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

AWS Panduan Preskriptif

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

Table of Contents

Pengantar 1
Crawl 3
  Rencana 3
    Ruang lingkup keamanan 4
    Model keamanan 7
    Model tujuan bisnis 12
  Build 13
  Menilai 15
    Prowler 16
    AWS Security Hub CSPM 16
Berjalan 17
  Mengoperasionalkan 17
    AWS Kerangka Adopsi Cloud 17
    Hasil yang diharapkan 18
  Dewasa 20
    Proses 20
    Alat 22
    Risiko 24
    Contoh 24
Jalankan 28
  Pengoptimalan 28
Kesimpulan 31
Sumber daya 34
  Kerangka kerja dan model 34
  Layanan AWS 34
  AWS Sumber daya lainnya 34
Kontributor 35
  Mengotorisasi 35
  Meninjau 35
  Penulisan teknis 35
Riwayat dokumen 36
 xxxvii

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

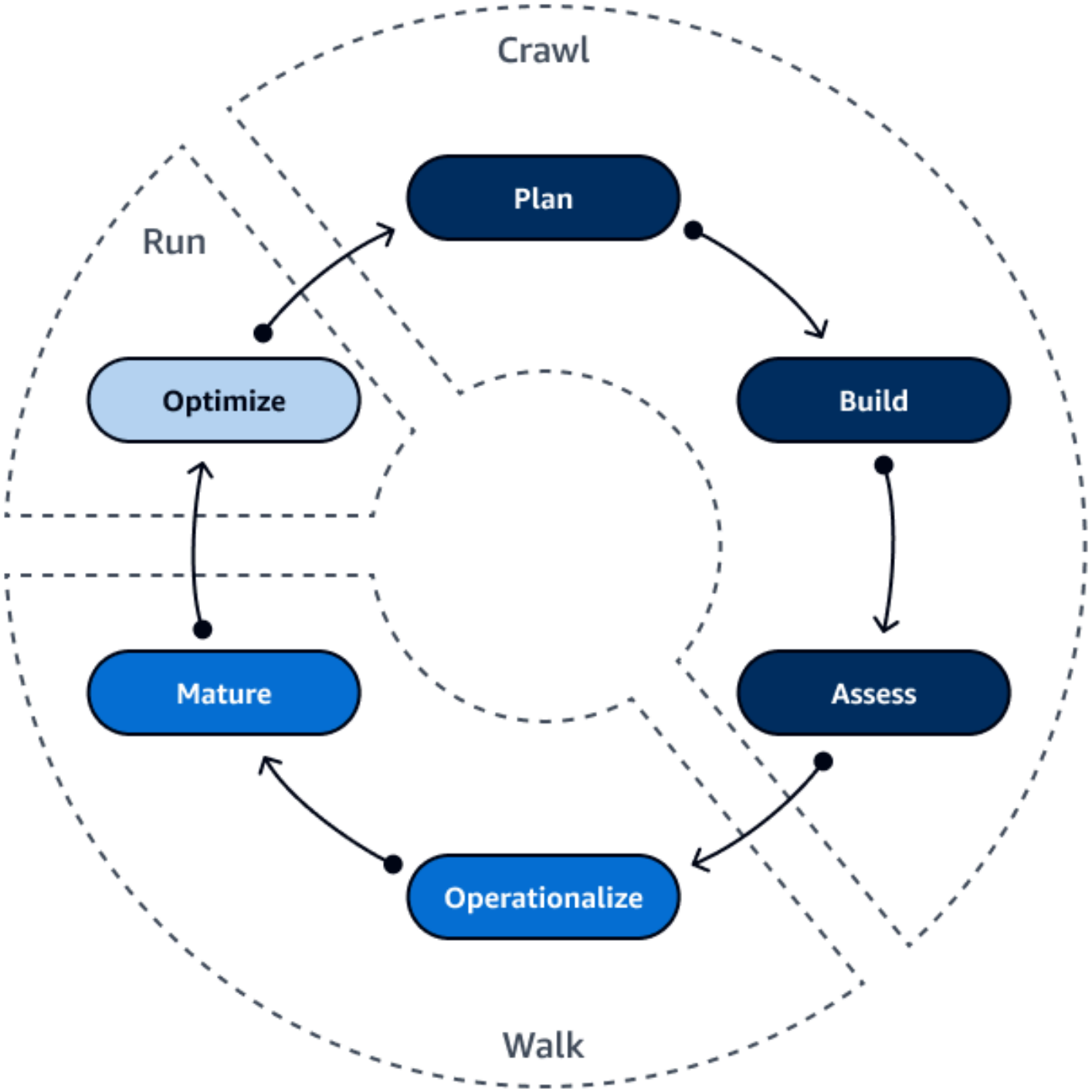
Amazon Web Services (kontributor)

Desember 2023 (riwayat dokumen)

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

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

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



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

Tahap merangkak: Merencanakan, membangun, dan menilai

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

Berikut ini adalah fase dalam tahap merangkak:

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

Rencana: Menetapkan ruang lingkup dan model keamanan Anda

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

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

Saat Anda mengembangkan rencana Anda, pertimbangkan hal berikut:

