aws

爬取、行走、執行：加速 中的安全成熟度 AWS 雲端

AWS 方案指引

AWS 方案指引: 爬取、行走、執行：加速 中的安全成熟度 AWS 雲端

Table of Contents

簡介 1
編目 3
計畫 3
安全範圍 4
安全模型 7
業務目標模型 12
建置 12
評估 14
Prowler 14
AWS Security Hub CSPM 15
Walk 16
操作化 16
AWS 雲端採用架構 16
預期成果 17
成熟 18
Processes 18
工具 20
Risk 22
範例 22
執行 26
最佳化 26
結論 29
資源 31
架構和模型 31
AWS 服務 31
其他 AWS 資源 31
貢獻者 32
編寫 32
檢閱 32
技術寫入 32
文件歷史紀錄 33
..... xxxiv

爬取、行走、執行：加速 中的安全成熟度 AWS 雲端

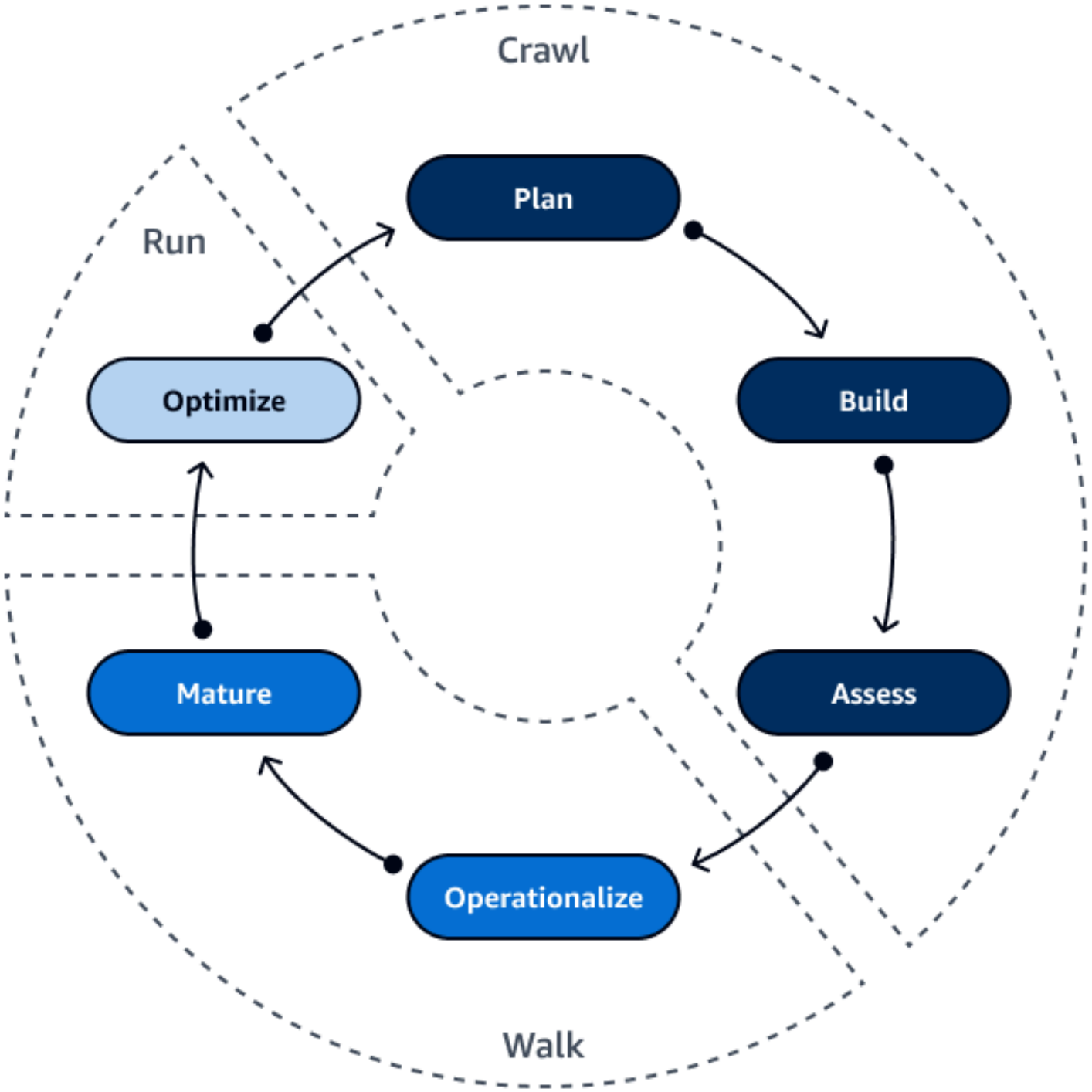
Amazon Web Services（貢獻者）

2023 年 12 月 (文件歷史記錄)

對於許多組織而言，安全是遷移至雲端時的第一要務和考量事項。實作雲端安全功能和控制不是一次性的活動，而是反覆的模型。隨著雲端操作的增加，您會逐漸提高安全狀態和成熟度。例如，您可以從 AWS 受管政策開始，然後在組織準備就緒時，您可以實作遵循最低權限原則的自訂政策。

本指南提供使用網路爬取、行走、執行方法加速組織雲端安全成熟度的藍圖。它定義step-by-step方法來自動化安全功能。它也以實際方式說明如何從 AWS 服務 和 功能中取得最多的功能。本指南可協助您了解雲端的挑戰和機會，以及如何快速向前邁進並取得成功 AWS。

雲端之旅需要建置架構、管理和使操作成熟，以及最佳化程序。下圖顯示爬蟲、行走、執行方法的每個階段中的階段：規劃、建置、評估、操作、成熟和最佳化。



爬蟲階段包含規劃、建置基礎和評估您目前的安全狀態。 在行走階段中，您會操作人員、程序和技術，然後透過調校和測量來成熟您的操作。執行階段包含透過評估和自動化進行最佳化。

爬蟲階段：規劃、建置和評估

爬蟲階段從規劃開始。規劃涉及確定安全範圍，並選擇最適合您組織的模型。建立計畫後，您可以開始建立基礎。接著評估您目前的安全狀態，並在您建置安全基礎設施後立即設定紀律。爬蟲階段是反覆的。雲端中的反覆運算比內部部署環境中的反覆運算更快。隨著雲端功能的成熟，反覆運算的程序會加速。

以下是爬蟲階段中的階段：

- 計畫 – 如何找出您的範圍並選取模型？
- 建置 – 您要如何建立架構？
- 評估 – 您目前的安全狀態為何？

計劃：建立您的安全範圍和模型

規劃是在您成熟安全模型時的反覆程序。規劃程序中的關鍵步驟包括：

- 了解安全範圍 – 安全範圍會有所不同，取決於雲端的使用方式。
- 選擇安全模型 – 識別最適合您安全使用案例的安全模型。
- 建立業務目標模型 – 定義明確的目標和機制以衡量成功。

當您制定計畫時，請考慮下列事項：

- 願意反覆運算。雲端中的反覆運算是固定的。反覆運算可協助您識別計劃中的差距。
- 請勿從 服務開始。從計畫開始，而不是挑選您需要的服務。這有助於推動您的組織實現其預期成果。

了解安全範圍

AWS 共同責任模型會定義您與 共同 AWS 承擔雲端安全與合規責任的方式。 會 AWS 保護執行 中提供之所有服務的基礎設施 AWS 雲端，而且您需負責保護對這些服務的使用，例如您的資料和應用程式。

此共用模型有助於減輕您的合規和操作負擔，因為 會 AWS 操作、管理和控制許多元件，從主機作業系統和虛擬化層，到服務操作所在設施的實體安全性。受管服務可讓您 AWS 管理一些安全任務，例如修補和漏洞管理，以協助您降低安全性和合規義務。使用受管服務是 AWS Well-Architected Framework 中的最佳實務。一般而言，隨著基礎設施的現代化，更多的責任會轉移到服務供應商。

