



雲端資安最佳實踐設計

Bard Lan, AWS 解決方案架構師

bardlan@amazon.com

Jun, 2022



雲的安全與合規基於對「共同責任模型」的認識

Compliance starts with the AWS "Shared Responsibility Model"

企業可依需求調整
雲端 **平台服務** 的安全性

Responsibility for security "in" the cloud

Customer
AWS

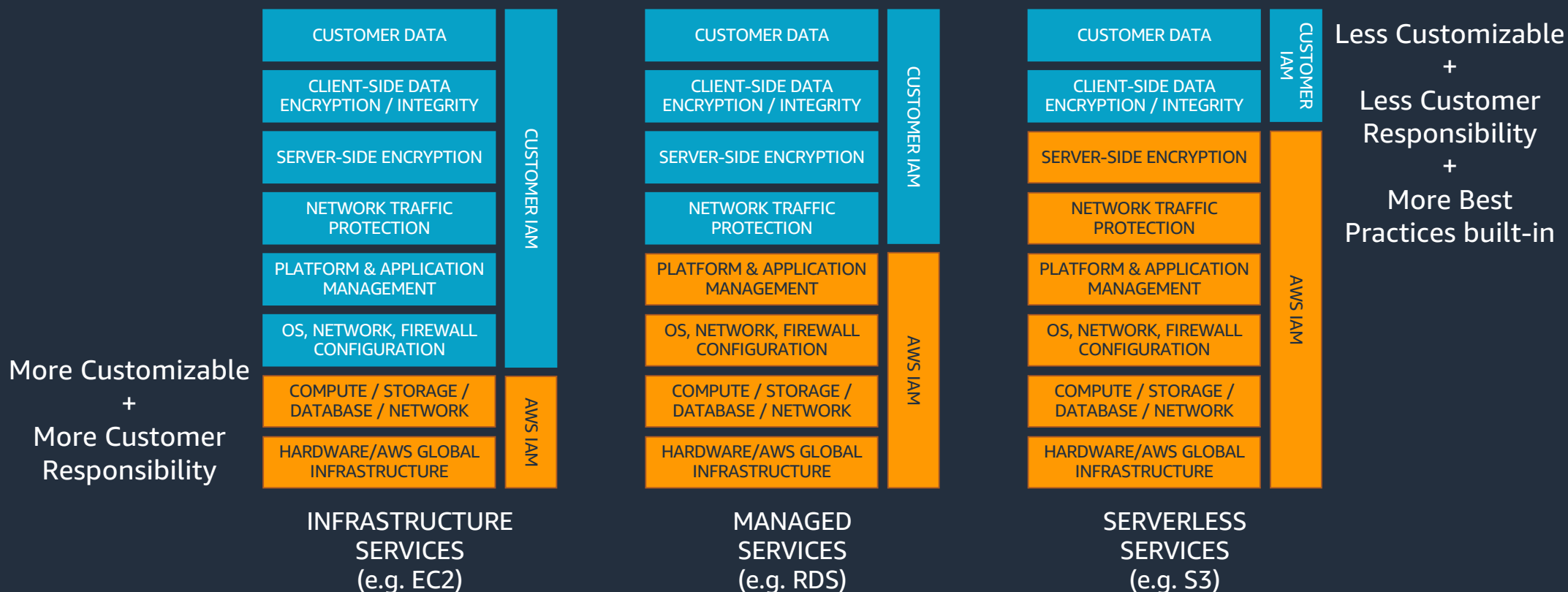
AWS 協助企業確保
雲端 **基礎設施** 的安全性

Responsibility for security "of" the cloud



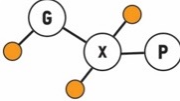
雲上不同的服務類型具有不同的共同責任模型

Different shared responsibility model for different service types



AWS 定期受第三方公正組織稽核，並更新雲安全性與合規認證

Inherit global security & compliance controls

					
 SOC 1	 SOC 2	 SOC 3	 CJIS		
 DoD SRG	 FedRAMP	 FERPA	 Federal Financial Institutions Examination Council		 SEC Rule 17a-4(f)
 GxP	 HIPAA	 International Traffic in Arms Regulations	 MPAA	 iDA SINGAPORE	 マイナンバー My Number Act
 VPAT Section 508			 Information Security Management System	 G-Cloud	
 GDPR	 CYBER ESSENTIALS PLUS	 CERTIFICACIÓN DE CONFORMIDAD CON EL ens Seguridad Empresa ALTA RD 1/2016			

提醒：使用 AWS 服務不表示您的應用就地合規

Applications built on top of AWS services are not implicitly compliant, customers need to get certified separately

Customer Applications

Your own
accreditation

Your own
certifications

Your own
external audits

Applications built on top of AWS services, **are not implicitly compliant** to security controls (that AWS services are compliant with).

Customers need to **certify applications separately** by engaging with external auditors.



AWS Well-Architected

Learn, measure, and build using architectural best practices

[AWS Architecture Center](#)[This is My Architecture](#)[AWS Answers](#)[AWS Solutions](#)[Case Studies](#)[Cloud Security](#)

Security **IN** the
Cloud
Managed by
customers

AWS Cloud Compliance

Assurance programs for finance, healthcare, government and more.

I'd like information about Compliance in the
Cloud →

[Compliance](#)[Cloud Security](#)[Assurance Programs](#)[Resources](#)[Latest News](#)[Testimonials](#)

AWS Artifact

No cost, self-service portal for on-demand access to AWS' compliance reports.

Start for Free with AWS Artifact

[Artifact](#)[Getting Started](#)[FAQ](#)[Documentation](#)[Compliance](#)[Security](#)

Security **OF** the
Cloud
Managed by
AWS



Well-Architected Tool

<https://aws.amazon.com/well-architected-tool/>

AWS Well-Architected Tool

Learn, measure, and build using architectural best practices

The AWS Well-Architected Tool helps you review your workloads against current AWS best practices and provides guidance on how to improve your cloud architectures. This tool is based on the AWS Well-Architected Framework.

Define a workload

Define a workload based on one of your existing cloud applications.

