威脅情報與網路可視性

Threat Intelligence and Network Visibility

Security Threat

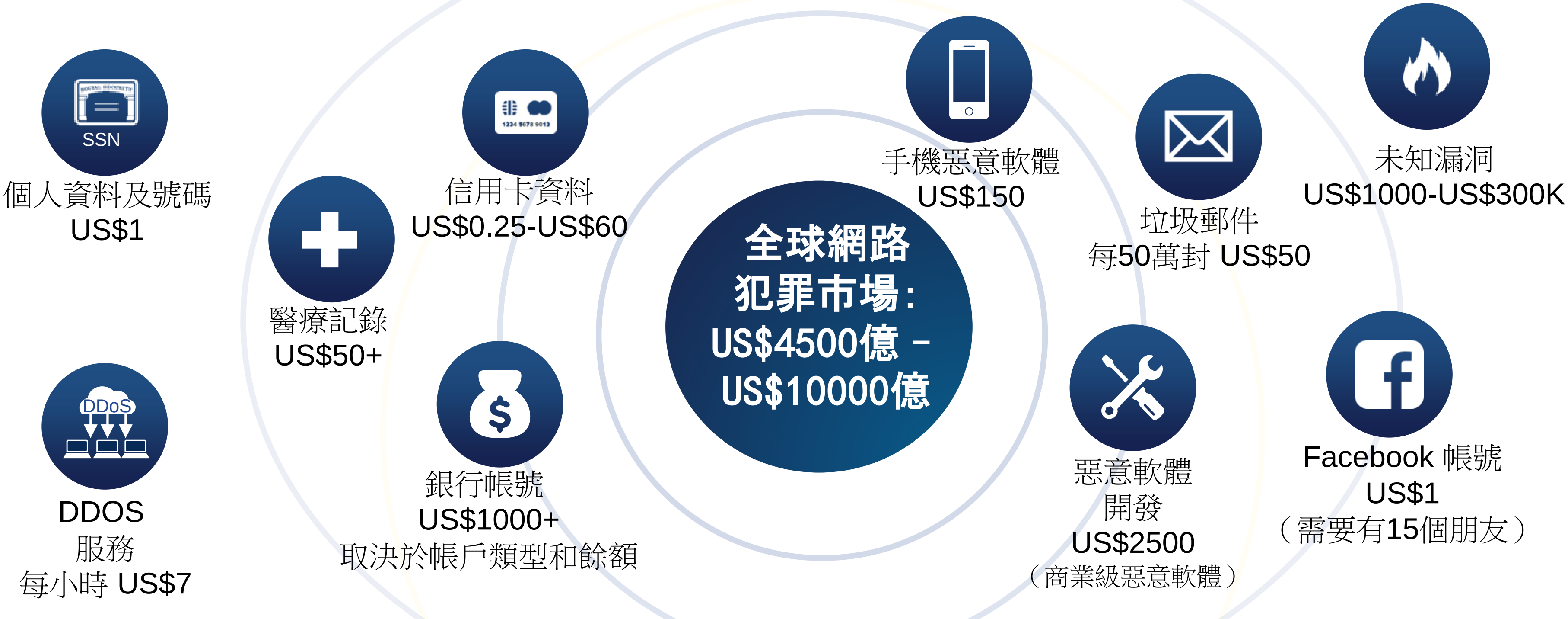
C. K. Lin (林傳凱)