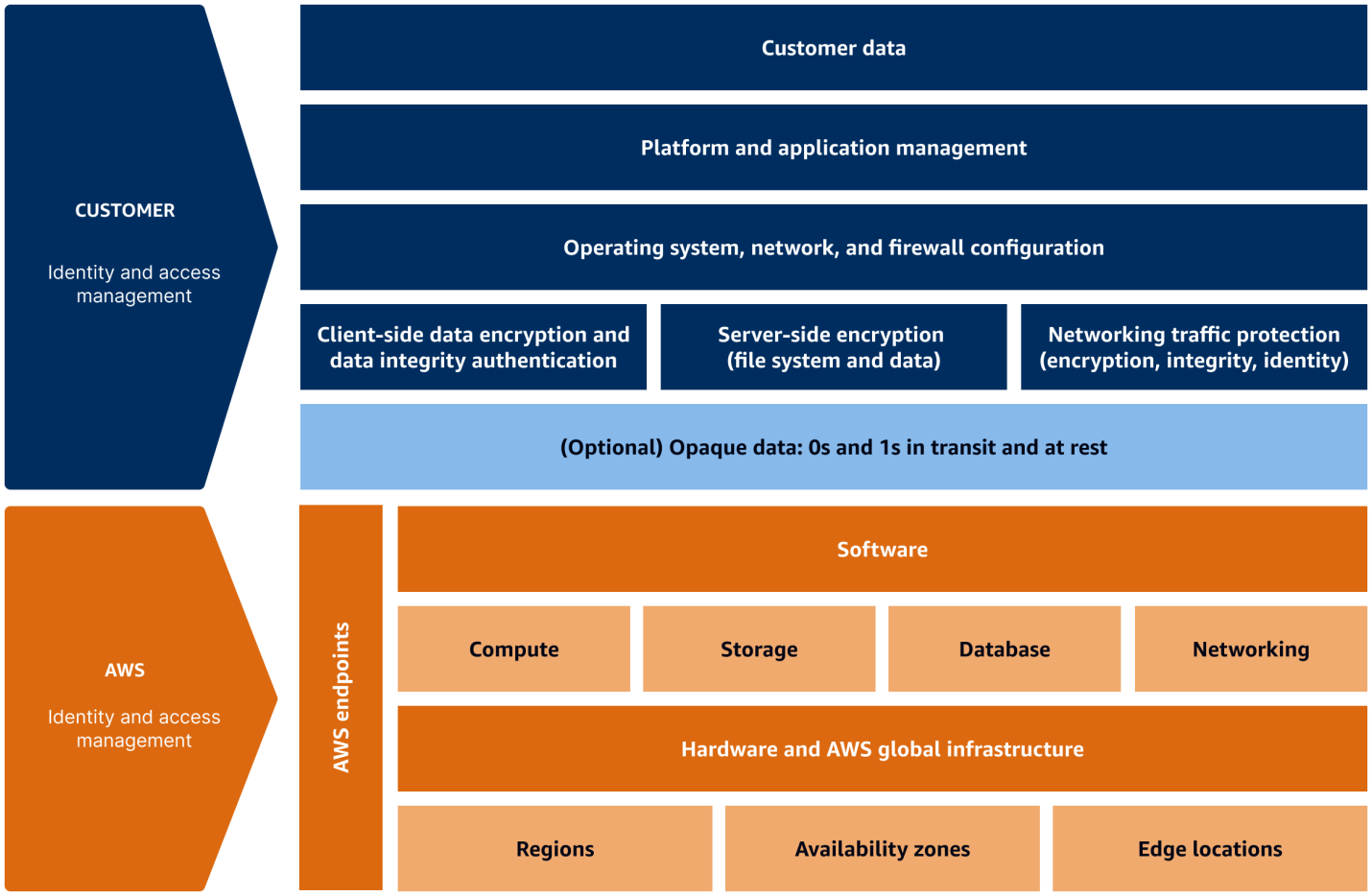
以下是三個不同的服務範例，可協助您了解安全範圍如何根據您選擇的服務而變更：

- 基礎設施服務
- 容器服務
- 無伺服器服務

您對安全的責任不是靜態的，而且會隨著您選擇的架構類型而改變。您的時間、精力和成本會受到您選擇的雲端架構影響。

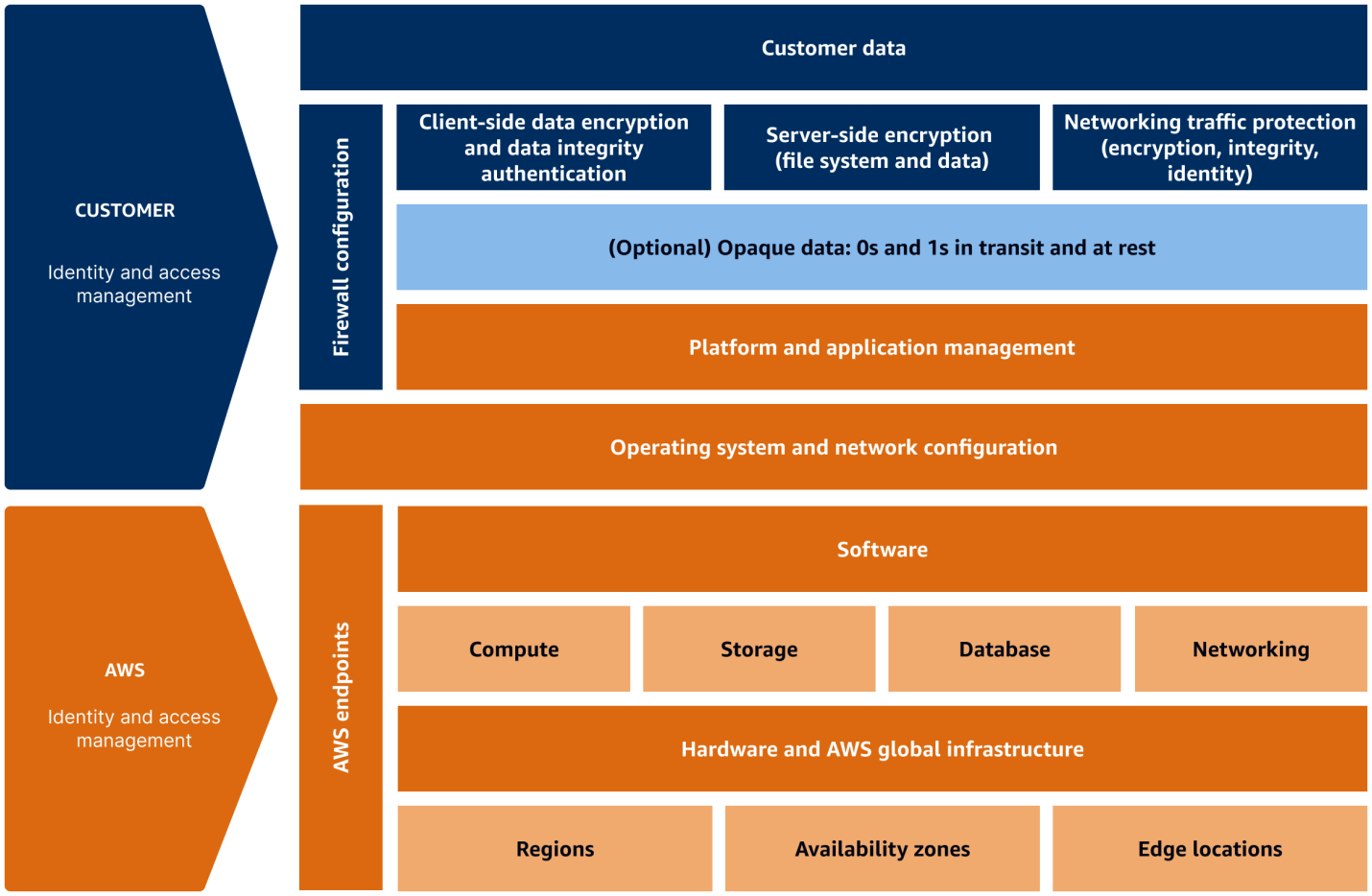
基礎設施服務

對於基礎設施服務， AWS 專注於保護基礎基礎設施。在基礎設施服務中，客戶的範圍較大，因為與其他模型相比，他們需要解決平台安全性、作業系統修補和應用程式管理的問題。Amazon Elastic Compute Cloud (Amazon EC2) 是常見基礎設施服務的範例。



