kaspersky

構建資安態勢感知平台

資安情資+ APT偵測系統
(Threat Intelligence +
Kaspersky Anti Target Attacks)

卡巴斯基實驗室
黃茂勳
Eden.Huang@kaspersky.com.tw

趨勢和威脅


Smart Cities
Privacy & data protection challenge
Connected cars
Blockchain
Increasing online commerce
Internet of Things
Consumerization & mobility
Cloud & virtualization
Critical infrastructure at risk
Big data
Cryptocurrency boom
Connected health
Industrial threats
Malware for ATMs
IoT botnets
Commercialization of APTs
Merger of cybercrime and APTs
Social-engineering attacks
Hacktivism
Miners & Web-mining
Decreasing cost of APTs
Targeted attacks
Vulnerable connected cars
Ransomware
Supply chain attacks
Massive data leaks
Internet of Things
Data breaches
Healthcare threats
Industrial cyberespionage
"Wipers" & cyber-sabotage
Mobile threats
Financial phishing attacks
Attacks on PoS terminals
Threats to Smart Cities

這些資安事件 不會遠在天邊

TLP: AMBER

KASPERSKY lab

Lazarus attacks against Taiwanese financial institutions

Report Id: 20171006
Version: 1.0 (13.October.2017)

Executive summary

It was recently published[1] a cyber-attack against a Taiwanese bank (FEIB) where attackers managed to transfer $60 million USD. Due to the early discovery of the attack, the bank managed to recover almost all money, except for $500000 USD.

A quick analysis on the malicious files used by the attackers revealed another potentially compromised bank, also locat
discovered in FEI

The TTPs of this campaigns again targeted several

TLP: AMBER

KASPE

ATMProxy: A new way to rob ATMs

Version: 1.0 (18.07.2017)

Executive summary

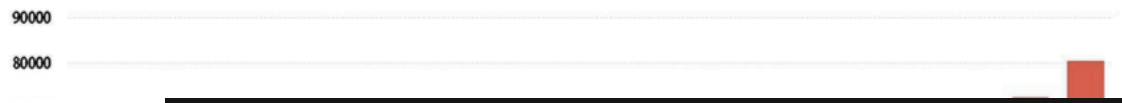
In June 2016, while doing an incident response in a financial organisation we found an interesting, previously unknown Automated Teller Machine (ATM) infection. The malware samples discovered on this organization's ATMs are very specific and were used only in this attack. We've decided to call it ATMProxy due to the unique technique used by this malware.

The way this new attack works is as following: the malware module running on the ATM is proxy-ing all the traffic between ATM and the server in bank's network. ATMProxy's operation interacts with cash withdrawal: the malware is looking for a special card with hardcoded number (4693 9573 0503 9922). If such card has been inserted in infected ATM, then the malware changes cassette number to dispense cash from the last cassette with the most valuable notes.

卡巴斯基率先發現 xDedic 黑市販賣 7 萬台伺服器

KASPERSKY LAB·2016 年 6 月 15 日

卡巴斯基實驗室 6 月 15 日宣佈率先發現 xDedic 地下黑市——販賣全球超過 7 萬台被感染伺服器許可權，最低售價僅為 6 美元！根據目前掌握的資料顯示，xDedic2014 年開始營業，並在 2015 年中快速增長。到 2016 年 5 月，該黑市共有來自 174 個國家的 70,624 台伺服器在販售，由 416 名不同的經銷商提供。其中，受影響最嚴重的十個國家分別為：巴西、中國、俄羅斯、印度、西班牙、義大利、法國、澳大利亞、南非和馬來西亞。在大中華地區（中國大陸、**臺灣**和香港），已有超過 100 家**知名大型企業和 ISP 的伺服器受到感染並在 xDedic 地下黑市出售，包括政府、營運商、電商、醫院、房地產公司和學校等機構。**



PowerShell scripts..+ Fileless Attack?

用PowerShell將 惡意程式 載入記憶體而非寫入硬碟

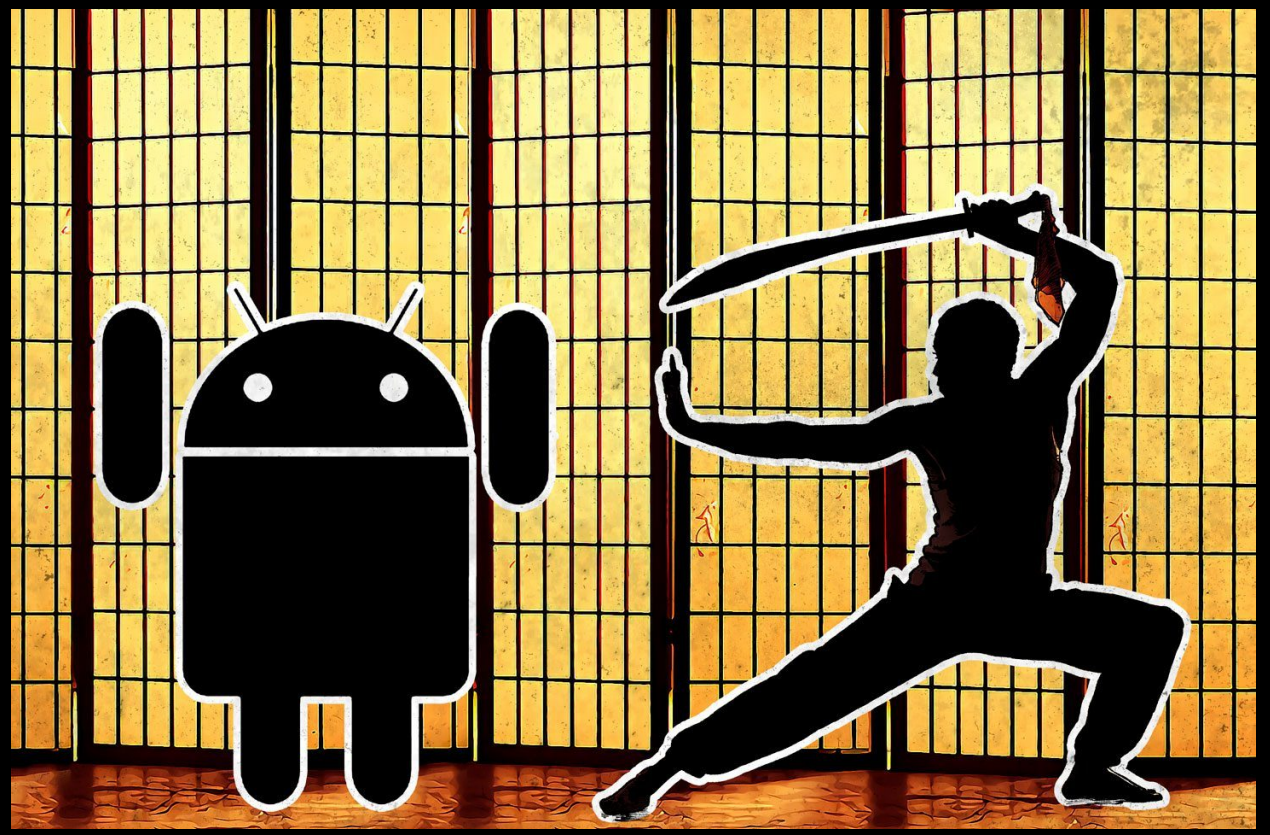
https://www.hackread.com/mirai-botnet-linked-to-dyn-dns-ddos-attacks

更多針對行動裝置

- ~95% 攻擊目標為 Windows 作業系統

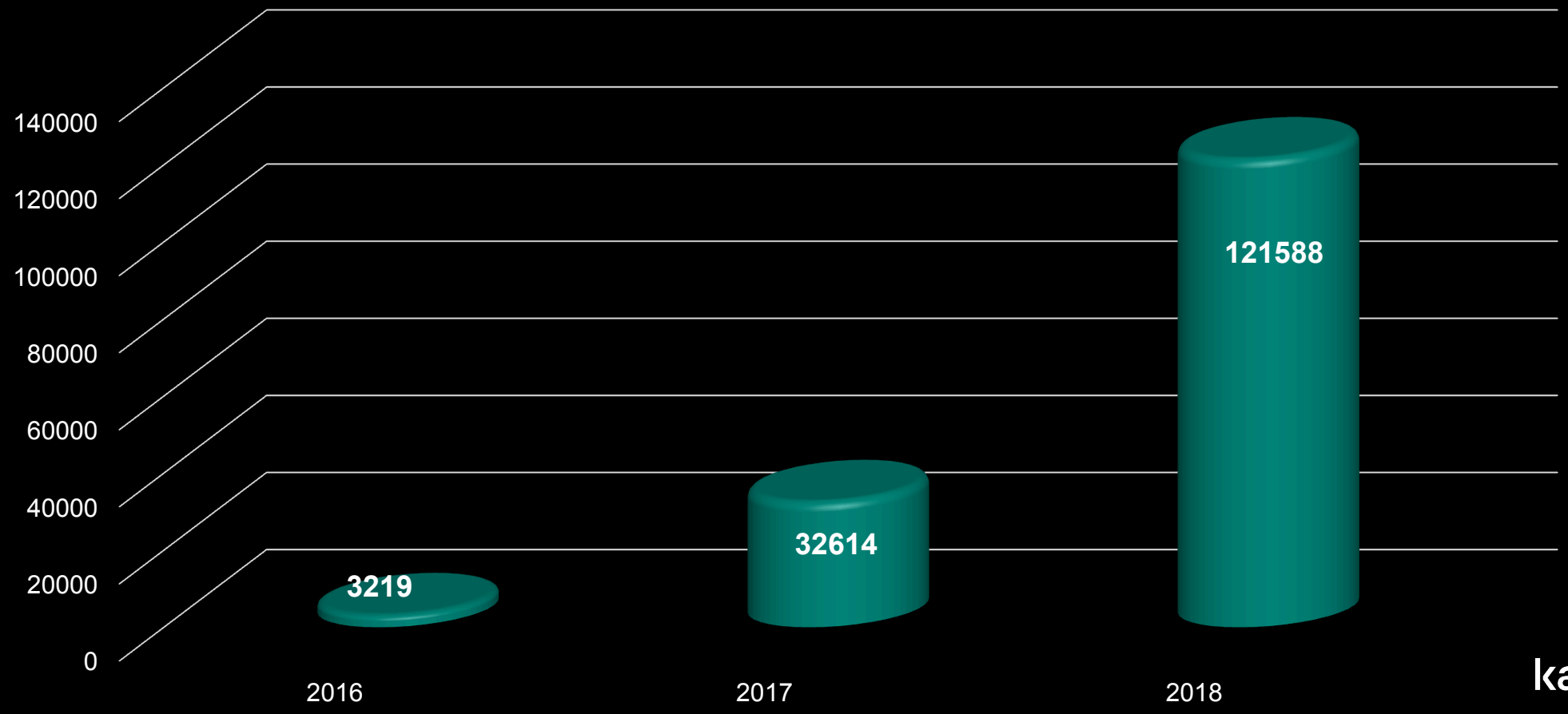
- 其餘非Windows 平台:
- 99% 是針對 Android

- 為什麼?
- 超過 2 000 000 000 Android 設備
- 可能從第三方來源安裝應用程序
- 可能研發進入的安全門檻較低
- 強大又好用的開發工具
- 開源系統及資源
- 熱門的應用程序缺乏安全驗証



kaspersky

IoT裝置的惡意程式樣本統計



kaspersky

新的零日漏洞

- FruityArmor is known to have used zero-days before, while SandCat is a new APT actor that we discovered only recently.
- 針對64位元Windows 8、Windows 10 系統
- 這二個組織使用的漏洞及手法幾乎一樣。應該是使用了相同"第三方"提供的工具。
- 透過反向報到 直接控制用戶端

New zero-day vulnerability CVE-2019-0859 in win32k.sys

By Vasily Berdnikov, Boris Larin, Anton Ivanov on April 15, 2019. 10:00 am

In March 2019, our automatic Exploit Prevention (EP) systems detected an attempt to exploit a vulnerability in the Microsoft Windows operating system. Further analysis of this event led to us discovering a zero-day vulnerability in win32k.sys. It was the fifth consecutive exploited Local Privilege Escalation vulnerability in Windows that we have discovered in recent months using our technologies. The previous ones were:

- Zero-day exploit (CVE-2018-8453) used in targeted attacks
- A new exploit for zero-day vulnerability CVE-2018-8589
- Zero-day in Windows Kernel Transaction Manager (CVE-2018-8611)
- The fourth horseman: CVE-2019-0797 vulnerability

On March 17, 2019 we reported our discovery to Microsoft; the company confirmed the vulnerability and assigned it CVE-2019-0859. Microsoft have just released a patch, part of its update, crediting Kaspersky Lab researchers **Vasiliy Berdnikov** and **Boris Larin**.

Kaspersky Lab products detected this exploit proactively through the following technologies:

1. Behavioral detection engine and Exploit Prevention for endpoint products;
2. Advanced Sandboxing and Anti-Malware engine of the Kaspersky Anti Targeted Attack (KATA) platform.

