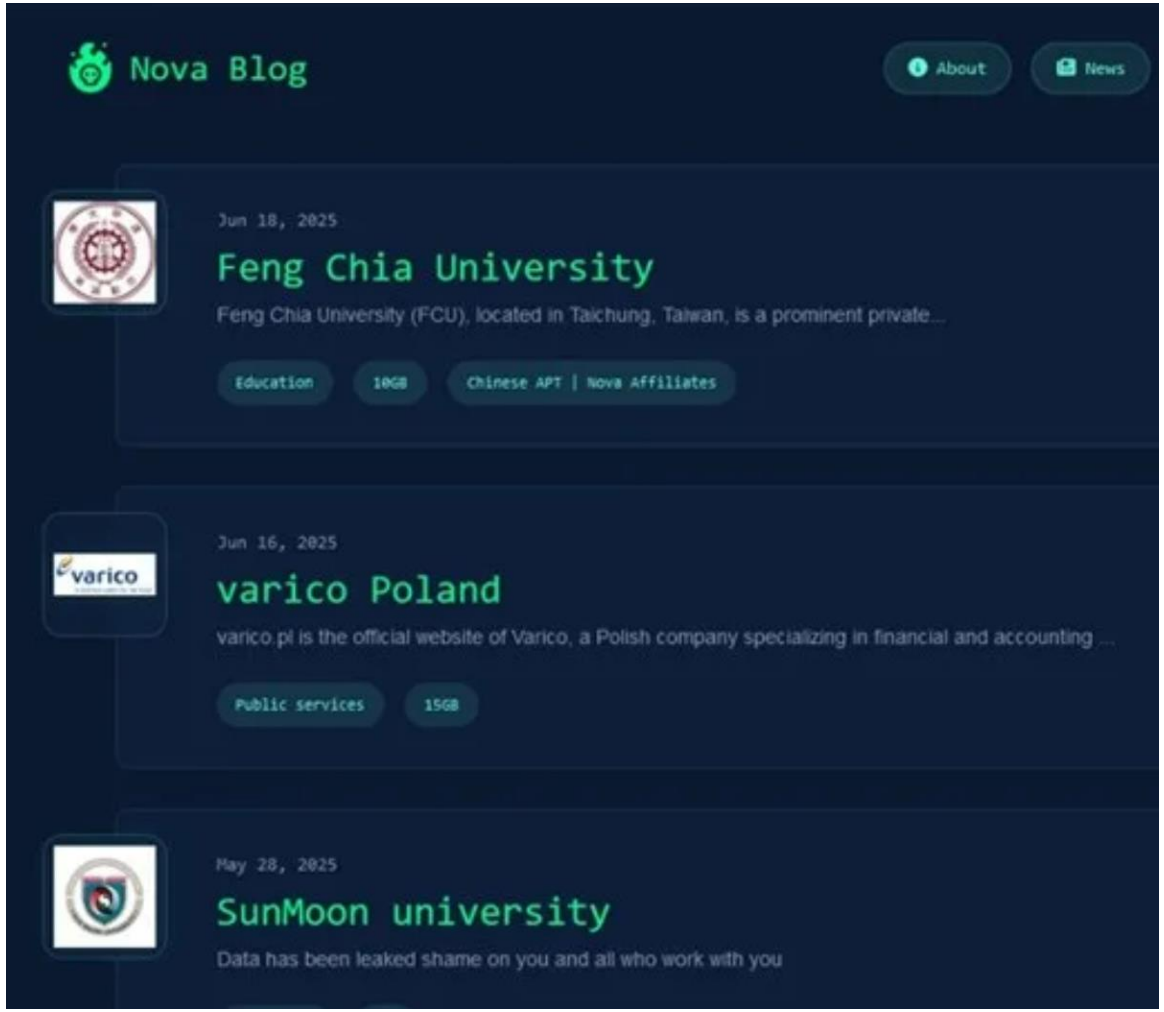
建構韌性校園

風險管理策略與實務分享

資深技術顧問
邱柏翰

勒索軟體聯手陸國家級駭客入侵大學

2025

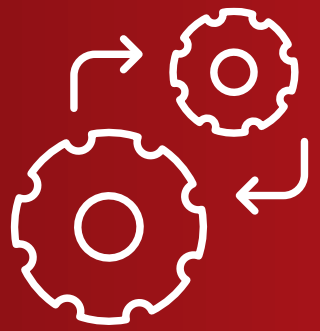


https://udn.com/news/story/6928/8818363

根據Nova暗網中顯示，此次入侵逢甲大學之後，已**拿到10GB資料**，這些資料**包含一些程式碼、員工數據、學生付款紀錄、數據庫架構**。如果逢甲大學不回應Nova的要求，10天之後，Nova將會對外公開部分資料。

資安業者指出，過往，勒索軟體大多比較喜歡入侵企業端，因為企業內部擁有許多極具商業價值的機密，一旦將這些資料拿到手，駭客就能夠向企業要求高昂的贖金，藉此大撈一票；近年，**學術單位成為駭客的新目標，主要原因在於學校內部也有許多研究機密、合作計劃、政府與產業機構資料庫，商業價值不低，因而成為駭客集團瞄準的對象。**

Reactive 被動反應



SIEM

EDR

防毒

NDR

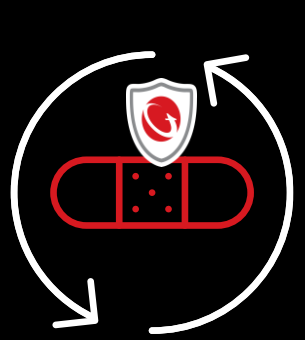
XDR

MDR

+ and more...