[Define workload](#)

Pricing (US)

Any usage

Free

Getting started

[What is the AWS Well-Architected Tool?](#)

[Getting started video](#)

More resources

[FAQ](#)

[AWS Well-Architected Partners](#)

How it works



Benefits and features

Get architectural guidance

Access the knowledge and best

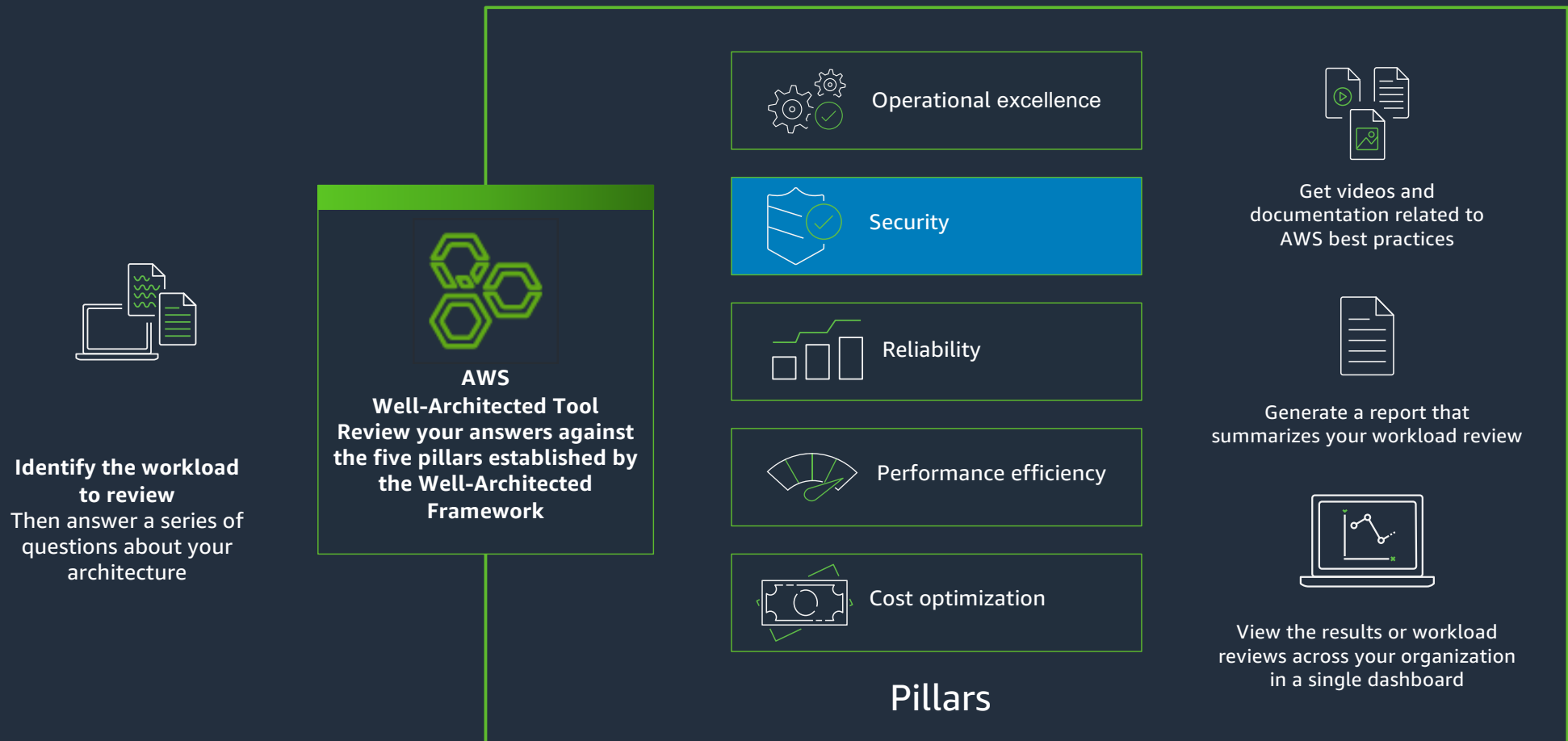
Enable consistent governance

Apply a consistent process to help you

Continuously improve architectures

Support continuous improvement

AWS Well-Architected Framework



AWS 雲端環境安全設計原則

Design principles for security

建立強大的身份識別基礎

Implement a strong identity foundation

在所有網路層套用安全性

Apply security at all layers

啟用可追溯性

Enable traceability

自動化安全最佳實務

Automate security best practices

保護傳輸中資料和靜態資料

Protect data in transit and at rest

讓人員遠離資料

Keep people away from data

為安全事件做準備

Prepare for security events



AWS 雲端環境安全設計原則

Design principles for security

建立強大的身份識別基礎

Implement a strong identity foundation

在所有網路層套用安全性

Apply security at all layers

啟用可追溯性

Enable traceability

自動化安全最佳實務

Automate security best practices

保護傳輸中資料和靜態資料

Protect data in transit and at rest

讓人員遠離資料

Keep people away from data

為安全事件做準備

Prepare for security events



最佳實踐：啟用多重驗證 (Multi-factor Authentication)



11

AWS Management Console

Login with **Username/Password** with optional **MFA** (recommended)

Account:

User Name:

Password:

☒ I have an MFA Token (more info)

MFA Code:

[Sign In](#)



