



威脅情報與網路可視性

Threat Intelligence and Network Visibility

Security Threat

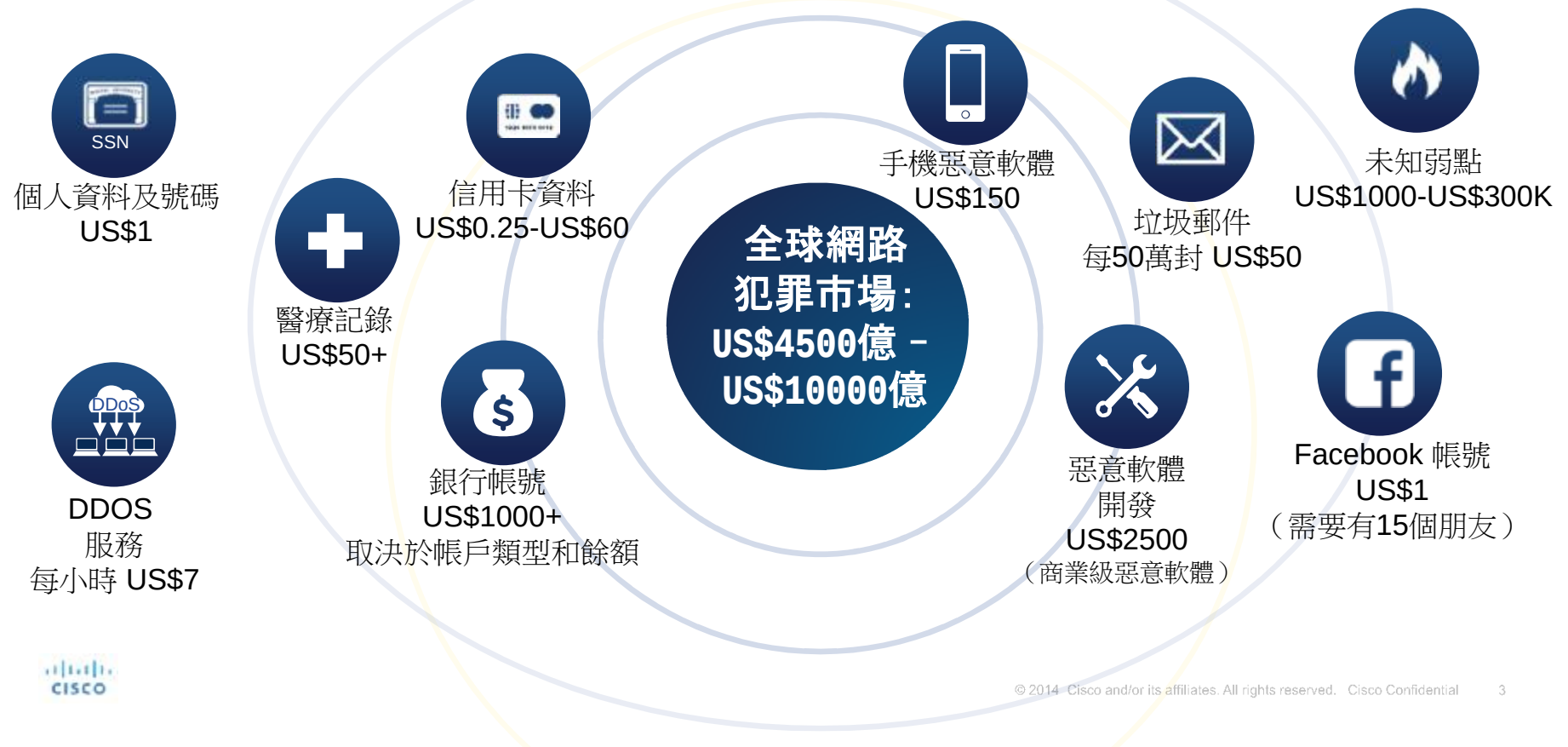
C. K. Lin (林傳凱)

