© 2020 SPLUNK INC.

獵殺多雲環境的資安威脅

2021 年 5 月

楊耀輝 Daniel Yeung

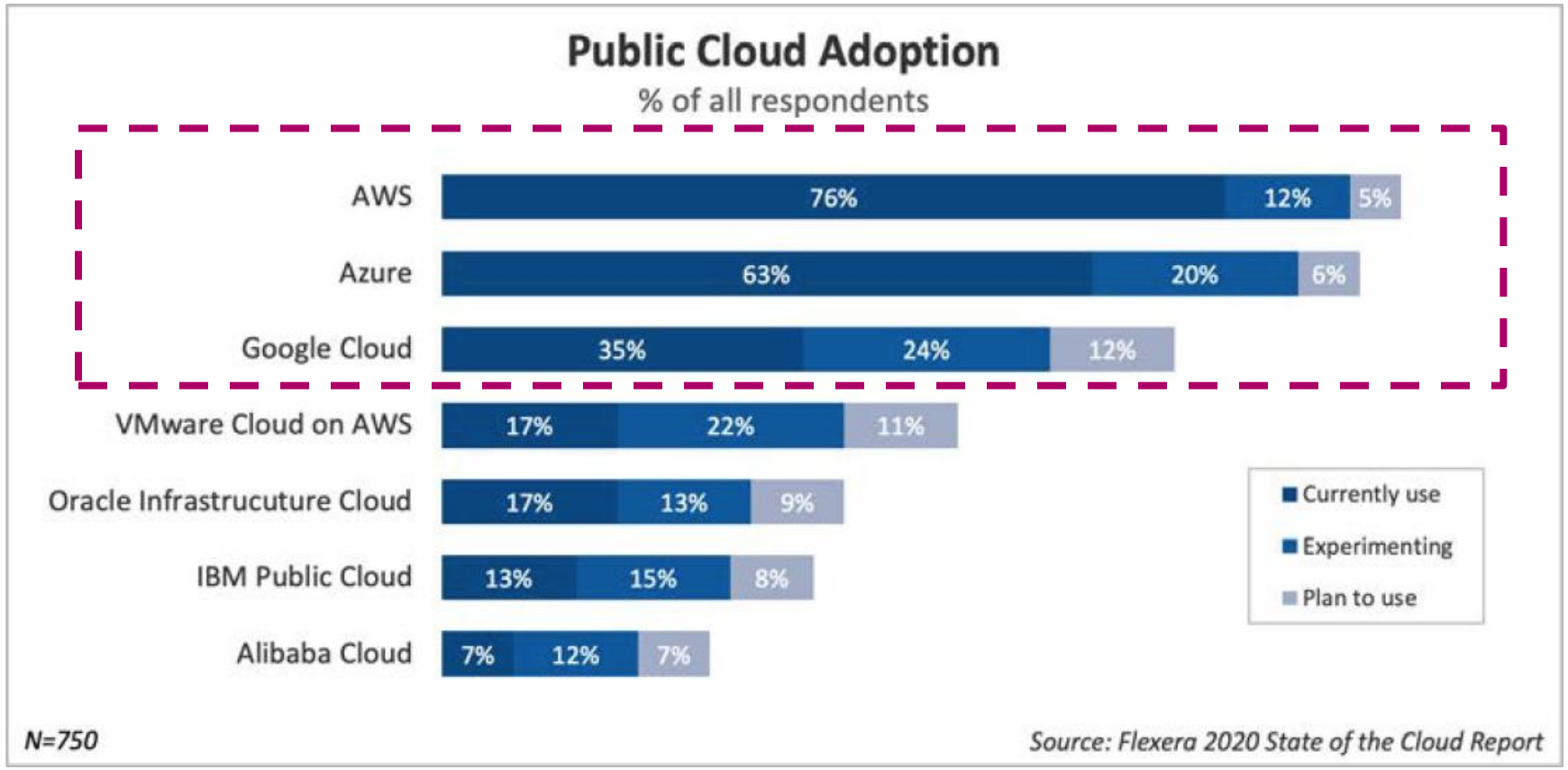
Splunk 北亞區資深合作夥伴售前工程師

splunk> turn data into doing™

© 2020 SPLUNK INC.

全球公用雲端採用情況

2020 年主要雲端供應商



© 2020 SPLUNK INC.

GOVTECH SINGAPORE

政府商業雲 (GCC)

amazon web services

Azure

Google Cloud

以雲端為基礎的開發作業 **(DevOps)** 和安全作業 **(SecOps)**。

- 建立和提供數位服務，為機構和組織內外的員工創造價值。
- 可以自動化並即時完成應用程式測試和部署，加快向民眾和企業提供高品量政府數位服務的速度。

https://www.developer.tech.gov.sg/technologies/infrastructure-and-hosting/government-commercial-cloud