API access

Access API using **Access Key + Secret Key**, with optional MFA

ACCESS KEY ID

Ex: AKIAIOSFODNN7EXAMPLE

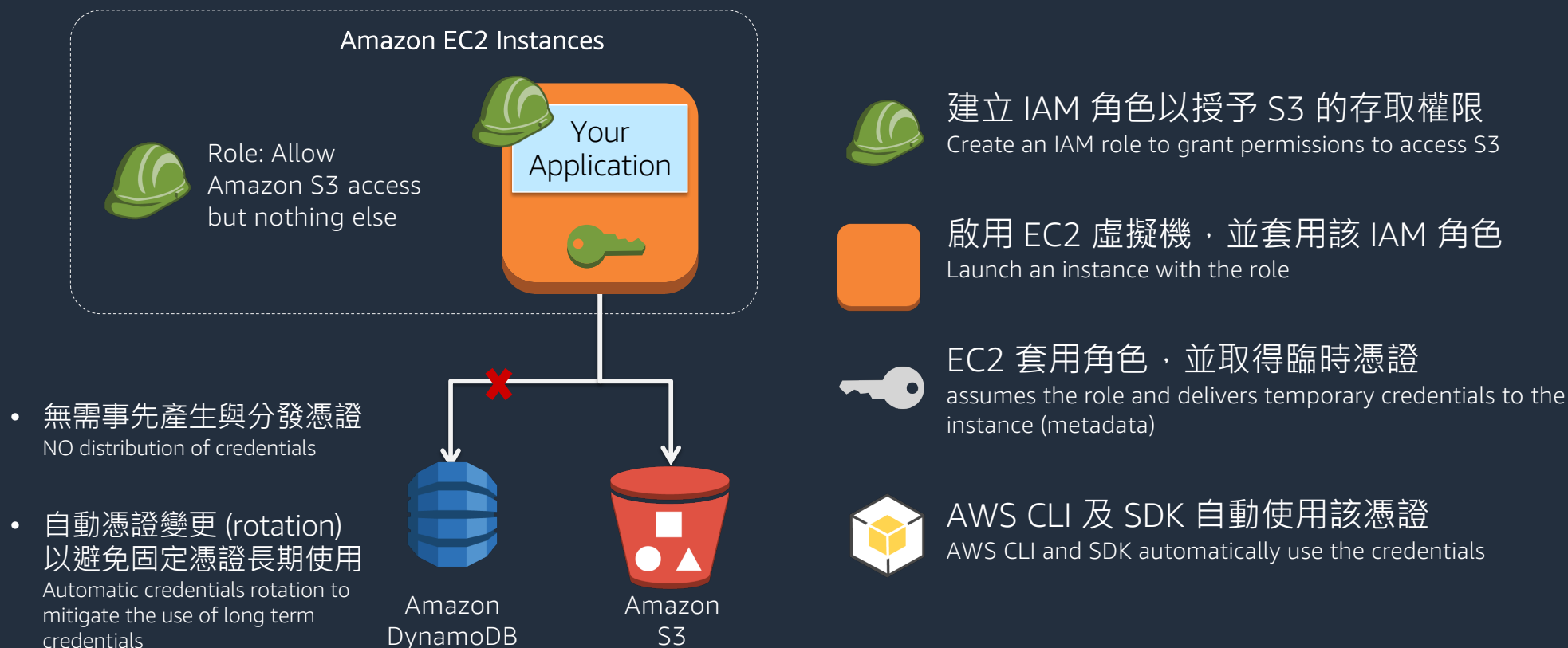
SECRET KEY

Ex: UtnFEMI/K7MDENG/bPxrFiCYEX



最佳實踐：避免將憑證直接存放於硬碟或程式碼中

Assign Role to EC2 Instances instead of kept Access Key and Secret Access Key in disk



最佳實踐：適當地授與所需的最低權限

Least Privilege Access to Data

安全最佳實踐 Security best practice

- 從最小的權限範圍開始
Start with a minimum set of permissions
- 再根據需要賦予其他所需權限
Grant additional permissions as necessary

僅定義所需的權限範圍 Define only the required set of permissions

- 個別服務的可操作動作
What actions a particular service supports
- 特定任務的操作範圍
What collection of API actions are required for the specific task
- 執行任務操作所需的具體權限
What permissions are required to perform those actions

定期檢視未被利用的使用者、角色或權限

Review unused users/roles/policies periodically



AWS 雲端環境安全設計原則

Design principles for security

建立強大的身份識別基礎

Implement a strong identity foundation

在所有網路層套用安全性

Apply security at all layers

啟用可追溯性

Enable traceability

自動化安全最佳實務

Automate security best practices

保護傳輸中資料和靜態資料

Protect data in transit and at rest

讓人員遠離資料

Keep people away from data

為安全事件做準備

Prepare for security events



Amazon Virtual Private Cloud (VPC) 安全元件

Security Components



Virtual Private Cloud

設置 AWS 的邏輯隔離環境，使企業能在獨立的虛擬網路環境中使用各種 AWS 服務與資源

Provision a logically isolated cloud where you can launch AWS resources into a virtual network



