威脅情報與網路可視性

Threat Intelligence and Network Visibility

Security Threat

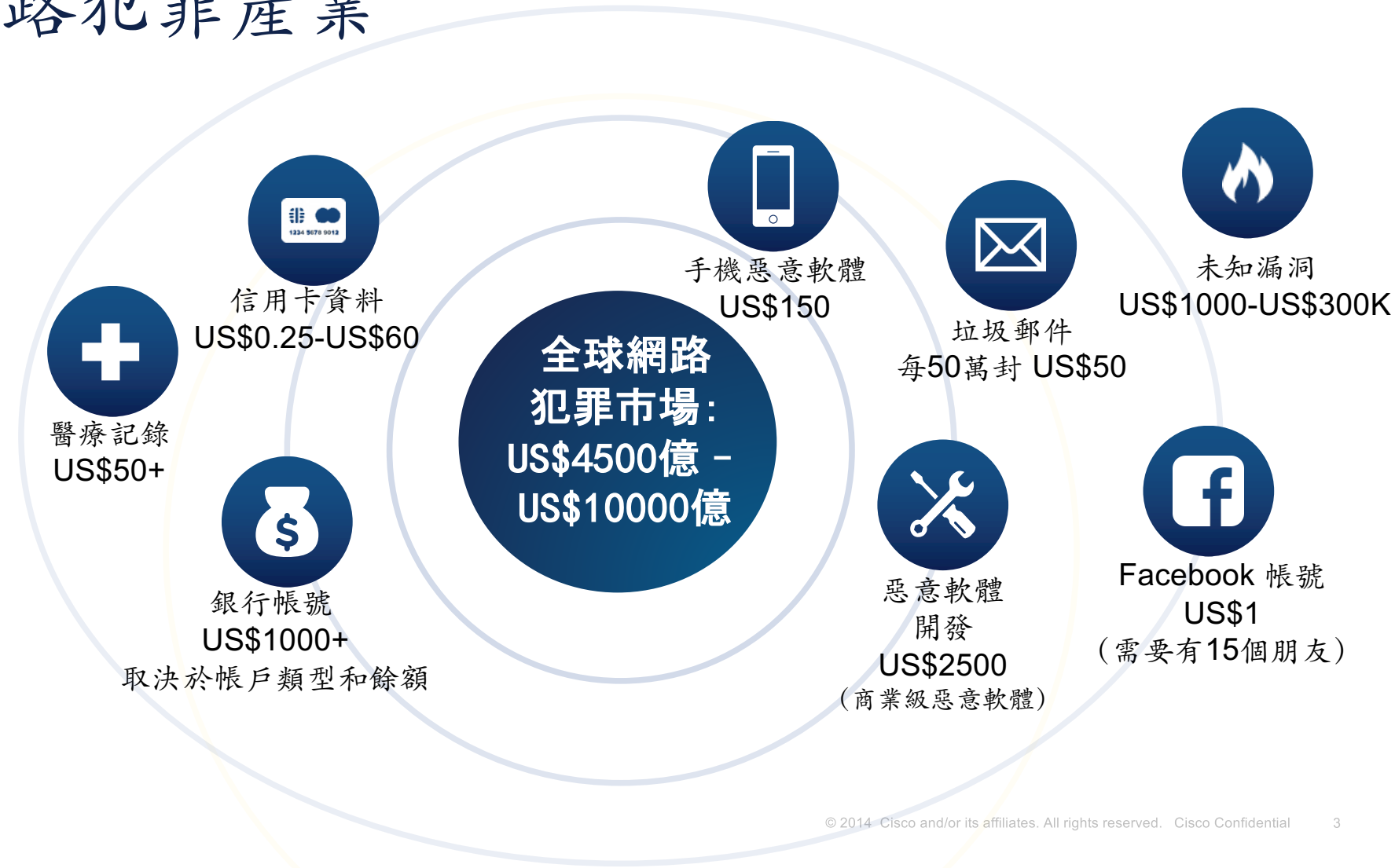
C. K. Lin (林傳凱)