與其被動回應，現在更需要主動防護

Proactive 積極管理

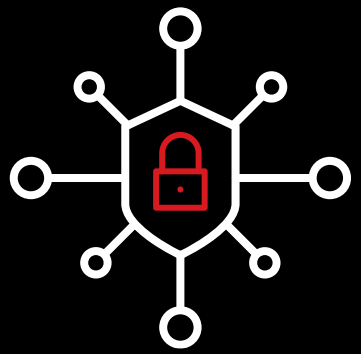


虛擬修補

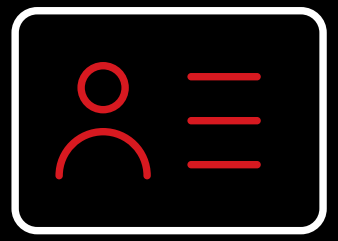
預測分析

威脅情報

脆弱性管理



零信任



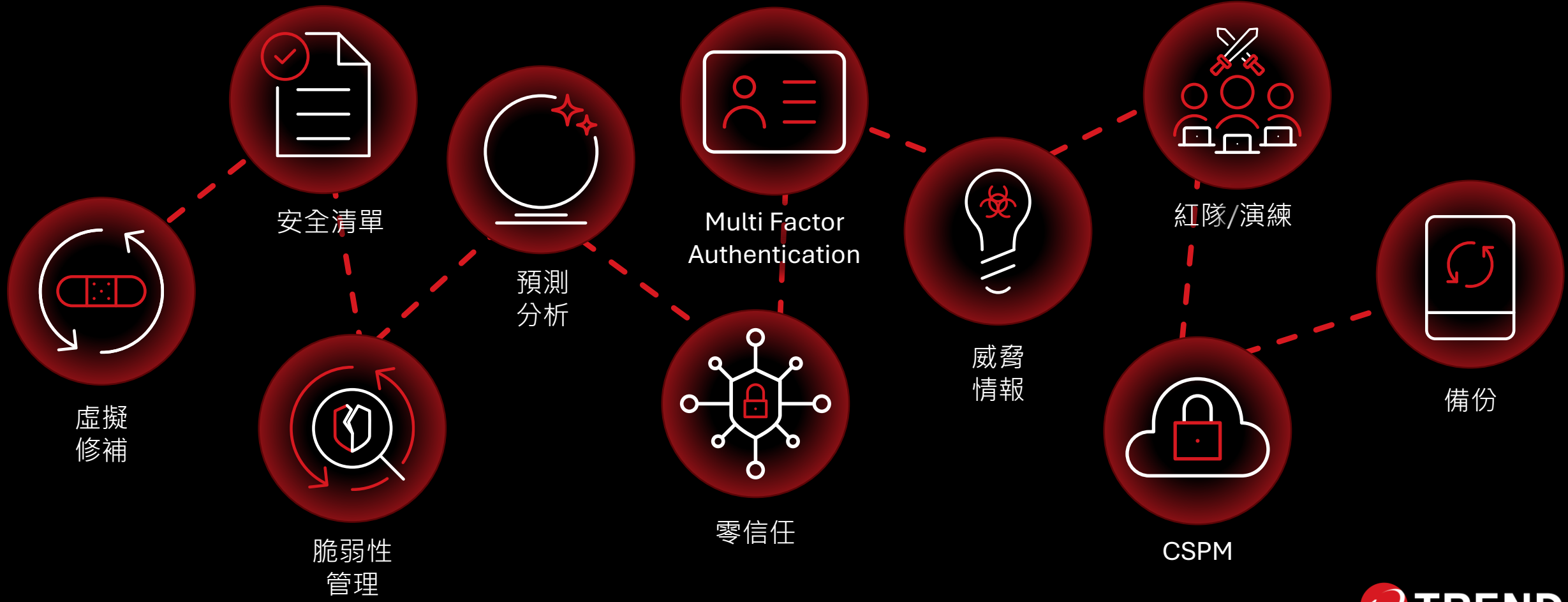
MFA

+ and more...

Reactive 被動反應

工具太多、資料分散，缺乏串接與整合

關聯這些各自為政的紀錄是一項花費大量時間與人力的工作.....



