Co-brand Logo
goes here

資安聯防 人人有責
案例分享

Dragon Chang (張士龍)
賽門鐵克

大綱

1 資訊安全現況說明

2 資訊安全鐵三角

3 案例分析

4 Lessons Learned

5 結論

Symantec™

資訊安全現況說明

現況說明

- 入侵攻擊事件頻傳，**該怎麼預防**呢？
- 如何**讓已投資的資安設備發揮應有的功效**呢？
- 目前環境有不同資安廠商在維護，**該如何整合**呢?
- 資安部門人手不足,如何**掌握最新資安資訊**呢？
- 怎確認我們的資安環境是否有**符合業界標準**呢？

2018 賽門鐵克網路威脅分析報告

Symantec

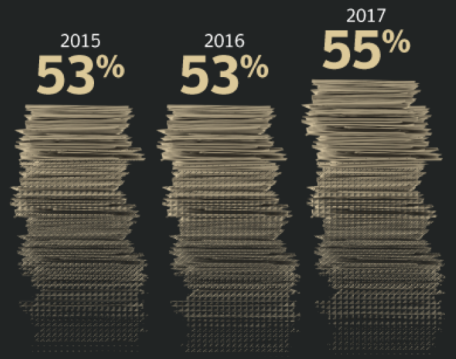
網頁威脅

賽門鐵克平均每天分析
超過10億次網頁請求
比2016年增長5%

每13個網頁請求中，
便有1個定向至惡意軟體
比2016年增長3%

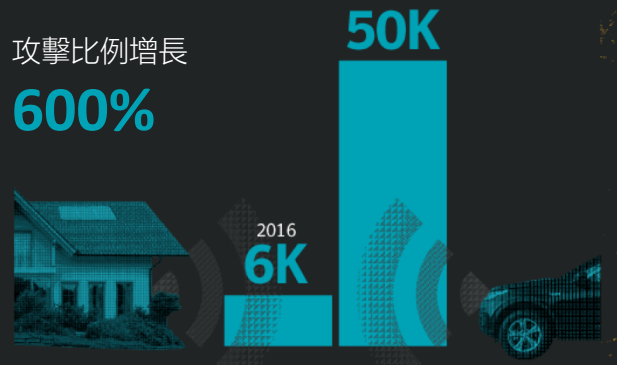
電子郵件

垃圾郵件
比重



物聯網

攻擊比例增長
600%



漏洞

已上報漏洞總
體增長
13%

惡意軟體

新下載器變種
的增長比例
92%

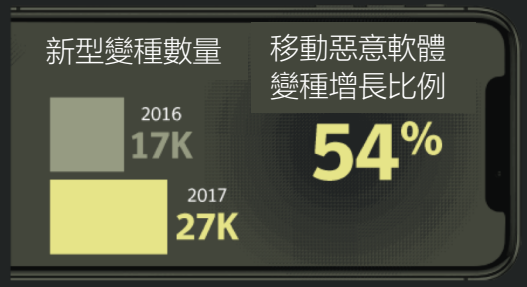
針對Mac系統
的新型惡意軟
體增長比例
80%

勒索軟體

已攔截的
WannaCry攻擊
54億

新型勒索軟體變種
增長
46%

行動設備



平均每天攔截的
惡意移動應用數量
24,000

資訊安全防護鐵三角：資安監控服務、基礎架構防護、資安顧問服務

Symantec
Global Intelligence Network

Symantec - Cyber Security Service

INTERNET

Messaging Gateway

Email Server

郵件安全防護

SSL Visibility

Proxy - SG

Security Analytics

閘道安全防護

Content & Malware Analysis

ATP

聯防整合防護

SEP 管理平臺

SEP/EDR

端點安全防護

Security Consultant

系統服務漏洞與威脅檢測

系統強化與參數優化

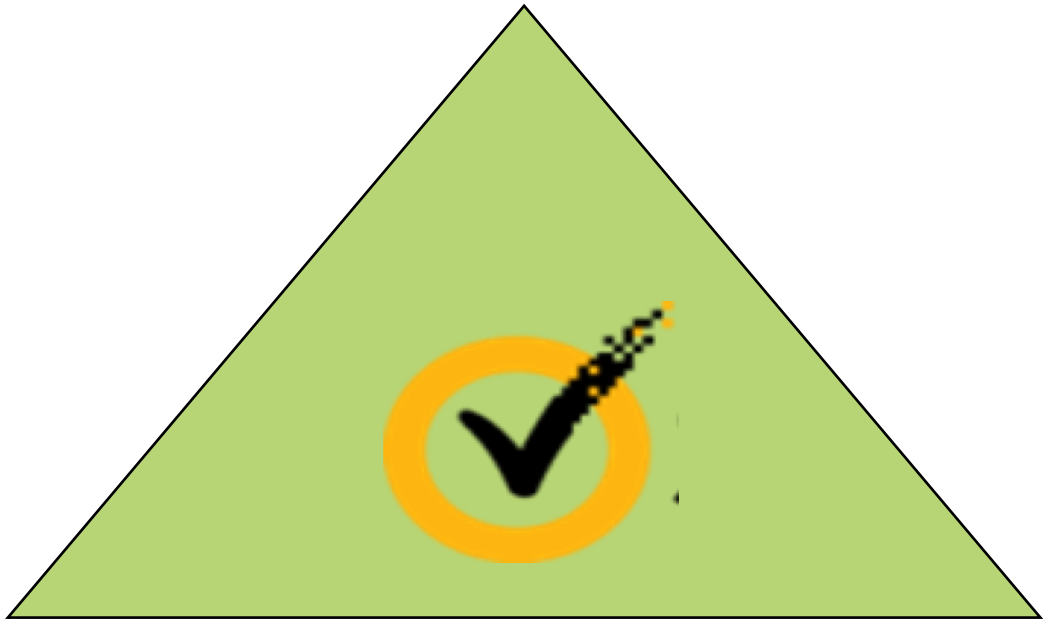
IT環境成熟度分析

鐵三角可以做到甚麼

- 基礎架構防護
  - 四個維度思考: 端點、閘道、郵件防護、雲端
    - 1. 威脅防護 2. 資料保護 3. 安全聯防 4. 行為鑑識分析

- 即時監控安全分析
  - 事前: 安全情知通報
  - 事中: 攻擊當下時即偵測

- 資安顧問服務
  - 系統服務漏洞與威脅檢測
  - 產品系統參數優化
  - IT 成熟度分析



Symantec™

案例分析

新加坡SingHealth醫療系統遭駭客入侵，150萬人個資外洩

新加坡衛生部（Ministry Of Health Singapore）對外公告，醫療系統的資料庫遭遇駭客入侵攻擊，150萬人個資恐外洩。他們同時強調這起網路攻擊事件，是針對總理李顯龍而來。

根據國內外多家媒體報導，新加坡發生最大規模駭客攻擊事件，150萬人在醫療系統中的個人資料遭到竊取，由於就醫紀錄也包含總理李顯龍，格外受到關注。

根據新加坡衛生部（Ministry Of Health Singapore）官方網站，在20日對外公告指出，新加坡醫療保健集團（SingHealth）遭到駭客入侵IT系統。這起事件起於2018年7月4日，整合健康資訊系統（Integrated Health Information Systems, IHiS）的系統管理員，在SingHealth的系統資料庫檢測到異常活動，他們立即採取必要行動並展開評估。之後經過新加坡網路安全局CSA（Cyber Security Agency），以及IHiS的調查證實，這次是醫療記錄遭竊取的攻擊事件，是一場針對性和精心策劃的網路攻擊。

在新加坡衛生部的聲明中，他們也特別指出這起駭客攻擊事件，是針對總理李顯龍而來，目的是竊取他前往診所的個人資料與相關資訊。

在整起事件中，駭客所竊取的個人衛生資料，包含了2015年5月1日到今年7月8日期間，前往SingHealth專科門診以及綜合診所患者等各大醫院診所就醫民眾的非醫療個人資料，包含像是姓名，身份證號碼，地址，性別，種族與出生日期，而外

狙擊智慧國家：新加坡史上最慘網路攻擊，150萬健保戶資料遭竊

antec

「我不明白攻擊者想找到什麼。可能他們想搜尋新加坡的『黑色機密』？或許只是想拿到資料，好對公開羞辱我本人？」在資安事件曝光後，李顯龍也透過Facebook發表了公開信，「如果目的只是這樣，那他們註定失望——雖然我個人的醫療紀錄，不是什麼值得公開或平時說嘴的資訊，但內容真的沒有什麼不可告人的東西。」