大中華區安全事業部資深技術顧問

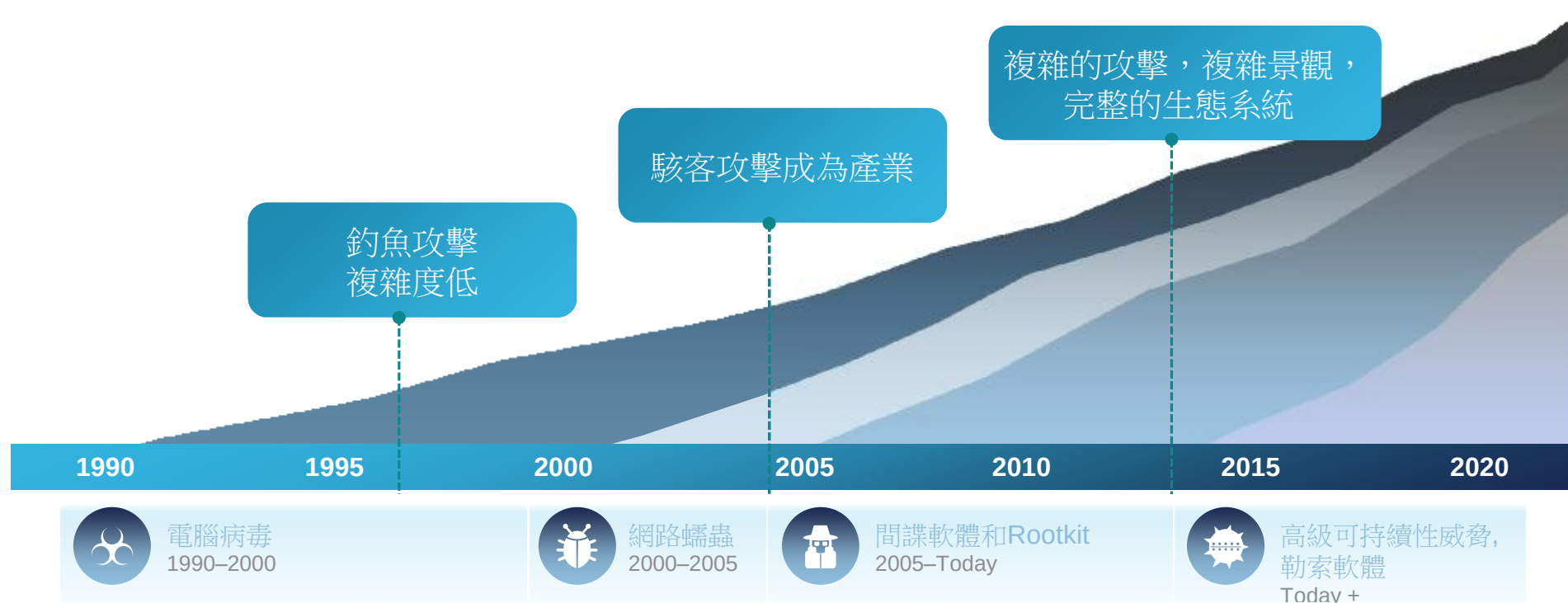
Mar. 23, 2018

威脅情報 – Cisco TALOS

全球網路犯罪產業

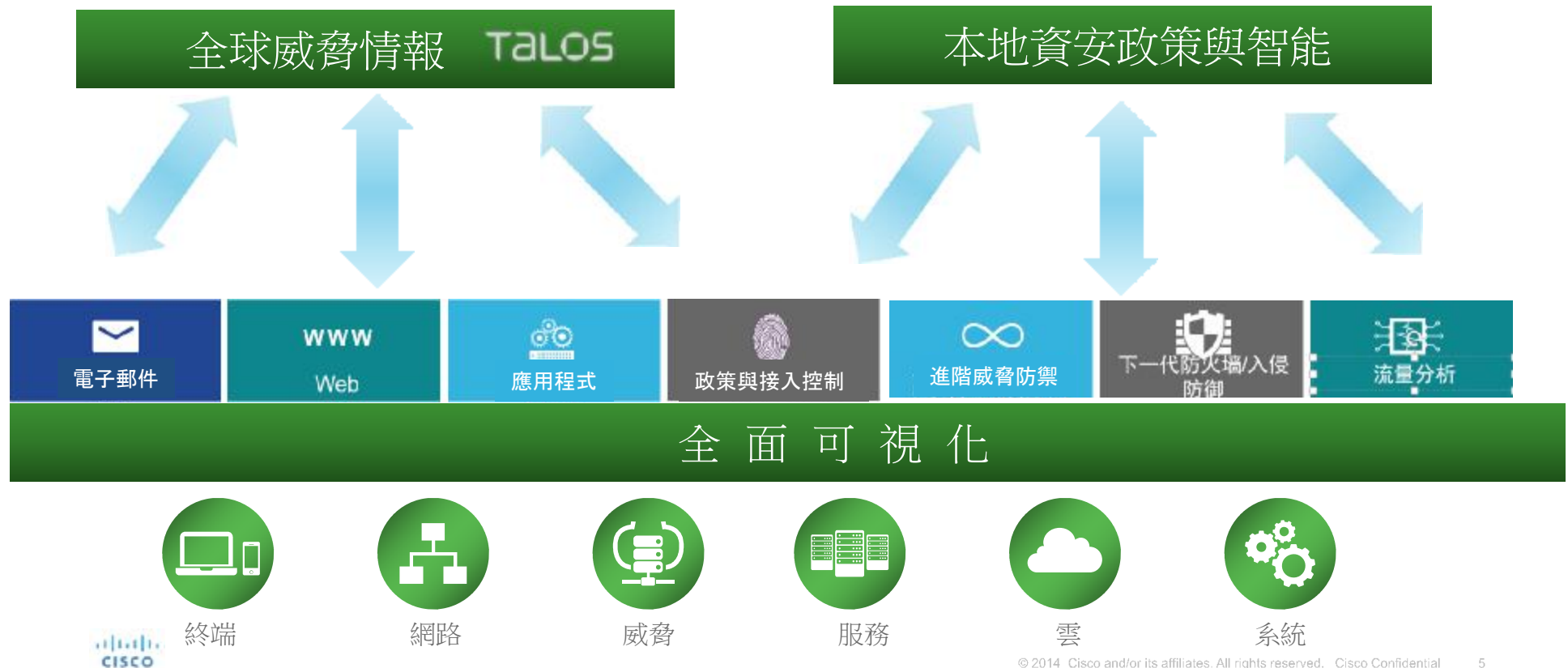


網路犯罪的產業化



重要的問題不是你 “是否” 會被攻擊，而是 “什麼時候” 會被攻破？

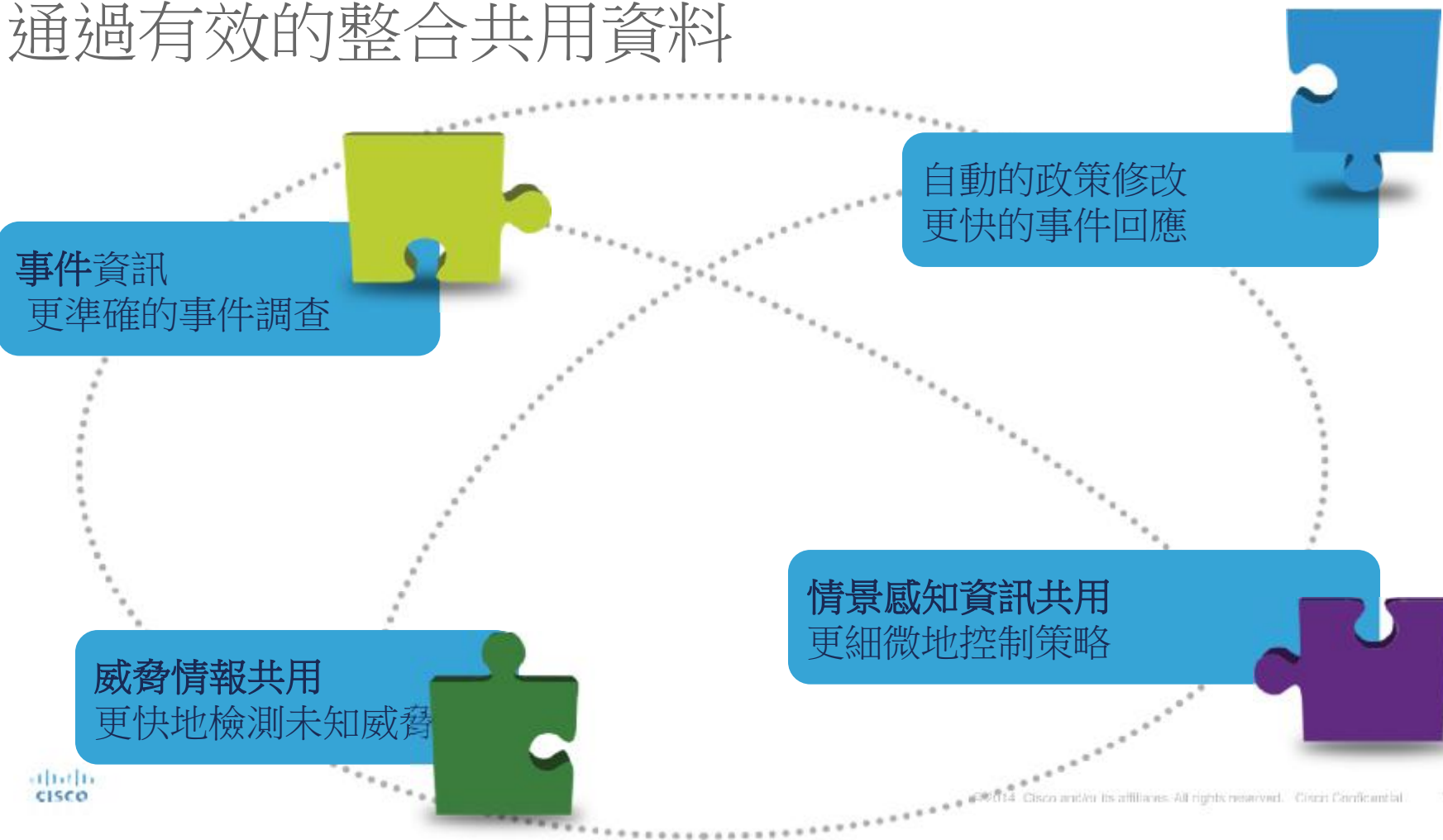
資安能力：可視性是基礎/資安情報是智慧



關鍵點：全球化的資安情報



通過有效的整合共用資料



事件資訊
更準確的事件調查

自動的政策修改
更快的事件回應

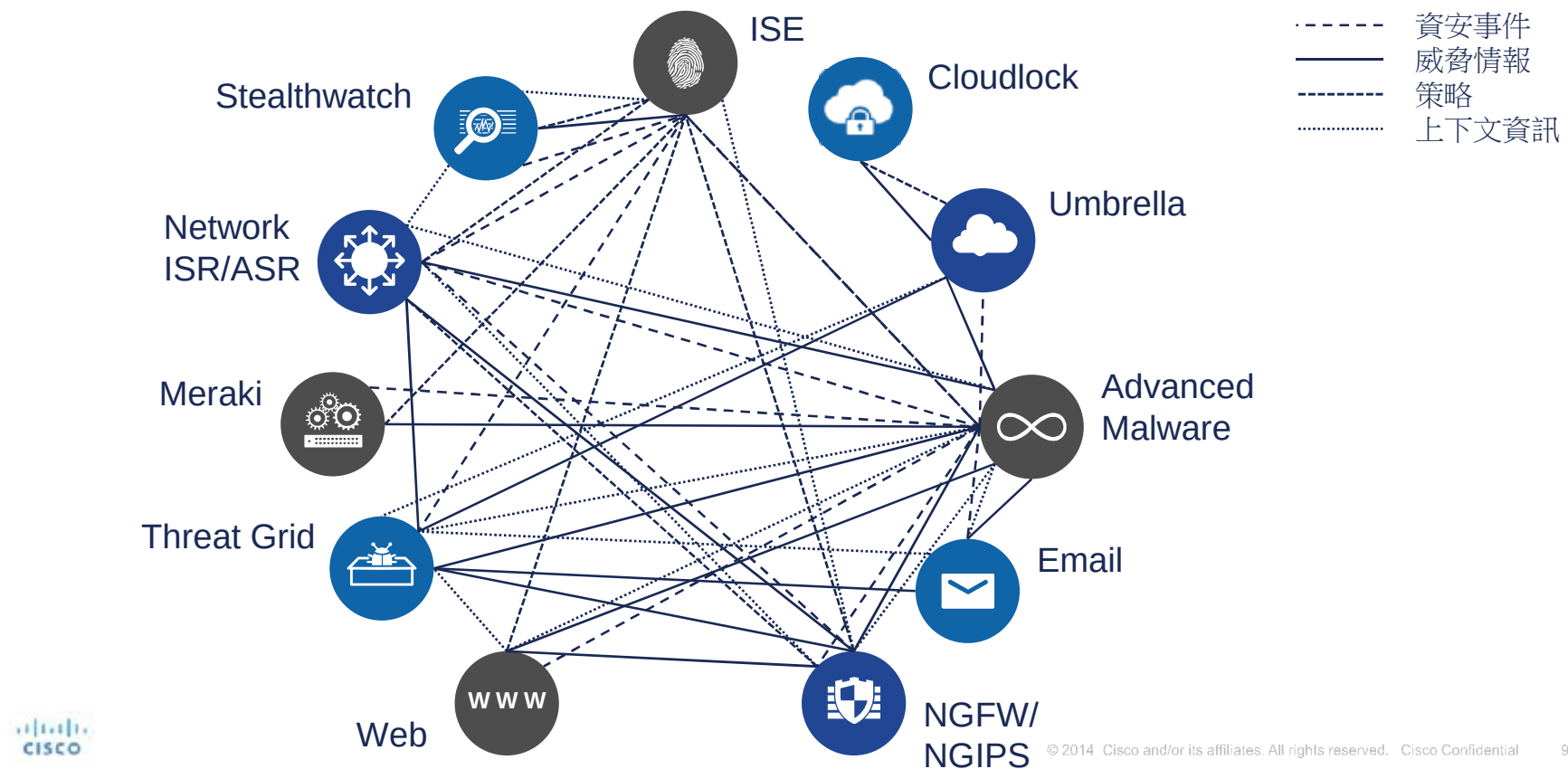
威脅情報共用
更快地檢測未知威脅

情景感知資訊共用
更細微地控制策略

思科把握正確方向，不斷縮短入侵檢測時間（TTD）



共享資訊才能達到更有效的資訊安全



Timeline of 'WannaCry' Ransomware Defense



Microsoft Security Bulletin March 14th, 2017

On March 14th, Microsoft released a patch (MS17-010) for a new SMB vulnerability.

Cisco NGFW | Meraki MX March 14th, 2017

On the same day, Cisco Talos released Snort™ signature #41928 to detect vulnerabilities identified in MS17-010.

Shadow Brokers April 14th, 2017

A group known as "The Shadow Brokers" released a set of vulnerabilities allegedly sourced from the National Security Agency (NSA) that go by the names of Eternal Blue and Double Pulsar.

Cisco NGFW | Meraki MX April 25th, 2017

Talos releases Snort™ signatures #42325, #42332, #42340 for Double Pulsar and Anonymous SMB shares.

TALOS

Cisco TALOS

With more than 250 world class researchers around the globe and a global network of intelligence and data sources, Cisco continues to monitor, research, and protect customers against 'WannaCry' and other emerging threats.

Cisco Umbrella May 12th, 2017 | 10:12 UTC

Cisco Umbrella adds attribution of the attack type to ransomware and moves the kill switch domain to the malware category.