資安工具不能再是

各自為政

CREM

Cyber Risk Exposure Management

資安曝險管理

資安曝險管理與服務 - 讓資安維運更快速簡單

每日 即時風險通報

- **威脅攻擊事件**

Workbench for Endpoint/Network /Cloud

- **帳號異常活動監控**

Microsoft Entra-ID/On premise AD/Okta

- 高風險雲端資產

AWS/Azure/GCP

高風險事件分析及調查

每週 重要主機風險通報

- **作業系統/應用程式重大弱點通報**

CVSS 9分 + CVE High
趨勢全球流通弱點情資

- **重要主機/雲端資產**

風險分析Risk Score統計

弱點修補系統更新

線上課程

- 線上實務分享

趨勢InfoSec資安實務分享
Vision One運用技巧
CREM新功能介紹

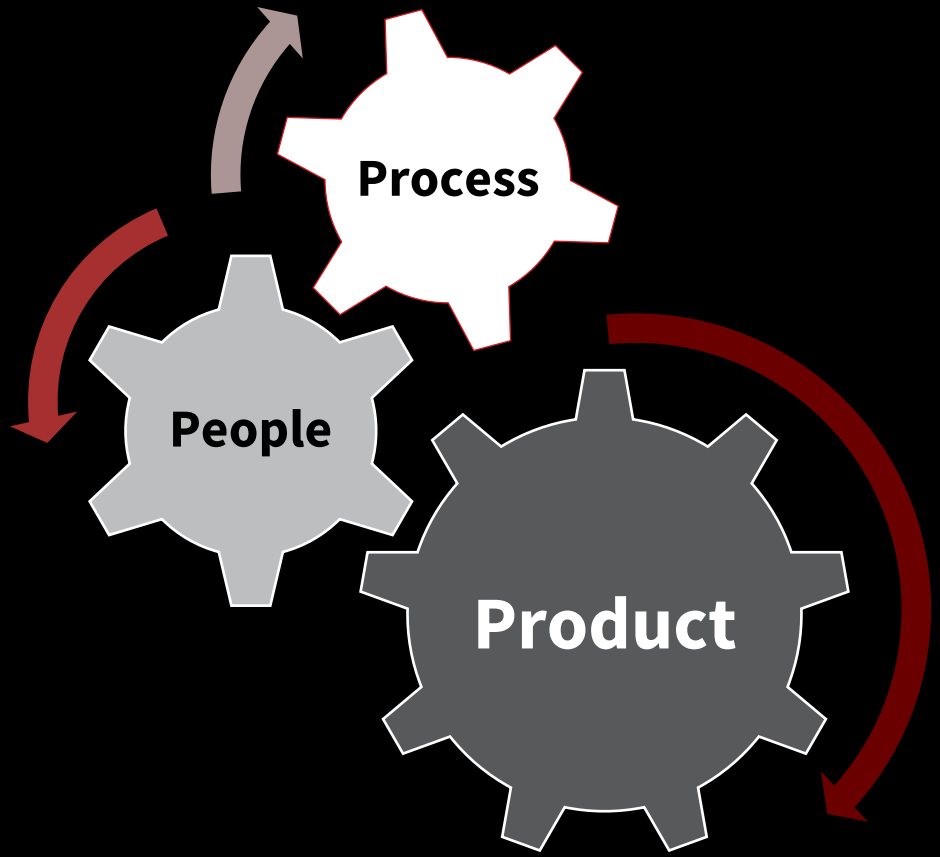
- **主題式及實務課程**

弱點管理實務
Public GenAI管理實務

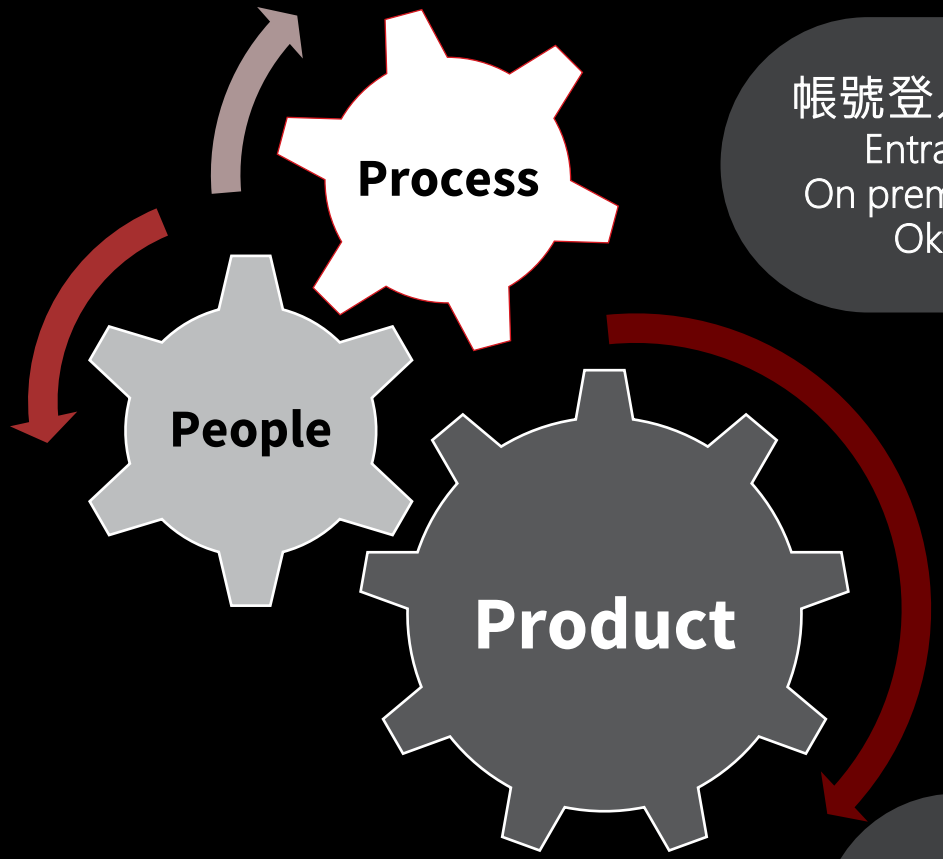
建立觀念實機練習

TREND MICRO

資安曝險管理與服務 - 運作流程



資安曝險管理與服務 - Product



同步防火牆記錄
PA/Fortinet/Defender..

Service Gateway

帳號登入記錄
Entra-ID
On premise AD
Okta

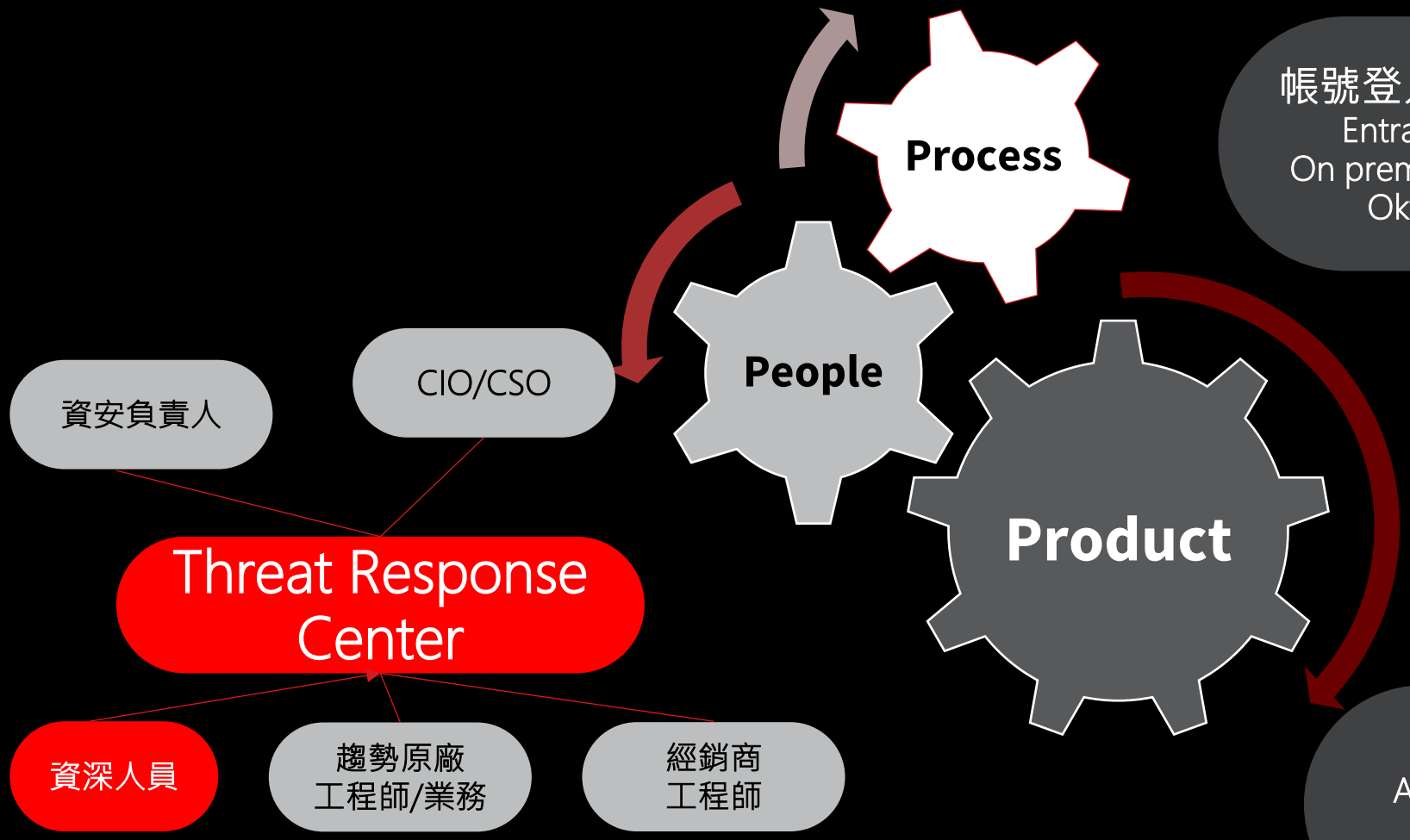
雲端服務IAM授權
AWS/Azure/GCP

Trend
Vision One

Sensor
Endpoint/Email

Product
ApexOne/Deep Security
郵件防護
DDI/Tipping Point...