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



全球網路犯罪市場：US$4500億－US$10000億

個人資料及號碼
US$1

醫療記錄
US$50+

信用卡資料
US$0.25-US$60

DDOS
服務
每小時 US$7

銀行帳號
US$1000+
取決於帳戶類型和餘額

手機惡意軟體
US$150

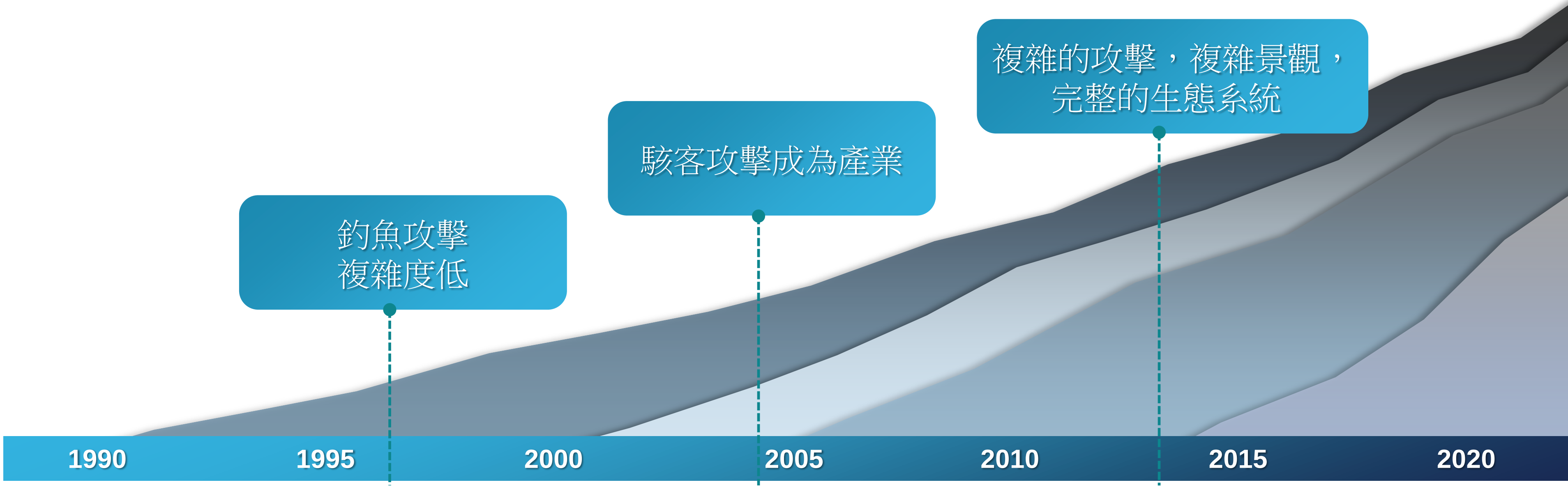
垃圾郵件
每50萬封 US$50

未知漏洞
US$1000-US$300K

惡意軟體
開發
US$2500
（商業級惡意軟體）

Facebook 帳號
US$1