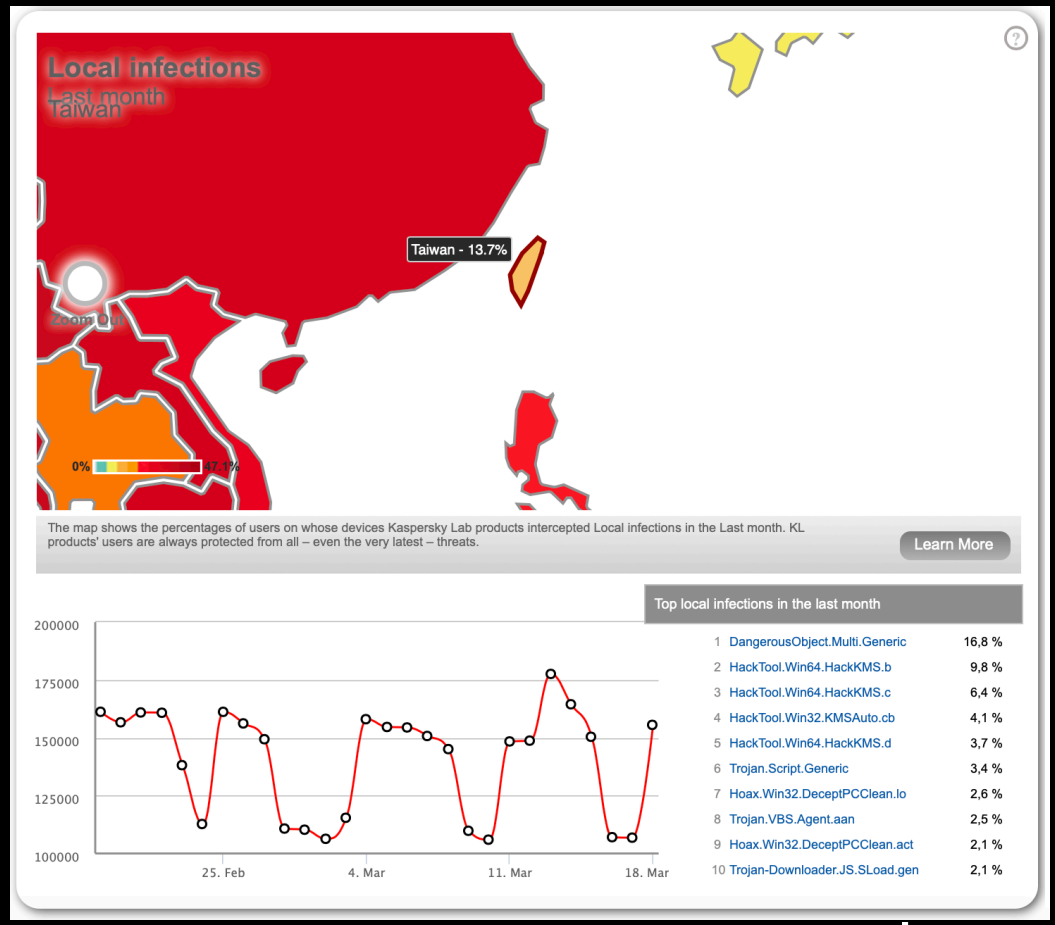
https://securelist.com/elevation-of-privileges-in-namco-driver/83707/ Feb 2018

https://securelist.com/new-win32k-zero-day-cve-2019-0859/90435/ Mar 2019

kaspersky

USB、共用資料夾的傳染途徑

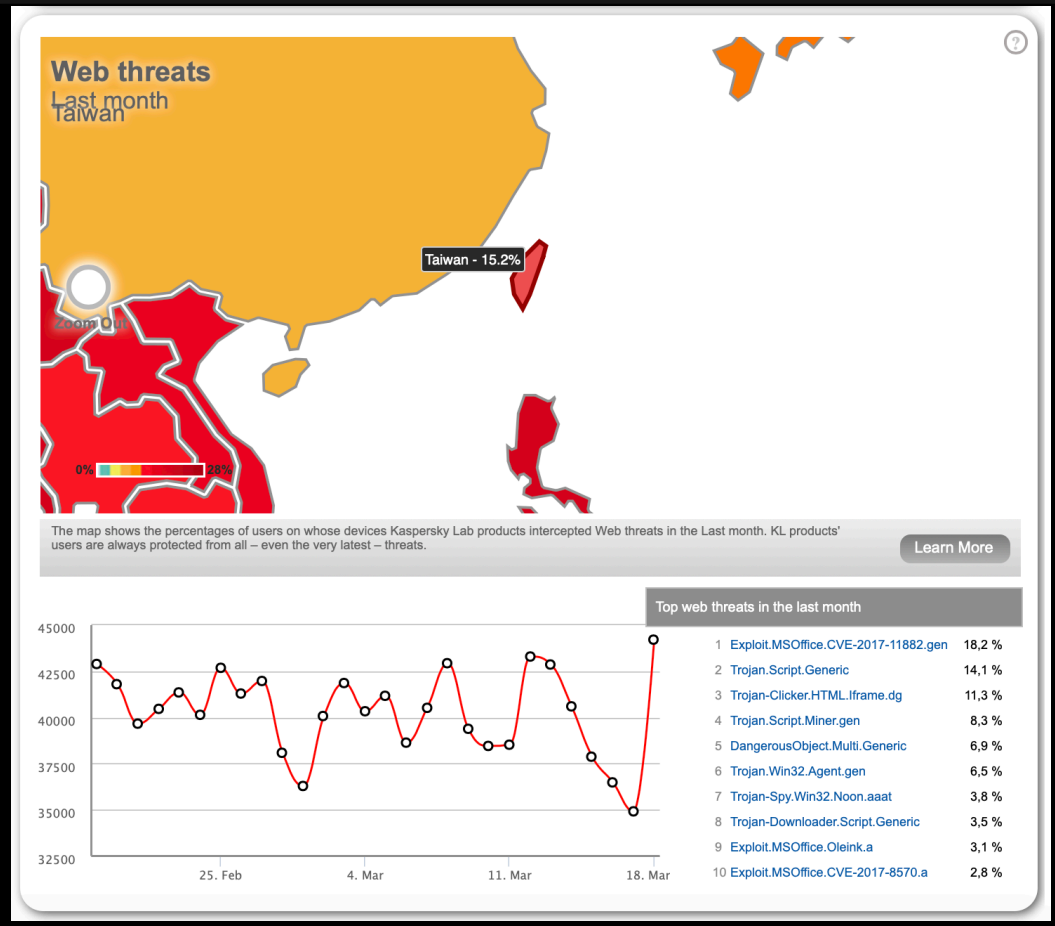
- 13.7% 的惡意程序是透過本機/共用資料夾/USB所感染的



kaspersky

惡意下載連結

- 15.2% 使用者是被透過網頁瀏覽所感染的
- 每七個人就有一個會透過網頁或瀏覽器下載惡意程序



kaspersky

另類的APT

- 因為區域化或政治化的影響，造成安全有國界、威脅無國界。
- 資料外洩已經成為常態。譬如: Facebook, Equifax, Uber, etc…
- APT的活動造成選舉結果的影響
- 宣傳大量的假新聞，成為新的目標/手法之一
- 愈來愈多針對特定目標的"商業化"惡意程式。如政府單位、金融單位…
- 加密勒索程式，有了新的功能。
- 全新的針對式供應鏈APT攻擊。提供了攻擊者新的應用方式。

kaspersky

所有產業都會成為目標

Business in general


竊取金錢


操作業務流程


破壞競爭對手


敲詐勒索


竊取身份資料

電信


攻擊企業用戶


利用郵件伺服器發送社交郵件


利用網頁資源發送釣魚網站


控制電信帳單

醫療


竊取病患資訊


攻擊醫療設備

金融


竊取金錢


竊取身份資料

政府


間諜


資料處理


限制線上服務可用性


竊取身份資料

新的威脅不再是一次性攻擊行為:
是一種持續性程序

滲出

- 保持休眠
- 攜出資
- 清除追蹤
- 安靜離開

準備

- 針對目標研
- 建立策略
- 製作工具

一個APT程序
可以潛服好多年
甚至我們可能從來沒有
發現過

深入存取

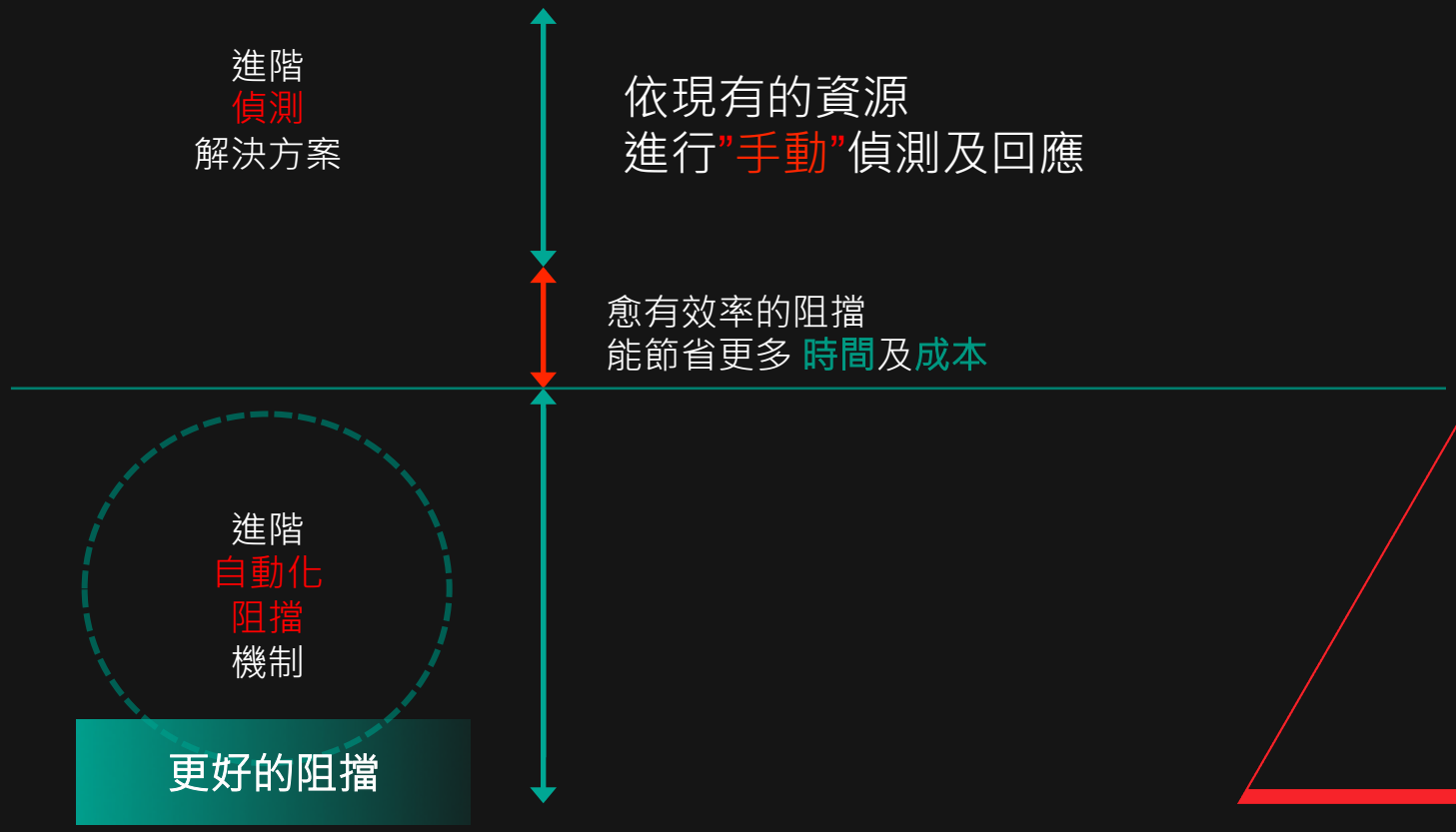
- 找出適合的身份
- 提高權限
- 建立連結
- 向旁擴散
- 取得控制

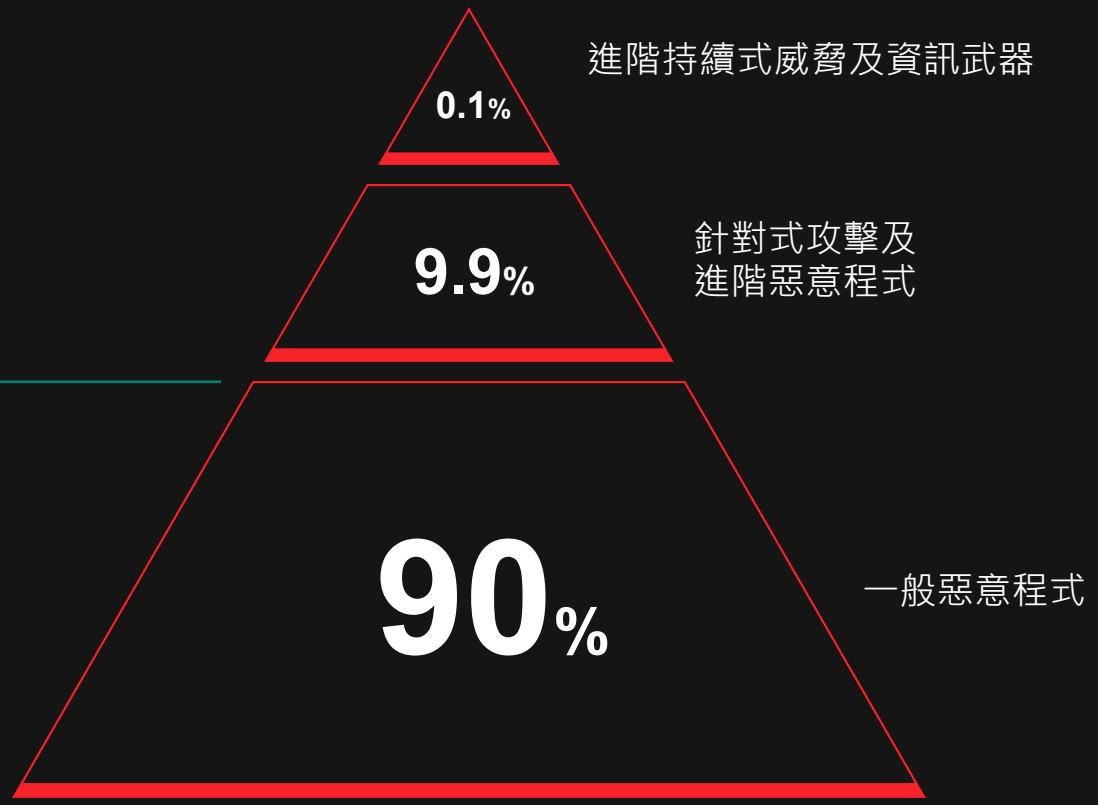
感染

- 利用弱點
- 滲透外層防護

為何只有阻擋是不夠的?