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

Memahami ruang lingkup keamanan

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

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

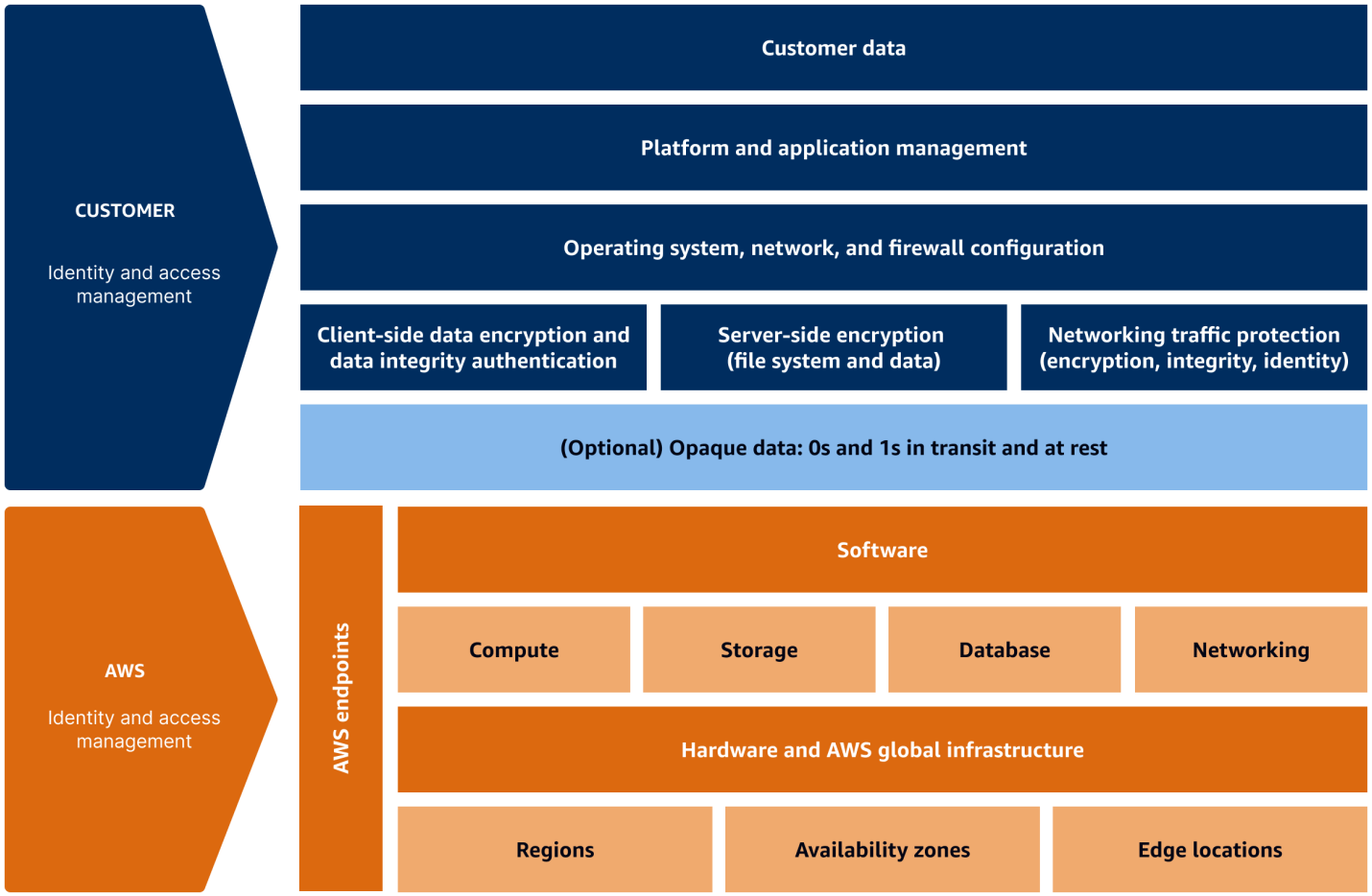
Berikut ini adalah tiga contoh layanan yang berbeda untuk membantu Anda memahami bagaimana cakupan keamanan Anda berubah berdasarkan layanan yang Anda pilih:

