilaian Delapan Penting

Kontributor

Para kontributor untuk dokumen ini antara lain:

- James Kingsmill, Arsitek Solusi Senior, AWS Arsitektur Solusi
- Chris Harding, Arsitek Solusi Senior, AWS Arsitektur Solusi
- Jess Modini, Arsitek Solusi Penasihat, Arsitektur Solusi AWS
- Justin Bowden, Kepala Jaminan Keamanan, Jaminan Keamanan AWS
- Rob Powell, Arsitek Solusi Senior, AWS Arsitektur Solusi
- Tony Mihaljevic, Arsitek Cloud Senior, Layanan Profesional AWS
- Volker Rath, Penasihat Keamanan Utama, AWS Keamanan Layanan Global

Lampiran: Esential Eight mengontrol matriks

Tabel berikut menghubungkan strategi Esential Eight dengan panduan AWS implementasi dan praktik terbaik yang relevan dalam AWS Well-Architected Framework. Untuk kontrol Essential Eight yang tidak berlaku dalam tabel AWS Cloud, tabel menyertakan tautan ke panduan tambahan dari Australian Cyber Security Centre (ACSC).

Matriks kontrol:

- Kontrol aplikasi
- Aplikasi patch
- Konfigurasi Microsoft Office pengaturan makro
- Pengerasan aplikasi pengguna
- Batasi hak administratif
- Sistem operasi patch
- Autentikasi multi-faktor
- Pencadangan reguler

Kontrol aplikasi

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Kontrol aplikasi diimplementasikan pada workstation dan server untuk membatasi eksekusi executable, pustaka perangkat lunak, skrip, installer, HTML yang dikompilasi, aplikasi HTML, applet panel kontrol dan	Tema 2: Mengelola infrastruktur yang tidak dapat diubah melalui jaringan pipa yang aman: Menerapkan AMI dan pipa pembuatan kontainer	Gunakan EC2 Image Builder dan bangun: • AWS Systems Manager Agen (Agen SSM) • Alat keamanan untuk kontrol aplikasi, seperti Security Enhanced Linux (SELinux) (GitHub), Daemon	SEC06-BP02 Komputasi ketentuan dari gambar yang diperkeras

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
driver ke set yang disetujui organisasi.		Kebijakan Akses File (fapolicyd) (), atau OpenSCAP GitHub CloudWatch Agen Amazon Berbagi AMIs dengan seluruh organisasi Pastikan tim aplikasi mereferensikan yang terbaru AMIs Gunakan pipeline AMI Anda untuk manajemen tambalan	
Microsoft'aturan blok yang direkomendasikan' diterapkan.	Lihat Menerapkan Kontrol Aplikasi (situs web ACSC)	Tidak berlaku	Tidak berlaku
Microsoft'aturan blok driver yang direkomendasikan' diterapkan.			
Aturan kontrol aplikasi divalidasi setiap tahun atau lebih sering.	Tema 8: Menerapkan mekanisme untuk proses manual: Menerapkan mekanisme untuk memperbarui kebijakan keamanan	Tidak tersedia	SEC01-BP08 Mengevaluasi dan menerapkan layanan dan fitur keamanan baru secara teratur

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Eksekusi yang diizinkan dan diblokir pada workstation dan server dicatat secara terpusat dan dilindungi dari modifikasi dan penghapusan yang tidak sah, dipantau untuk tanda-tanda kompromi, dan ditindaklanjuti ketika peristiwa keamanan cyber terdeteksi.	Tema 7: Memusatkan logging dan monitoring: Aktifkan pencatatan	Gunakan CloudWatch agen untuk mempublikasikan log tingkat sistem ke Log CloudWatch Siapkan peringatan untuk temuan GuardDuty Buat jejak organisasi di CloudTrail Lindungi data yang disimpan di Amazon S3 dengan menggunakan versi dan Kunci Objek S3	SEC04-BP01 Mengonfigurasi pencatatan log layanan dan aplikasi SEC04-BP02 Tangkap log, temuan, dan metrik di lokasi standar
	Tema 7: Memusatkan logging dan monitoring: Menerapkan praktik terbaik keamanan logging	Menerapkan praktik terbaik CloudTrail keamanan Gunakan SCPs untuk mencegah pengguna menonaktifkan layanan keamanan (AWS posting blog) Enkripsi data log di CloudWatch Log dengan menggunakan AWS Key Management Service	SEC04-BP01 Mengonfigurasi pencatatan log layanan dan aplikasi SEC04-BP02 Tangkap log, temuan, dan metrik di lokasi standar

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
	Tema 7: Memusatkan logging dan monitoring: Memusatkan log	Menerima CloudTrail log dari beberapa akun Kirim log ke akun arsip log Sentralisasi CloudWatch Log dalam akun untuk audit dan analisis (AWS posting blog) Memusatkan manajemen Amazon Inspector Buat agregator seluruh organisasi di AWS Config(posting blog)AWS Memusatkan manajemen Security Hub Memusatkan manajemen GuardDuty Pertimbangkan untuk menggunakan Amazon Security Lake	SEC04-BP02 Tangkap log, temuan, dan metrik di lokasi standar

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
	Tema 8: Menerapkan mekanisme untuk proses manual: Menerapkan mekanisme untuk meninjau dan mengatasi kesenjangan kepatuhan	Pertimbangkan untuk menerapkan otomatisasi, seperti AWS Config aturan, untuk mengurangi beban proses manual	OPS02-BP02 Proses dan Prosedur memiliki pemilik teridentifikasi OPS02-BP03 Aktivitas operasi memiliki pemilik teridentifikasi yang bertanggung jawab atas kinerjanya OPS02-BP04 Mekanisme tersedia untuk mengelola tanggung jawab dan kepemilikan

Aplikasi patch

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Metode otomatis penemuan aset digunakan setidaknya dua minggu untuk mendukung deteksi aset untuk aktivitas pemindaian kerentanan berikutnya.	Tema 1: Gunakan layanan terkelola: Pindai kerentanan Tema 2: Mengelola infrastruktur yang tidak dapat diubah melalui jaringan pipa yang aman: Menerapkan	Aktifkan Amazon Inspector di semua akun di organisasi Anda Konfigurasikan pemindaian yang disempurnakan untuk repositori Amazon ECR	SEC06-BP01 Lakukan manajemen kerentanan SEC06-BP05 Mengotomatiskan perlindungan komputasi

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
	pemindaian kerentanan Tema 3: Kelola infrastruktur yang bisa berubah dengan otomatisasi: Menerapkan pemindaian kerentanan	dengan menggunakan Amazon Inspector Membangun program manajemen kerentanan untuk melakukan triase dan memulihkan temuan keamanan	

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
	Tema 7: Memusatkan logging dan monitoring: Memusatkan log	Menerima CloudTrail log dari beberapa akun Kirim log ke akun arsip log Sentralisasi CloudWatch Log dalam akun untuk audit dan analisis (AWS posting blog) Memusatkan manajemen Amazon Inspector Buat agregator seluruh organisasi di AWS Config(posting blog)AWS Memusatkan manajemen Security Hub Memusatkan manajemen GuardDuty Pertimbangkan untuk menggunakan Security Lake	SEC04-BP02 Tangkap log, temuan, dan metrik di lokasi standar

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Pemindai kerentanan dengan database up-to-date kerentanan digunakan untuk aktivitas pemindaian kerentanan.	Tema 1: Gunakan layanan terkelola: Pindai kerentanan Tema 2: Mengelola infrastruktur yang tidak dapat diubah melalui jaringan pipa yang aman: Menerapkan pemindaian kerentanan Tema 3: Kelola infrastruktur yang bisa berubah dengan otomatisasi: Menerapkan pemindaian kerentanan	Aktifkan Amazon Inspector di semua akun di organisasi Anda Konfigurasikan pemindaian yang disempurnakan untuk repositori Amazon ECR dengan menggunakan Amazon Inspector Membangun program manajemen kerentanan untuk melakukan triase dan memulihkan temuan keamanan	SEC06-BP01 Lakukan manajemen kerentanan SEC06-BP05 Mengotomatiskan perlindungan komputasi
Pemindai kerentanan digunakan setidaknya setiap hari untuk mengidentifikasi patch atau pembaruan yang hilang untuk kerentanan keamanan dalam layanan yang menghadap ke internet.			