使用較高偵測率的方案

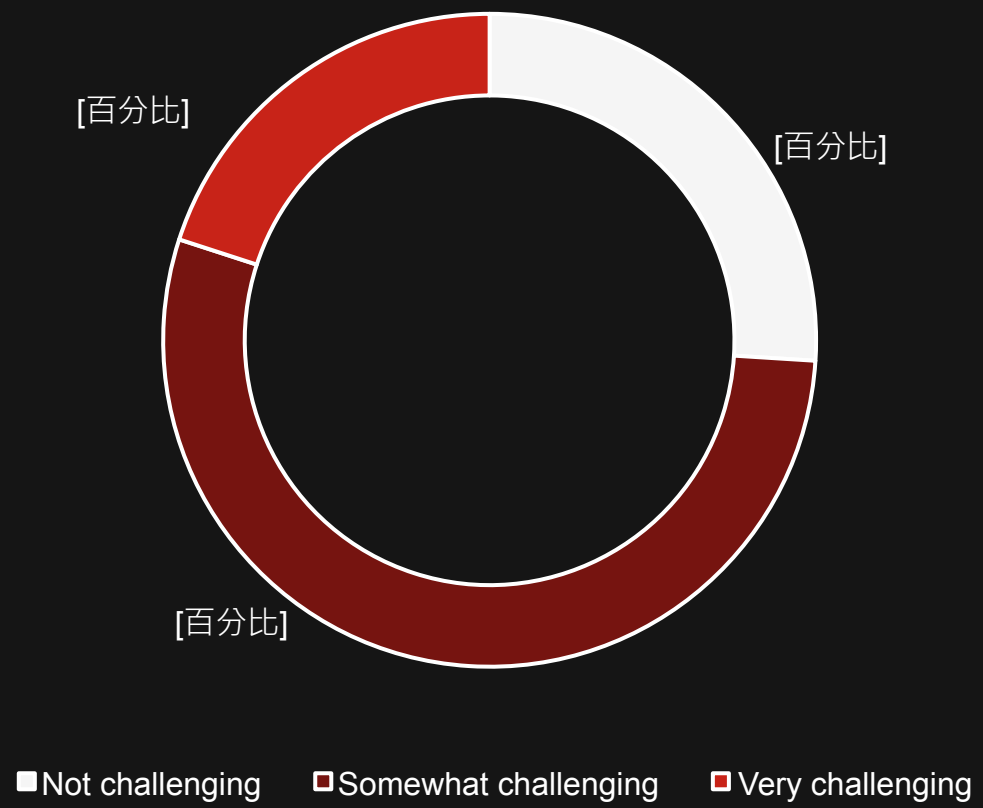




kaspersky

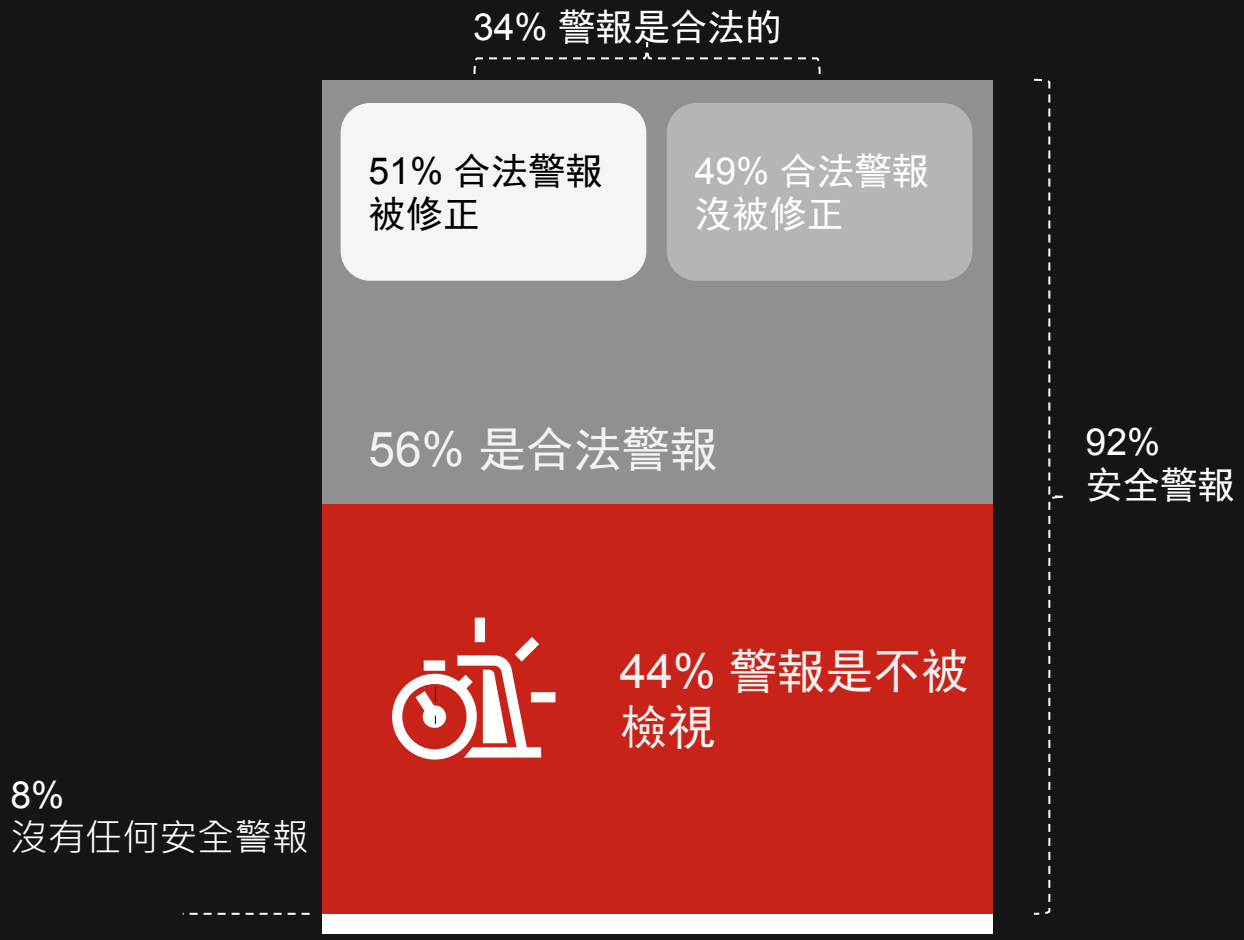
安全警報數量

The challenge of orchestrating alerts

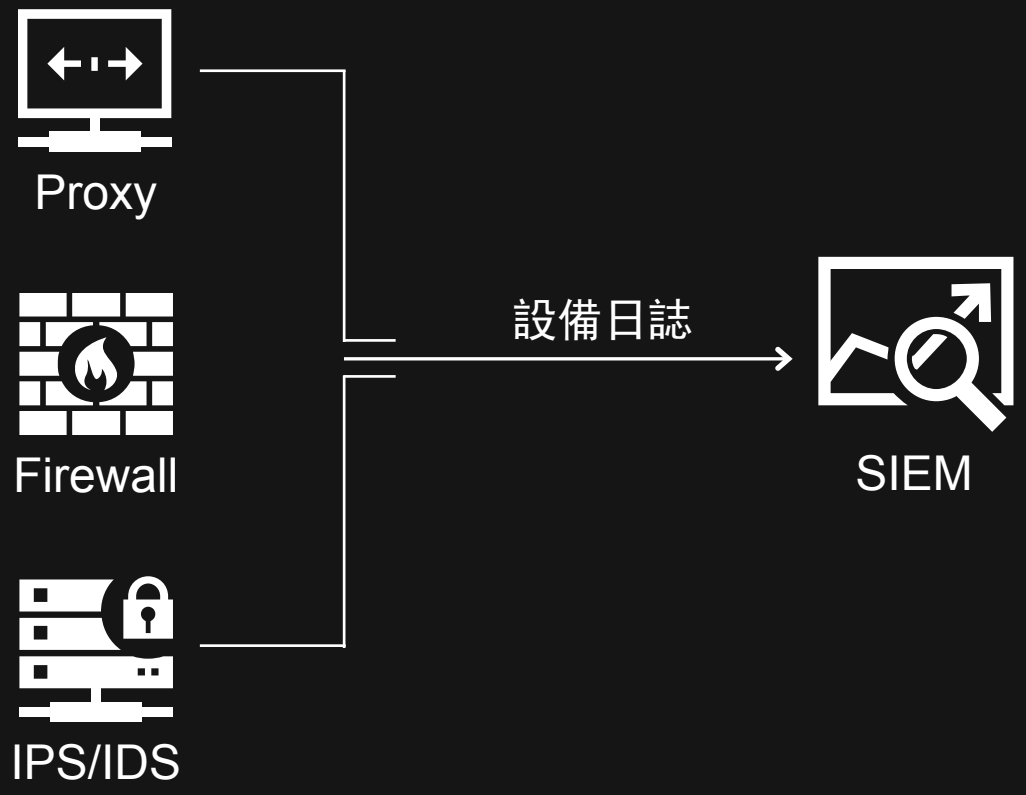


Source: Cisco 2018 Capabilities Benchmark Study

很多威脅警報不會被檢視或修復



不斷發展的網路安全挑戰



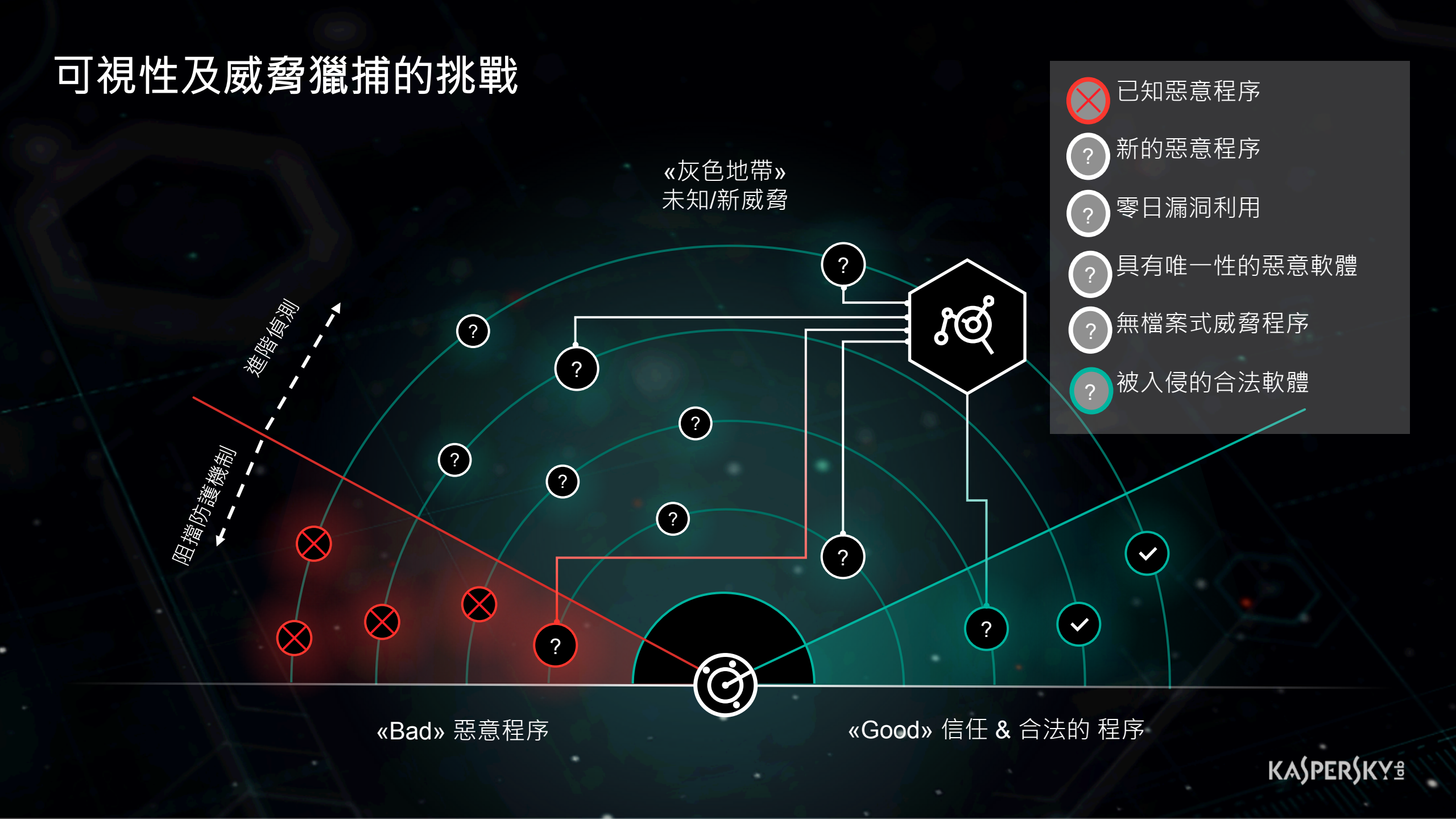
缺乏全面的威脅概述，阻礙了安全計劃規劃

很多安全警報資訊的優先等級不足

潛伏在企業內部的威脅

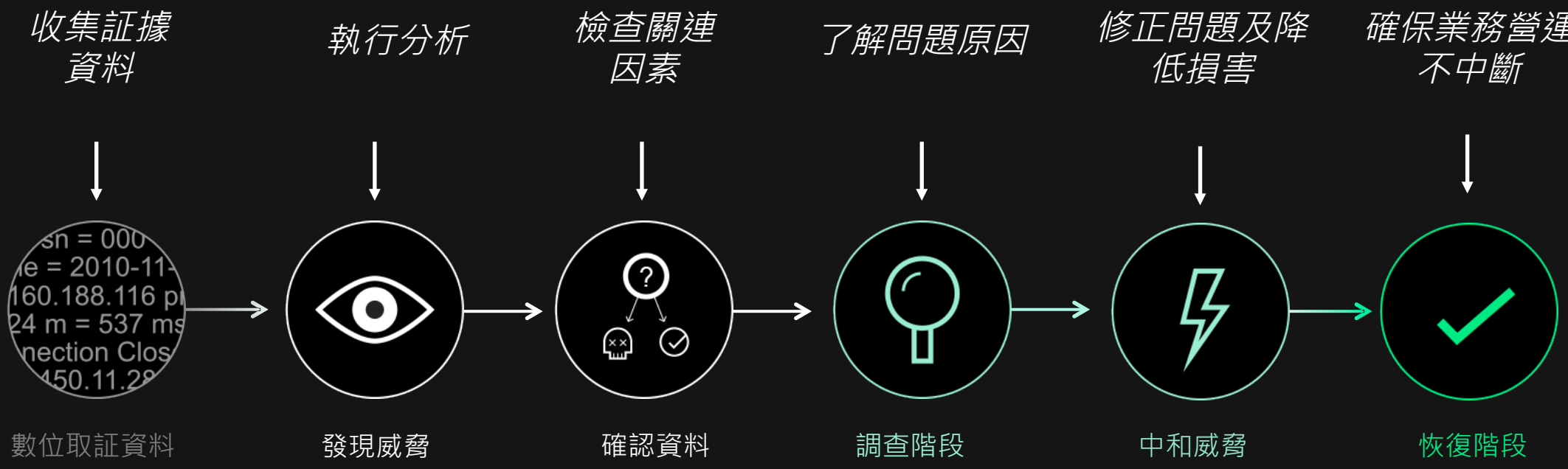
事件回應效率低而導致高恢復成本

可視性及威脅獵捕的挑戰

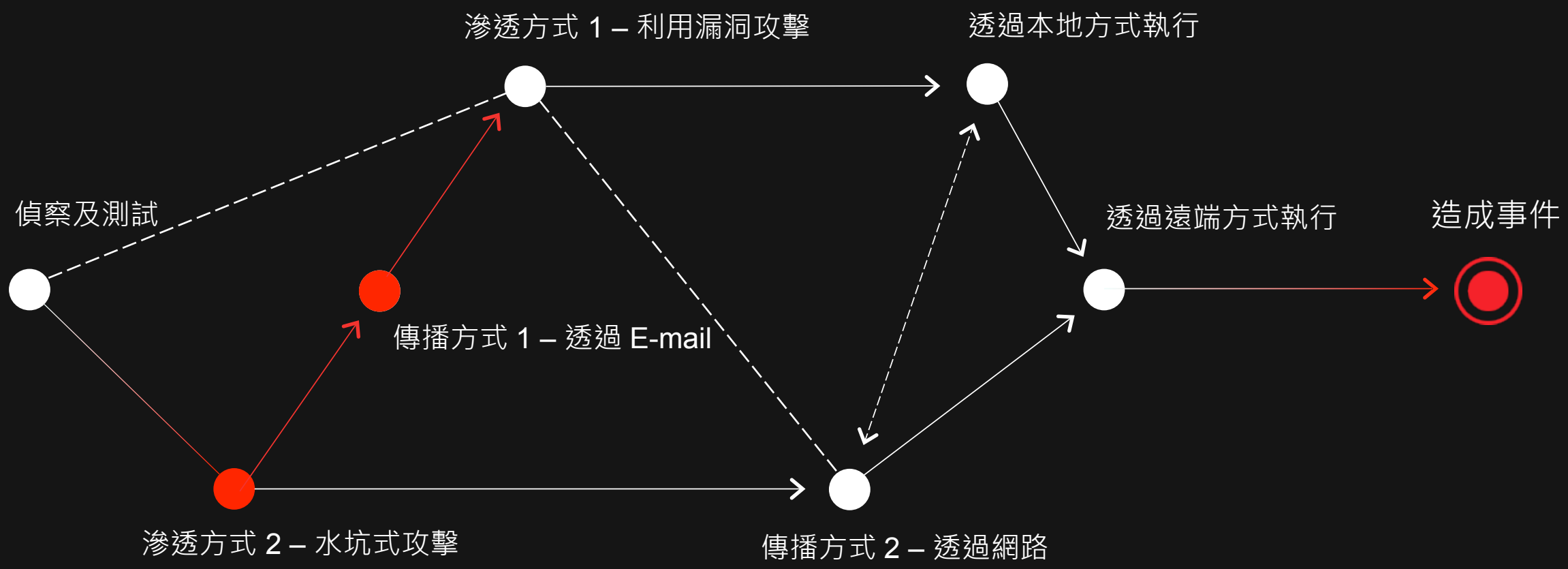


KASPERSKY lab

威脅防護是一套流程及策略



進階威脅分析: 複雜及非線性



...但...! 這些流程對企業安全團隊是巨大的挑戰

手動/ 半自動

缺乏
專業知識

缺少跨部門的
參與

缺乏關聯資訊

缺乏資源
及整合問題

«快速修復»
比研究問題原因
更為重要

*收集証據
資料*

執行分析

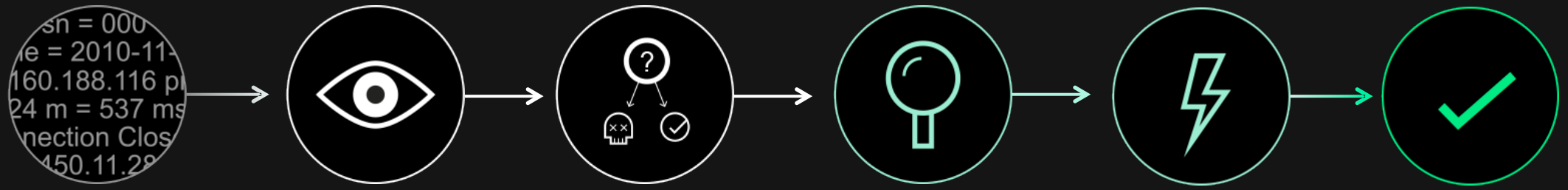
*檢查關連
因素*

了解問題原因

*修正問題及降
低損害*

*確保業務營運
不中斷*

相同事件重複發生



數位取証資料

發現威脅

確認資料

調查階段

中和威脅

恢復階段

- 建置威脅防護平台 與 威脅獵捕 前 先了解

- 真正的 可適性 安全策略??

kaspersky

可適性安全模型

預測 Predict

- 分析潛在性安全威脅的間隙
- 調整可執行的反制機制
- 透過威脅情資強化SOC管理
- 主動進行威脅誘捕

阻擋 Prevent

- 減少風險
- 提昇安全意識
- 落實重要系統資產盤點
- 改善調整現有防護機制對新型態威脅防護的效能

回應 Response

- 事件回應的管理機制建立
- 事件調查機制的流程
- 可立刻執行降低災害持續影響的步驟
- 災害還原的機制

偵測 Detect

- 持續性的監控機制
- 資安事件的發現
- 資安事件威脅及風險等級的定義

可適性企業安全平台

PREDICT

- 滲透測試服務
- 應用程式安全評估
- 針對式攻擊探索服務
- 威脅資料查詢服務
  (Kaspersky Threat Lookup)
- APT portal

PREVENT

- 資訊安全專業訓練
- 各種企業解決方案
  - Endpoint security
  - Datacenter Security
  - Embedded security
  - …
- 資訊安全意識教育訓練
- 工控資訊安全訓練

RESPOND

- 安全回應服務(MSA)
- 專家窗口回應服務(SAM)
- 事件回應服務
- 數位鑑識
- 惡意程式分析
- Endpoint Detection & **Response**

DETECT

- APT & 客制化報告
- Threat data feeds
- Kaspersky Managed Protection
- Kaspersky Anti Targeted Attack (KATA) platform
- Endpoint **Detection** & Response