Cisco AMP May 12th, 2017 | 9:33 UTC

Approximately 50 minutes after the first seen samples, AMP detected the ransomware. Threat was detected via automatic analysis rules and low prevalence methods.

AMP successfully detected and blocked on endpoints, email and web gateways and network security.

Cisco Umbrella May 12th, 2017 | 7:43 UTC

Cisco Umbrella pushes kill switch domain globally into Newly Seen Domains categories which resulted in protection against the ransomware and spreading of the worm.

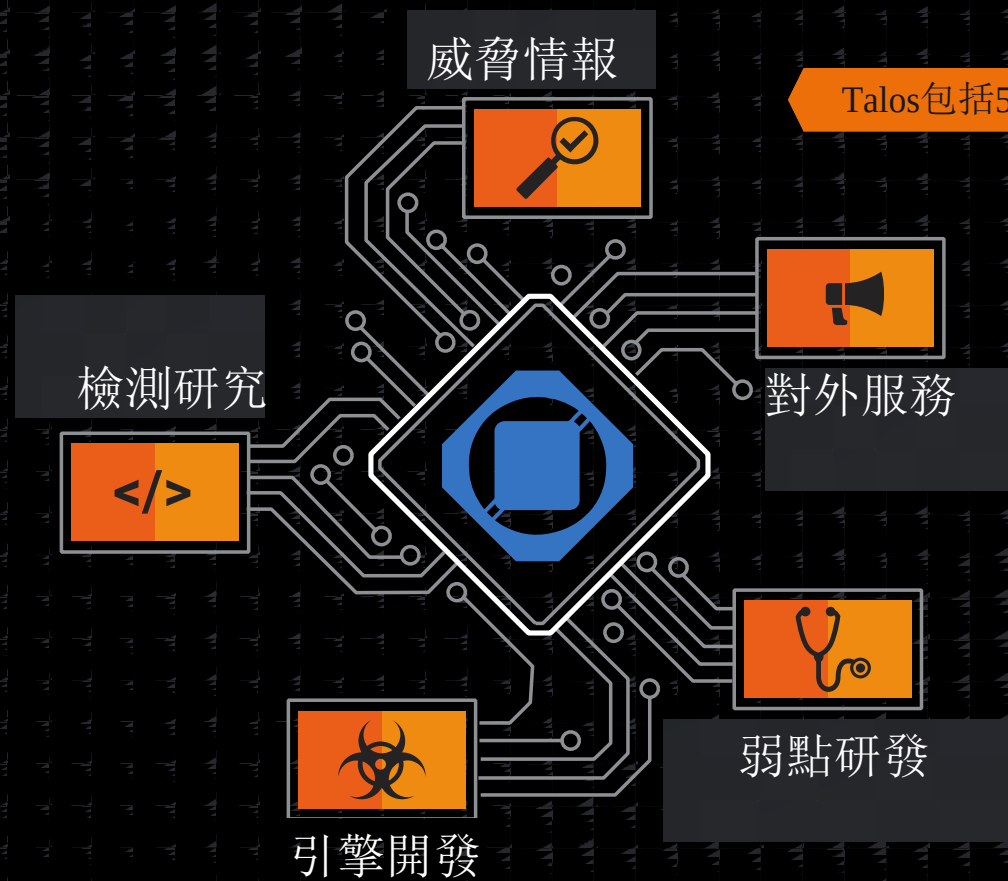
Cisco Investigate May 12th, 2017 | 7:30 UTC

@MalwareTechBlog releases information about a new attack dubbed 'WannaCry' on Twitter and his blog.

Cisco Investigate screenshot was included in the blog as it was used as a part of the intelligence collection and discovery.