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Pemindai kerentanan digunakan setidaknya setiap minggu untuk mengidentifikasi tambalan atau pembaruan yang hilang untuk kerentanan keamanan di suite produktivitas kantor, browser web dan ekstensinya, klien email, perangkat lunak PDF, dan produk keamanan.	Lihat contoh Teknis: Aplikasi patch (situs web ACSC)	Tidak berlaku	Tidak berlaku

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Pemindai kerentanan digunakan setidaknya a dua minggu untuk mengidentifikasi tambalan atau pembaruan yang hilang untuk kerentanan keamanan di aplikasi lain.	Tema 1: Gunakan layanan terkelola: Pindai kerentanan Tema 2: Mengelola infrastruktur yang tidak dapat diubah melalui jaringan pipa yang aman: Menerapkan pemindaian kerentanan Tema 3: Kelola infrastruktur yang bisa berubah dengan otomatisasi: Menerapkan pemindaian kerentanan	Aktifkan Amazon Inspector di semua akun di organisasi Anda Konfigurasikan pemindaian yang disempurnakan untuk repositori Amazon ECR dengan menggunakan Amazon Inspector Membangun program manajemen kerentanan untuk melakukan triase dan memulihkan temuan keamanan	SEC06-BP01 Lakukan manajemen kerentanan SEC06-BP05 Mengotomatiskan perlindungan komputasi

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Tambalan, pembaruan, atau mitigasi vendor untuk kerentanan keamanan di layanan yang dihadapi internet diterapkan dalam waktu dua minggu setelah rilis, atau dalam waktu 48 jam jika ada eksploitasi.	Tema 1: Gunakan layanan terkelola: Pindai kerentanan Tema 2: Mengelola infrastruktur yang tidak dapat diubah melalui jaringan pipa yang aman: Menerapkan pemindaian kerentanan Tema 3: Kelola infrastruktur yang bisa berubah dengan otomatisasi: Menerapkan pemindaian kerentanan	Aktifkan Amazon Inspector di semua akun di organisasi Anda Konfigurasikan pemindaian yang disempurnakan untuk repositori Amazon ECR dengan menggunakan Amazon Inspector Membangun program manajemen kerentanan untuk melakukan triase dan memulihkan temuan keamanan	SEC06-BP01 Lakukan manajemen kerentanan
	Tema 3: Kelola infrastruktur yang bisa berubah dengan otomatisasi: Otomatiskan penambalan	Aktifkan Patch Manager di semua akun di AWS organisasi Anda	SEC06-BP01 Lakukan manajemen kerentanan SEC06-BP05 Mengotomatiskan perlindungan komputasi

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Tambalan, pembaruan, atau mitigasi vendor untuk kerentanan keamanan di suite produktivitas kantor, browser web dan ekstensinya, klien email, perangkat lunak PDF, dan produk keamanan diterapkan dalam waktu dua minggu setelah rilis, atau dalam waktu 48 jam jika ada eksploitasi.	Lihat contoh Teknis: Aplikasi patch (situs web ACSC)	Tidak berlaku	Tidak berlaku

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Tambalan, pembaruan, atau mitigasi vendor untuk kerentanan keamanan di aplikasi lain diterapkan dalam waktu satu bulan setelah rilis.	Tema 1: Gunakan layanan terkelola: Pindai kerentanan Tema 2: Mengelola infrastruktur yang tidak dapat diubah melalui jaringan pipa yang aman: Menerapkan pemindaian kerentanan Tema 3: Kelola infrastruktur yang bisa berubah dengan otomatisasi: Menerapkan pemindaian kerentanan	Aktifkan Amazon Inspector di semua akun di organisasi Anda Konfigurasikan pemindaian yang disempurnakan untuk repositori Amazon ECR dengan menggunakan Amazon Inspector Membangun program manajemen kerentanan untuk melakukan triase dan memulihkan temuan keamanan	SEC06-BP01 Lakukan manajemen kerentanan
	Tema 3: Kelola infrastruktur yang bisa berubah dengan otomatisasi: Otomatiskan penambalan	Aktifkan Patch Manager di semua akun di AWS organisasi Anda	SEC06-BP01 Lakukan manajemen kerentanan SEC06-BP05 Mengotomatiskan perlindungan komputasi

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Aplikasi yang tidak lagi didukung oleh vendor dihapus.	Tema 8: Menerapkan mekanisme untuk proses manual: Menerapkan mekanisme untuk meninjau dan mengatasi kesenjangan kepatuhan	Pertimbangkan untuk menggunakan AWS Systems Manager Inventaris untuk mendapatkan visibilitas ke instans mana yang menjalankan perangkat lunak yang diperlukan oleh kebijakan perangkat lunak Anda	SEC06-BP02 Komputasi ketentuan dari gambar yang diperkeras

Konfigurasi Microsoft Office pengaturan makro

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Microsoft Office makro dinonaktifkan untuk pengguna yang tidak memiliki persyaratan bisnis yang ditunjukkan.	Lihat contoh teknis: Konfigurasi pengaturan makro (situs web ACSC)	Tidak berlaku	Tidak berlaku
Hanya Microsoft Office Makro yang berjalan dari dalam lingkungan kotak pasir, Lokasi Tepercaya, atau yang ditandatangani secara digital oleh penerbit			

Kontrol Esential Delapan	Panduan implement asi	AWS sumber daya	AWS Panduan Well-Architected
tepercaya diizinkan untuk dijalankan.			
Hanya pengguna istimewa yang bertanggung jawab untuk memvalidasi itu Microsoft Office makro bebas dari kode berbahaya dapat menulis dan memodifikasi konten dalam Lokasi Tepercaya.			
Microsoft Office makro yang ditandata ngani secara digital oleh penerbit yang tidak tepercaya tidak dapat diaktifka n melalui Bilah Pesan atau Tampilan Belakang Panggung.			
Microsoft OfficeDaf tar penerbit tepercaya divalidasi setiap tahun atau lebih sering.			
Microsoft Office makro dalam file yang berasal dari internet diblokir.			

Kontrol Esential Delapan	Panduan implement asi	AWS sumber daya	AWS Panduan Well-Architected
Microsoft Office pemindaian antivirus makro diaktifkan.			
Microsoft Office makro diblokir dari pembuatan Win32 Panggilan API.			
Microsoft Office pengaturan keamanan makro tidak dapat diubah oleh pengguna.			
Diizinkan dan diblokir Microsoft Office Eksekusi makro dicatat secara terpusat dan dilindung i dari modifikasi dan penghapusan yang tidak sah, dipantau untuk tanda-tan da kompromi, dan ditindaklanjuti ketika peristiwa keamanan cyber terdeteksi.			

