Menerapkan strategi kontrol bot pada AWS

AWS Bimbingan Preskriptif

AWS Bimbingan Preskriptif: Menerapkan strategi kontrol bot pada AWS

Table of Contents

Menerapkan strategi kontrol bot pada AWS

Amazon Web Services (kontributor)

Februari 2024 (riwayat dokumen)

Internet seperti yang kita tahu tidak akan mungkin tanpa bot. Bot menjalankan tugas otomatis melalui internet dan mensimulasikan aktivitas atau interaksi manusia. Mereka memungkinkan bisnis untuk membangun efisiensi ke dalam proses dan tugas. Bot yang berguna, seperti perayap web, mengindeks informasi di internet dan membantu kami dengan cepat menemukan informasi yang paling relevan untuk permintaan pencarian kami. Bot adalah mekanisme yang baik untuk meningkatkan bisnis dan memberikan nilai kepada perusahaan. Namun, seiring berjalannya waktu, aktor jahat mulai menggunakan bot sebagai sarana untuk menyalahgunakan sistem dan aplikasi yang ada dengan cara baru dan kreatif.

Botnet adalah mekanisme paling terkenal untuk skala bot dan dampaknya. Botnet adalah jaringan bot yang terinfeksi oleh malware dan berada di bawah kendali satu pihak, yang dikenal sebagai bot herder atau operator bot. Dari satu titik pusat, operator dapat memerintahkan setiap komputer di botnetnya untuk secara bersamaan melakukan tindakan terkoordinasi, itulah sebabnya botnet juga disebut sebagai sistem command-and-control (C2).

Skala botnet bisa jutaan bot. Botnet membantu operator untuk melakukan tindakan skala besar. Karena botnet tetap berada di bawah kendali operator jarak jauh, mesin yang terinfeksi dapat menerima pembaruan dan mengubah perilaku mereka dengan cepat. Akibatnya, untuk keuntungan finansial yang signifikan, sistem C2 dapat menyewa akses ke segmen botnet mereka di pasar gelap.

Prevalensi botnet terus tumbuh. Hal ini dianggap oleh para ahli sebagai alat favorit aktor jahat. Mirai adalah salah satu botnet terbesar. Ini muncul pada tahun 2016, masih beroperasi, dan diperkirakan telah menginfeksi hingga 350.000 perangkat Internet of Things (IoT). Botnet ini telah diadaptasi dan digunakan untuk berbagai jenis kegiatan, termasuk serangan distributed denial of service (DDoS). Baru-baru ini, aktor jahat mencoba untuk lebih mengaburkan aktivitas mereka dan sumber lalu lintas mereka dengan mendapatkan alamat IP melalui penggunaan layanan proxy perumahan. Ini menciptakan peer-to-peer sistem yang saling berhubungan yang sah yang menambah kecanggihan aktivitas dan membuatnya lebih menantang untuk dideteksi dan dikurangi.

Dokumen ini berfokus pada lanskap bot, pengaruhnya terhadap aplikasi Anda, dan strategi serta opsi mitigasi yang tersedia. Panduan preskriptif ini dan praktik terbaiknya membantu Anda memahami dan mengurangi berbagai jenis serangan bot. Selain itu, panduan ini menjelaskan Layanan AWS

dan fitur yang mendukung strategi mitigasi bot dan bagaimana masing-masing dapat membantu Anda melindungi aplikasi Anda. Ini juga mencakup ikhtisar pemantauan bot dan praktik terbaik untuk mengoptimalkan biaya solusi.

Memahami ancaman dan operasi bot

Menurut Security Today, lebih dari 47% dari semua lalu lintas di internet disebabkan oleh bot. Ini termasuk bagian bot yang bermanfaat, yang mengidentifikasi diri dan memberikan nilai. Sekitar 30% lalu lintas bot adalah bot tak dikenal yang melakukan aktivitas jahat, seperti serangan DDo S, scalping tiket, pengikisan inventaris, atau penimbunan. Majalah Keamanan melaporkan peningkatan 300% dalam peristiwa DDo S volumetrik selama paruh pertama tahun 2023. Ini membuat topik ini lebih relevan, dan itu membuat pengetahuan tentang alat dan teknologi pencegahan dan pelindung yang tersedia menjadi lebih penting.

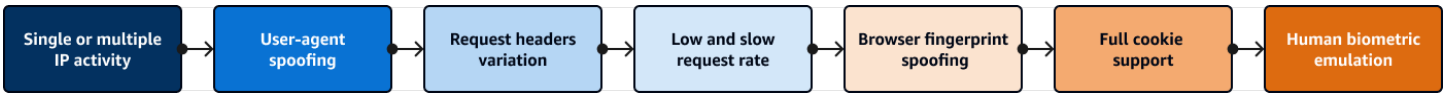
Tabel berikut mengkategorikan berbagai jenis aktivitas bot dan dampak bisnis yang dapat dimiliki masing-masing. Ini tidak dimaksudkan untuk menjadi daftar yang luas; ini adalah ringkasan dari aktivitas bot yang paling umum. Ini menyoroti pentingnya pemantauan dan kontrol mitigasi. Untuk daftar ekstensif ancaman bot, kunjungi buku pegangan ancaman otomatis terhadap aplikasi OWASP (situs web OWASP).

Jenis aktivitas bot	Deskripsi	Potensi dampak
Pengikisan konten	Menyalin konten berpemilik untuk digunakan oleh situs pihak ketiga	Dampak terhadap SEO Anda karena duplikasi konten, dampak merek, dan masalah kinerja yang disebabkan oleh pencakar agresif
Isian kredensi	Menguji database kredensi yang dicuri di situs web Anda untuk mendapatkan akses atau memvalidasi informasi	Masalah bagi pengguna, seperti penipuan dan penguncian akun, yang meningkatkan kueri dukungan dan mengurangi kepercayaan merek
Retak kartu	Menguji database data kartu kredit curian untuk memvalida si atau melengkapi informasi yang hilang	Masalah bagi pengguna, seperti pencurian identitas dan penipuan, dan kerusakan skor penipuan Anda

Jenis aktivitas bot	Deskripsi	Potensi dampak
Penolakan layanan	Meningkatkan lalu lintas ke situs web tertentu untuk memperlambat respons atau membuatnya tidak tersedia untuk lalu lintas yang sah	Kehilangan pendapatan dan kerusakan reputasi
Pembuatan akun	Pembuatan beberapa akun dengan tujuan penyalahg unaan atau keuntungan finansial	Pertumbuhan yang terhambat dan analisis pemasaran yang miring
Scalping	Mendapatkan barang ketersediaan terbatas, sering tiket, lebih dari konsumen asli	Kehilangan pendapatan dan masalah bagi pengguna, seperti kurangnya akses ke barang yang dijual

Bagaimana botnet beroperasi

Taktik, teknik, dan prosedur (TTP) operator botnet telah berkembang pesat dari waktu ke waktu. Mereka harus mengikuti teknologi deteksi dan mitigasi yang dikembangkan oleh perusahaan. Gambar berikut menunjukkan evolusi ini. Botnet dimulai hanya dengan menggunakan alamat IP sebagai alat operasi, dan mereka akhirnya berevolusi untuk menggunakan emulasi biometrik manusia yang canggih. Kecanggihan ini mahal, dan tidak semua botnet menggunakan alat paling canggih. Ada campuran operator di internet, dan mereka mungkin mengevaluasi alat terbaik untuk pekerjaan itu untuk memberikan pengembalian investasi yang baik. Salah satu tujuan dalam pertahanan bot adalah membuat aktivitas botnet menjadi mahal sehingga target tidak lagi layak.



Umumnya, bot dikategorikan sebagai umum atau ditargetkan:

- Bot umum — Bot ini mengidentifikasi diri sendiri dan tidak akan mencoba meniru browser. Banyak dari bot ini melakukan tugas-tugas yang berguna, seperti crawling konten, optimasi mesin pencari

(SEO), atau agregasi. Penting untuk mengidentifikasi dan memahami bot umum mana yang datang ke situs Anda dan pengaruhnya terhadap lalu lintas dan kinerja Anda.

- Bot yang ditargetkan — Bot ini mencoba menghindari deteksi dengan meniru browser. Mereka menggunakan teknologi browser, seperti browser tanpa kepala, atau mereka memalsukan sidik jari browser. Mereka memiliki kemampuan untuk mengeksekusi JavaScript dan mendukung cookie. Maksud mereka tidak selalu jelas, dan lalu lintas yang mereka hasilkan dapat terlihat seperti lalu lintas pengguna normal.

