AI驅動防護:
建構零信任自適應安全架構

2023 JLead Customer Day

Danny Yang, Cyber Security Evangelist

Check Point Software Technologies, Ltd.

YOU DESERVE THE BEST SECURITY

過去數年間威脅趨勢仍持續增長，重大危害遽增

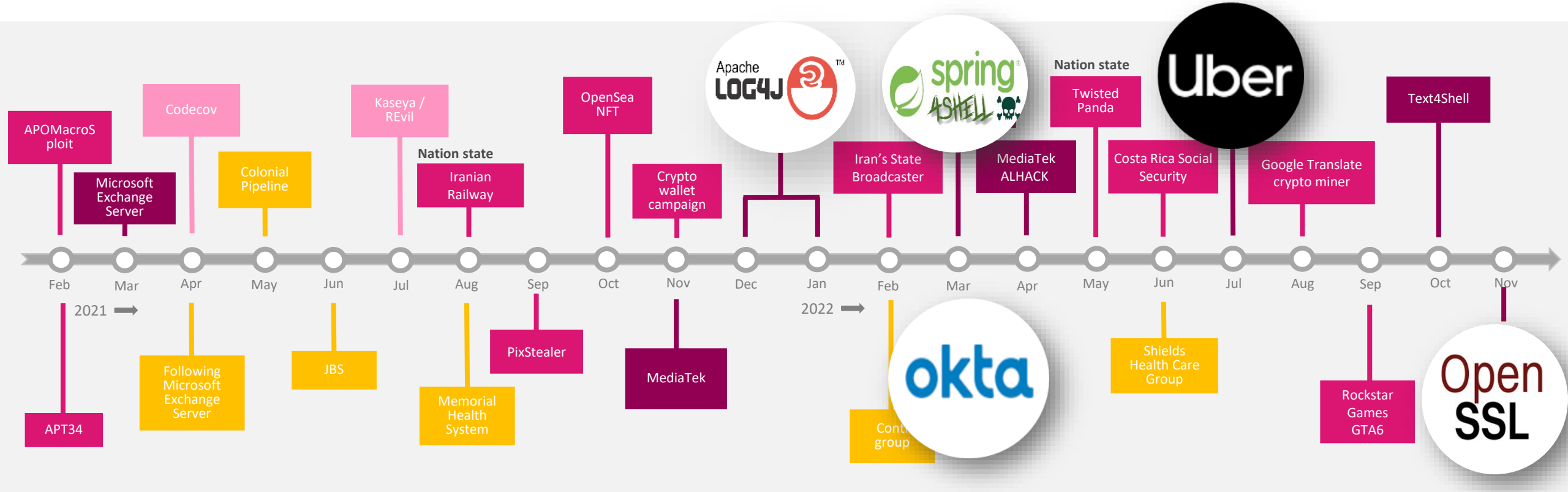
Check Point Infinity

每月

百萬個攻擊

400K 為零時差*

- APT
- 供應鏈
- 勒索軟體
- 軟體漏洞



重大系統漏洞數量與日俱增，風險越來越高

資安因全球區域衝突與新興應用蓬勃而更為嚴峻

Check Point Infinity

38%
增加

全球組織平均每週
遭受攻擊次數(YoY)