大中華區安全事業部資深技術顧問

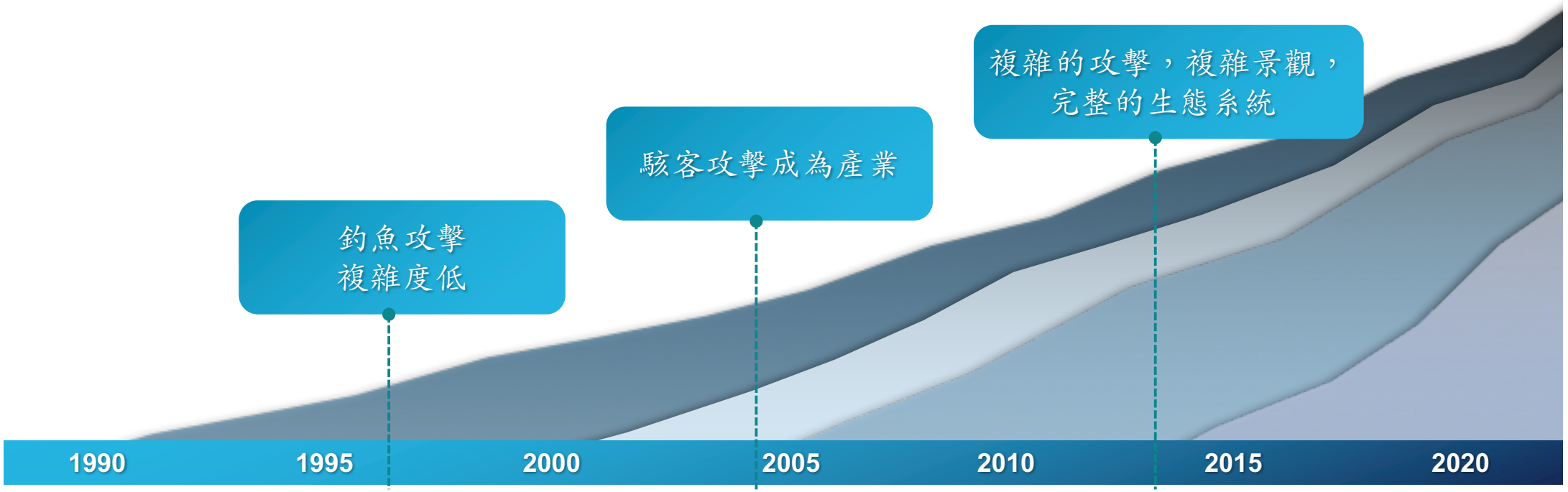
Dec. 22, 2017

威脅情報 – Cisco TALOS

全球網路犯罪產業

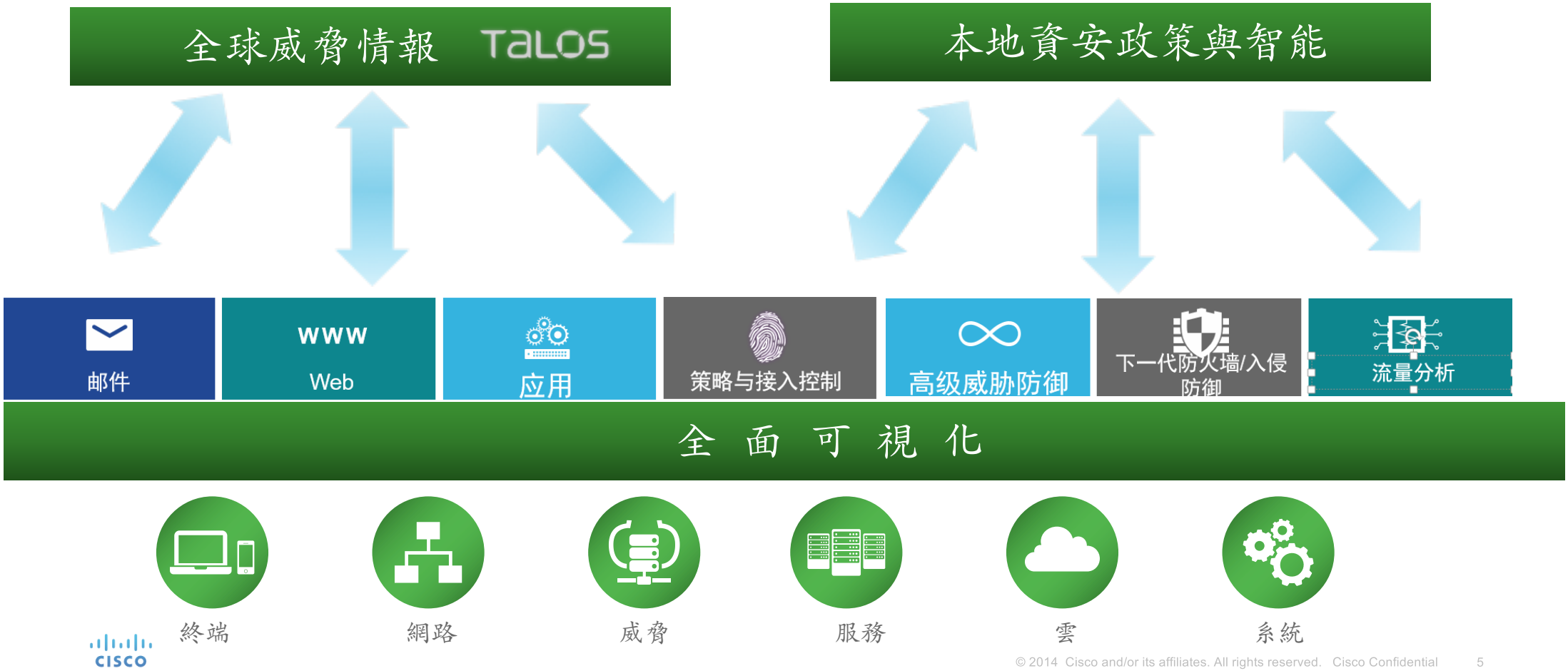


網路犯罪的產業化

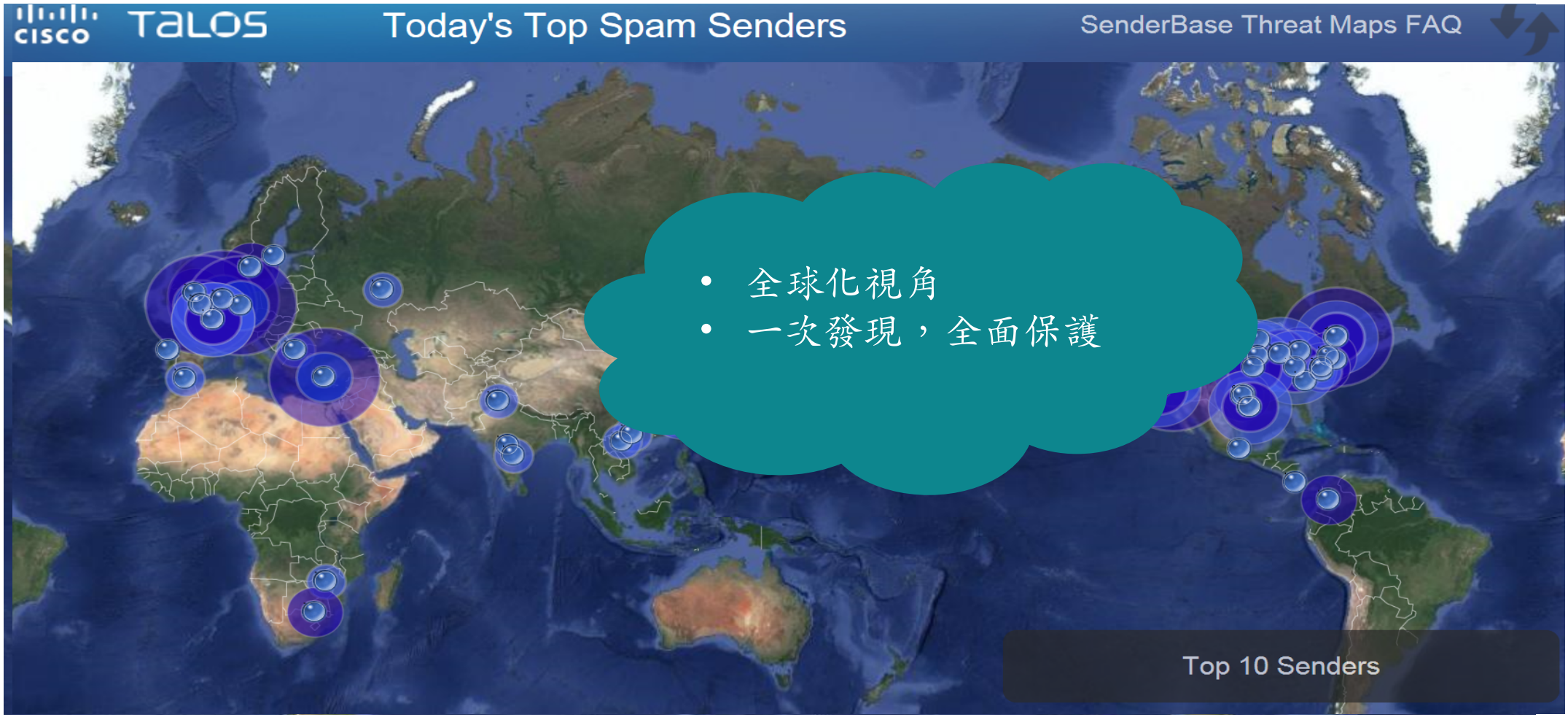


重要的問題不是你“是否”會被攻擊，而是“什麼時候”會被攻破？

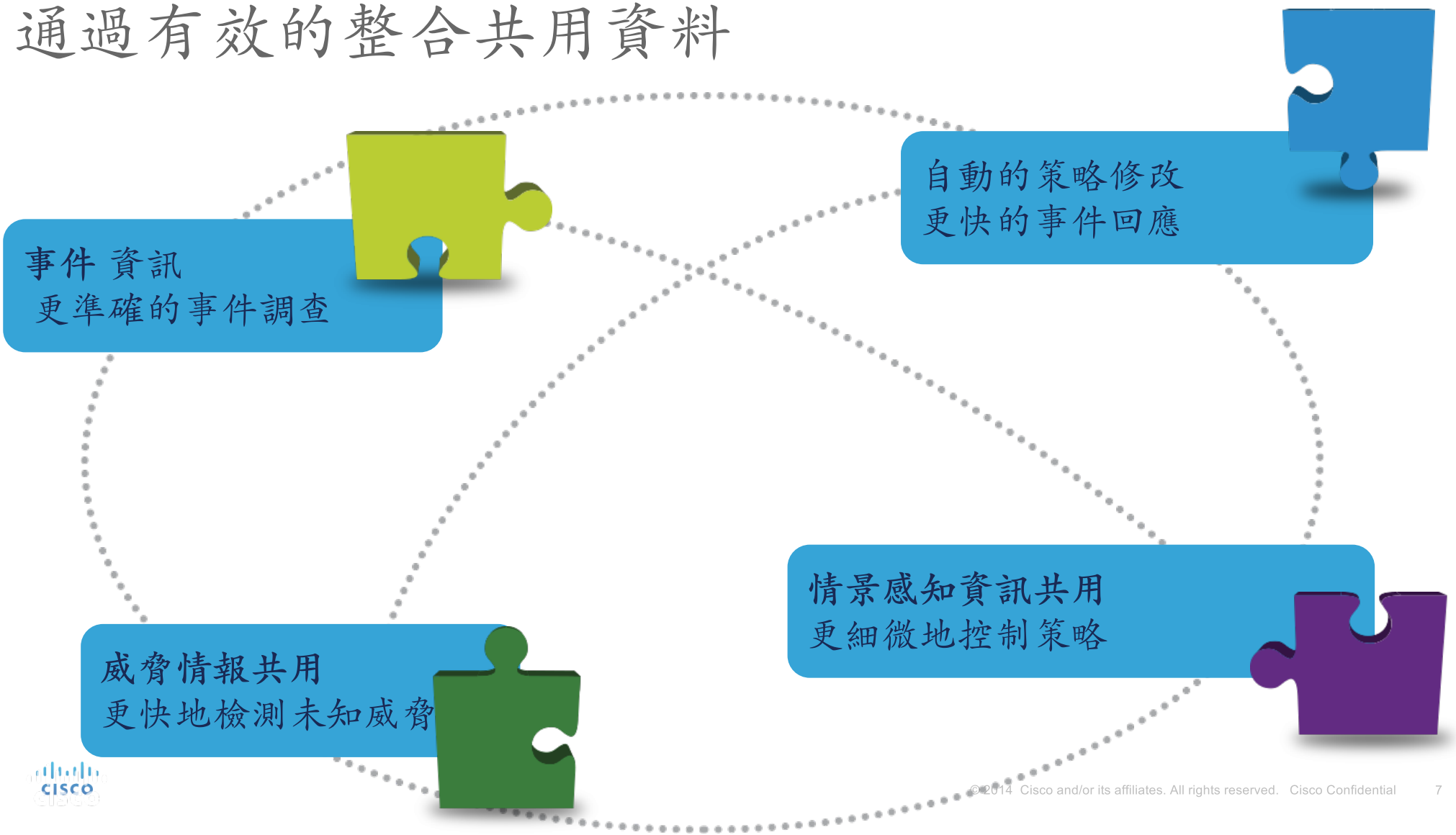