如何打造企業的資訊安全架構

可適性安全策略的導入
從簡單化的導入方案

傳統的安全機制/
阻擋為主的技術

進階的偵測技術及
回應的機制

整合智能情報及
主動式威脅獵捕

含蓋大部份的威脅範圍

進階式威脅

針對特定對像所建立的威脅

步驟一

阻擋愈多可能的威脅
愈好

自動化威脅阻擋

步驟二

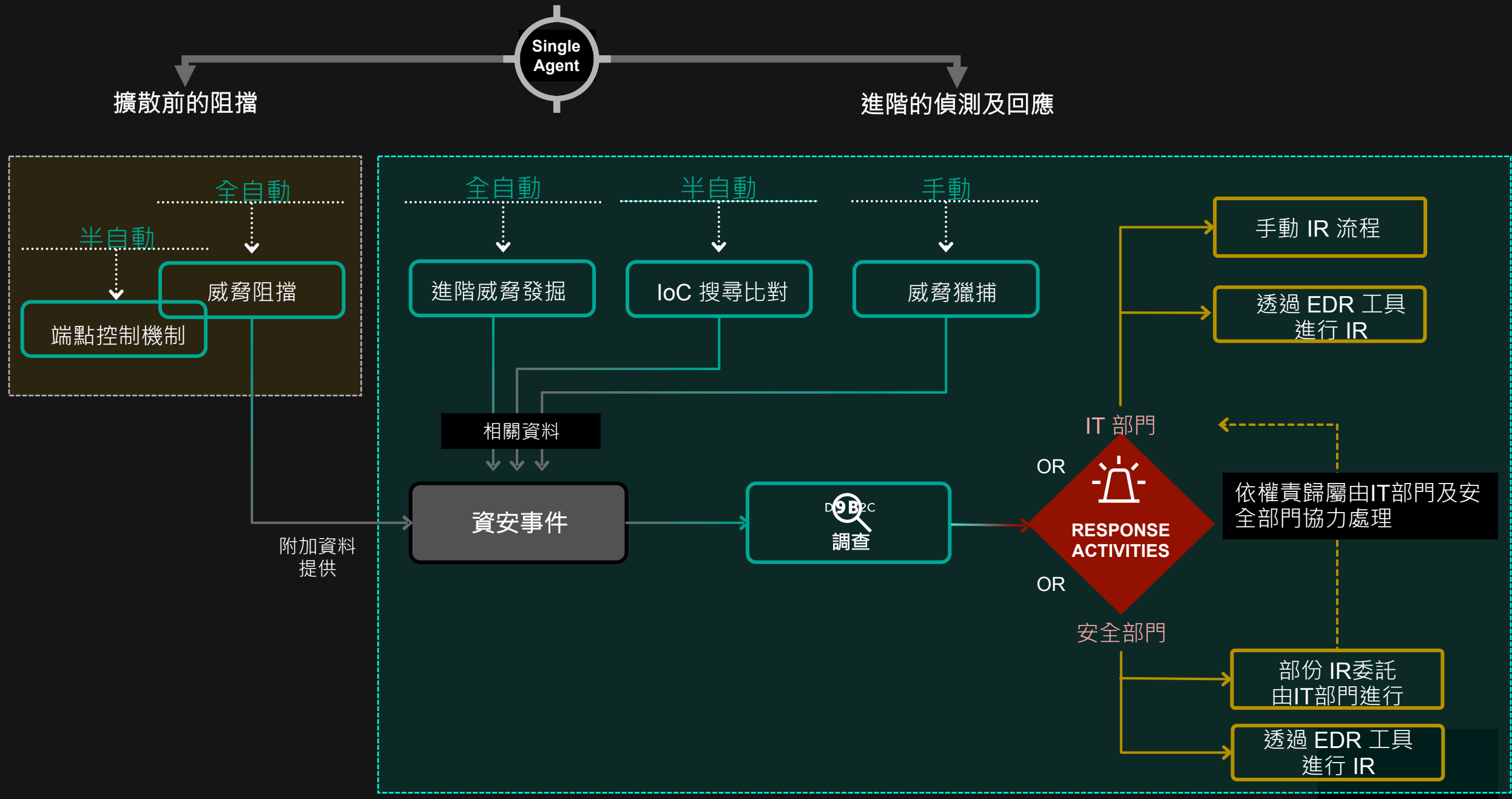
如何偵測及快速回應
無法自動阻擋的進階式
威脅

自動化威脅發現、調查
及回應

步驟三

準備好面對APT級別
的威脅攻擊。
需要透過高水平的專
業知識、先進的威脅
情報及人工威脅獵捕

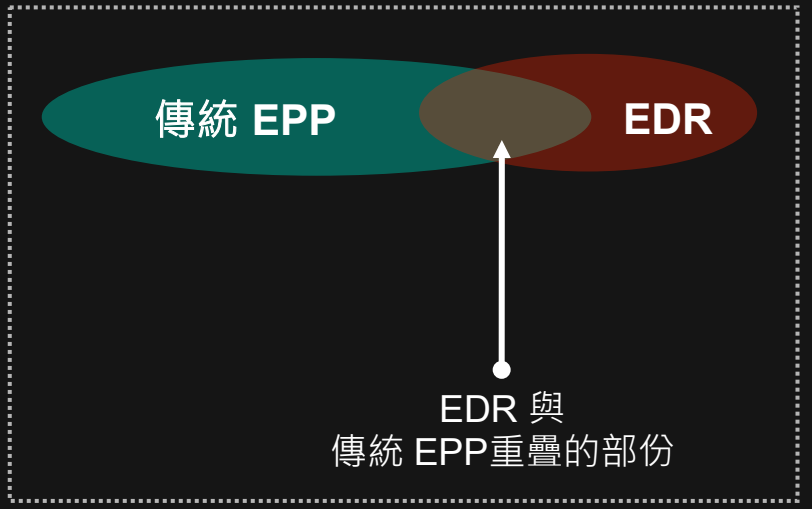
端點防護概念分享

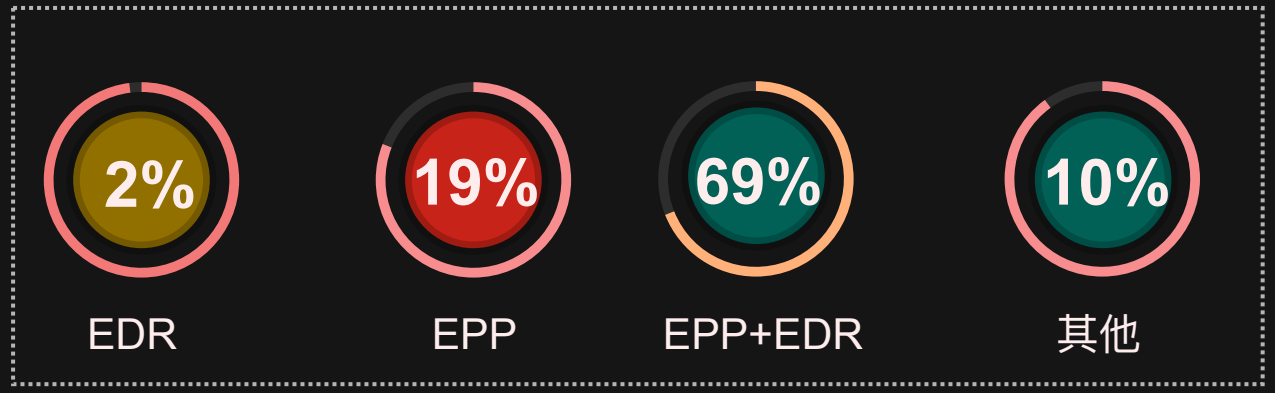

Single Agent
擴散前的阻擋
進階的偵測及回應
全自動
半自動
威脅阻擋
端點控制機制
附加資料提供
全自動
半自動
手動
進階威脅發掘
IoC 搜尋比對
威脅獵捕
相關資料
資安事件
調查
IT 部門
OR
RESPONSE ACTIVITIES
OR
安全部門
手動 IR 流程
透過 EDR 工具進行 IR
依權責歸屬由IT部門及安全部門協力處理
部份 IR委託由IT部門進行
透過 EDR 工具進行 IR

關於進階端點防護機制 (EPP+EDR)

“Antivirus 已死" NOT TRUE!

EDR 替換 EPP NOT TRUE!