資安曝險管理與服務 - People



同步防火牆記錄
PA/Fortinet/Defender..

Service Gateway

帳號登入記錄
Entra-ID
On premise AD
Okta

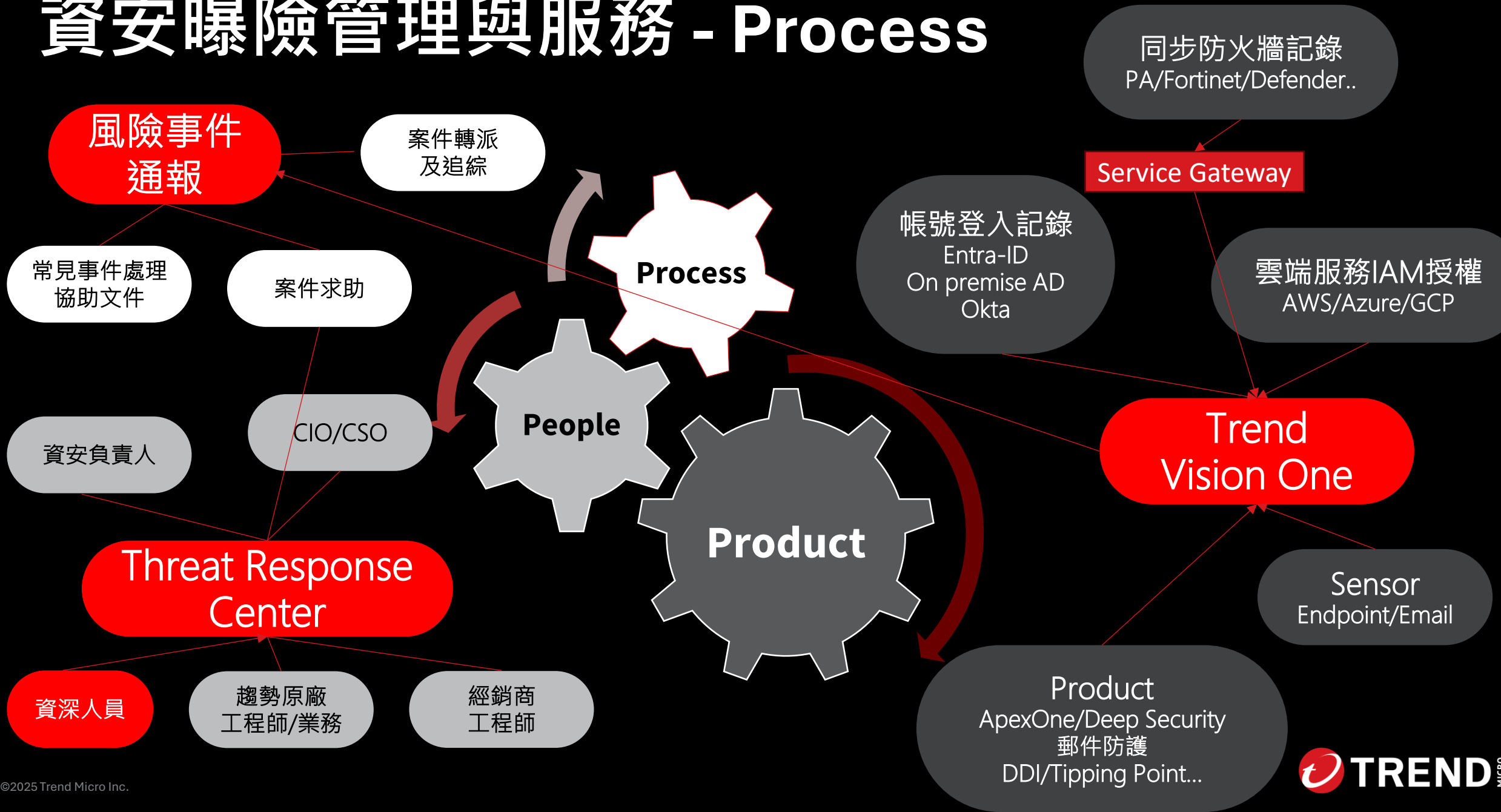
雲端服務IAM授權
AWS/Azure/GCP

Trend Vision One

Sensor
Endpoint/Email

Product
ApexOne/Deep Security
郵件防護
DDI/Tipping Point...

資安曝險管理與服務 - Process



(1).高風險威脅攻擊事件通報-快速回應

Threat Response Center

大型社團法人

(1).高風險 快速回應

Threat Response Center

[Heuristic Attribute] Impair Defenses 是什麼攻擊

什麼是 Heuristic Attribute: Impair Defenses 攻擊？

Heuristic Attribute: Impair Defenses 是一種惡意軟體或攻擊的行為特徵，它指的是該惡意行為嘗試**削弱或禁用電腦系統上的防禦機制**。

想像一下，你的電腦有一道道的防線來保護它，例如：

- **防毒軟體 (Antivirus software):** 偵測並移除惡意程式。
- **防火牆 (Firewall):** 阻止未經授權的網路連線。
- **使用者帳戶控制 (User Account Control, UAC):** 在程式嘗試更改系統設定時提醒你。
- **安全性更新 (Security updates):** 修補系統漏洞。

當惡意軟體具有 "Impair Defenses" 這個啟發式屬性時，它代表該軟體正在試圖做以下一種或多種事情：

- **關閉或禁用防毒軟體：** 阻止防毒軟體偵測到它。
- **修改防火牆設定：** 開啟特定的網路埠，讓攻擊者可以遠端存取。
- **禁用或繞過 UAC：** 在沒有使用者同意的情況下進行系統變更。
- **阻止系統更新：** 讓系統保持在有已知漏洞的狀態。
- **刪除或破壞安全性相關檔案：** 讓防禦機制無法正常運作。