安全能力：可視性是基礎/資安情報是智慧



關鍵點：全球化的安全情報



通過有效的整合共用資料



思科把握正確方向，不斷縮短侵入檢測時間（TTD）

2016 年 TTD 為 14 小時

可見性為基礎，連續的安全能力設計

資訊共用，高效防禦的架構設計

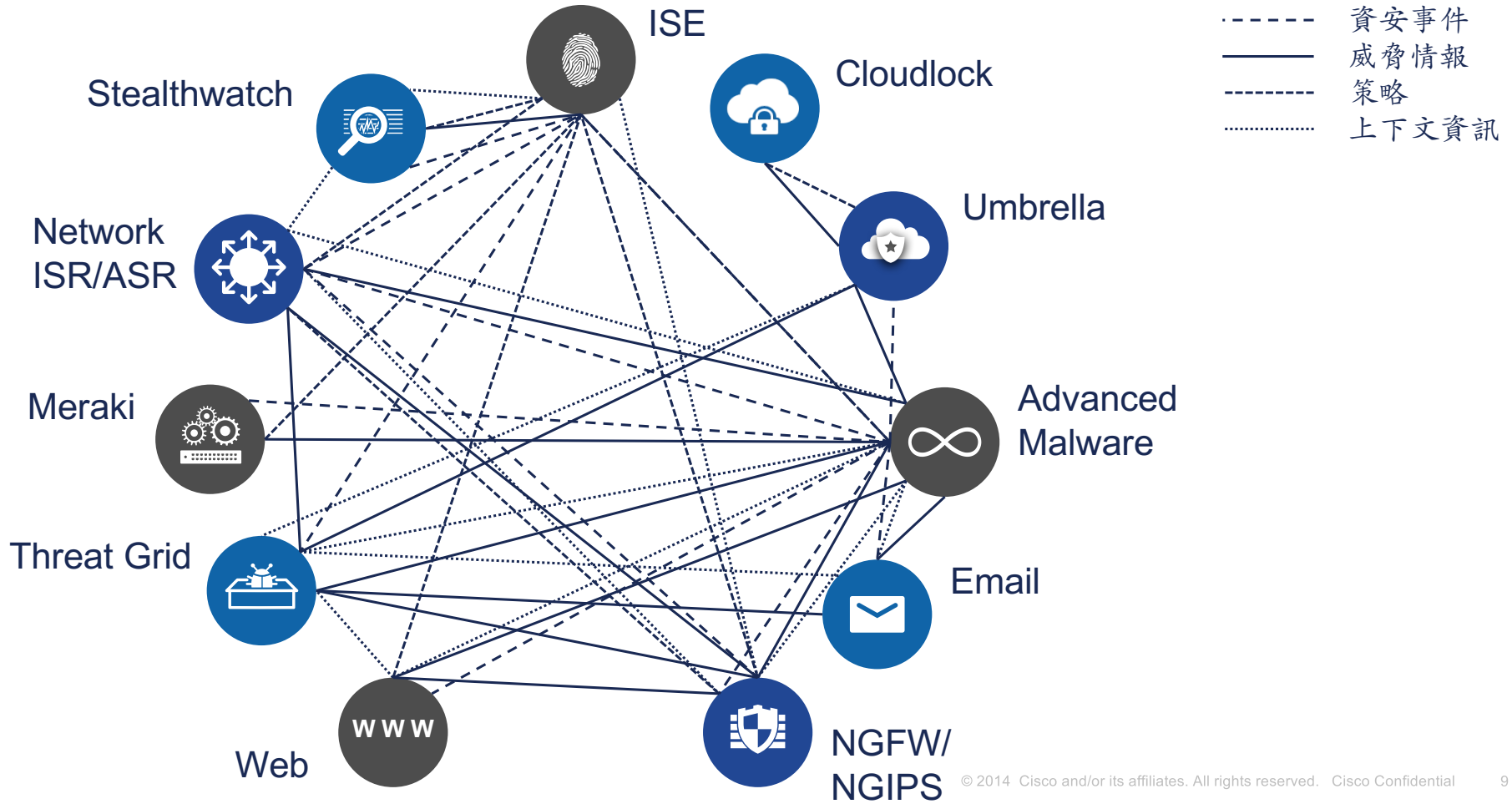
基於最佳實踐的部署設計

3.5 小時
2017 年 5 月

cisco

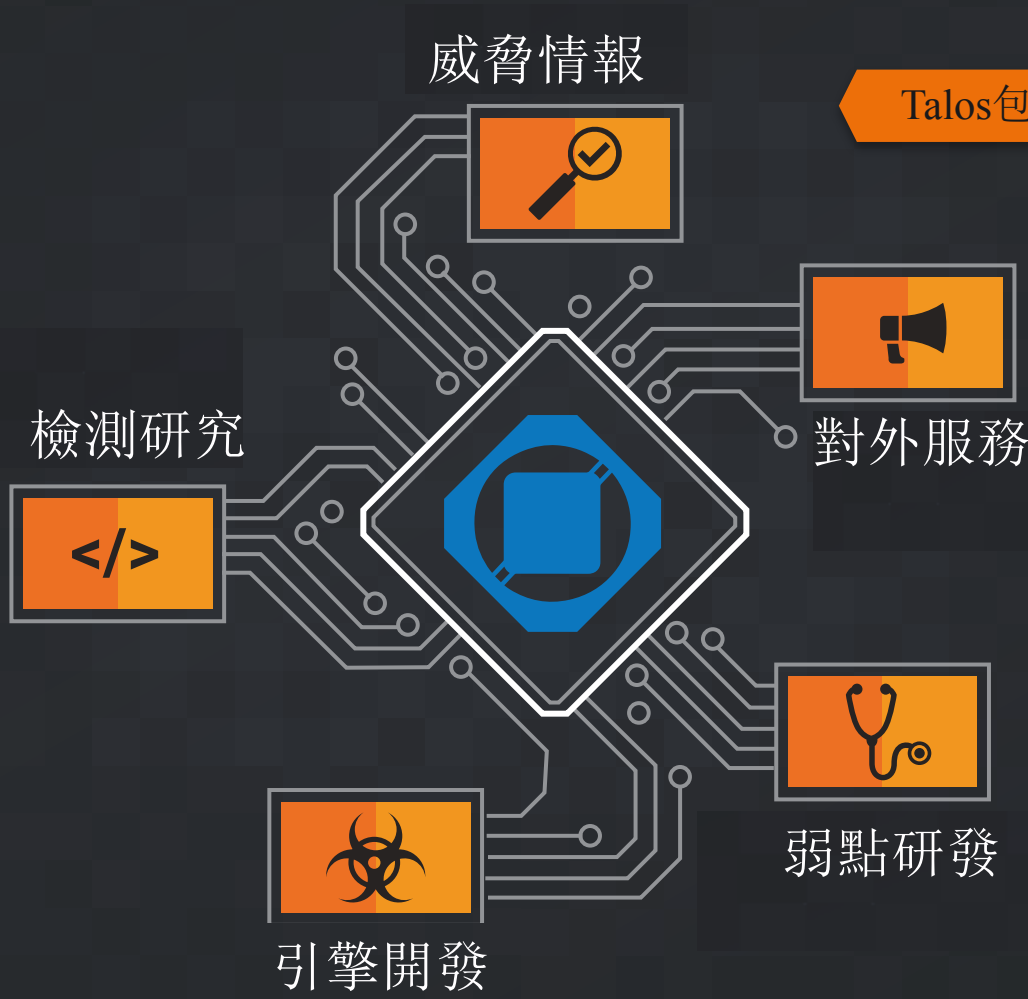