Pengerasan aplikasi pengguna

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Browser web tidak memproses Java dari internet.	Lihat contoh Teknis: Pengerasan aplikasi pengguna (situs web ACSC)	Tidak berlaku	Tidak berlaku
Browser web tidak memproses iklan web dari internet.			
Internet Explorer 11 dinonaktifkan atau dihapus.			
Microsoft Office diblokir dari membuat proses anak.			
Microsoft Office diblokir dari membuat konten yang dapat dieksekusi.			
Microsoft Office diblokir dari menyuntikkan kode ke proses lain.			
Microsoft Office dikonfigurasi untuk mencegah aktivasi paket OLE.			

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Perangkat lunak PDF diblokir dari membuat proses anak.			
Panduan pengerasan ACSC atau vendor untuk browser web, Microsoft Office dan perangkat lunak PDF diimplementasikan.			
Peramban web, Microsoft Office dan pengaturan keamanan perangkat lunak PDF tidak dapat diubah oleh pengguna.			
.NET Framework 3.5 (termasuk .NET 2.0 dan 3.0) dinonaktifkan atau dihapus.			
Windows PowerShell 2.0 dinonaktifkan atau dihapus.			
PowerShell dikonfigurasi untuk menggunakan Mode Bahasa Terbatas.			

Kontrol Esential Delapan	Panduan implement asi	AWS sumber daya	AWS Panduan Well-Architected
Diblokir PowerShell Eksekusi skrip dicatat secara terpusat dan dilindungi dari modifikasi dan penghapusan yang tidak sah, dipantau untuk tanda-tan da kompromi, dan ditindaklanjuti ketika peristiwa keamanan cyber terdeteksi.			

Batasi hak administratif

Kontrol Esential Delapan	Panduan implement asi	AWS sumber daya	AWS Panduan Well-Architected
Permintaan untuk akses istimewa ke sistem dan aplikasi divalidasi saat pertama kali diminta.	Tema 4: Mengelola identitas: Menerapkan federasi identitas	Mewajibkan pengguna manusia untuk berfederasi dengan penyedia identitas untuk mengakses AWS dengan menggunakan kredensi sementara	SEC02-BP04 Mengandalkan penyedia identitas tersentralisasi SEC03-BP01 Menetapkan persyaratan akses
Akses istimewa ke sistem dan aplikasi dinonaktifkan secara otomatis setelah 12 bulan kecuali divalidasi ulang.	Tema 4: Mengelola identitas: Menerapkan federasi identitas	Mewajibkan pengguna manusia untuk berfederasi dengan penyedia identitas untuk mengakses AWS	SEC02-BP04 Mengandalkan penyedia identitas tersentralisasi

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
		dengan menggunakan kredensi sementara	
	Tema 4: Mengelola identitas: Putar kredensi	Memerlukan beban kerja untuk menggunakan peran IAM untuk mengakses AWS Mengotomatiskan penghapusan peran IAM yang tidak digunakan Putar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensil jangka panjang AWS Summit ANZ 2023: Perjalanan Anda menuju kredensil sementara di cloud (YouTube video)	SEC02-BP05 Melakukan audit dan rotasi kredensial secara berkala

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Akses istimewa ke sistem dan aplikasi dinonaktifkan secara otomatis setelah 45 hari tidak aktif.	Tema 4: Mengelola identitas: Menerapkan federasi identitas Tema 4: Mengelola identitas: Putar kredensi	Mewajibkan pengguna manusia untuk berfederasi dengan penyedia identitas untuk mengakses AWS dengan menggunakan kredensi sementara Memerlukan beban kerja untuk menggunakan peran IAM untuk mengakses AWS Mengotomatiskan penghapusan peran IAM yang tidak digunakan Putar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensil jangka panjang AWS Summit ANZ 2023: Perjalanan Anda menuju kredensil sementara di cloud (YouTube video)	SEC02-BP04 Mengandalkan penyedia identitas tersentralisasi SEC02-BP05 Melakukan audit dan rotasi kredensial secara berkala

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Akses istimewa ke sistem dan aplikasi terbatas hanya pada apa yang diperlukan bagi pengguna dan layanan untuk menjalankan tugas mereka.	Tema 4: Mengelola identitas: Terapkan izin hak istimewa paling sedikit	Lindungi kredensil pengguna root Anda dan jangan menggunakannya untuk tugas sehari-hari Gunakan IAM Access Analyzer untuk menghasilkan kebijakan hak istimewa paling sedikit berdasarkan aktivitas akses Verifikasi akses publik dan lintas akun ke sumber daya dengan IAM Access Analyzer Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk izin yang aman dan fungsional Menetapkan pagar pembatas izin di beberapa akun Gunakan batas izin untuk menetapkan izin maksimum yang dapat diberikan oleh	SEC01-BP02 Pengguna root akun aman dan properti SEC03-BP02 Memberikan hak akses paling rendah

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
		kebijakan berbasis identitas Gunakan ketentuan dalam kebijakan IAM untuk membatasi akses lebih lanjut Secara teratur meninjau dan menghapus pengguna, peran, izin, kebijakan, dan kredensil yang tidak digunakan Memulai kebijakan AWS terkelola dan beralih ke izin dengan hak istimewa paling sedikit Gunakan fitur set izin di IAM Identity Center	
Akun istimewa dicegah mengakses internet, email, dan layanan web.	Lihat Contoh teknis: Batasi hak administratif (situs web ACSC)	Pertimbangkan untuk menerapkan SCP yang mencegah VPC apa pun yang belum memiliki akses internet mendapatkannya	Tidak berlaku

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Pengguna istimewa menggunakan lingkungan operasi istimewa dan tidak memiliki hak istimewa yang terpisah.	Tema 5: Menetapkan perimeter data	Membuat perimeter data. Pertimbangkan untuk menerapkan batas data antara lingkungan dengan klasifikasi data yang berbeda, seperti `OFFICIAL: SENSITIVE` atau`PROTECTED` , atau tingkat risiko yang berbeda, seperti pengembangan, pengujian, atau produksi.	SEC06-BP03 Kurangi manajemen manual dan akses interaktif
Lingkungan operasi istimewa tidak tervirtualisasi dalam lingkungan operasi yang tidak memiliki hak istimewa.			
Akun yang tidak memiliki hak istimewa tidak dapat masuk ke lingkungan operasi yang memiliki hak istimewa.			
Akun istimewa (tidak termasuk akun administrator lokal) tidak dapat masuk ke lingkungan operasi yang tidak memiliki hak istimewa.			

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Just-in-time administrasi digunakan untuk mengelola sistem dan aplikasi.	Tema 4: Mengelola identitas: Menerapkan federasi identitas	Mewajibkan pengguna manusia untuk berfederasi dengan penyedia identitas untuk mengakses AWS dengan menggunakan kredensi sementara Menerapkan akses sementara yang ditinggikan ke AWS lingkungan Anda (posting AWS blog)	SEC02-BP04 Mengandalkan penyedia identitas tersentralisasi
Kegiatan administratif dilakukan melalui server lompat.	Tema 1: Gunakan layanan terkelola Tema 3: Kelola infrastruktur yang bisa berubah dengan otomatisasi: Gunakan otomatisasi daripada proses manual	Gunakan Session Manager atau Run Command alih-alih akses SSH atau RDP langsung	SEC01-BP05 Mengurangi ruang lingkup manajemen keamanan SEC06-BP03 Kurangi manajemen manual dan akses interaktif
Kredensi untuk akun administrator lokal dan akun layanan unik, tidak dapat diprediksi, dan dikelola.	Lihat Contoh teknis: Batasi hak administratif (situs web ACSC)	Tidak berlaku	Tidak berlaku

Kontrol Esential Delapan	Panduan implement asi	AWS sumber daya	AWS Panduan Well-Architected
Windows Defender Credential Guard and Windows Defender Remote Credential Guard diaktifkan.			