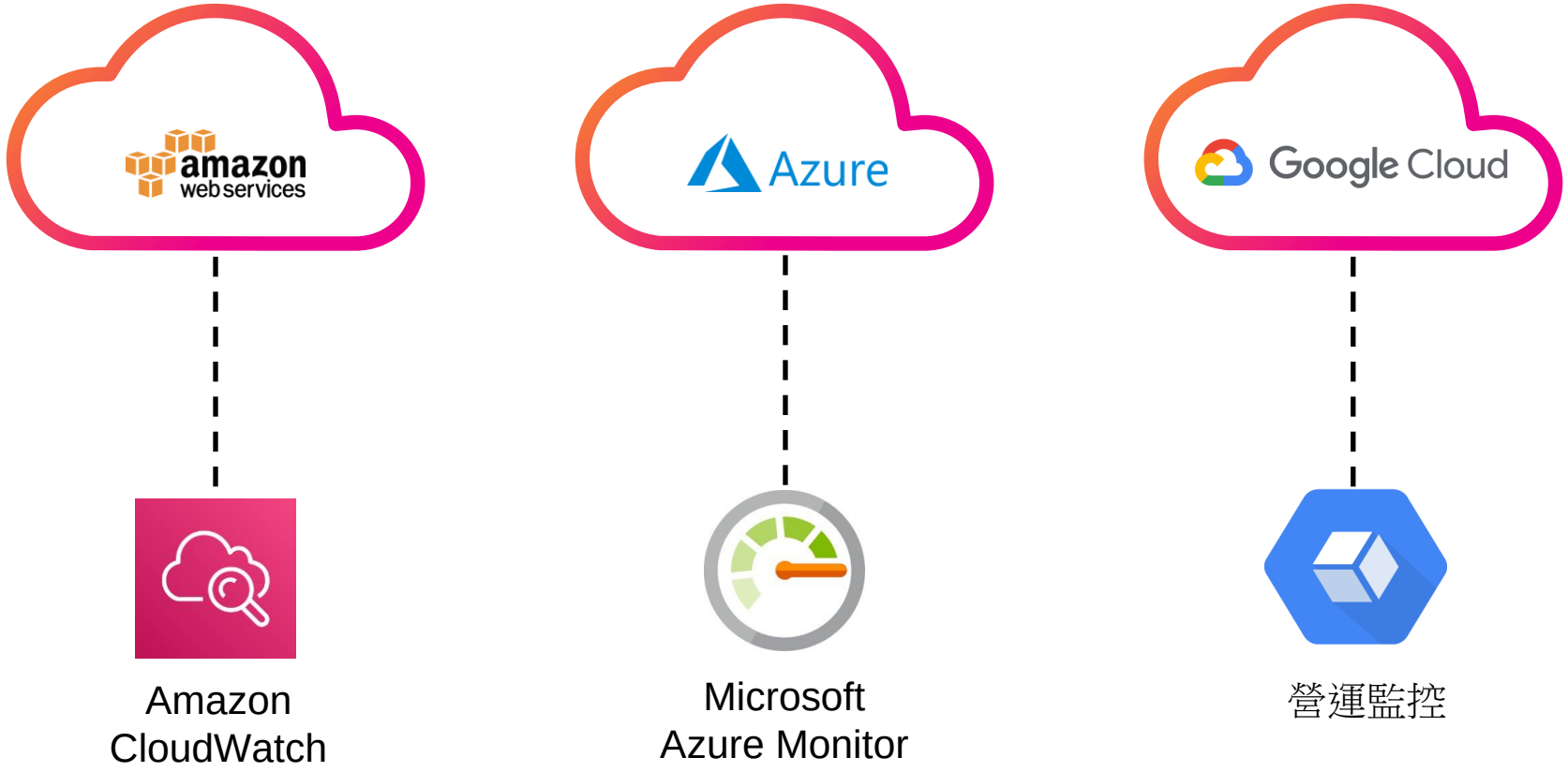
© 2020 SPLUNK INC.

不同的技術和功能

不同的入口網站、合規性、移轉和服務產品組合增加了複雜性

© 2020 SPLUNK INC.