60.9%
高風險

臺灣於全球排名前五
風險等級偏高

Gen V
攻擊

區域政治衝突
與國家級別攻擊

企業資安團隊
應更著重於防護與韌性

- 減少誤報與過多告警，聚焦重要安全事件
- 勿成為資安孤島與加速反應時間
- 快速透視駭侵根因並增加高可視能力
- 降低教育訓練不足與人才缺乏的衝擊

https://go.checkpoint.com/2023-cyber-security-report/

生成式AI- 對資安產業憂喜參半的創新科技應用

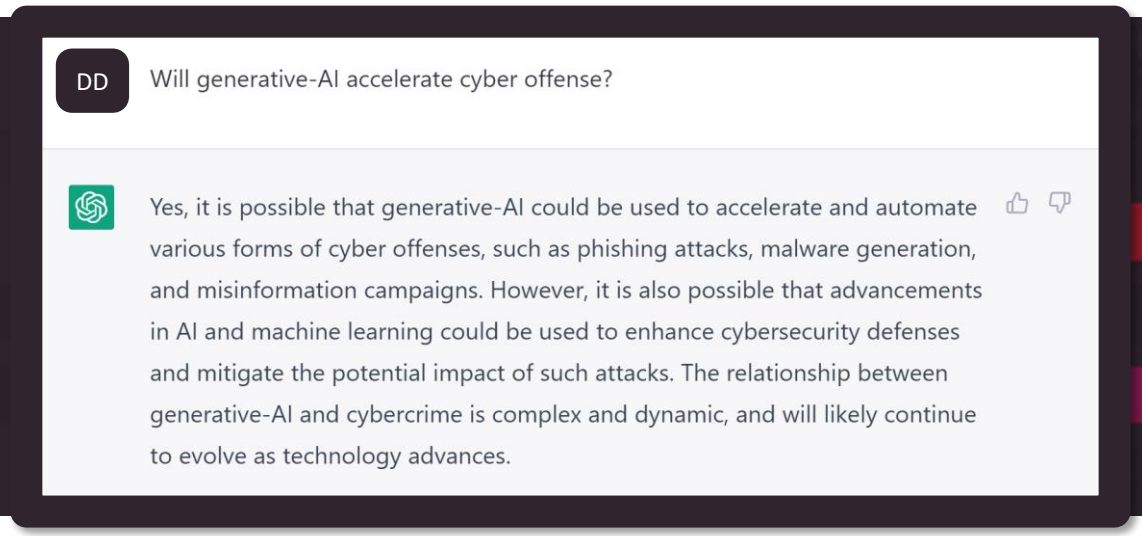
Check Point Infinity

啟發更多創新網路防禦技術機會

- 更快速的系統開發整合
- 提升人員管理維運能力
- 增進事件分析準確度與回應效率

對日益增加的網路攻擊活動帶來隱憂

- 加速惡意程式變種與新型釣魚的生成
- 更巨量的偽冒身分資訊與內容
- 有效模擬測試攻擊以增加成功率



正處於歷史發展的轉折點!