為什麼這很重要？

如果惡意軟體成功削弱了你的防禦，那麼它就能更容易地：

- **安裝額外的惡意程式 (如勒索軟體、間諜軟體)。**
- 竊取敏感資訊。

問問 Gemini

+ Deep Research Canvas 圖像

efenses

大型社團法人

TREND MICRO

(1).高風險威脅攻擊事件通報-快速回應

Threat Response Center

威脅事件摘要

通報時間	2025/6/12 上午 11:41:05
威脅等級	High
威脅情境	[Heuristic Attribute] Impair Defenses
受影響主機名稱 / IP	tz[redacted]4

大型社團法人

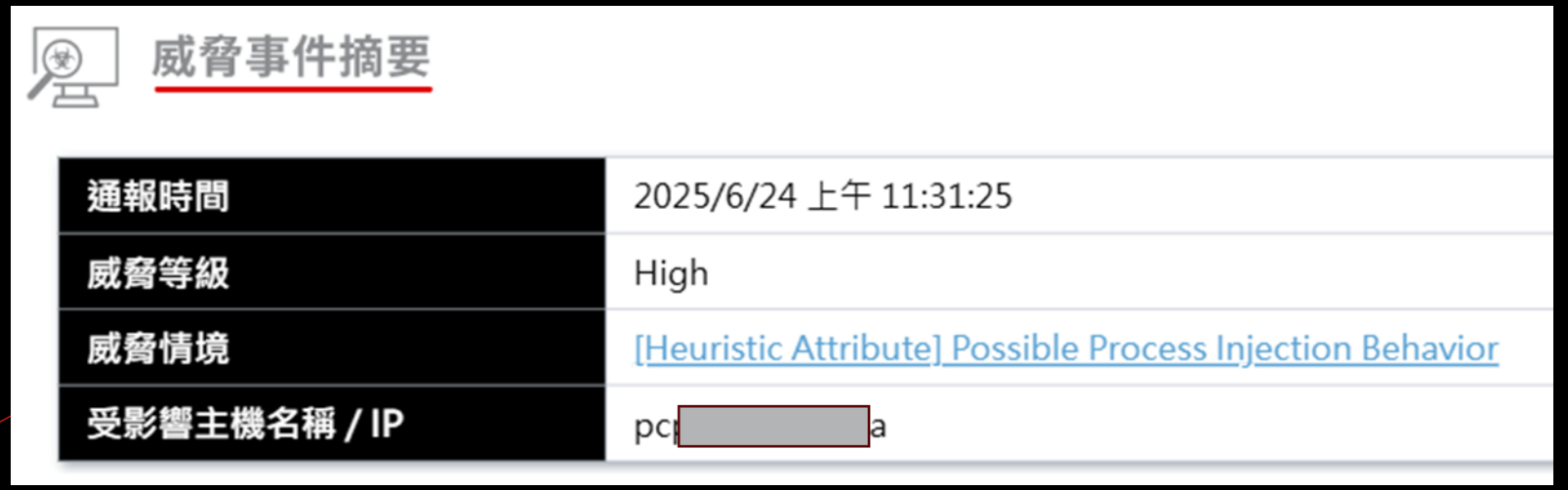
週四 2025/6/12 下午 01:42

經查
為委外廠商提出進行該電腦(Tzxxxx4)安裝廠商系統Client軟體，故資訊人員進行暫時關閉該電腦防火牆功能
安裝完成即會恢復開啟，為已知行為
以上

資安其實不會很難

(2).高風險威脅攻擊事件通報-快速回應

Threat Response Center



重點產業
零件製造商

(2).高風險威脅攻擊事

Threat Response Center

威脅事件摘要

通報時間	20
威脅等級	Hi
威脅情境	[H
受影響主機名稱 / IP	pc

重點產業
零件製造商

[Heuristic Attribute] Possible Process Injection Behavior是什麼行為

什麼是 Heuristic Attribute: Possible Process Injection Behavior 攻擊？

Heuristic Attribute: Possible Process Injection Behavior 是一種惡意程式的行為特徵，它表示該程式可能正在嘗試執行**程序注入（Process Injection）**。

想像一下，你的電腦上有很多不同的「程序」（program 或 process），它們各自負責不同的任務，就像一個個獨立運作的工廠。程序注入就像是：

- **一個壞人（惡意程式）** 試圖把自己**偷偷塞進**一個**正在合法運作的工廠（合法程序）** 裡。
- 它們這樣做是為了**隱藏自己**，避免被偵測。
- 一旦進入，這個壞人就可以**利用這個合法工廠的權限**，做一些原本它自己做不到的壞事。

程序注入的常見目的：

1. **規避防禦：** 許多安全軟體會監控新啟動的程式或可疑的執行檔。通過注入到一個已經受信任的程序中，惡意程式可以**繞過這些初始的檢查**。
2. **提升權限：** 如果惡意程式注入到一個具有更高權限的系統程序中，它就可以**獲得相同的權限**，從而進行更深層的系統破壞或數據竊取。
3. **持久化：** 有些程序注入技術可以讓惡意程式在系統重啟後依然存在，保持其**持久的控制能力**。
4. **隱藏惡意活動：** 惡意程式的行為會被**歸因於被注入的合法程序**，使得安全分析師難以追蹤真正的威脅來源。
5. **竊取資訊或執行惡意程式碼：** 一旦注入成功，惡意程式就可以在被注入的程序上下文中執行任何惡意操作，例如竊取密碼、鍵盤記錄、傳播勒索軟體等。

常見的程序注入技術：

問問 Gemini

+ Deep Research Canvas 圖像

Gemini 可能會出錯，請查證回覆內容

TREND MICRO

(2).高風險威脅攻擊事件通報-快速回應

Threat Response Center

威脅事件摘要

通報時間	2025/6/24 上午 11:31:25
威脅等級	High
威脅情境	[Heuristic Attribute] Possible Process Injection Behavior
受影響主機名稱 / IP	pc[redacted]a