*思科 AMP 數據（思科 2017 年年中網路安全報告）

共用資訊才能達到更有效的資訊安全



Talos骨幹團隊

Talos包括5個團隊：



TALOS

TALOS情報類型細分

威脅情報

150萬
每天的惡意程式樣本數量

6000億
每天的電子郵件資訊數量

160億
每天的網頁請求數量

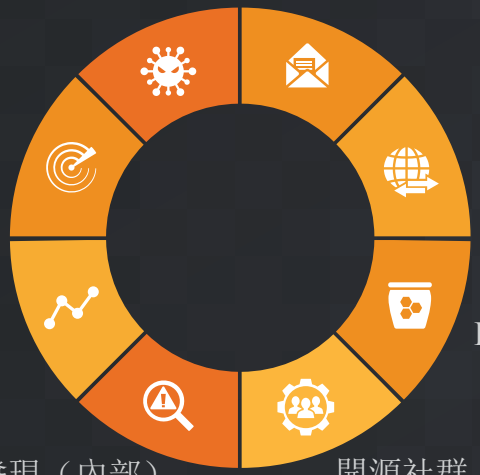
Honeypot蜜罐技術

開源社群

弱點發現（內部）

遙測資料

對整個網際網路的掃描



情報共用

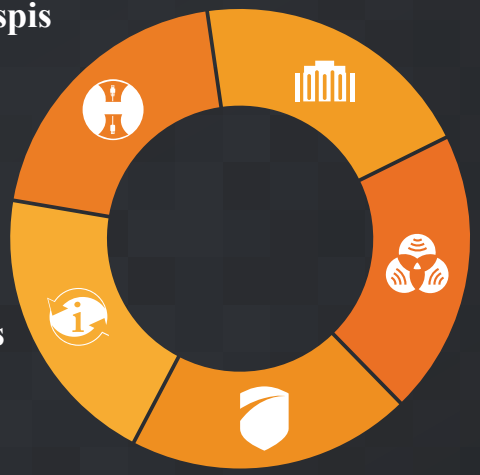