運用AI攻擊，將使供應鏈攻擊危害風險倍增

供應鏈安全將成為產業共通面臨的重要議題

3CX

Mar'23

- **240,000組**
  VoIP電話系統遭駭

LOG4J

Dec'21 – Jan'22

- **超過 46%** 惡意攻擊嘗試來自已知團體
- 試圖滲透全球超過 36.8% 的企業網路

solarwinds

Mar'20 – Dec'20

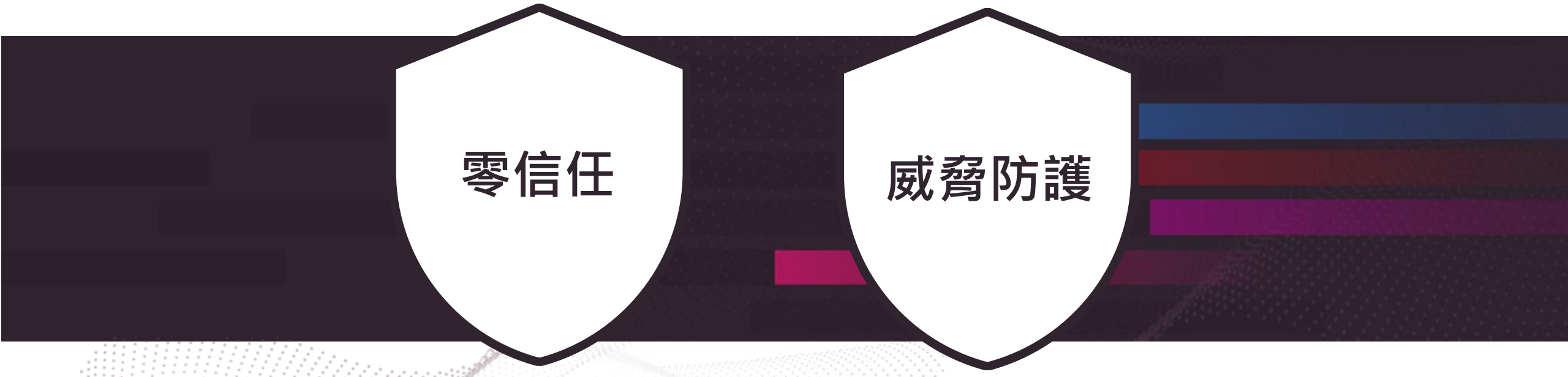
- 影響 **18,000 企業客戶**

系統強固設計與安全防護整合至開發流程將是關鍵因子

AI應用如何強化資安防護?

全球最先進的資安3C原則: 企業具體實踐方式

Check Point Infinity



全面性
Comprehensive

整合性
Consolidated

協作性
Collaborative

確保安全策略可被執行，並由AI驅動引擎即時提供防護

重新構思安全防護策略

Check Point Infinity

主動式防護

Prevention First!

在威脅影響前
率先反應與阻擋

即時監控與緩解問題

快速調查與動態分析
立即回應與應變措施

持續偵測

於整體資訊資產環境中強化資安與數位韌性

ThreatCloud: Check Point資安防護的核心引擎

Check Point Infinity

AI 高端科技
40 種以上AI引擎與機器學習技術
可識別和阻止前所未見的新威脅

海量資料與威脅情資
自動化運算和威脅活動監測
提取IoC並即時更新防護

99.7%
業界最佳
安全防護效益

準確的防護判定
(惡意/良性)

