Menerapkan kontrol keamanan pada AWS

AWS Bimbingan Preskriptif

AWS Bimbingan Preskriptif: Menerapkan kontrol keamanan pada AWS

Table of Contents

Menerapkan kontrol keamanan pada AWS

Iqbal Umair, Gurpreet Kaur Cheema, Wasim Hossain, Joseph Nguyen, San Brar, dan Lucia Vanta, Amazon Web Services () AWS

Desember 2023 (riwayat dokumen)

Keamanan sangat penting bagi setiap perusahaan, dan ini adalah pilar utama dalam Kerangka Kerja AWS Well-Architected. Namun, banyak yang tidak tahu bagaimana bekerja melalui pertimbangan keamanan dan membuat pengujian keamanan otomatis holistik dan strategi remediasi untuk lingkungan cloud mereka. Dengan menggunakan Layanan AWS dan alat, sepertiAWS Config, Amazon GuardDuty, danAWS CloudFormation, Anda dapat membuat strategi pengujian keamanan dan membangunnya ke AWS Cloud lingkungan Anda.

Untuk membantu memenuhi kebijakan dan standar keamanan perusahaan Anda, kontrol keamanan adalah pagar pembatas teknis atau administratif yang membantu mencegah, mendeteksi, atau mengurangi kemampuan pelaku ancaman untuk mengeksploitasi kerentanan keamanan. Mereka dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan sumber daya dan data. Berikut ini adalah contoh kontrol keamanan:

- Menerapkan otentikasi multi-faktor untuk pengguna yang perlu masuk ke aplikasi
- Tindakan pencatatan, pemantauan, dan kueri untuk tujuan melakukan audit aktivitas akun secara real-time
- Memastikan bahwa data sensitif dienkripsi
- Memastikan log disimpan sesuai dengan kebijakan retensi perusahaan Anda

Ada empat jenis kontrol keamanan: preventif, proaktif, detektif, dan responsif. Panduan ini menjelaskan setiap jenis secara lebih rinci dan berfokus pada cara menerapkan dan mengotomatiskan kontrol ini diAWS Cloud. Panduan ini membantu Anda menerapkan kontrol keamanan yang berkelanjutan dan proaktif.

Audiens yang dituju

Panduan ini ditujukan untuk arsitek dan insinyur keamanan yang bertanggung jawab untuk menerapkan kontrol keamanan diAWS Cloud. Jika perusahaan Anda belum menetapkan kebijakan keamanan, tujuan pengendalian, atau standar, seperti yang dijelaskan dalamKontrol keamanan

dalam kerangka tata kelola, kami sarankan Anda menyelesaikan tugas tata kelola ini sebelum melanjutkan dengan panduan ini.

Hasil bisnis yang ditargetkan

Perusahaan menggunakan kontrol keamanan untuk mengurangi atau bertindak sebagai penanggulangan terhadap risiko terhadap sistem TI-nya. Kontrol menentukan dasar persyaratan untuk memenuhi tujuan keamanan utama dari program TI dan strategi keamanannya. Memiliki kontrol di tempat meningkatkan postur keamanan perusahaan dengan melindungi kerahasiaan, integritas, dan ketersediaan data dan aset TI. Tanpa kontrol, akan sulit untuk mengetahui di mana Anda perlu fokus dan berinvestasi untuk menetapkan garis dasar keamanan.

Kontrol keamanan dapat digunakan untuk mengatasi berbagai skenario. Contohnya termasuk memenuhi persyaratan yang berasal dari penilaian risiko, mencapai standar industri, atau mematuhi peraturan. Kontrol keamanan yang memuaskan menunjukkan bahwa Anda telah mengukur risiko terhadap suatu sistem, menentukan tingkat perlindungan yang diperlukan, dan solusi yang diterapkan secara proaktif. Faktor tambahan, seperti bisnis, industri, dan geografi, semuanya dapat menentukan kontrol keamanan yang Anda butuhkan.

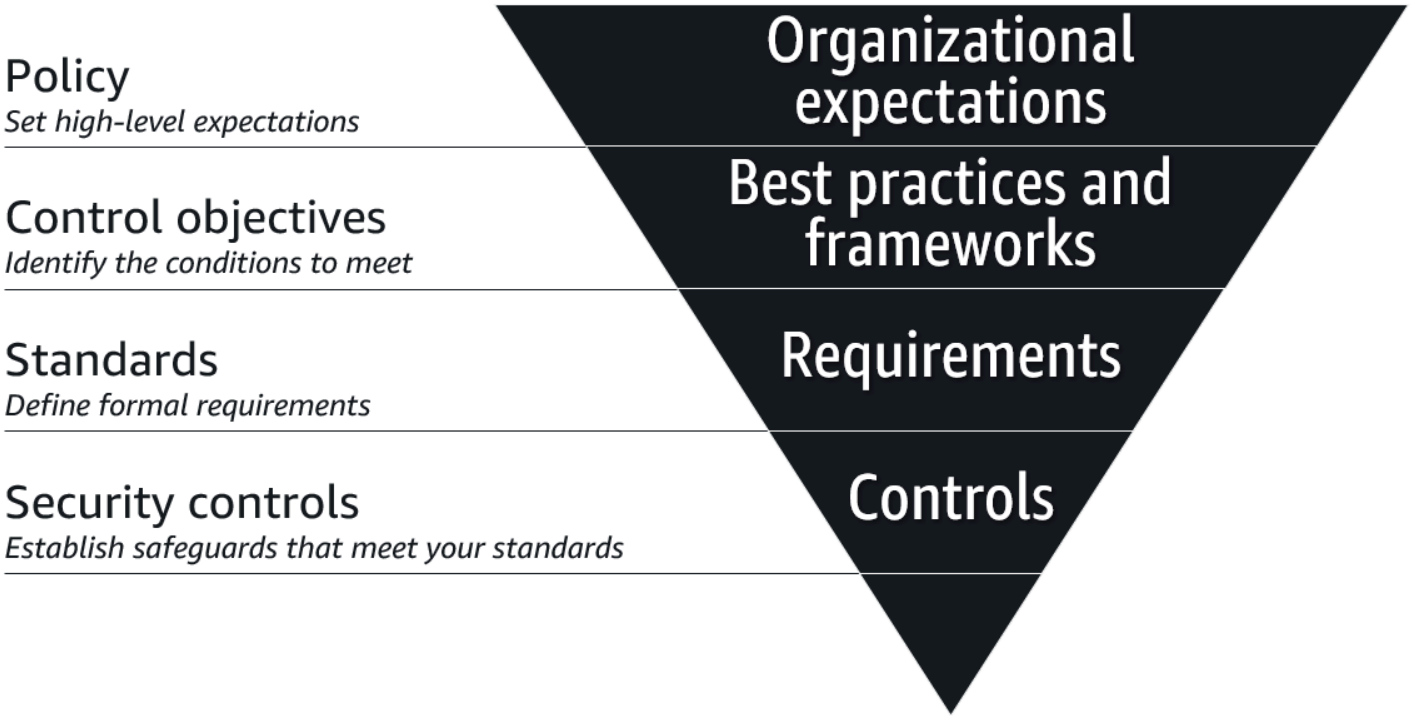
Berikut ini adalah kasus penggunaan umum untuk menerapkan kontrol keamanan:

- Penilaian keamanan aplikasi telah mengidentifikasi kebutuhan untuk kontrol akses berdasarkan sensitivitas data yang sedang diproses.
- Anda harus mematuhi standar keamanan, seperti Payment Card Industry Data Security Standard (PCI DSS), HIPAA (Health Insurance Portability and Accountability Act), atau National Institute of Standards and Technology (NIST).
- Anda perlu melindungi informasi sensitif untuk transaksi bisnis.
- Perusahaan Anda telah berkembang menjadi wilayah geografis yang memerlukan kontrol keamanan, seperti wilayah yang memerlukan kepatuhan terhadap Peraturan Perlindungan Data Umum (GDPR).