Security Groups & ACLs



NAT Gateway



Flow Logs

VPC Endpoints

Private and secure connectivity to Amazon S3 and Amazon DynamoDB



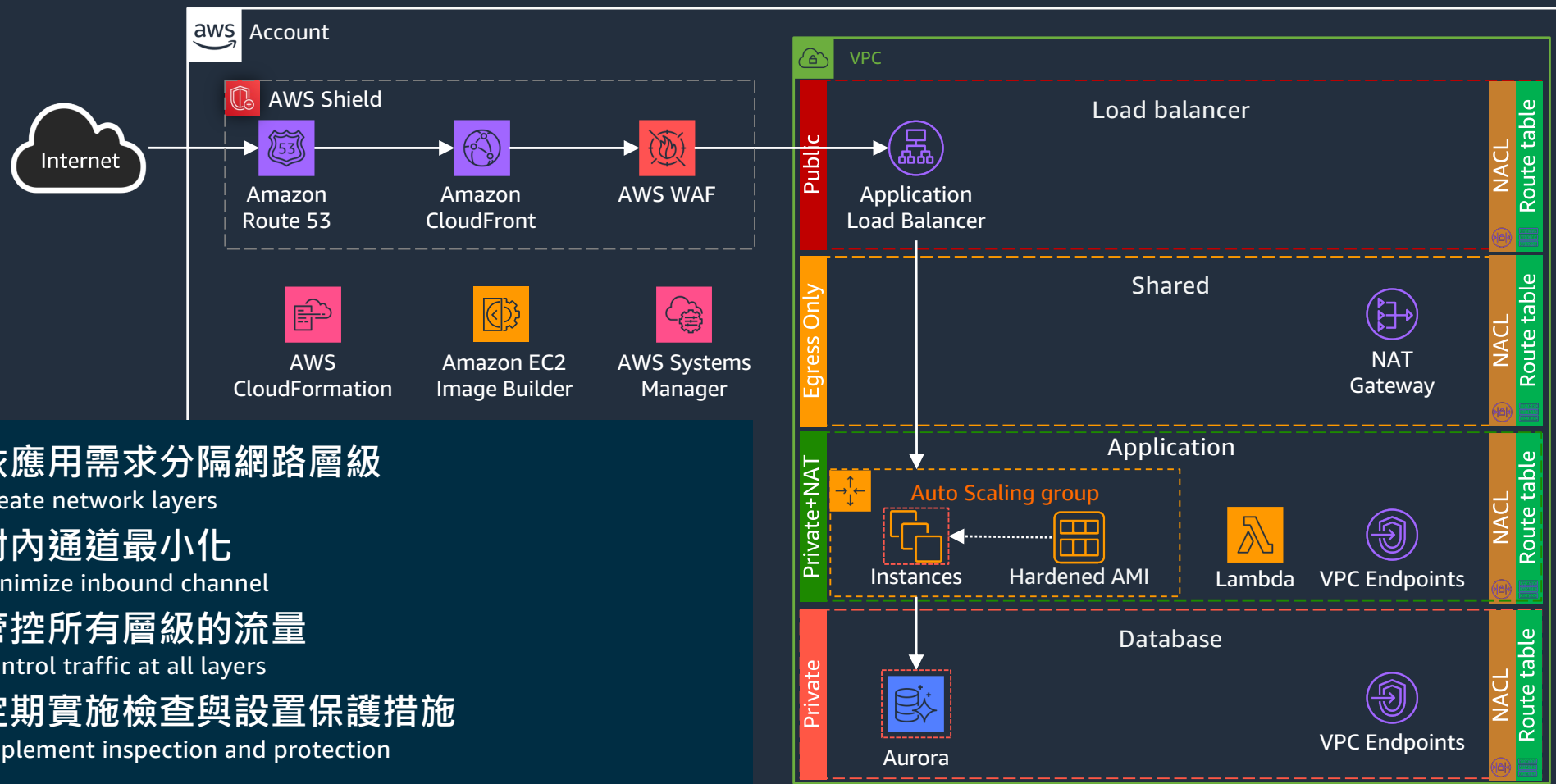
Amazon S3



Amazon DynamoDB

最佳實踐：建構良善架構以最小化網路攻擊面

Well-architected



- 依應用需求分隔網路層級
Create network layers
- 對內通道最小化
Minimize inbound channel
- 管控所有層級的流量
Control traffic at all layers
- 定期實施檢查與設置保護措施
Implement inspection and protection

AWS 雲端環境安全設計原則

Design principles for security

建立強大的身份識別基礎

Implement a strong identity foundation

在所有網路層套用安全性

Apply security at all layers

啟用可追溯性

Enable traceability

自動化安全最佳實務

Automate security best practices

保護傳輸中資料和靜態資料

Protect data in transit and at rest

讓人員遠離資料

Keep people away from data

為安全事件做準備

Prepare for security events



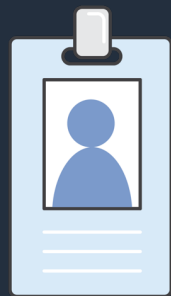
AWS CloudTrail – 記錄帳號的 AWS API 存取日誌

Web service that records AWS API calls for your account and delivers logs



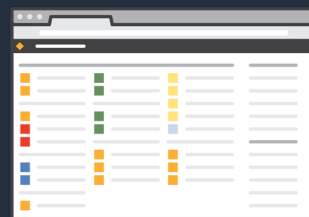
18

人 (Who) 時 (When) 地 (Where)

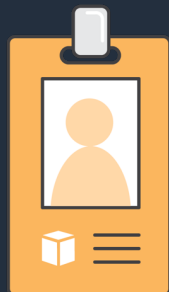


John

2021/01/01 00:01:00

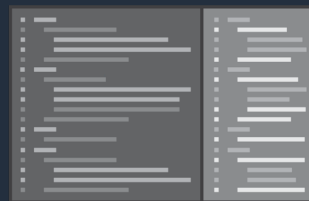


Web console
54.2.1.100



Peter

2021/01/01 00:01:00



CLI
54.2.1.102

事 (What)

RunInstances

StopInstances

UpdateInstanceInformation

TerminateInstances

CreateBucket

UpdateSecurityGroup

物 (Which)



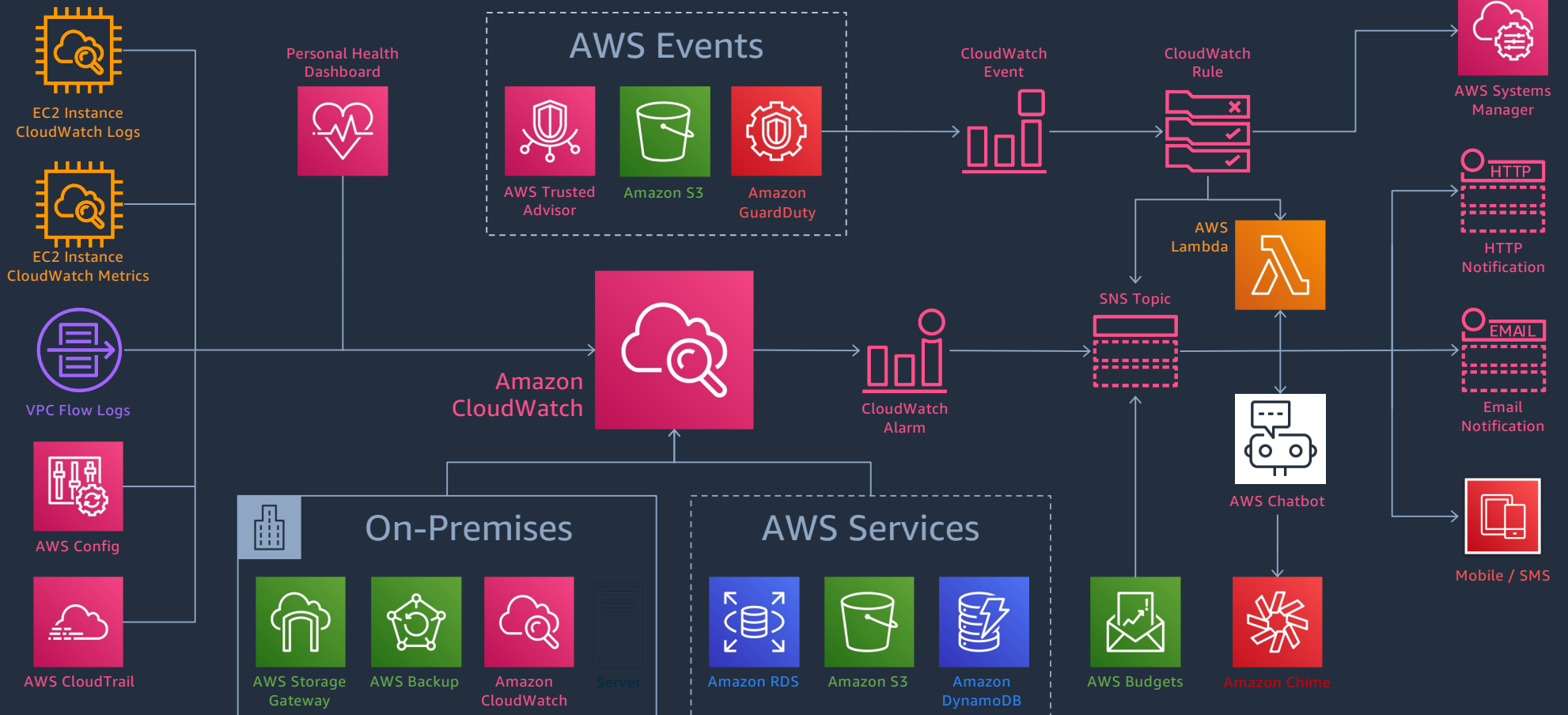
Record and evaluate configurations of your AWS resources