For more information, please visit cisco.com and talosintelligence.com

Talos 骨幹團隊



Talos包括5個團隊：

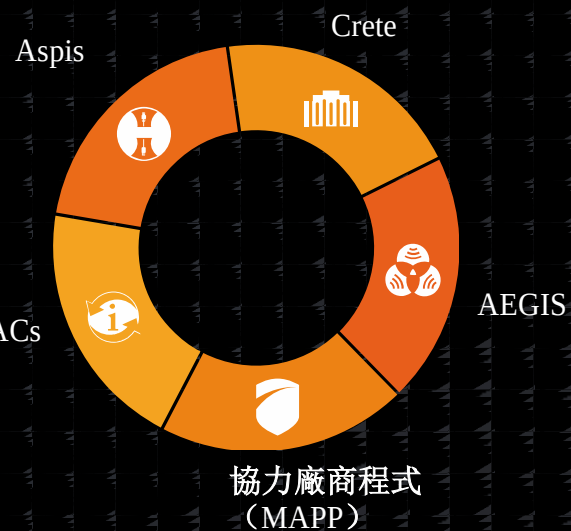
TALOS

TALOS 情報類型細分

威脅情報



情報共用



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

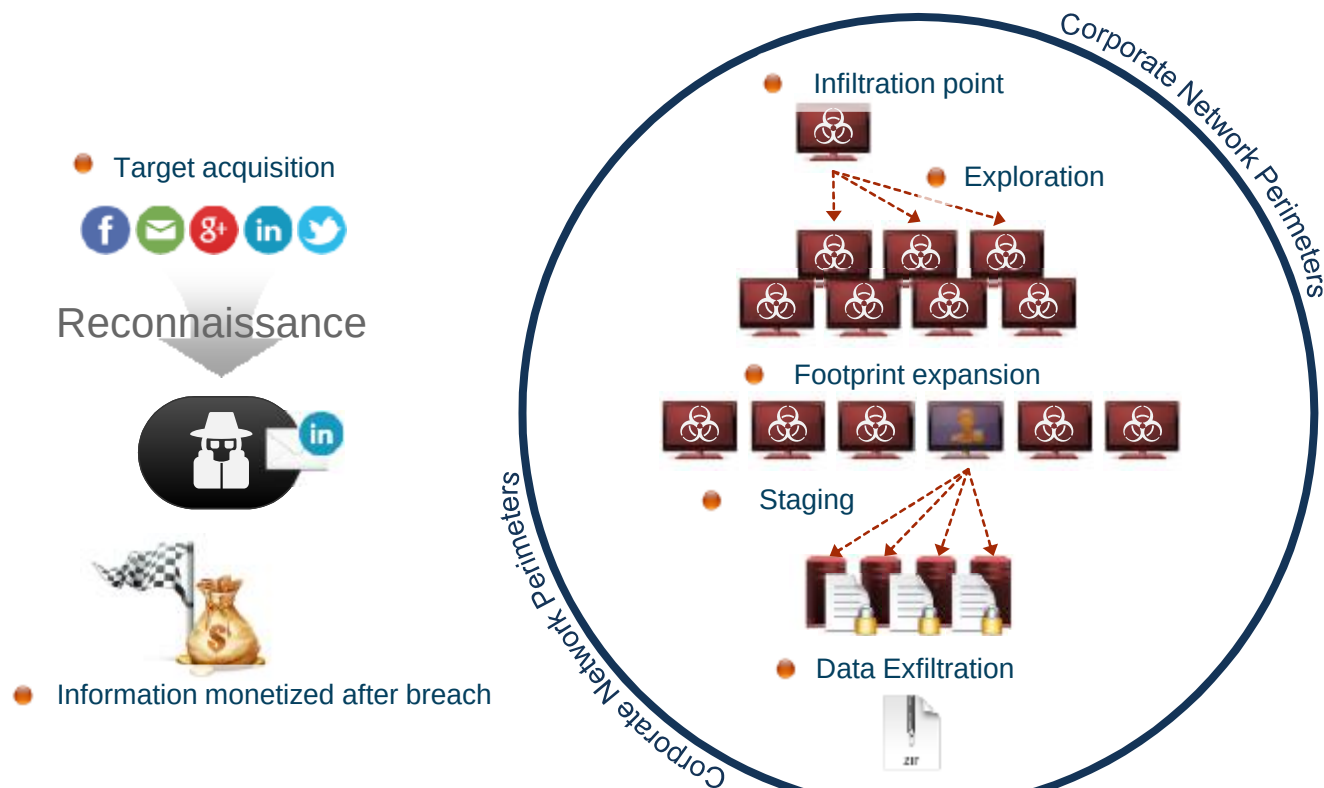


1100個
威脅捕獲程式

網路可視性

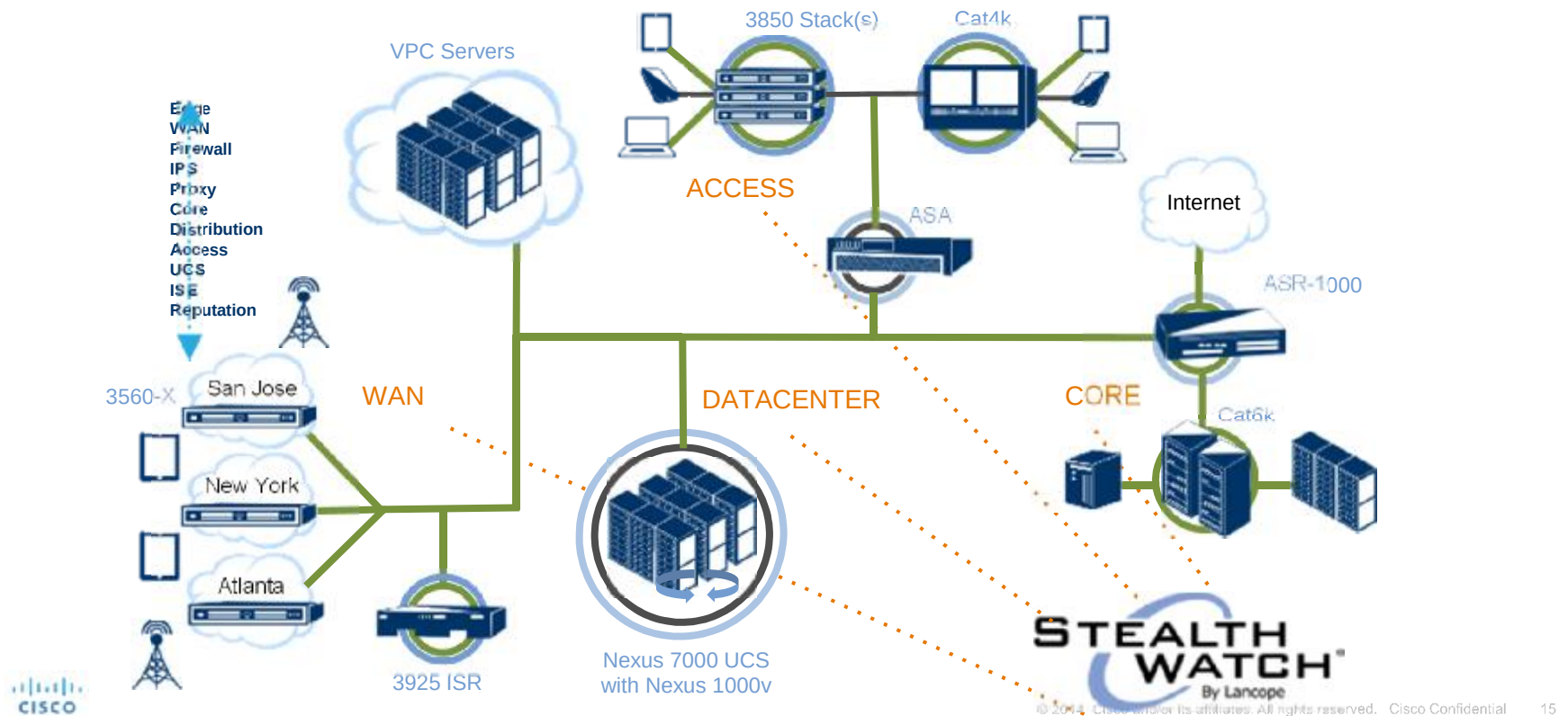
– Cisco StealthWatch + ETA

剖析資料洩漏流程



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 $\neq$ SIEM

- **Logs**

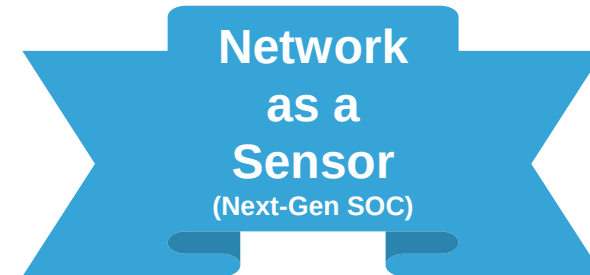
- CEF? LEEF? Free App?
- Latest version of security devices? Customized parser?
- All fields? Uncovered logs?
- License? Performance?

- **Use Cases**

- Compromise cases
- What kind of the logs
- Dashboards/Reports
- Correlation rules
- Professional services