（需要有15個朋友）

網路犯罪的產業化



電腦病毒
1990–2000

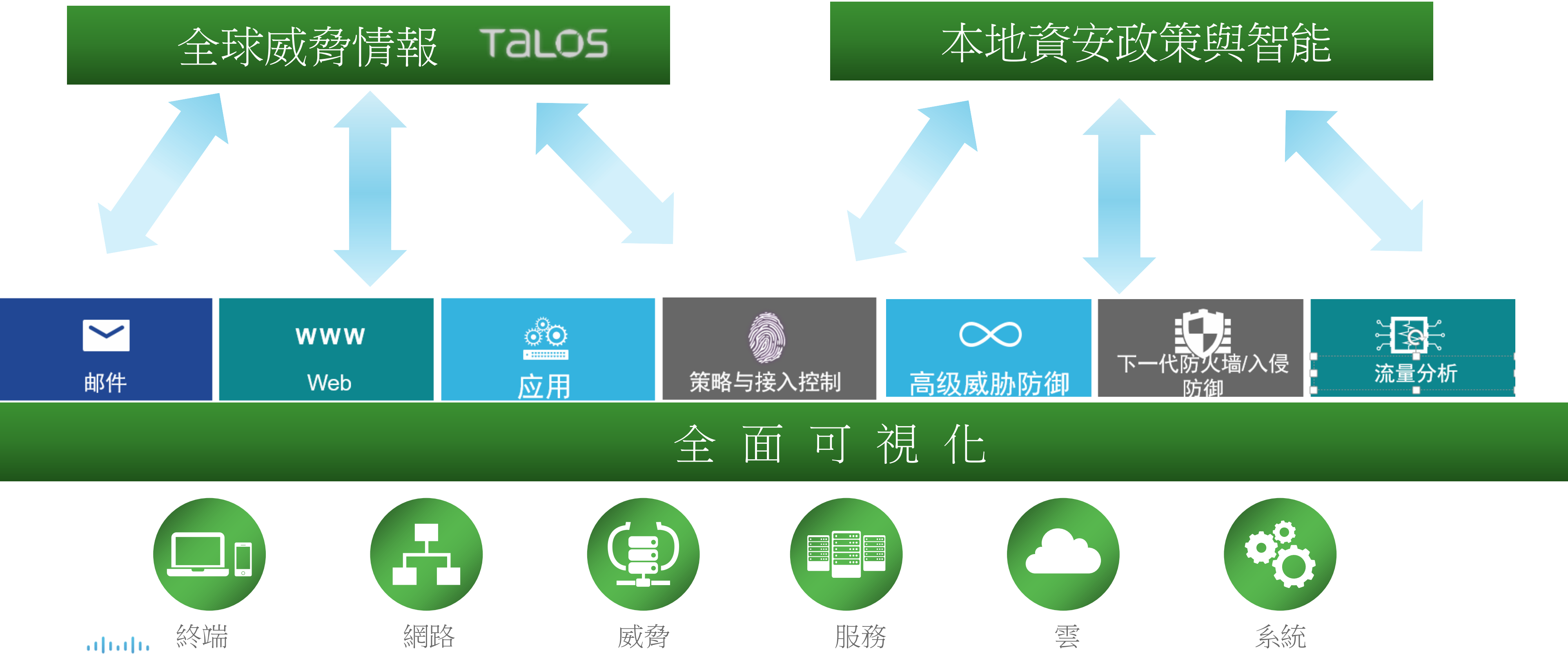
網路蠕蟲
2000–2005

間諜軟體和Rootkit
2005–Today

高級可持續性威脅,
勒索軟體
Today +

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



全球威脅情報 Talos

本地資安政策與智能

郵件

WWW

Web

应用

策略与接入控制

高级威胁防御

下一代防火墙/入侵防御

流量分析

全面可視化

終端

網路

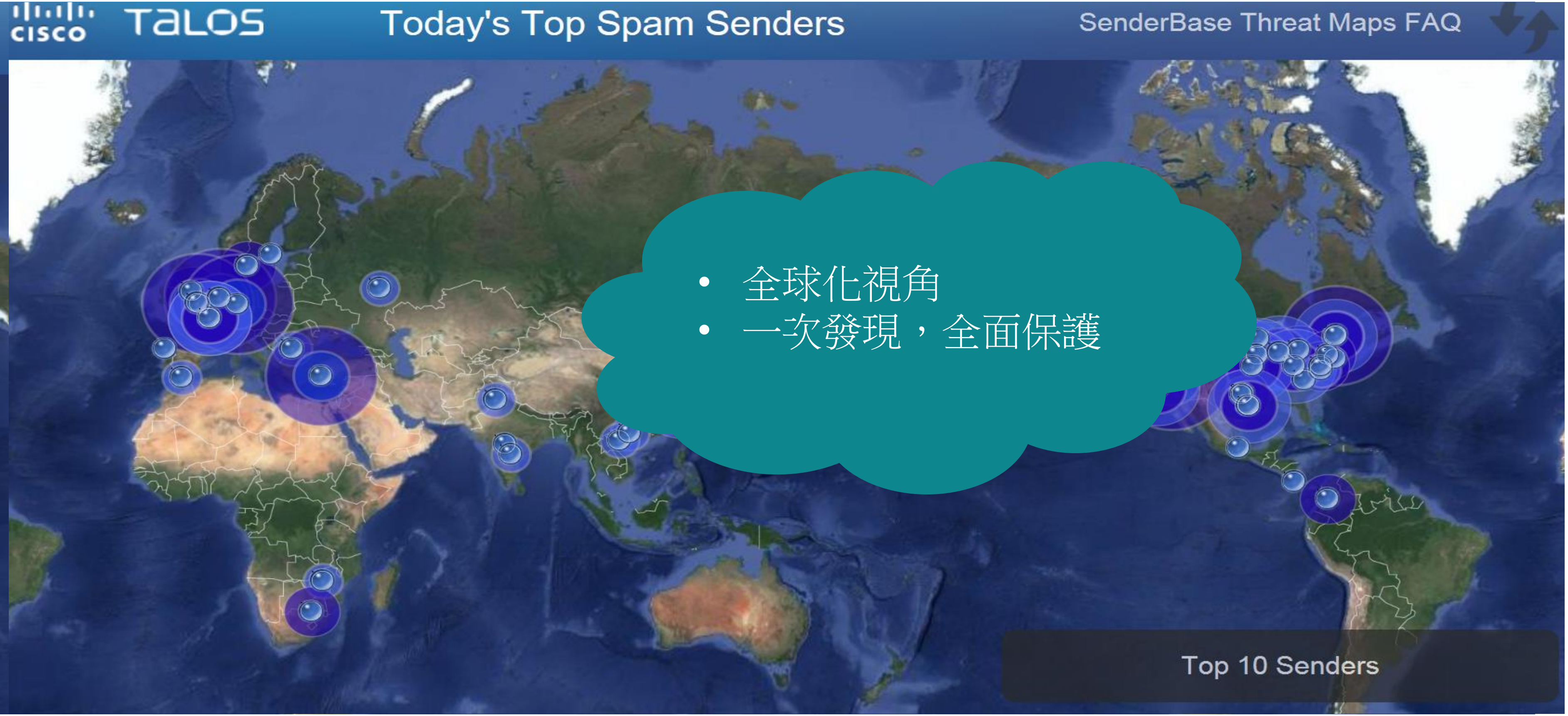