Setelah membaca panduan ini, Anda harus terbiasa dengan empat jenis kontrol keamanan, memahami bagaimana mereka adalah bagian dari kerangka tata kelola keamanan Anda, dan bersiaplah untuk mulai menerapkan dan mengotomatiskan kontrol keamanan di. AWS Cloud

Kontrol keamanan dalam kerangka tata kelola

Penting untuk merencanakan dari tingkat dasar. Bagaimana seseorang memulai? Gambar berikut menunjukkan bagaimana Anda dapat membangun strategi tata kelola keamanan berdasarkan kebijakan, tujuan kontrol, standar, dan kontrol keamanan.



Berikut ini adalah komponen hierarkis dari strategi tata kelola untuk keamanan:

- Kebijakan — Kebijakan adalah dasar dari setiap strategi tata kelola keamanan siber. Ini adalah dokumen yang menyatakan harapan perusahaan, seperti kewajiban hukum, peraturan, atau kontrak yang harus dipenuhi. Kebijakan dapat bervariasi menurut industri dan wilayah.
- Tujuan pengendalian — Tujuan pengendalian adalah target, seperti praktik terbaik yang diakui industri, yang membantu Anda memenuhi maksud kebijakan. Untuk komputasi awan, banyak perusahaan mengadopsi Cloud Controls Matrix (CCM) (situs web Cloud Security Alliance), yang merupakan kerangka kerja tujuan kontrol keamanan siber.
- Standar — Standar adalah persyaratan yang ditetapkan secara formal yang memenuhi tujuan kontrol. Standar mungkin mencakup proses, tindakan, atau konfigurasi, dan dapat diukur sehingga Anda dapat mengukur kinerja terhadap standar.
- Kontrol keamanan — Kontrol keamanan adalah mekanisme teknis atau administratif yang Anda tempatkan untuk menerapkan standar. Semua kontrol keamanan dipetakan ke standar, tetapi tidak

semua standar dipetakan ke kontrol keamanan. Pengujian kontrol keamanan dirancang untuk memantau dan mengukur apakah Anda secara efektif memenuhi standar yang ditetapkan.

Panduan ini berfokus pada bagaimana merancang dan menerapkan jenis kontrol keamanan umum diAWS Cloud.

Jenis kontrol keamanan

Ada empat jenis kontrol keamanan utama:

- Kontrol pencegahan— Kontrol ini dirancang untuk mencegah suatu peristiwa terjadi.
- Kontrol proaktif— Kontrol ini dirancang untuk mencegah penciptaan sumber daya yang tidak sesuai.
- Kontrol Detektif— Kontrol ini dirancang untuk mendeteksi, mencatat, dan memperingatkan setelah suatu peristiwa terjadi.
- Kontrol responsifKontrol ini dirancang untuk mendorong remediasi efek samping atau penyimpangan dari garis dasar keamanan Anda.

Strategi keamanan yang efektif mencakup keempat jenis kontrol keamanan. Meskipun kontrol pencegahan adalah garis pertahanan pertama untuk membantu mencegah akses tidak sah atau perubahan yang tidak diinginkan ke jaringan Anda, penting untuk memastikan bahwa Anda membuat kontrol detektif dan responsif sehingga Anda tahu kapan suatu peristiwa terjadi dan dapat mengambil tindakan segera dan tepat untuk memperbaikinya. Menggunakan kontrol proaktif menambahkan lapisan keamanan lain karena melengkapi kontrol pencegahan, yang umumnya lebih ketat di alam.

Bagian berikut menjelaskan setiap jenis kontrol secara lebih rinci. Mereka membahas tujuan, proses implementasi, kasus penggunaan, pertimbangan teknologi, dan hasil target dari setiap jenis kontrol.

Kontrol pencegahan

Kontrol pencegahan adalah kontrol keamanan yang dirancang untuk mencegah suatu peristiwa terjadi. Pagar pembatas ini adalah garis pertahanan pertama untuk membantu mencegah akses tidak sah atau perubahan yang tidak diinginkan ke jaringan Anda. Contoh kontrol preventif adalah peran AWS Identity and Access Management (IAM) yang memiliki akses hanya-baca karena membantu mencegah tindakan penulisan yang tidak diinginkan dari pengguna yang tidak sah.

Tinjau hal-hal berikut tentang jenis kontrol ini:

- Tujuan
- Proses
- Kasus penggunaan
- Teknologi

- Hasil bisnis

Tujuan

Tujuan utama dari pengendalian pencegahan adalah untuk meminimalkan atau menghindari kemungkinan terjadinya peristiwa ancaman. Kontrol harus membantu mencegah akses tidak sah ke sistem dan membantu mencegah perubahan yang tidak disengaja mempengaruhi sistem. Berikut ini adalah tujuan dari pengendalian pencegahan:

- Pemisahan tugas — Kontrol pencegahan dapat menetapkan batasan logis yang membatasi hak istimewa, memungkinkan izin untuk hanya melakukan tugas tertentu di akun atau lingkungan yang ditunjuk. Contohnya termasuk:
  - Mensegmentasi beban kerja ke akun yang berbeda untuk layanan tertentu
  - Memisahkan dan memperhitungkan ke dalam lingkungan produksi, pengembangan, dan pengujian yang terisolasi
  - Mendelegasikan akses dan tanggung jawab ke beberapa entitas untuk melakukan fungsi tertentu, seperti menggunakan peran IAM atau peran yang diasumsikan untuk memungkinkan hanya fungsi pekerjaan tertentu untuk melakukan tindakan tertentu
- Kontrol akses — Kontrol pencegahan dapat secara konsisten memberikan atau menolak akses ke sumber daya dan data di lingkungan. Contohnya termasuk:
  - Mencegah pengguna melebihi izin yang dimaksudkan, yang dikenal sebagai eskalasi hak istimewa
  - Membatasi akses ke aplikasi dan data hanya untuk pengguna dan layanan yang berwenang
  - Menjaga grup administrator tetap kecil
  - Menghindari penggunaan kredensi pengguna root
- Penegakan — Kontrol pencegahan dapat membantu perusahaan Anda mematuhi kebijakan, pedoman, dan standarnya. Contohnya termasuk:
  - Konfigurasi penguncian yang berfungsi sebagai dasar keamanan minimum
  - Menerapkan langkah-langkah keamanan tambahan, seperti otentikasi multi-faktor
  - Menghindari tugas dan tindakan yang tidak standar yang dilakukan oleh peran yang tidak disetujui

Proses

Pemetaan kontrol preventif adalah proses pemetaan kontrol terhadap persyaratan dan menggunakan kebijakan untuk mengimplementasikan kontrol tersebut dengan membatasi, menonaktifkan, atau memblokir. Saat memetakan kontrol, pertimbangkan efek proaktif yang mereka miliki terhadap lingkungan, sumber daya, dan pengguna. Berikut ini adalah praktik terbaik untuk kontrol pemetaan:

- Kontrol ketat yang melarang suatu aktivitas harus dipetakan ke lingkungan produksi di mana tindakan tersebut memerlukan proses peninjauan, persetujuan, dan perubahan.
- Pengembangan atau lingkungan yang terkandung mungkin memiliki kontrol pencegahan yang lebih sedikit untuk memberikan kelincahan untuk membangun dan menguji.
- Klasifikasi data, tingkat risiko aset, dan kebijakan manajemen risiko menentukan kontrol preventif.
- Memetakan kerangka kerja yang ada sebagai bukti kepatuhan terhadap standar dan peraturan.
- Menerapkan kontrol pencegahan berdasarkan lokasi geografis, lingkungan, akun, jaringan, pengguna, peran, atau sumber daya.