Amazon CloudWatch 自動化事件驅動整合架構

Integration architecture of Amazon CloudWatch

20



AWS 雲端環境安全設計原則

Design principles for security

建立強大的身份識別基礎

Implement a strong identity foundation

在所有網路層套用安全性

Apply security at all layers

啟用可追溯性

Enable traceability

自動化安全最佳實務

Automate security best practices

保護傳輸中資料和靜態資料

Protect data in transit and at rest

讓人員遠離資料

Keep people away from data

為安全事件做準備

Prepare for security events



AWS Security Hub - 安全與合規中心

AWS Security Hub - Security and compliance center

Account 1
Account 2
Account 3



可啟用到企業
所有的 AWS 帳號
*Enable AWS Security Hub for
all your accounts*



持續彙總安全服務的
資安事件並確定
其優先等級
*Continuously aggregate and
prioritize findings*



制定自動化合規掃描
與檢查
*Conduct automated
compliance scans and checks*



根據安全事件發現
採取行動
*Take action based on
findings*

Better visibility into **security issues**.

Easier to stay in **compliance**.

最佳實踐：啟用自動安全與合規檢查

Automated security checks



23

aws 服務 ▾

Q 搜尋服務、功能、市集產品和文件 [Option+S]

🔗 🔔 bardlan @ bardlan ▾ 維吉尼亞州北部 ▾ 支援 ▾

Security Hub ×

摘要

安全標準

洞見

問題清單

整合

設定

最新消息 6

安全標準

AWS 基礎安全最佳實務 v1.0.0 採用 AWS 技術

描述

AWS 基礎安全最佳實務標準是一組自動化安全檢查，可偵測 AWS 帳戶和部署的資源何時不符合安全最佳實務。該標準由 AWS 安全專家定義。這組精心設計的控制項有助於改善您在 AWS 的安全狀態，並涵蓋 AWS 最熱門和基礎的服務。

安全分數

69%

停用 檢視結果

CIS AWS Foundations 基準 v1.2.0 採用 AWS 技術

描述

Center for Internet Security (CIS) AWS Foundations 基準 v1.2.0 是一組 AWS 的安全組態最佳實務。此 Security Hub 標準會根據 CIS 要求的細項，自動檢查您的合規整備程度。

安全分數

21%

停用 檢視結果

PCI DSS v3.2.1 採用 AWS 技術

描述

支付卡產業資料安全標準 (PCI DSS) v3.2.1 是存放、處理和/或傳輸持卡人資料的實體資訊安全標準。此 Security Hub 標準會根據 PCI DSS 要求的細項，自動檢查您的合規整備程度。