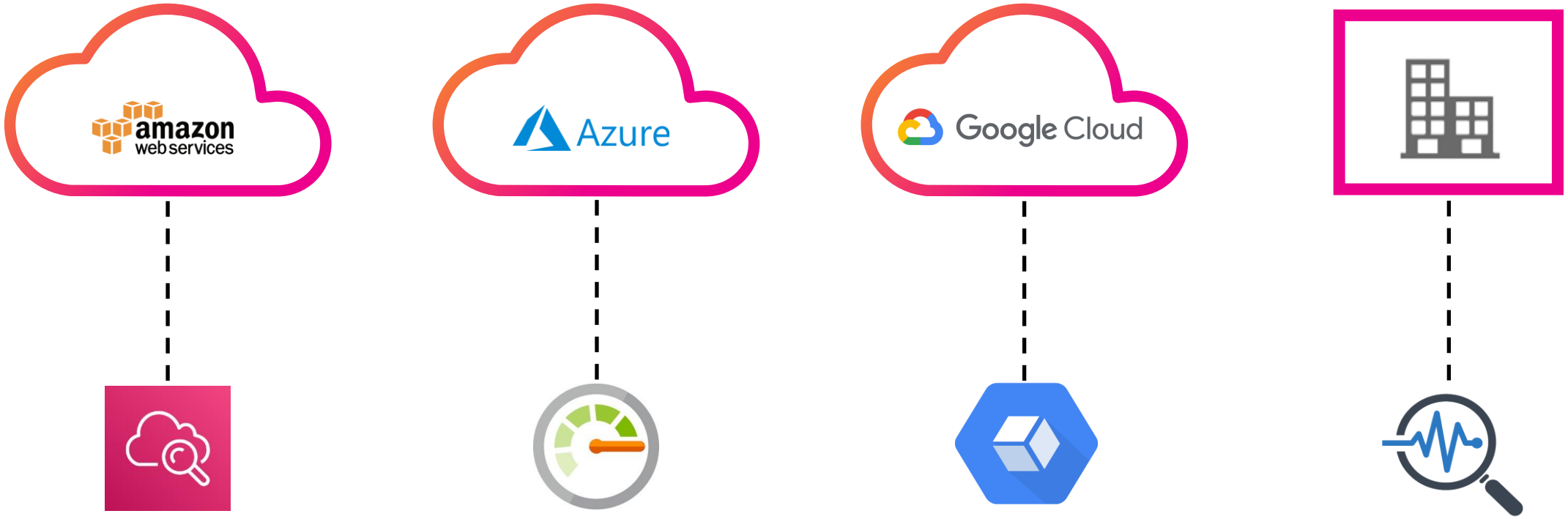
跨雲端供應商的監控 – 範例



3 個不同供應商有 3(+) 個日誌服務/介面

© 2020 SPLUNK INC.

跨雲端供應商和內部部署的監控



© 2020 SPLUNK INC.

雲端安全是共同的責任

splunk> turn data into doing™

© 2020 SPLUNK INC.

雲端安全中的共同責任模型

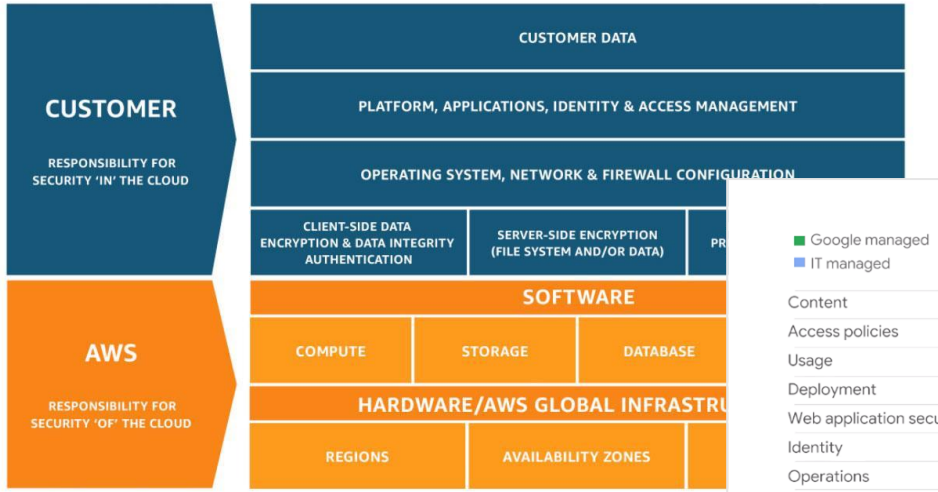
內部部署	IaaS (基礎架構即服務)	PaaS (平台即服務)	SaaS (軟體即服務)
使用者存取	使用者存取	使用者存取	使用者存取
資料	資料	資料	資料
應用程式	應用程式	應用程式	應用程式
作業系統	作業系統	作業系統	作業系統
網路流量	網路流量	網路流量	網路流量
虛擬機器管理程序	虛擬機器管理程序	虛擬機器管理程序	虛擬機器管理程序
基礎架構	基礎架構	基礎架構	基礎架構
實體	實體	實體	實體

客戶責任　　雲端供應商責任

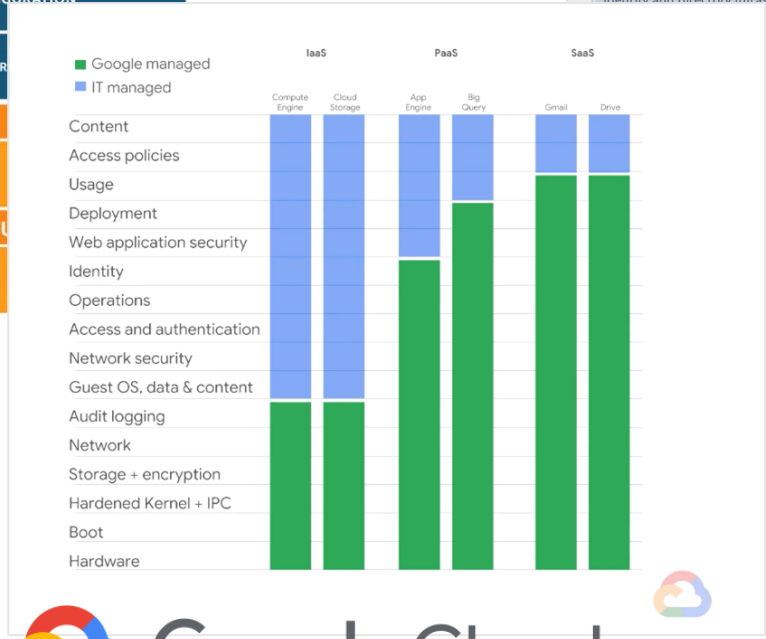
© 2020 SPLUNK INC.

所有雲端平台都採用一個共用安全責任模型

amazon web services



Azure



Google Cloud

© 2020 SPLUNK INC.

底線 – 安全是雲端的共同責任

客戶

客戶資料、應用程式和內容

網路控制

身分識別和存取管理

作業系統/平台

資料加密

負責
安全業務 -
在雲端中

amazon web services

Azure

Google Cloud Platform

運算

儲存

資料庫

網路

可用區域

區域

邊緣位置

負責
安全業務 -
雲端本身

© 2020 SPLUNK INC.