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Penggunaan akses istimewa dicatat secara terpusat dan dilindungi dari modifikasi dan penghapusan yang tidak sah, dipantau untuk tanda-tanda kompromi, dan ditindaklanjuti ketika peristiwa keamanan cyber terdeteksi.	Tema 7: Memusatkan logging dan monitoring: Aktifkan pencatatan Tema 7: Memusatkan logging dan monitoring: Memusatkan log	Gunakan CloudWatch Agen untuk mempublikasikan log tingkat OS ke Log CloudWatch Aktifkan CloudTrail untuk organisasi Anda Sentralisasi CloudWatch Log dalam akun untuk audit dan analisis (AWS posting blog) Memusatkan manajemen Amazon Inspector Memusatkan manajemen Security Hub Buat agregator seluruh organisasi di AWS Config(posting blog)AWS Memusatkan manajemen GuardDuty Pertimbangkan untuk menggunakan Amazon Security Lake	SEC04-BP01 Mengonfigurasi pencatatan log layanan dan aplikasi SEC04-BP02 Tangkap log, temuan, dan metrik di lokasi standar
Perubahan pada akun dan grup istimewa dicatat secara terpusat dan dilindungi dari modifikasi dan penghapusan yang tidak sah, dipantau untuk tanda-tanda kompromi, dan ditindaklanjuti ketika peristiwa keamanan cyber terdeteksi.			

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
		Menerima CloudTrail log dari beberapa akun Kirim log ke akun arsip log	

Sistem operasi patch

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Tambalan, pembaruan, atau mitigasi vendor untuk kerentanan keamanan dalam sistem operasi layanan yang menghadap ke internet diterapkan dalam waktu dua minggu setelah rilis, atau dalam waktu 48 jam jika ada eksploitasi.	Tema 2: Mengelola infrastruktur yang tidak dapat diubah melalui jaringan pipa yang aman: Menerapkan AMI dan pipa pembuatan kontainer	Gunakan EC2 Image Builder dan bangun: • AWS Systems Manager Agen (Agen SSM) • Alat keamanan untuk kontrol aplikasi, seperti Security Enhanced Linux (SELinux) (GitHub), Daemon Kebijakan Akses File (fapolicyd) (), atau OpenSCAP GitHub • CloudWatch Agen Amazon Berbagi AMIs dengan seluruh organisasi	SEC01-BP05 Mengurangi ruang lingkup manajemen keamanan SEC06-BP01 Lakukan manajemen kerentanan SEC06-BP03 Kurangi manajemen manual dan akses interaktif

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
		Pastikan tim aplikasi mereferensikan yang terbaru AMIs Gunakan pipeline AMI Anda untuk manajemen tambalan	
	Tema 1: Gunakan layanan terkelola: Aktifkan penambalan Tema 3: Kelola infrastruktur yang bisa berubah dengan otomatisasi: Otomatiskan penambalan	Aktifkan Patch Manager di semua akun di AWS organisasi Anda	SEC06-BP01 Lakukan manajemen kerentanan SEC06-BP05 Mengotomatiskan perlindungan komputasi

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Tambalan, pembaruan, atau mitigasi vendor untuk kerentanan keamanan dalam sistem operasi workstation, server, dan perangkat jaringan diterapkan dalam waktu dua minggu setelah rilis, atau dalam waktu 48 jam jika ada eksploitasi.	Tema 2: Mengelola infrastruktur yang tidak dapat diubah melalui jaringan pipa yang aman: Menerapkan AMI dan pipa pembuatan kontainer	Gunakan EC2 Image Builder dan bangun: • AWS Systems Manager Agen (Agen SSM) • Alat keamanan untuk kontrol aplikasi, seperti Security Enhanced Linux (SELinux) (GitHub), Daemon Kebijakan Akses File (fapolicyd) (), atau OpenSCAP GitHub • CloudWatch Agen Amazon Berbagi AMIs dengan seluruh organisasi Pastikan bahwa tim aplikasi mereferensikan yang terbaru AMIs Gunakan pipeline AMI Anda untuk manajemen tambalan	SEC01-BP05 Mengurangi ruang lingkup manajemen keamanan SEC06-BP01 Lakukan manajemen kerentanan SEC06-BP02 Komputasi ketentuan dari gambar yang diperkeras

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
	Tema 1: Gunakan layanan terkelola: Aktifkan penambalan Tema 3: Kelola infrastruktur yang bisa berubah dengan otomatisasi: Otomatiskan penambalan	Aktifkan Patch Manager di semua akun di AWS organisasi Anda	SEC06-BP01 Lakukan manajemen kerentanan SEC06-BP05 Mengotomatiskan perlindungan komputasi
Pemindai kerentanan digunakan setidaknya setiap hari untuk mengidentifikasi patch atau pembaruan yang hilang untuk kerentanan keamanan dalam sistem operasi layanan yang menghadap ke internet.	Tema 1: Gunakan layanan terkelola: Pindai kerentanan Tema 2: Mengelola infrastruktur yang tidak dapat diubah melalui jaringan pipa yang aman: Menerapkan pemindaian kerentanan Tema 3: Kelola infrastruktur yang bisa berubah dengan otomatisasi: Menerapkan pemindaian kerentanan	Aktifkan Amazon Inspector di semua akun di organisasi Anda Konfigurasikan pemindaian yang disempurnakan untuk repositori Amazon ECR dengan menggunakan Amazon Inspector Membangun program manajemen kerentanan untuk melakukan triase dan memulihkan temuan keamanan	SEC01-BP05 Mengurangi ruang lingkup manajemen keamanan SEC06-BP01 Lakukan manajemen kerentanan SEC06-BP02 Komputasi ketentuan dari gambar yang diperkeras
Pemindai kerentanan digunakan setidaknya setiap minggu untuk mengidentifikasi patch atau pembaruan yang hilang untuk kerentanan keamanan dalam sistem operasi workstation, server, dan perangkat jaringan.			