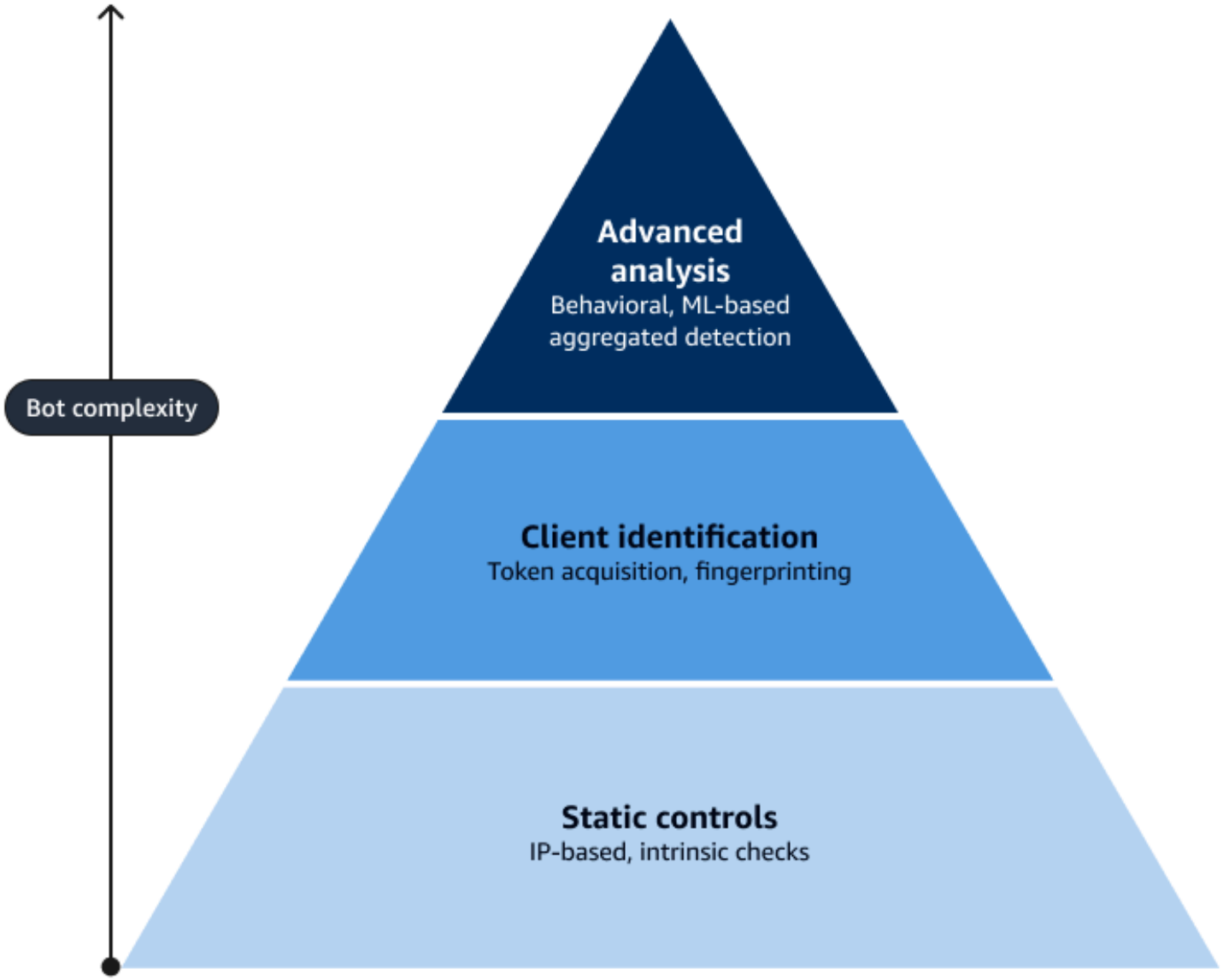
Bot yang ditargetkan paling canggih dan gigih meniru perilaku manusia dengan menghasilkan gerakan mouse seperti manusia dan klik di situs web. Mereka adalah yang paling canggih dan sulit dideteksi, tetapi mereka juga yang paling mahal untuk dioperasikan.

Seringkali, operator menggabungkan teknik-teknik ini. Ini menciptakan permainan pengejaran konstan, di mana Anda harus sering mengubah pendekatan perlindungan dan mitigasi untuk beradaptasi dengan teknik terbaru operator. Bot ini dianggap sebagai ancaman persisten lanjutan (APT). Untuk informasi selengkapnya, lihat Ancaman persisten lanjutan di pusat sumber daya NIST.

Teknik untuk kontrol bot

Tujuan utama mitigasi bot adalah membatasi dampak negatif dari aktivitas bot otomatis pada situs web, layanan, dan aplikasi organisasi. Teknologi dan teknik yang digunakan tergantung pada jenis lalu lintas atau aktivitas yang ingin Anda pertahankan. Memahami aplikasi dan lalu lintasnya adalah kunci untuk mencapai hal ini. Untuk informasi lebih lanjut tentang di mana harus memulai, lihat Pedoman untuk memantau strategi kontrol bot Anda bagian dalam panduan ini.

Secara umum, kontrol yang disediakan solusi mitigasi bot dapat dikelompokkan ke dalam kategori tingkat tinggi berikut: statis, identifikasi klien, dan analisis lanjutan. Gambar berikut menunjukkan berbagai teknik yang tersedia dan bagaimana mereka dapat digunakan tergantung pada kompleksitas aktivitas bot. Ini menyoroti bagaimana basis, atau mitigasi terluas, dapat diperoleh melalui penggunaan kontrol statis, seperti izinkan daftar dan pemeriksaan intrinsik. Bagian terkecil dari bot selalu yang paling canggih, dan mengurangi bot ini membutuhkan teknologi yang lebih maju dan kombinasi kontrol.



Selanjutnya, panduan ini mengeksplorasi setiap kategori dan tekniknya. Ini juga menjelaskan opsi yang tersedia AWS WAFuntuk mengimplementasikan kontrol ini:

- Kontrol statis untuk mengelola bot
- Kontrol identifikasi klien untuk mengelola bot
- Kontrol analisis lanjutan untuk mengelola bot

Kontrol statis untuk mengelola bot

Untuk mengambil tindakan, kontrol statis mengevaluasi informasi statis dari permintaan HTTP (S), seperti alamat IP atau header-nya. Kontrol ini dapat berguna untuk aktivitas bot buruk dengan

kecanggihan rendah atau untuk lalu lintas bot menguntungkan yang diharapkan yang perlu diverifikasi dan dikelola. Teknik kontrol statis meliputi: izinkan daftar, kontrol berbasis IP, dan pemeriksaan intrinsik.

Izinkan daftar

Izinkan daftar adalah kontrol yang memungkinkan lalu lintas ramah yang teridentifikasi melalui kontrol mitigasi bot yang ada. Ada berbagai cara untuk mencapai ini. Yang paling sederhana adalah dengan menggunakan aturan yang cocok dengan satu set alamat IP atau kondisi kecocokan serupa. Ketika permintaan cocok dengan aturan yang diatur ke `Allow` tindakan, itu tidak dievaluasi oleh aturan berikutnya. Dalam beberapa kasus, Anda hanya perlu mencegah aturan tertentu agar tidak ditindaklanjuti; dengan kata lain, Anda perlu mengizinkan daftar untuk satu aturan tetapi tidak semua aturan. Ini adalah skenario umum untuk menangani positif palsu untuk aturan. Izinkan daftar dianggap sebagai aturan cakupan luas. Untuk mengurangi potensi negatif palsu, kami sarankan Anda memasangkannya dengan opsi lain yang lebih terperinci, seperti kecocokan jalur atau header.

Kontrol berbasis IP

Blok alamat IP tunggal

Alat yang umum digunakan untuk mengurangi dampak bot adalah membatasi permintaan dari satu pemohon. Contoh paling sederhana adalah memblokir alamat IP sumber lalu lintas jika permintaannya berbahaya atau volumenya tinggi. Ini menggunakan aturan pencocokan set AWS WAF IP untuk mengimplementasikan blok berbasis IP. Aturan-aturan ini cocok pada alamat IP dan menerapkan tindakan`Block`,`Challenge`, atau`CAPTCHA`. Anda dapat menentukan kapan terlalu banyak permintaan yang masuk dari alamat IP dengan melihat Content Delivery Network (CDN), firewall aplikasi web, atau log aplikasi dan layanan. Namun, dalam banyak kasus, kontrol ini tidak praktis tanpa otomatisasi.

Mengotomatiskan daftar blok alamat IP AWS WAF biasanya dilakukan dengan aturan berbasis tarif. Untuk informasi selengkapnya, lihat Aturan berbasis tarif dalam panduan ini. Anda juga dapat menerapkan Otomatisasi Keamanan untuk AWS WAF solusi. Solusi ini secara otomatis memperbarui daftar alamat IP untuk diblokir, dan AWS WAF aturan menolak permintaan yang cocok dengan alamat IP tersebut.

Salah satu cara untuk mengenali serangan bot adalah jika banyak permintaan dari alamat IP yang sama berfokus pada sejumlah kecil halaman web. Ini menunjukkan bahwa bot tersebut membuang harga atau berulang kali mencoba login yang gagal pada persentase tinggi. Anda dapat membuat

otomatisasi yang segera mengenali pola ini. Otomatisasi memblokir alamat IP, yang mengurangi kemanjuran serangan dengan mengidentifikasi dan menguranginya dengan cepat. Memblokir alamat IP tertentu kurang efektif ketika penyerang memiliki banyak koleksi alamat IP untuk meluncurkan serangan dari atau ketika perilaku menyerang sulit dikenali dan dipisahkan dari lalu lintas normal.

Reputasi alamat IP

Layanan reputasi IP menyediakan intelijen yang membantu mengevaluasi kepercayaan alamat IP. Kecerdasan ini umumnya diturunkan dengan menggabungkan informasi terkait IP dari aktivitas masa lalu dari alamat IP tersebut. Aktivitas sebelumnya membantu menunjukkan seberapa besar kemungkinan alamat IP menghasilkan permintaan berbahaya. Data ditambahkan ke daftar terkelola yang melacak perilaku alamat IP.

Alamat IP anonim adalah kasus khusus reputasi alamat IP. Alamat IP sumber berasal dari sumber yang diketahui dari alamat IP yang mudah diperoleh, seperti mesin virtual berbasis cloud, atau dari proxy, seperti penyedia VPN yang dikenal atau node Tor. Daftar reputasi IP AWS WAF Amazon dan grup aturan terkelola daftar IP Anonim menggunakan intelijen ancaman internal Amazon untuk membantu mengidentifikasi alamat IP ini.

Kecerdasan yang disediakan oleh daftar terkelola ini dapat membantu Anda bertindak berdasarkan aktivitas yang diidentifikasi dari sumber-sumber ini. Berdasarkan kecerdasan ini, Anda dapat membuat aturan yang secara langsung memblokir lalu lintas atau aturan yang membatasi jumlah permintaan (seperti aturan berbasis tarif). Anda juga dapat menggunakan kecerdasan ini untuk mengevaluasi sumber lalu lintas dengan menggunakan aturan dalam `COUNT` mode. Ini memeriksa kriteria kecocokan dan menerapkan label yang dapat Anda gunakan untuk membuat aturan khusus.

Aturan berbasis tarif

Aturan berbasis tarif dapat menjadi alat yang berharga untuk skenario tertentu. Misalnya, aturan berbasis tarif efektif ketika lalu lintas bot mencapai volume tinggi dibandingkan dengan pengguna dalam pengidentifikasi sumber daya seragam sensitif (URIs) atau ketika volume lalu lintas mulai mempengaruhi operasi normal. Pembatasan tarif dapat menjaga permintaan pada tingkat yang dapat dikelola dan membatasi serta mengontrol akses. AWS WAF dapat menerapkan aturan pembatasan laju dalam daftar kontrol akses web (web ACL) dengan menggunakan pernyataan aturan berbasis tarif. Pendekatan yang disarankan saat menggunakan aturan berbasis tarif adalah dengan menyertakan aturan menyeluruh yang mencakup seluruh situs, aturan khusus URI, dan aturan berbasis tingkat reputasi IP. Aturan berbasis tingkat reputasi IP menggabungkan kecerdasan reputasi alamat IP dengan fungsionalitas pembatas kecepatan.