Aspis

Crete

AEGIS

協力廠商程式（MAPP）

ISACs



超過250名
全職威脅情報研究人員

上百萬個
遙測代理

4個全球資料中心

超過100家
威脅情報合作夥伴

1100個
威脅捕獲程式

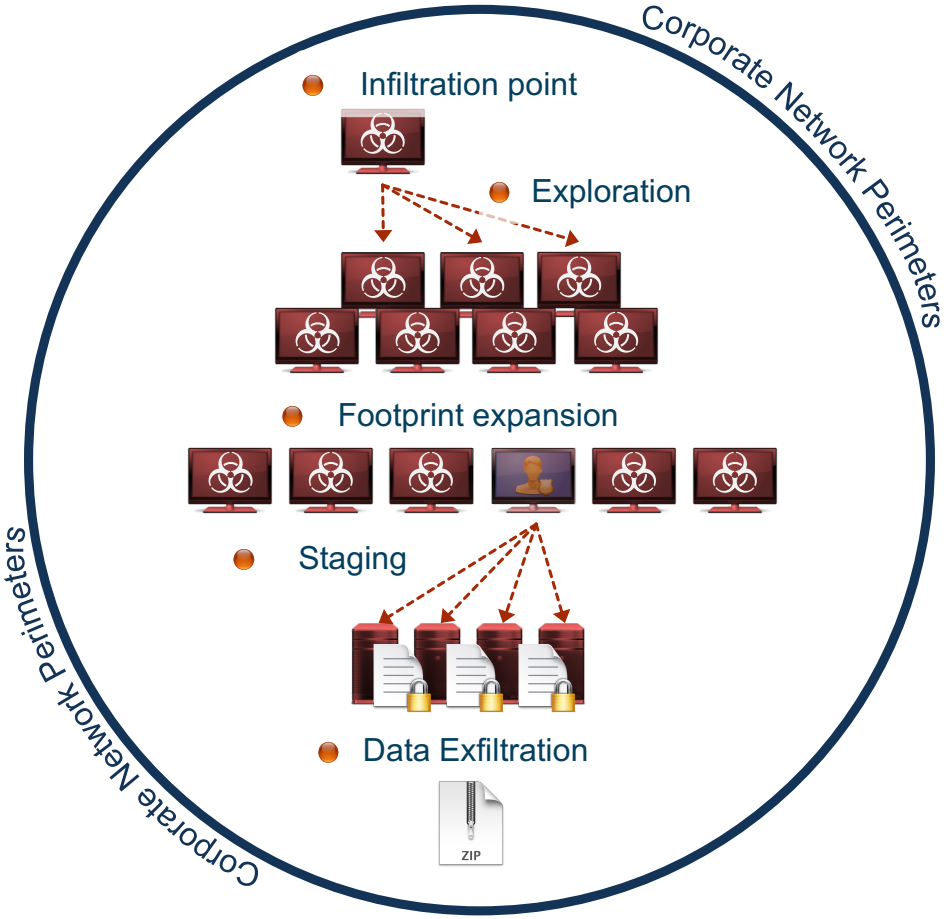
網路可視性
– Cisco StealthWatch + ETA

剖析資料洩漏流程

- Target acquisition

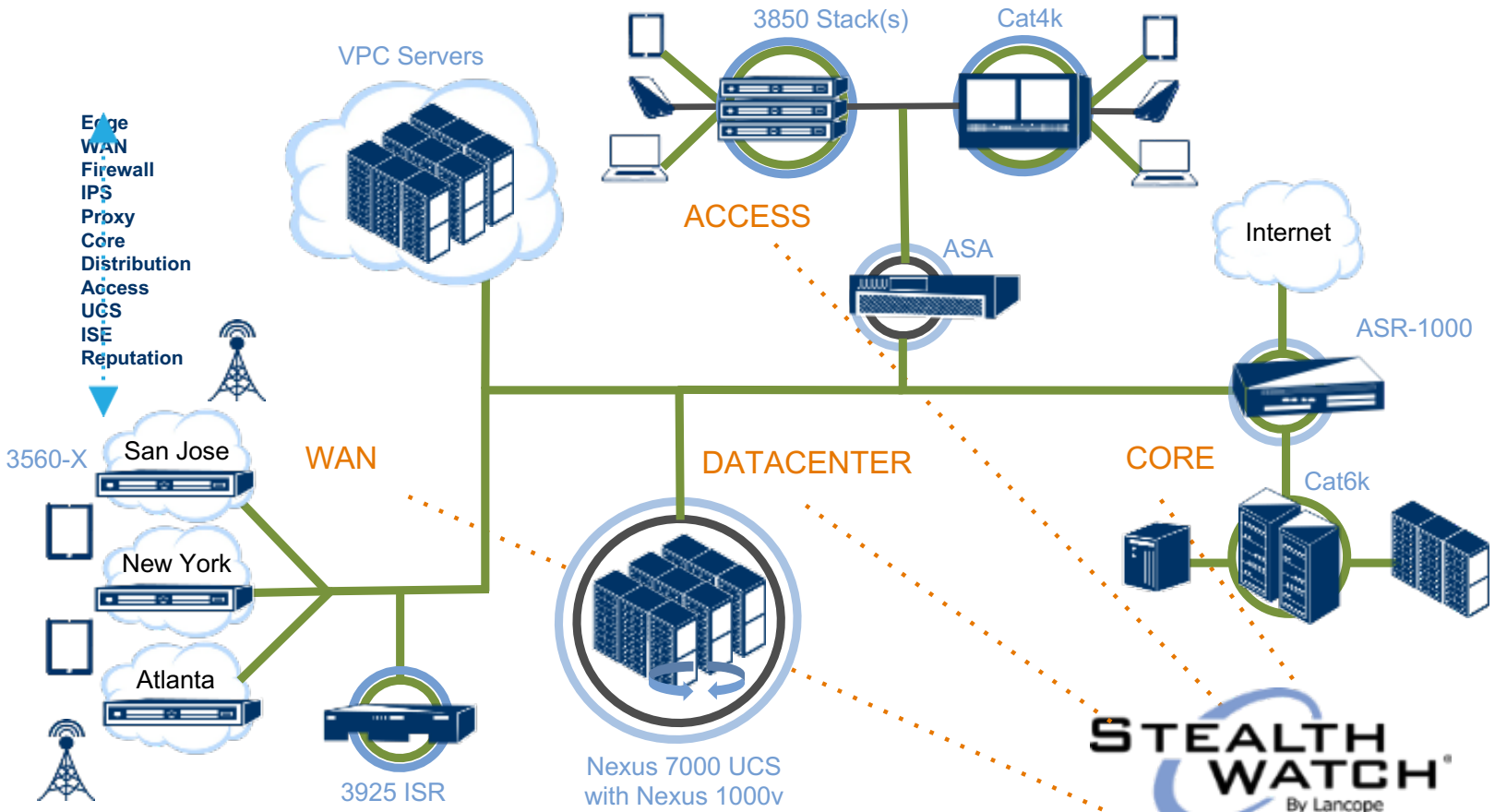