現年66歲的李顯龍，過去雖不曾傳出重大傷病史；但近兩年來，李顯龍卻多次在國慶大典等公開場合，出現暈眩、發軟、體力不支，甚至抽搐無法行走等的症狀，去年年底更因此休了長假，神隱10多日。

雖然官方的說法一直強調「李顯龍只是工作壓力太大，導致身心過勞」，但坊間仍不時有「李顯龍心臟病發」、「李顯龍得癌症」...等流言傳出。再加上李顯龍已任總理14年，一般預期他打算在2022年內閣任滿後「退休」，並於近期從內閣官員中欽點接班人選。交棒的關鍵時刻，國家領導人的健康與身心狀況，也就成為了極為敏感的政治問題。

李顯龍強調，在推行智慧國家、數位城市的時代，來自網路的安全威脅始終不曾降低，政府內部對於「百密終究會有一疏」的發生，也早有預期；但攻擊健保系統，影響眾多國民的個人資安，仍是極為嚴重且令人遺憾的重大事件。

根據新加坡政府目前的調查進度，新保集團這回之所以遇襲，疑似是駭客透過「惡意程式」，控制了一部醫療前端的工作站，並藉此滲透進中央系統，直到7月4日系統偵測到「資料異常活動」後，才透過封阻反制與全系統外部斷網，中斷了駭客的入侵；但像是新加坡主推的「智慧國家計畫」中，各種醫療資訊的電子平台整合與建置，都因本案的爆發而暫時凍結。

入侵成功細部說明

- The cyberattacker had actually gained an initial presence in SingHealth's network as early as August 2017 by "infecting workstations", the Solicitor-General said

- The attacker was able to gain access to an end-user workstation via a publicly available hacking tool because the workstation was running on a version of Microsoft Outlook that was not patched to address the use of that hacking tool," he said, citing the Cyber Security Agency of Singapore's (CSA) findings.

- Between December 2017 and May 2018, the attacker moved sideways in the network, making use of malware planted in one of the initially infected workstations to gain remote access to and control of the workstation. He then used that computer to distribute malware to infect other computers.

入侵成功細部說明

- The attacker moved in a targeted manner, planning his route in the network to reach the SCM database, which was the attacker's ultimate objective,"

- From May to June this year, the attacker used a compromised workstation and some Citrix local administrator accounts to remotely log in to Citrix servers. One of those Citrix local administrator accounts had protection measures, including a password - P@ssw0rd – that could be easily deciphered.

- At this point, the attacker had not yet obtained SCM database credentials that would have allowed him to log in. In fact, the attacker had made multiple failed attempts to log in to the database "using either non-existent user accounts or user accounts that had insufficient privileges to gain access".