Untuk seluruh situs, aturan berbasis tingkat reputasi IP selimut menciptakan langit-langit yang mencegah bot yang tidak canggih membanjiri situs dari sejumlah kecil. IPs Pembatasan tarif sangat disarankan untuk melindungi URIs yang memiliki biaya atau dampak tinggi, seperti halaman login atau pembuatan akun.

Aturan pembatas tingkat dapat memberikan lapisan pertahanan pertama yang hemat biaya. Anda dapat menggunakan aturan yang lebih canggih untuk melindungi sensitif URIs. Aturan berbasis tingkat khusus URI dapat membatasi dampak pada halaman penting atau APIs yang memengaruhi backend, seperti akses basis data. Mitigasi lanjutan untuk melindungi tertentu URIs, yang dibahas nanti dalam panduan ini, sering menimbulkan biaya tambahan, dan aturan berbasis tarif khusus URI ini dapat membantu Anda mengendalikan biaya. Untuk informasi selengkapnya tentang aturan berbasis tarif yang umum direkomendasikan, lihat Tiga aturan AWS WAF berbasis tarif paling penting di Blog Keamanan. AWS Dalam beberapa situasi, akan berguna untuk membatasi jenis permintaan apa yang dievaluasi oleh aturan berbasis tarif. Anda dapat menggunakan pernyataan cakupan ke bawah untuk, misalnya, membatasi aturan berbasis tarif berdasarkan wilayah geografis alamat IP sumber.

AWS WAF menawarkan kemampuan canggih untuk aturan berbasis tarif melalui penggunaan kunci agregasi. Dengan fungsi ini, Anda dapat mengonfigurasi aturan berbasis tarif untuk menggunakan berbagai kunci agregasi dan kombinasi tombol lainnya, selain dari alamat IP sumber. Misalnya, sebagai kombinasi tunggal, Anda dapat menggabungkan permintaan berdasarkan alamat IP yang diteruskan, metode HTTP, dan argumen kueri. Ini membantu Anda mengonfigurasi aturan yang lebih halus untuk mitigasi lalu lintas volumetrik yang canggih.

Pemeriksaan intrinsik

Pemeriksaan intrinsik adalah berbagai jenis validasi internal atau inheren atau verifikasi dalam suatu sistem atau proses. Untuk kontrol bot, AWS WAF lakukan pemeriksaan intrinsik dengan memvalidasi bahwa informasi yang dikirim dalam permintaan cocok dengan sinyal sistem. Misalnya, ia melakukan pencarian DNS terbalik dan verifikasi sistem lainnya. Beberapa permintaan otomatis diperlukan, seperti permintaan terkait SEO. Izinkan daftar adalah cara untuk mengizinkan bot yang baik dan diharapkan lewat. Namun terkadang, bot jahat meniru bot yang bagus, dan sulit untuk memisahkannya. AWS WAF menyediakan metode untuk mencapai ini melalui grup aturan Kontrol AWS WAF Bot terkelola. Aturan dalam grup ini memberikan verifikasi bahwa bot yang diidentifikasi sendiri adalah siapa yang mereka katakan. AWS WAF memeriksa rincian permintaan terhadap pola bot yang diketahui, dan juga melakukan pencarian DNS terbalik dan verifikasi objektif lainnya.

Kontrol identifikasi klien untuk mengelola bot

Jika lalu lintas terkait serangan tidak dapat dengan mudah dikenali melalui atribut statis, maka deteksi harus dapat secara akurat mengidentifikasi klien yang membuat permintaan. Misalnya, aturan berbasis tarif seringkali lebih efektif dan lebih sulit untuk dihindari ketika atribut yang dibatasi tarif khusus aplikasi, seperti cookie atau token. Menggunakan cookie yang terkait dengan sesi mencegah operator botnet untuk dapat menduplikasi aliran permintaan serupa di banyak bot.

Akuisisi token biasanya digunakan untuk identifikasi klien. Untuk akuisisi token, JavaScript kode mengumpulkan informasi untuk menghasilkan token yang dievaluasi di sisi server. Evaluasi dapat berkisar dari memverifikasi JavaScript yang berjalan pada klien hingga mengumpulkan informasi perangkat untuk sidik jari. Akuisisi token memerlukan integrasi JavaScript SDK ke dalam situs atau aplikasi, atau mengharuskan penyedia layanan melakukan injeksi secara dinamis.

Memerlukan JavaScript dukungan menambahkan rintangan tambahan untuk bot yang mencoba meniru browser. Ketika SDK terlibat, seperti dalam aplikasi seluler, akuisisi token memverifikasi implementasi SDK dan mencegah bot meniru permintaan aplikasi.

Akuisisi token membutuhkan penggunaan SDKs diimplementasikan di sisi klien koneksi. AWS WAF Fitur berikut menyediakan SDK JavaScript berbasis untuk browser dan SDK berbasis aplikasi untuk perangkat seluler: Kontrol Bot, Pencegahan pengambilalihan akun Kontrol Penipuan (ATP) dan Pencegahan Penipuan Pembuatan Akun Kontrol Penipuan (ACFP).

Teknik untuk identifikasi klien termasuk CAPTCHA, profil browser, sidik jari perangkat, dan sidik jari TLS.

CAPTCHA

Tes Turing publik yang sepenuhnya otomatis untuk membedakan komputer dan manusia (CAPTCHA) digunakan untuk membedakan antara pengunjung robot dan manusia dan untuk mencegah pengikisan web, isian kredensyal, dan spam. Ada berbagai implementasi, tetapi mereka sering melibatkan teka-teki yang dapat dipecahkan manusia. CAPTCHAsmenawarkan lapisan pertahanan tambahan terhadap bot umum dan dapat mengurangi positif palsu dalam deteksi bot.

AWS WAF memungkinkan aturan untuk menjalankan tindakan CAPTCHA terhadap permintaan web yang sesuai dengan kriteria inspeksi aturan. Tindakan ini adalah hasil evaluasi informasi identifikasi klien yang dikumpulkan oleh layanan. AWS WAF aturan dapat mengharuskan tantangan CAPTCHA diselesaikan untuk sumber daya tertentu yang sering ditargetkan oleh bot, seperti login, pencarian,

dan pengiriman formulir. AWS WAF dapat langsung melayani CAPTCHA melalui sarana pengantara atau dengan menggunakan SDK untuk menanganinya di sisi klien. Untuk informasi lebih lanjut lihat CAPTCHA dan Tantangan di. AWS WAF

Profil peramban

Browser profiling adalah metode mengumpulkan dan mengevaluasi karakteristik browser, sebagai bagian dari akuisisi token, untuk membedakan manusia nyata menggunakan browser interaktif dari aktivitas bot terdistribusi. Anda dapat melakukan pembuatan profil browser secara pasif melalui header, urutan header, dan karakteristik permintaan lainnya yang melekat pada cara kerja browser.

Anda juga dapat melakukan pembuatan profil browser dalam kode dengan menggunakan akuisisi token. Dengan menggunakan JavaScript untuk profil browser, Anda dapat dengan cepat menentukan apakah klien mendukung JavaScript. Ini membantu Anda mendeteksi bot sederhana yang tidak mendukungnya. Profil browser memeriksa lebih dari sekadar header dan JavaScript dukungan HTTP; pembuatan profil browser menyulitkan bot untuk sepenuhnya meniru browser web. Kedua opsi profil browser memiliki tujuan yang sama: untuk menemukan pola dalam profil browser yang menunjukkan ketidakkonsistenan dengan perilaku browser nyata.

AWS WAF kontrol bot untuk bot yang ditargetkan memberikan indikasi, sebagai bagian dari evaluasi token, apakah browser menunjukkan bukti otomatisasi atau sinyal yang tidak konsisten. AWS WAF menandai permintaan untuk mengambil tindakan yang ditentukan dalam aturan. Untuk informasi selengkapnya, lihat Mendeteksi dan memblokir lalu lintas bot tingkat lanjut di Blog AWS Keamanan.

Sidik jari perangkat

Sidik jari perangkat mirip dengan profil browser, tetapi tidak terbatas pada browser. Kode yang berjalan pada perangkat (yang dapat berupa perangkat seluler atau browser web) mengumpulkan dan melaporkan detail perangkat ke server backend. Rinciannya dapat mencakup atribut sistem, seperti memori, tipe CPU, jenis kernel sistem operasi (OS), versi OS, dan virtualisasi.

Anda dapat menggunakan sidik jari perangkat untuk mengenali apakah bot meniru lingkungan atau jika ada tanda-tanda langsung bahwa otomatisasi sedang digunakan. Selain itu, sidik jari perangkat juga dapat digunakan untuk mengenali permintaan berulang dari perangkat yang sama.

Mengenali permintaan berulang dari perangkat yang sama, bahkan jika perangkat mencoba mengubah beberapa karakteristik permintaan, memungkinkan sistem backend untuk memberlakukan aturan pembatasan laju. Aturan pembatasan tarif yang didasarkan pada sidik jari perangkat biasanya

lebih efektif daripada aturan pembatas kecepatan berdasarkan alamat IP. Ini membantu Anda mengurangi lalu lintas bot yang berputar antara VPNs atau proxy tetapi bersumber dari sejumlah kecil perangkat.

Ketika digunakan dengan integrasi aplikasi SDKs, kontrol AWS WAF bot untuk bot yang ditargetkan, dapat menggabungkan perilaku permintaan sesi klien. Ini membantu Anda mendeteksi dan memisahkan sesi klien yang sah dari sesi klien jahat, bahkan ketika keduanya berasal dari alamat IP yang sama. Untuk informasi selengkapnya tentang kontrol AWS WAF bot untuk bot yang ditargetkan, lihat Mendeteksi dan memblokir lalu lintas bot tingkat lanjut di Blog AWS Keamanan.

Sidik jari TLS

Sidik jari TLS, juga dikenal sebagai aturan berbasis tanda tangan, biasanya digunakan ketika bot berasal dari banyak alamat IP tetapi menunjukkan karakteristik yang serupa. Saat menggunakan HTTPS, sisi klien dan server bertukar pesan untuk mengakui dan memverifikasi satu sama lain. Mereka membangun algoritma kriptografi dan kunci sesi. Ini disebut jabat tangan TLS. Bagaimana jabat tangan TLS diimplementasikan adalah tanda tangan yang seringkali berharga untuk mengenali serangan besar yang tersebar di banyak alamat IP.