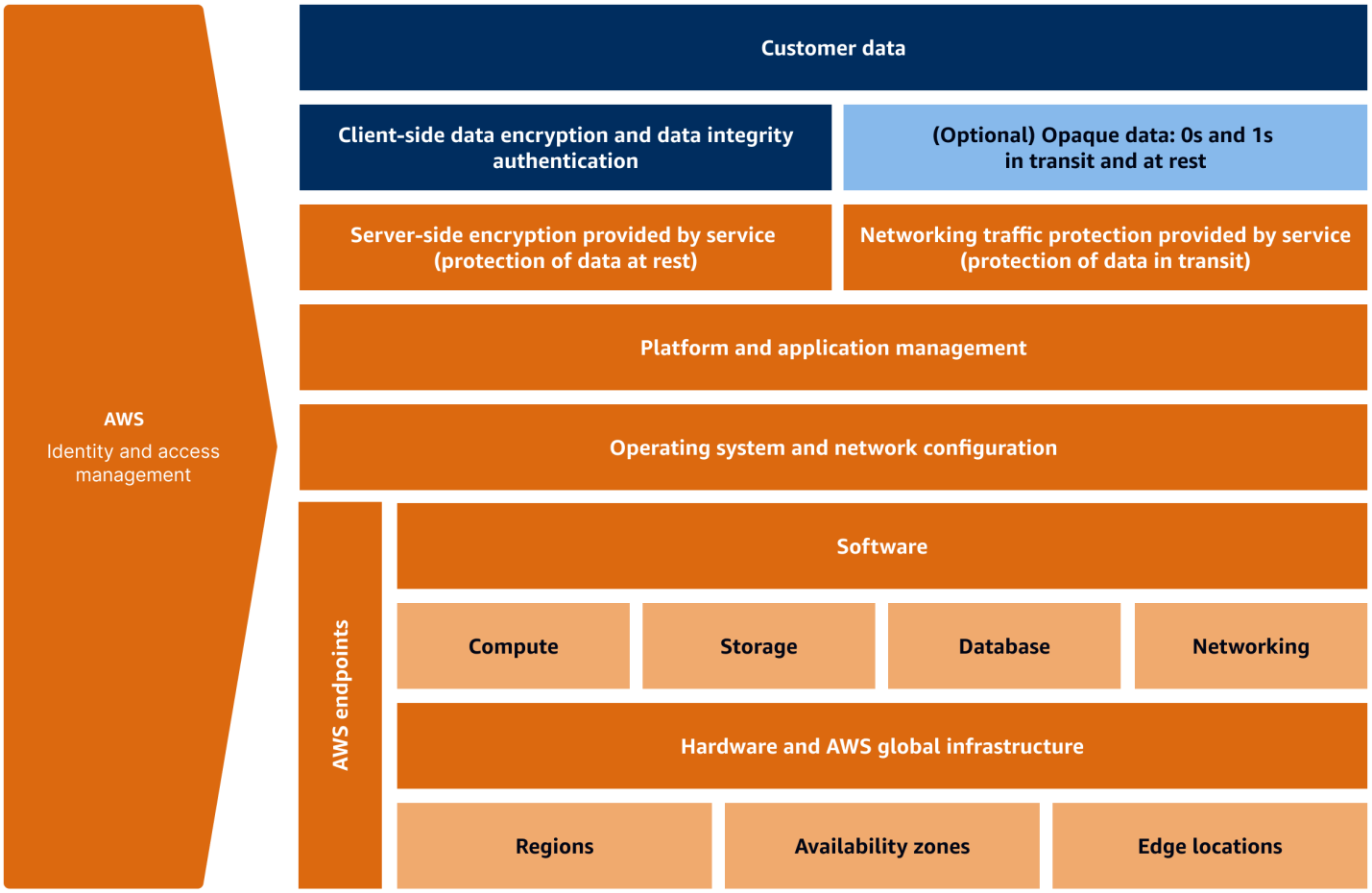
容器服務

隨著基礎設施的抽象化和現代化，足跡也會變小。您的範圍會縮小，因為某些安全元素的責任會轉移為 AWS。容器服務是一些後端責任轉移回的範例 AWS。例如， AWS 負責作業系統 (OS) 組態、網路組態、平台管理和應用程式管理。常見容器服務的範例包括 Amazon Elastic Kubernetes Service (Amazon EKS)、Amazon Elastic Container Registry (Amazon ECR)、Amazon Elastic Container Service (Amazon ECS) 和 AWS Fargate。



無伺服器服務

使用無伺服器服務時，幾乎所有的安全責任都屬於其中 AWS。您的責任範圍很小。例如，受管無伺服器資料庫 (DB) 不需要保護網路、硬體和作業系統。涵蓋所有作業系統和資料庫修補 AWS。您唯一的考量是透過加密和身分驗證來保護對資料的存取。



選擇安全模型

您可以從各種安全模型或方法中進行選擇 AWS。方法的選擇和最適合的模型取決於您的受眾、目標業務成果和整體業務流程。您可以使用多個模型的混合。

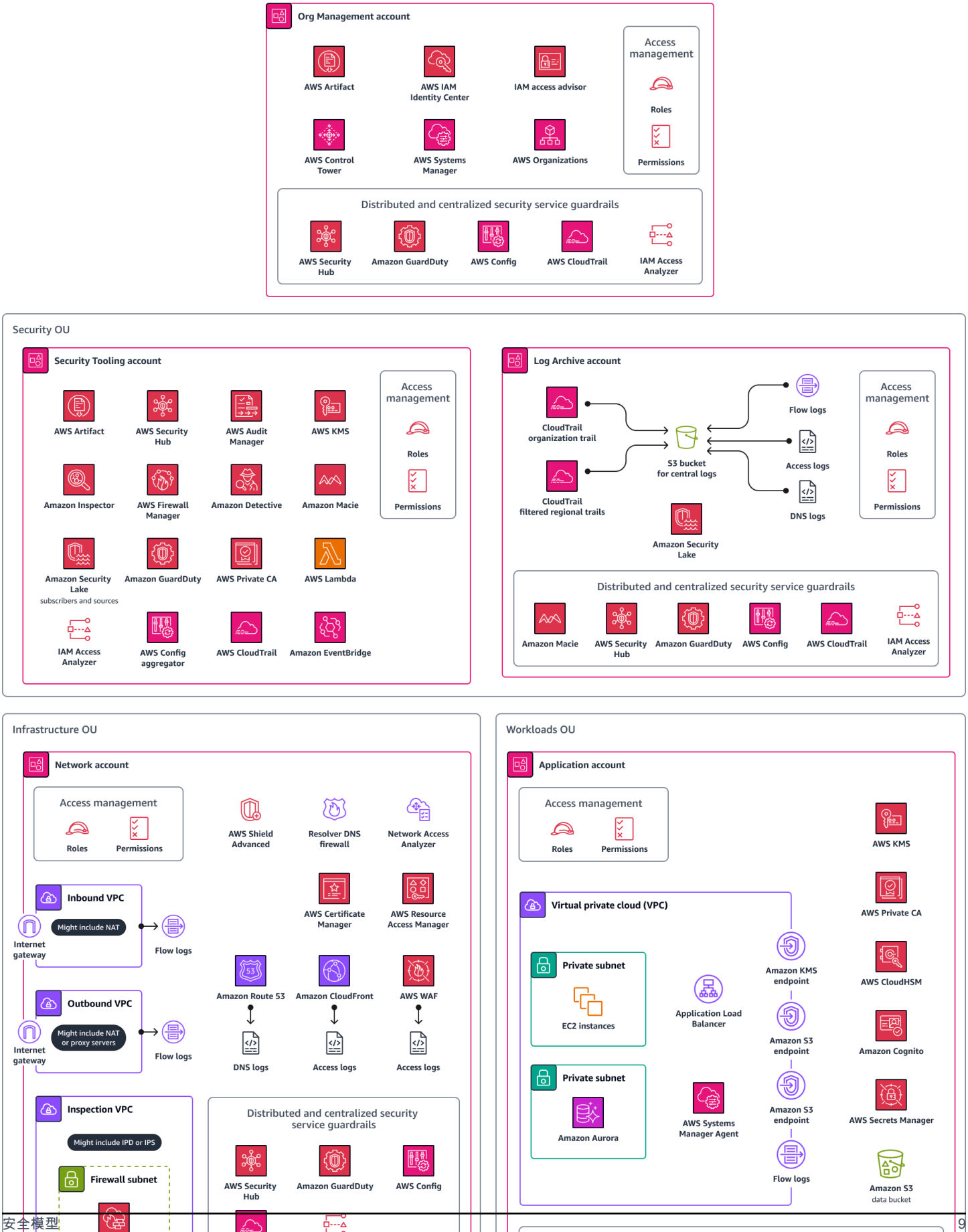
以下是一些常見的模型：

- 架構模型
- 成熟度模型
- 控管模型

每個模型都有自己的一組優點和缺點。請務必考慮哪種方法最適合您的組織。在現代化基礎設施和採用雲端策略的過程中，儘早讓安全專業人員參與其中。您選擇的模型會對組織中的角色和責任產生重大影響。

架構模型

下圖顯示 AWS 安全參考架構。這種架構方法提供安全模型的藍圖。當您與組織內的技術團隊互動時，此方法最適合您。它有助於設定 理想的未來狀態目標。它也符合許多合規和 AWS 架構。


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
Inbound VPC
Might include NAT
Internet gateway
Flow logs
AWS Certificate Manager
AWS Resource Access Manager
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
Shared Services account
Workloads OU
Application account
Access management
Roles
Permissions
AWS KMS
AWS Private CA
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
AWS CloudHSM
Amazon Cognito
AWS Secrets Manager
Amazon S3
data bucket
Distributed and centralized security service guardrails
Amazon Macie
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer

架構模型的優點：

- 符合健康保險流通與責任法案 (HIPAA) 和健康資訊信任聯盟共同安全架構 (HITRUST CSF) 要求
- 提供架構觀點
- 符合大型企業的雲端策略和指引
- 與AWS 雲端採用架構 (AWS CAF) 保持一致
- 與 AWS Well-Architected 架構保持一致