Reconnaissance

- Information monetized after breach



當你看不見攻擊的時候，肯定無法保護自己

Internal Visibility from Edge to Access, **Network Is Your Sensor**



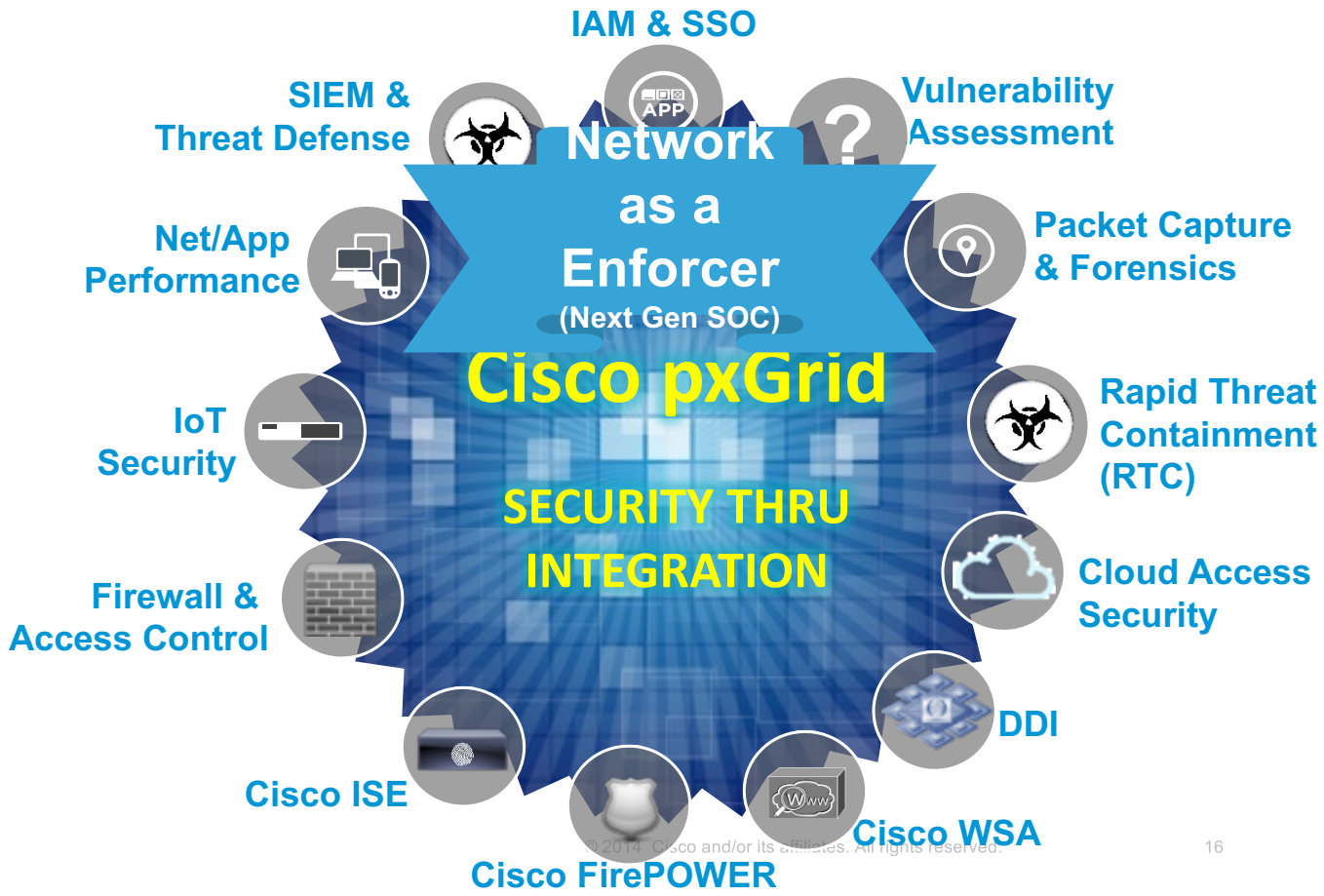
可視性 ≠ SIEM

Network as a Sensor
(Next-Gen SOC)

- **Logs**
  - CEF? LEEF? Free App?
  - Latest version of security devices? Customized parser?
  - All fields? Uncovered logs?
  - License? Performance?
- **Use Cases**
  - Compromise cases
  - What kind of the logs
  - Dashboards/Reports
  - Correlation rules
  - Professional services
  - APT