Sidik jari TLS memungkinkan server web untuk menentukan identitas klien web dengan tingkat akurasi yang tinggi. Ini hanya membutuhkan parameter dalam koneksi paket pertama, sebelum pertukaran data aplikasi terjadi. Dalam hal ini, klien web mengacu pada aplikasi yang memulai permintaan, yang mungkin berupa browser, alat CLI, skrip (bot), aplikasi asli, atau klien lainnya.

Salah satu pendekatan sidik jari SSL dan TLS adalah sidik jari. JA3 JA3sidik jari koneksi klien berdasarkan bidang dalam pesan Client Hello dari jabat tangan SSL atau TLS. Ini membantu Anda membuat profil klien SSL dan TLS tertentu di berbagai alamat IP sumber, port, dan sertifikat X.509.

Amazon CloudFront mendukung penambahan JA3 header ke permintaan. `CloudFront-Viewer-JA3-Fingerprint`Header berisi sidik jari hash 32 karakter dari paket TLS Client Hello dari permintaan penampil yang masuk. Sidik jari merangkum informasi tentang bagaimana klien berkomunikasi. Informasi ini dapat digunakan untuk profil klien yang memiliki pola yang sama. Anda dapat menambahkan `CloudFront-Viewer-JA3-Fingerprint` header ke kebijakan permintaan asal dan melampirkan kebijakan ke CloudFront distribusi. Anda kemudian dapat memeriksa nilai header di aplikasi asal atau di Lambda @Edge CloudFront dan Functions. Anda dapat membandingkan nilai header dengan daftar sidik jari malware yang diketahui untuk memblokir klien jahat. Anda juga dapat membandingkan nilai header dengan daftar sidik jari yang diharapkan untuk mengizinkan permintaan hanya dari klien yang dikenal.

Kontrol analisis lanjutan untuk mengelola bot

Beberapa bot menggunakan alat penipuan canggih untuk secara aktif menghindari deteksi. Bot ini meniru perilaku manusia untuk melakukan aktivitas tertentu, seperti scalping. Bot ini memiliki tujuan, dan biasanya dikaitkan dengan hadiah uang yang besar.

Bot canggih dan gigih ini menggunakan campuran teknologi untuk menghindari deteksi atau berbaur dengan lalu lintas reguler. Pada gilirannya, ini juga membutuhkan campuran teknologi deteksi yang berbeda untuk mengidentifikasi dan mengurangi lalu lintas berbahaya secara akurat.

Kasus penggunaan yang ditargetkan

Data kasus penggunaan dapat memberikan peluang deteksi bot. Deteksi penipuan adalah kasus penggunaan khusus di mana mitigasi khusus diperlukan. Misalnya, untuk membantu mencegah pengambilalihan akun, Anda dapat membandingkan daftar nama pengguna dan kata sandi akun yang disusupi dengan permintaan login atau pembuatan akun. Ini membantu pemilik situs web untuk mendeteksi upaya login yang menggunakan kredensyal yang dikompromikan. Penggunaan kredensyal yang dikompromikan dapat menunjukkan bot yang mencoba mengambil alih akun, atau bisa jadi pengguna yang tidak menyadari kredensialnya dikompromikan. Dalam kasus penggunaan ini, pemilik situs web dapat mengambil langkah tambahan untuk memverifikasi pengguna dan kemudian membantu mereka mengubah kata sandi mereka. AWS WAF menyediakan aturan terkelola pencegahan pengambilalihan akun Kontrol Penipuan (ATP) untuk kasus penggunaan ini.

Deteksi bot tingkat aplikasi atau agregat

Beberapa kasus penggunaan memerlukan penggabungan data tentang permintaan dari jaringan pengiriman konten (CDN) AWS WAF, dan backend aplikasi atau layanan. Terkadang, Anda bahkan perlu mengintegrasikan intelijen pihak ketiga untuk dapat membuat keputusan dengan percaya diri tinggi tentang bot.

Fitur di Amazon CloudFront dan AWS WAF dapat mengirim sinyal ke infrastruktur backend, atau mereka selanjutnya dapat menggabungkan aturan melalui header dan label. CloudFront mengekspos header JA3 sidik jari, seperti yang disebutkan sebelumnya. Ini adalah contoh CloudFront penyediaan data tersebut melalui header. AWS WAF dapat mengirim label saat cocok dengan aturan. Aturan selanjutnya dapat menggunakan label ini untuk membuat keputusan yang lebih baik tentang bot. Ketika beberapa aturan digabungkan, Anda dapat menerapkan kontrol yang sangat terperinci. Kasus penggunaan umum adalah mencocokkan bagian aturan terkelola melalui label dan kemudian menggabungkannya dengan data permintaan lainnya. Untuk informasi selengkapnya, lihat Contoh pencocokan label dalam AWS WAF dokumentasi.

Analisis pembelajaran mesin

Machine leaning (ML) adalah teknik yang ampuh untuk menangani bot. ML dapat beradaptasi dengan perubahan detail, dan ketika dikombinasikan dengan alat lain, menyediakan cara yang paling kuat dan lengkap untuk mengurangi bot dengan positif palsu minimal. Dua teknik ML yang paling umum adalah analisis perilaku dan deteksi anomali. Dengan analisis perilaku, sistem (di klien, server, atau keduanya) memantau bagaimana pengguna berinteraksi dengan aplikasi atau situs web. Ini memonitor pola gerakan mouse atau frekuensi interaksi klik dan sentuh. Perilaku tersebut kemudian dianalisis dengan model ML untuk mengenali bot. Deteksi anomali serupa. Ini berfokus pada mendeteksi perilaku atau pola yang secara signifikan berbeda dari baseline yang didefinisikan untuk aplikasi atau situs web.

AWS WAF kontrol yang ditargetkan untuk bot menyediakan teknologi MLM prediktif. Teknologi ini membantu mempertahankan diri dari serangan berbasis proxy terdistribusi yang dibuat oleh bot yang dirancang untuk menghindari deteksi. Grup aturan AWS WAF Bot Control yang dikelola menggunakan analisis ML otomatis dari statistik lalu lintas situs web untuk mendeteksi perilaku anomali yang menunjukkan aktivitas bot terdistribusi dan terkoordinasi.

Penerapan dan implementasi strategi kontrol bot Anda

Ada beberapa faktor yang perlu dipertimbangkan ketika merencanakan strategi penyebaran kontrol bot. Selain karakteristik unik dari aplikasi web, ukuran lingkungan, proses pengembangan, dan struktur organisasi mempengaruhi strategi penyebaran. Bergantung pada lingkungan dan karakteristik aplikasi Anda, strategi penyebaran terpusat atau terdesentralisasi dapat digunakan:

- Strategi penyebaran terpusat — Pendekatan terpusat memungkinkan tingkat kontrol yang lebih tinggi ketika Anda menginginkan penegakan kontrol bot yang ketat. Pendekatan ini sangat cocok jika tim aplikasi lebih suka manajemen offload. Pendekatan terpusat paling efektif ketika aplikasi web berbagi karakteristik yang sama. Dalam hal ini, aplikasi mendapat manfaat dari seperangkat aturan kontrol bot dan tindakan mitigasi bot yang umum.
- Strategi penyebaran terdesentralisasi — Pendekatan terdesentralisasi memberi tim aplikasi otonomi untuk mendefinisikan dan mengimplementasikan konfigurasi kontrol bot secara independen. Pendekatan ini umum untuk lingkungan yang lebih kecil atau ketika tim aplikasi perlu mempertahankan kendali atas kebijakan kontrol bot mereka. Karena sifat dari banyak aplikasi web, seringkali perlu untuk mempertahankan kebijakan kontrol bot independen yang disesuaikan untuk karakteristik aplikasi yang unik, menghasilkan pendekatan terdesentralisasi.
- Strategi gabungan — Kombinasi dari kedua pendekatan ini cocok untuk campuran aplikasi web. Misalnya, ini mungkin memerlukan seperangkat aturan dasar yang berlaku untuk semua web ACLs, sementara pengelolaan kebijakan kontrol bot yang lebih spesifik didelegasikan ke tim aplikasi.

Anda dapat menggunakan AWS Firewall Manageruntuk memusatkan dan mengotomatiskan penyebaran AWS WAF web ACLs yang menentukan kebijakan kontrol bot. Saat menggunakan Firewall Manager, pertimbangkan apakah pantas untuk memusatkan kebijakan kontrol bot, termasuk apakah kebijakan tersebut harus didelegasikan ke tim aplikasi. Dengan Firewall Manager, Anda dapat menggunakan penandaan untuk memungkinkan tim aplikasi ikut serta dalam kebijakan. AWS WAF Ini menyediakan AWS WAF fungsionalitas mitigasi ancaman cerdas. Anda juga dapat mengaktifkan AWS WAF pencatatan terpusat untuk operasi aplikasi dan keamanan.

Terlepas dari strategi penyebaran yang digunakan, disarankan untuk mendefinisikan dan mengelola proses orientasi melalui kerangka kerja berbasis infrastruktur sebagai kode (IAc), seperti atau. AWS CloudFormationAWS Cloud Development Kit (AWS CDK) Ini membantu Anda mengonfigurasi kontrol sumber untuk menyimpan dan versi objek konfigurasi. Untuk informasi selengkapnya, lihat contoh AWS WAF konfigurasi untuk AWS CDK(GitHub) dan CloudFormation(AWS dokumentasi).

Strategi implementasi

Setelah Anda memilih strategi penyebaran, implementasi dapat dimulai. Strategi penyebaran mendefinisikan bagaimana aturan diluncurkan ke aplikasi yang berbeda. Dalam strategi implementasi, fokusnya adalah pada proses berulang penambahan kontrol, pengujian, pemantauan terus menerus, dan kemudian mengevaluasi efeknya.

Memahami pola lalu lintas

Untuk benar-benar memahami pola lalu lintas, penting untuk membiasakan diri dengan fungsi bisnis aplikasi dan atribut yang diharapkan, seperti pola penggunaan, sumber daya utama, dan persona pengguna. Menggabungkan lalu lintas produksi dan lalu lintas yang dihasilkan selama pengujian terhadap aplikasi untuk menetapkan dasar untuk evaluasi. Pastikan bahwa jangka waktu menyertakan data lalu lintas yang cukup mewakili beberapa puncak penggunaan.