週二 2025/6/24 下午 12:07

Dear Service
終止網路:已拔除pcxxxxxxa
已改user密碼
請提供更詳細風險資訊

重點產業
零件製造商

TREND MICRO

專業的事情
交給專業的人

(3).帳號異常事件通報-帳號外洩快速回應

Threat Response Center

某知名媒體公司

(3).帳號異常事件通報-帳號外洩快速回應

Threat Response Center

2025年5月21日 上午10:25

某知名媒體公司

各位好！
請問這個通知（除了請USER改密碼之外），我們需要做什麼加強的部分？
這位是我們公司的高層經營USER，他的帳號資訊被收集是很容易的，他長期有再經營FB群組及MAIL帳號已經使用20多年。

除了請USER更換高強度的密碼外，是否有其他建議的事項或作法，謝謝！

(3).帳號異常事件通報-帳號外洩快速回應

Threat Response Center

May 21, 2025 2:30 PM

通常帳密被利用，有以下幾道防線：

1. 帳號（帳號格式很難猜，但只要有「範本」就可以推論，並擴大測試範圍）
2. 密碼（如果外洩的明碼看得出規律，那就有機會推論下一個密碼，甚至大大縮小字典檔案需要猜測的範圍）
3. 多因子驗證（MFA）

一定得公開的帳號，通常只能給最小權限，或限定只能存取特定主機，絕對不能碰high-risk device。
制定資安規則，要求員工不可以使用公司email在外面註冊任何服務。
密碼的部分，除了長度（如：13碼）、複雜度（含英文大小寫、數字、符號）之外，
必須檢視不具規則，類似：P@ssw0rdJan，依照大多30改一次密碼，就可以猜下次會變成P@ssw0rdFeb。
另外，如果還沒有MFA機制，建議導入MFA機制。

2025年5月21日 上午10:25

各位好！
請問這個通知（除了請USER改密碼之外），我們需要做什麼加強的部分？
這位是我們公司的高層經營USER，他的帳號資訊被收集是很容易的，他長期有再經營FB群組及MAIL帳號已經使用20多年。

除了請USER更換高強度的密碼外，是否有其他建議的事項或作法，謝謝！

某知名媒體公司

2025年5月21日 下午2:37

OK，收到。
謝謝你們的建議！
上午已經請老闆更換新的PW，並達到14-15個字元的高強度密碼機制。
因他前2-3年有一次FB帳號密碼被盜，應該也有被紀錄出去暗網資料，所以我們會再三留意他的帳號狀況。
除了請USER更換高強度的密碼外，是否有其他建議的事項或作法，謝謝！

不見得只是危機
也可以是轉機

(4).重大弱點通報

Threat Response Center

台灣
資安負責人

IT主管

Trend Vision One™ 重要主機風險統計週報

TREND MICRO

2025/05/17 星期一 下午3:30

	主機名稱	作業系統版本	主機風險分數 Risk Score	作業系統及應用程式弱點	
				未更新	已修補
1	[redacted]_TH_DC01.[redacted]	Windows Server 2016	91	5	0
2	AG[redacted]	Windows Server, version 1809	87	26	0
3	[redacted]VDC01.g[redacted]w	Microsoft Windows Server 2016	87	4	0
4	[redacted]VDC02[redacted].tw	Microsoft Windows Server 2016	87	4	0
5	TWDDC01	Windows Server, version 1809	87	33	0
6	TWDDC02	Windows Server, version 1809	87	29	0

TREND MICRO

(4).重大弱點通報

Threat Response Center

台灣
資安負責人

IT主管

目標主機資訊

2025/05/12 下午4：52

電腦名稱	ApexOneNew
IP	192.168.2.88
Operation System	Windows Server, version 1809 Build 17763
User Name	

重大風險清單

需修補的作業系統或應用程式	CVE弱點說明	CVSS 分數	修正弱點方式
Windows Server 2019	CVE-2024-38063	9.8	Solution Link

TREND MICRO

(4).重大弱點通報

Threat Response Center

2025/05/17上午8：12

請提供要更新的hotfix

台灣資安負責人

2025/05/12 下午4：52

Cxxxx,Txxx,如下請立即查核與確認,無更新請處理,更新有問題請發出請教
Xxxx
集團資訊處副總.

IT主管

2025/05/17 上午8:13

Cxxxx,Txxx有問題電腦全部斷網拆下.
Xxxx
集團資訊處副總

(4).重大弱點通報

Threat Response Center

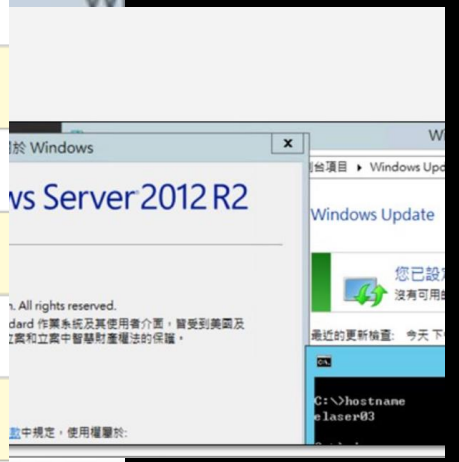
台灣
資安負責人

IT主管

Trend Vision One™ 重要主機風險統計週報

TREND MICRO

	主機名稱	作業系統版本	主機風險分數 Risk Score	作業系統及應用程式弱點	
				未更新	已修補
1	[redacted]	Windows Server, version 1809	87	3	0
2	[redacted]	Windows Server, version 1809	87	3	0
3	[redacted]	Windows Server, version 1809	87	3	0
4	[redacted]	Windows Server, version 1809	87	3	0
5	[redacted]	Windows Server, version 1809	87	3	0
6	[redacted]	Windows Server, version 1809	87	6	0
7	[redacted]	Windows Server, version 1809	87	5	0
8	[redacted]	Windows Server, version 1809	87	4	0
9	[redacted]	Windows Server, version 1809	87	3	0
10	[redacted]	Windows Server, version 1809	87	25	0