威脅

服務

雲

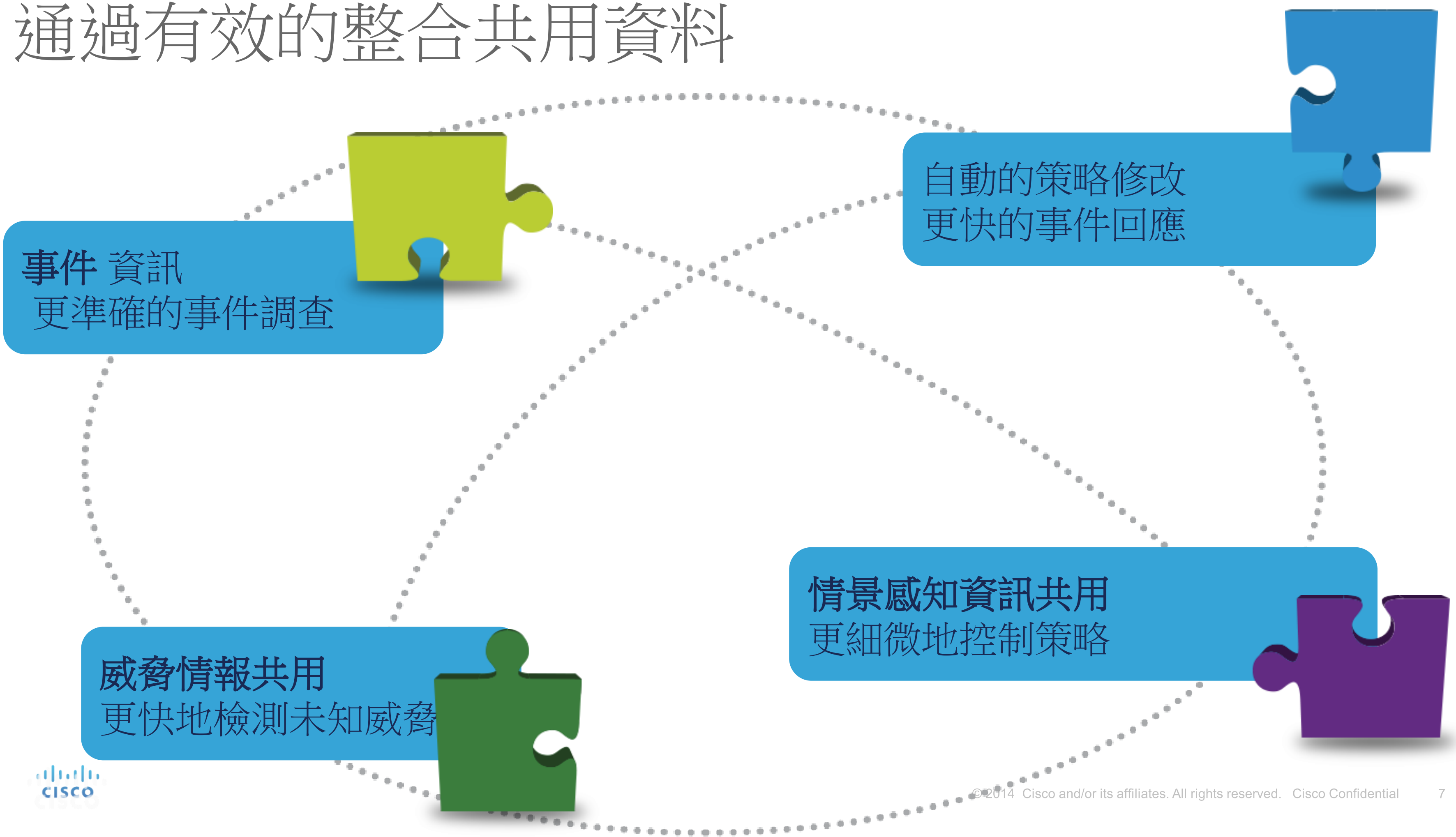
系統

關鍵點：全球化的安全情報



- 全球化視角
- 一次發現，全面保護

通過有效的整合共用資料



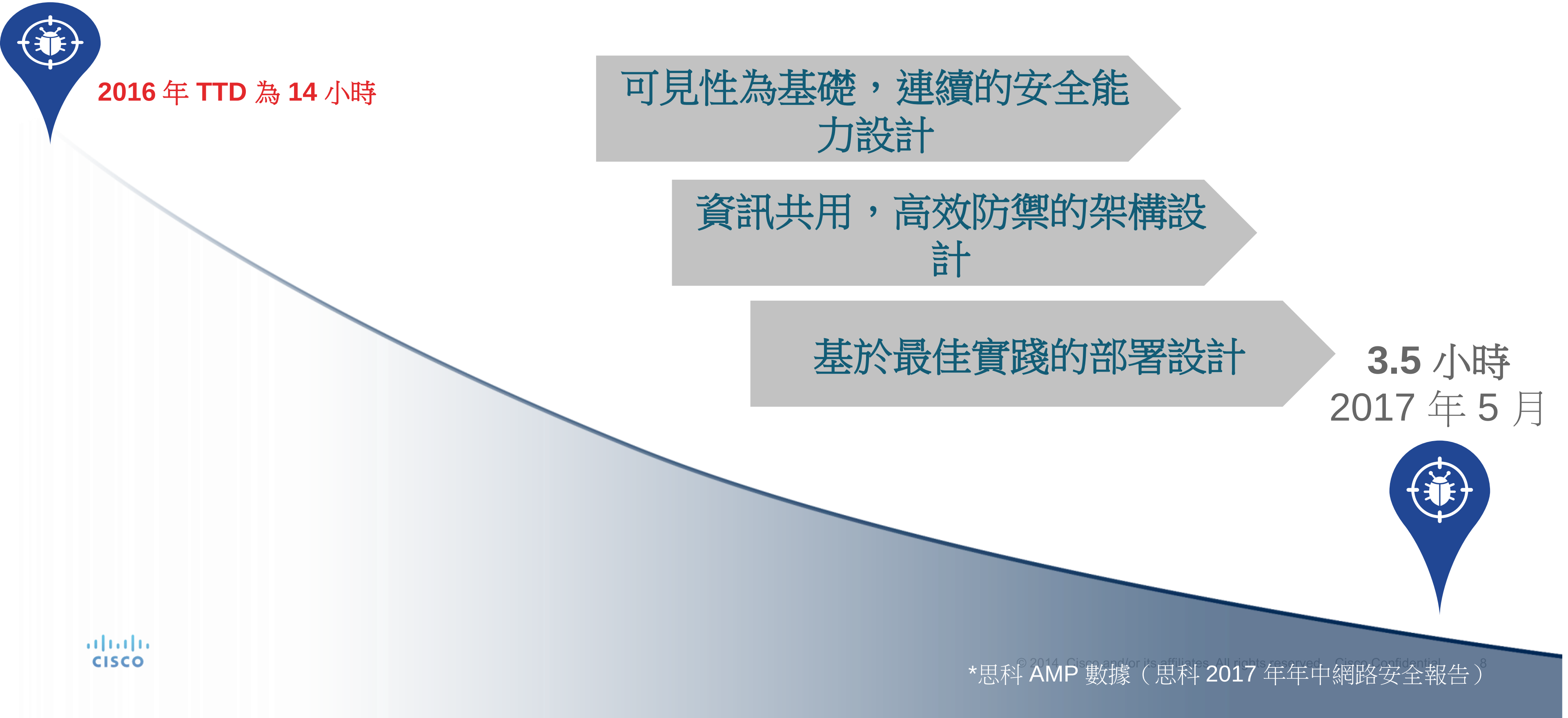
事件 資訊
更準確的事件調查

自動的策略修改
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

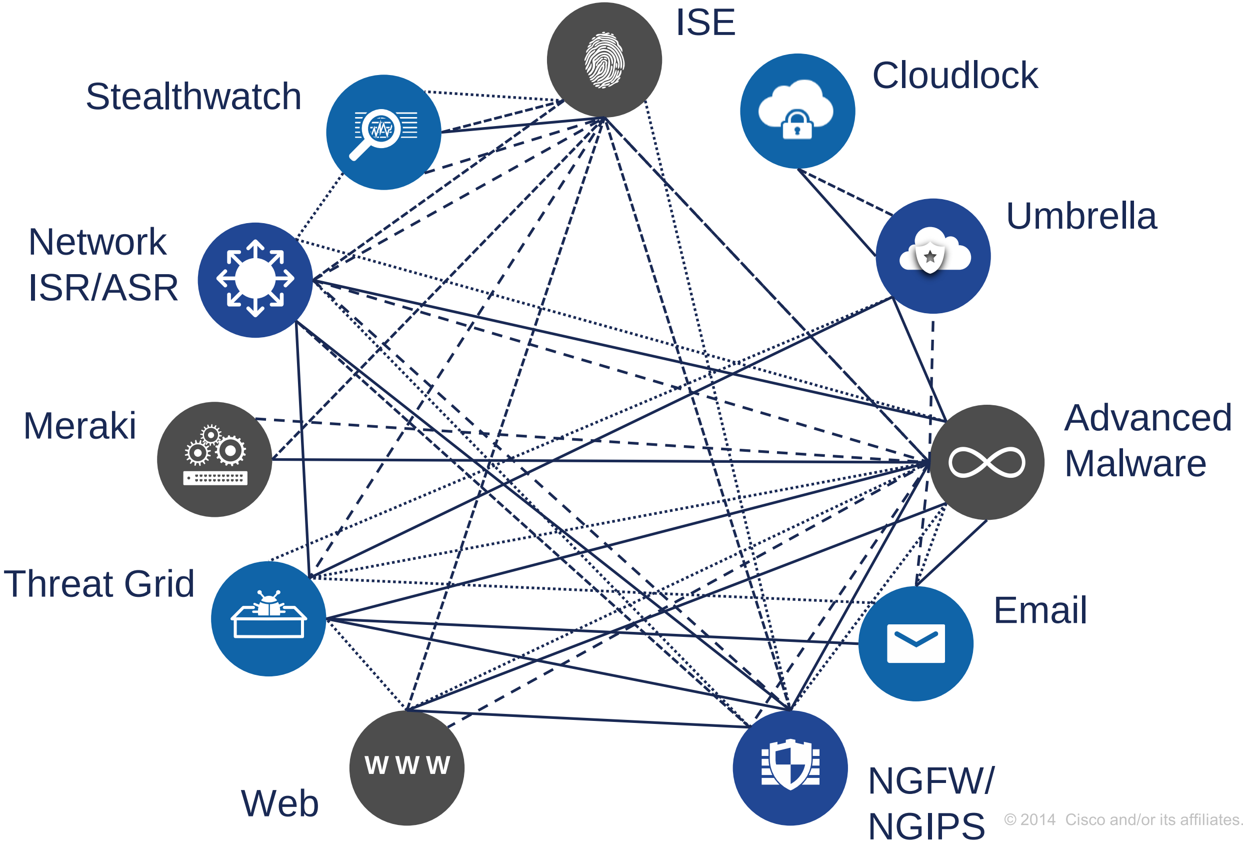
資訊共用，高效防禦的架構設計

基於最佳實踐的部署設計

3.5 小時
2017 年 5 月