Dengan menggunakan alat pilihan Anda, tinjau log lalu lintas dan metrik selama periode penggunaan yang representatif. Menganalisis data AWS WAF log untuk permintaan anomali dengan memfilter pada bidang log seperti `headers` (misalnya, `User-Agent` dan`Referer`),, dan. `country` `clientIp` Catat pengidentifikasi sumber daya seragam (URIs) dan frekuensi aksesnya. Kategorikan lalu lintas, seperti mengidentifikasi bot yang baik. Misalnya, mengizinkan akses untuk bot yang bermanfaat, seperti crawler mesin pencari dan monitor.

Di AWS WAF konsol, di dasbor kontrol Bot, sampel aktivitas bot tersedia untuk ACL web aktif apa pun. Meskipun ini memberikan perspektif awal volume permintaan bot umum, lakukan konfigurasi dan analisis lebih lanjut untuk lebih memahami aktivitas bot.

Untuk implementasi yang efektif, Anda harus memiliki pemahaman yang baik tentang lalu lintas bot, efeknya, dan permintaan bot mana yang bermanfaat vs berbahaya. Ini membantu fase berikutnya, memilih kontrol, dan membantu Anda mengevaluasi lalu lintas bot secara paralel.

Memilih dan menambahkan kontrol

Analisis lalu lintas awal membantu menentukan kontrol bot mana yang akan digunakan dan tindakan apa yang harus dipilih untuk masing-masing. Anda juga dapat memilih untuk mencatat dan memantau aktivitas untuk potensi tindakan masa depan. Analisis lalu lintas awal membantu Anda memilih kontrol terbaik untuk mengelola lalu lintas. Untuk informasi selengkapnya tentang kontrol yang tersedia, lihat Teknik untuk kontrol bot di panduan ini.

Pertimbangkan untuk menyertakan implementasi SDK tambahan selama langkah ini. Ini membantu Anda menguji dan menyelesaikan implementasi SDK di semua aplikasi yang diperlukan. AWS WAF kontrol bot dan aturan kontrol penipuan memberikan manfaat evaluasi token penuh saat Anda menerapkan JavaScript SDK atau SDK seluler. Untuk informasi selengkapnya, lihat Mengapa Anda harus menggunakan integrasi aplikasi SDKs dengan Kontrol Bot dalam AWS WAF dokumentasi.

Kami merekomendasikan penerapan akuisisi token untuk berbagai jenis aplikasi sebagai berikut:

- Aplikasi satu halaman (SPA) - JavaScript SDK (tanpa pengalihan)
- Browser seluler - JavaScript SDK atau tindakan aturan (CAPTCHA atau Tantangan)
- Tampilan web — JavaScript SDK atau tindakan aturan (CAPTCHA atau Tantangan)
- Aplikasi asli — SDK Seluler
- iFrames — JavaScript SDK

Untuk informasi selengkapnya tentang cara menerapkan SDKs, lihat integrasi aplikasi AWS WAF klien dalam AWS WAF dokumentasi.

Menguji dan menyebarkan ke produksi

Kontrol harus awalnya digunakan di lingkungan non-produksi di mana Anda dapat melakukan pengujian untuk memverifikasi bahwa fungsionalitas aplikasi web yang diharapkan dipertahankan. Selalu lakukan validasi menyeluruh di lingkungan pengujian sebelum penerapan produksi.

Setelah pengujian dan validasi di lingkungan non-produksi, rilis produksi dapat dilanjutkan. Pilih tanggal dan waktu dengan lalu lintas pengguna terendah yang diharapkan. Sebelum penerapan, tim aplikasi dan keamanan harus meninjau kesiapan operasional, mendiskusikan cara mengembalikan perubahan, dan meninjau dasbor untuk memastikan semua metrik dan alarm yang diperlukan dikonfigurasi.

Dengan penerapan CloudFront berkelanjutan Amazon, Anda dapat mengirim sejumlah kecil lalu lintas ke distribusi pementasan yang memiliki ACL AWS WAF web yang dikonfigurasi khusus untuk evaluasi kontrol bot. AWS WAF menyediakan manajemen versi dari setiap aturan terkelola baru atau yang diperbarui sehingga Anda dapat menguji dan menyetujui perubahan sebelum mereka mulai mengevaluasi lalu lintas produksi.

Mengevaluasi dan menyetel kontrol

Kontrol yang diterapkan dapat memberikan wawasan dan visibilitas lebih lanjut ke dalam aktivitas dan pola lalu lintas. Sering memantau dan menganalisis lalu lintas aplikasi untuk menambah atau menyesuaikan kontrol keamanan. Biasanya ada fase penyetelan untuk mengurangi potensi negatif palsu dan positif palsu. Negatif palsu adalah serangan yang tidak tertangkap oleh kontrol Anda dan mengharuskan Anda untuk mengeraskan aturan Anda. Positif palsu mewakili permintaan yang sah yang salah diidentifikasi sebagai serangan dan diblokir sebagai konsekuensinya.

Analisis dan penyetelan dapat dilakukan secara manual atau dengan bantuan alat. Sistem Informasi Keamanan dan Manajemen Acara (SIEM) adalah alat umum yang membantu menyediakan metrik dan pemantauan cerdas. Ada banyak yang tersedia dengan berbagai tingkat kecanggihan, tetapi semuanya memberikan titik awal yang baik untuk mendapatkan wawasan lalu lintas.

Mendefinisikan indikator kinerja kunci penting (KPIs) untuk situs web dan aplikasi dapat membantu Anda mengidentifikasi dengan lebih cepat ketika segala sesuatunya tidak berfungsi seperti yang diharapkan. Misalnya, Anda dapat menggunakan pengembalian tagihan kartu kredit, penjualan per akun, atau tingkat konversi sebagai indikator anomali bisnis yang dapat dihasilkan oleh bot. Mendefinisikan dan memahami metrik mana dan KPIs berharga untuk dipantau bahkan lebih penting daripada hanya tindakan pemantauan.

Memahami cara mendapatkan metrik dan log yang tepat dari solusi kontrol bot sama pentingnya dengan mengidentifikasi metrik yang akan dipantau. Bagian selanjutnya,Pedoman untuk memantau strategi kontrol bot Anda, detail pemantauan dan opsi visibilitas untuk dipertimbangkan.

Pedoman untuk memantau strategi kontrol bot Anda

Untuk lalu lintas bot dan lalu lintas aplikasi web, pemantauan dan visibilitas sangat penting. Ini membantu Anda memprioritaskan kegiatan serta operasi keamanan. Jika pencatatan terperinci atau menggunakan sistem SIEM tidak memungkinkan, maka titik awal yang baik adalah memantau metrik dasar yang disediakan oleh solusi atau vendor pilihan Anda.

Visibilitas ini berguna untuk intelijen ancaman, aturan pengerasan, pemecahan masalah positif palsu, dan menanggapi suatu insiden. Ada beberapa opsi pemantauan yang tersedia dengan AWS WAF. Untuk pemantauan tingkat tinggi, AWS WAF berikan informasi ikhtisar lalu lintas di. Konsol Manajemen AWS Ini tersedia untuk semua lalu lintas serta tampilan terperinci untuk lalu lintas bot, ketika grup aturan Kontrol Bot diaktifkan di ACL web Anda.

AWS WAF menyediakan opsi berbeda untuk pencatatan rinci lalu lintas ACL web. Anda juga dapat menambahkan label ke permintaan, yang dapat Anda gunakan untuk memfasilitasi analisis log dan mengonfigurasi aturan evaluasi bot. Dengan mengintegrasikan Amazon CloudWatch Logs Insights, Anda dapat menanyakan AWS WAF log dan memvisualisasikan hasilnya.

Jika Anda mengaktifkan pencatatan terperinci, AWS WAF berikan visibilitas tambahan di luar dasbor kontrol Bot yang telah dikonfigurasi sebelumnya. Menggunakan AWS WAF log untuk memvisualisasikan lalu lintas, serta investigasi ad-hoc, dapat memberikan pemahaman mendalam tentang pola lalu lintas dan opsi untuk mitigasi aplikasi web.

Anda dapat mengintegrasikan data AWS WAF log dengan Amazon CloudWatch Logs, Amazon Simple Storage Service (Amazon S3), atau Amazon Data Firehose. Untuk informasi selengkapnya, lihat Mengaktifkan AWS WAF pencatatan dan mengirim log ke CloudWatch, Amazon S3, atau Amazon Data Firehose. Anda juga dapat mengirim log ke berbagai target untuk analisis, termasuk ke Amazon OpenSearch Service atau AWS Marketplacesolusi. Untuk informasi selengkapnya, lihat Setelan tujuan dalam dokumentasi Firehose. Jika beberapa sumber log digunakan, solusi logging terpusat direkomendasikan untuk menghubungkan sumber.

Selanjutnya, panduan ini memberikan rekomendasi tentang cara mulai memantau lalu lintas bot dan mendapatkan visibilitas dengan menggunakan Amazon CloudWatch.

Melacak aturan teratas

Melacak aturan yang paling populer dapat menyoroti tren dan aktivitas yang berpotensi anomali. Peningkatan tarif untuk aturan tertentu mungkin menunjukkan potensi aktivitas positif palsu atau

bertarget yang harus Anda selidiki. Aturan yang paling umum untuk melacak adalahKontrol berbasis IP, aturan pemblokiran geografis (lonjakan di sini dapat menunjukkan lalu lintas dari negara yang tidak biasa, yang mungkin tidak diblokir secara otomatis), dan. Aturan berbasis tarif Aturan-aturan ini akan selalu memiliki variasi yang melekat, tetapi anomali dalam pola lalu lintas dapat menjadi indikasi aktivitas bot. Pertimbangkan ini jika Anda mengatur ambang batas secara manual.

Melacak label dan ruang nama teratas

Dengan menggunakan CloudWatch metrik untuk melacak label teratas, Anda dapat melihat AWS WAF aturan mana yang sering dipanggil. Ini membantu Anda mendeteksi anomali, seperti peningkatan aktivitas scraper, lalu lintas dari sumber yang mencurigakan, atau percobaan penyalahgunaan halaman login aplikasi atau API.