入侵成功細部說明

- CSA's Mr Dan, who said the attacker was able to run bulk queries because the system did not have existing rules or controls to detect such behaviour or the illegitimate use of certain SQL programmes
- The Allscripts SCM software was mentioned as there is evidence there was "insecure coding vulnerability" in it and it is "highly probable" the vulnerability allowed the attacker to easily retrieve SCM database credentials from the Citrix server on H-Cloud, which can then be used to log in to the database. And IHIS was said to have known of this back in 2014.
- The cyberattacker eventually managed to access a H-Cloud Citrix server through which users were accessing the SCM database, and CSA hypothesised that it is probable that the perpetrator stole the needed credentials through this avenue. The SCM database was successfully accessed on Jun 26 but no queries were made on that date.

入侵成功細部說明

- The real activity started the day after, when the attacker began sending queries to the database up till Jul 4, running “numerous bulk SQL queries from the Citrix server against the SCM database server (via the open network connection)”. These activities were only terminated by IHIS database administrator Katherine Tan on Jul 4.
- The data unlawfully accessed and exfiltrated from Jun 27 to Jul 4 this year belonged to 1,495,367 patients comprising their demographic records. The attackers also made off with 2,001,008 dispensed medication records pertaining to about 159,000 of these patients.
- Among the first two witnesses for the public hearing on Friday is IHIS assistant director (Infra Services - Systems Management) Lim Yuan Woh, who had first discovered on Jun 11 that certain accounts had been compromised.

事後檢討分析

事前

- 系統漏洞未能執行(Outlook & SCM)
- 安全政策未能落實(Citrix Weak Pass)
- 未知行惡意程式分析能力

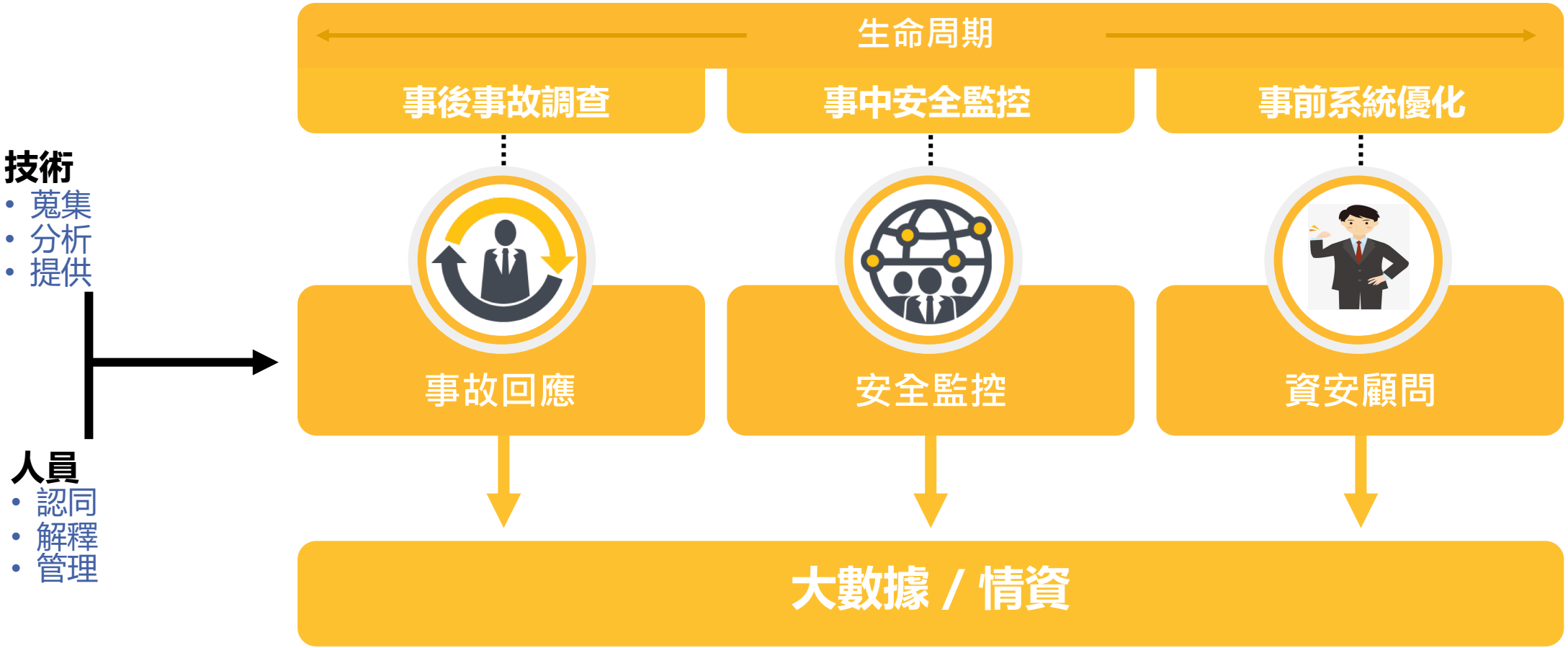
事中

- 一年時間異常連線而並未偵測
- 日誌檔監控未落實(login Fail)
- 重要系統監控(執行大量DB查詢)