架構模型的缺點：

- 以技術為中心，而不是以業務為中心

成熟度模型

AWS 安全成熟度模型方法著重於透過優先實作安全措施來管理和降低風險。這種方法非常適合安全主管和 CISOs，但不是以業務為中心。

成熟度模型的優點：

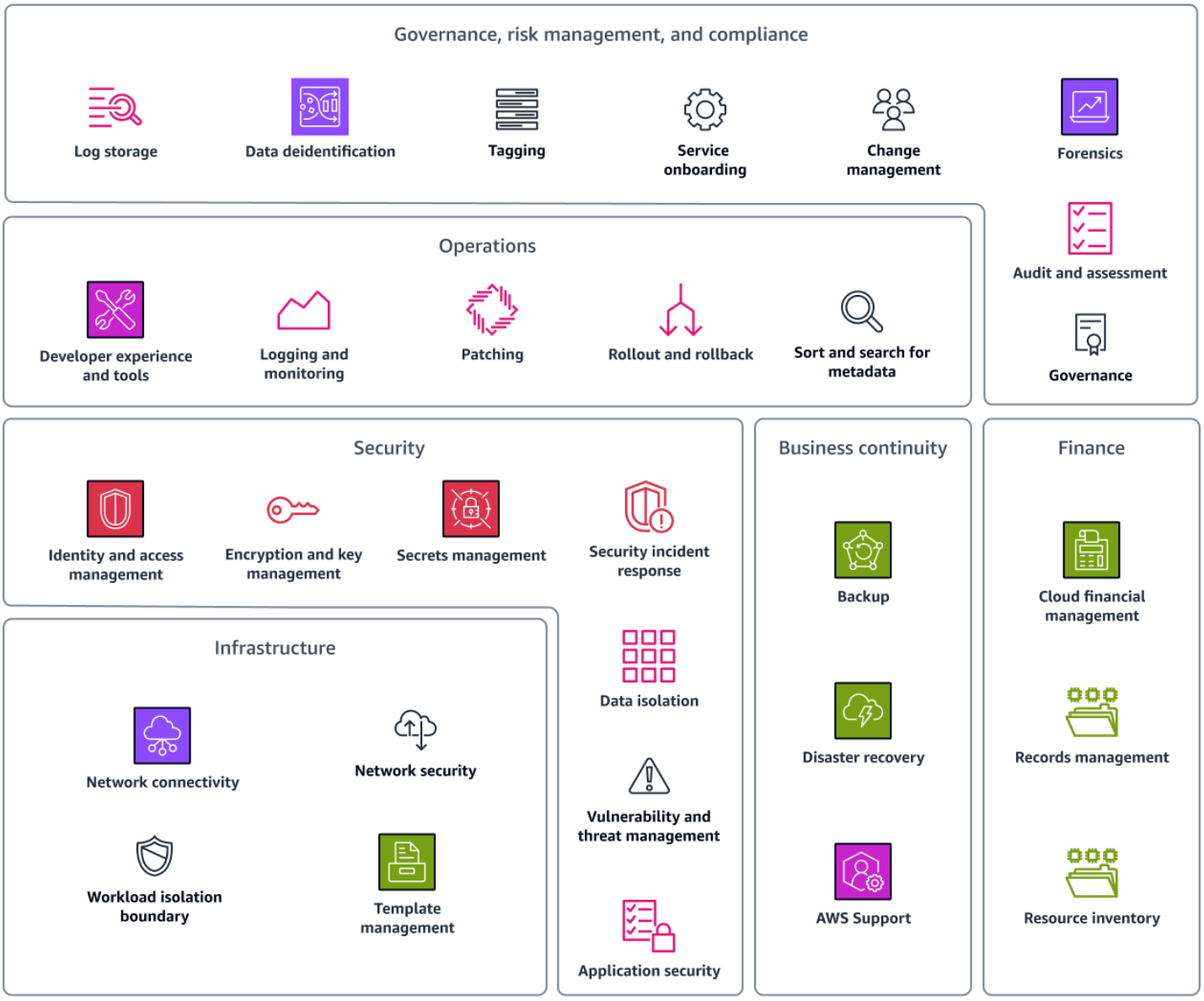
- 以安全為重心
- 是一種專注於使用敏捷型實作方法的模型
- 協助您快速降低風險
- 與AWS 雲端採用架構 (AWS CAF) 保持一致

成熟度模型的缺點：

- 以技術為中心，而不是以業務為中心

控管模型

Cloud Foundation on AWS Model 使用控管、風險管理和合規 (GRC) 方法來協助組織滿足安全和合規要求。它定義您的雲端環境應遵循的整體政策。此模型中的功能可協助您定義動作項目、定義您的風險偏好，以及調整內部政策。



Cloud Foundation 模型是一種功能和控管指南，可協助您建置和發展您的 AWS 雲端 環境。它以一組定義、案例、指引和自動化為基礎。本指南包含建立環境 AWS 雲端 的人員、程序和技術層面。它涵蓋雲端基礎所需的六個功能類別：

- 控管、風險管理和合規
- 作業
- 安全
- 業務持續性
- 財務
- 基礎設施

本指南也提供每個功能的範例、時間表和進一步閱讀。

控管模型的優點：

- 具有廣泛的技術焦點
- 專為可靠性而設計
- 使用操作方法

控管模型的缺點：

- 以技術為中心，而不是以業務為中心

建立業務目標模型

業務目標模型涉及定義業務成果。它類似於 AWS 雲端採用架構和 AWS Well-Architected 架構。這種方法著重於透過解讀目標業務成果來了解業務感興趣的內容。這種方法的價值在於，將業務目標與安全目標輕鬆關聯。業務目標的一個範例是「啟用安全外部連線並加速佈建新使用者和環境，方法是自動化可見性和根據最佳實務測量以持續降低風險。」 您可以建立技術目標，協助您達成對應的業務成果。業務目標模型與安全目標相關聯，例如維持可見性。然後，您實作技術目標，例如 AWS Identity and Access Management (IAM) 安全最佳實務，以降低安全風險。

業務目標方法的優點：

- 包含成本對正
- 提供清晰且符合業務的安全方向
- 透過實現目標業務成果來定義成功指標

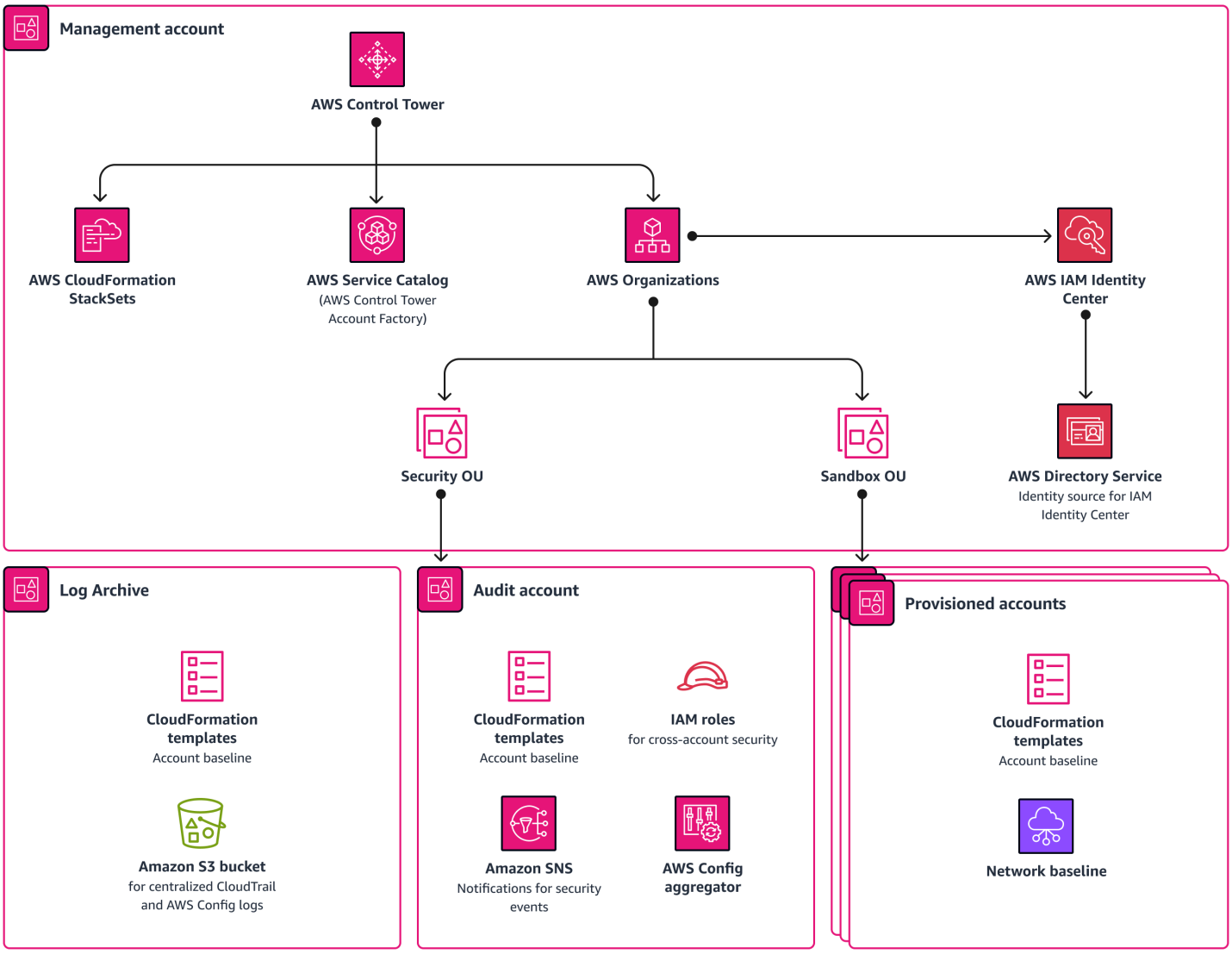
業務目標方法的缺點：

- 可能很耗時，因為您必須了解企業想要什麼
- 以業務為中心，而不是以技術為中心

建置：奠定穩固雲端安全基礎的基礎

現在您已有計劃，下一步是鋪設基礎。此步驟示範如何在 AWS 跨多個帳戶的安全、彈性、可擴展和自動化基礎上建立初始雲端基礎。根據您的業務目標，可以專門設計和自訂基礎。您可以根據新的登陸區

域調整控制項，也可以將其包含在現有的登陸區域中。中的自動化AWS Control Tower可協助您在 中鋪設安全基礎 AWS 雲端。下圖顯示透過 設定的登陸區域 AWS Control Tower。



AWS Control Tower AWS 服務 代表您協調多個 ，例如 AWS Organizations AWS Service Catalog和 AWS IAM Identity Center。您可以在一小時內設定新的登陸區域，該登陸區域旨在滿足您的安全和合規要求。 AWS Control Tower 會根據規範性安全最佳實務來設定您的登陸區域。 AWS Control Tower 透過增強對帳戶和最終使用者的可見性和控制，協助您管理雲端佈建。它可協助管理員有效率地配置和監督運算資源、實作角色型存取控制、透過記錄和監控工具來監控效能、有效管理成本、自動化部署程序、強制執行安全措施，並確保符合業界標準。

AWS Control Tower 根據最佳實務， 是設定和管理安全、合規、多帳戶 AWS 環境的最快方法。如需使用 的詳細資訊， AWS Control Tower 以及 AWS 多帳戶策略中概述的最佳實務，請參閱AWS 多帳戶策略：最佳實務指引。