Berikut ini adalah contoh label yang mungkin menarik:

- `awswaf:managed:aws:bot-control:signal:non_browser_user_agent`
- `awswaf:managed:aws:bot-control:bot:category:http_library`
- `awswaf:managed:aws:bot-control:bot:name:curl`
- `awswaf:managed:aws:atp:signal:credential_compromised`
- `awswaf:managed:aws:core-rule-set:NoUserAgent_Header`
- `awswaf:managed:token:rejected`

Berikut ini adalah contoh ruang nama label yang mungkin menarik:

- `awswaf:managed:aws:bot-control:`
- `awswaf:managed:aws:atp:`
- `awswaf:managed:aws:anonymous-ip-list:`

Membuat ekspresi matematika

Di Amazon CloudWatch, Anda dapat membuat ekspresi matematika untuk salah satu atau semua aturan. Jika Anda menetapkan peringatan pada ekspresi matematika, Anda akan diberi tahu tentang anomali dalam tarif, bukan kuantitas, metrik tertentu. Ini adalah alat penting untuk mengurangi kelelahan waspada.

Buat metrik kustom yang dibangun dari ekspresi matematika. Lihatlah tarif relatif untuk aturan, dari jumlah keseluruhan permintaan ke aplikasi. Berikut ini adalah ekspresi matematika umum:

```
[ruleX count * 100]/[All allowed requests + All blocked requests]
```

Ekspresi matematika ini memberikan persentase sehingga Anda dapat melacak aturan tertentu dan memvisualisasikan trennya dari waktu ke waktu.

Cara menggunakan deteksi anomali

Menggunakan deteksi CloudWatch anomali pada CloudWatch metrik apa pun dapat memberikan peringatan tentang tren rendah atau tinggi yang tidak normal, tanpa menyiapkan ambang batas aktual secara manual. Algoritma ini terus menganalisis metrik sistem dan aplikasi, menentukan garis dasar normal, dan anomali permukaan dengan intervensi pengguna minimal. CloudWatch menerapkan algoritma statistik dan ML dalam fitur deteksi anomali.

Menggunakan CloudWatch metrik Amazon

AWS WAF memproses lalu lintas dan menambahkan label ke permintaan yang sesuai dengan aturan yang ditentukan dalam ACL web. Setiap label membuat metrik di CloudWatch. Pada saat yang sama, setiap aturan ACL web juga membuat metrik untuk setiap tindakan yang mungkin. Gunakan label dan metrik tindakan ini untuk mendapatkan pemahaman tingkat tinggi tentang lalu lintas bot. Ini adalah pendekatan hemat biaya untuk memvisualisasikan tren. Untuk informasi selengkapnya, lihat Melihat metrik dan metrik Grafik yang tersedia di dokumentasi. CloudWatch

CloudWatch menyediakan opsi untuk mengirim data ke pengumpul log atau agregator, baik itu solusi Layanan AWS atau pihak ketiga. Menelan data dari CloudWatch dapat memberikan pengalaman observabilitas keamanan yang lebih terkonsolidasi, di mana Anda dapat mengkorelasikan data dari berbagai sumber. Ini dapat membantu Anda menyelidiki, melihat, atau mengatur peringatan dan otomatisasi keamanan Anda.

Membangun dasbor

Setelah mengidentifikasi metrik penting untuk dilacak, buat dasbor yang berisi metrik paling relevan. Menampilkannya side-by-side, di bawah satu panel kaca dapat memberikan visibilitas dan kontrol tambahan.

Itu selalu lebih baik untuk mengkonfigurasi peringatan dan aturan otomatisasi untuk nilai metrik anomali. Jangan mengandalkan manusia untuk mengidentifikasi anomali dengan melihat dasbor. Namun, dasbor dapat berguna untuk tujuan investigasi setelah peringatan diterima.

Mengoptimalkan biaya untuk strategi kontrol bot Anda

Sifat lalu lintas web adalah dinamis. Ini berarti bahwa teknologi dan layanan yang digunakan untuk mengurangi ancaman dapat bervariasi dan disetel dari waktu ke waktu. Ini adalah kunci ketika mempertimbangkan strategi kontrol bot dan kontrol yang termasuk di dalamnya. Optimasi dari waktu ke waktu adalah prinsip utama yang perlu diingat, dan itu berasal dari pilar optimasi biaya dari Kerangka AWS Well-Architected.

AWS WAF Web ACLs bisa dinamis, terutama ketika fitur baru dirilis atau Anda mencoba untuk mengurangi ancaman baru. Mengawasi biaya Anda melibatkan pemahaman dimensi biaya AWS WAF layanan dan bagaimana masing-masing mempengaruhi pengeluaran akhir Anda. Biaya mengemudi utama adalah jumlah permintaan yang dievaluasi oleh layanan. Ada biaya tambahan jika Anda menggunakan grup aturan yang dikelola Kontrol Bot dan pencegahan pengambilalihan akun (ATP) atau jika Anda menggunakan tindakan lanjutan, seperti CAPTCHA atau tantangan.

Karena kontrol bot khusus datang dengan biaya premium, tujuan pengoptimalan biaya utama adalah untuk mengurangi jumlah permintaan yang diperiksa oleh kontrol lanjutan ini. Teknik yang berlaku termasuk memisahkan konten bernilai tinggi, menerapkan tindakan berbiaya lebih rendah terlebih dahulu, meringkas area evaluasi, dan menggabungkan perlindungan bot dengan jenis kontrol lainnya. Teknik pemantauan biaya memberikan visibilitas tambahan di seluruh organisasi Anda.

Memisahkan konten dinamis dan statis

Salah satu teknik pengurangan biaya adalah mengisolasi konten statis dari aplikasi dinamis. Mayoritas permintaan untuk aplikasi web tipikal adalah permintaan ke objek statis. Metode umum untuk mengurangi beban pada server aplikasi adalah dengan memindahkan konten statis ke URL-nya sendiri, seperti`static.example.com`. Hal ini sering dicapai dengan membuat distribusi pengiriman konten yang unik dengan konfigurasi caching yang dioptimalkan untuk konten statis. Teknik ini juga dapat membantu menurunkan biaya kontrol bot jika konten statis tidak umum ditargetkan di situs atau aplikasi. Memisahkan konten statis dari aplikasi dinamis dapat memungkinkan aplikasi kontrol bot tingkat lanjut yang lebih tepat.

Menerapkan aturan biaya lebih rendah terlebih dahulu

Teknik lain adalah menerapkan aturan dasar berbiaya rendah yang menyaring lalu lintas yang tidak diinginkan sebelum menggunakan kontrol lanjutan, yang lebih mahal. Dalam praktiknya, ini biasanya berarti menempatkan mitigasi kontrol bot sebagai lapisan pertahanan terakhir dan

menggunakan kontrol sebelumnya untuk menyaring lalu lintas yang tidak diinginkan. Pendekatan piramida ini sebelumnya dibahas Teknik untuk kontrol bot dalam panduan ini. Tujuan utamanya adalah menggunakan opsi berbiaya rendah ini untuk menghentikan lalu lintas yang tidak diinginkan, yang mengurangi jumlah permintaan yang diproses oleh teknik mitigasi canggih dan berbiaya lebih tinggi.

Pelingkupan area evaluasi

AWS WAFpernyataan scope-down memberikan teknik yang ampuh untuk mengurangi jumlah permintaan yang diperiksa oleh aturan lanjutan. Jika memisahkan konten statis ke URL-nya sendiri tidak dapat diimplementasikan, maka pernyataan scope-down adalah metode lain untuk menyaring permintaan yang tidak memerlukan teknik mitigasi lanjutan. Ini dapat dilakukan dengan mendefinisikan jalur aplikasi tertentu, metode HTTP (seperti POST), atau kombinasi serupa.

Menggabungkan perlindungan bot dengan kontrol lain

Pertimbangan kontrol biaya tambahan harus ditinjau saat melindungi aplikasi dari berbagai ancaman selain lalu lintas bot yang tidak diinginkan. Misalnya, melindungi terhadap serangan penolakan layanan (DDoS) terdistribusi dan terhadap pengambilalihan akun memerlukan konfigurasi tambahan yang dapat memengaruhi biaya. Shield Advanced direkomendasikan untuk membantu melindungi aplikasi terhadap serangan DDo S. Secara khusus, mitigasi lapisan aplikasi-nya dapat secara otomatis mengatasi banjir permintaan, sehingga mengurangi jumlah permintaan yang dapat diproses oleh grup aturan Kontrol AWS WAF Bot, saat menempatkan aturan di depan dalam urutan evaluasi. Shield Advanced memiliki manfaat tambahan; AWS WAF aturan standar terkelola dan kustom tidak dikenakan biaya tambahan untuk sumber daya yang dilindungi oleh Shield Advanced. Perhatikan bahwa kelompok aturan mitigasi ancaman cerdas, termasuk Kontrol Bot, memang menimbulkan biaya tambahan, bahkan untuk sumber daya yang dilindungi oleh Shield Advanced.

Aplikasi yang memerlukan pencegahan pengambilalihan akun dapat menggunakan kelompok aturan pencegahan pengambilalihan akun Kontrol AWS WAF Penipuan (ATP). Biaya inspeksi per permintaan grup aturan ATP lebih tinggi daripada kelompok aturan Kontrol Bot. Biaya yang lebih tinggi membuatnya penting untuk menerapkan kelompok aturan ATP setepat mungkin. Menggunakan grup aturan Kontrol Bot bersama dengan ATP dapat membantu mencapai tujuan ini. Grup aturan Bot Control harus ditempatkan di depan ATP di ACL web untuk menyaring permintaan bot dan mengurangi jumlah permintaan yang diperiksa oleh ATP.

Untuk optimasi berkelanjutan, aktivitas yang paling signifikan adalah memantau CloudWatchmetrik yang terkait dengan grup aturan Kontrol Bot. Tujuannya dari waktu ke waktu adalah untuk

menurunkan jumlah permintaan yang dievaluasi oleh grup aturan Kontrol Bot menjadi hanya permintaan yang menargetkan sumber daya yang Anda butuhkan untuk melindungi dari aktivitas bot yang tidak diinginkan. CloudWatch Dasbor bangunan menyediakan visibilitas metrik paling penting untuk aplikasi, termasuk AWS WAF biaya dan penggunaan.

Biaya pemantauan

AWS Cost Exploreradalah alat yang memungkinkan Anda untuk melihat dan menganalisis biaya dan penggunaan Anda. Cost Explorer memfasilitasi analisis AWS biaya, termasuk AWS WAF biaya yang dikeluarkan. Alat ini memberikan informasi biaya untuk 12 bulan terakhir dan memperkirakan pengeluaran masa depan untuk 12 bulan ke depan.