2019 年企業準備導入的端點防護機制

Source: Enterprise Strategy Group, Gartner

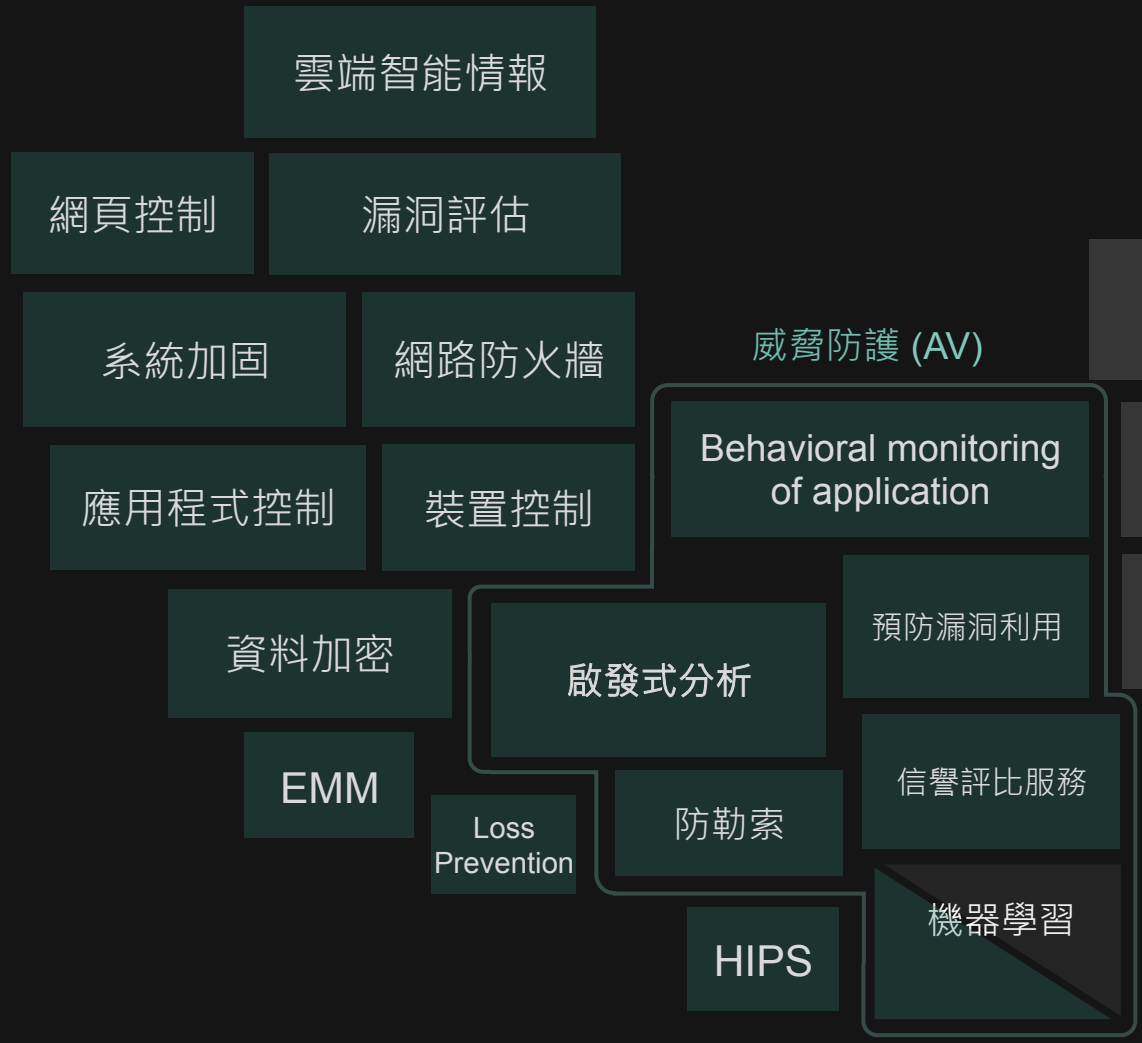
kaspersky

EDR: 完整的結合事件調查回應工作流程

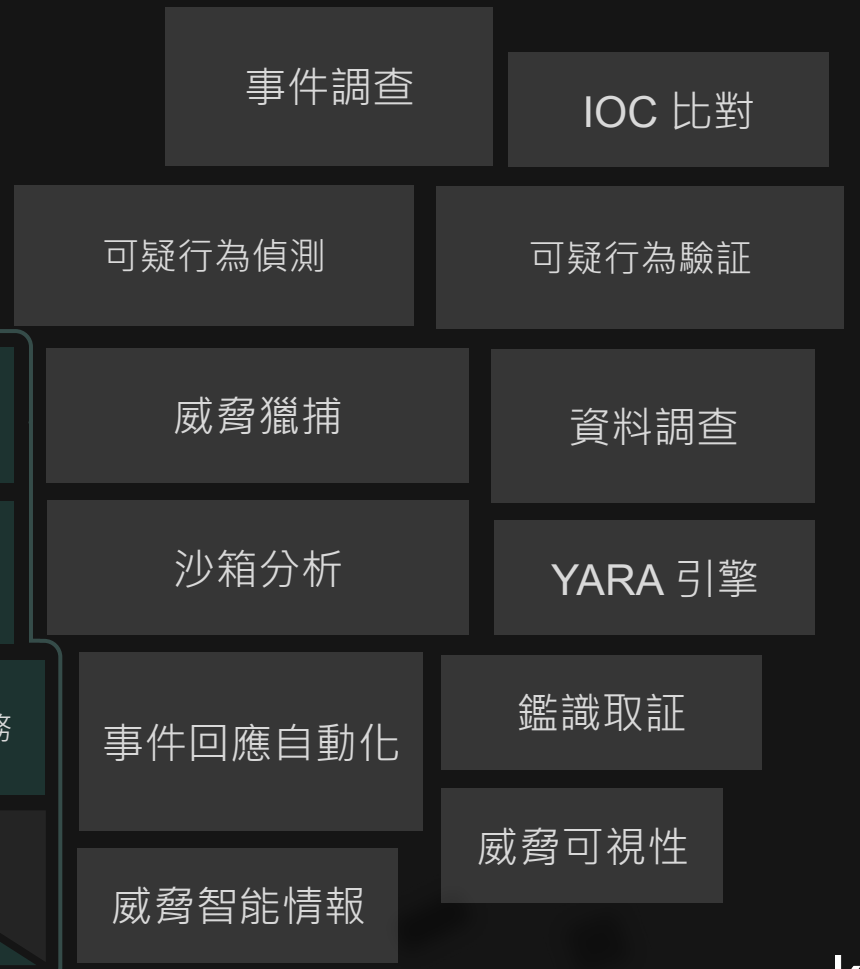
KASPERSKY lab

Kaspersky Integrated Endpoint Protection Solution

Kaspersky Endpoint Security



Kaspersky EDR

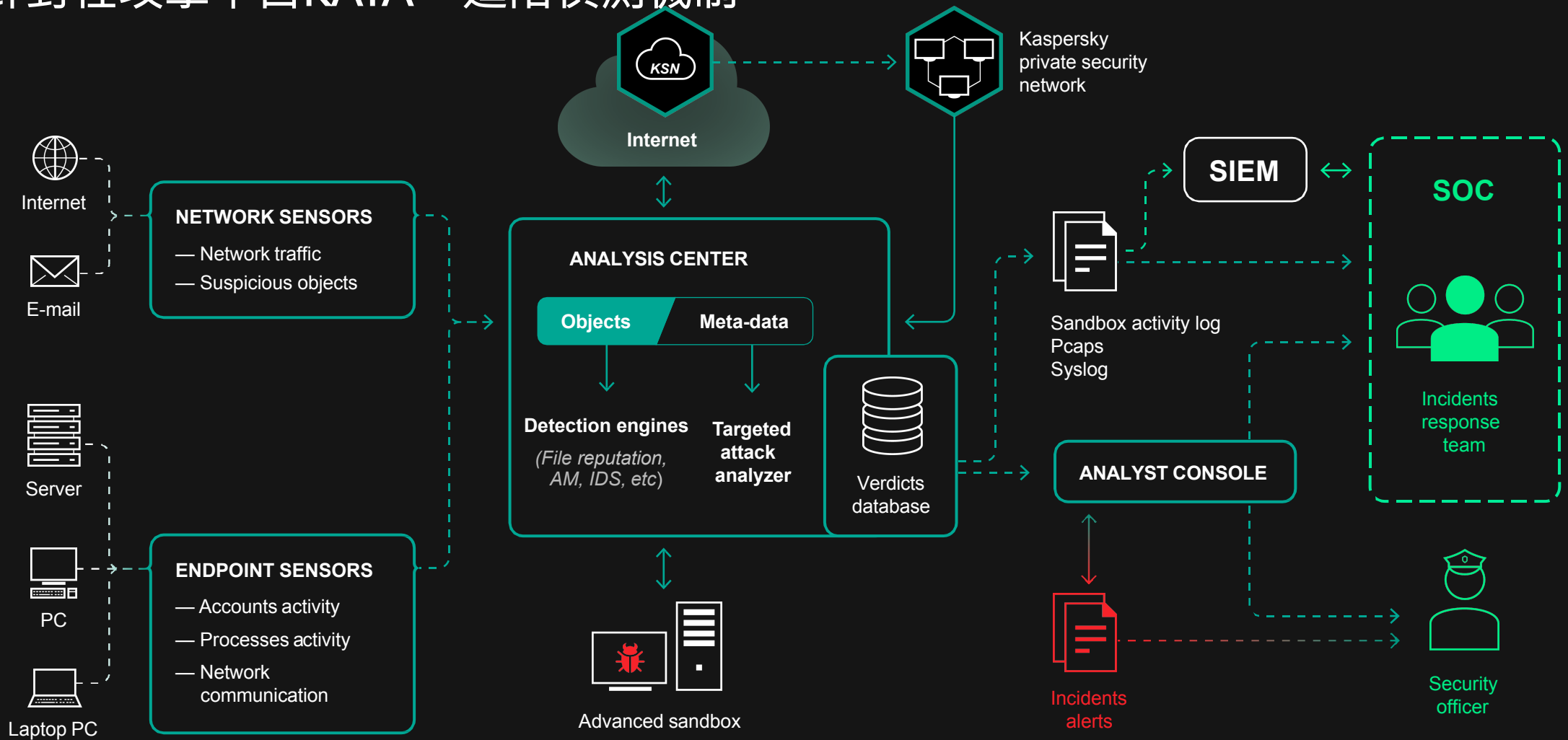


kaspersky

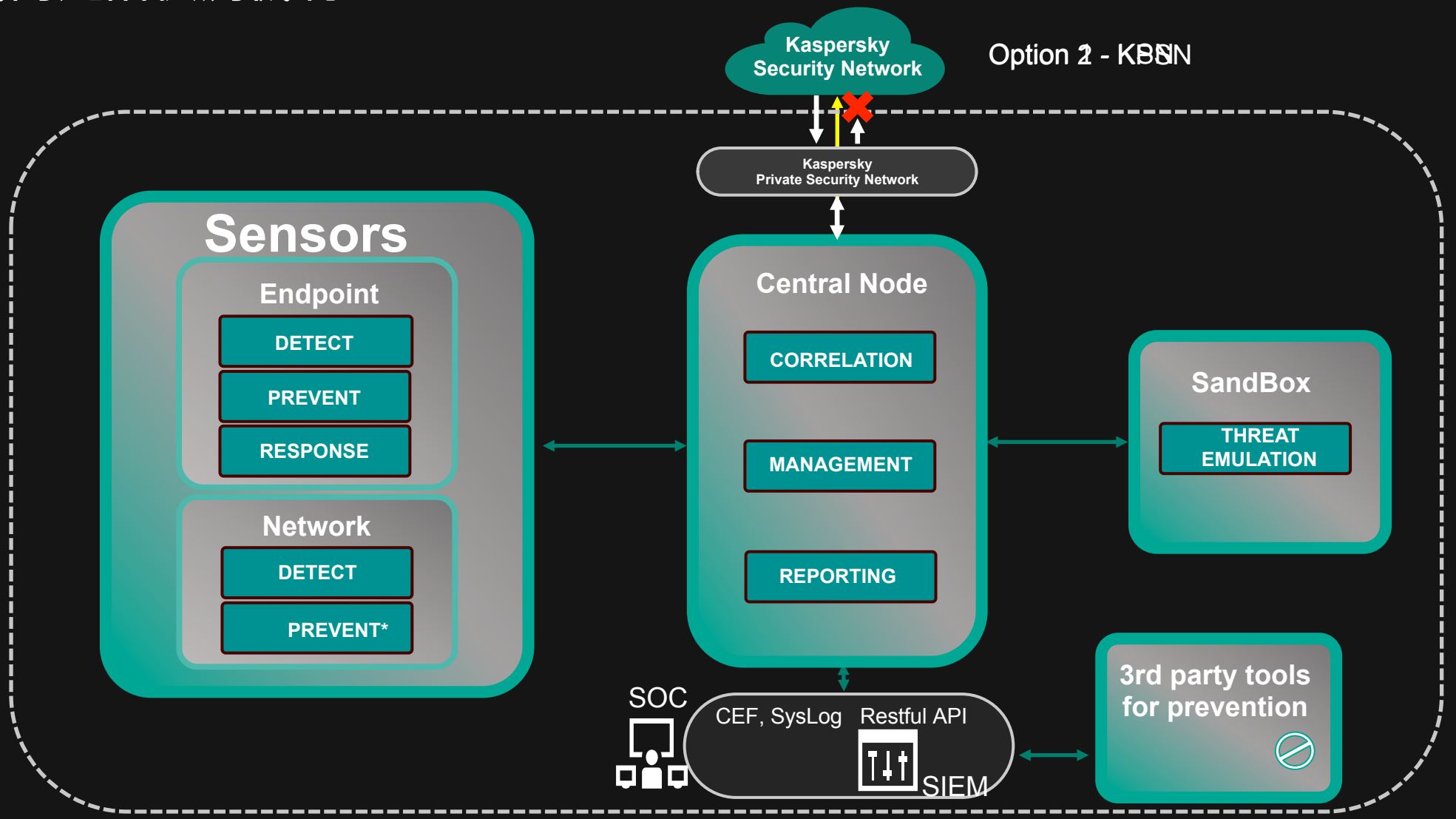
建構威脅態勢感知平台


透過外部專家
透過內部經驗及人員
Expert services
專家指導
即刻救援
內部安全教育
威脅情報整合
選擇好的外部服務廠商
提高內部安全應變處理能力