*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



- - - - -	資安事件
——	威脅情報
---------	策略
·········	上下文資訊

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

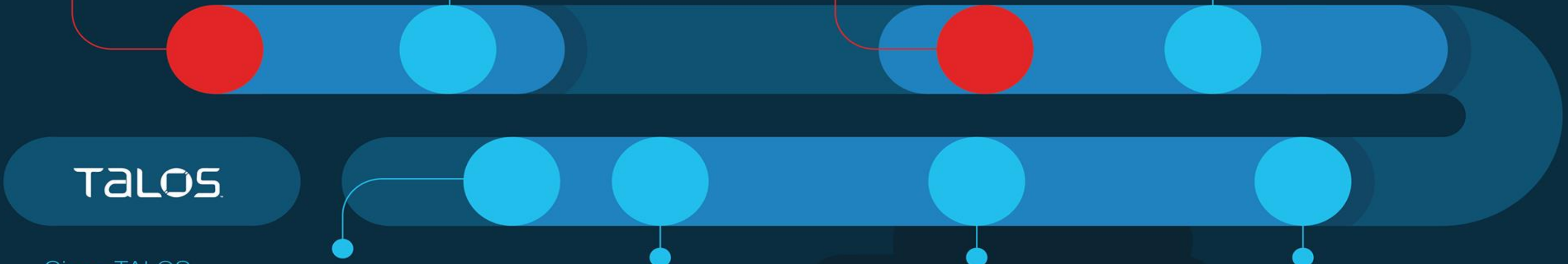
On the same day, Cisco Talos released Snort™ signature #41978 to detect vulnerabilities identified in MS17-010.