Kasus penggunaan

Penanganan data

Peran dibuat yang dapat mengakses semua data dalam akun. Jika ada data sensitif dan terenkripsi, hak istimewa yang terlalu permisif mungkin menimbulkan risiko, tergantung pada pengguna atau grup yang dapat mengambil peran tersebut. Dengan menggunakan kebijakan kunci di AWS Key Management Service (AWS KMS), Anda dapat mengontrol siapa yang memiliki akses ke kunci dan dapat mendekripsi data.

Eskalasi hak istimewa

Jika izin administratif dan tulis diberikan terlalu luas, pengguna dapat menghindari batas izin yang dimaksudkan dan memberikan hak istimewa tambahan kepada diri mereka sendiri. Pengguna yang membuat dan mengelola peran dapat menetapkan batas izin, yang menentukan hak istimewa maksimum yang diizinkan untuk peran tersebut.

Penguncian beban kerja

Jika bisnis Anda tidak memiliki kebutuhan yang dapat diperkirakan untuk menggunakan layanan tertentu, aktifkan kebijakan kontrol layanan yang membatasi layanan mana yang dapat beroperasi

di akun anggota organisasi atau membatasi layanan berdasarkan layanan. Wilayah AWS Kontrol pencegahan ini dapat mengurangi cakupan dampak jika pelaku ancaman berhasil berkompromi dan mengakses akun di organisasi Anda. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan dalam panduan ini.

Dampak terhadap aplikasi lain

Kontrol pencegahan dapat menegakkan penggunaan layanan dan fitur, seperti IAM, enkripsi, dan pencatatan, untuk memenuhi persyaratan keamanan aplikasi Anda. Anda juga dapat menggunakan kontrol ini untuk membantu melindungi terhadap kerentanan dengan membatasi tindakan yang dapat dieksploitasi oleh aktor ancaman karena kesalahan atau kesalahan konfigurasi yang tidak disengaja.

Teknologi

Kebijakan kontrol layanan

Dalam AWS Organizations, kebijakan kontrol layanan (SCP) menentukan izin maksimum yang tersedia untuk akun anggota dalam suatu organisasi. Kebijakan ini membantu akun tetap berada dalam pedoman kontrol akses organisasi. Perhatikan hal berikut saat mendesain SCP untuk organisasi Anda:

- SCP adalah kontrol pencegahan karena mereka menentukan dan menegakkan izin maksimum yang diizinkan untuk peran IAM dan pengguna di akun anggota organisasi.
- SCP hanya memengaruhi peran IAM dan pengguna di akun anggota organisasi. Itu tidak mempengaruhi pengguna dan peran dalam akun manajemen organisasi.

Anda dapat membuat SCP lebih terperinci dengan menentukan izin maksimum untuk masing-masing. Wilayah AWS

Batas izin IAM

Dalam AWS Identity and Access Management (IAM), batas izin digunakan untuk menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM (pengguna atau peran). Batas izin entitas memungkinkannya untuk melakukan hanya tindakan yang diizinkan oleh kebijakan berbasis identitas dan batas izinnya. Perhatikan hal berikut saat menggunakan batas izin:

- Anda dapat menggunakan kebijakan AWS terkelola atau kebijakan yang dikelola pelanggan untuk menetapkan batas entitas IAM.

- Batas izin tidak memberikan izin sendiri. Kebijakan batas izin membatasi izin yang diberikan kepada entitas IAM.

Hasil bisnis

Penghematan waktu

- Dengan menambahkan otomatisasi setelah Anda mengatur kontrol pencegahan, Anda dapat mengurangi kebutuhan akan intervensi manual dan mengurangi frekuensi kesalahan.
- Menggunakan batas izin sebagai kontrol pencegahan membantu tim keamanan dan IAM fokus pada tugas-tugas penting, seperti tata kelola dan dukungan.

Kepatuhan terhadap peraturan

- Perusahaan mungkin perlu mematuhi peraturan internal atau industri. Ini mungkin pembatasan regional, pembatasan pengguna dan peran, atau pembatasan layanan. SCP dapat membantu Anda tetap patuh dan menghindari hukuman pelanggaran.

Pengurangan risiko

- Dengan pertumbuhan, jumlah permintaan untuk membuat dan mengelola peran dan kebijakan baru meningkat. Menjadi lebih menantang untuk memahami konteks apa yang diperlukan untuk membuat izin secara manual untuk setiap aplikasi. Menetapkan kontrol pencegahan bertindak sebagai dasar dan membantu mencegah pengguna melakukan tindakan yang tidak diinginkan, bahkan jika mereka secara tidak sengaja diberi akses.
- Menerapkan kontrol pencegahan untuk mengakses kebijakan menyediakan lapisan tambahan untuk membantu melindungi data dan aset.

Kontrol proaktif

Kontrol proaktif adalah kontrol keamanan yang dirancang untuk mencegah penciptaan sumber daya yang tidak sesuai. Kontrol ini dapat mengurangi jumlah peristiwa keamanan yang ditangani oleh kontrol responsif dan detektif. Kontrol ini memastikan bahwa sumber daya yang digunakan sesuai sebelum digunakan; oleh karena itu, tidak ada peristiwa deteksi yang memerlukan respons atau remediasi.

Misalnya, Anda mungkin memiliki kontrol detektif yang memberi tahu Anda jika bucket Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) dapat diakses publik. Anda mungkin juga memiliki kontrol responsif yang memperbaikinya. Meskipun Anda sudah memiliki dua kontrol ini, Anda dapat menambahkan lapisan perlindungan lain dengan menambahkan kontrol proaktif. Melalui AWS CloudFormation, kontrol proaktif dapat mencegah pembuatan pembaruan bucket S3 apa pun yang mengaktifkan akses publik. Aktor ancaman masih dapat melewati kontrol ini dan menyebarkan atau memodifikasi sumber daya di luar. CloudFormation Dalam hal ini, detektif dan kontrol responsif akan memulihkan peristiwa keamanan.

Tinjau hal-hal berikut tentang jenis kontrol ini:

- Tujuan
- Proses
- Kasus penggunaan
- Teknologi
- Hasil bisnis

Tujuan

- Kontrol proaktif membantu Anda meningkatkan operasi keamanan dan proses kualitas.
- Kontrol proaktif dapat membantu Anda mematuhi kebijakan keamanan, standar, dan kewajiban peraturan atau kepatuhan.
- Kontrol proaktif dapat mencegah penciptaan sumber daya yang tidak sesuai.
- Kontrol proaktif dapat mengurangi jumlah temuan keamanan.
- Kontrol proaktif memberikan lapisan perlindungan lain terhadap pelaku ancaman yang melewati kontrol pencegahan dan mencoba menyebarkan sumber daya yang tidak patuh.
- Dalam kombinasi dengan kontrol preventif, detektif, dan responsif, kontrol proaktif dapat membantu Anda mengatasi potensi insiden keamanan.