Managed Detection and Response (MDR)
針對式攻擊發掘
事件響應服務
安全培訓
Threat Intelligence
內部技能
無專門安全團隊
缺乏IT安全專家
提高內部安全
完整的安全團隊部門
具備充足專業知識及能力
Steps
全自動
步驟一
強化阻擋機制 & 安全意識
半自動
步驟二
進階偵測技術及回應機制
手動/人工
步驟三
深入調查、威脅獵捕及改善戰略

反針對性攻擊平台KATA – 進階偵測機制

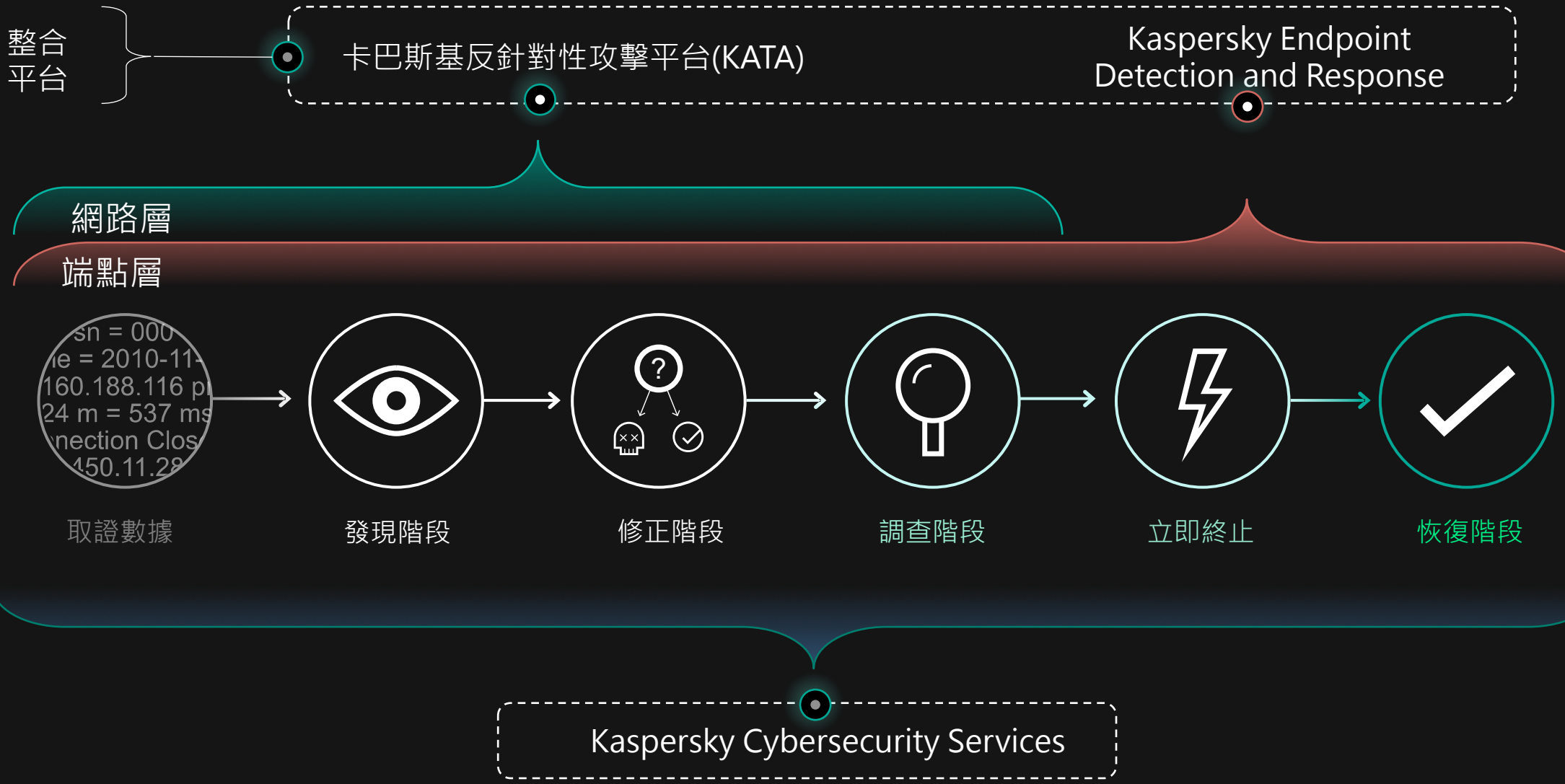


落地式的進階偵測機制



kaspersky

解決方案:卡巴斯基威脅管理和防禦平台



進階偵測機制及事件調查響應能力

網路流量分析

沙箱分析

端點偵測機制

威脅智能情報來源

威脅獵捕工具

持續監控機制

事件回應工具

kaspersky

ALL-IN-ONE SOLUTION

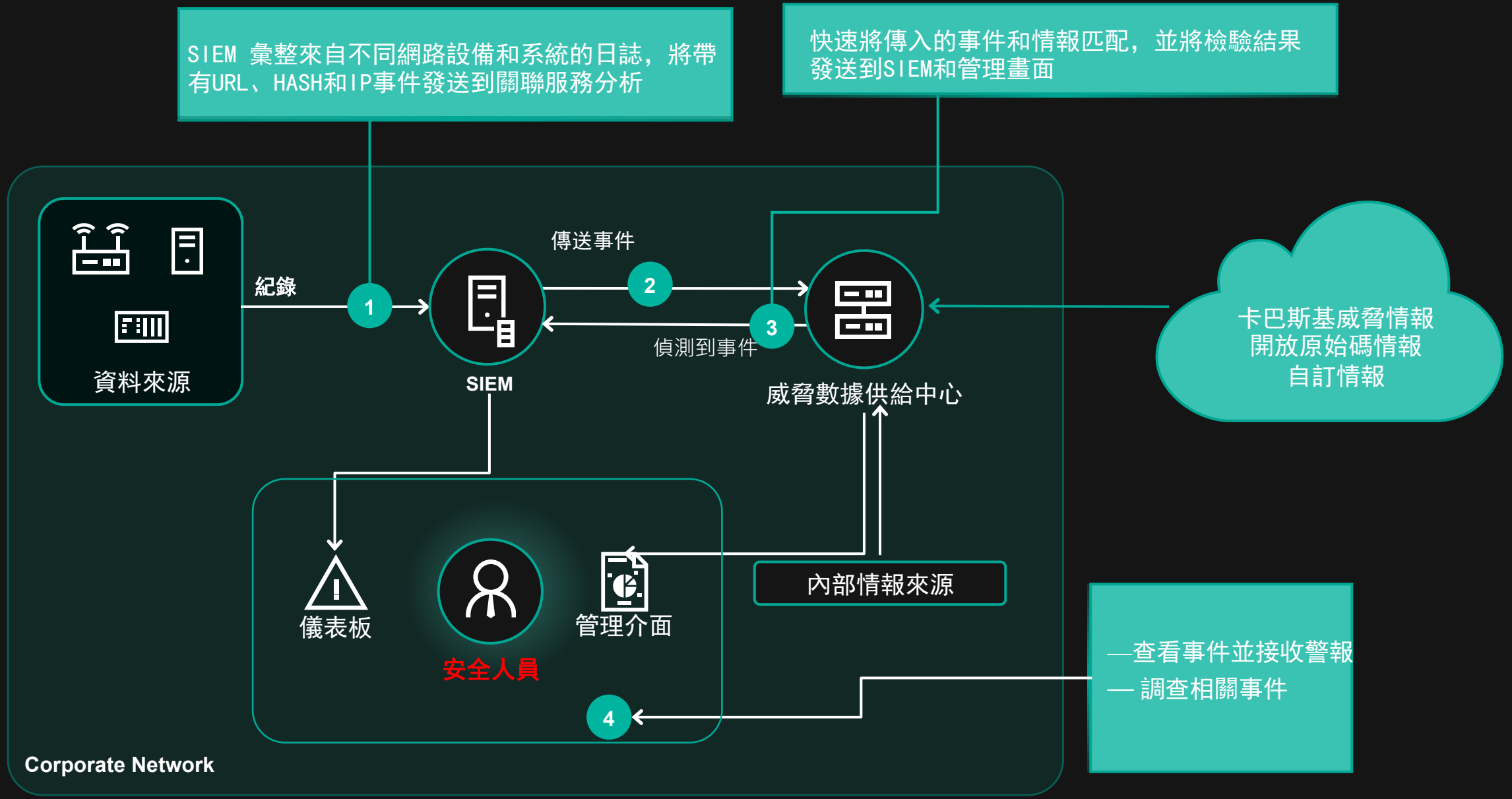
什麼挑戰及結果?