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Rilis terbaru, atau rilis sebelumnya, dari sistem operasi digunakan untuk workstation, server dan perangkat jaringan. Sistem operasi yang tidak lagi didukung oleh vendor diganti.	Tema 2: Mengelola infrastruktur yang tidak dapat diubah melalui jaringan pipa yang aman: Menerapkan pemindaian kerentanan	Gunakan EC2 Image Builder dan bangun: • AWS Systems Manager Agen (Agen SSM) • Alat keamanan untuk kontrol aplikasi, seperti Security Enhanced Linux (SELinux) (GitHub), Daemon Kebijakan Akses File (fapolicyd) (), atau OpenSCAP GitHub • CloudWatch Agen Amazon Berbagi AMIs dengan seluruh organisasi Pastikan bahwa tim aplikasi mereferensikan yang terbaru AMIs Gunakan pipeline AMI Anda untuk manajemen tambalan	SEC01-BP05 Mengurangi ruang lingkup manajemen keamanan SEC06-BP01 Lakukan manajemen kerentanan SEC06-BP02 Komputasi ketentuan dari gambar yang diperkeras

Autentikasi multi-faktor

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Otentikasi multi-faktor digunakan oleh pengguna organisasi jika mereka mengautentikasi ke layanan yang menghadap ke internet organisasi mereka.	Tema 4: Mengelola identitas: Menerapkan federasi identitas	Mewajibkan pengguna manusia untuk berfederasi dengan penyedia identitas untuk mengakses AWS dengan menggunakan kredensi sementara Menerapkan akses sementara yang ditinggikan ke AWS lingkungan Anda	SEC02-BP04 Mengandalkan penyedia identitas tersentralisasi
	Tema 4: Mengelola identitas: Menegakkan MFA	Memerlukan MFA untuk pengguna root Membutuhkan MFA melalui AWS IAM Identity Center Pertimbangkan untuk mewajibkan MFA untuk melakukan tindakan API khusus layanan	SEC02-BP01 Gunakan mekanisme masuk yang kuat
Otentikasi multi-faktor digunakan oleh pengguna organisasi jika mereka mengautentikasi ke layanan pihak ketiga	Lihat Menerapkan Otentikasi Multi-Faktor (situs web ACSC)	Tidak berlaku	Tidak berlaku

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
yang menghadap ke internet yang memproses, menyimpan, atau mengkomunikasikan data sensitif organisasi mereka.			
Otentikasi multi-faktor (jika tersedia) digunakan oleh pengguna organisasi jika mereka mengautentikasi ke layanan pihak ketiga yang menghadap ke internet yang memproses, menyimpan, atau mengkomunikasikan data non-sensitif organisasi mereka.			
Autentikasi multi-faktor diaktifkan secara default untuk pengguna non-organisasi (tetapi pengguna dapat memilih untuk memilih keluar) jika mereka mengautentikasi ke layanan yang menghadap ke internet organisasi.			

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Otentikasi multi-faktor digunakan untuk mengautentikasi pengguna sistem yang memiliki hak istimewa.	Tema 4: Mengelola identitas: Menerapkan federasi identitas	Mewajibkan pengguna manusia untuk berfederasi dengan penyedia identitas untuk mengakses AWS dengan menggunakan kredensi sementara Menerapkan akses sementara yang ditinggikan ke AWS lingkungan Anda	SEC02-BP04 Mengandalkan penyedia identitas tersentralisasi
	Tema 4: Mengelola identitas: Menegakkan MFA	Memerlukan MFA untuk pengguna root Memerlukan MFA melalui IAM Identity Center Pertimbangkan untuk mewajibkan MFA untuk melakukan tindakan API khusus layanan	SEC02-BP01 Gunakan mekanisme masuk yang kuat
Otentikasi multi-faktor digunakan untuk mengautentikasi pengguna yang mengakses repositori data penting.	Tema 4: Mengelola identitas: Menegakkan MFA	Pertimbangkan untuk mewajibkan MFA untuk melakukan tindakan API khusus layanan	SEC02-BP01 Gunakan mekanisme masuk yang kuat

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Otentikasi multi-faktor tahan peniruan verifier dan menggunakan: sesuatu yang dimiliki pengguna dan sesuatu yang diketahui pengguna, atau sesuatu yang dimiliki pengguna yang dibuka oleh sesuatu yang diketahui atau diketahui pengguna.	Lihat Menerapkan Otentikasi Multi-Faktor (situs web ACSC)	Tidak berlaku	Tidak berlaku

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Otentikasi multi-faktor yang berhasil dan tidak berhasil dicatat secara terpusat dan dilindungi dari modifikasi dan penghapusan yang tidak sah, dipantau untuk tanda-tanda kompromi, dan ditindaklanjuti ketika peristiwa keamanan cyber terdeteksi.	Tema 7: Memusatkan logging dan monitoring: Aktifkan pencatatan Tema 7: Memusatkan logging dan monitoring: Memusatkan log	Sentralisasi CloudWatch Log dalam akun untuk audit dan analisis (AWS posting blog) Memusatkan manajemen Amazon Inspector Memusatkan manajemen Security Hub Buat agregator seluruh organisasi di AWS Config(posting blog)AWS Memusatkan manajemen GuardDuty Pertimbangkan untuk menggunakan Security Lake Menerima CloudTrail log dari beberapa akun Kirim log ke akun arsip log	SEC04-BP01 Mengonfigurasi pencatatan log layanan dan aplikasi SEC04-BP02 Tangkap log, temuan, dan metrik di lokasi standar

Pencadangan reguler

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Pencadangan data penting, perangkat lunak dan pengaturan konfigurasi dilakukan dan disimpan secara terkoordinasi dan tangguh sesuai dengan persyaratan kelangsungan bisnis.	Tema 6: Mengotomatiskan cadangan: Otomatiskan pencadangan dan pemulihan data	Menerapkan cadangan data pada AWS Mengotomatiskan cadangan data dalam skala besar (posting AWS blog)	REL09-BP01 Mengidentifikasi dan mencadangkan data yang perlu dicadangkan, atau melakukan reproduksi ulang data dari sumber REL09-BP02 Mengamankan dan mengenkripsikan cadangan REL09-BP03 Melakukan pencadangan data secara otomatis
Pemulihan sistem, perangkat lunak, dan data penting dari cadangan diuji secara terkoordinasi sebagai bagian dari latihan pemulihan bencana.	Tema 6: Mengotomatiskan cadangan: Otomatiskan pencadangan dan pemulihan data Tema 6: Mengotomatiskan cadangan: Menerapkan tata kelola di seluruh hasil Anda AWS Backup	Mengotomatiskan validasi pemulihan data dengan AWS Backup (AWS posting blog) Gunakan AWS Backup Audit Manager untuk mengaudit kepatuhan AWS Backup ke bijakan Anda	REL09-BP04 Melakukan pemulihan data secara berkala untuk memverifikasi integritas dan proses pencadangan

Kontrol Esential Delapan	Panduan implementasi	AWS sumber daya	AWS Panduan Well-Architected
Akun yang tidak memiliki hak istimewa, dan akun istimewa (tidak termasuk administrator cadangan), tidak dapat mengakses cadangan.	Tema 6: Mengotomatiskan cadangan: Menerapkan tata kelola di seluruh hasil Anda AWS Backup	10 praktik terbaik keamanan teratas untuk mengamankan cadangan di AWS (AWS posting blog) Gunakan AWS Backup Vault Lock untuk meningkatkan keamanan brankas cadangan Anda Gunakan AWS Backup Audit Manager untuk mengaudit kepatuhan AWS Backup ke bijakan Anda	SEC08-BP04 Menerapkan kontrol akses
Akun yang tidak memiliki hak istimewa, dan akun istimewa (tidak termasuk akun break glass cadangan), dicegah untuk memodifikasi atau menghapus cadangan.			