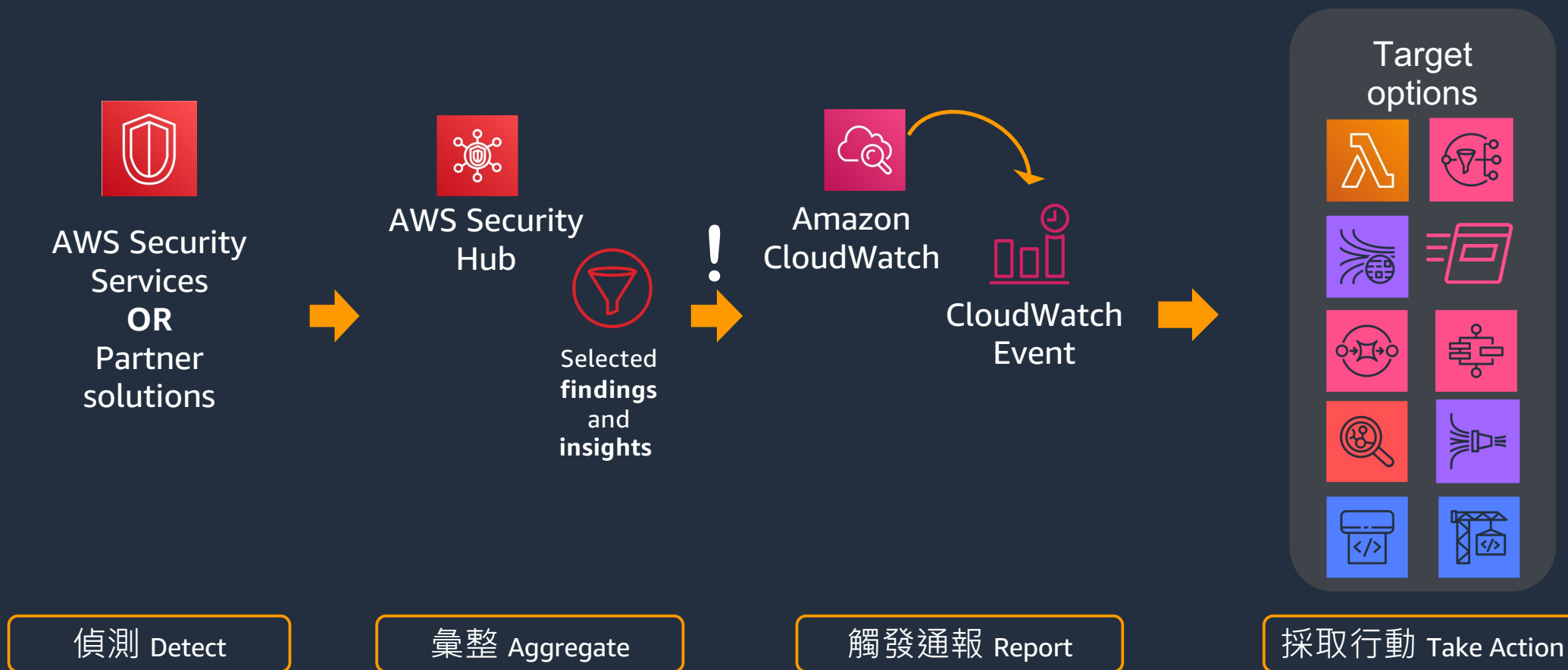
安全分數

55%

停用 檢視結果

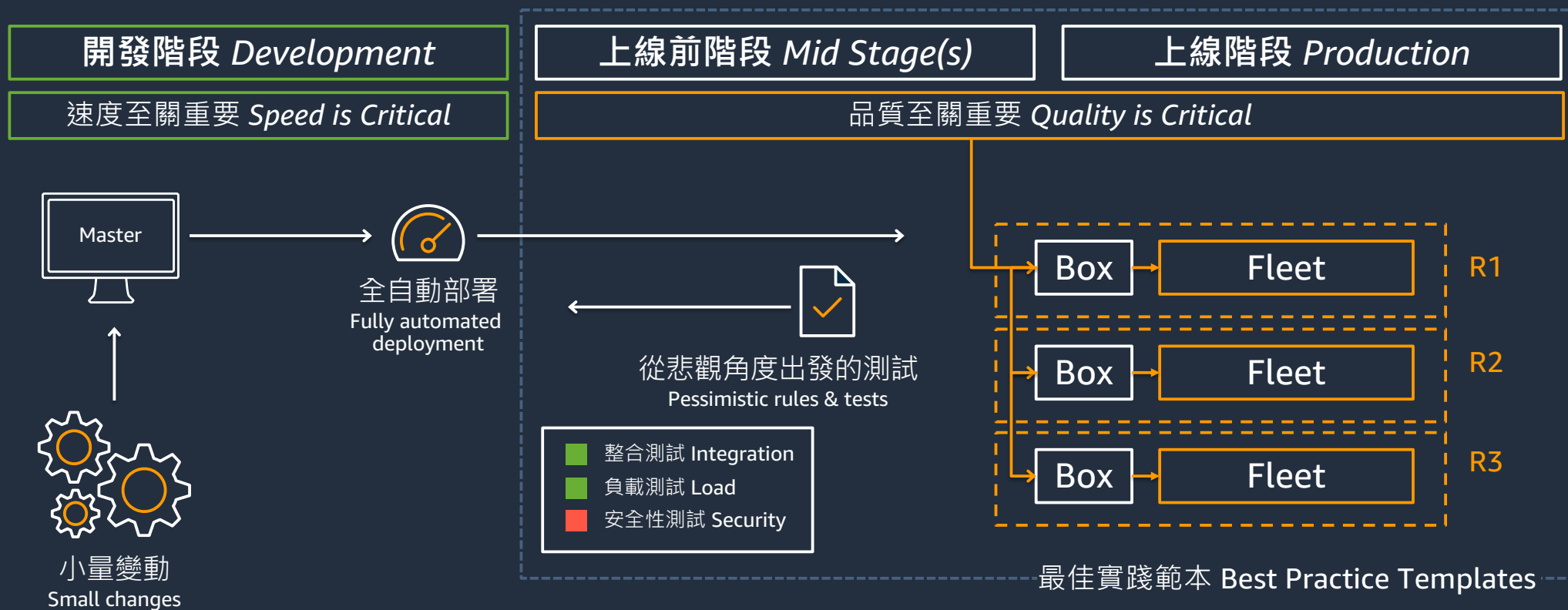
針對不安全或不符合規的設定自動通報及採取行動

Take Action for Non-compliant configurations



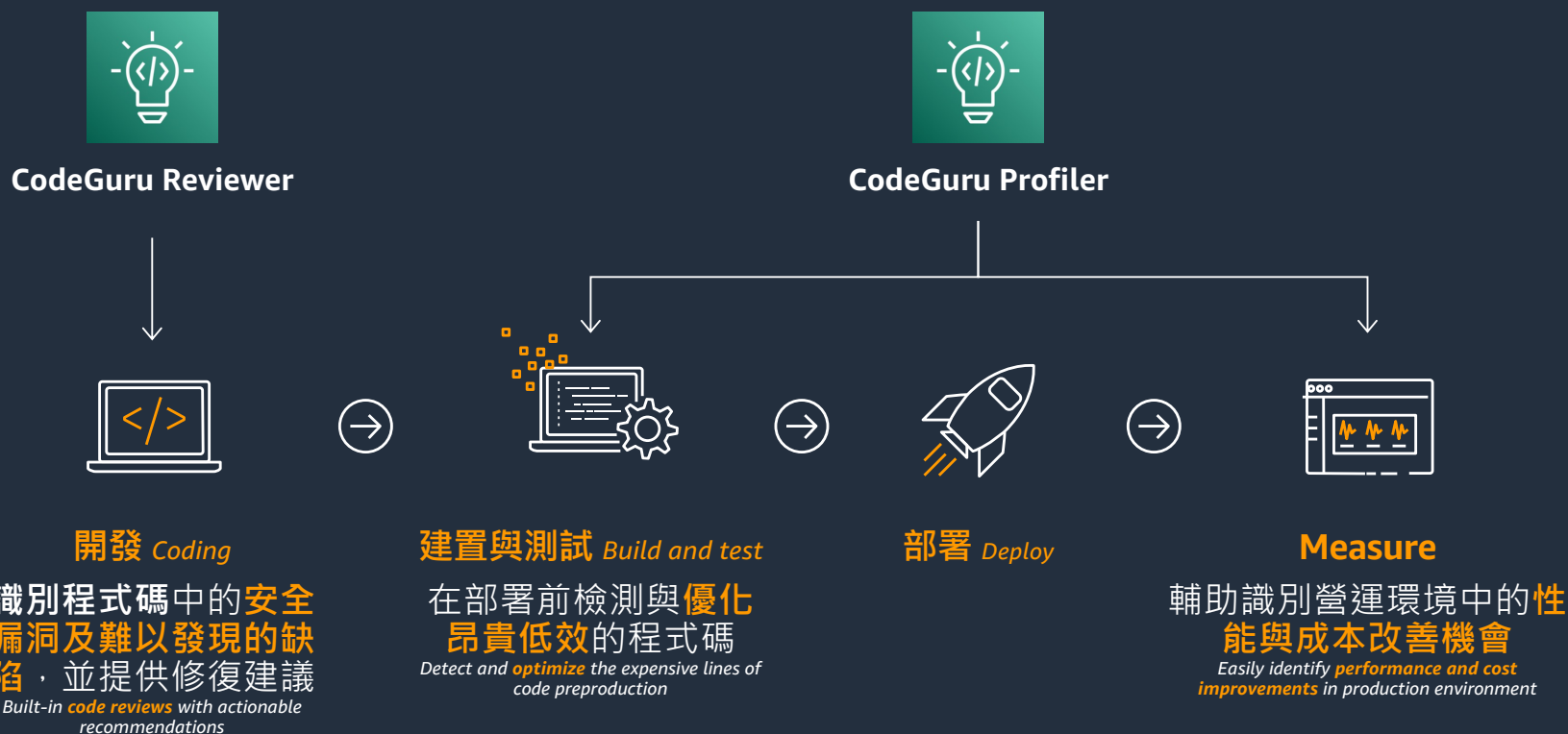
程式碼自動化持續整合、持續交付與部署

CI/CD



可藉助機器學習技術，自動執行程式碼檢測和效能優化

Automate code reviews and optimize application performance with ML-powered recommendations