AWS Deteksi Anomali Biaya adalah alat kontrol manajemen biaya lain yang dapat berguna untuk memantau AWS WAF biaya. Ini menggunakan teknologi ML canggih untuk mengidentifikasi pengeluaran anomali dan akar penyebab. Ini membantu Anda dengan cepat mengambil tindakan atau menerima peringatan jika ada kenaikan biaya yang tidak terduga. Untuk menerima peringatan ketika ambang biaya tertentu tercapai, AWS Budgetsdapat menyediakan fungsionalitas pelacakan dan pemantauan tersebut.

Sumber daya

AWS dokumentasi

- AWS WAF panduan pengembang
- AWS Praktik Terbaik untuk Ketahanan DDoS (Whitepaper)AWS
- Pedoman penerapan AWS WAF (AWS Whitepapers)

AWS Sumber daya lainnya

- Menganalisis AWS WAF Log di CloudWatch Log Amazon (posting AWS blog)
- Menyebarkan dashboard untuk AWS WAF dengan sedikit usaha (posting AWS blog)
- Otomatisasi Keamanan untuk AWS WAF (Perpustakaan AWS Solusi)
- Tiga aturan AWS WAF berbasis tarif paling penting (AWS posting blog)
- Visualisasikan AWS WAF log dengan CloudWatch dasbor Amazon (posting AWS blog)

Kontributor

Mengotorisasi

- Diana Alvarado, Arsitek Solusi Senior, AWS
- Cameron Worrell, Arsitek Perusahaan, AWS
- Geary Scherer, Arsitek Solusi, AWS
- Tzoori Tamam, Arsitek Solusi Utama, AWS

Meninjau

- Jess Izen, Insinyur Pengembangan Perangkat Lunak Senior, AWS
- Kaustubh Phatak, Manajer Produk Senior, AWS
- Vikramaditya Bhatnagar, Konsultan Keamanan Senior, AWS

Penulisan teknis

- Lilly AbouHarb, Penulis Teknis Senior, AWS

Riwayat dokumen

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

Perubahan	Deskripsi	Tanggal
Publikasi awal	—	Februari 21, 2024

AWS Glosarium Panduan Preskriptif

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

Nomor

7 Rs

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

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

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

A

A2A () Agent-to-Agent

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

ABAC

Lihat kontrol akses berbasis atribut.

layanan abstrak

Lihat layanan terkelola.

ASAM

Lihat atomisitas, konsistensi, isolasi, daya tahan.

migrasi aktif-aktif

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

migrasi aktif-pasif

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

Agen

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

Agen Ops

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

fungsi agregat

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

AI

Lihat kecerdasan buatan.

AIOps

Lihat operasi kecerdasan buatan.

anonimisasi

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

anti-pola

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

kontrol aplikasi

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

portofolio aplikasi

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

kecerdasan buatan (AI)

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

operasi kecerdasan buatan (AIOps)

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

enkripsi asimetris

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

atomisitas, konsistensi, isolasi, daya tahan (ACID)

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

kontrol akses berbasis atribut (ABAC)

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

sumber data otoritatif

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

Zona Ketersediaan

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

AWS Kerangka Adopsi Cloud (AWS CAF)

Kerangka pedoman dan praktik terbaik AWS untuk membantu organisasi mengembangkan rencana yang efisien dan efektif untuk bergerak dengan sukses ke cloud. AWS CAF mengatur panduan ke dalam enam area fokus yang disebut perspektif: bisnis, orang, tata kelola, platform, keamanan, dan operasi. Perspektif bisnis, orang, dan tata kelola fokus pada keterampilan dan proses bisnis; perspektif platform, keamanan, dan operasi fokus pada keterampilan dan proses teknis. Misalnya, perspektif masyarakat menargetkan pemangku kepentingan yang menangani

sumber daya manusia (SDM), fungsi kepegawaian, dan manajemen orang. Untuk perspektif ini, AWS CAF memberikan panduan untuk pengembangan, pelatihan, dan komunikasi orang untuk membantu mempersiapkan organisasi untuk adopsi cloud yang sukses. Untuk informasi lebih lanjut, lihat situs web AWS CAF dan whitepaper AWS CAF.

AWS Kerangka Kualifikasi Beban Kerja (AWS WQF)

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

B

bot buruk

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

BCP

Lihat perencanaan kontinuitas bisnis.

grafik perilaku

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

sistem big-endian

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

klasifikasi biner

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

filter mekar

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

blue/green penyebaran

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

bot

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

botnet

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

cabang

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

akses break-glass

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

strategi brownfield

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

cache penyangga

Area memori tempat data yang paling sering diakses disimpan.

kemampuan bisnis

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

perencanaan kelangsungan bisnis (BCP)

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

C

KAFE

Lihat Kerangka Adopsi AWS Cloud.

penyebaran kenari

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

CCoE

Lihat Cloud Center of Excellence.

CDC

Lihat mengubah pengambilan data.

ubah pengambilan data (CDC)

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

rekayasa kekacauan

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

CI/CD

Lihat integrasi berkelanjutan dan pengiriman berkelanjutan.

klasifikasi

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

Pengembang Warga

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

Enkripsi sisi klien

Enkripsi data secara lokal, sebelum target Layanan AWS menerimanya.

Cloud Center of Excellence (CCoE)

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

komputasi cloud

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

model operasi cloud

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

tahap adopsi cloud

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

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

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

CMDB

Lihat database manajemen konfigurasi.

repositori kode

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

cache dingin

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

data dingin

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

visi komputer (CV)

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

konfigurasi drift

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

database manajemen konfigurasi (CMDB)

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

paket kesesuaian

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

integrasi berkelanjutan dan pengiriman berkelanjutan (CI/CD)

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

CV

Lihat visi komputer.

D

data saat istirahat

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

klasifikasi data

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

penyimpangan data

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

data dalam transit

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

jala data

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

minimalisasi data

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

perimeter data

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

prapemrosesan data

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

asal data

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

subjek data

Individu yang datanya dikumpulkan dan diproses.

gudang data

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

bahasa definisi database (DDL)

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

bahasa manipulasi basis data (DHTML)

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

DDL

Lihat bahasa definisi database.

ansambel yang dalam

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

pembelajaran mendalam

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

pertahanan-mendalam

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

administrator yang didelegasikan

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

deployment

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

lingkungan pengembangan

Lihat lingkungan.

kontrol detektif

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

pemetaan aliran nilai pengembangan (DVSM)

Sebuah proses yang digunakan untuk mengidentifikasi dan memprioritaskan kendala yang mempengaruhi kecepatan dan kualitas dalam siklus hidup pengembangan perangkat lunak. DVSM memperluas proses pemetaan aliran nilai yang awalnya dirancang untuk praktik manufaktur ramping. Ini berfokus pada langkah-langkah dan tim yang diperlukan untuk menciptakan dan memindahkan nilai melalui proses pengembangan perangkat lunak.

kembar digital

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

tabel dimensi

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

musibah

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

pemulihan bencana (DR)

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

DML~

Lihat bahasa manipulasi database.

desain berbasis domain

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

DR

Lihat pemulihan bencana.

deteksi drift

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

DVSM

Lihat pemetaan aliran nilai pengembangan.

E

EDA

Lihat analisis data eksplorasi.

EDI

Lihat pertukaran data elektronik.

komputasi tepi

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

pertukaran data elektronik (EDI)

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

enkripsi

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

kunci enkripsi

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

endianness

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

titik akhir

Lihat titik akhir layanan.

layanan endpoint

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

perencanaan sumber daya perusahaan (ERP)

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

enkripsi amplop

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

lingkungan

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

- Development Environment — Sebuah contoh dari aplikasi yang berjalan yang hanya tersedia untuk tim inti yang bertanggung jawab untuk memelihara aplikasi. Lingkungan pengembangan digunakan untuk menguji perubahan sebelum mempromosikannya ke lingkungan atas. Jenis lingkungan ini kadang-kadang disebut sebagai lingkungan pengujian.

- lingkungan yang lebih rendah — Semua lingkungan pengembangan untuk aplikasi, seperti yang digunakan untuk build awal dan pengujian.
- lingkungan produksi — Sebuah contoh dari aplikasi yang berjalan yang dapat diakses oleh pengguna akhir. Dalam sebuah CI/CD pipeline, lingkungan produksi adalah lingkungan penyebaran terakhir.
- lingkungan atas — Semua lingkungan yang dapat diakses oleh pengguna selain tim pengembangan inti. Ini dapat mencakup lingkungan produksi, lingkungan praproduksi, dan lingkungan untuk pengujian penerimaan pengguna.

epik

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

ERP

Lihat perencanaan sumber daya perusahaan.

analisis data eksplorasi (EDA)

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

F

tabel fakta

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

gagal cepat

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

batas isolasi kesalahan

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

cabang fitur

Lihat cabang.

fitur

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

pentingnya fitur

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

transformasi fitur

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

beberapa tembakan mendorong

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

FGAC

Lihat kontrol akses berbutir halus.

kontrol akses berbutir halus (FGAC)

Penggunaan beberapa kondisi untuk mengizinkan atau menolak permintaan akses.

migrasi flash-cut

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

FM

Lihat model pondasi.

model pondasi (FM)

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

Gerbang FM

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

G

AI generatif

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

pemblokiran geografis

Lihat pembatasan geografis.

pembatasan geografis (pemblokiran geografis)

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

Alur kerja Gitflow

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

gambar emas

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

strategi greenfield

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

pagar pembatas

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

pagar pembatas (AI)

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

H

HA

Lihat ketersediaan tinggi.

migrasi database heterogen

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

ketersediaan tinggi (HA)

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

modernisasi sejarawan

Pendekatan yang digunakan untuk memodernisasi dan meningkatkan sistem teknologi operasional (OT) untuk melayani kebutuhan industri manufaktur dengan lebih baik. Sejarawan adalah jenis database yang digunakan untuk mengumpulkan dan menyimpan data dari berbagai sumber di pabrik.

data penahanan

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

manusia-dalam-lingkaran (HiTL)

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

migrasi database homogen

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

data panas

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

perbaikan terbaru

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

periode hypercare

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

I

IAc

Lihat infrastruktur sebagai kode.

kebijakan berbasis identitas

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

aplikasi idle

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

IIoT

Lihat Internet of Things industri.

infrastruktur yang tidak dapat diubah

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

masuk (masuknya) VPC

Dalam arsitektur AWS multi-akun, VPC yang menerima, memeriksa, dan merutekan koneksi jaringan dari luar aplikasi. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan

akun Jaringan Anda dengan VPC masuk, keluar, dan inspeksi untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

migrasi inkremental

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

Industri 4.0

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

infrastruktur

Semua sumber daya dan aset yang terkandung dalam lingkungan aplikasi.

infrastruktur sebagai kode (IAc)

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

Internet of Things industri (IIoT)

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

inspeksi VPC

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

Internet of Things (IoT)

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

interpretabilitas

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

IoT

Lihat Internet of Things.