Pemberitahuan

Pelanggan bertanggung jawab untuk membuat penilaian independen mereka sendiri atas informasi dalam dokumen ini. Dokumen ini: (a) hanya untuk tujuan informasi, (b) mewakili penawaran dan praktik AWS produk saat ini, yang dapat berubah tanpa pemberitahuan, dan (c) tidak membuat komitmen atau jaminan apa pun dari AWS dan afiliasinya, pemasok, atau pemberi lisensinya. AWS produk atau layanan disediakan “sebagaimana adanya” tanpa jaminan, representasi, atau kondisi apa pun, baik tersurat maupun tersirat. Tanggung jawab dan kewajiban AWS kepada pelanggannya dikendalikan oleh AWS perjanjian, dan dokumen ini bukan bagian dari, juga tidak mengubah, perjanjian apa pun antara AWS dan pelanggannya.

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
Pembaruan praktik terbaik	Kami memperbarui panduan ini untuk mencerminkan praktik terbaik terbaru dalam pilar keamanan Kerangka AWS Well-Architected.	6 November 2024
Publikasi awal	—	20 Oktober 2023

AWS Glosarium Panduan Preskriptif

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

Nomor

7 Rs

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

- Refactor/Re-Architect — Memindahkan aplikasi dan memodifikasi arsitekturnya dengan memanfaatkan sepenuhnya fitur cloud-native untuk meningkatkan kelincahan, kinerja, dan skalabilitas. Ini biasanya melibatkan porting sistem operasi dan database. Contoh: Migrasikan database Oracle lokal Anda ke Amazon Aurora PostgreSQL Compatible Edition.
- Replatform (angkat dan bentuk ulang) — Pindahkan aplikasi ke cloud, dan perkenalkan beberapa tingkat pengoptimalan untuk memanfaatkan kemampuan cloud. Contoh: 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 instance EC2 di. AWS Cloud
- Relokasi (hypervisor-level lift and shift) — Pindahkan infrastruktur ke cloud tanpa membeli perangkat keras baru, menulis ulang aplikasi, atau memodifikasi operasi yang ada. Anda memigrasikan server dari platform lokal ke layanan cloud untuk platform yang sama. Contoh: Migrasikan Microsoft Hyper-V aplikasi ke AWS.
- Pertahankan (kunjungi kembali) - Simpan aplikasi di lingkungan sumber Anda. Ini mungkin termasuk aplikasi yang memerlukan refactoring besar, dan Anda ingin menunda pekerjaan itu sampai nanti, dan aplikasi lama yang ingin Anda pertahankan, karena tidak ada pembenaran bisnis untuk memigrasikannya.

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

A

ABAC

Lihat kontrol akses berbasis atribut.

layanan abstrak

Lihat layanan terkelola.

ASAM

Lihat atomisitas, konsistensi, isolasi, daya tahan.

migrasi aktif-aktif

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

migrasi aktif-pasif

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

fungsi agregat

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

AI

Lihat kecerdasan buatan.

AIOps

Lihat operasi kecerdasan buatan.

anonimisasi

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

anti-pola

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

kontrol aplikasi

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

portofolio aplikasi

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

kecerdasan buatan (AI)

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

operasi kecerdasan buatan (AIOps)

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

enkripsi asimetris

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

atomisitas, konsistensi, isolasi, daya tahan (ACID)

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

kontrol akses berbasis atribut (ABAC)

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

sumber data otoritatif

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

Zona Ketersediaan

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

AWS Kerangka Adopsi Cloud (AWS CAF)

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

AWS Kerangka Kualifikasi Beban Kerja (AWS WQF)

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

B

bot buruk

Bot yang dimaksudkan untuk mengganggu atau membahayakan individu atau organisasi.

BCP

Lihat perencanaan kontinuitas bisnis.

grafik perilaku

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

sistem big-endian

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

klasifikasi biner

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

filter mekar

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

deployment biru/hijau

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

bot

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

botnet

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

cabang

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

akses break-glass

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

strategi brownfield

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

cache penyangga

Area memori tempat data yang paling sering diakses disimpan.

kemampuan bisnis

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

perencanaan kelangsungan bisnis (BCP)

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

C

KAFE

Lihat Kerangka Adopsi AWS Cloud.

penyebaran kenari

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

CCoE

Lihat Cloud Center of Excellence.

CDC

Lihat mengubah pengambilan data.

ubah pengambilan data (CDC)

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

rekayasa kekacauan

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

CI/CD

Lihat integrasi berkelanjutan dan pengiriman berkelanjutan.

klasifikasi

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

Enkripsi sisi klien

Enkripsi data secara lokal, sebelum target Layanan AWS menerimanya.

Pusat Keunggulan Cloud (CCoE)

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

komputasi cloud

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

model operasi cloud

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

tahap adopsi cloud

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

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

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

CMDB

Lihat database manajemen konfigurasi.

repositori kode

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

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

cache dingin

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

data dingin

Data yang jarang diakses dan biasanya historis. Saat menanyakan jenis data ini, kueri lambat biasanya dapat diterima. Memindahkan data ini ke tingkat atau kelas penyimpanan 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 is commonly described as a pipeline. CI/CDdapat membantu

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

CV

Lihat visi komputer.

D

data saat istirahat

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

klasifikasi data

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

penyimpangan data

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

data dalam transit

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

jala data

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

minimalisasi data

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

perimeter data

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

prapemrosesan data

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

asal data

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

subjek data

Individu yang datanya dikumpulkan dan diproses.

gudang data

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

bahasa definisi database (DDL)

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

bahasa manipulasi basis data (DHTML)

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

DDL

Lihat bahasa definisi database.

ansambel yang dalam

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

pembelajaran mendalam

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

defense-in-depth

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

administrator yang didelegasikan

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

deployment

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

lingkungan pengembangan

Lihat lingkungan.

kontrol detektif

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

pemetaan aliran nilai pengembangan (DVSM)

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

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

kembar digital

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

tabel dimensi

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

musibah

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

pemulihan bencana (DR)

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

DML~

Lihat bahasa manipulasi basis data.

desain berbasis domain

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

DR

Lihat pemulihan bencana.

deteksi drift

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

DVSM

Lihat pemetaan aliran nilai pengembangan.

E

EDA

Lihat analisis data eksplorasi.

EDI

Lihat pertukaran data elektronik.

komputasi tepi

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

pertukaran data elektronik (EDI)

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

enkripsi

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

kunci enkripsi

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

endianness

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

titik akhir

Lihat titik akhir layanan.

layanan endpoint

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

perencanaan sumber daya perusahaan (ERP)

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

enkripsi amplop

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

lingkungan

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

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

epik

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

ERP

Lihat perencanaan sumber daya perusahaan.

analisis data eksplorasi (EDA)

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

F

tabel fakta

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

gagal cepat

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

batas isolasi kesalahan

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

cabang fitur

Lihat cabang.

fitur

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

pentingnya fitur

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

transformasi fitur

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

beberapa tembakan mendorong

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

FGAC

Lihat kontrol akses berbutir halus.

kontrol akses berbutir halus (FGAC)

Penggunaan beberapa kondisi untuk mengizinkan atau menolak permintaan akses.

migrasi flash-cut

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

FM

Lihat model pondasi.

model pondasi (FM)

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

G

AI generatif

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

pemblokiran geografis

Lihat pembatasan geografis.

pembatasan geografis (pemblokiran geografis)

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

Alur kerja Gitflow

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

gambar emas

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

strategi greenfield

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

pagar pembatas

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

H

HA

Lihat ketersediaan tinggi.

migrasi database heterogen

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

ketersediaan tinggi (HA)

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

modernisasi sejarawan

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

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

data penahanan

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

migrasi database homogen

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

data panas

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

perbaikan terbaru

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

periode hypercare

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

I

IAc

Lihat infrastruktur sebagai kode.

kebijakan berbasis identitas

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

aplikasi idle

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

IIoT

Lihat Internet of Things industri.

infrastruktur yang tidak dapat diubah

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

masuk (masuknya) VPC

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

migrasi inkremental

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

Industri 4.0

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

infrastruktur

Semua sumber daya dan aset yang terkandung dalam lingkungan aplikasi.

infrastruktur sebagai kode (IAc)

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

Internet of Things industri (IIoT)

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

inspeksi VPC

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

Internet of Things (IoT)

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

interpretabilitas

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

IoT

Lihat Internet of Things.