雖然 AWS Control Tower 是最快的方法，但不是唯一的方法。重要部分是您設定至少提供下列項目的登陸區域：

- 多帳戶管理
- 身分和聯合存取管理
- 日誌的集中式封存
- 跨帳戶稽核存取權
- 最終使用者帳戶佈建
- 集中式監控和通知

評估：評估您目前的雲端安全狀態

在您將任何項目部署到登陸區域之前，請評估您的登陸區域，以確保其符合您的需求並建立基準。此實務稱為雲端狀態評估。它可協助您識別和修復整個雲端基礎設施的風險。評估您的雲端安全狀態可讓您了解雲端環境中的相關安全控制。

以下是雲端狀態評估的優點：

- 它可協助您了解目前的安全狀態，並取得建議，以減少您的風險設定檔、修復現有的漏洞，或修正設定錯誤。
- 它可協助您識別安全最佳實務，以避免失誤並降低業務風險。
- 它提供的指標可協助您追蹤改進並衡量成功。

本節會檢閱服務和工具， AWS Security Hub CSPM 以及 Prowler，您可以用來在環境中執行雲端狀態評估。

Prowler

Prowler 是一種開放原始碼命令列工具，可協助您評估、稽核和監控您的帳戶是否符合 AWS 安全最佳實務和其他安全架構和標準。它會檢查您的組態並識別安全問題。您可以在Prowler多帳戶環境中使用 ，而第三方供應商也可以使用它來評估 AWS 環境的安全性。

以下是 的優點Prowler：

- 它是免費的開放原始碼。
- 它具有靈活的部署選項，並且可擴展。

- 它執行合規檢查，例如 的網際網路安全中心 (CIS) 基準 AWS、一般資料保護法規 (GDPR) 和 HIPAA。
- 它可協助您建立快照和基準。

AWS Security Hub CSPM

AWS Security Hub CSPM 提供 中安全狀態的完整檢視 AWS。它還可協助您根據安全產業標準和最佳實務來檢查環境。它與 整合， AWS Control Tower 因此您可以透過 AWS Control Tower 服務設定 Security Hub CSPM 偵測控制。加速安全成熟度的目標是將評估程序從一次性快照成熟為持續監控進度的程序。

以下是 Security Hub CSPM 的優點：

- 它提供統一的儀表板，可顯示環境的目前狀態，並協助您識別和修復問題。
- 它會透過自動檢查執行持續評估。

行走階段：操作化和成熟

步行階段著重於操作。在此階段，您的組織需要評估其目前的操作模型、判斷應如何針對雲端進行調整、實作這些變更，然後測量進度。這包括處理技能、操作程序和技術。調校雲端部署和測量進度在整個步行階段都很重要，以驗證成功。

以下是行走階段中的階段：

- 操作化 – 如何為雲端的人員、技術和程序做好準備？
- 成熟 – 如何衡量進度和成功？

操作化：為您的組織做好成熟雲端安全狀態的準備

為了繼續將操作負載部署到雲端的程序，請務必專注於人員、程序和技術的一致性。這在雲端環境中特別重要，因為程序和技能可能與內部部署操作不同。在本節中，您使用架構來調整人員、程序和技術，然後確認架構已協助您實現預期成果。

AWS 雲端採用架構

AWS 雲端採用架構 (AWS CAF) 可協助您透過創新使用 AWS 服務 和 功能來加速業務成果。 AWS CAF 識別六個特定組織觀點，這些觀點有助於成功的雲端轉型：商業、人員、治理、平台、安全和營運。每個觀點都包含的功能可以改善雲端準備度，並協助您加速雲端轉型之旅。

下圖顯示 AWS CAF 中的六個觀點，以及每個觀點的功能。如需詳細資訊，請參閱 AWS 雲端採用架構概觀中的基礎功能。

預期成果

當您使用 AWS CAF 來調整人員、程序和技術時，您可以預期達到下列結果：

- DevSecOps 管道和 程序 – 使用整合式安全工具實作 DevOps 管道，可協助您更安全地部署基礎設施即程式碼 (IaC)。您可以在管道程序中實作程式碼掃描和安全檢查，例如 cfn_nag (GitHub)，這是開放原始碼靜態程式碼分析器。
- 標記和資產管理 – 標籤可協助您更有效率且一致地管理雲端中的資源。如需詳細資訊，請參閱標記您的 AWS 資源。請務必制定動態資產管理策略，以適應不斷變化的雲端性質。AWS Systems Manager 庫存可協助您指派標籤，以便快速搜尋、管理和識別資源。

- 監控和偵測整合 – 建立從雲端傳送警示到內部部署安全操作中心 (SOCs) 和安全資訊和事件管理 (SIEM) 系統的方法至關重要。Amazon GuardDuty 是一種持續的安全監控服務，可分析和處理日誌，以識別您 AWS 環境中非預期和可能未經授權的活動。它也會與許多第三方工具整合。
- 雲端事件回應計劃和程式 – 與內部部署警示相比，請務必確保負責處理雲端警示的人員熟悉擷取這些警示的程序，並知道如何回應雲端警示。為了改善事件回應功能，請訓練人員使用 Amazon Detective 進行日誌分析。Amazon Detective 可協助您分析、調查和識別安全調查結果或可疑活動的根本原因。Amazon Detective 應該是事件回應計畫的一部分。
- 雲端漏洞管理 – 管理雲端漏洞的程序與內部部署環境不同。除了傳統的漏洞管理之外，您還必須評估基礎設施程式碼層。Amazon Inspector 是一種自動化漏洞管理服務，可持續評估您的資源是否有漏洞和意外的網路暴露。
- 雲端狀態管理 – 雲端狀態管理，如評估一節所述，是雲端安全的重要層面。您可以使用 AWS Security Hub CSPM 自動化安全性最佳實務檢查，並評估您所有 的整體雲端狀態 AWS 帳戶。
- 雲端安全培訓 – 為員工提供適當的培訓至關重要，以便他們精通雲端安全。這包括提供資源的存取權，並分配時間讓員工取得必要的知識和技能。 AWS 提供許多訓練資源來提升技能和教育，例如AWS 技能建置器。

成熟：調校和測量程序、工具和風險

在雲端安全模型的成熟階段，重點在於讓安全團隊與 AWS 雲端採用架構 (AWS CAF) 安全功能保持一致，並制定敏捷的流程。這種一致性有助於專業團隊在短衝刺中加速創新，同時整合藍圖和長期規劃。成熟階段強調與 IT 操作的協同合作，並擴展深入且專門的雲端技能。每個安全功能都會實作關鍵工具和程序來提高效率和影響，並隨附指標和報告機制的開發，以測量增量變更和整體影響。