雲端運算的主要威脅

雲端安全聯盟：《十一大威脅》(2020 年)

1. 資料外洩
2. 設定錯誤和變更控制不足
3. 缺乏雲端安全架構和策略
4. 身分識別、憑證、存取和金鑰管理不足
5. 帳戶劫持
6. 內部威脅
7. 不安全的介面和 API
8. 功能不足的控制面板
9. 元結構和應用程式結構故障
10. 雲端使用可見度有限
11. 濫用和惡意使用雲端服務

來源：https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/

© 2020 SPLUNK INC.

雲端運算的主要威脅

雲端安全聯盟：《十一大威脅》(2020 年)

1. 資料外洩
2. **設定錯誤和變更控制不足**
3. **缺乏雲端安全架構和策略**
4. **身分識別、憑證、存取和金鑰管理不足**
5. 帳戶劫持
6. **內部威脅**
7. 不安全的介面和 API
8. **功能不足的控制面板**
9. 元結構和應用程式結構故障
10. 雲端使用可見度有限
11. 濫用和惡意使用雲端服務

粗體字 = *完全是客戶的責任*

來源：https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/

© 2020 SPLUNK INC.

如何使用 Splunk 實現您肩負的共同責任模型

一個可用於監控、偵測、調查和回應的平台

splunk> turn data into doing™

多雲可見度

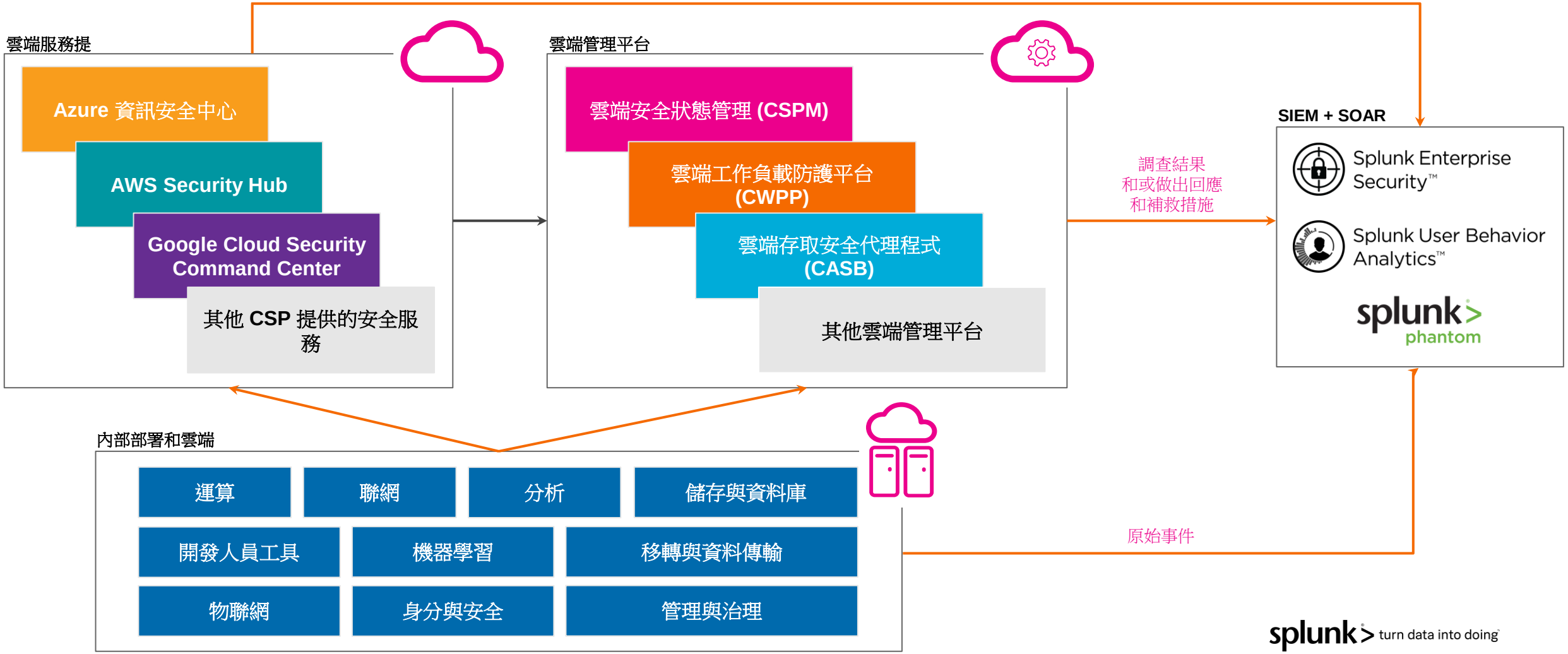
監控、調查和偵測跨雲環境的漏洞和錯誤設定

可見度和分析多雲的威脅面和漏洞

建立和增強用於跨多個雲端供應商的雲端稽核工具

© 2020 SPLUNK INC.

集中式資料和搜尋結果來自所有供應商



splunk> turn data into doing

© 2020 SPLUNK INC.