- 太多分散的工具
- 太多的事件
- 太多人工關聯的程序

- 缺乏可視性
- 缺乏整合性
- 缺乏資源
- 缺乏專家的支援

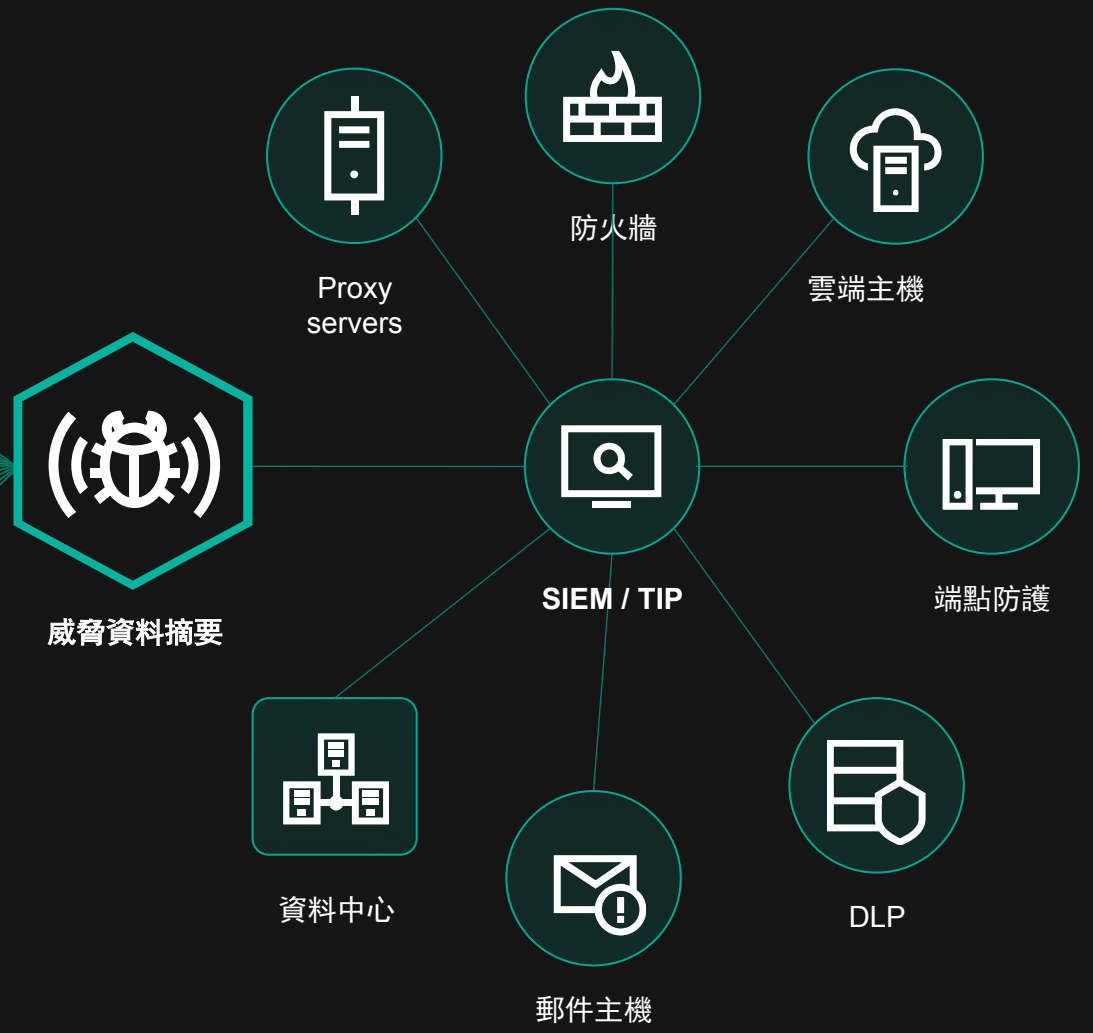
- 單一軟體及單一管理介面
- 內建關聯分析比對機制
- 提供與全球威脅智能情報整合及專家服務
- 容易與第三方安全產品或SIEM/SOC整合

整合智能情報

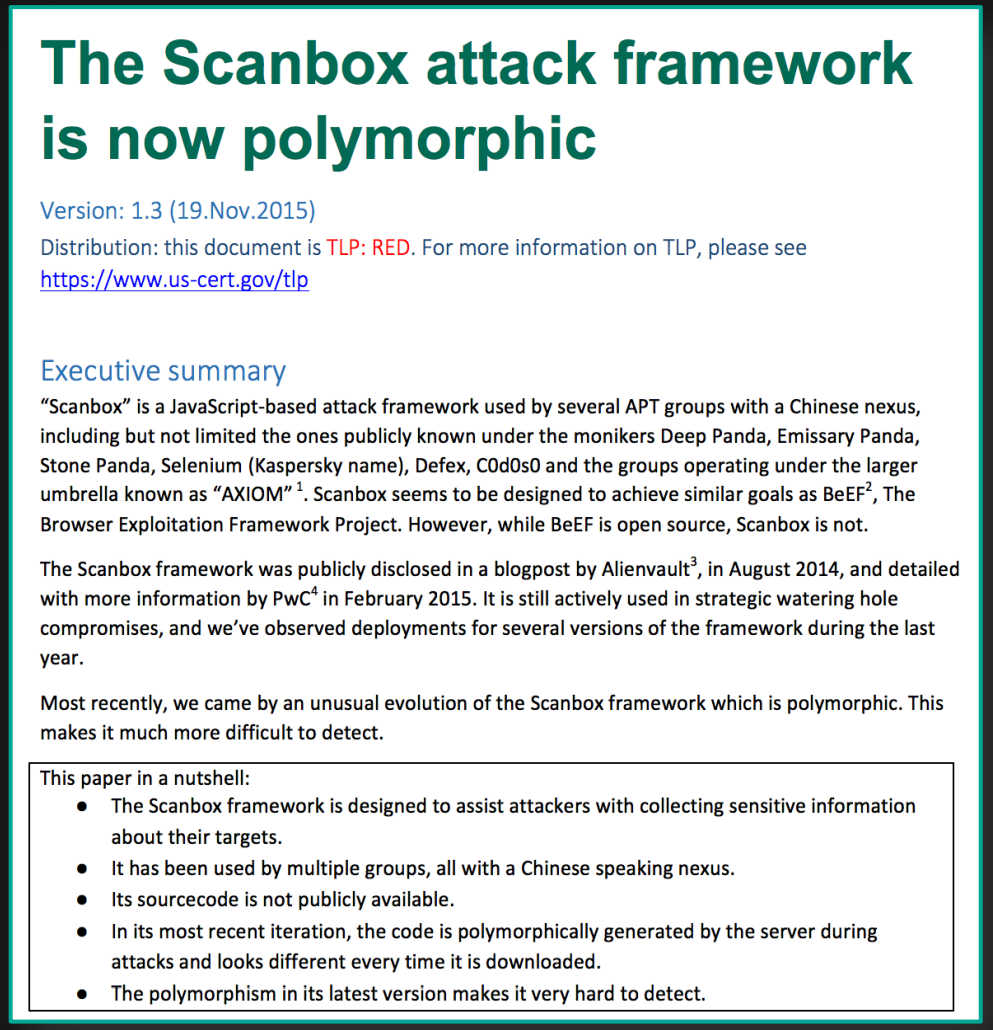

SIEM 彙整來自不同網路設備和系統的日誌，將帶有URL、HASH和IP事件發送到關聯服務分析
快速將傳入的事件和情報匹配，並將檢驗結果發送到SIEM和管理畫面
資料來源
紀錄
1
SIEM
傳送事件
2
偵測到事件
3
威脅數據供給中心
卡巴斯基威脅情報
開放原始碼情報
自訂情報
儀表板
安全人員
管理介面
內部情報來源
—查看事件並接收警報
— 調查相關事件
4
Corporate Network

威脅資料摘要

- IP 評價摘要
- 雜湊碼摘要(WIN / *nix / MacOS / AndroidOS / iOS)
- 惡意和網路釣魚網址摘要
- 勒索軟體摘要
- APT IOC 摘要
- 白名單資料摘要
- 電信雜湊碼摘要
- PASSIVE DNS (pDNS) 摘要
- IoT 網址摘要



APT 和金融威脅情報報告



The Scanbox attack framework is now polymorphic

Version: 1.3 (19.Nov.2015)

Distribution: this document is TLP: RED. For more information on TLP, please see https://www.us-cert.gov/tlp

Executive summary

"Scanbox" is a JavaScript-based attack framework used by several APT groups with a Chinese nexus, including but not limited the ones publicly known under the monikers Deep Panda, Emissary Panda, Stone Panda, Selenium (Kaspersky name), Defex, C0d0s0 and the groups operating under the larger umbrella known as "AXIOM" [1]. Scanbox seems to be designed to achieve similar goals as BeEF[2], The Browser Exploitation Framework Project. However, while BeEF is open source, Scanbox is not.

The Scanbox framework was publicly disclosed in a blogpost by Alienvault[3], in August 2014, and detailed with more information by PwC[4] in February 2015. It is still actively used in strategic watering hole compromises, and we've observed deployments for several versions of the framework during the last year.

Most recently, we came by an unusual evolution of the Scanbox framework which is polymorphic. This makes it much more difficult to detect.

This paper in a nutshell:

- The Scanbox framework is designed to assist attackers with collecting sensitive information about their targets.
- It has been used by multiple groups, all with a Chinese speaking nexus.
- Its sourcecode is not publicly available.
- In its most recent iteration, the code is polymorphically generated by the server during attacks and looks different every time it is downloaded.
- The polymorphism in its latest version makes it very hard to detect.

→ 摘要
- C-level 資訊

→ 技術分析
- 攻擊方法
- 使用的漏洞攻擊
- 惡意軟體描述
- C&C 相關描述
- 受害者分析
- 數據滲透分析
- 原因

→ 結論和建議

→ Indicators of Compromise 指標和YARA 規則

金融威脅情報報告

Lazarus attacks against Taiwanese financial institutions

Report Id: 20171006
Version: 1.1 (17.October.2017)
Update: Technical detail in Loader analysis fixed

Executive summary

It was recently published[1] a cyber-attack against a Taiwanese bank (FEIB) where attackers managed to transfer $60 million USD. Due to the early discovery of the attack, the bank managed to recover almost all money, except for $500000 USD.

A quick analysis on the malicious files used by the attackers revealed another potentially compromised bank, also located in Taiwan, which one of its servers presenting identical malware than the one discovered in FEIB.

The TTPs of this campaign reminded us of Lazarus, where some malware is being reused from previous campaigns against banks, stretching from the end of 2016 to early 2017. In previous campaigns, Lazarus targeted several of European and African banks.

This paper in a nutshell:

- A new major cyber heist has occurred in the Asian region;
- The discovered malware seems to indicate that Lazarus group has restarted its activity, exploiting servers connected to SWIFT network;
- A new technique to drop self-spreading ransomware during the attack, apparently for distraction purposes, suggests a new persistent tactic used by the group, and raises questions about the Wannacry real purpose.

- 針對式攻擊
  - 用繞過安全機制的方法
  - Monetization methods
- 攻擊ATM
- 攻擊POS 裝置
- 網路犯罪開發和銷售的特定工具

國家、特定行業別的威脅情報報告

政府

網路邊界漏洞: 危險

網路犯罪份子惡意軟體活動和威脅: 高

地下組織活動: 高

其他...

製造業

網路邊界漏洞: 危險

網路犯罪份子惡意軟體活動和威脅:高

地下組織活動:中等

電信

網路邊界漏洞:危險

網路犯罪份子惡意軟體活動和威脅: 中等以上

地下組織活動: 中等

銀行

網路邊界漏洞:中等

網路犯罪份子惡意軟體活動和威脅:高

地下組織活動: 危險

威脅資料摘要

SIEM


THREAT INTELLIGENCE PLATFORMS

DATA MINING TOOLS

NETWORK SECURITY CONTROLS

資料整合及調查

要分析的物件

- 網址
- 網域
- IP 位址
- 雜湊碼
- 威脅名稱
- 檔案

卡巴斯基威脅查詢

查詢

網頁服務

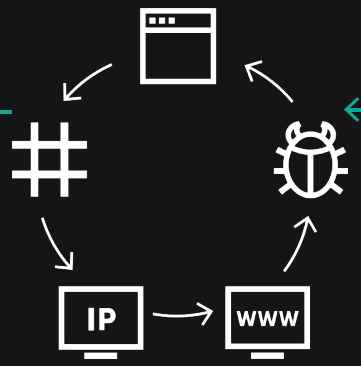
事件回應

- 是否為惡意?
- 有什麼正在入侵?
- 之間有哪些關係?
- 我們是否容易遭到入侵?