Proses

Kontrol proaktif melengkapi kontrol pencegahan. Kontrol proaktif mengurangi risiko keamanan organisasi Anda dan menerapkan penerapan sumber daya yang sesuai. Kontrol ini mengevaluasi kepatuhan sumber daya sebelum sumber daya dibuat atau diperbarui. Kontrol proaktif umumnya diimplementasikan dengan menggunakan CloudFormation kait. Jika sumber daya gagal dalam

validasi kontrol proaktif, Anda dapat memilih untuk gagal dalam penerapan sumber daya atau menyajikan pesan peringatan. Berikut ini adalah beberapa tips dan praktik terbaik untuk membangun kontrol proaktif:

- Pastikan kontrol proaktif dipetakan sesuai dengan persyaratan kepatuhan organisasi Anda.
- Pastikan kontrol proaktif mengikuti praktik terbaik keamanan untuk layanan terkait.
- Gunakan CloudFormation StackSets atau solusi lain untuk menerapkan kontrol proaktif di beberapa Wilayah AWS atau akun.
- Pastikan pesan peringatan atau kegagalan yang terkait dengan kontrol proaktif eksplisit dan jelas. Ini membantu pengembang memahami alasan mengapa sumber daya tidak lulus evaluasi.
- Saat membuat kontrol proaktif baru, mulailah dalam mode amati. Ini berarti Anda mengirim pesan peringatan alih-alih gagal dalam penerapan sumber daya. Ini membantu Anda memahami dampak dari kontrol proaktif.
- Aktifkan login di Amazon CloudWatch Logs untuk kontrol proaktif.
- Jika Anda perlu memantau pemanggilan kontrol proaktif tertentu, gunakan EventBridge aturan Amazon dan berlangganan acara pemanggilan untuk hook. CloudFormation

Kasus penggunaan

- Mencegah penyebaran sumber daya yang tidak sesuai
- Memenuhi persyaratan kepatuhan
- Meningkatkan kualitas kode dengan menegakkan remediasi masalah keamanan sebelum penerapan
- Mengurangi downtime operasional yang terkait dengan perbaikan masalah keamanan setelah penerapan

Teknologi

CloudFormation kait

AWS CloudFormationmembantu Anda menyiapkan AWS sumber daya, menyediakannya dengan cepat dan konsisten, dan mengelolanya sepanjang siklus hidupnya di seluruh Akun AWS dan Wilayah. CloudFormation hook secara proaktif mengevaluasi konfigurasi sumber CloudFormation daya Anda sebelum digunakan. Jika sumber daya yang tidak sesuai ditemukan, ia mengembalikan status kegagalan. Berdasarkan mode kegagalan hook, CloudFormation dapat gagal operasi atau

menyajikan peringatan yang memungkinkan pengguna untuk melanjutkan penyebaran. Anda dapat menggunakan kait yang tersedia, atau Anda dapat mengembangkannya sendiri.

AWS Control Tower

AWS Control Towermembantu Anda mengatur dan mengatur lingkungan AWS multi-akun, mengikuti praktik terbaik preskriptif. AWS Control Tower menawarkan kontrol proaktif yang telah dikonfigurasi sebelumnya yang dapat Anda aktifkan di landing zone Anda. Jika landing zone Anda diatur AWS Control Tower, Anda dapat menggunakan kontrol proaktif opsional ini sebagai titik awal untuk organisasi Anda. Anda dapat membangun kontrol proaktif tambahan dan kustom sesuai CloudFormation kebutuhan.

Hasil bisnis

Kurang upaya dan kesalahan manusia

Kontrol proaktif mengurangi risiko kesalahan manusia yang mengarah pada penyebaran sumber daya yang tidak patuh. Mereka juga mengurangi upaya manusia di kemudian hari dalam siklus pengembangan karena mereka membuat pengembang mempertimbangkan keamanan sumber daya sebelum penerapan. Ini menerapkan praktik shift left untuk membangun sumber daya yang aman karena memaksa kepatuhan lebih awal dalam siklus hidup pengembangan.

Mengurangi biaya

Umumnya lebih mahal untuk memperbaiki masalah keamanan setelah penerapan. Mengidentifikasi dan memperbaiki masalah sebelumnya dalam siklus pengembangan mengurangi biaya pengembangan.

Penghematan waktu

Karena kontrol proaktif mencegah penyebaran sumber daya yang tidak sesuai, mereka mengurangi jumlah waktu yang Anda habiskan untuk melakukan triaging dan memperbaiki masalah keamanan. Mereka juga jumlah temuan keamanan, yang akan diidentifikasi oleh kontrol detektif nanti dalam siklus pengembangan.

Kepatuhan terhadap peraturan

Jika organisasi Anda perlu mematuhi peraturan internal atau industri, kontrol proaktif dapat membantu Anda tetap patuh dan menghindari hukuman pelanggaran.

Pengurangan risiko

Kontrol proaktif membantu pengembang menerapkan sumber daya yang sesuai dan dibangun dengan lebih aman, sehingga kontrol proaktif mengurangi risiko keamanan organisasi Anda.

Kontrol Detektif

Kontrol Detektif adalah kontrol keamanan yang dirancang untuk mendeteksi, mencatat, dan memperingatkan setelah suatu peristiwa terjadi. Detective control adalah bagian dasar dari kerangka kerja tata kelola. Pagar pembatas ini adalah garis pertahanan kedua, memberi tahu Anda tentang masalah keamanan yang melewati kontrol pencegahan.

Misalnya, Anda mungkin menerapkan kontrol detektif yang mendeteksi dan memberi tahu Anda jika bucket Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) dapat diakses publik. Meskipun Anda mungkin memiliki kontrol pencegahan yang menonaktifkan akses publik ke bucket S3 di tingkat akun dan kemudian menonaktifkan akses melalui SCP, aktor ancaman dapat menghindari kontrol pencegahan ini dengan masuk sebagai pengguna administratif. Dalam situasi ini, kontrol detektif dapat mengingatkan Anda tentang kesalahan konfigurasi dan potensi ancaman.

Tinjau hal-hal berikut tentang jenis kontrol ini:

- Tujuan
- Proses
- Kasus penggunaan
- Teknologi
- Hasil bisnis

Tujuan

- Kontrol Detektif membantu Anda meningkatkan proses operasi keamanan dan proses kualitas.
- Kontrol Detektif membantu Anda memenuhi kewajiban peraturan, hukum, atau kepatuhan.
- Detective control menyediakan tim operasi keamanan dengan visibilitas untuk menanggapi masalah keamanan, termasuk ancaman lanjutan yang melewati kontrol pencegahan.
- Kontrol detektif dapat membantu Anda mengidentifikasi respons yang tepat terhadap masalah keamanan dan potensi ancaman.

Proses

Anda menerapkan kontrol detektif yang diterapkan dalam dua fase. Pertama, Anda mengatur sistem untuk mencatat peristiwa dan status sumber daya ke lokasi terpusat, seperti Amazon CloudWatch Logs. Setelah pencatatan terpusat dilakukan, Anda menganalisis log tersebut untuk mendeteksi anomali yang mungkin mengindikasikan ancaman. Setiap analisis adalah kontrol yang dipetakan kembali ke persyaratan dan kebijakan awal Anda. Misalnya, Anda dapat membuat kontrol detektif yang mencari log untuk pola tertentu dan menghasilkan peringatan jika cocok. Kontrol Detektif digunakan oleh tim keamanan untuk meningkatkan visibilitas mereka secara keseluruhan terhadap ancaman dan risiko yang mungkin dihadapi sistem mereka.