安全資料之旅

安全記錄與調查

傳統 SIEM

- 集中式記錄和查詢
- 鑑識與調查

持續監控

SIEM+

- 威脅情報自動搜尋
- 以 ML 為基礎的分析
- 連結/模式分析 (威脅搜尋)

自動化

SIEM、SOAR

- 實作 SOAR
- 自動化事件處理
- 攻擊類型的劇本
- 整合式工具

安全控制中心

SIEM、SOAR、UEBA

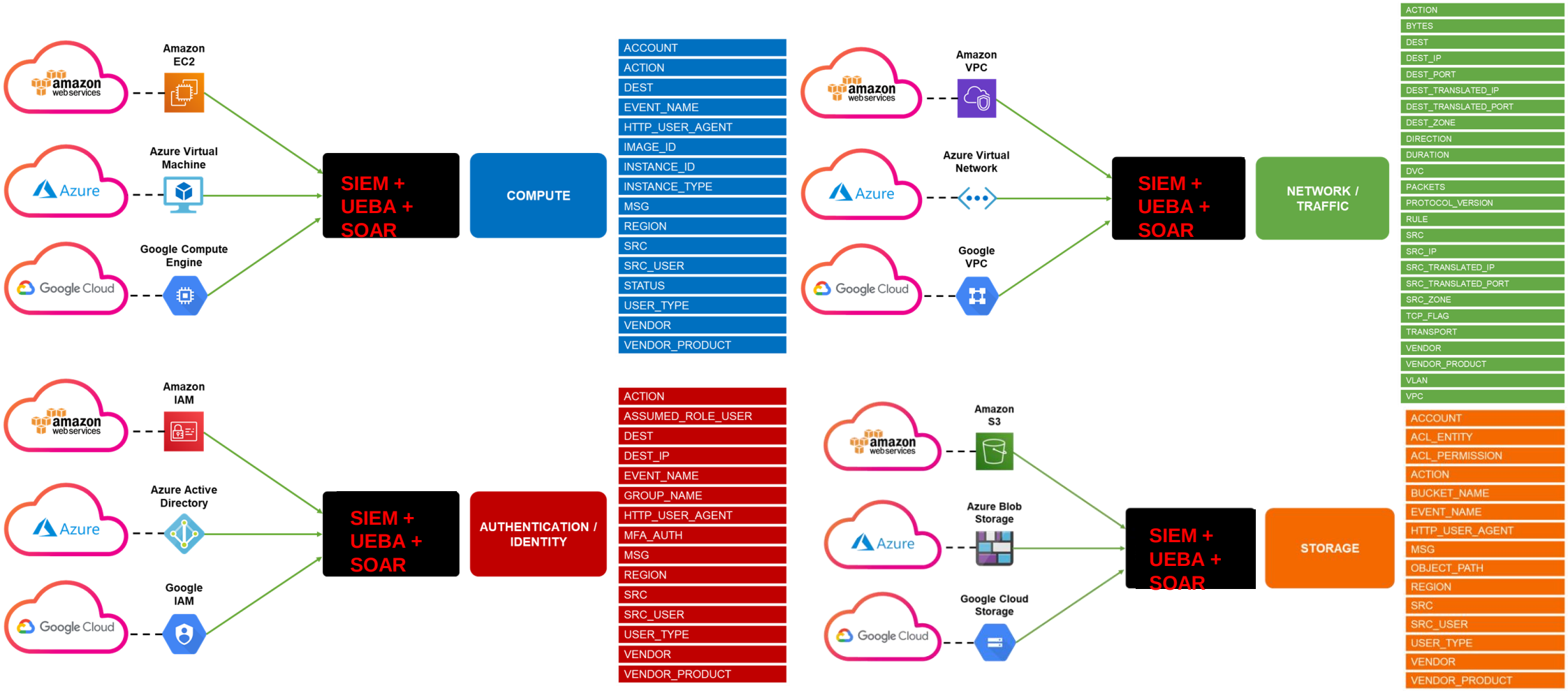
- 進行預測
- 確定可能的攻擊路徑
- 使用者異常和行為分析
- 敵人模擬

splunk> turn data into doing

© 2020 SPLUNK INC.

可用於多雲安全監控的深度分析

跨雲威脅搜尋和事件回應 (IR)



© 2020 SPLUNK INC.

MITRE 雲端矩陣

適用於 AWS、GCP、Azure、Azure AD、Office 365、SaaS (v7) 的雲端技術

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
5 techniques	5 techniques	1 techniques	5 techniques	4 techniques	10 techniques	2 techniques	4 techniques	1 techniques	4 techniques
Drive-by Compromise	Account Manipulation (3)	Valid Accounts (2)	Impair Defenses (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Data from Cloud Storage Object	Transfer Data to Cloud Account	Defacement (1)
Exploit Public-Facing Application	Create Account (1)		Modify Cloud Compute Infrastructure (4)	Steal Application Access Token	Cloud Service Dashboard	Use Alternate Authentication Material (2)	Data from Information Repositories (2)		Endpoint Denial of Service (3)
Phishing (1)	Implant Container Image		Unused/Unsupported Cloud Regions	Steal Web Session Cookie	Cloud Service Discovery		Data Staged (1)		Network Denial of Service (2)
Trusted Relationship	Office Application Startup (6)		Use Alternate Authentication Material (2)	Unsecured Credentials (2)	Network Service Scanning		Email Collection (2)		Resource Hijacking
Valid Accounts (2)	Valid Accounts (2)		Valid Accounts (2)		Network Share Discovery				
					Permission Groups Discovery (1)				
					Remote System Discovery				
					Software Discovery (1)				
					System Information Discovery				
					System Network Connections Discovery				

*來源：*https://attack.mitre.org/matrices/enterprise/cloud/

上次修改日期：2020 年 7 月 2 日

splunk> turn data into doing

© 2020 SPLUNK INC.