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 #42329, #42332, #42340 for Double Pulsar and Anonymous SMB shares.



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 60 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

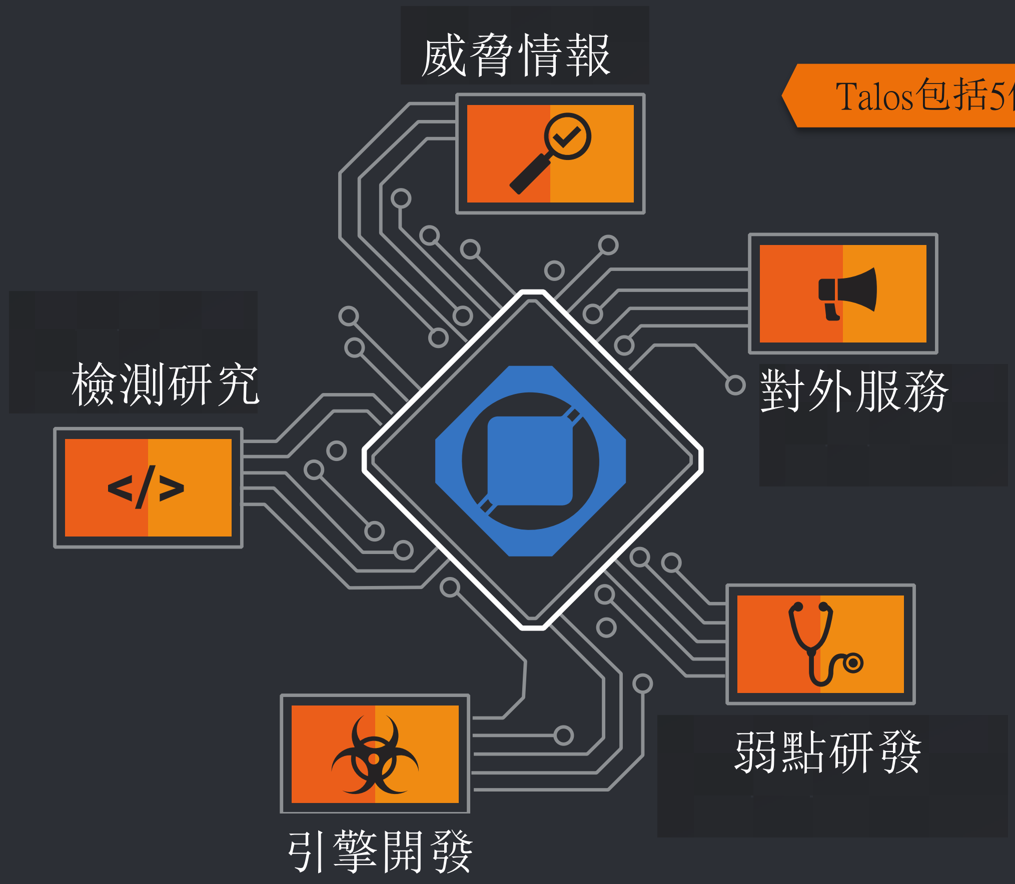
@MalwareTechBlog releases information about a new attack dubbed ‘WannaCry’ on Twitter and his blog.