Telemetry

Telemetry

API

ThreatCloud APIs

Quantum
Secure the Network

CloudGuard
Secure the Cloud

Harmony
Secure Users & Access

Horizon
Unified Management &
Security Operations

應用實例: 即時阻擋零時差威脅

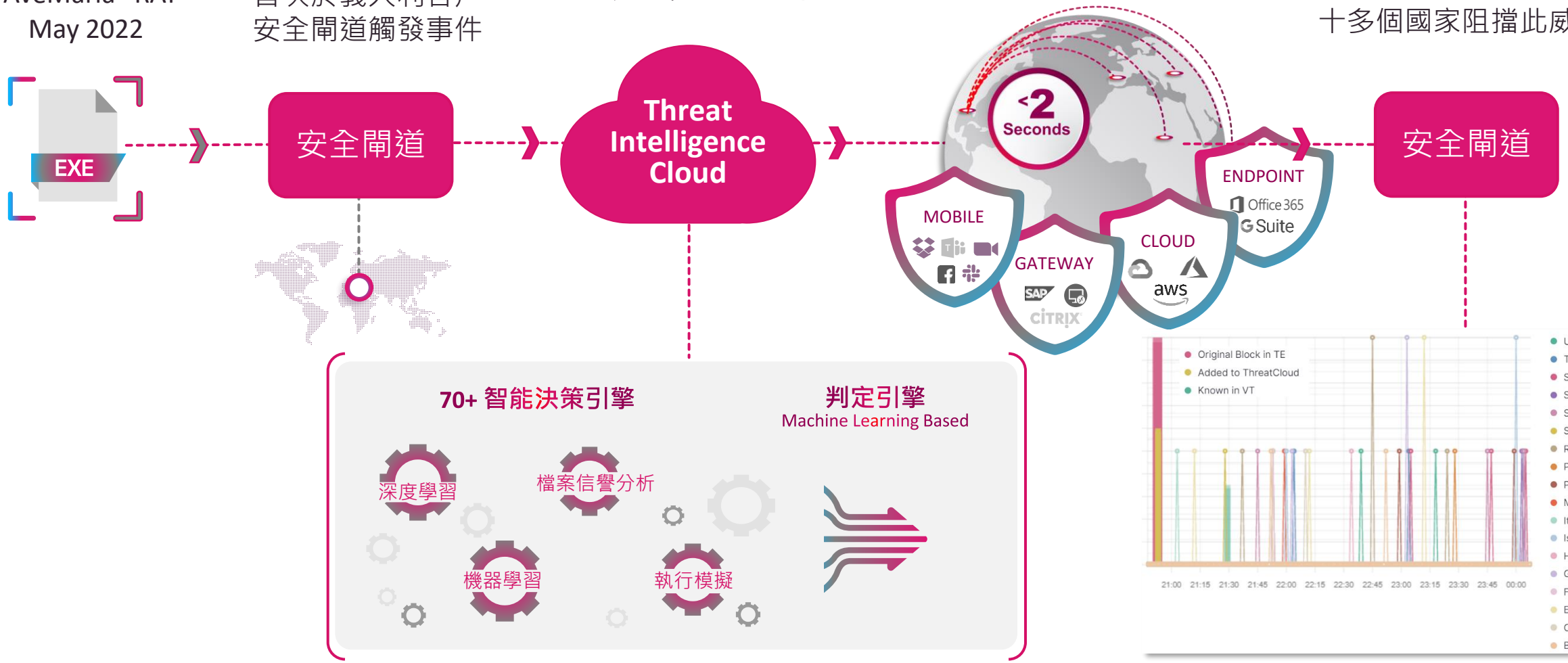
零時差惡意程式
“AveMaria” RAT
May 2022

首次於義大利客戶
安全閘道觸發事件

於數分鐘內模擬威脅

即時同步IoC資訊
於全球威脅防護感知器

於三小時內即於全球
十多個國家阻擋此威脅



Infinity: 落實零信任安全的完整防護架構

Check Point Infinity

1 **最高水平的先進安全科技**

以即時阻擋為最高原則

2 **達成安全管理效益與目標**

單一安全管理與一致性政策標準

3 **統合所有資安部署實施**

橫跨網路、雲端、端點、行動, IoT

零信任安全架構與自動化安全規則

網路隔離與裝置身份識別

Quantum Secure the Network

CloudGuard Secure the Cloud

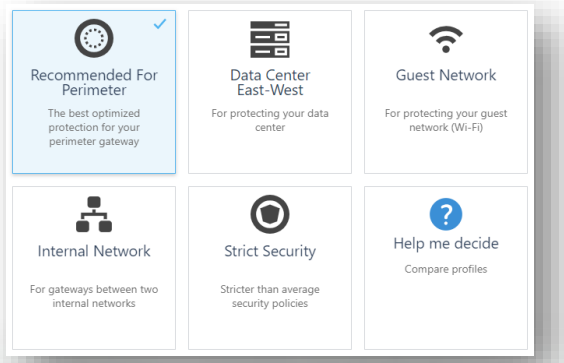
- 透由機器學習與低人為介入處理增加反應效率
- 智能化統合管理與操作，無須複雜繁瑣設定
- 應用最佳安全情資與龐大威脅研究團隊
- 自動化更新並感知態勢以因應可能的變化