Splunk ES 內容更新
Splunk Security Essentials

https://splunkbase.splunk.com/app/3435

使用者呼叫 Cloud API 的頻率比較高

來自異常國家/地區的雲端佈建活動

來自異常 IP 的雲端佈建活動

異常使用者建立的執行個體

異常使用者變更的執行個體

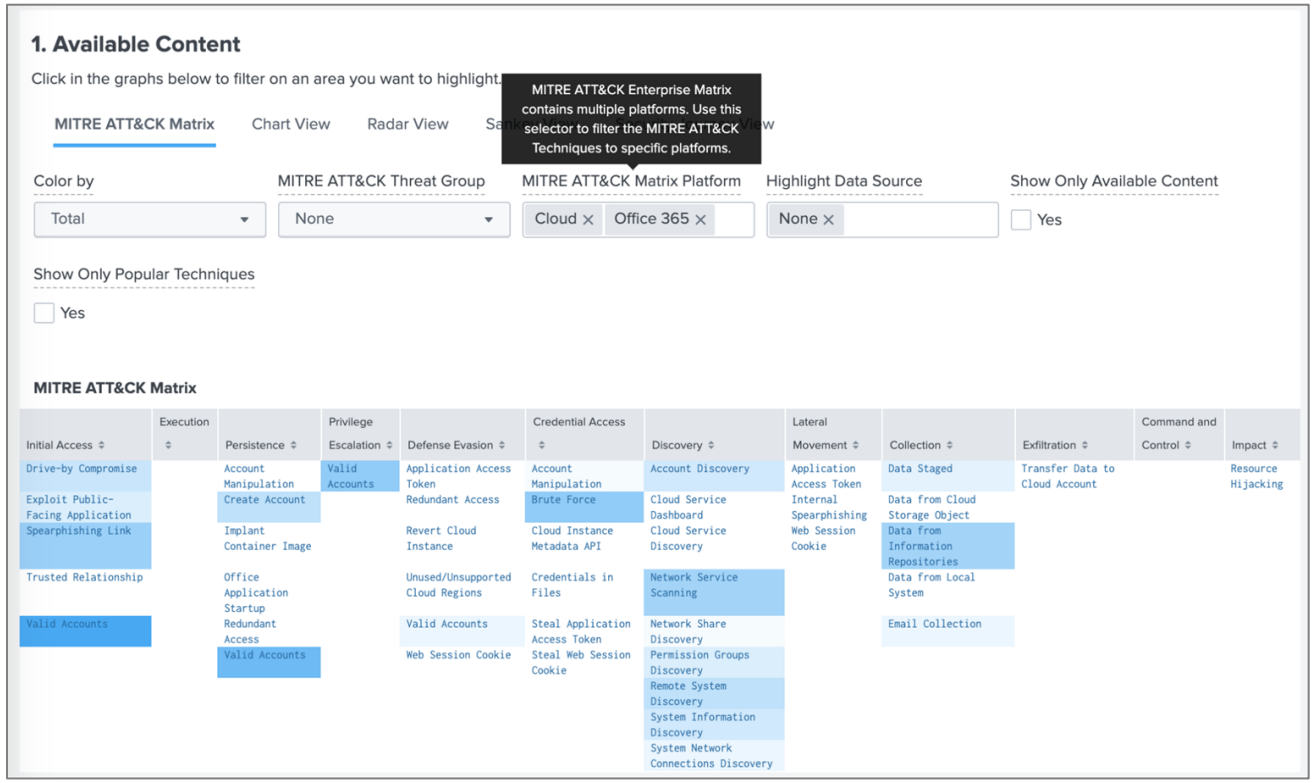
每個對等群組的新 Cloud API 呼叫

每個使用者的新 IaaS API 呼叫

公用雲端儲存 (貯體)