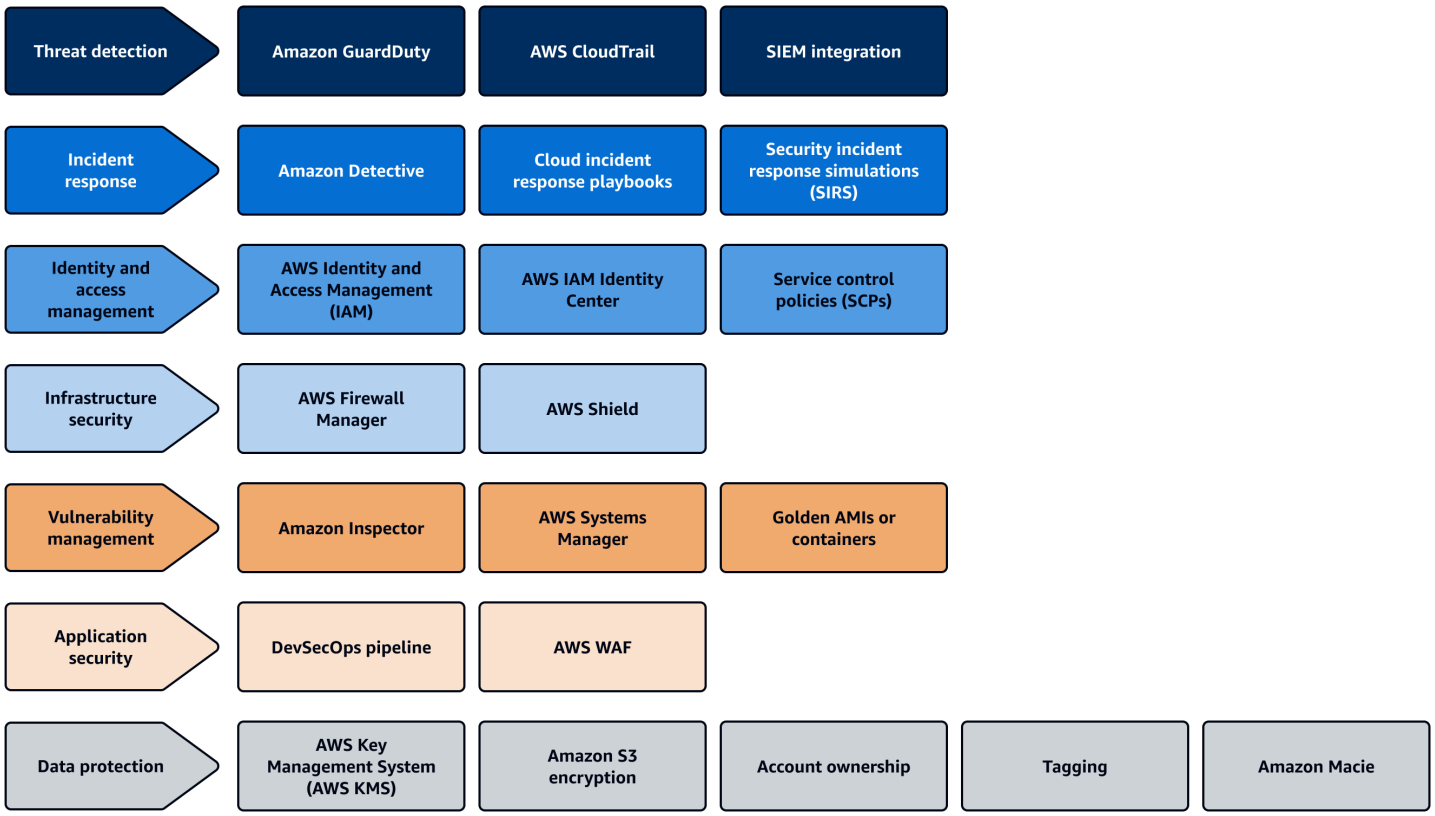
在此階段中，您會：

- 調校和測量程序
- 調校和測量工具
- 調校和測量風險
- 檢閱成熟階段中的使用案例範例

調校和測量程序

敏捷的方法提供更多彈性和創新，可協助您快速測試和實作新想法。將您的安全團隊劃分為特殊角色，例如事件回應者和漏洞管理員。角色應與下圖中的類別相符，對應至 AWS 雲端採用架構 (AWS CAF) 中的功能。敏捷的方法鼓勵團隊進行大型思考、創新、簡化和識別潛在的安全漏洞。這會導致建立使用者案例或藍圖的待處理項目，以供日後改善。

敏捷的程序允許更動態和調整性的解決方案，而不是僅依賴特定工具的功能。快速失敗是一種使用頻繁和增量測試來縮短開發生命週期的理念，它是敏捷方法的關鍵部分。進行變更、測試，然後決定是否要繼續目前的方法或切換到替代方法。如果團隊在此週期中運作，則有助於您的組織隨時掌握雲端的快節奏本質。重點訓練也很重要，您應該提供特定雲端安全領域的特定訓練。



> **Note**
>
> 此映像不包含 AWS CAF 中的安全保證和安全控管功能。本指南著重於安全操作，且安全保證和控管超出本指南的範圍。如需安全保證的詳細資訊，請參閱 YouTube 上的 AWS re：Inforce 2023 - Scaling 合規 AWS Control Tower。

在您的組織中，使用敏捷的方法，協助您的組織跟上雲端的快速開發和變更。以下是在雲端環境中開始實驗和反覆運算的一些方法：

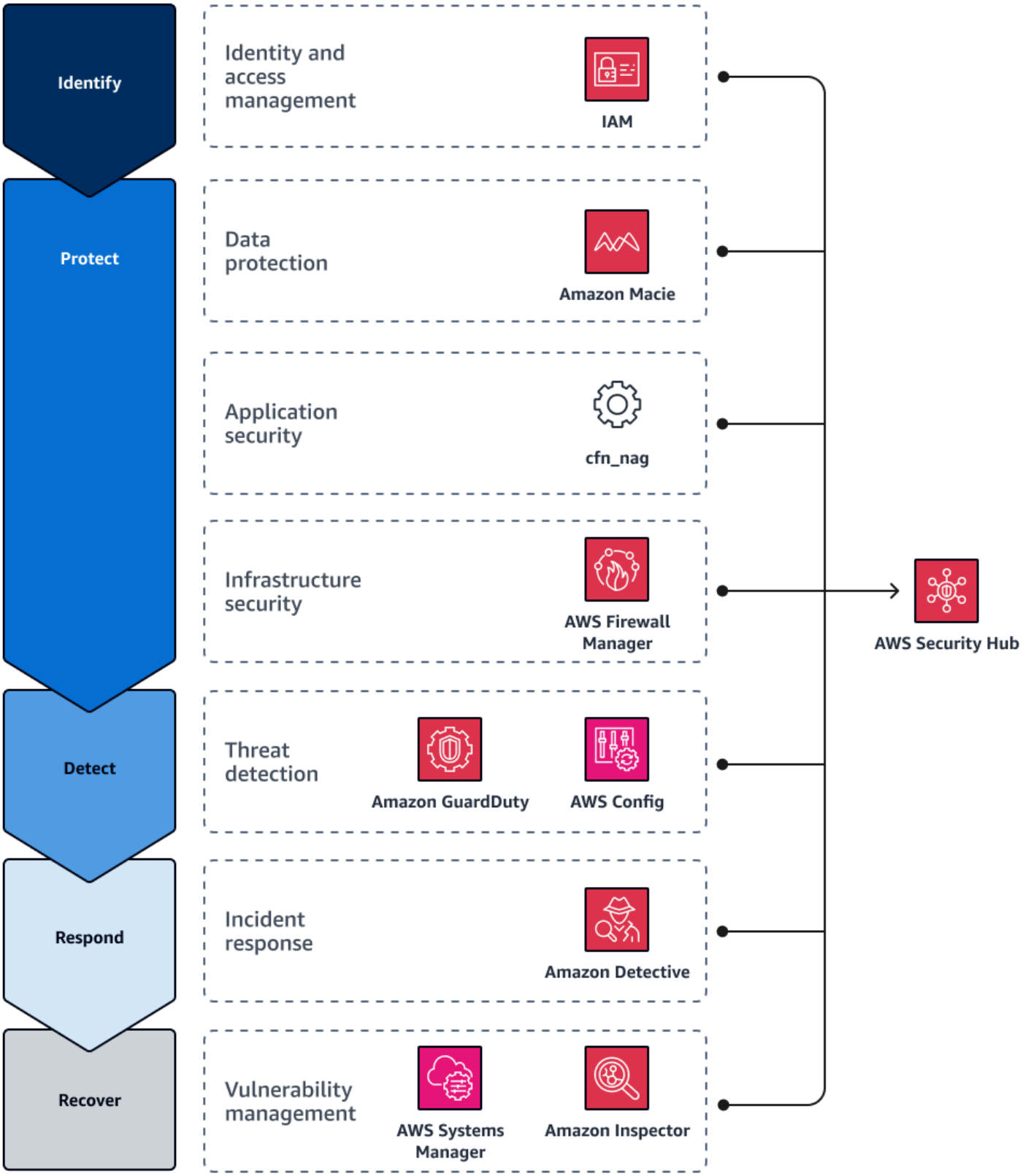
- 專注於 AWS CAF 中定義的類別，如上圖所示。
- 若要更動態，請專注於創新而非操作。
- 在衝刺中快速移動，允許人員測試、快速失敗和快速實作，並繼續此週期，以跟上業務。
- 為了支援持續操作，請盡可能調整雲端和內部部署環境的程序。

- 為了協助個人深入研究並專注於一個領域，請提供重點培訓，而不是廣泛的培訓。
- 鼓勵人們深思熟慮、調查「假設」並建立積壓項目 （例如藍圖或差距）。

調校和測量工具

為不同的安全網域建立專業團隊後，請將團隊彼此對齊。 AWS Security Hub CSPM可協助您達成此目標。Security Hub CSPM 提供集中、統一的儀表板，以監控架構的進度。它也與許多第三方工具 AWS 的安全服務整合。

NIST 網站上的國家標準技術研究所 (NIST) 網路安全架構由五個函數組成：識別、保護、偵測、回應和復原。下圖顯示如何在每個函數 AWS 服務 期間使用不同的 ，然後設定這些服務將其調查結果傳送到 Security Hub CSPM 以進行合併報告。如果您選擇使用其他工具，您可以使用 Security Hub CSPM API、 AWS Command Line Interface (AWS CLI) 和 AWS Security Finding Format (ASFF) 來建立自訂整合。如需 Security Hub CSPM 與其他 服務整合的詳細資訊，請參閱 Security Hub CSPM 文件中的中的產品整合 AWS Security Hub CSPM。



Security Hub CSPM 與所有這些服務和工具整合，並提供下列項目：

- 提供統一的儀表板，顯示更新並協助團隊迭代到位
- 自動與 AWS 安全服務整合，例如 Amazon Macie、Amazon GuardDuty 和 Amazon Detective
- 支援與第三方工具整合，例如 Prowler和 cfn_nag
- 支援與 Security Hub CSPM API AWS CLI和 AWS Security Finding Format (ASFF) 等工具的自訂整合

調校和測量風險

在行走階段的成熟階段，您可以使用 AWS Security Hub CSPM 持續調校和測量安全風險。Security Hub CSPM 會持續評估組織的安全狀態，並採取動作來修復已識別的問題。Security Hub CSPM 會集中並排定來自 AWS 帳戶、 服務和支援第三方合作夥伴的安全調查結果的優先順序。這可協助您分析安全趨勢，並識別高優先順序的安全問題。

Security Hub CSPM 會執行數百次安全檢查，並根據對您 AWS 環境的風險進行分類。您可以在 Security Hub CSPM 主控台的統一儀表板中，針對安全控制項檢視您的分數。如需詳細資訊，請參閱 Security Hub CSPM 文件中的判斷安全分數。透過此儀表板，DevSecOps 函數可以快速識別任何失敗的檢查、安全問題的嚴重性，以及哪些 AWS 區域 和資源受到影響。一旦確定，DevSecOps 團隊就可以優先處理並修復問題。隨著問題修復，Security Hub CSPM 會自動更新狀態。