Perpustakaan informasi TI (ITIL)

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

Manajemen layanan TI (ITSM)

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

ITIL

Lihat perpustakaan informasi TI.

ITSM

Lihat manajemen layanan TI.

L

kontrol akses berbasis label (LBAC)

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

landing zone

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

model bahasa besar (LLM)

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

migrasi besar

Migrasi 300 atau lebih server.

LBAC

Lihat kontrol akses berbasis label.

hak istimewa paling sedikit

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

angkat dan geser

Lihat 7 Rs.

sistem endian kecil

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

LLM

Lihat model bahasa besar.

lingkungan yang lebih rendah

Lihat lingkungan.

M

pembelajaran mesin (ML)

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

cabang utama

Lihat cabang.

malware

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

layanan terkelola

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

sistem eksekusi manufaktur (MES)

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

PETA

Lihat Program Percepatan Migrasi.

MCP

Lihat Protokol Konteks Model.

Protokol Konteks Model (MCP)

Protokol stateless untuk komunikasi agen -to- alat.

Server MCP

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

mekanisme

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

akun anggota

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

MES

Lihat sistem eksekusi manufaktur.

Transportasi Telemetri Antrian Pesan (MQTT)

Protokol komunikasi mesin-ke-mesin (M2M) yang ringan, berdasarkan pola publish/subscribe, untuk perangkat IoT yang dibatasi sumber daya.

layanan mikro

Layanan kecil dan independen yang berkomunikasi melalui API yang terdefinisi dengan baik dan biasanya dimiliki oleh tim kecil yang mandiri. Misalnya, sistem asuransi mungkin mencakup layanan mikro yang memetakan kemampuan bisnis, seperti penjualan atau pemasaran, atau subdomain, seperti pembelian, klaim, atau analitik. Manfaat layanan mikro termasuk kelincahan, penskalaan yang fleksibel, penyebaran yang mudah, kode yang dapat digunakan kembali, dan ketahanan. Untuk informasi selengkapnya, lihat Mengintegrasikan layanan mikro dengan menggunakan layanan tanpa AWS server.

arsitektur microservices

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

Program Percepatan Migrasi (MAP)

AWS Program yang menyediakan dukungan konsultasi, pelatihan, dan layanan untuk membantu organisasi membangun fondasi operasional yang kuat untuk pindah ke cloud, dan untuk membantu mengimbangi biaya awal migrasi. MAP mencakup metodologi migrasi untuk

mengeksekusi migrasi lama dengan cara metodis dan seperangkat alat untuk mengotomatisasi dan mempercepat skenario migrasi umum.

migrasi dalam skala

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

pabrik migrasi

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

metadata migrasi

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

pola migrasi

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

Penilaian Portofolio Migrasi (MPA)

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

Penilaian Kesiapan Migrasi (MRA)

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

strategi migrasi

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

ML

Lihat pembelajaran mesin.

modernisasi

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

penilaian kesiapan modernisasi

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

aplikasi monolitik (monolit)

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

perjanjian tingkat operasional (OLA)

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

Tinjauan Kesiapan Operasional (ORR)

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

teknologi operasional (OT)

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

integrasi operasi (OI)

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

jejak organisasi

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

manajemen perubahan organisasi (OCM)

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

kontrol akses asal (OAC)

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

identitas akses asal (OAI)

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

ORR

Lihat tinjauan kesiapan operasional.

OT

Lihat teknologi operasional.

keluar (jalan keluar) VPC

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

P

batas izin

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

Informasi Identifikasi Pribadi (PII)

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

PII

Lihat informasi yang dapat diidentifikasi secara pribadi.

buku pedoman

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

PLC

Lihat pengontrol logika yang dapat diprogram.

PLM

Lihat manajemen siklus hidup produk.

kebijakan

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

persistensi poliglot

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

penilaian portofolio

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

predikat

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

predikat pushdown

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

kontrol preventif

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

principal

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

privasi berdasarkan desain

Pendekatan rekayasa sistem yang memperhitungkan privasi melalui seluruh proses pengembangan.

zona host pribadi

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

kontrol proaktif

Kontrol keamanan yang dirancang untuk mencegah penyebaran sumber daya yang tidak sesuai. Kontrol ini memindai sumber daya sebelum disediakan. Jika sumber daya tidak sesuai dengan kontrol, maka itu tidak disediakan. Untuk informasi selengkapnya, lihat panduan referensi Kontrol

dalam AWS Control Tower dokumentasi dan lihat Kontrol proaktif dalam Menerapkan kontrol keamanan pada AWS.

manajemen siklus hidup produk (PLM)

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

lingkungan produksi

Lihat lingkungan.

pengontrol logika yang dapat diprogram (PLC)

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

rantai cepat

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

pseudonimisasi

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

publish/subscribe (pub/sub)

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

Q

rencana kueri

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

regresi rencana kueri

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

R

Matriks RACI

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

LAP

Lihat Retrieval Augmented Generation.

ransomware

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

Matriks RASCI

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

RCAC

Lihat kontrol akses baris dan kolom.

replika baca

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

arsitek ulang

Lihat 7 Rs.

tujuan titik pemulihan (RPO)

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

tujuan waktu pemulihan (RTO)

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

refactor

Lihat 7 Rs.

Region

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

regresi

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

rehost

Lihat 7 Rs.

melepaskan

Dalam proses penyebaran, tindakan mempromosikan perubahan pada lingkungan produksi.

memindahkan

Lihat 7 Rs.

memplatform ulang

Lihat 7 Rs.

pembelian kembali

Lihat 7 Rs.

ketahanan

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

kebijakan berbasis sumber daya

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

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

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

kontrol responsif

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

melestarikan

Lihat 7 Rs.

pensiun

Lihat 7 Rs.

Retrieval Augmented Generation (RAG)

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

rotasi

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

kontrol akses baris dan kolom (RCAC)

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

RPO

Lihat tujuan titik pemulihan.

RTO

Lihat tujuan waktu pemulihan.

buku runbook

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

D

SAML 2.0

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

SCADA

Lihat kontrol pengawasan dan akuisisi data.

SCP

Lihat kebijakan kontrol layanan.

Rahasia

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

keamanan dengan desain

Pendekatan rekayasa sistem yang memperhitungkan keamanan melalui seluruh proses pengembangan.

kontrol keamanan

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

pengerasan keamanan

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

sistem informasi keamanan dan manajemen acara (SIEM)

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

otomatisasi respons keamanan

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

enkripsi sisi server

Enkripsi data di tujuannya, oleh Layanan AWS yang menerimanya.

kebijakan kontrol layanan (SCP)

Kebijakan yang menyediakan kontrol terpusat atas izin untuk semua akun di organisasi. AWS Organizations SCP menentukan pagar pembatas atau menetapkan batasan pada tindakan yang dapat didelegasikan oleh administrator kepada pengguna atau peran. Anda dapat menggunakan SCP sebagai daftar izin atau daftar penolakan, untuk menentukan layanan atau tindakan mana

yang diizinkan atau dilarang. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan dalam AWS Organizations dokumentasi.

titik akhir layanan

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

perjanjian tingkat layanan (SLA)

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

indikator tingkat layanan (SLI)

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

tujuan tingkat layanan (SLO)

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

model tanggung jawab bersama

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

Bayangan AI

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

SIEM

Lihat informasi keamanan dan sistem manajemen acara.

titik kegagalan tunggal (SPOF)

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

SLA

Lihat perjanjian tingkat layanan.

SLI

Lihat indikator tingkat layanan.

SLO

Lihat tujuan tingkat layanan.

model split-and-seed

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

SPOF

Lihat satu titik kegagalan.

skema bintang

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

pola ara pencekik

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

subnet

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

kontrol pengawasan dan akuisisi data (SCADA)

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

enkripsi simetris

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

pengujian sintetis

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

sistem prompt

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

T

tag

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

variabel target

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

daftar tugas

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

lingkungan uji

Lihat lingkungan.

pelatihan

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

alat

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

gerbang transit

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

alur kerja berbasis batang

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

akses tepercaya

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

penyetelan

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

tim dua pizza

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

U

waswas

Sebuah konsep yang mengacu pada informasi yang tidak tepat, tidak lengkap, atau tidak diketahui yang dapat merusak keandalan model ML prediktif. Ada dua jenis ketidakpastian:

ketidakpastian epistemik disebabkan oleh data yang terbatas dan tidak lengkap, sedangkan ketidakpastian aleatorik disebabkan oleh kebisingan dan keacakan yang melekat dalam data.

tugas yang tidak terdiferensiasi

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

lingkungan atas

Lihat lingkungan.

V

menyedot debu

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

kendali versi

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

Peering VPC

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

kerentanan

Kelemahan perangkat lunak atau perangkat keras yang membahayakan keamanan sistem.

W

cache hangat

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

data hangat

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

fungsi jendela

Fungsi SQL yang melakukan perhitungan pada sekelompok baris yang berhubungan dengan catatan saat ini. Fungsi jendela berguna untuk memproses tugas, seperti menghitung rata-rata bergerak atau mengakses nilai baris berdasarkan posisi relatif dari baris saat ini.

beban kerja

Kumpulan sumber daya dan kode yang memberikan nilai bisnis, seperti aplikasi yang dihadapi pelanggan atau proses backend.

aliran kerja

Grup fungsional dalam proyek migrasi yang bertanggung jawab atas serangkaian tugas tertentu. Setiap alur kerja independen tetapi mendukung alur kerja lain dalam proyek. Misalnya, alur kerja portofolio bertanggung jawab untuk memprioritaskan aplikasi, perencanaan gelombang, dan mengumpulkan metadata migrasi. Alur kerja portofolio mengirimkan aset ini ke alur kerja migrasi, yang kemudian memigrasikan server dan aplikasi.

CACING

Lihat menulis sekali, baca banyak.

WQF

Lihat AWS Kerangka Kualifikasi Beban Kerja.

tulis sekali, baca banyak (WORM)

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

Z

eksploitasi zero-day

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

kerentanan zero-day

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

bisikan zero-shot

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

aplikasi zombie

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

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