Kasus penggunaan

Deteksi perilaku mencurigakan

Kontrol Detektif membantu mengidentifikasi aktivitas anomali apa pun, seperti kredensi pengguna istimewa yang dikompromikan atau akses ke atau eksfiltrasi data sensitif. Kontrol ini adalah faktor reaktif penting yang dapat membantu perusahaan Anda mengidentifikasi dan memahami ruang lingkup aktivitas anomali.

Deteksi penipuan

Kontrol ini membantu mendeteksi dan mengidentifikasi ancaman di dalam perusahaan Anda, seperti pengguna yang menghindari kebijakan dan melakukan transaksi yang tidak sah.

Kepatuhan

Kontrol Detektif membantu Anda memenuhi persyaratan kepatuhan, seperti Payment Card Industry Data Security Standard (PCI DSS), dan dapat membantu mencegah pencurian identitas. Kontrol ini dapat membantu Anda menemukan dan melindungi informasi sensitif yang tunduk pada kepatuhan terhadap peraturan, seperti informasi yang dapat diidentifikasi secara pribadi.

Analisis otomatis

Kontrol Detektif dapat secara otomatis menganalisis log untuk mendeteksi anomali dan indikator lain dari aktivitas yang tidak sah.

Anda dapat secara otomatis menganalisis log dari berbagai sumber seperti AWS CloudTrail log, Log Aliran VPC, dan log Sistem Nama Domain (DNS), untuk indikasi aktivitas yang berpotensi berbahaya.

Untuk membantu organisasi, agregat peringatan keamanan atau temuan dari beberapa Layanan AWS ke lokasi terpusat.

Teknologi

Kontrol detektif umum adalah menerapkan satu atau lebih layanan pemantauan, yang dapat menganalisis sumber data, seperti log, untuk mengidentifikasi ancaman keamanan. Di dalamnya AWS Cloud, Anda dapat menganalisis sumber seperti AWS CloudTrail log, log akses Amazon S3, dan log aliran Amazon Virtual Private Cloud untuk membantu mendeteksi aktivitas yang tidak biasa. AWS Layanan keamanan, seperti Amazon GuardDuty, Amazon Detective AWS Security Hub, dan Amazon Macie memiliki fungsi pemantauan bawaan.

GuardDuty dan Security Hub

Amazon GuardDuty menggunakan intelijen ancaman, pembelajaran mesin, dan teknik deteksi anomali untuk terus memantau sumber log Anda untuk aktivitas berbahaya atau tidak sah. Dasbor memberikan wawasan tentang kesehatan waktu nyata Akun AWS dan beban kerja Anda. Anda dapat berintegrasi GuardDuty dengan AWS Security Hub, layanan manajemen postur keamanan cloud yang memeriksa kepatuhan terhadap praktik terbaik, mengumpulkan peringatan, dan memungkinkan remediasi otomatis. GuardDuty mengirimkan temuan ke Security Hub sebagai cara untuk memusatkan informasi. Anda dapat mengintegrasikan Security Hub lebih lanjut dengan solusi informasi keamanan dan manajemen acara (SIEM) untuk memperluas kemampuan pemantauan dan peringatan bagi organisasi Anda.

Macie

Amazon Macie adalah layanan keamanan data dan privasi data yang dikelola sepenuhnya yang menggunakan pembelajaran mesin dan pencocokan pola untuk membantu menemukan dan melindungi data sensitif. AWS Berikut ini adalah beberapa kontrol detektif dan fitur yang tersedia di Macie:

- Macie memeriksa inventaris bucket dan semua objek yang disimpan di Amazon S3. Informasi ini dapat disajikan dalam satu tampilan dasbor, memberikan visibilitas dan membantu Anda mengevaluasi keamanan bucket.
- Untuk menemukan data sensitif, Macie menggunakan pengidentifikasi data terkelola bawaan dan juga mendukung pengidentifikasi data khusus.
- Macie terintegrasi secara native dengan alat dan lainnya Layanan AWS . Misalnya, Macie mengeluarkan temuan sebagai EventBridge peristiwa Amazon, yang secara otomatis dikirim ke Security Hub.

Berikut ini adalah praktik terbaik untuk mengonfigurasi kontrol detektif di Macie:

- Aktifkan Macie di semua akun. Dengan menggunakan fitur manajemen yang didelegasikan, aktifkan Macie di beberapa akun dengan menggunakan. AWS Organizations
- Gunakan Macie untuk mengevaluasi postur keamanan bucket S3 di akun Anda. Ini membantu mencegah kehilangan data dengan memberikan visibilitas ke lokasi dan akses data. Untuk informasi selengkapnya, lihat Menganalisis postur keamanan Amazon S3 Anda (dokumentasi Macie).
- Otomatiskan penemuan data sensitif di bucket S3 Anda dengan menjalankan dan menjadwalkan pekerjaan pemrosesan dan penemuan data otomatis. Ini memeriksa bucket S3 untuk data sensitif pada jadwal reguler.

AWS Config

AWS Configmengaudit dan mencatat kepatuhan AWS sumber daya. AWS Config menemukan AWS sumber daya yang ada dan menghasilkan inventaris lengkap, bersama dengan detail konfigurasi setiap sumber daya. Jika ada perubahan konfigurasi, ia mencatat perubahan tersebut dan memberikan pemberitahuan. Ini dapat membantu Anda mendeteksi dan mengembalikan perubahan infrastruktur yang tidak sah. Anda dapat menggunakan aturan AWS terkelola dan dapat membuat aturan khusus.

Berikut ini adalah praktik terbaik untuk mengonfigurasi kontrol detektif di: AWS Config

- Aktifkan AWS Config untuk setiap akun anggota di organisasi dan untuk masing-masing Wilayah AWS yang berisi sumber daya yang ingin Anda lindungi.
- Siapkan peringatan Amazon Simple Notification Service (Amazon SNS) untuk setiap perubahan konfigurasi.
- Simpan data konfigurasi dalam bucket S3 dan gunakan Amazon Athena untuk menganalisisnya.
- Otomatiskan remediasi sumber daya yang tidak patuh dengan menggunakan Otomasi, kemampuan. AWS Systems Manager
- Gunakan EventBridge atau Amazon SNS untuk menyiapkan notifikasi tentang sumber daya yang tidak AWS sesuai.

Trusted Advisor

AWS Trusted Advisordapat digunakan sebagai layanan untuk kontrol detektif. Melalui serangkaian pemeriksaan, Trusted Advisor mengidentifikasi area di mana Anda dapat mengoptimalkan infrastruktur Anda, meningkatkan kinerja dan keamanan, atau mengurangi biaya. Trusted Advisor memberikan rekomendasi berdasarkan praktik AWS terbaik yang dapat Anda ikuti untuk meningkatkan layanan dan sumber daya Anda. Paket Business and Enterprise Support menyediakan akses ke semua pemeriksaan yang tersedia untuk pilar AWS Well-Architected Framework.