- Layanan infrastruktur
- Layanan kontainer
- Layanan tanpa server

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

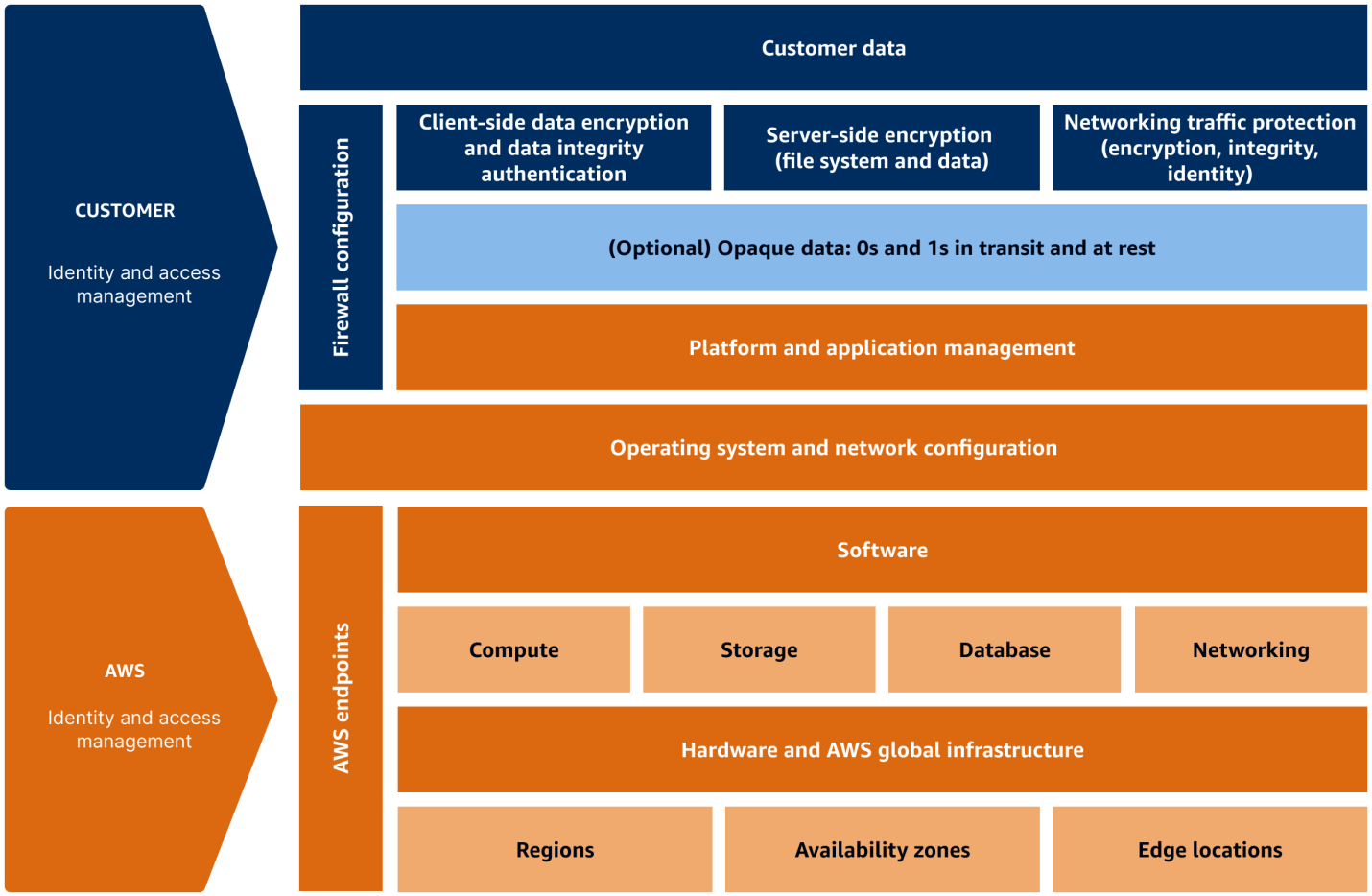
Layanan infrastruktur

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



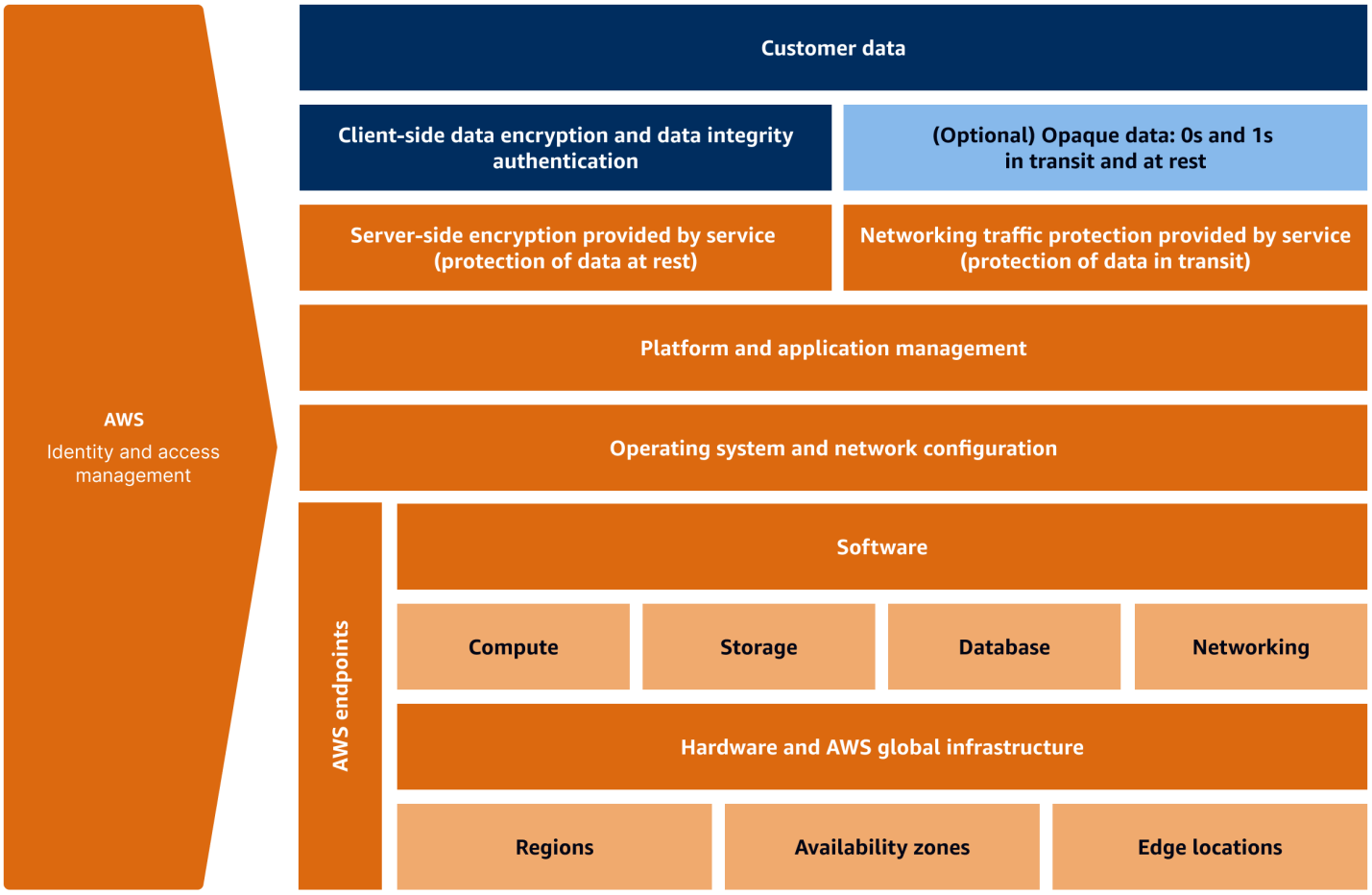
Layanan kontainer

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



Layanan tanpa server

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



Memilih model keamanan

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

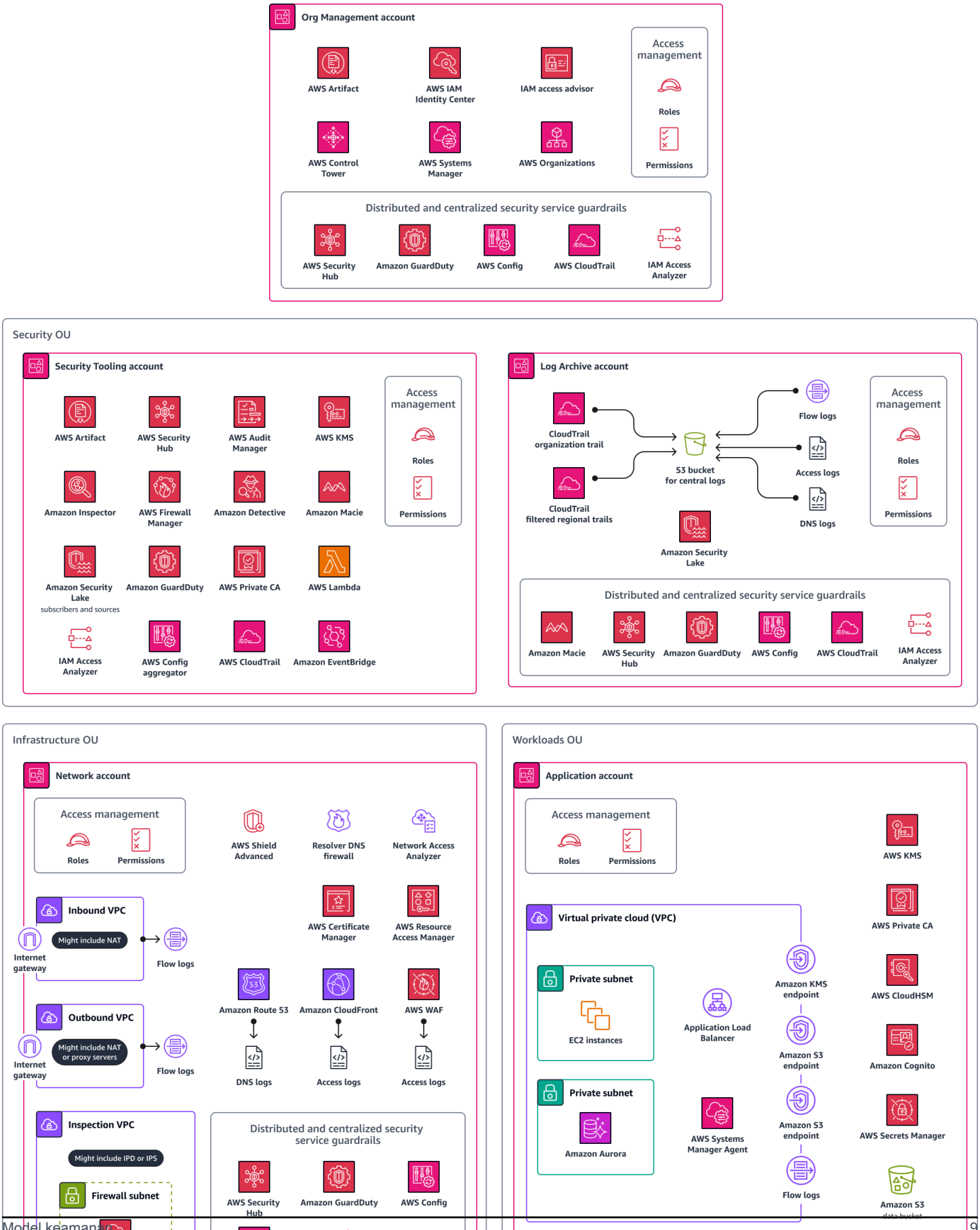
Berikut ini adalah beberapa model umum:

- Model arsitektur
- Model kedewasaan
- Model tata kelola

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

Model arsitektur

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


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

Keuntungan dari model arsitektur:

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

Kerugian dari model arsitektur:

- Berfokus pada teknologi daripada berfokus pada bisnis

Model kedewasaan

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

Keuntungan dari model kematangan:

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

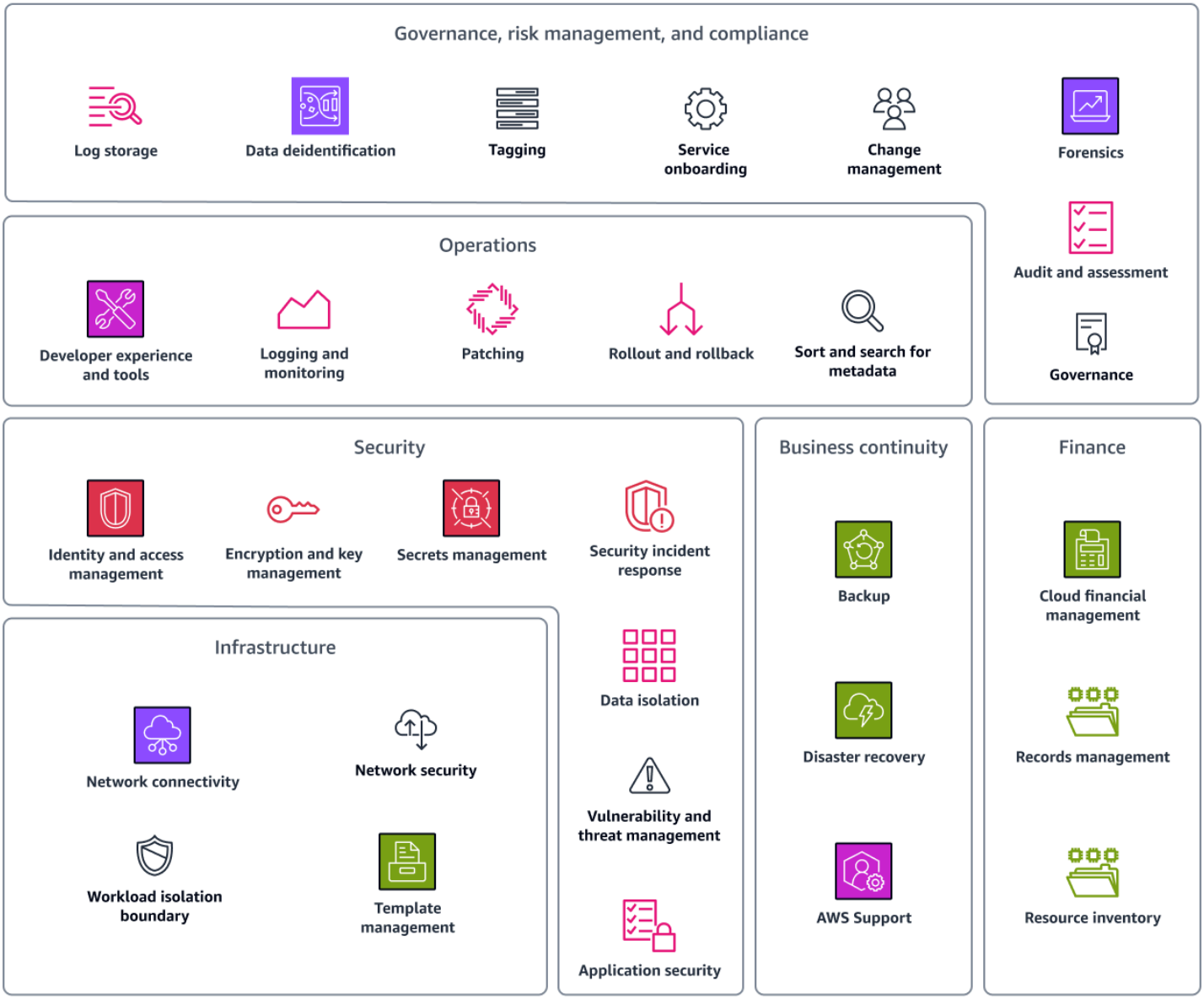
Kerugian dari model kematangan:

- Berfokus pada teknologi daripada berfokus pada bisnis

Model tata kelola

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

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



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

- Tata kelola, manajemen risiko, dan kepatuhan
- Operasi

- Keamanan
- Kelanjutan bisnis
- Keuangan
- Infrastruktur

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

Keuntungan dari model tata kelola:

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

Kerugian dari model tata kelola:

- Berfokus pada teknologi daripada berfokus pada bisnis

Menciptakan model tujuan bisnis

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

Keuntungan dari pendekatan objektif bisnis:

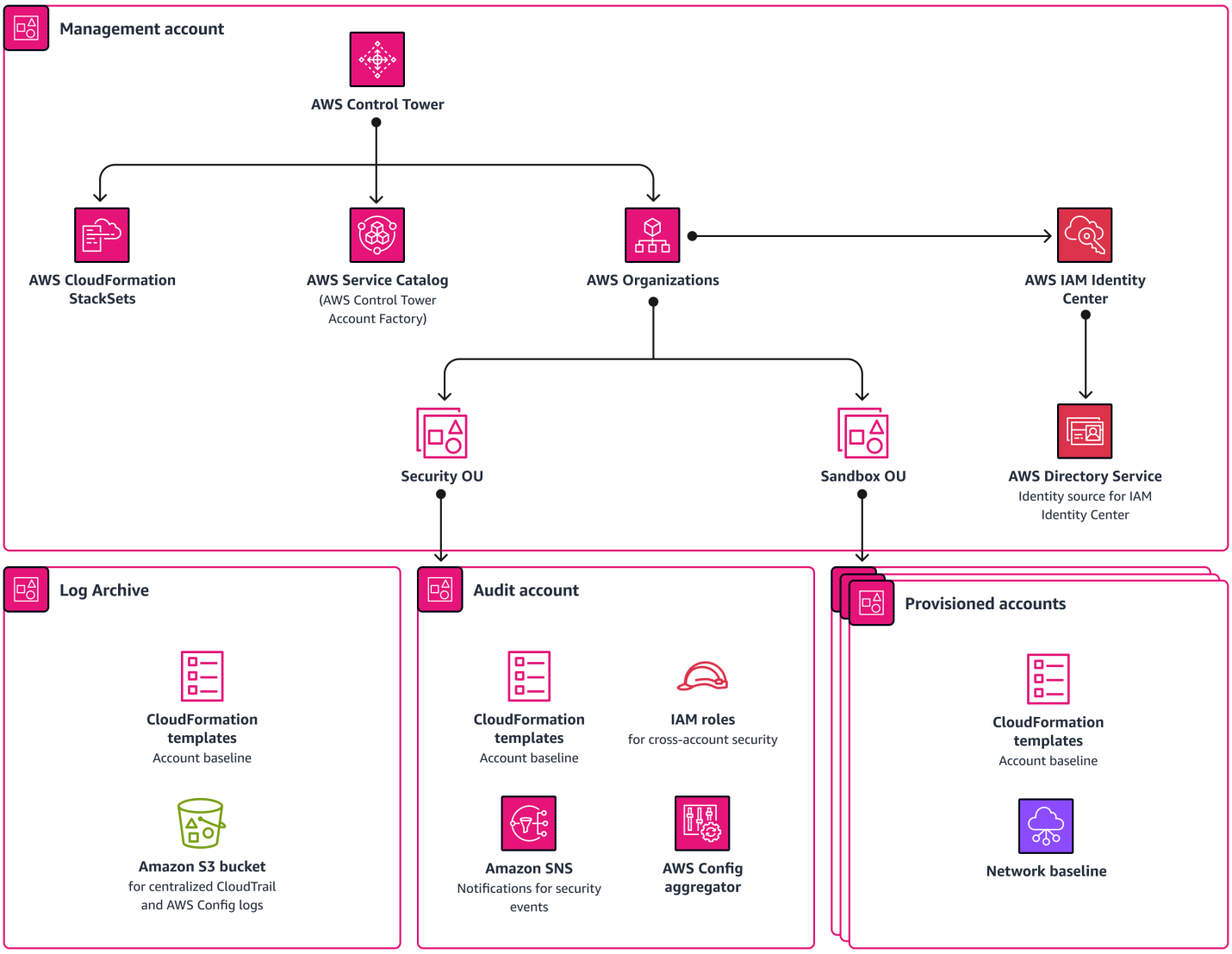
- Termasuk pembenaran biaya
- Memberikan arah keamanan yang jelas dan selaras dengan bisnis
- Mendefinisikan ukuran keberhasilan melalui pencapaian target hasil bisnis

Kerugian dari pendekatan objektif bisnis:

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

Membangun: Meletakkan dasar untuk fondasi keamanan cloud yang kuat

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



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

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

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

- Multi-account manajemen
- Identitas dan manajemen akses federasi
- Arsip terpusat untuk log
- Cross-account akses audit
- End-user penyediaan akun
- Pemantauan dan pemberitahuan terpusat

Menilai: Mengevaluasi postur keamanan cloud Anda saat ini

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

Berikut ini adalah manfaat dari penilaian postur cloud:

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

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

Prowler

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

Berikut ini adalah manfaat dariProwler:

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

AWS Security Hub CSPM

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

Berikut ini adalah manfaat dari Security Hub CSPM:

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

Panggung berjalan: Operasionalisasi dan pematangan

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

Berikut ini adalah fase dalam tahap berjalan:

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

Operasionalisasi: Mempersiapkan organisasi Anda untuk postur keamanan cloud yang matang

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

AWS Kerangka Adopsi Cloud

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

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

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

Hasil yang diharapkan

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

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

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

Dewasa: Proses penyetelan dan pengukuran, alat, dan risiko

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

Pada fase ini, Anda:

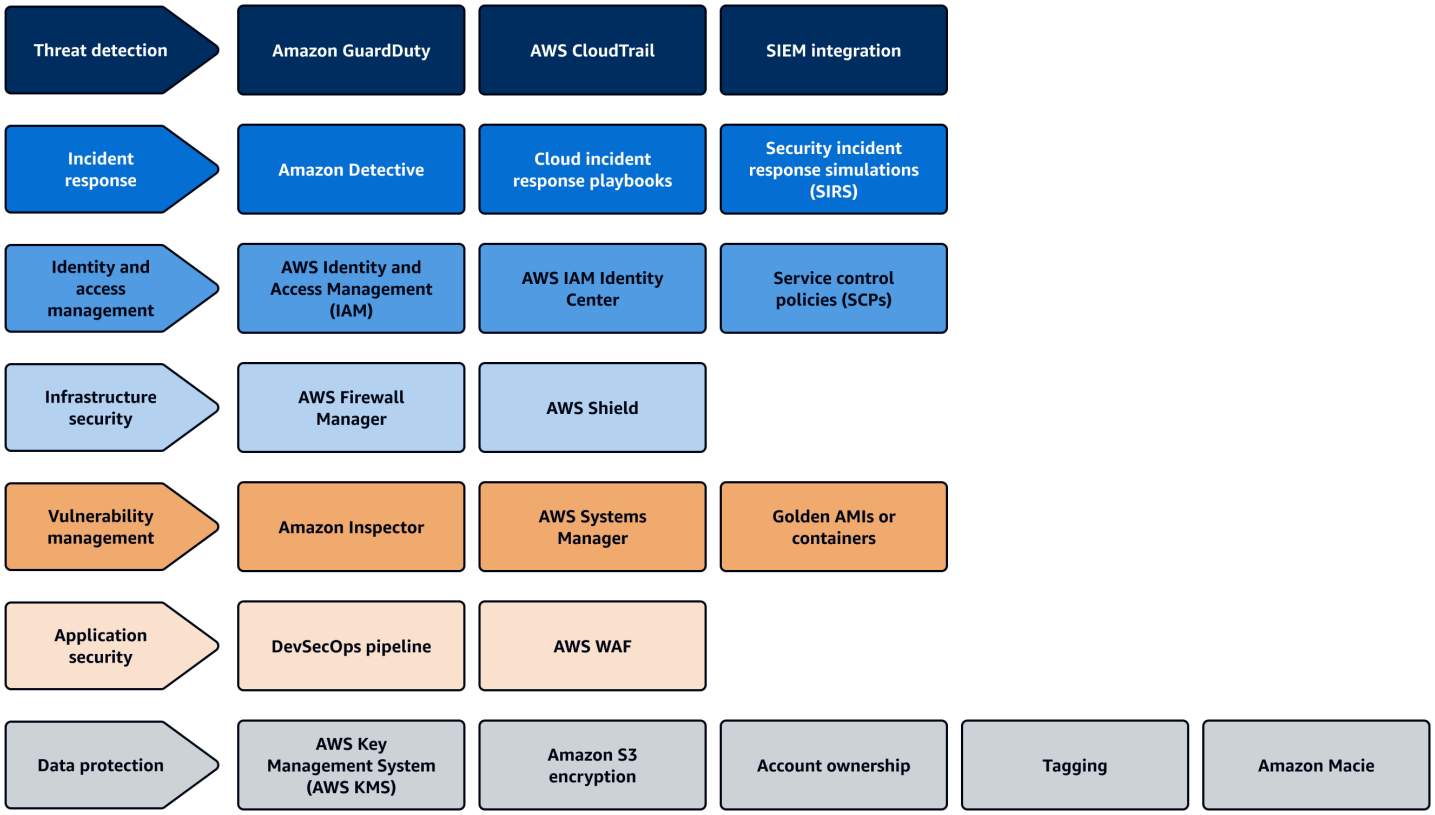
- Menyetel dan mengukur proses
- Menyetel dan mengukur alat
- Menyetel dan mengukur risiko
- Tinjau contoh kasus penggunaan pada fase matang

Menyetel dan mengukur proses

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

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

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



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

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

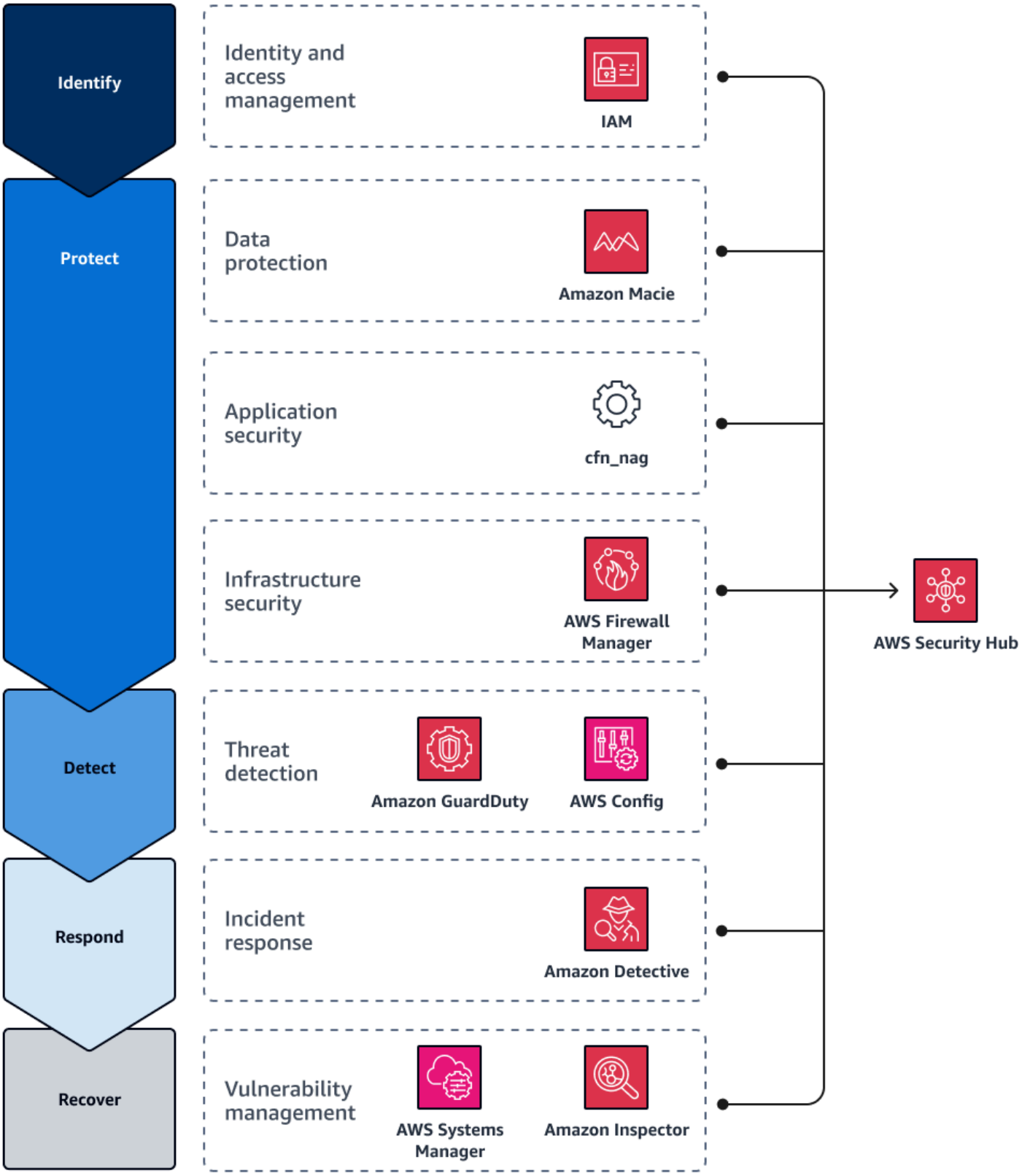
- Spesialisasi pada kategori yang ditentukan dalam AWS CAF, seperti yang ditunjukkan pada gambar sebelumnya.
- Agar lebih dinamis, fokuslah pada inovasi daripada operasi.