CHECK POINT ZERO TRUST

THREATCLOUD

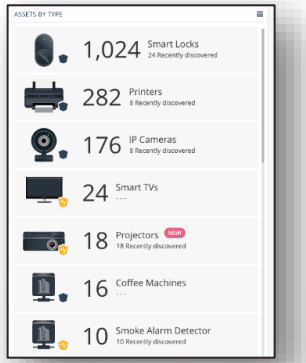
自動化執行威脅防護政策

安全閘道

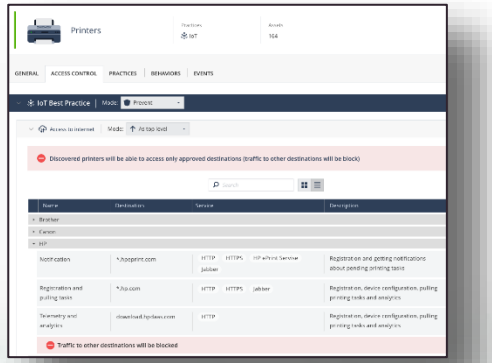


自動生成威脅防護模版

1 裝置識別



2 自動化產生零信任安全政策



依據身份與裝置屬性決定安全存取規則

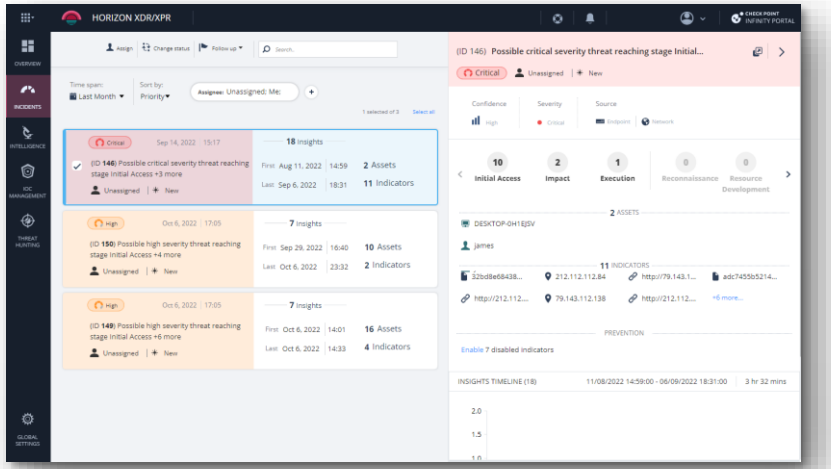
超前部署並預防下一次的攻擊行為

用於事件關聯、威脅獵捕、可視化和自動響應的AI分析

Harmony
Secure Users & Access

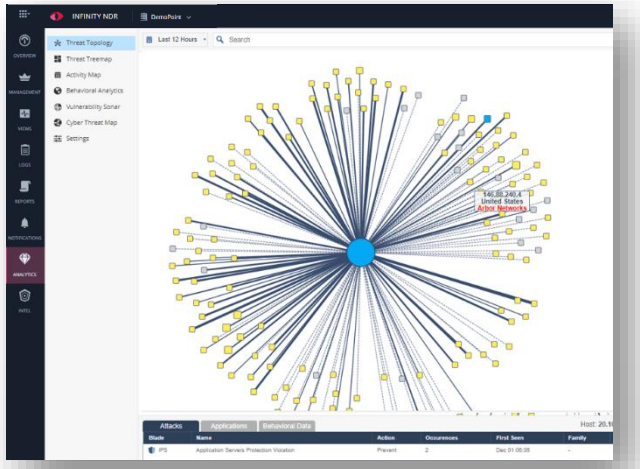
Horizon
Unified Management & Security Operations

事件關聯



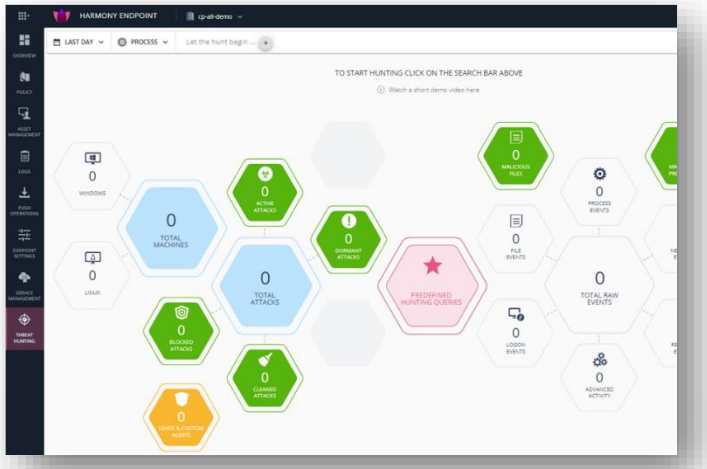
AI/ML提供自動威脅優先排序。 即時於ThreatCloud的情資資料庫中展開調查