Berikut ini adalah praktik terbaik untuk mengonfigurasi kontrol detektif di: Trusted Advisor

- Tinjau ringkasan level cek
- Menerapkan rekomendasi khusus sumber daya untuk peringatan dan status kesalahan.
- Periksa Trusted Advisor sering untuk secara aktif meninjau dan menerapkan rekomendasinya.

Amazon Inspector

Amazon Inspector adalah layanan manajemen kerentanan otomatis yang, setelah diaktifkan, terus memindai beban kerja Anda untuk setiap eksposur jaringan atau kerentanan perangkat lunak yang tidak diinginkan. Ini mengontekstualisasikan temuan menjadi skor risiko yang dapat membantu Anda menentukan langkah selanjutnya, seperti memulihkan atau mengonfirmasi status kepatuhan.

Berikut ini adalah praktik terbaik untuk mengonfigurasi kontrol detektif di Amazon Inspector:

- Aktifkan Amazon Inspector di semua akun dan integrasikan ke dalam EventBridge dan Security Hub untuk mengonfigurasi pelaporan dan pemberitahuan untuk kerentanan keamanan.
- Prioritaskan remediasi dan tindakan lain berdasarkan skor risiko Amazon Inspector.

Hasil bisnis

Kurang upaya dan kesalahan manusia

Anda dapat mencapai otomatisasi dengan menggunakan infrastruktur sebagai kode (IAc). Mengotomatiskan penyebaran, konfigurasi layanan dan alat pemantauan dan remediasi mengurangi risiko kesalahan manual dan mengurangi jumlah waktu dan upaya yang diperlukan untuk mengukur kontrol detektif ini. Otomasi membantu pengembangan runbook keamanan dan mengurangi operasi manual untuk analis keamanan. Ulasan reguler membantu menyetel alat otomatisasi dan terus mengulangi dan meningkatkan kontrol detektif.

Tindakan yang tepat terhadap potensi ancaman

Menangkap dan menganalisis peristiwa dari log dan metrik sangat penting untuk mendapatkan visibilitas. Ini membantu analis bertindak atas peristiwa keamanan dan potensi ancaman untuk membantu mengamankan beban kerja Anda. Mampu dengan cepat mengidentifikasi kerentanan mana yang ada membantu analis mengambil tindakan yang tepat untuk mengatasi dan memperbaikinya.

Respon insiden dan penanganan investigasi yang lebih baik

Otomatisasi alat kontrol detektif dapat meningkatkan kecepatan deteksi, investigasi, dan pemulihan. Peringatan dan pemberitahuan otomatis berdasarkan kondisi yang ditentukan memungkinkan analis keamanan untuk menyelidiki dan merespons dengan tepat. Faktor-faktor responsif ini dapat membantu Anda mengidentifikasi dan memahami ruang lingkup aktivitas anomali.

Kontrol responsif

Kontrol responsif adalah kontrol keamanan yang dirancang untuk mendorong perbaikan efek samping atau penyimpangan dari garis dasar keamanan Anda. Contoh kontrol responsif teknis termasuk menambal sistem, mengkarantina virus, mematikan proses, atau me-reboot sistem.

Tinjau hal-hal berikut tentang jenis kontrol ini:

- Tujuan
- Proses
- Kasus penggunaan
- Teknologi
- Hasil bisnis

Tujuan

- Kontrol responsif dapat membantu Anda membuat runbook untuk jenis serangan umum, seperti phishing atau brute force.
- Kontrol responsif dapat menerapkan respons otomatis terhadap potensi masalah keamanan.
- Kontrol responsif dapat secara otomatis memulihkan tindakan yang tidak diinginkan atau tidak disetujui pada AWS sumber daya, seperti menghapus bucket S3 yang tidak terenkripsi.

- Kontrol responsif dapat diatur untuk bekerja dengan kontrol pencegahan dan detektif untuk menciptakan pendekatan holistik dan proaktif untuk mengatasi potensi insiden keamanan.

Proses

Detective control adalah prasyarat untuk membangun kontrol responsif. Anda harus dapat mendeteksi masalah keamanan sebelum Anda dapat memperbaikinya. Anda kemudian dapat membuat kebijakan atau tanggapan terhadap masalah keamanan. Misalnya, jika terjadi serangan brute force, proses remediasi akan dilaksanakan. Setelah proses remediasi ada, kemudian dapat diotomatisasi dan dijalankan sebagai skrip dengan menggunakan bahasa pemrograman, seperti skrip shell.

Pertimbangkan apakah kontrol responsif dapat merusak beban kerja produksi yang ada. Misalnya, jika kontrol keamanan detektif adalah bucket S3 tidak boleh diakses publik dan remediasi mematikan akses publik untuk Amazon S3, ini dapat memiliki implikasi signifikan bagi perusahaan Anda dan pelanggannya. Jika bucket S3 melayani situs web publik, mematikan akses publik dapat menyebabkan pemadaman. Database adalah contoh serupa. Jika database tidak boleh diakses publik melalui internet, mematikan akses publik dapat memengaruhi konektivitas ke aplikasi.

Kasus penggunaan

- Respons otomatis terhadap peristiwa keamanan yang terdeteksi
- Remediasi otomatis dari kerentanan keamanan yang terdeteksi
- Kontrol pemulihan otomatis untuk mengurangi waktu henti operasional

Teknologi

Security Hub

AWS Security Hubsecara otomatis mengirimkan semua temuan baru dan semua pembaruan temuan yang ada ke EventBridge sebagai peristiwa. Anda juga dapat membuat tindakan kustom yang mengirimkan temuan dan hasil wawasan yang dipilih EventBridge. Anda dapat mengonfigurasi EventBridge untuk merespons setiap jenis acara. Acara dapat memulai AWS Lambda fungsi yang melakukan tindakan remediasi.

AWS Config

AWS Configmenggunakan aturan untuk mengevaluasi AWS sumber daya Anda dan membantu Anda memulihkan sumber daya yang tidak sesuai. AWS Config menerapkan remediasi menggunakan AWS Systems Manager Otomasi. Dalam dokumen Otomasi, Anda menentukan tindakan yang ingin Anda lakukan pada sumber daya yang AWS Config menentukan tidak patuh. Setelah membuat dokumen Otomasi, Anda dapat menggunakannya di Systems Manager melalui AWS Management Console atau dengan menggunakan API. Anda dapat memilih untuk memulihkan sumber daya yang tidak sesuai secara manual atau otomatis.

Hasil bisnis

Minimalkan kehilangan data

Setelah insiden keamanan siber, menggunakan kontrol keamanan responsif dapat membantu meminimalkan kehilangan data dan kerusakan pada sistem atau jaringan. Kontrol responsif juga dapat membantu memulihkan sistem dan proses bisnis penting secepat mungkin, menambah ketahanan beban kerja Anda.

Mengurangi biaya

Otomatisasi mengurangi biaya yang terkait dengan sumber daya manusia karena anggota tim tidak harus secara manual menanggapi insiden atau mengelolanya case-by-case secara manual.

Langkah selanjutnya

Setelah membaca panduan ini, Anda harus terbiasa dengan empat jenis kontrol keamanan, memahami bagaimana mereka adalah bagian dari kerangka tata kelola keamanan Anda, dan bersiaplah untuk mulai menerapkan dan mengotomatiskan kontrol keamanan di. AWS Cloud Untuk informasi lebih lanjut dan, kami sarankan Anda meninjau referensi yang termasuk dalam Sumber daya bagian ini.