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

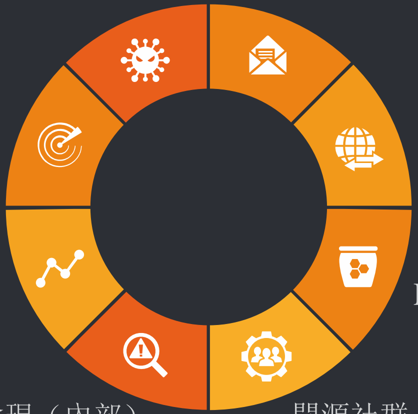
Talos包括5個團隊：



Talos

TALOS情報類型細分

威脅情報



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

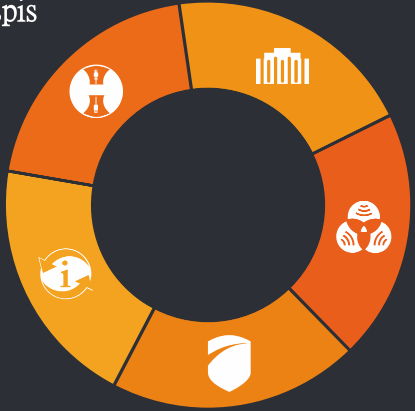
開源社群

弱點發現（內部）

遙測資料

對整個網際網路的掃描

情報共用



Crete

AEGIS

協力廠商程式（MAPP）

ISACs

Aspis

超過250名
全職威脅情報研究人員

上百萬個
遙測代理

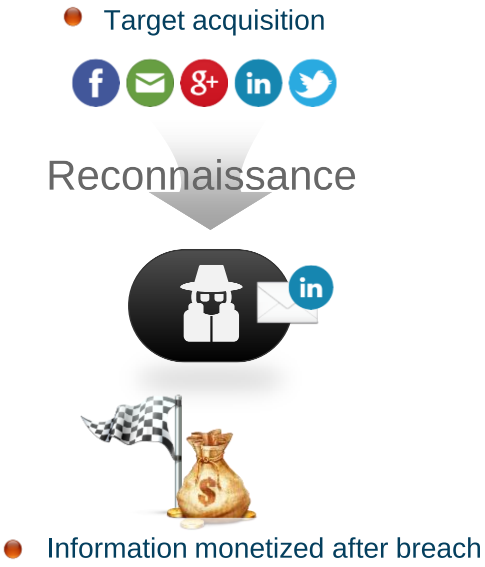
4個全球資料中心

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

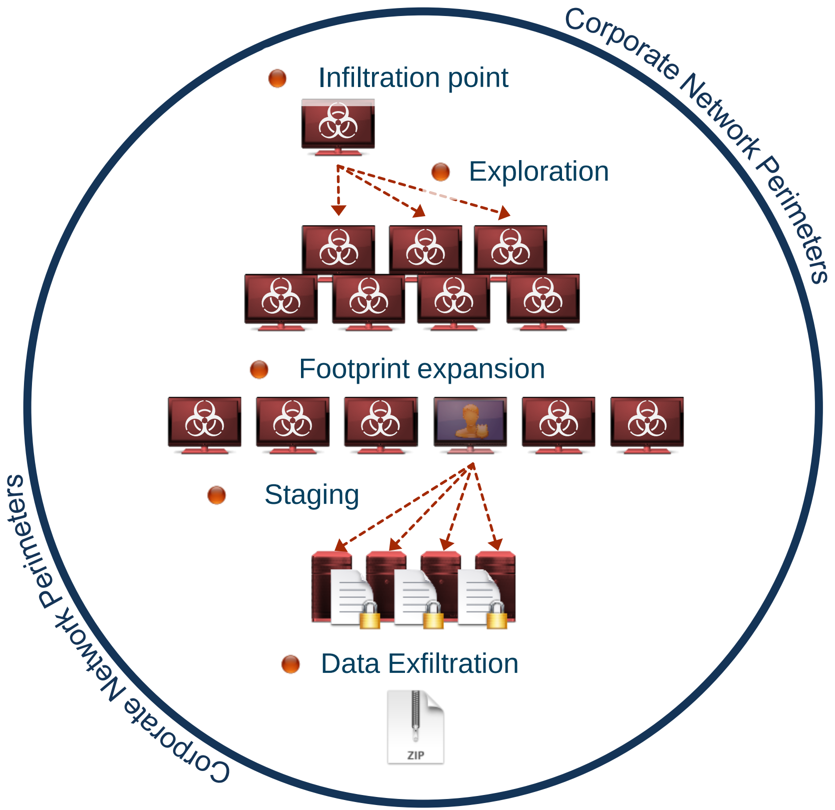
剖析資料洩漏流程



- Target acquisition

Reconnaissance

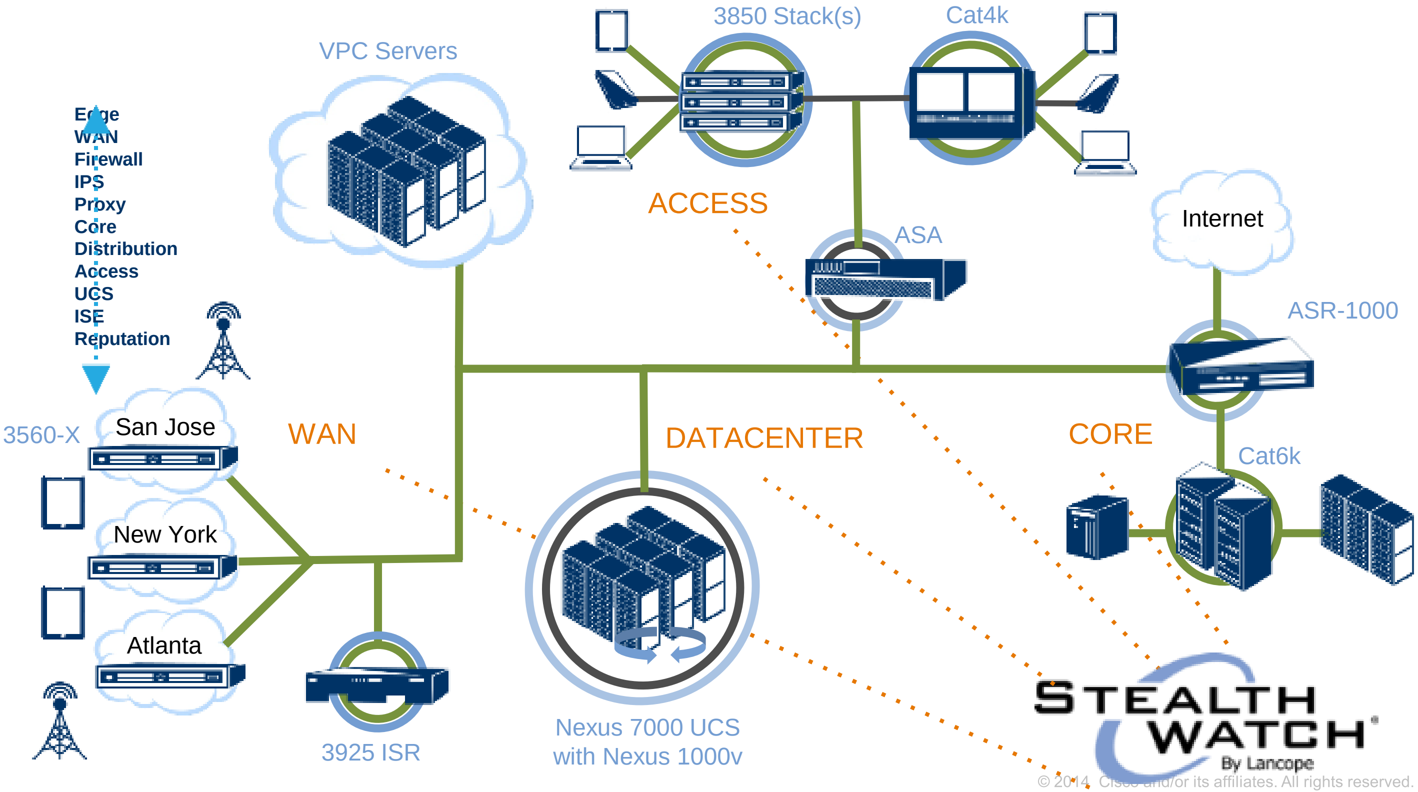
- Information monetized after breach



- Infiltration point
- Exploration
- Footprint expansion
- Staging
- Data Exfiltration