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

Menyetel dan mengukur alat

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

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



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

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

Menyetel dan mengukur risiko

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

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

Tinjau contoh kasus penggunaan pada fase matang

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

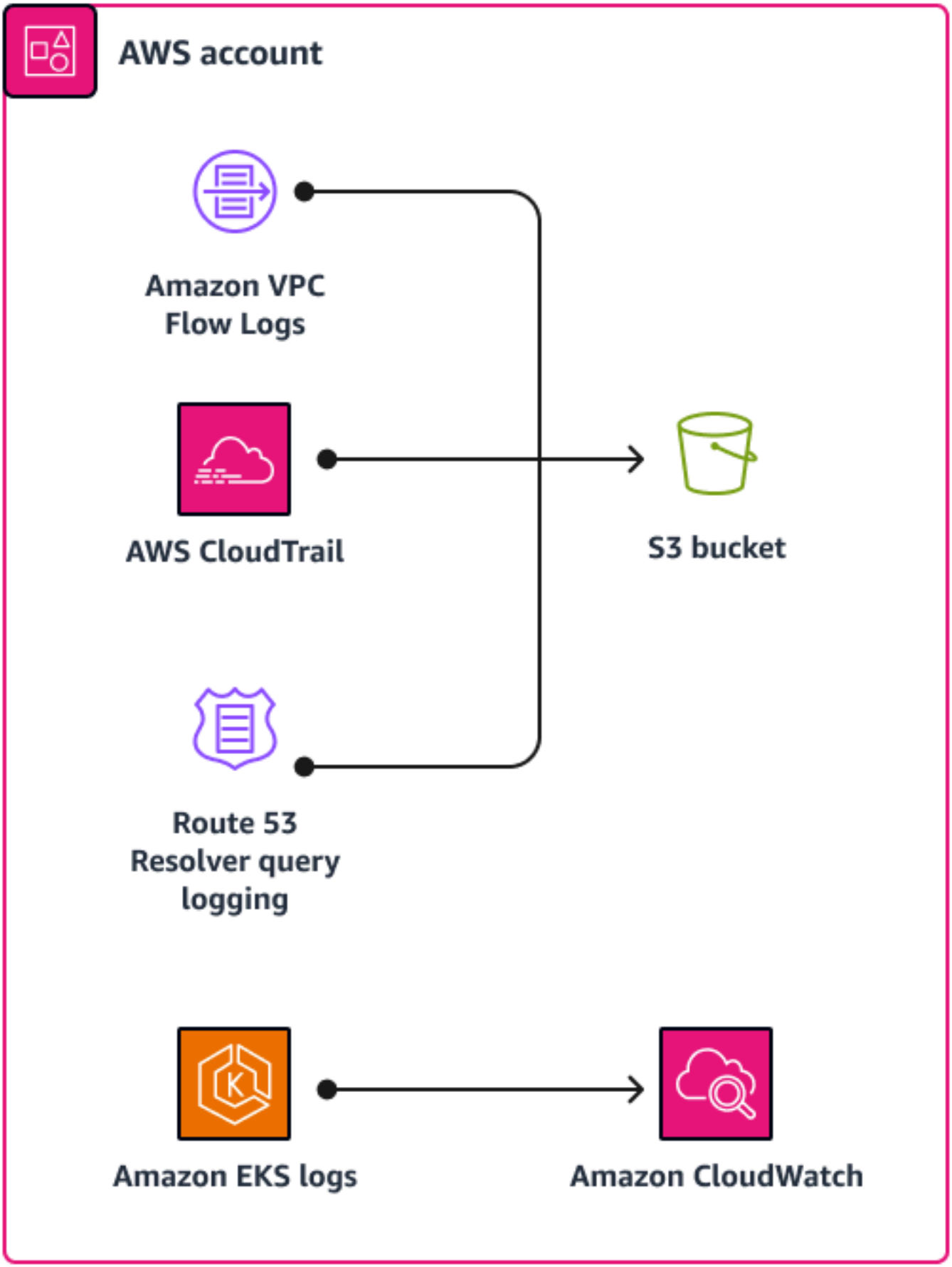
Dewasa: Contoh deteksi ancaman

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

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

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

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


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

Berikut ini adalah fitur utama dariAssisted Log Enabler for AWS:

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

Dewasa: Contoh IAM

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

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

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

Jalankan tahap: Mengoptimalkan operasi keamanan cloud Anda

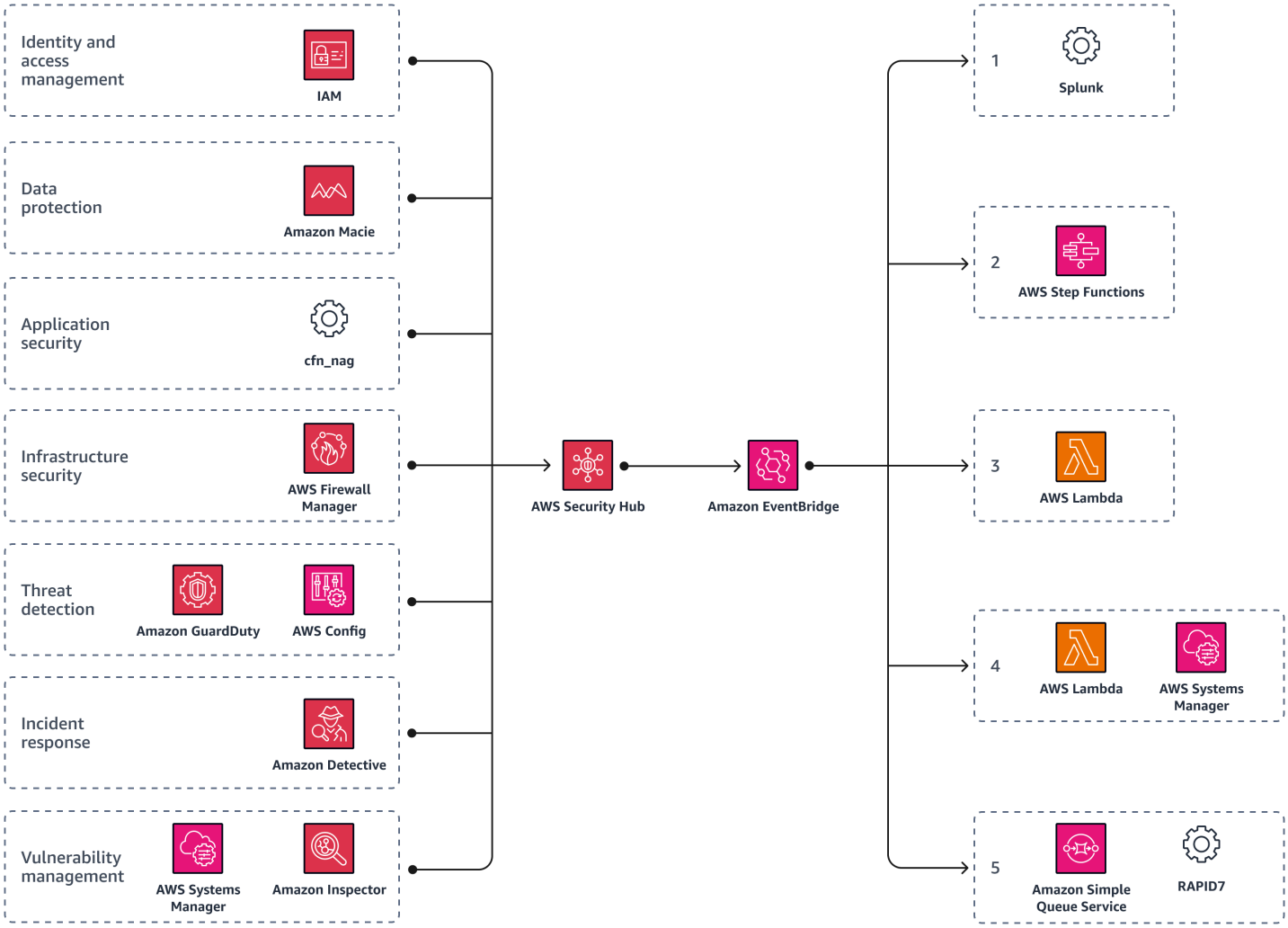
Setelah Anda menerapkan baseline di tahap berjalan, organisasi Anda maju ke tahap lari. Tahap ini difokuskan untuk menunjukkan kemampuan keamanan siber yang tersedia di cloud, banyak di antaranya tidak mungkin atau sangat sulit diterapkan dengan solusi lokal. Tahap ini menyatukan berbagai komponen keamanan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