TREND MICRO

持續落實修正

風險就會降低

進階的XDR / MDR服務
Agentic SIEM

Our Vision: Trend Vision One™

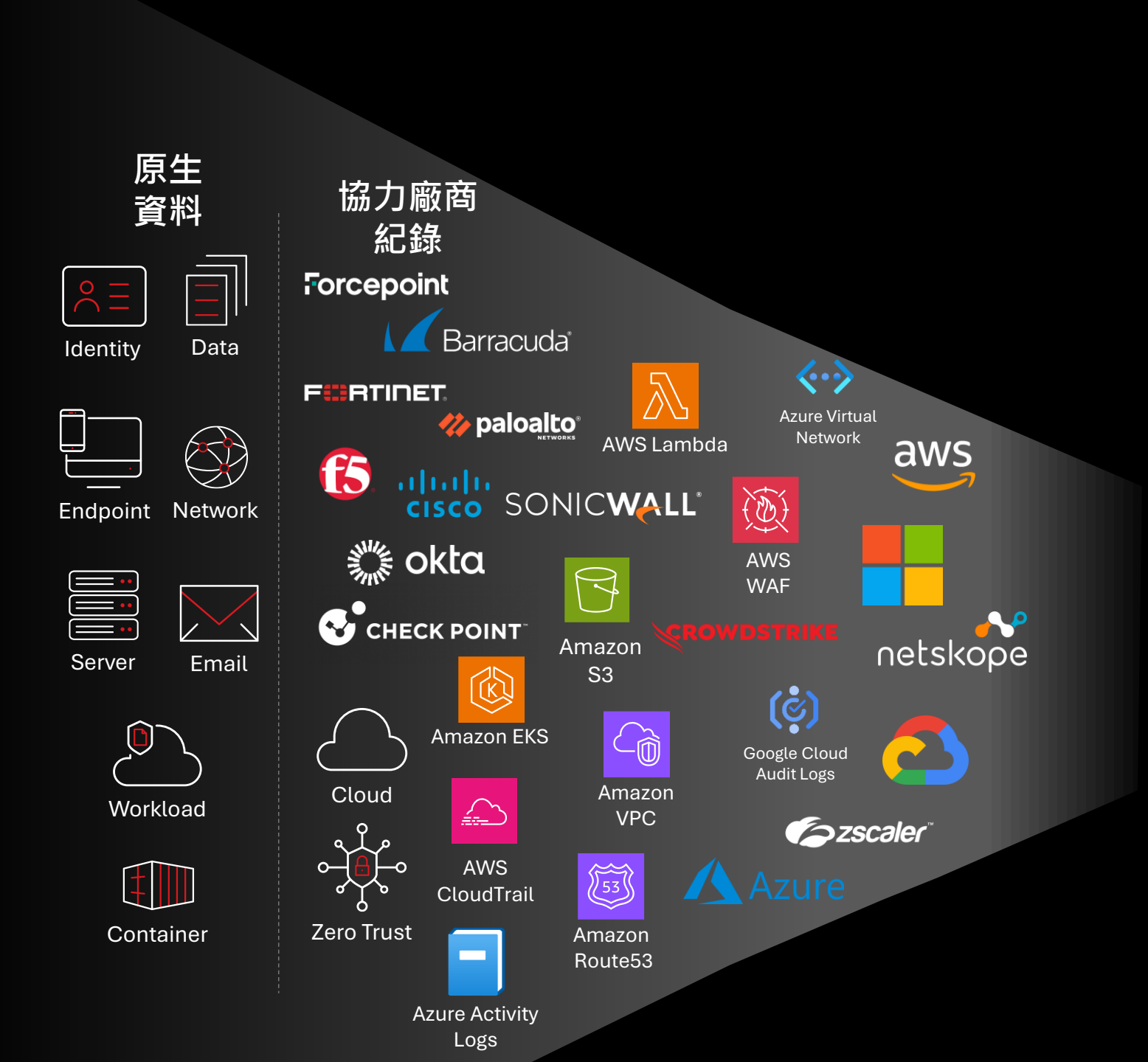
AI 驅動的安全平台，可在威脅出現之前進行預測

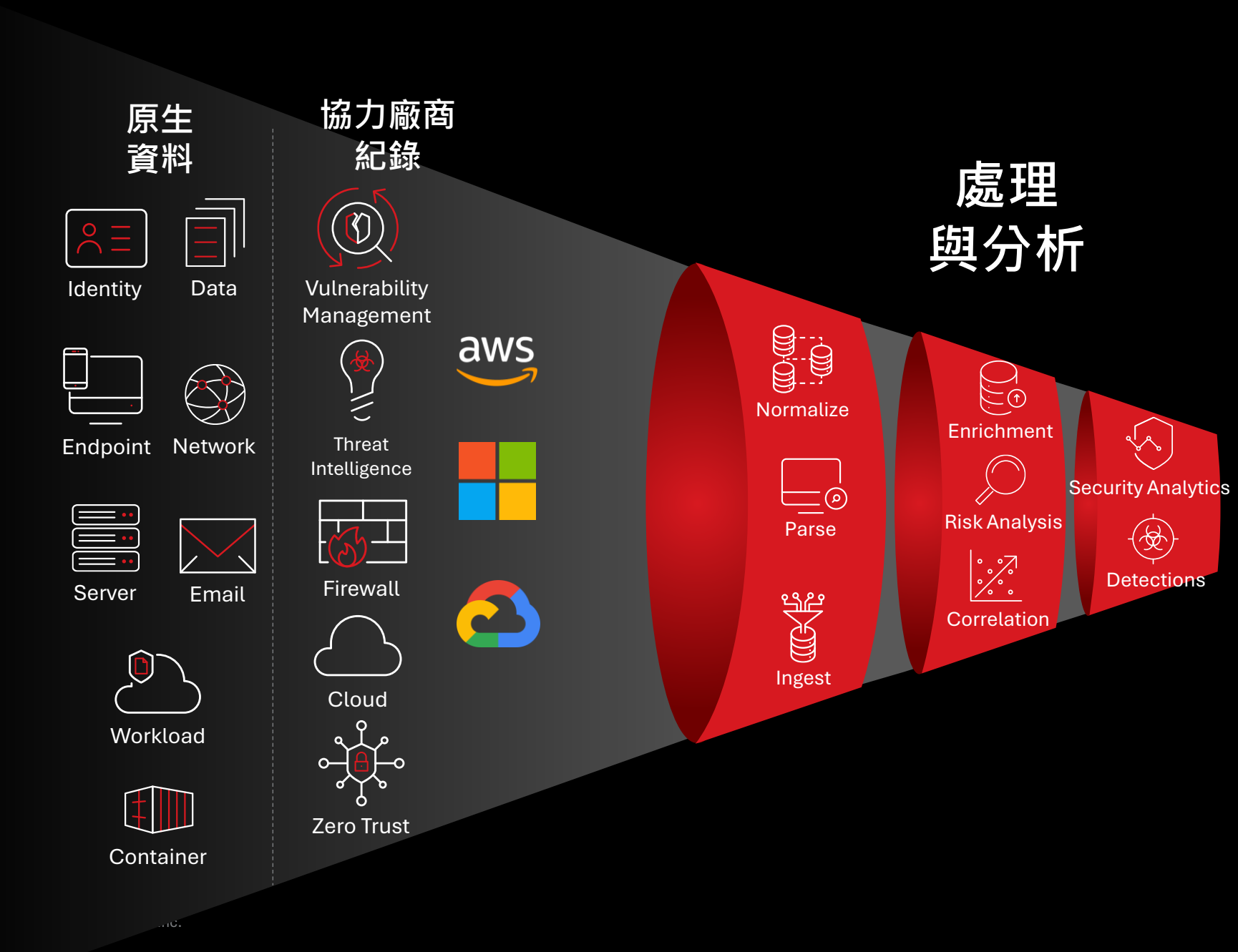
將安全性從防禦者提升為
策略性業務推動者

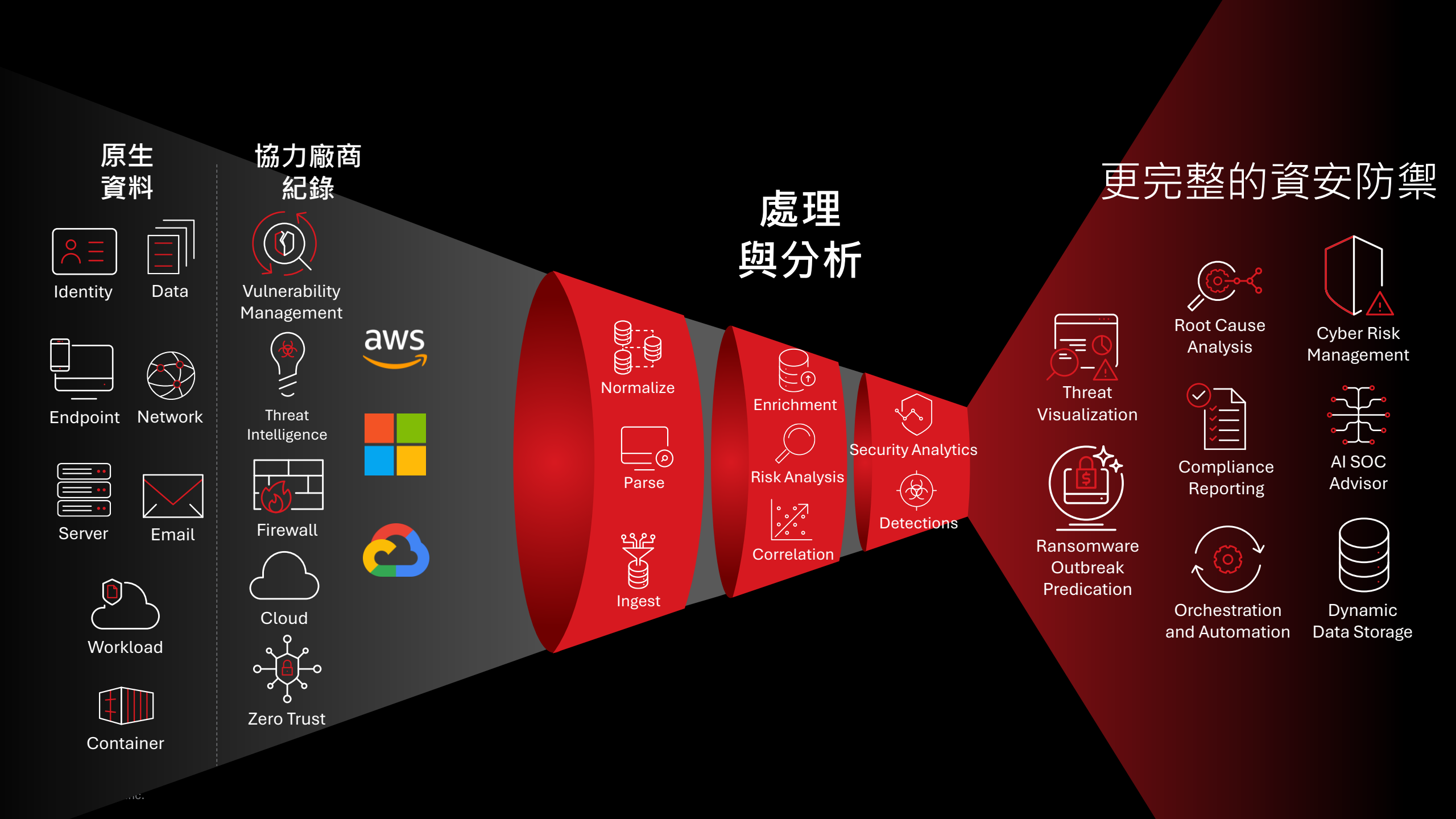
集中式方法:

- 暴險管理
- 安全作業
- 分層保護

+支援現有投資方案整合


原生資料
協力廠商紀錄
Identity
Data
Endpoint
Network
Server
Email
Workload
Container
Forcepoint
Barracuda
FORTINET
paloalto NETWORKS
f5
CISCO
SONICWALL
okta
CHECK POINT
AWS Lambda
Azure Virtual Network
aws
AWS WAF
Amazon S3
CROWDSTRIKE
netskope
Amazon EKS
Cloud
Amazon VPC
Google Cloud Audit Logs
zscaler
AWS CloudTrail
Azure
Zero Trust
Amazon Route53
Azure Activity Logs


原生
資料
協力廠商
紀錄
處理
與分析
Identity
Data
Endpoint
Network
Server
Email
Workload
Container
Vulnerability
Management
Threat
Intelligence
Firewall
Cloud
Zero Trust
aws
Normalize
Parse
Ingest
Enrichment
Risk Analysis
Correlation
Security Analytics
Detections


原生資料
Identity
Data
Endpoint
Network
Server
Email
Workload
Container
協力廠商紀錄
Vulnerability Management
Threat Intelligence
Firewall
Cloud
Zero Trust
aws
處理與分析
Normalize
Parse
Ingest
Enrichment
Risk Analysis
Correlation
Security Analytics
Detections
更完整的資安防禦
Threat Visualization
Ransomware Outbreak Predication
Root Cause Analysis
Compliance Reporting
Orchestration and Automation
Cyber Risk Management
AI SOC Advisor
Dynamic Data Storage

結語

- 資安事件不是會不會發生的問題。
- 技術升級 + 整體資安策略升級。
- 主動管理風險、守護校園的教學與運作安全。