異常雲端區域

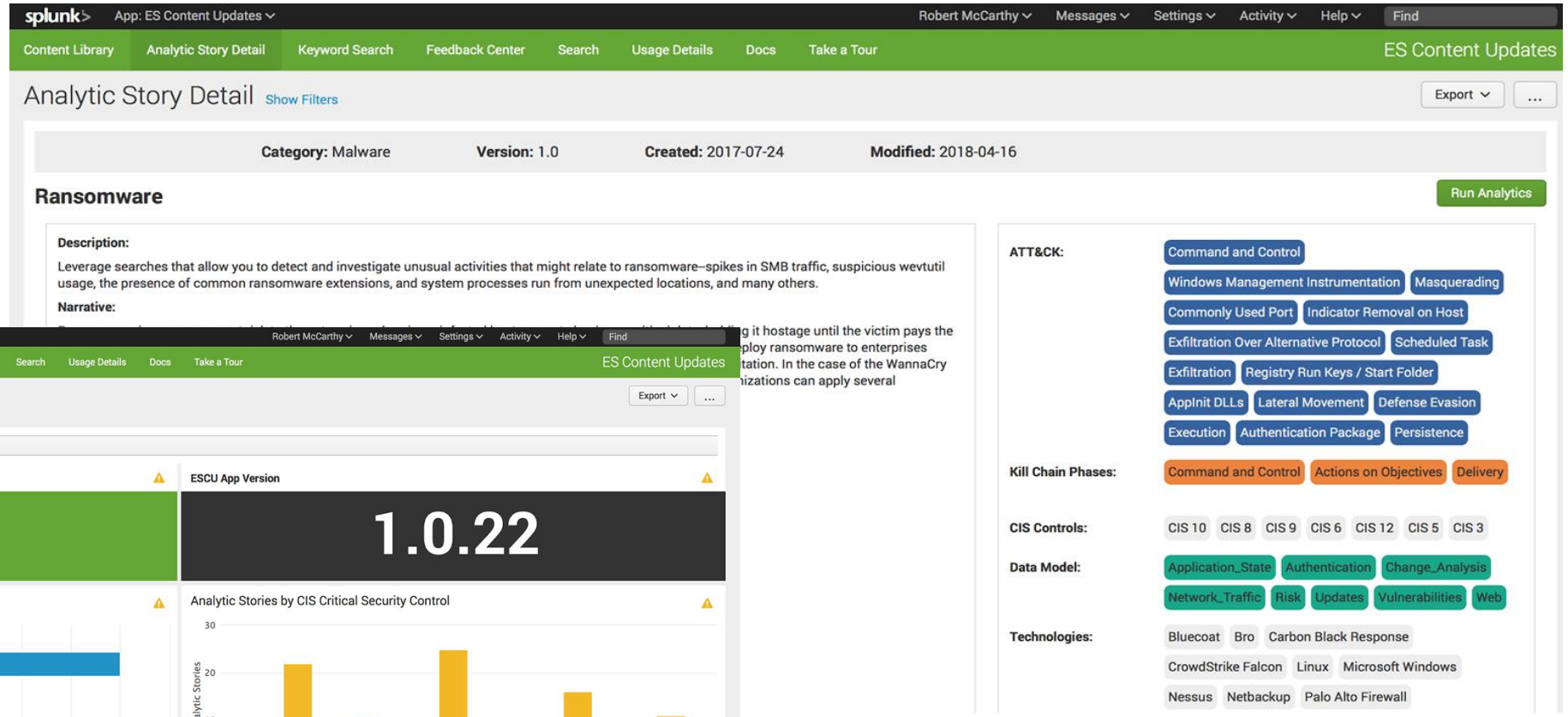
對雲端 ACL 的異常變更次數

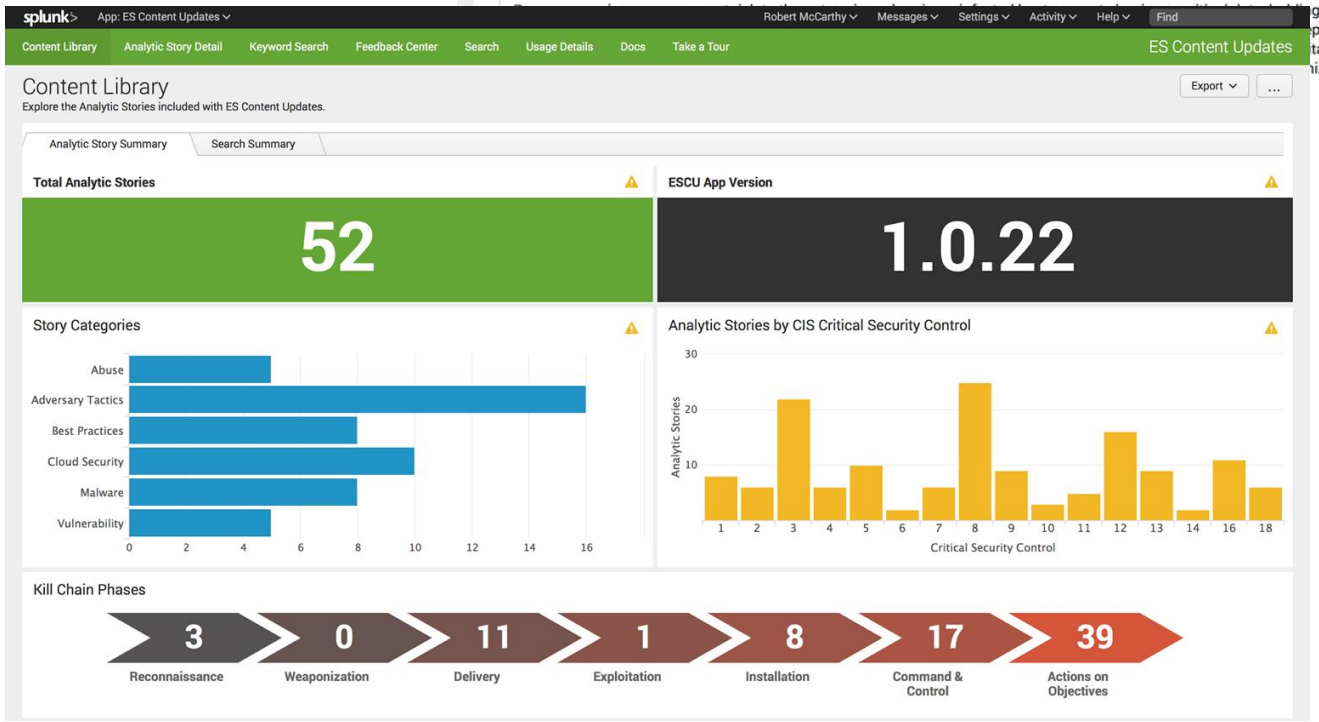


© 2020 SPLUNK INC.