事後

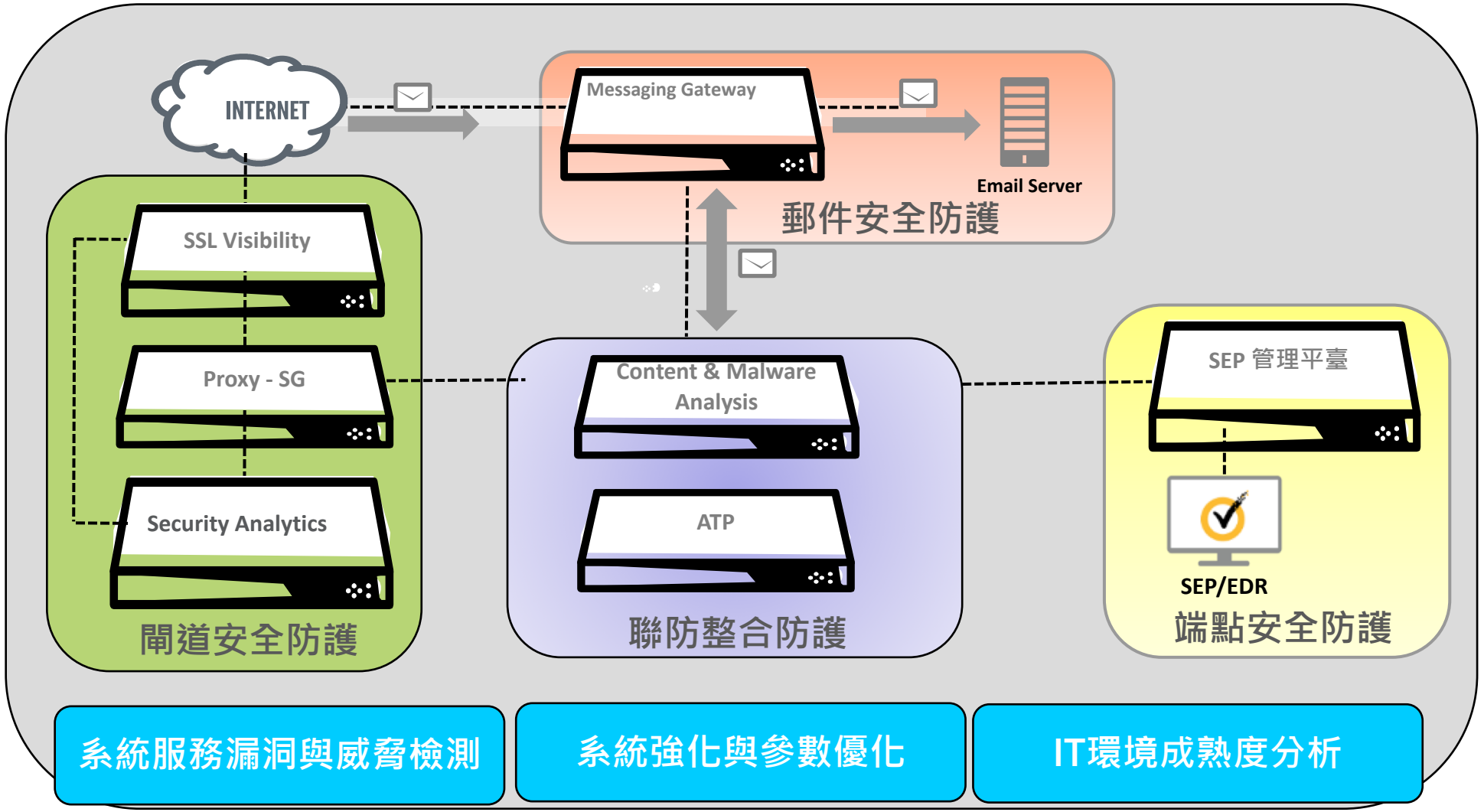
- 未執行通報流程
- 鑑識分析啟動

專業資安服務需求｜資安事故全生命週期服務



事前防護 – 打造安全防護網

打造安全防護網



賽門鐵克資安顧問服務

賽門鐵克
顧問服務
解決方案

1

專案規劃與執行

- 架構規劃與設計
- 政策規劃與系統建置
- 第三方系統整合

2

系統維運

- 系統優化
- 系統運作狀態檢查
- 系統配置參數檢查
- 系統日誌分析及建議

3

系統優化

- 系統架構分析及優化
- 系統參數分析及優化
- 系統效能分析及優化
- 系統策略分析及優化
- 優化結果驗證

4

SOC 預警響應

- SOC 組織規劃 / 事件監控管理流程
- 7x24資安事件監控
- 定期風險分析報告與資安強化建議

5

駐點服務

- 系統監控與健檢
- 系統維護
- 系統維護日誌檢視

6

顧問諮詢服務

- 資安健檢服務
- 產品教育訓練
- API/SDK客製化開發

顧問諮詢服務效果介绍-資安檢測服務

服務週期	專案規劃與執行	系統維運	系统優化	預警響應	駐點服務	駐點服務

- Symantec 資安建議策略三個構面
  - People – “Strategic”
  - Process – “Operations”
  - Technology – “Tactical”
- 跨越七個核心領域
  - 階段一資安檢測
    - Network & System Security
    - Data Security
  - 階段二資安檢測
    - Business Continuity
    - Application Security
    - Security Operations
  - 階段三資安檢測
    - Security Strategy
    - Security Organization
  - 輸出成果
    - 《企業資安成熟度分析報告》
    - 《安全領域成熟度分析與改進建議》
    - 《企業資訊安全發展計畫》

《企業資安成熟度分析報告》

事中防護 – 即時監控服務

目前安全挑戰

- 無法提供人員 7X24 監控企業即時事件
- 無法建立有效關連事件分析與建議處理流程
- 無法跟上最新的威脅
- 缺乏專業資安分析師來分析與回應企業資安事件
- 低估SIEM複雜性

賽門鐵克網路服務監控主要優勢

大數據分析	安全情報來源	世界一流資安專家
大數據引擎系統中，已經載入 150TB 資料	6900萬攻擊感測器.	全球擁有 6 座 SOCs.
每天分析過的日誌超過 300 億	5百萬郵件誘捕帳號.	超過 1,000 資安專家
每天確認新可疑資安事件超過3萬筆	每天過濾超過80億郵件	所有資安事件分析師 100% 擁有 GIAC 認證
	每天有14億次網站內容檢測請求	資安分析師成為貴公司資安團隊一員

What Is GIAC?