全自動關聯

內容情報

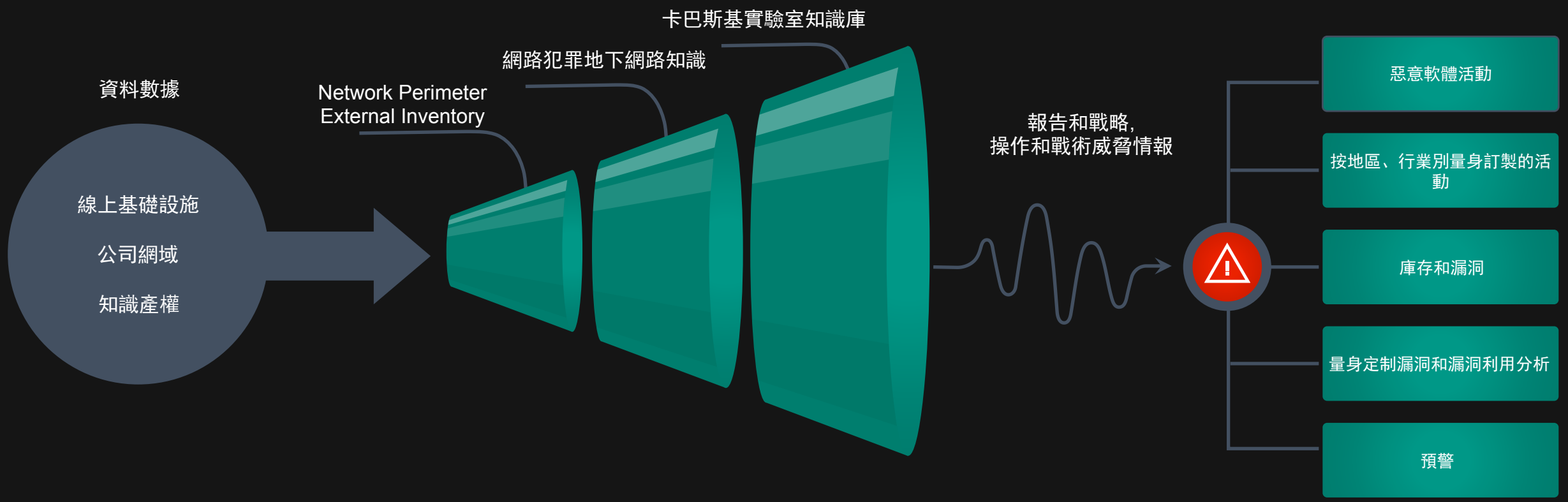
情報



資料來源

- Kaspersky Security Network
- 安全合作夥伴
- 垃圾郵件陷阱
- 網路感應器
- 網路編目程式
- 殭屍網路監控
- 雲端沙箱

量身自訂的威脅情報報告(客戶/國家/地區)



卡巴斯基實驗室知識庫:

- 惡意軟體樣本分析
- 殭屍網路和網路釣魚追蹤
- APT 威脅情報報告
- Sinkhole和惡意軟體服務器
- 威脅情報摘要

網路犯罪地下網路相關知識:

- 網路犯罪活動
- 資訊洩漏
- 內部惡意人員
- 員工社群網路
- 開放原始碼情報(OSINT)

NETWORK PERIMETER EXTERNAL INVENTORY:

- 可用服務
- 指紋識別
- 漏洞識別
- 利用分析
- 評分和風險分析

APT 和金融的威脅情報報告

→目前有超過100+威脅報告

→事件發生時後會通知有訂閱的客戶

→我們報告包含：事件摘要、技術描述和IOC

威脅情報

全球威脅情資可深入瞭解企業組織的網路威脅

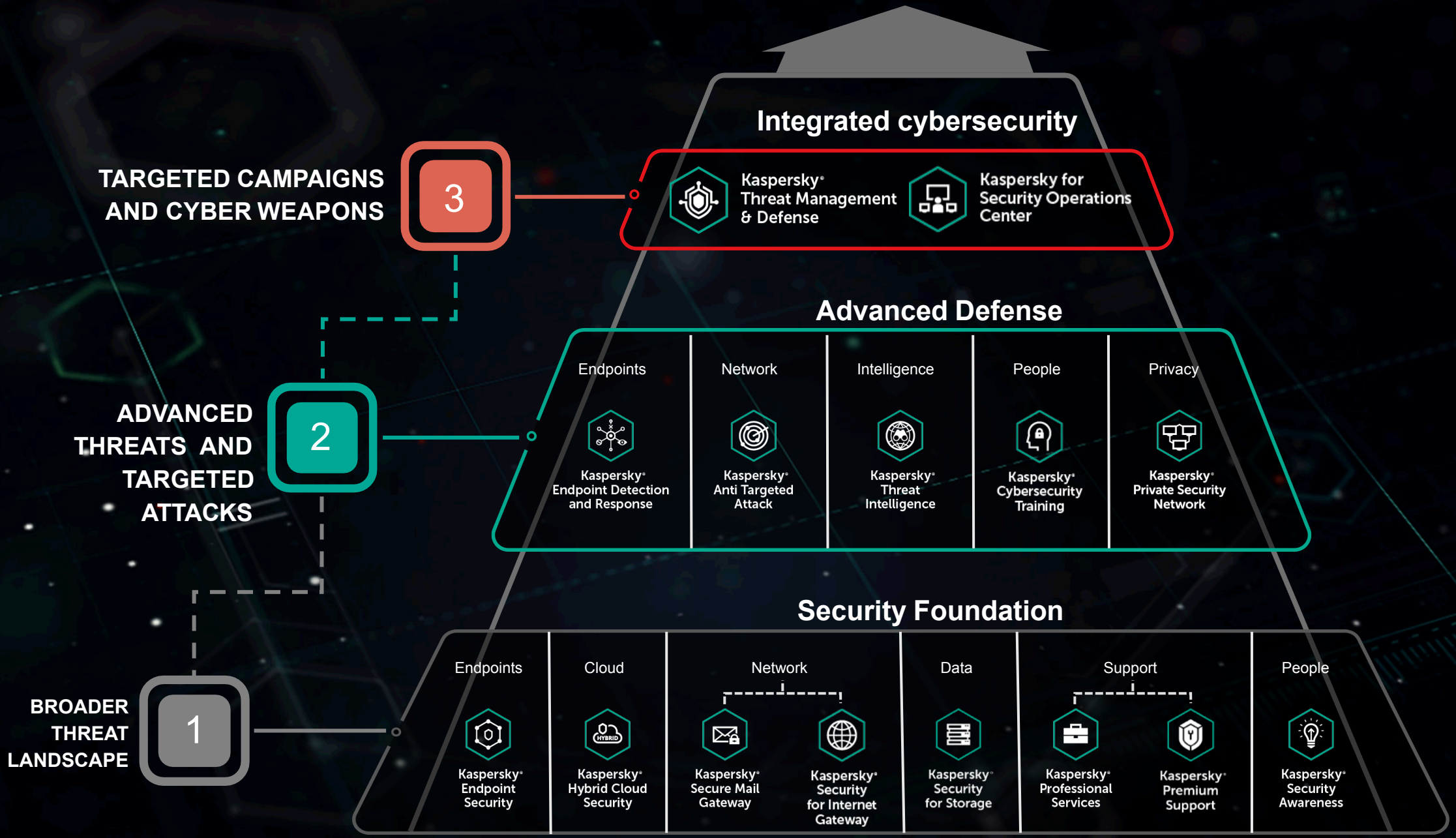
能有效查找暗網中受限制和有威脅的資源

整合成高偵測率的威脅情報

提供各國家的相關攻擊資訊

在整個事件管理週期中提供有意義的上下文

建構整合安全情資的安全架構



Kaspersky Managed Detection and Response

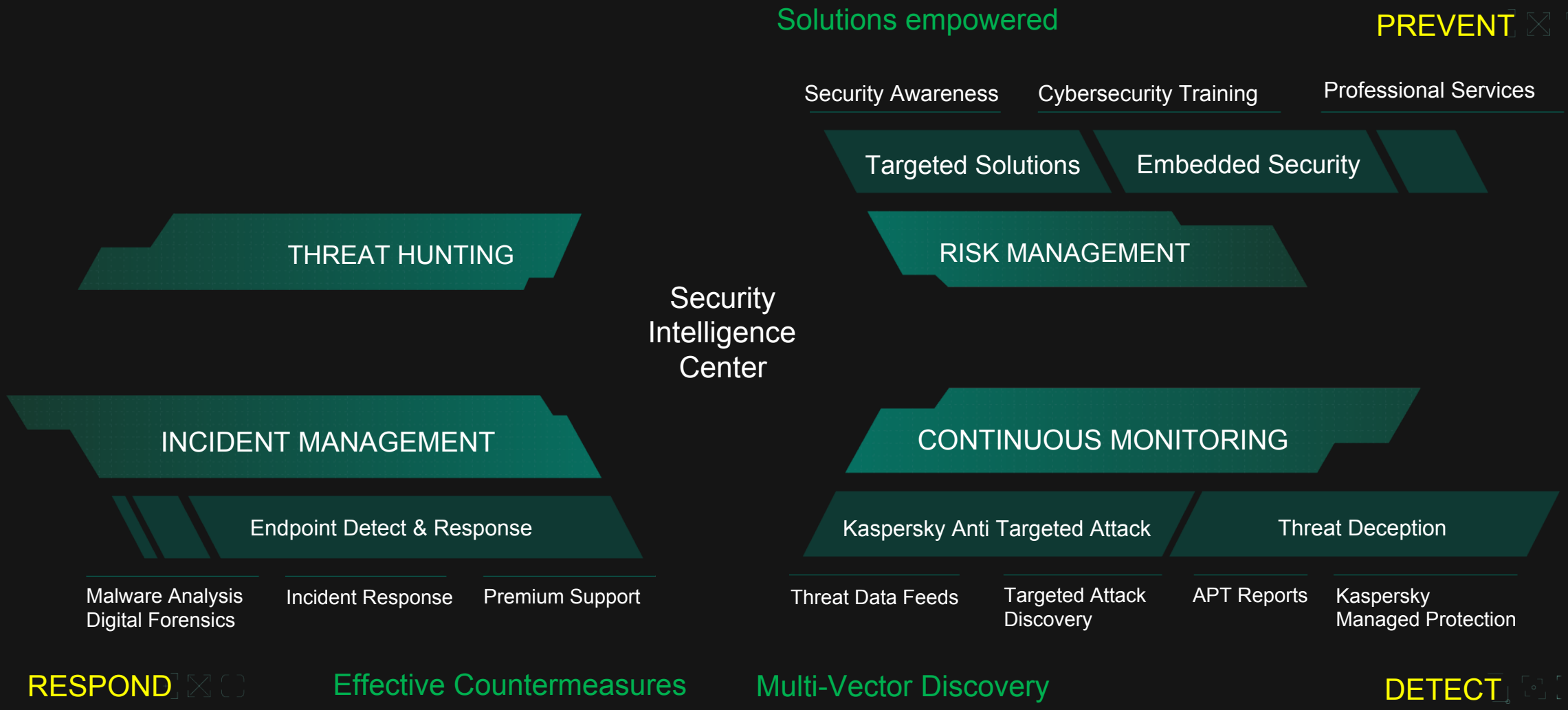
企業安全的挑戰

- 絕大多數的針對式攻擊都是透過常見的威脅及社交工程發起的 – 資安意識的養成
- 偵測及回應比阻擋及預防來的更有價值
- 回應相關事件→提供了安全的假像 – 無告警不代表無威脅
- 針對式攻擊是一個複雜且結構化的過程 而非只是依靠產品就可完成防護
- 持續性的監控及安全分析是下個世代安全解決方案對抗進階式威脅最主要的部份
- 自動化修正 – 需修正的觀念 應導入可適性安全策略 來面對不斷進化的針對式攻擊威脅

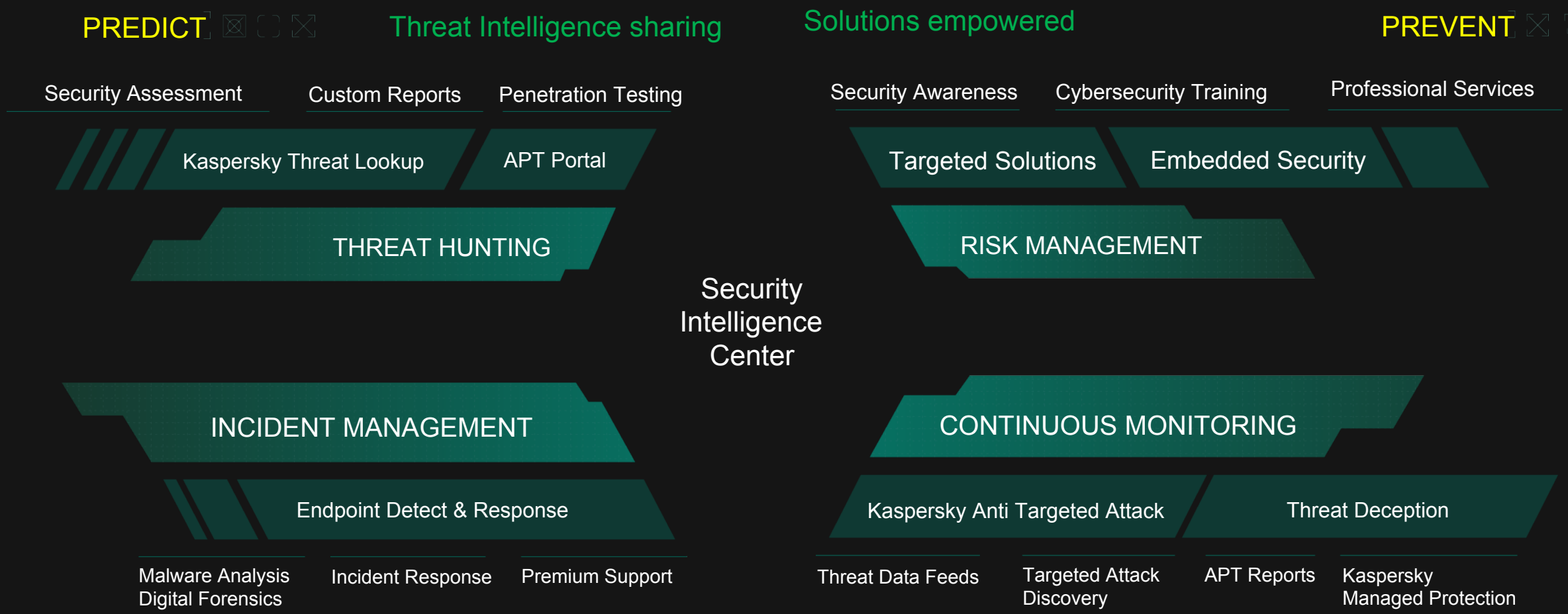
強化現有安全機制來減低針對式攻擊威脅的風險

發現各種微量的滲透事件提早應對針對式攻擊威脅的入侵

發展合適的回應機制及方法 提昇SOC技術能量



利用外部的資訊及事件回應的經驗強化現有威脅管理機制



LET’S TALK