Perpustakaan informasi TI (ITIL)

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

Manajemen layanan TI (ITSM)

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

ITIL

Lihat perpustakaan informasi TI.

ITSM

Lihat manajemen layanan TI.

L

kontrol akses berbasis label (LBAC)

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

landing zone

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

model bahasa besar (LLM)

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

migrasi besar

Migrasi 300 atau lebih server.

LBAC

Lihat kontrol akses berbasis label.

hak istimewa paling sedikit

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

angkat dan geser

Lihat 7 Rs.

sistem endian kecil

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

LLM

Lihat model bahasa besar.

lingkungan yang lebih rendah

Lihat lingkungan.

M

pembelajaran mesin (ML)

Jenis kecerdasan buatan yang menggunakan algoritma dan teknik untuk pengenalan 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.

mekanisme

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

akun anggota

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

MES

Lihat sistem eksekusi manufaktur.

Transportasi Telemetri Antrian Pesan (MQTT)

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

layanan mikro

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

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

arsitektur microservices

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

Program Percepatan Migrasi (MAP)

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

migrasi dalam skala

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

pabrik migrasi

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

metadata migrasi

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

pola migrasi

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

Penilaian Portofolio Migrasi (MPA)

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

Penilaian Kesiapan Migrasi (MRA)

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

strategi migrasi

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

ML

Lihat pembelajaran mesin.

modernisasi

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

penilaian kesiapan modernisasi

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

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

aplikasi monolitik (monolit)

Aplikasi yang berjalan sebagai layanan tunggal dengan proses yang digabungkan secara ketat. Aplikasi monolitik memiliki beberapa kelemahan. Jika satu fitur aplikasi mengalami lonjakan permintaan, seluruh arsitektur harus diskalakan. Menambahkan atau meningkatkan fitur aplikasi monolitik juga menjadi lebih kompleks ketika basis kode tumbuh. Untuk mengatasi masalah ini, Anda dapat menggunakan arsitektur microservices. Untuk informasi lebih lanjut, lihat 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 machine-to-machine (M2M) untuk otomasi industri. OPC-UA menyediakan standar interoperabilitas dengan enkripsi data, otentikasi, dan skema otorisasi.

perjanjian tingkat operasional (OLA)

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

Tinjauan Kesiapan Operasional (ORR)

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

teknologi operasional (OT)

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

integrasi operasi (OI)

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

jejak organisasi

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

manajemen perubahan organisasi (OCM)

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

kontrol akses asal (OAC)

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

identitas akses asal (OAI)

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

ORR

Lihat tinjauan kesiapan operasional.

OT

Lihat teknologi operasional.

keluar (jalan keluar) VPC

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

P

batas izin

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

Informasi Identifikasi Pribadi (PII)

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

PII

Lihat informasi yang dapat diidentifikasi secara pribadi.

buku pedoman

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

PLC

Lihat pengontrol logika yang dapat diprogram.

PLM

Lihat manajemen siklus hidup produk.

kebijakan

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

ketekunan poliglot

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

penilaian portofolio

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

predikat

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

predikat pushdown

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

kontrol preventif

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

principal

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

privasi berdasarkan desain

Pendekatan rekayasa sistem yang memperhitungkan privasi melalui seluruh proses pengembangan.

zona yang dihosting pribadi

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

kontrol proaktif

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

manajemen siklus hidup produk (PLM)

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

lingkungan produksi

Lihat lingkungan.

pengontrol logika yang dapat diprogram (PLC)

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

rantai cepat

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

pseudonimisasi

Proses penggantian 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.

Wilayah

Kumpulan AWS sumber daya di wilayah geografis. Masing-masing Wilayah AWS terisolasi dan independen dari yang lain untuk memberikan toleransi kesalahan, stabilitas, dan ketahanan. Untuk informasi selengkapnya, lihat Menentukan Wilayah AWS akun yang dapat digunakan.

regresi

Teknik ML yang memprediksi nilai numerik. Misalnya, untuk memecahkan masalah “Berapa harga rumah ini akan dijual?” Model ML dapat menggunakan model regresi linier untuk memprediksi harga jual rumah berdasarkan fakta yang diketahui tentang rumah (misalnya, luas persegi).

rehost

Lihat 7 Rs.

melepaskan

Dalam proses penyebaran, tindakan mempromosikan perubahan pada lingkungan produksi.

memindahkan

Lihat 7 Rs.

memplatform ulang

Lihat 7 Rs.

pembelian kembali

Lihat 7 Rs.

ketahanan

Kemampuan aplikasi untuk melawan atau pulih dari gangguan. Ketersediaan tinggi dan pemulihan bencana adalah pertimbangan umum ketika merencanakan ketahanan di. AWS Cloud Untuk informasi lebih lanjut, lihat AWS Cloud Ketahanan.

kebijakan berbasis sumber daya

Kebijakan yang dilampirkan ke sumber daya, seperti bucket Amazon S3, titik akhir, atau kunci enkripsi. Jenis kebijakan ini menentukan prinsipal mana yang diizinkan mengakses, tindakan yang didukung, dan kondisi lain yang harus dipenuhi.

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

Matriks yang mendefinisikan peran dan tanggung jawab untuk semua pihak yang terlibat dalam kegiatan migrasi dan operasi cloud. Nama matriks berasal dari jenis tanggung jawab yang didefinisikan dalam matriks: bertanggung jawab (R), akuntabel (A), dikonsultasikan (C), dan diinformasikan (I). Tipe dukungan (S) adalah opsional. Jika Anda menyertakan dukungan, matriks disebut matriks RASCI, dan jika Anda mengecualikannya, itu disebut matriks RACI.

kontrol responsif

Kontrol keamanan yang dirancang untuk mendorong remediasi efek samping atau penyimpangan dari garis dasar keamanan Anda. Untuk informasi selengkapnya, lihat Kontrol responsif dalam Menerapkan kontrol keamanan pada AWS.

melestarikan

Lihat 7 Rs.

pensiun

Lihat 7 Rs.

Retrieval Augmented Generation (RAG)

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

rotasi

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

kontrol akses baris dan kolom (RCAC)

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

RPO

Lihat tujuan titik pemulihan.