檢閱成熟階段中的使用案例範例

以下是成熟階段的範例。這些範例在實際層面深入探討不同業務目標的模型、工具和程序。

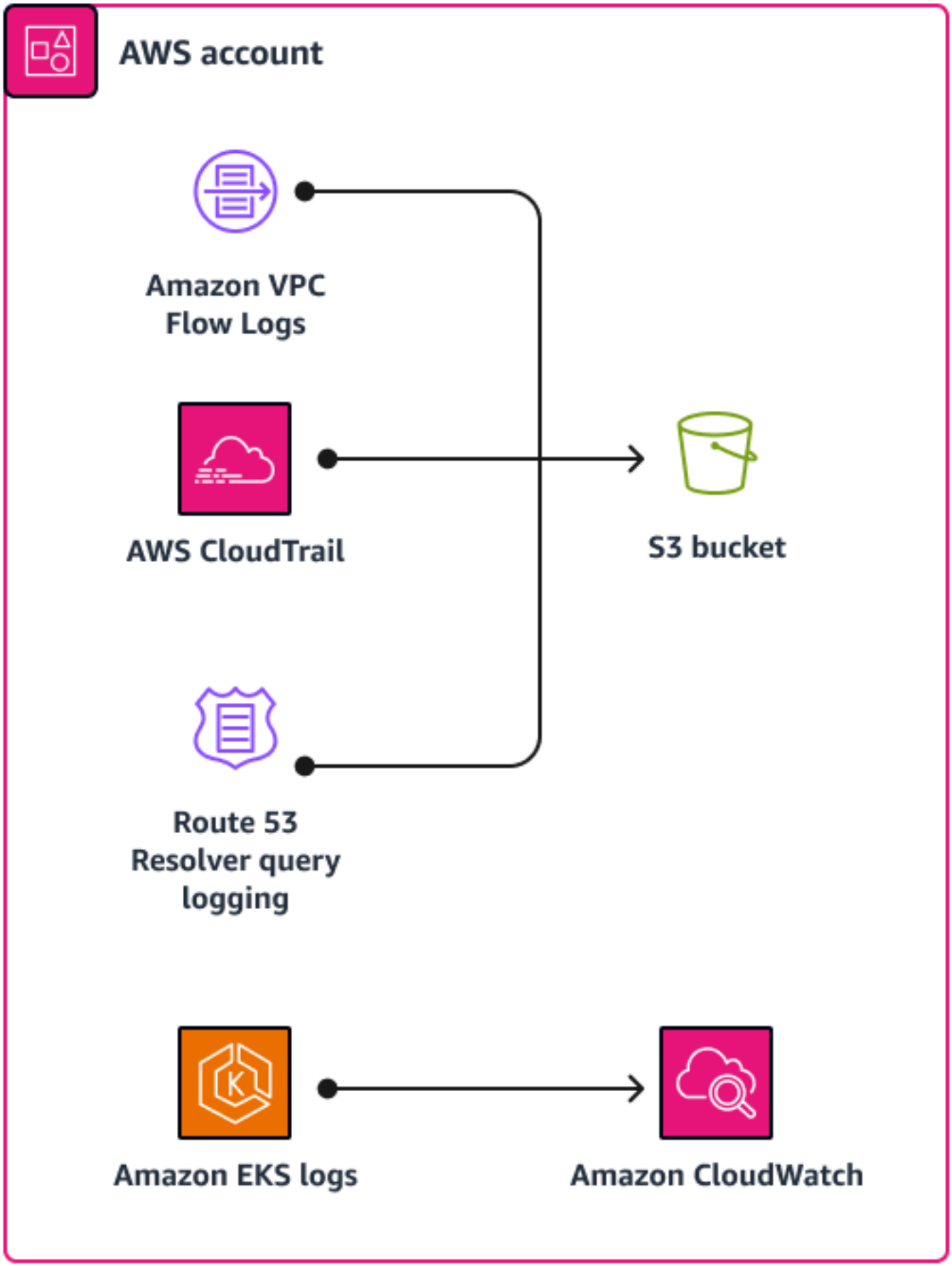
成熟：威脅偵測範例

偵測性控制的業務成果：提高雲端事件的可見性和偵測速度，以降低風險並加速雲端資源的使用和開發。

工具：Assisted Log Enabler for AWS(GitHub) 是一種開放原始碼工具，可協助您在安全事件期間開啟記錄。它可以快速提高您對事件的可見性。

範例使用案例：考慮下圖所述的單一帳戶使用案例。有些事件需要進一步調查。您不確定是否已啟用記錄。在這種情況下，最佳動作是使用 執行試轉Assisted Log Enabler，以查看啟用或停用哪些服務。會Assisted Log Enabler檢查 AWS CloudTrail 線索、DNS 查詢日誌、VPC 流程日誌和其他日誌。如果未啟用， 會Assisted Log Enabler啟用它們。 Assisted Log Enabler可以檢查並開啟所有記錄 AWS 區域。

您也可以Assisted Log Enabler調高或調低。完成試轉、關閉事件並解決問題後，您發現不再需要此層級的記錄。您可以快速清除部署以停止記錄。此功能可讓您使用 Assisted Log Enabler做為分類工具。


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

以下是 的主要功能Assisted Log Enabler for AWS：

- 您可以在單一帳戶或多帳戶環境中執行它。
- 您可以使用它來建立登入環境的基準。
- 您可以使用試轉功能來檢查目前狀態，並判斷哪些服務已啟用記錄。
- 您可以選取要啟用記錄的服務。
- 您可以針對您的使用案例Assisted Log Enabler調高或調低。

成熟：IAM 範例

IAM 業務成果：根據最佳實務自動化可見性和衡量，以持續降低風險、啟用安全的外部連線，以及快速佈建新的使用者和環境

工具：AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) 可協助您識別與外部實體共用的資源、根據政策文法和最佳實務驗證 IAM 政策，並根據歷史存取活動產生 IAM 政策。強烈建議您在帳戶和組織層級啟用 IAM Access Analyzer。

服務優勢：IAM Access Analyzer 提供豐富的洞見調查結果。它可以識別與外部實體共用的組織資源和帳戶。它可以偵測資源，例如公有 S3 儲存貯體、與其他 帳戶 AWS KMS key 共用的 ，或與外部帳戶共用的角色，讓您有絕佳的可見性來識別組織無法控制的資源。它不僅會驗證 IAM 政策，還可以為您產生這些政策。

執行階段：最佳化您的雲端安全操作

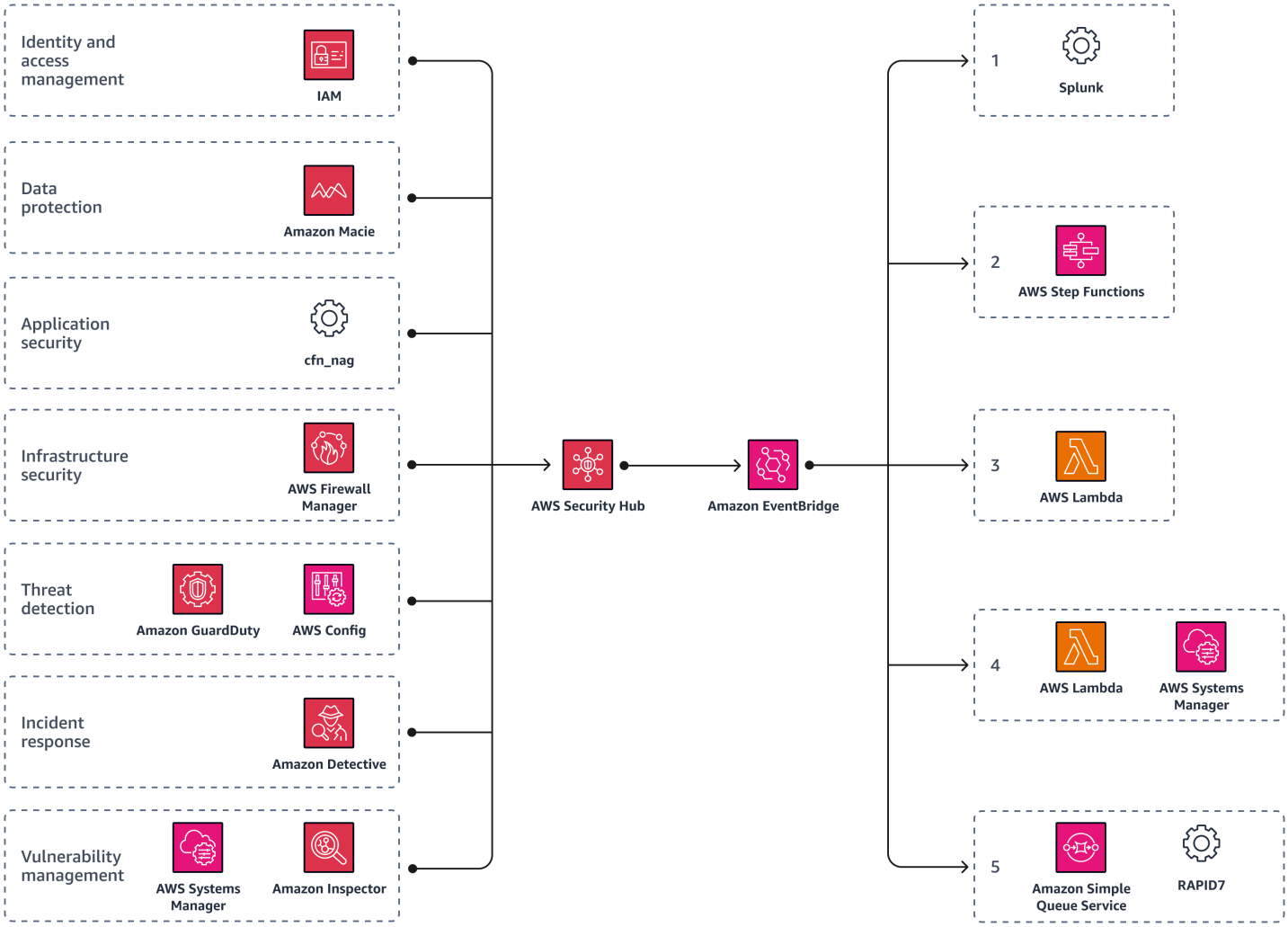
在行走階段實作基準後，您的組織會進入執行階段。此階段著重於示範雲端中可用的網路安全功能，其中許多功能是不可能的，或者很難透過內部部署解決方案實作。此階段將不同的安全元件整合在一起，並自動化程序。自動化會釋放您的資源，讓他們可以專注於高價值的工作。