AWS 雲端環境安全設計原則

Design principles for security

建立強大的身份識別基礎

Implement a strong identity foundation

在所有網路層套用安全性

Apply security at all layers

啟用可追溯性

Enable traceability

自動化安全最佳實務

Automate security best practices

保護傳輸中資料和靜態資料

Protect data in transit and at rest

讓人員遠離資料

Keep people away from data

為安全事件做準備

Prepare for security events



最佳實踐：啟用伺服器端預設加密

Enable default encryption

AWS Key Management Service (KMS)

安全地創建、控制、輪換與使用加密金鑰的託管服務

Managed service to securely create, control, rotate, and use encryption keys

EBS

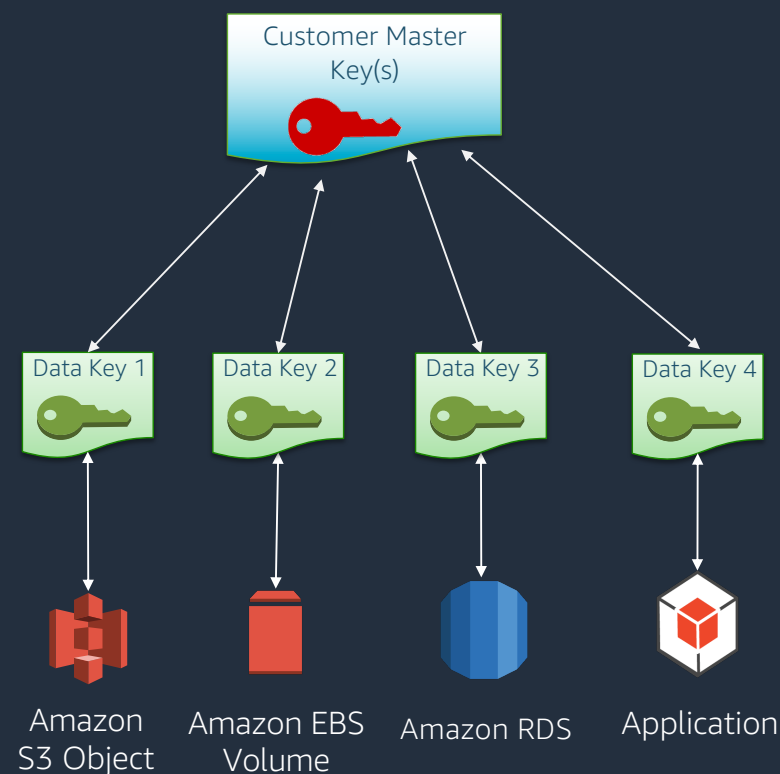
S3

RDS

AWS SDK

AWS CloudTrail

- 集中式密鑰管理 (創建、刪除、檢視、策略權限設置)
Centralized key management (create, delete, view, set policies)
- 匯入您自己的密鑰 (Import your own keys)
- 強制且自動的密鑰輪換 (Enforced, automatic key rotation)



AWS 雲端環境安全設計原則

Design principles for security

建立強大的身份識別基礎

Implement a strong identity foundation

在所有網路層套用安全性

Apply security at all layers

啟用可追溯性

Enable traceability

自動化安全最佳實務

Automate security best practices

保護傳輸中資料和靜態資料

Protect data in transit and at rest

讓人員遠離資料

Keep people away from data

為安全事件做準備

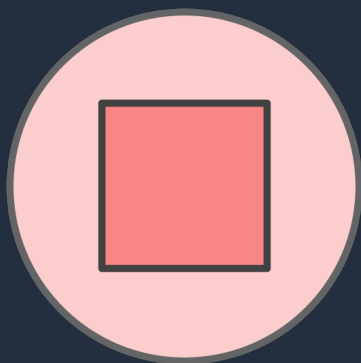
Prepare for security events



最佳實踐：讓人員遠離對資料的直接操作

keep people away from data

- 不儲存在非安全之處
 - Don't store
- 避免授與過大的權限
 - Don't grant



- 資料分類
 - Data categorization
- 重要資料加密儲存
 - Data encryption
- 機敏資料遮罩
 - Data masking
- 依需要去識別化
 - Tokenize data



- 規劃資料隔離策略
 - Isolate
- 應用工具來操作資料
 - Tooling
- 消除人員的直接操作
 - Eliminate human access



- 作業即程式碼
 - Infrastructure as code
 - Policy as code
- 版本控制
 - Version control



AWS 雲端環境安全設計原則

Design principles for security

建立強大的身份識別基礎

Implement a strong identity foundation

在所有網路層套用安全性

Apply security at all layers

啟用可追溯性

Enable traceability

自動化安全最佳實務

Automate security best practices

保護傳輸中資料和靜態資料

Protect data in transit and at rest

讓人員遠離資料

Keep people away from data

為安全事件做準備

Prepare for security events



持續追蹤最新安全威脅與補救建議

Keep up to date with security threats & recommendations



CVEs
Social media
Forums



Subscribe



Blogs



AWS Marketplace

<https://aws.amazon.com/blogs/>
<https://aws.amazon.com/security/>
<https://cve.mitre.org/>

定期舉辦災防演練

Run a gameday

33



各式雲端安全服務，協助客戶控管「雲中」的安全與合規

Aligning to the NIST Cybersecurity Framework (CSF) in the AWS Cloud (NIST 800-53)



廣泛安全合作夥伴與解決方案生態系上架在 AWS Marketplace

Largest ecosystem of security partners & solutions



AWS 雲端安全學習資源

AWS Cloud Security Resources

AWS 雲端安全 概觀 安全服務 合規服務 資料保護 學習 資源 合作夥伴

AWS 雲端安全

基礎架構和服務可提升您在雲端的安全性

利用 AWS 基礎架構和服務提升安全性。

藉助 AWS，您將獲得所需的控制權和信心，以利用當今最靈活、最安全的雲端運算環境來安全地開展業務。作為 AWS 客戶，您將受益於 AWS 資料中心和架構網路，可對您的資訊、身分、應用程式和裝置提供保護。憑藉 AWS，您可以透過我們全面的服務和功能，來提升滿足核心安全性和合規性要求的能力，例如資料本地性、保護性和機密性。

AWS 可讓您自動執行手動安全任務，因此您可以將重心轉移至業務擴展和創新上。另外，您只需為使用的服務付費。所有客戶都能從 AWS 這個唯一商業平台獲益，其中的服務產品和服務供應鏈都經過審查，且被認為是安全、可用於高

什麼是 AWS Security ?