Berikut ini adalah satu-satunya fase dalam tahap lari:

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

Optimalkan: Otomatiskan dan ulangi operasi keamanan cloud Anda

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



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

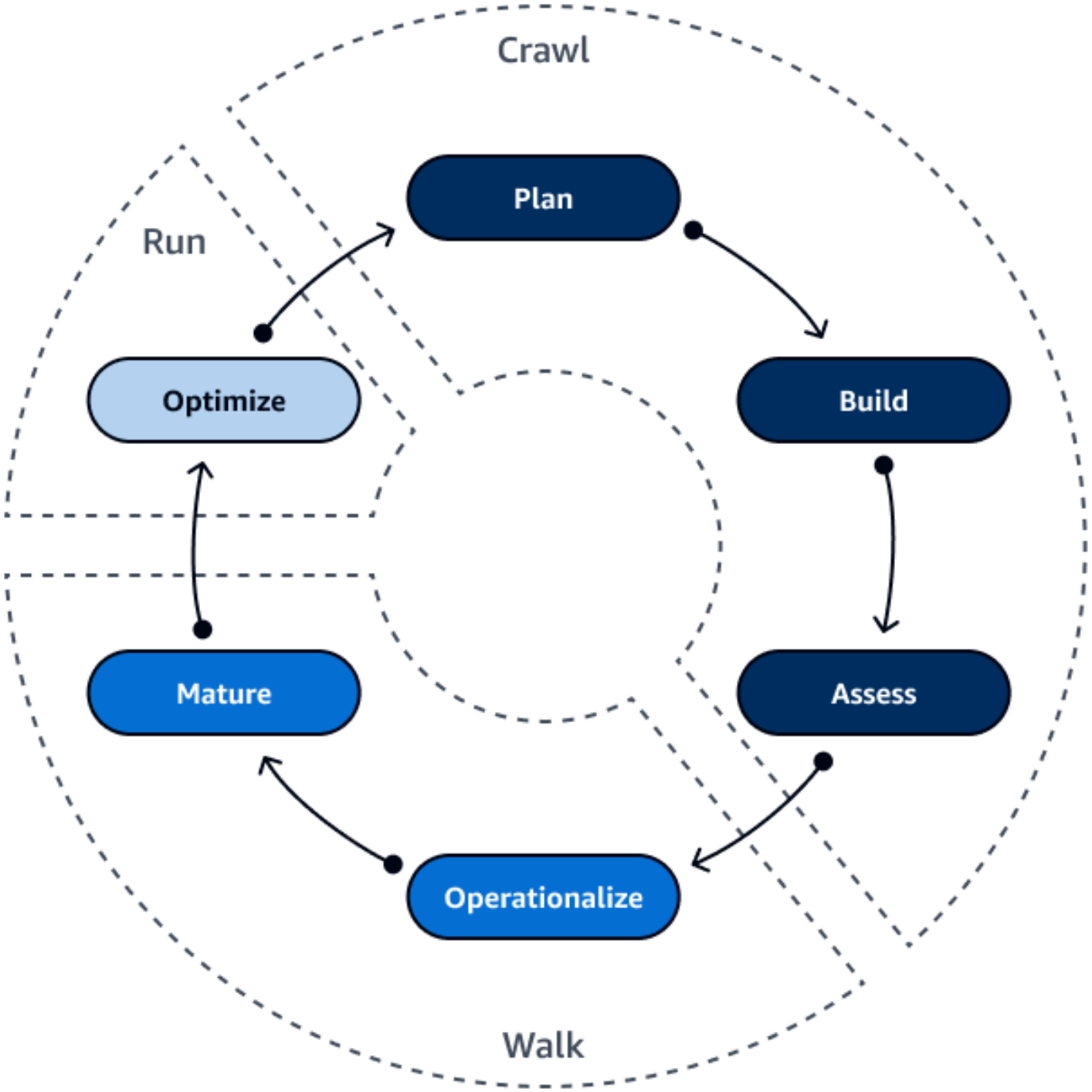
Berikut ini adalah contoh tindakan otomatis berulang, seperti yang ditunjukkan pada gambar sebelumnya:

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

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

Kesimpulan: Merangkak, berjalan, lari, lalu terbang!

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



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

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

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

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

Sumber daya

Kerangka kerja dan model

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

Layanan AWS

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

AWS Sumber daya lainnya

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

Kontributor

Individu berikut berkontribusi pada panduan ini.

Mengotorisasi

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

Meninjau

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

Penulisan teknis

- Lilly AbouHarb, Penulis Teknis Senior, AWS

Riwayat dokumen

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

Perubahan	Deskripsi	Tanggal
Publikasi awal	—	20 Desember 2023

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