Global Information Assurance Certification (GIAC) is the leading provider and developer of Cyber Security Certifications. GIAC tests and validates the ability of practitioners in information security, forensics, and software security. GIAC certification holders are recognized as experts in the IT industry and are sought after globally by government, military and industry to protect the cyber environment.

賽門鐵克網路監控服務

外部即時威脅資訊來源

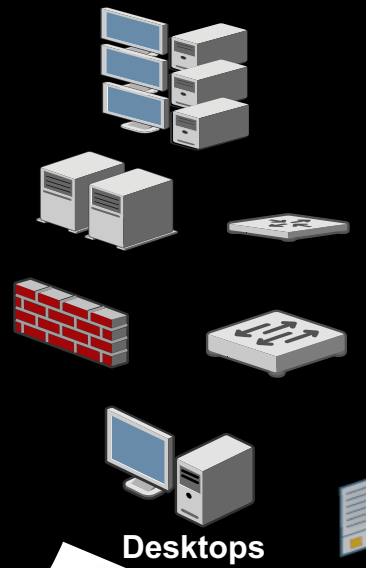
- Threats
- Vulnerabilities
- Malcode
- File & Site Reputation

監控中心

- Compliance Restriction
- Organization
- Asset Value
- System Function

分析與處置

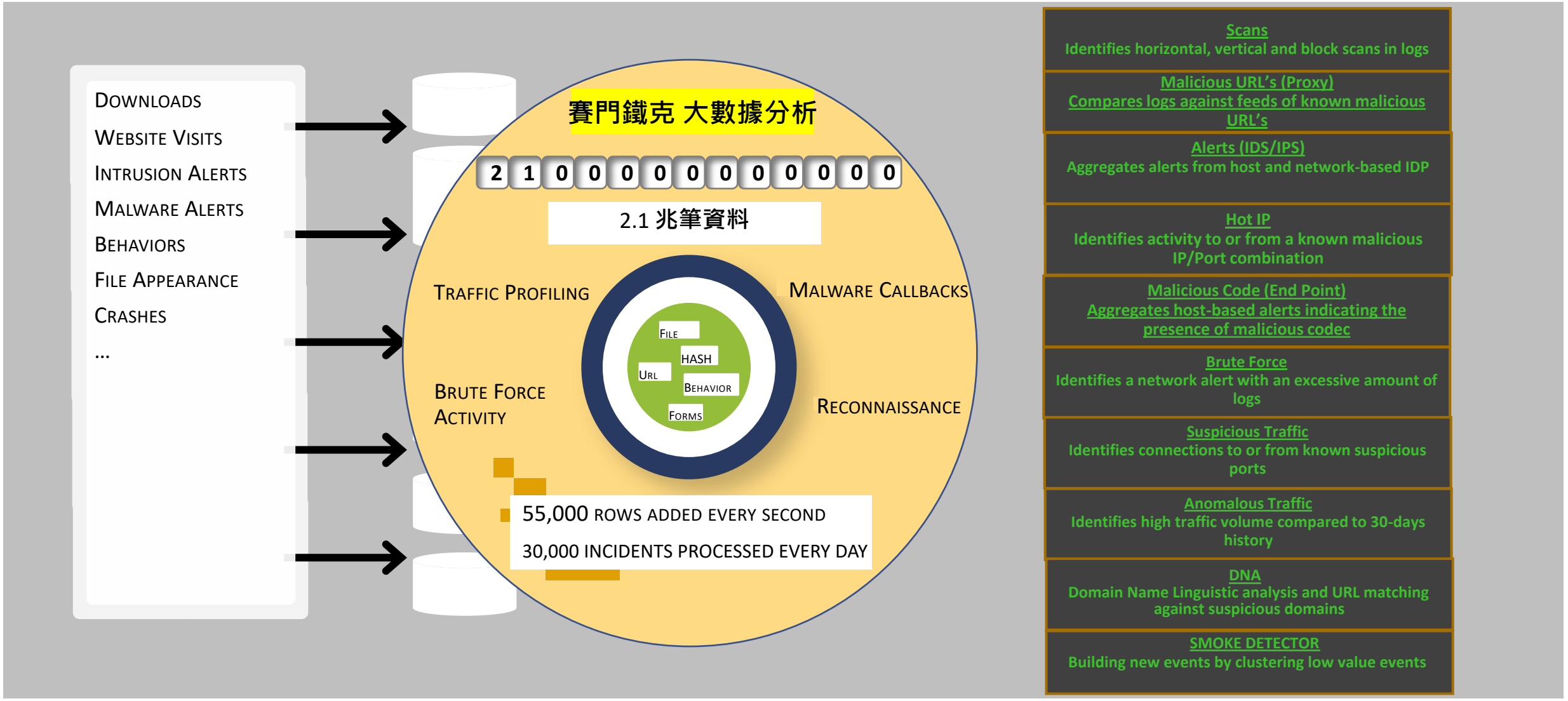
監控環境



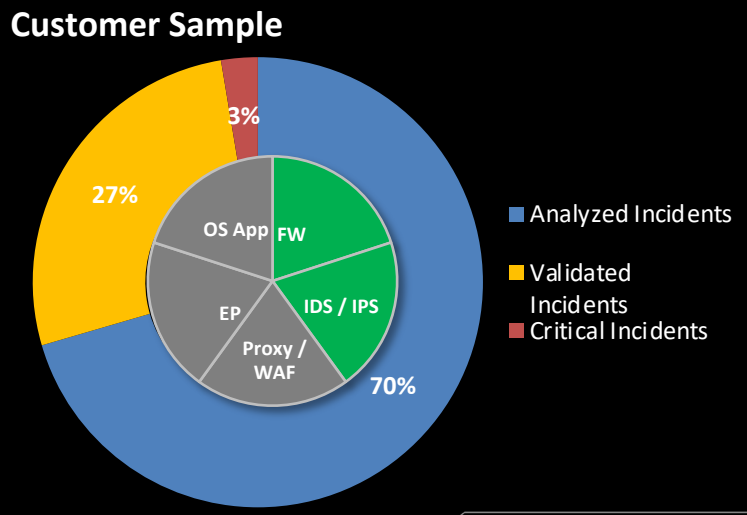
Desktops

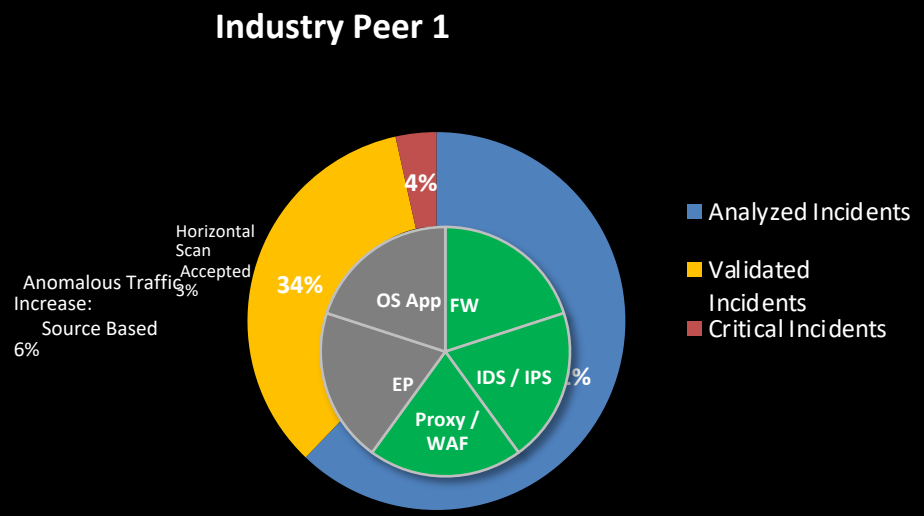
- Network
- Server
- Endpoint
- Data