RTO

Lihat tujuan waktu pemulihan.

buku runbook

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

D

SAML 2.0

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

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

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 EC2 Amazon, atau memutar kredensil.

enkripsi sisi server

Enkripsi data di tujuannya, oleh Layanan AWS yang menerimanya.

kebijakan kontrol layanan (SCP)

Kebijakan yang menyediakan kontrol terpusat atas izin untuk semua akun di organisasi. AWS Organizations SCPs menentukan pagar pembatas atau menetapkan batasan pada tindakan yang dapat didelegasikan oleh administrator kepada pengguna atau peran. Anda dapat menggunakan SCPs daftar izin atau daftar penolakan, untuk menentukan layanan atau tindakan mana yang diizinkan atau dilarang. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan dalam AWS Organizations dokumentasi.

titik akhir layanan

URL titik masuk untuk file Layanan AWS. Anda dapat menggunakan endpoint untuk terhubung secara terprogram ke layanan target. Untuk informasi selengkapnya, lihat Layanan AWS titik akhir di Referensi Umum AWS.

perjanjian tingkat layanan (SLA)

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

indikator tingkat layanan (SLI)

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

tujuan tingkat layanan (SLO)

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

model tanggung jawab bersama

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

SIEM

Lihat informasi keamanan dan sistem manajemen acara.

titik kegagalan tunggal (SPOF)

Kegagalan dalam satu komponen penting dari aplikasi yang dapat mengganggu sistem.

SLA

Lihat perjanjian tingkat layanan.

SLI

Lihat indikator tingkat layanan.

SLO

Lihat tujuan tingkat layanan.

split-and-seed model

Pola untuk menskalakan dan mempercepat proyek modernisasi. Ketika fitur baru dan rilis produk didefinisikan, tim inti berpisah untuk membuat tim produk baru. Ini membantu meningkatkan kemampuan dan layanan organisasi Anda, meningkatkan produktivitas pengembang, dan mendukung inovasi yang cepat. Untuk informasi lebih lanjut, lihat Pendekatan bertahap untuk memodernisasi aplikasi di. AWS Cloud

SPOF

Lihat satu titik kegagalan.

skema bintang

Struktur organisasi database yang menggunakan satu tabel fakta besar untuk menyimpan data transaksional atau terukur dan menggunakan satu atau lebih tabel dimensi yang lebih kecil untuk menyimpan atribut data. Struktur ini dirancang untuk digunakan dalam gudang data atau untuk tujuan intelijen bisnis.

pola ara pencekik

Pendekatan untuk memodernisasi sistem monolitik dengan menulis ulang secara bertahap dan mengganti fungsionalitas sistem sampai sistem warisan dapat dinonaktifkan. Pola ini menggunakan analogi pohon ara yang tumbuh menjadi pohon yang sudah mapan dan akhirnya mengatasi dan menggantikan inangnya. Pola ini diperkenalkan oleh Martin Fowler sebagai cara untuk mengelola risiko saat menulis ulang sistem monolitik. Untuk contoh cara menerapkan pola ini, lihat Memodernisasi layanan web Microsoft ASP.NET (ASMX) lama secara bertahap menggunakan container dan Amazon API Gateway.

subnet

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

kontrol pengawasan dan akuisisi data (SCADA)

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

enkripsi simetris

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

pengujian sintetis

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

sistem prompt

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

T

tag

Pasangan nilai kunci yang bertindak sebagai metadata untuk mengatur sumber daya Anda. AWS Tanda dapat membantu Anda mengelola, mengidentifikasi, mengatur, dan memfilter sumber daya. Untuk informasi selengkapnya, lihat Menandai AWS sumber daya Anda.

variabel target

Nilai yang Anda coba prediksi dalam ML yang diawasi. Ini juga disebut sebagai variabel hasil. Misalnya, dalam pengaturan manufaktur, variabel target bisa menjadi cacat produk.

daftar tugas

Alat yang digunakan untuk melacak kemajuan melalui runbook. Daftar tugas berisi ikhtisar runbook dan daftar tugas umum yang harus diselesaikan. Untuk setiap tugas umum, itu termasuk perkiraan jumlah waktu yang dibutuhkan, pemilik, dan kemajuan.

lingkungan uji

Lihat lingkungan.

pelatihan

Untuk menyediakan data bagi model ML Anda untuk dipelajari. Data pelatihan harus berisi jawaban yang benar. Algoritma pembelajaran menemukan pola dalam data pelatihan yang memetakan atribut data input ke target (jawaban yang ingin Anda prediksi). Ini menghasilkan model ML yang menangkap pola-pola ini. Anda kemudian dapat menggunakan model ML untuk membuat prediksi pada data baru yang Anda tidak tahu targetnya.

gerbang transit

Hub transit jaringan yang dapat Anda gunakan untuk menghubungkan jaringan Anda VPCs dan lokal. Untuk informasi selengkapnya, lihat Apa itu gateway transit dalam AWS Transit Gateway dokumentasi.

alur kerja berbasis batang

Pendekatan di mana pengembang membangun dan menguji fitur secara lokal di cabang fitur dan kemudian menggabungkan perubahan tersebut ke cabang utama. Cabang utama kemudian dibangun untuk pengembangan, praproduksi, dan lingkungan produksi, secara berurutan.

akses tepercaya

Memberikan izin ke layanan yang Anda tentukan untuk melakukan tugas di organisasi Anda di dalam AWS Organizations dan di akunnya atas nama Anda. Layanan tepercaya menciptakan peran terkait layanan di setiap akun, ketika peran itu diperlukan, untuk melakukan tugas manajemen untuk Anda. Untuk informasi selengkapnya, lihat Menggunakan AWS Organizations dengan AWS layanan lain dalam AWS Organizations dokumentasi.

penyetelan

Untuk mengubah aspek proses pelatihan Anda untuk meningkatkan akurasi model ML. Misalnya, Anda dapat melatih model ML dengan membuat set pelabelan, menambahkan label, dan kemudian mengulangi langkah-langkah ini beberapa kali di bawah pengaturan yang berbeda untuk mengoptimalkan model.

tim dua pizza

Sebuah DevOps tim kecil yang bisa Anda beri makan dengan dua pizza. Ukuran tim dua pizza memastikan peluang terbaik untuk berkolaborasi dalam pengembangan perangkat lunak.

U

waswas

Sebuah konsep yang mengacu pada informasi yang tidak tepat, tidak lengkap, atau tidak diketahui yang dapat merusak keandalan model ML prediktif. Ada dua jenis ketidakpastian: ketidakpastian epistemik disebabkan oleh data yang terbatas dan tidak lengkap, sedangkan ketidakpastian aleatorik disebabkan oleh kebisingan dan keacakan yang melekat dalam data. Untuk informasi lebih lanjut, lihat panduan Mengukur ketidakpastian dalam sistem pembelajaran mendalam.

tugas yang tidak terdiferensiasi

Juga dikenal sebagai angkat berat, pekerjaan yang diperlukan untuk membuat dan mengoperasikan aplikasi tetapi itu tidak memberikan nilai langsung kepada pengguna akhir atau memberikan keunggulan kompetitif. Contoh tugas yang tidak terdiferensiasi termasuk pengadaan, pemeliharaan, dan perencanaan kapasitas.

lingkungan atas

Lihat lingkungan.

V

menyedot debu

Operasi pemeliharaan database yang melibatkan pembersihan setelah pembaruan tambahan untuk merebut kembali penyimpanan dan meningkatkan kinerja.

kendali versi

Proses dan alat yang melacak perubahan, seperti perubahan kode sumber dalam repositori.

Peering VPC

Koneksi antara dua VPCs yang memungkinkan Anda untuk merutekan lalu lintas dengan menggunakan alamat IP pribadi. Untuk informasi selengkapnya, lihat Apa itu peering VPC di dokumentasi VPC Amazon.

kerentanan

Kelemahan perangkat lunak atau perangkat keras yang membahayakan keamanan sistem.

W

cache hangat

Cache buffer yang berisi data saat ini 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.