攻擊可視化



跨雲和地端網路的使用者行為分析
攻擊可視化介面與威脅拓樸圖

進階威脅獵捕



針對端點惡意活動的獨特獵捕經驗
用於EDR事件調查和處理回應

AI-driven威脅防護阻擋入侵進程，並於各階段感知展開回應

3CX JBS COLONIAL PIPELINE CO. Exchange Kaseya LOG4J

Reconnaissance → Resource Development → Initial Access → Execution → Persistence → Privilege Escalation → Defense Evasion → Credential Access → Discovery → Lateral Movement → Collection → Command and Control → Exfiltration → Impact

入侵破口

- 社交工程
- 供應鏈攻擊
- 軟體與通訊協定漏洞利用
- 雲端不當配置

系統提權

- 零信任與強大的存取控制原則
- 基於對惡意程式、檔案、釣魚的AI防護
- 阻擋 C&C 連線通訊
- 雲端態勢感知管理與工作負載保護
- 硬體/伺服器強固化
- Shift-left 程式源碼與開發流程安全整合
- Native XDR – 橫跨網路、端點、伺服器、雲、行動裝置、郵件、AD, 與更多設備

橫向移動

- 雲端態勢感知管理
- 零信任與微分段安全
- 基於對端點與主機的AI防護
- 分析來自於AD / ADFS / Access token (SAML, OAuth 2.0等)使用者行為與異常存取
- Native XDR

資料外洩

- 雲端態勢感知管理
- 基於對端點與主機的AI防護
- Gateway啟用IPS / Anti-Bot 安全防護
- Native XDR
- DLP (資料外洩防護)
- NDR (網路流量分析)

CHECK POINT ENTERPRISE SECURITY FRAMEWORK

適合中大型企業的全方位資安架構評估與設計規劃

CESF Layer	Assets & Motivation	Process	Owner	When
REVIEW	Identify the business **context** to security. Understand the security **context** to the corporate strategy and transformation goals.	F2F interviews, identify business requirements (BR's) and drivers for security. Business processes modeling. Attribute mapping. Compliance responsibility. Organizational structure.	CISO/CIO, Business Stakeholders & Global Security Architect	Workshop
ARCHITECTURE	Review entire security architecture, controls and attack-surface. Review **security concepts** in use, and planned.	Security design and security controls review. Cyber-risk assessment. Zero Trust review. Risk appetite assessment. Threat analysis.	Technical Stake-holders & Global Security Architect	
DESIGN	Define the **logical** security architecture and the services required to meet business and architectural requirements.	Create logical security architecture aligned with **Zero Trust** methodology. Align security services to attributes,	Check Point Global Security Architect	Post-Workshop
BUILD	Define the **physical** assets that deliver the required security.	Define tangible security assets and functions including their placement in the architecture. Apply Check Point **Infinity** principles.		
IMPLEMENT	Define build **components**. Deploy real-world configured, integrated, operational solutions.	Low-level design templates including specific vendor components. Sizing. Document configuration. Apply Check Point **Infinity** components.	Solutions Architect, Professional Services, Incident Response	
MANAGE	Ongoing management and support.	Account services, life-cycle-management and ongoing support.	Account Manage-ment, IRT, TAC	