ES 內容更新

▶ 關聯搜尋 ▶ 自適應回應動作 ▶ 知識增強 ▶ 易於實作





‘Analytic Stories’ 包含封裝的知識物件

splunk> turn data into doing

© 2020 SPLUNK INC.

快速、準確地採取正確的行動

Splunk 提供架構和整合功能，可在速度至上的重要時刻時快速回應

單一信任來源

從單一平台跨團隊共用重要的安全情報。

更快地回應

透過自動調查減少暫留時間。以機器速度執行的劇本可以縮短回應時間。

關聯式協作

透過整合的聊天和共用案例筆記，提升整個團隊的溝通效率，並提高狀態感知能力。

提高標準

使用回應範本和內容相關搜索為初級分析人員提供可遵循的指導路徑。

報告和評量

追蹤關鍵的績效指標以識別流程延遲，並專注在需要改進的部份。

© 2020 SPLUNK INC.

下一個步驟

1. **後續培訓**：
   a. AWS 安全實機操作研討會
   b. MS Cloud 搜尋研討會
2. 參與對您環境的**評估**：
   a. 雲端來源的資料來源評估 (Data Soruce Assessment)
   b. 安全規範性價值路徑 (Prescriptive Value Paths)
3. **關於從您的雲端資源中取得資料的技術討論**
   a. 與安全諮詢銷售工程師/雲端架構師安排一次深入的會議
   b. 在 GCP 環境中使用 Splunk (https://github.com/amiracle/cooking_with_Splunk_and_GCP)
   c. 在 AWS 環境中使用 Splunk (https://github.com/amiracle/cooking_with_Splunk_and_AWS)

© 2020 SPLUNK INC.

Thank You

splunk> turn data into doing™

© 2020 SPLUNK INC.

附錄

© 2020 SPLUNK INC.

競爭產品

splunk> turn data into doing™

© 2020 SPLUNK INC.

Azure Sentinel

要考慮的主題

可擴展性

與 ITSM 整合/案例管理

合作夥伴和客戶生態系統

廠商鎖定

對雲端資源的有限支援

新產品 (2019 年 9 月推出正式版本)

歷史分析

資料保留

© 2020 SPLUNK INC.

Chronicle Security

評估重點

報告和儀表板

它是否支援 Google Cloud Logging 和 Cloud Monitoring*？

- 資料擷取的透明度/模糊性

協作、自動化和回應的能力

威脅偵測使用新的 YARA-L 規則語言

新產品 (2020 年 3 月推出正式版本)

**先前稱為 Stackdriver*

© 2020 SPLUNK INC.

Palo Alto Prisma Cloud/Cortex XDR

評估重點

兩種獨立的解決方案：Prisma Cloud (僅雲端資料來源) (CSPM) 和 Cortex XDR (SIEM)

Prisma Cloud 比 SIEM 更像是雲端安全狀態管理工具 (CSPM)

對非 Palo Alto 資料來源和 Cortex XDR 中的 Prisma Cloud 資料支援有限

對除 AWS、Azure、GCP 以外的任何雲端支援有限

對「鑑識」的支援有限

- 沒有提供原始資料
- 僅可使用 Prisma 收集的中繼資料

可以與 Splunk 解決方案 (ES、Phantom、Mission Control) 整合

© 2020 SPLUNK INC.

為什麼選擇 Splunk

Unique Splunk value	It matters because …	Did you know that -
Any Data	data silos and structure dependent tools cannot deliver integrated holistic outcomes	Splunk is the only solution that delivers capabilities across - APM, ITOA, SIEM, UBA, SOAR, IoT, Streaming, Federated search, Incident mgmt. automation industries. When we say Data to Everything, we mean - 'Everything'.
Any Source	Data sources can be anywhere - public cloud, private clouds, Industrial IoT	Splunk has the broadest and deepest data ingestion ecosystem with 2000 Splunkbase apps
Any Timescale	Real time streaming data for instant action or historical data for investigations - Splunk supports it all	a Data lake, Data store is not an investigation tool - data stored in a repository does not equate to outcomes which can be used instantly. Splunk delivers this. E.g. SOC/NOC investigations. "Investigation" is the outcome
Any insight	insights, like data should not be siloed by use cases, business units	because Splunk ML/AI is applied to all data it ingests, it allows end users to conduct cross use-case investigations and derive insights which would otherwise take complex custom integrations
Any Action	insights are only valuable if they trigger Actions	Splunk is the only integrated solution that provides all of the above capabilities along with the ability to take Action - whether it's Security Automation or Incident mgmt. automation
Any Cloud	Customers do not like vendor lock-ins. They want true Cloud neutrality for deployment and monitoring	~84% of large enterprise customers already have a multi-cloud strategy. They need investment protection and no vendor lock-ins
Trusted platform by 92% of Fortune 100 customers	Maturity and experience cannot be manufactured	most Splunk competitors do not have regional references which span more than 1-2 use cases.
Active & thriving partner and customer ecosystem	End users can find local, regional support. It also helps support their own career planning with Splunk opportunities	Most Splunk competitors do not even have a regional end user community or anything compared to Splunk Live ~50% of all Splunkbase apps are created by Splunk partners and customers. That's a mature, extensible & proven platform that will continue to deliver ROI as technologies change