以下是執行階段中的唯一階段：

- 最佳化 – 如何改善此程序並新增自動化？

最佳化：自動化和重複您的雲端安全操作

在最佳化階段，您可以自動化安全操作。如同爬蟲和行走階段，您可以在執行階段 AWS Security Hub CSPM 期間使用 來實現自動化和反覆運算。下圖顯示 Security Hub CSPM 如何觸發自訂 Amazon EventBridge 規則，以定義要針對特定調查結果和洞見採取的自動動作。如需詳細資訊，請參閱 Security Hub CSPM 文件中的自動化。



透過使用 Security Hub CSPM 做為中央自動化中樞，您也可以將活動轉送至 Splunk。 然後， Splunk 可以偵測異常的活動，並在 EventBridge 中觸發對應的動作。這可協助您自動化重複性任務，並為熟練的團隊成員提供更多時間專注於更高價值的活動。您也可以使用 AWS Step Functions來收集日誌、擷取鑑識快照、隔離遭到入侵的伺服器，並將它們取代為黃金映像。此外，您可以使用 AWS Lambda函數AWS Systems Manager來修復環境中的漏洞，並使用 Amazon Simple Queue Service (Amazon SQS) 函數來驗證系統的安全性。透過採取這種方法，可以快速遏制和修復安全事件，並將對正常業務營運的影響降至最低。

以下是重複自動化動作的範例，如上圖所示：

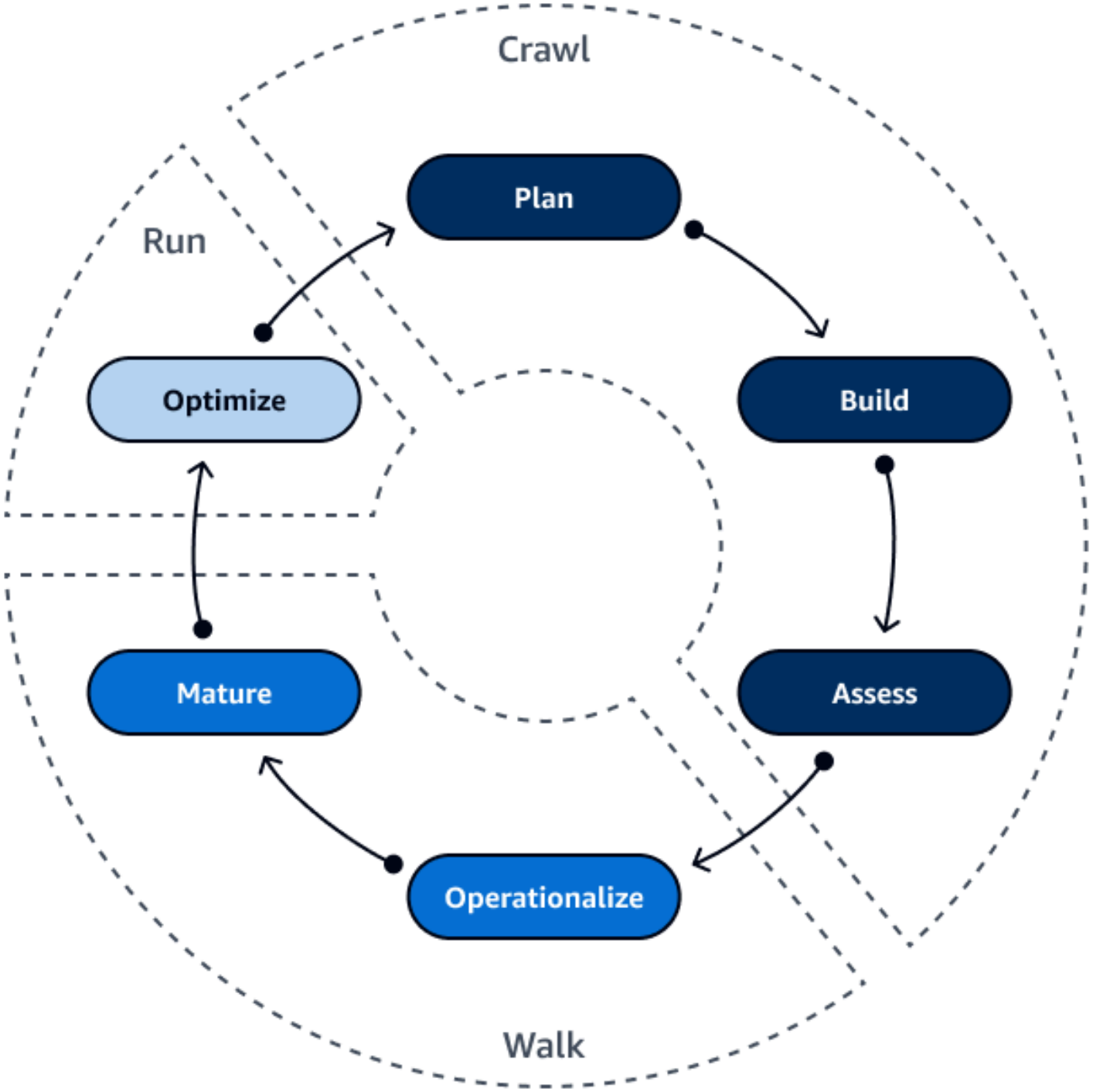
1. 使用 Splunk 偵測可疑的活動。
2. 使用 Step Functions 收集日誌、撤銷存取權、隔離和取得鑑識快照。
3. 使用 EventBridge 規則啟動 Lambda 函數，以隔離、取得鑑識快照，並以黃金映像取代遭到入侵的伺服器。

4. 啟動 Lambda 函數，該函數使用 Systems Manager 來修復並在整個環境中套用修補程式。
5. 啟動使用 Rapid7 掃描器掃描並驗證 AWS 資源是否安全的 Amazon SQS 訊息。

如需詳細資訊，請參閱 AWS 安全部落格中的 EC2 AWS 雲端 執行個體的 中的如何自動化事件回應。

結論：爬蟲、行走、跑步，然後飛行！

總而言之，爬蟲、行走、執行模型是一種架構，可協助您逐步改善安全狀態，並採用最佳實務來保護 AWS 基礎設施。隨著新技術和業務需求的出現，此程序會持續發展。透過遵循此架構並使用 提供的資源 AWS，您可以為雲端安全建立堅實的基礎、有效管理安全風險、加速安全成熟度並推動創新。



在爬蟲階段，您可以設定基礎。您可以定義您的安全計畫是什麼、使用定義的安全最佳實務架構，並推動持續評估以達成組織的業務目標。

在行走階段中，您會採取第一步。您可以查看政策、建置手冊、訓練人員並調整策略。此階段可協助您了解如何利用創新來跟上雲端的技術。

在執行階段，您會認為很大。您可以使用自動化，並以策略方式將熟練的人員放在正確的位置。您可以實作自動化，以推動持續評估組織業務目標。

現在是您的飛行時間。使用本指南中的建議來加速 中的安全成熟度 AWS 雲端。

資源

架構和模型

- AWS 雲端採用架構 (AWS CAF)
- AWS Well-Architected 架構
- AWS 安全參考架構 (AWS SRA)
- AWS 安全成熟度模型
- HIPAA 參考架構
- HITRUST 參考架構

AWS 服務

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

其他 AWS 資源

- AWS 解決方案程式庫中的 上的自動化安全回應 AWS
- AWS 運算部落格中的使用 AWS Step Functions 和 Amazon CloudWatch Events 自動化您的 IT 操作
- 如何在 安全部落格的 AWS 雲端 EC2 執行個體的 中自動化事件回應 AWS
- AWS 安全部落格中的如何在多帳戶環境中執行自動事件回應
- AWS re：Inforce 2022 - 爬取、行走、執行：加速 上的安全成熟度影片 YouTube
- AWS re：Inforce 2022 - 爬取、行走、執行：加速安全成熟度 PowerPoint 簡報 （附件）

貢獻者

下列個人對本指南有所貢獻。

編寫

- Chad Lorenc，安全實務經理 AWS
- Ivy Gin，安全保證顧問， AWS
- Sayali Paseband，安全顧問 AWS

檢閱

- Deeps Baisya，資深安全架構師 AWS
- Mike LaRue，資深安全顧問 AWS
- Raul Radu，資深安全工程師 AWS

技術寫入

- 資深技術作者，Lilly AbouHarb AWS

文件歷史紀錄

下表描述了本指南的重大變更。如果您想收到有關未來更新的通知，可以訂閱 RSS 摘要。

變更	描述	日期
初次出版	—	2023 年 12 月 20 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。