零信任
成熟度分析

資安
風險評估

NIST/CIS
架構評估

GDPR
合規遵循

SOC
評估

建議架構

整體安全評估報告

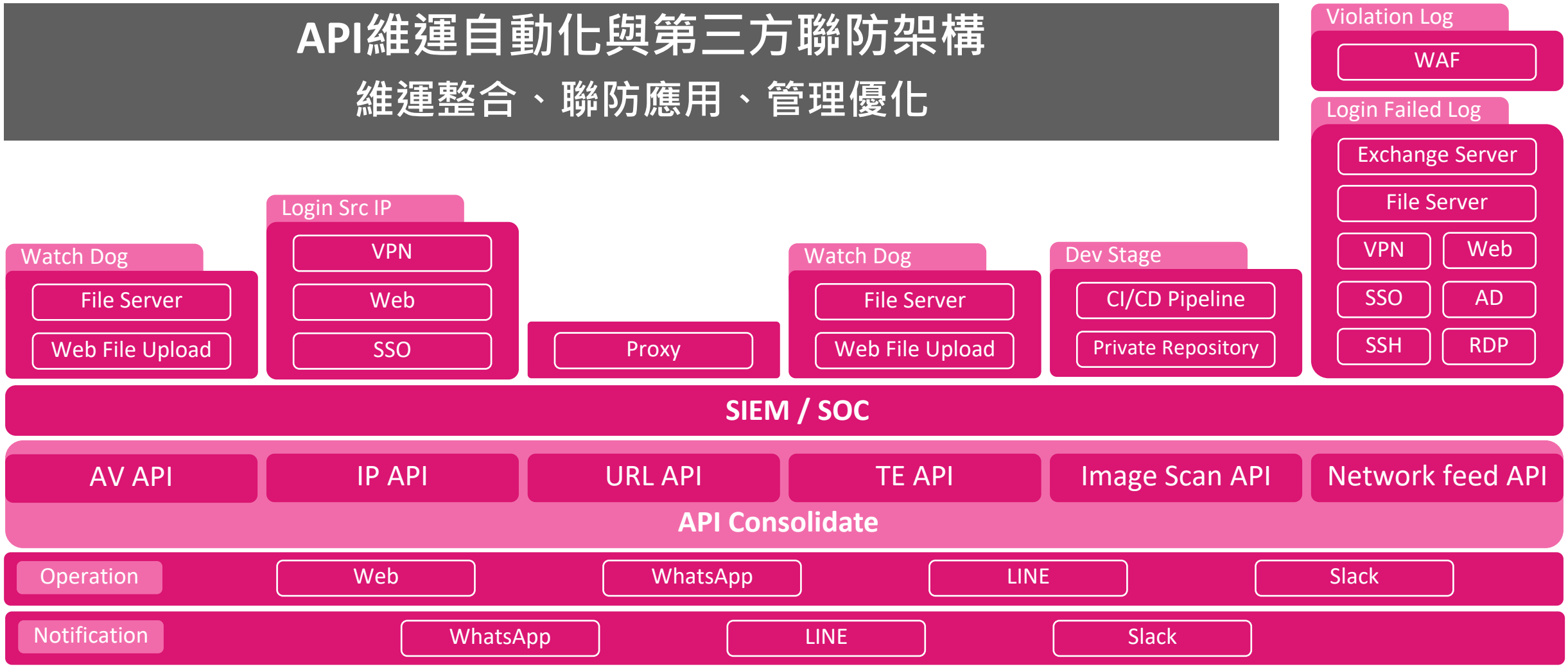
Summary

- **資安實務與實踐建議**
  - Standardized -治理制度化
  - Visibility -管理可視化
  - Consolidated -架構統合化
  - Prevention -防護最佳化
  - Autonomous -回應自動化
  - Awareness -教育系統化