APT



Alarm vs. Response – 資安聯防

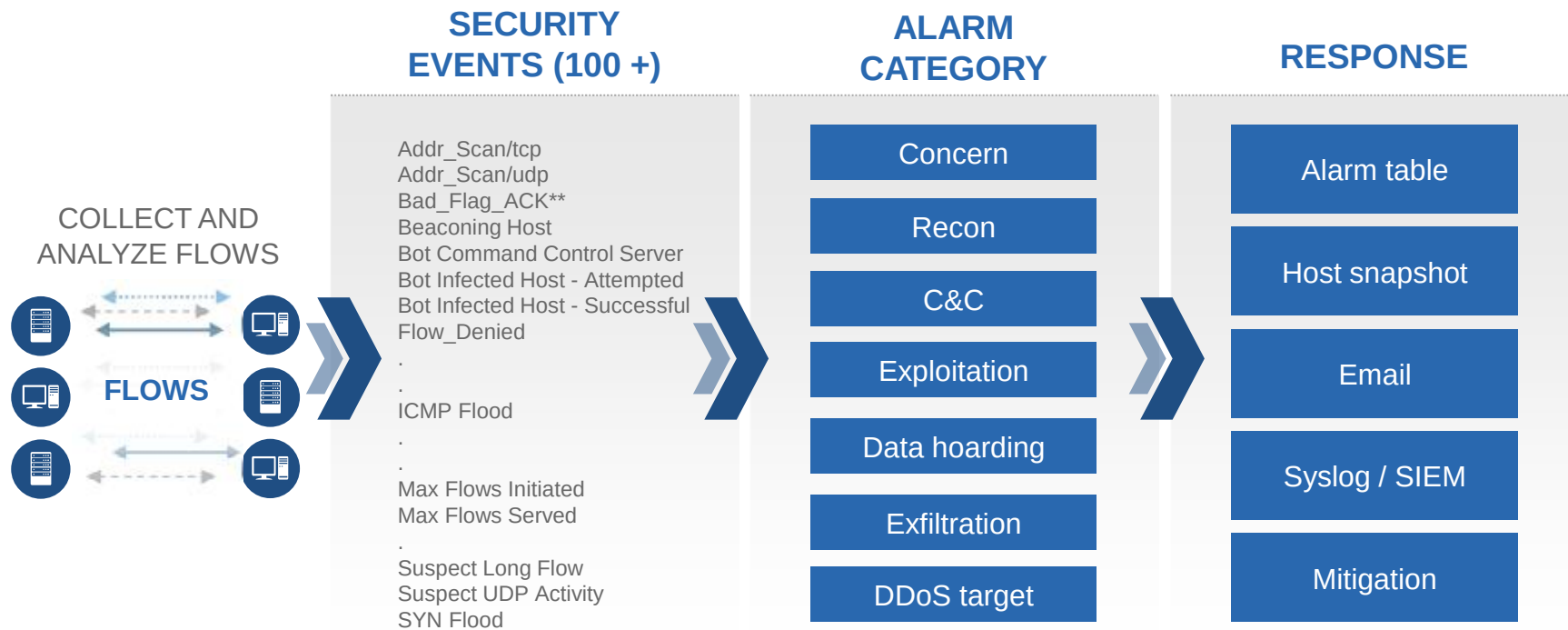
- **Response**

- IPS? FireWall?
- API
- In-line



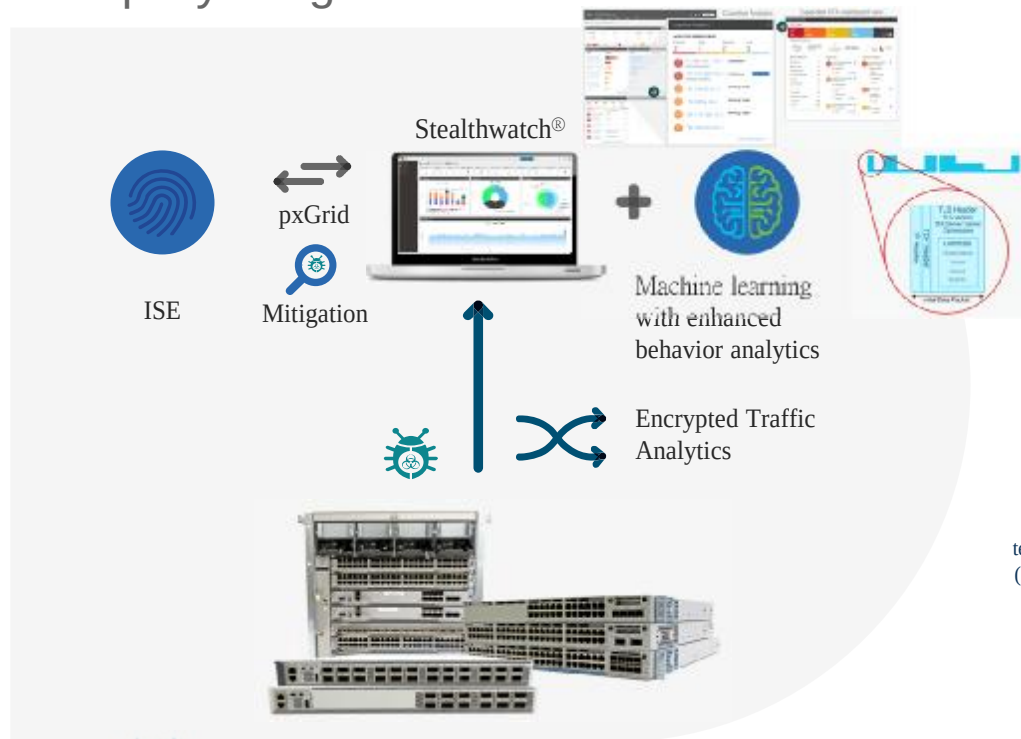
Behavioral and Anomaly Detection Model

Behavioral Algorithms Are Applied to Build “Security Events”

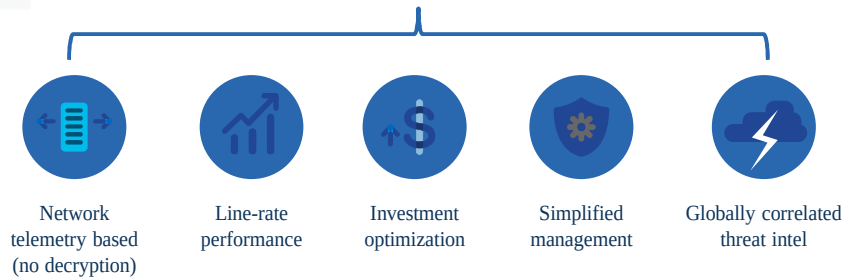


Cisco Catalyst 9000 系列結合ETA (Encrypted Traffic Analytics)升級網路加密可視性

Rapidly mitigate malware and vulnerabilities in encrypted traffic



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





TOMORROW starts here.