Kami juga menyarankan Anda mengambil langkah-langkah berikut untuk menilai keamanan infrastruktur cloud Anda dan mulai menerapkan kontrol keamanan:

1. Aktifkan dan konfigurasikanAWS Security Hub. Sebagai praktik terbaik, kami merekomendasikan untuk mengaktifkan kontrol standar yang tersedia. Untuk informasi selengkapnya, lihat Standar dan kontrol keamanan (dokumentasi Security Hub).
2. Aktifkan dan konfigurasikanAWS Config. Untuk informasi selengkapnya, lihat Memulai (AWS Configdokumentasi).
3. Menggunakan Layanan AWS seperti Security Hub, Amazon Macie,, AWS ConfigAWS Trusted Advisor, dan Amazon Inspector, menilai organisasi dan infrastruktur akun Anda, mengidentifikasi area yang perlu ditingkatkan, serta meninjau serta rekomendasi dalam layanan ini. Gunakan fitur pemeriksaan keamanan di Security Hub untuk menghasilkan skor keamanan untuk standar keamanan. Untuk informasi selengkapnya, lihat Menentukan skor keamanan (dokumentasi Security Hub).
4. Menerapkan kontrol keamanan preventif, proaktif, detektif, dan responsif berdasarkan perbaikan yang diidentifikasi.
5. Melakukan penilaian keamanan tindak lanjut untuk mengevaluasi efektivitas kontrol keamanan yang diterapkan. Di Security Hub, tentukan apakah skor keamanan telah meningkat. Iterasi untuk meningkatkan atau menambahkan kontrol keamanan baru.
6. Tetapkan irama reguler untuk melakukan penilaian keamanan, seperti tahunan.

Pertanyaan yang Sering Diajukan

Apa yang harus saya fokuskan jika saya memiliki waktu dan sumber daya yang terbatas dan tidak dapat menerapkan semua jenis kontrol ini?

Kami merekomendasikan implementasiAWS Security Hub. Security Hub memiliki seperangkat kontrol keamanan otomatis yang disebut standar Praktik Terbaik Keamanan AWS Dasar (dokumentasi Security Hub). Ini adalah serangkaian praktik terbaik keamanan yang dikuratori yang dikelola oleh pakar AWS keamanan. Anda dapat menjalankan kontrol standar ini secara terus menerus, setiap kali ada perubahan pada sumber daya terkait, atau secara berkala, pada jadwal reguler. Setiap kontrol memiliki skor keparahan tertentu untuk membantu Anda memprioritaskan upaya remediasi Anda. Untuk informasi selengkapnya, lihat Menjalankan pemeriksaan keamanan (dokumentasi Security Hub). Jika Anda menggunakanAWS Control Tower, Anda juga dapat meninjau dan memilih untuk mengaktifkan kontrol pencegahan, detektif, dan proaktifnya.

Sumber daya

Dokumentasi AWS

- AWSArsitektur Referensi Keamanan (AWSSRA)
- AWSPerspektif keamanan CAF
- Praktik Terbaik untuk keamanan, identitas, dan kepatuhan
- Respon Keamanan Otomatis pada AWS (AWSSolusi)
  - Halaman arahan solusi
  - Panduan implementasi

AWSposting blog

- Panduan Identitas - Kontrol pencegahan dengan AWS Identitas - SCP
- Cara menerapkan kebijakan kontrol layanan hanya-baca (SCP) untuk akun di AWS Organizations
- Praktik Terbaik untuk Kebijakan Kontrol AWS Organizations Layanan di Lingkungan Multi-Akun
- Pertahankan kepatuhan menggunakan Kebijakan Kontrol Layanan dan pastikan selalu diterapkan
- Kapan dan di mana menggunakan batas izin IAM
- Secara proaktif menjaga sumber daya tetap aman dan sesuai dengan kait AWS CloudFormation

Sumber daya lainnya

- Matriks Kontrol Cloud (CCM) (Aliansi Keamanan Cloud)
- Contoh batas izin () GitHub

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
Kontrol proaktif	Kami menambahkan informasi tentang kontrol proaktif ke panduan ini, termasuk bagian Kontrol proaktif.	Desember 4, 2023
Publikasi awal	—	Desember 12, 2022

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 Postgre -Compatible Edition. SQL
- 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 (RDSAmazon) 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: Migrasi a Microsoft Hyper-V aplikasi untuk 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.

ACID

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

SQLFungsi 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 AWS di 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 pemrosesan atau modifikasi 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 CAFMengatur panduan ke dalam enam bidang 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 berikan panduan untuk pengembangan, pelatihan, dan komunikasi orang untuk membantu mempersiapkan organisasi untuk adopsi cloud yang sukses. Untuk informasi lebih lanjut, lihat situs AWS CAFweb dan AWS CAFwhitepaper.

AWS Kerangka Kualifikasi Beban Kerja ()AWS WQF

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

B

bot buruk

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

BCP

Lihat perencanaan kontinuitas bisnis.

grafik perilaku

Pandangan interaktif yang terpadu tentang perilaku dan interaksi sumber daya dari waktu ke waktu. Anda dapat menggunakan grafik perilaku dengan Amazon Detective untuk memeriksa upaya logon yang gagal, API panggilan 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

CAF

Lihat Kerangka Adopsi AWS Cloud.

penyebaran kenari

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

CCoE

Lihat Cloud Center of Excellence.

CDC

Lihat mengubah pengambilan data.

ubah pengambilan data (CDC)

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

rekayasa kekacauan

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

CI/CD

Lihat integrasi berkelanjutan dan pengiriman berkelanjutan.

klasifikasi

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

Enkripsi sisi klien

Enkripsi data secara lokal, sebelum target Layanan AWS menerimanya.

Pusat Keunggulan Cloud (CCoE)

Tim multi-disiplin yang mendorong upaya adopsi cloud di seluruh organisasi, termasuk mengembangkan praktik terbaik cloud, memobilisasi sumber daya, menetapkan jadwal migrasi, dan memimpin organisasi melalui transformasi skala besar. Untuk informasi selengkapnya, lihat CCoEposting 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, mendefinisikanCCoE, membuat model operasi)
- Migrasi — Migrasi aplikasi individual
- Re-invention — Mengoptimalkan produk dan layanan, dan berinovasi di cloud

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

CMDB

Lihat database manajemen konfigurasi.

repositori kode

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

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

cache dingin

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

data dingin

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

visi komputer (CV)

Bidang AI yang menggunakan pembelajaran mesin untuk menganalisis dan mengekstrak informasi dari format visual seperti gambar dan video digital. Misalnya, AWS Panorama menawarkan perangkat yang menambahkan CV ke jaringan kamera lokal, dan Amazon SageMaker menyediakan algoritme pemrosesan gambar untuk CV.

konfigurasi drift

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

database manajemen konfigurasi (CMDB)

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

paket kesesuaian

Kumpulan AWS Config aturan dan tindakan remediasi yang dapat Anda kumpulkan untuk menyesuaikan kepatuhan dan pemeriksaan keamanan Anda. Anda dapat menerapkan paket kesesuaian sebagai entitas tunggal di Akun AWS dan Wilayah, atau di seluruh organisasi, dengan menggunakan templat. YAML 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 database (DML)

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

DDL

Lihat bahasa definisi database.

ansambel yang dalam

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

pembelajaran mendalam

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

defense-in-depth

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

administrator yang didelegasikan

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

deployment

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

lingkungan pengembangan

Lihat lingkungan.

kontrol detektif

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

pemetaan aliran nilai pengembangan () DVSM

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

lean. 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 bagaimana Anda dapat menggunakan desain berbasis domain dengan pola ara pencekik, lihat Memodernisasi Microsoft lama. ASP NET(ASMX) layanan web secara bertahap dengan menggunakan kontainer 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 to AWS Identity and Access Management (IAM). Akun atau prinsipal ini dapat terhubung ke layanan endpoint Anda secara pribadi dengan membuat titik akhir antarmuka. VPC Untuk informasi selengkapnya, lihat Membuat layanan titik akhir di dokumentasi Amazon Virtual Private Cloud (AmazonVPC).