<https://aws.amazon.com/security/>

學習

雲端安全與內部部署資料中心安全類似，只是無需維護設備和硬體的費用。在雲端中，您不必管理實體伺服器或儲存裝置。而是使用以軟體為基礎的安全工具，以監控和保護進出雲端資源的資訊流。因此，雲端安全是客戶與 AWS 的**共同責任**，其中客戶負責「雲端內容安全」，而 AWS 則負責「雲端安全」。

AWS 雲端可讓您擴展及創新，同時維護環境安全。您身為 AWS 的客戶，將能從資料中心和網路架構的設計中獲益，以滿足組織最為敏感的安全要求。AWS 基礎架構專為雲端定製，全天候受到監控，以助力保護客戶資料的機密性、完整性和可用性。

瀏覽此頁面進一步了解有關 AWS 雲端安全的關鍵主題、研究領域和培訓機會。

白皮書、技術指南和參考資料 | 安全文件 | 可證明的安全性：研究和見解 | 培訓 | AWS 安全控制網域 | 圖庫內容

<http://aws.amazon.com/security/security-resources/>

AWS 雲端安全 概觀 安全服務 合規服務 資料保護 學習 資源 合作夥伴

安全佈告欄

無論我們如何小心翼翼地建構服務，有時還是可能需要通知客戶有關 AWS 服務的安全與隱私相關事件。我們將發佈底下的安全佈告欄。您也可以訂閱我們的**安全佈告欄 RSS 摘要**，以了解安全性宣告的最新資訊。

我想取得有關安全佈告欄的更多資訊

內容類型

☐ 重要

☐ 資訊性

年份

回報的 Apache Log4j 熱修補程式問題
AWS-2022-006, 2022年4月19日

回報的 Windows 的 AWS 桌面 VPN 用戶端問題
AWS-2022-005, 2022年4月12日

已報告的 Amazon RDS PostgreSQL 問題

<https://aws.amazon.com/security/security-bulletins/>

AWS Solutions Library Industry Technology Resource Libraries

Solutions for Security & Compliance

AWS Resilience Day | Join us in NYC to learn how to build resilient architectures in this all-day, hands-on event. Register »

Filter Solutions by:

Clear all filters

Content Type

☐ AWS Solutions

☐ AWS Quick Starts

1-30 (56)

SECURITY, IDENTITY, & COMPLIANCE

SECURITY, IDENTITY, & COMPLIANCE

ANALYTICS | SECURITY, IDENTITY, & COMPLIANCE | MACHINE...

Sort By: Name (A-Z)

<https://aws.amazon.com/solutions/security/>

Blog Home Category Edition Follow

Search Blogs

AWS Security Blog

AWS re:Inforce 2022: Threat detection and incident response track preview
by Celeste Bishop and Charles Goldberg | on 23 JUN 2022 | in Announcements, AWS Reinforce, Events, Security, Identity, & Compliance | Permalink | Comments | Share

Register today

Register now with discount code SALXTDVB7y to get \$150 off your full conference pass to AWS re:Inforce. For a limited time only and while supplies last. Today we're going to highlight just some of the sessions focused on threat detection and incident response that are planned for AWS re:Inforce 2022. AWS re:Inforce is a learning [...]

Read More

New AWS whitepaper: AWS User Guide to Financial Services Regulations and Guidelines in New Zealand
by Julian Busic | on 21 JUN 2022 | in Announcements, Security, Identity, & Compliance | Permalink | Comments | Share

Amazon Web Services (AWS) has released a new whitepaper to help financial services customers in New Zealand accelerate their use of the AWS Cloud. The new AWS User Guide to Financial Services Regulations and Guidelines in New Zealand—along with the existing AWS Workbook for the RBNZ's Guidance on Cyber Resilience—continues our efforts to help AWS [...]

Read More

<http://blogs.aws.amazon.com/security/>

Amazon Linux Security Center Amazon Linux Amazon Linux 2 Amazon Linux 2022 Announcements

Below are bulletins for security or privacy events pertaining to the Amazon Linux AMI. You can also subscribe to our [RSS feed](#).

Date Created	Date Updated	ALAS	Severity	Package	CVE(s)
2022-06-13 16:56	2022-06-15 18:44	ALAS-2022-1601	Important	log4j-cve-2021-44228-hotpatch	
2022-06-06 19:52	2022-06-09 19:01	ALAS-2022-1600	Medium	containerd	CVE-2022-31030
2022-05-31 23:47	2022-06-09 18:57	ALAS-2022-1598	Important	xz	CVE-2022-1271
2022-05-31 23:47	2022-06-09 18:56	ALAS-2022-1597	Important	vim	CVE-2022-0361 CVE-2022-0318 CVE-2022-0359 CVE-2022-0361 CVE-2022-0392 CVE-2022-0413 CVE-2022-0572 CVE-2022-0943 CVE-2022-1154 CVE-2022-1160 CVE-2022-1381 CVE-2022-1420
2022-05-31 23:47	2022-06-09 18:55	ALAS-2022-1595	Important	rubygem-nokogiri rubygem18-nokogiri	CVE-2022-24836
2022-05-31 23:47	2022-06-09 18:54	ALAS-2022-1594	Important	rsyslog	CVE-2014-3634 CVE-2022-24903
2022-05-31 23:47	2022-06-09 18:53	ALAS-2022-1593	Medium	python27	CVE-2020-27619 CVE-2021-23336 CVE-2021-3733 CVE-2021-3737 CVE-2021-4189 CVE-2022-0391
2022-05-31 23:47	2022-06-09 18:52	ALAS-2022-1592	Important	python-twisted-conch	CVE-2022-21716
2022-05-31 23:47	2022-06-09 18:45	ALAS-2022-1591	Medium	kernel	CVE-2022-0854 CVE-2022-1011 CVE-2022-1353 CVE-2022-1516 CVE-2022-1729 CVE-2022-28389 CVE-2022-28390 CVE-2022-29581 CVE-2022-30594
2022-05-31 23:47	2022-06-09 18:43	ALAS-2022-1590	Important	gzip	CVE-2022-1271
2022-05-31 23:47	2022-06-09 18:42	ALAS-2022-1589	Medium	git	CVE-2022-24765

<https://alas.aws.amazon.com/>



Thank you!