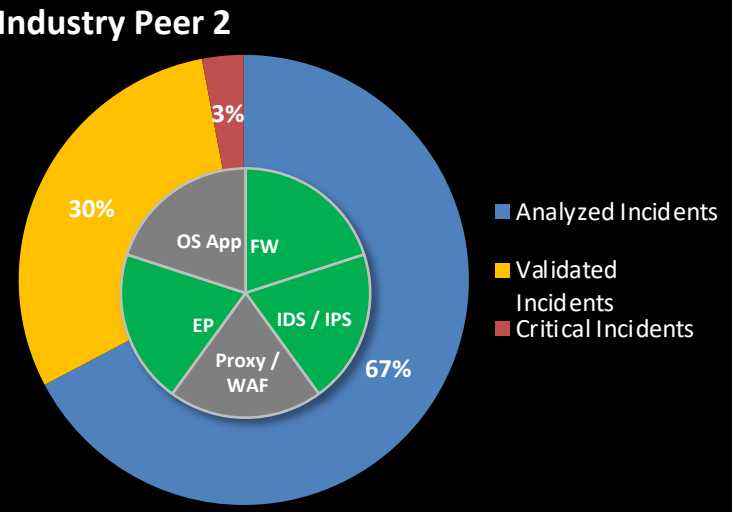
SOC 技術平台 - 分析模組

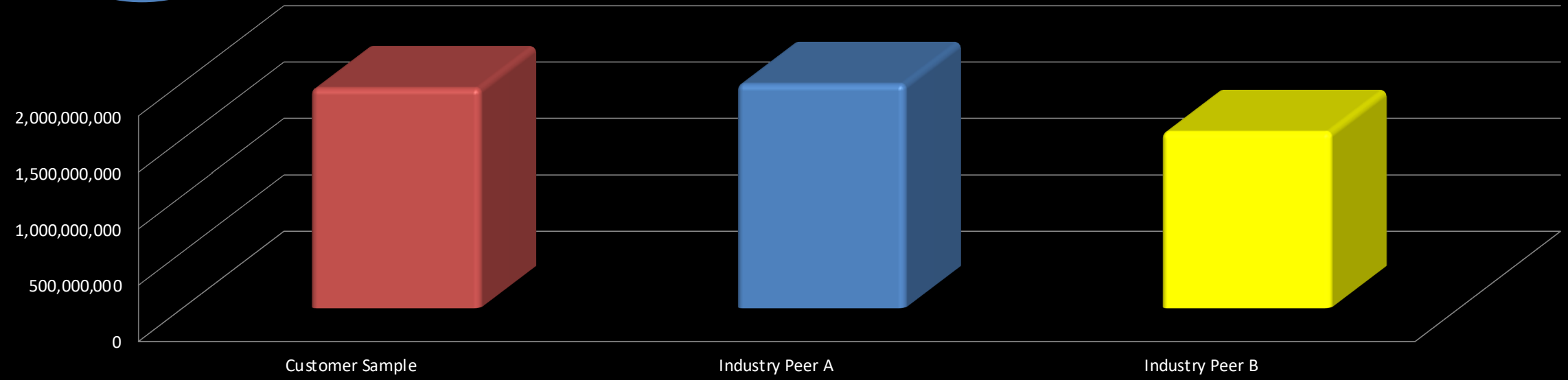


同產業安全係數評比









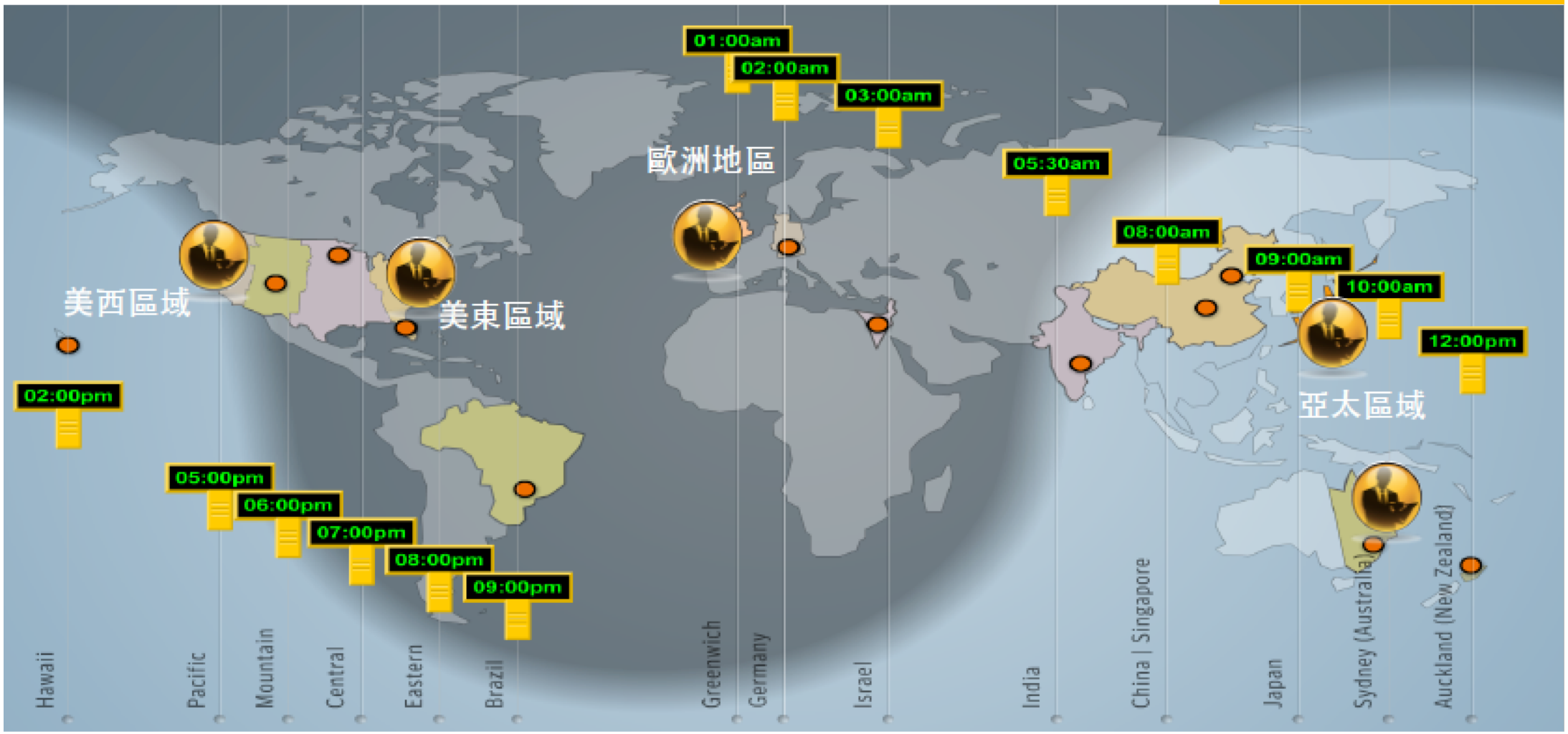
事後防護 – 事件鑑識與分析

事件處理類型

- APT 攻擊
  - 魚叉式網路釣魚攻擊（Spear Phishing Attacks）
  - 水坑式攻擊（Watering Hole Attacks）
- 網站入侵調查
  - 網頁置換
  - 網站開始寄送垃圾郵件
  - 網站加入DDOS攻擊
- 網路入侵調查
  - 網路出現可疑流量
- 一般電腦入侵調查
  - 垃圾郵件攻擊
  - 病毒入侵
- 殭屍網路偵辦
- 新型變種病毒偵測
- 電腦病毒感染入侵指標（IOC）
- 入侵來源分析
- 第二層潛在攻擊分析
- 其他