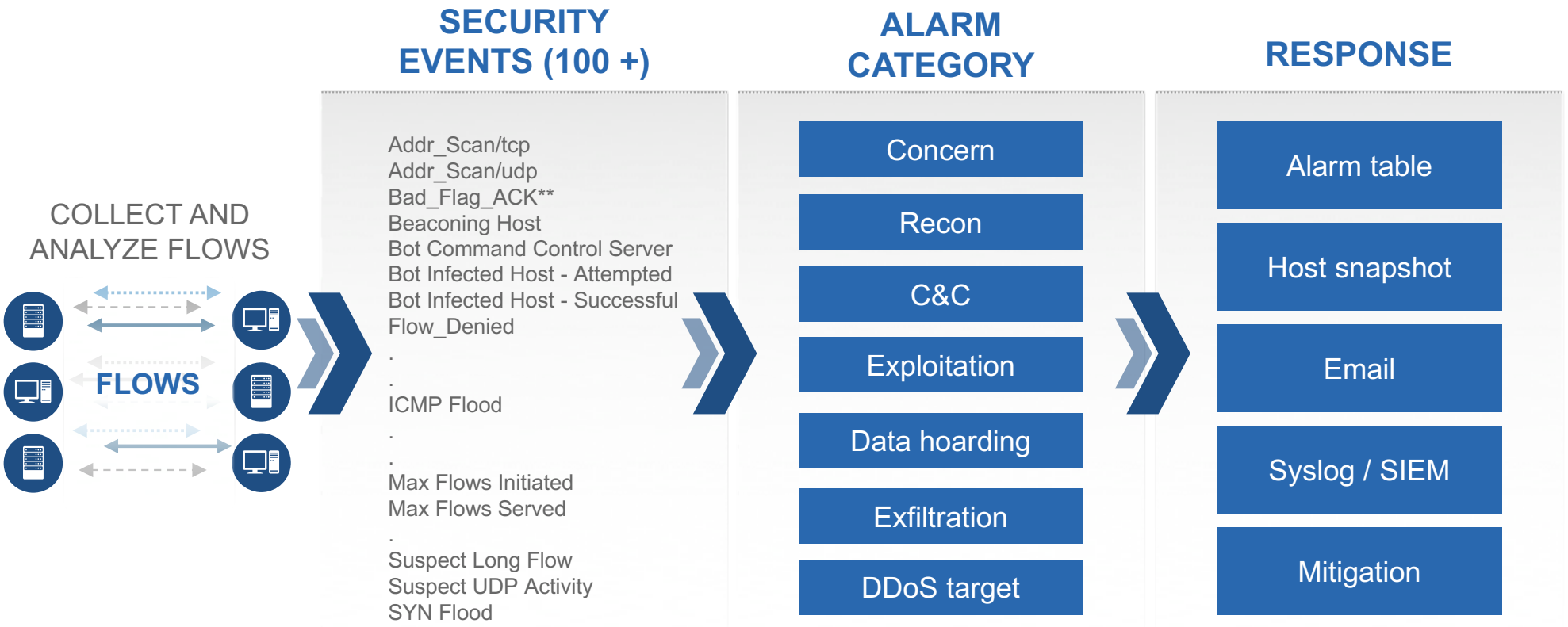
Alarm vs. Response – 資安聯防

- **Response**
  - IPS? FireWall?
  - API
  - In-line



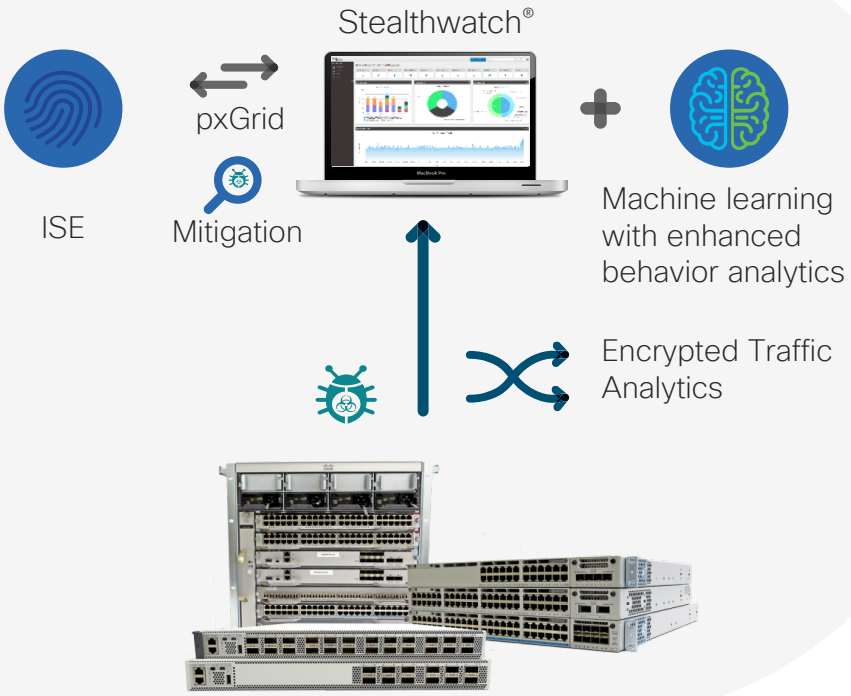
Behavioral and Anomaly Detection Model

Behavioral Algorithms Are Applied to Build “Security Events”

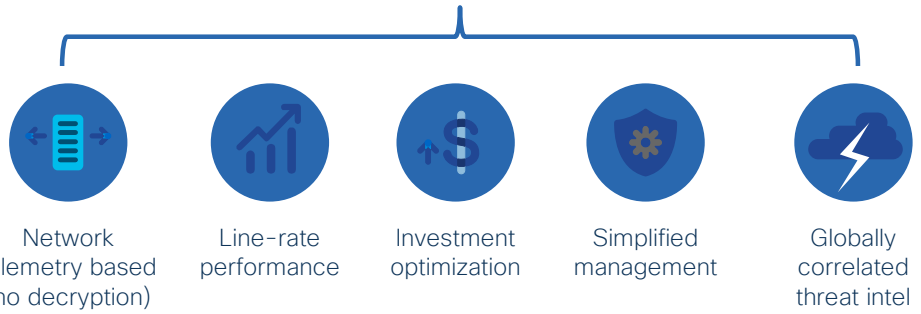


Cisco Catalyst 9000 系列結合ETA (Encrypted Traffic Analytics)升級網路可視性

Rapidly mitigate malware and vulnerabilities in encrypted traffic



- Industry's most pervasively deployable solution for Encrypted Traffic Analytics
- Complements other encrypted traffic management solutions




CISCO
TOMORROW starts here.