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 AWS CAF keamanan termasuk 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. EDAdilakukan 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

Memberikan sejumlah kecil contoh yang menunjukkan tugas dan output yang diinginkan sebelum memintanya untuk melakukan tugas serupa. LLM 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. FMsmampu 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 IAM izin. 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 untuk 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 IAM prinsip yang mendefinisikan izin mereka dalam lingkungan. AWS Cloud

aplikasi idle

Aplikasi yang memiliki rata-rata CPU dan penggunaan memori 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, a 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 selengkapnya, lihat Membangun strategi transformasi digital Internet of Things (IIoT) industri.

inspeksi VPC

Dalam arsitektur AWS multi-akun, terpusat VPC yang mengelola inspeksi lalu lintas jaringan antara VPCs (dalam hal 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. ITILmenyediakan fondasi untukITSM.

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 ITSM alat, 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. An LLM dapat melakukan banyak 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.

MAP

Lihat Program Percepatan Migrasi.

mekanisme

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

akun anggota

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

MES

Lihat sistem eksekusi manufaktur.

Transportasi Telemetri Antrian Pesan () MQTT

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

layanan mikro

Layanan kecil dan independen yang berkomunikasi melalui definisi yang 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. MAPmencakup metodologi migrasi untuk mengeksekusi migrasi lama dengan cara metodis dan seperangkat alat untuk mengotomatiskan dan mempercepat skenario migrasi umum.

migrasi dalam skala

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

pabrik migrasi

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

metadata migrasi

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

pola migrasi

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

Penilaian Portofolio Migrasi (MPA)

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

Penilaian Kesiapan Migrasi () MRA

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

strategi migrasi

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

ML

Lihat pembelajaran mesin.

modernisasi

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

penilaian kesiapan modernisasi

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

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

aplikasi monolitik (monolit)

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

MPA

Lihat Penilaian Portofolio Migrasi.

MQTT

Lihat Transportasi Telemetri Antrian Pesan.

klasifikasi multiclass

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

infrastruktur yang bisa berubah

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

O

OAC

Lihat kontrol akses asal.

OAI

Lihat identitas akses asal.

OCM

Lihat manajemen perubahan organisasi.

migrasi offline

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

OI

Lihat integrasi operasi.

OLA

Lihat perjanjian tingkat operasional.

migrasi online

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

OPC-UA

Lihat Komunikasi Proses Terbuka - Arsitektur Terpadu.

Komunikasi Proses Terbuka - Arsitektur Terpadu (OPC-UA)

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

perjanjian tingkat operasional () OLA

Perjanjian yang menjelaskan apa yang dijanjikan oleh 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 AWS Well-Architected.

teknologi operasional (OT)

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

integrasi operasi (OI)

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

jejak organisasi

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

manajemen perubahan organisasi (OCM)

Kerangka kerja untuk mengelola transformasi bisnis utama yang mengganggu dari perspektif orang, budaya, dan kepemimpinan. OCMmembantu 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 OCMpanduannya.

kontrol akses asal (OAC)

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

identitas akses asal (OAI)

Di CloudFront, opsi untuk membatasi akses untuk mengamankan konten Amazon S3 Anda. Saat Anda menggunakanOAI, 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, a 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 IAM manajemen yang dilampirkan pada IAM prinsipal untuk menetapkan izin maksimum yang dapat dimiliki pengguna atau peran. Untuk informasi selengkapnya, lihat Batas izin dalam IAM dokumentasi.

Informasi Identifikasi Pribadi () PII

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

PII

Lihat informasi yang dapat diidentifikasi secara pribadi.

buku pedoman

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

PLC

Lihat pengontrol logika yang dapat diprogram.

PLM

Lihat manajemen siklus hidup produk.

kebijakan

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

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

kontrol preventif

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

principal

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

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 DNS kueri 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 LLMprompt 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 layanan mikro berbasis MES, layanan mikro dapat mempublikasikan pesan peristiwa ke saluran yang dapat berlangganan oleh 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 SQL relasional.

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

RACImatriks

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

RAG

Lihat Retrieval Augmented Generation.

ransomware

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

RASCImatriks

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). Jenis dukungan (S) adalah opsional. Jika Anda menyertakan dukungan, matriks disebut RASCImatriks, dan jika Anda mengecualikannya, itu disebut RACImatriks.

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.

Pengambilan Generasi Augmented () RAG

Teknologi AI generatif di mana LLMreferensi sumber data otoritatif yang berada di luar sumber data pelatihannya sebelum menghasilkan respons. Misalnya, RAG model 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 SQL ekspresi dasar dan fleksibel yang telah menetapkan aturan akses. RCACterdiri 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 (SSO) gabungan, sehingga pengguna dapat masuk ke AWS Management Console atau memanggil AWS API operasi tanpa Anda harus membuat pengguna untuk semua orang di IAM organisasi Anda. Untuk informasi lebih lanjut tentang federasi SAML berbasis 2.0, lihat Tentang federasi SAML berbasis 2.0 dalam dokumentasi. IAM

SCADA

Lihat kontrol pengawasan dan akuisisi data.

SCP

Lihat kebijakan kontrol layanan.

Rahasia

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

keamanan dengan desain

Pendekatan rekayasa sistem yang memperhitungkan keamanan melalui seluruh proses pengembangan.

kontrol keamanan

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

pengerasan keamanan

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

informasi keamanan dan manajemen acara (SIEM) sistem

Alat dan layanan yang menggabungkan sistem manajemen informasi keamanan (SIM) dan manajemen peristiwa keamanan (SEM). Sebuah SIEM sistem 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 VPC keamanan, menambal EC2 instans 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 SCPsmenentukan 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

Titik masuk untuk sebuah Layanan AWS. URL 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.

satu titik kegagalan (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 Microsoft lama. ASP NET(ASMX) layanan web secara bertahap dengan menggunakan kontainer dan Amazon API Gateway.

subnet

Berbagai alamat IP di AndaVPC. 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 LLMuntuk 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.

VPCmengintip

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

kerentanan

Kelemahan perangkat lunak atau perangkat keras yang membahayakan keamanan sistem.

W

cache hangat

Cache buffer yang berisi data terkini dan relevan yang sering diakses. Instance database dapat membaca dari cache buffer, yang lebih cepat daripada membaca dari memori utama atau disk.

data hangat

Data yang jarang diakses. Saat menanyakan jenis data ini, kueri yang cukup lambat biasanya dapat diterima.

fungsi jendela

SQLFungsi 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.

WORM

Lihat menulis sekali, baca banyak.

WQF

Lihat AWSKerangka 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

LLMMemberikan instruksi untuk melakukan tugas tetapi tidak ada contoh (bidikan) yang dapat membantu membimbingnya. LLMHarus 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 rata-rata CPU 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.