賽門鐵克事件處理團隊

7 X 24 全球監控



其他事件服務項目

事件處理計畫發展

- 事件處理計畫需求及現有情況差距分析
- 為主要事件客制事件處理流程及準則
- 定義事件處理團隊任務及職責
- 事件處理團隊能力編制
- 溝通流程及通報程序

事件處理團隊訓練

- 事件處理團隊能力評鑑
- 記憶體鑑識
- 網路鑑識
- 系統鑑識 及 現場處理
- 事件最佳處理方式
  - 資料取證
  - 保護證據連續性

事件處理靜態演練

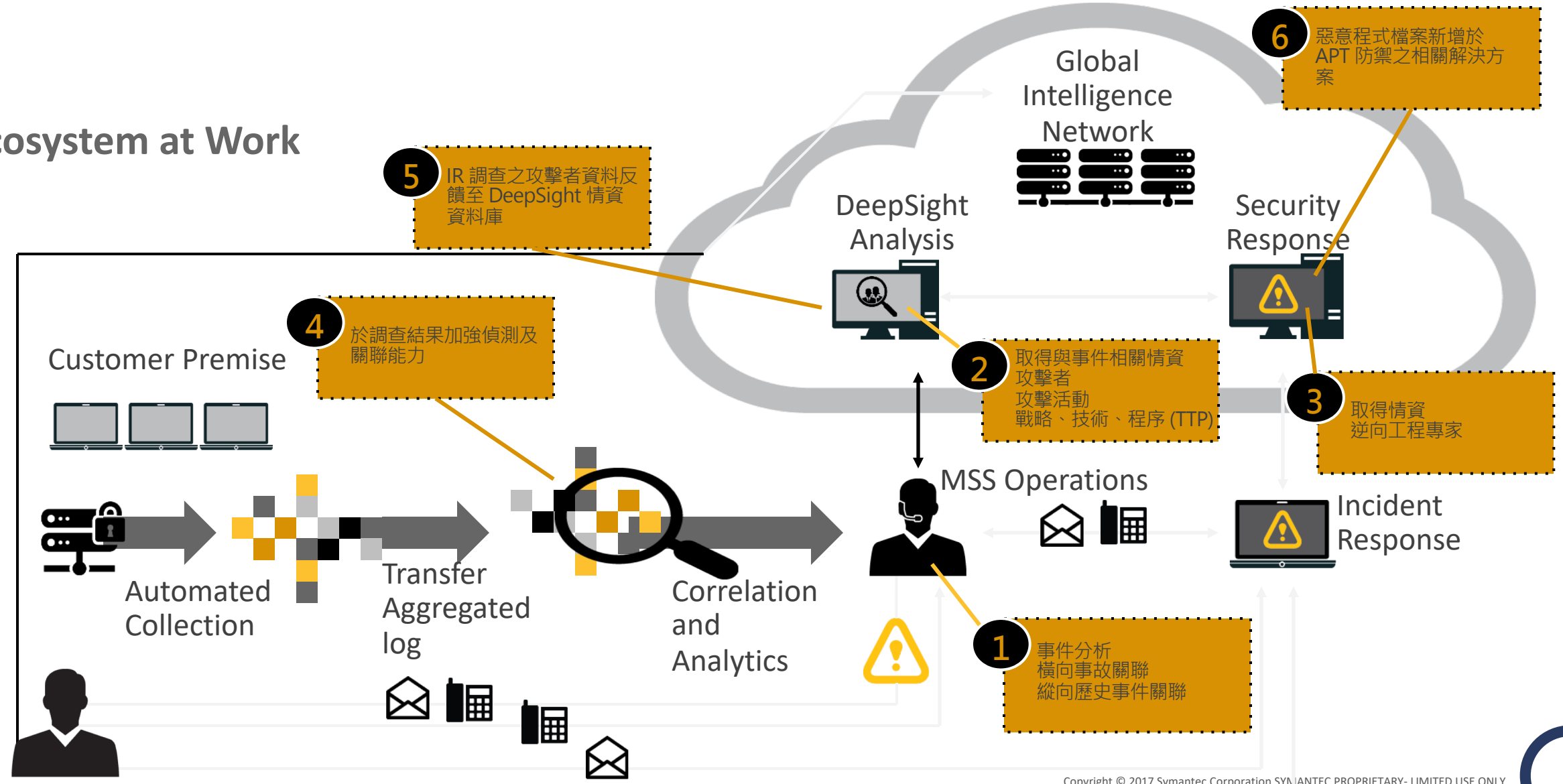
- 事件處理計畫評估
  - 計劃是否有效
  - 事件處理團隊是否有能力執行
- 事件處理團隊培訓
- 鑑定計劃與現有情況差距
- 鑑定事件處理需強化領域

進階威脅搜索 (APT Hunting)

- 採用最新資安情資搜索被入侵的跡象
- 深層系統及網路資料分析，搜索潛在被入侵的跡象
- 詳盡的搜索報告，包含搜索發現事項，資安強化建議
- 如果確定被入侵，可迅速提供事件處理服務

Cyber Security Services

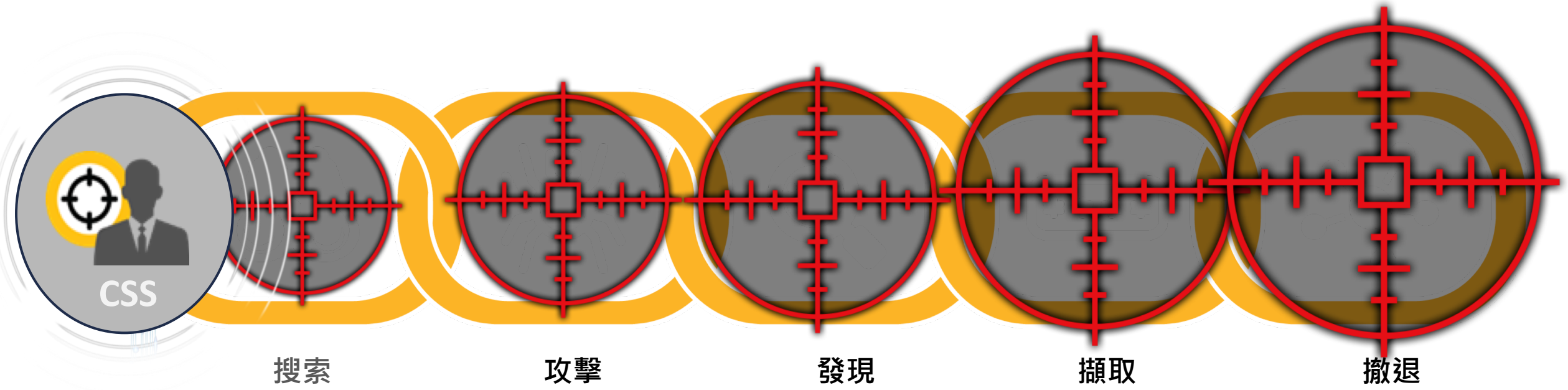
Ecosystem at Work



ATTACK CHAIN

搜索 攻擊 發現 擷取 撤退

KILL CHAIN



事前 Secure Infra + Security Consultant

事中 Managed Security Services

事後 Incident Response

技能強化 Security Simulation Services

Symantec™

Thank You!