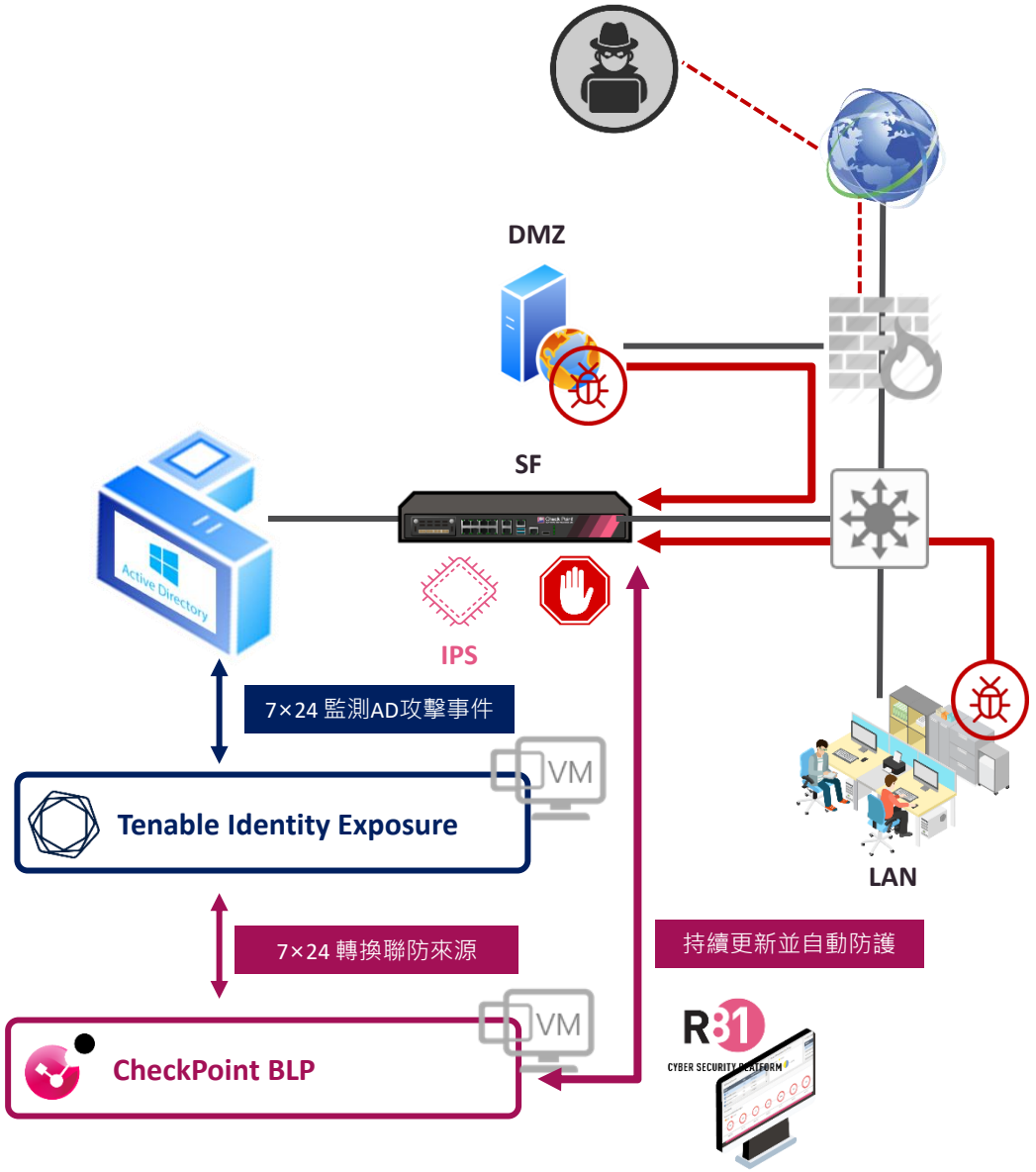
ONE MORE THING…

自動整合聯防，緩解安全威脅加速回應

CP API Middleware Platform



Use case: AD關鍵設施聯防與即時緩解異常



- **Tenable Identity Exposure (.ad)**
  負責監控異常AD登入事件並將Syslog轉拋至CP BLP
- **CP BLP(Block List Parser/Birdlex Log Parser)**
  蒐集由聯防來源(e.g. Tenable)的syslog資訊，並建立事件觸發閥值(例如幾分鐘內發現幾次事件則提取IP至Web list)
- **Check Point Management**
  建立動態物件(Network Feeds Object)與相關存取規則，後續可透過SmartConsole Extension調整CP BLP設定
- **Check Point Gateway**
  負責抓取CP BLP內的Web List (Interval 最低一分鐘), 並透過規則進行阻擋(Deny)，Web List更新可設定阻擋時間(TTL)
- **加值整合應用**
  如通報MDR, 或以IFTTT整合Line通知等

Thank you!

Danny Yang, Cyber Security Evangelist
dannyy@checkpoint.com