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**



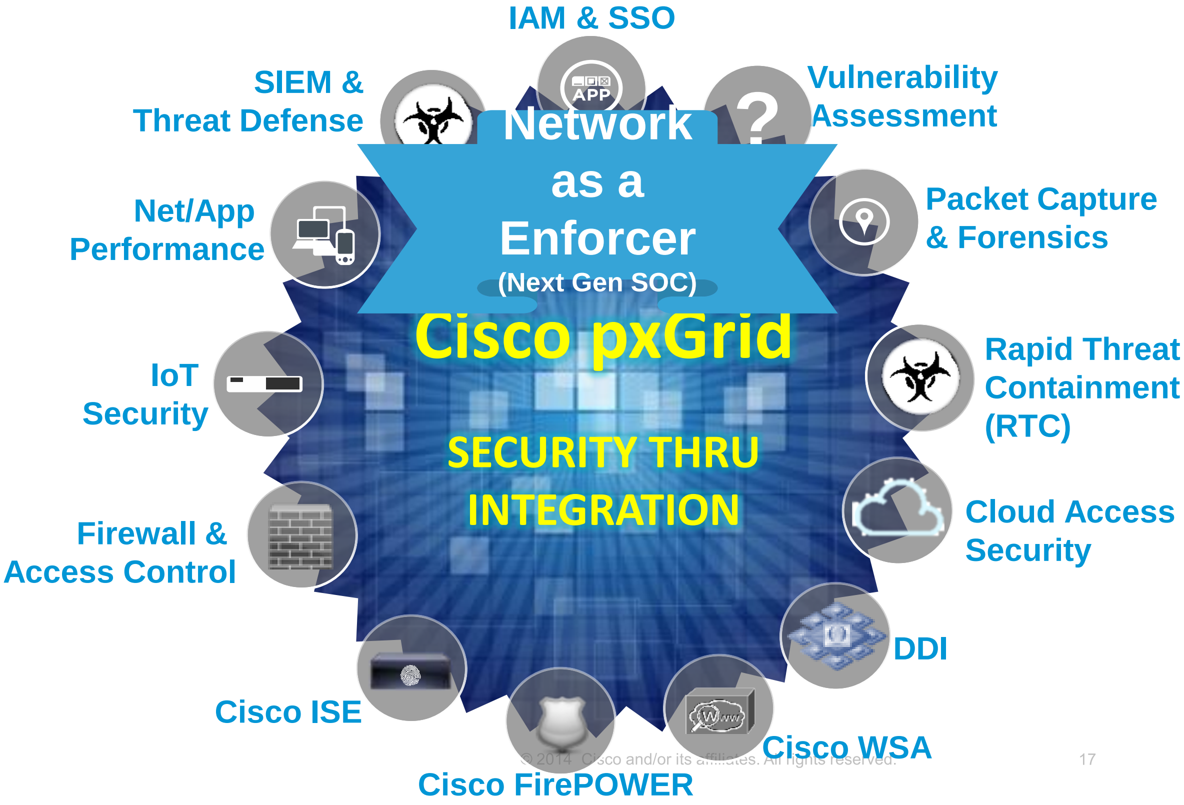
可視性 ≠ SIEM

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

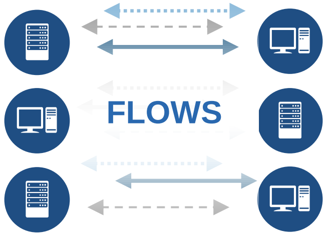
- **Response**
  - IPS? FireWall?
  - API
  - In-line



Behavioral and Anomaly Detection Model

Behavioral Algorithms Are Applied to Build "Security Events"

COLLECT AND ANALYZE FLOWS



SECURITY EVENTS (100 +)

Addr_Scan/tcp
Addr_Scan/udp
Bad_Flag_ACK**
Beaconing Host
Bot Command Control Server
Bot Infected Host - Attempted
Bot Infected Host - Successful
Flow_Denied
.
.
ICMP Flood
.
.
Max Flows Initiated
Max Flows Served
.
Suspect Long Flow
Suspect UDP Activity
SYN Flood

ALARM CATEGORY

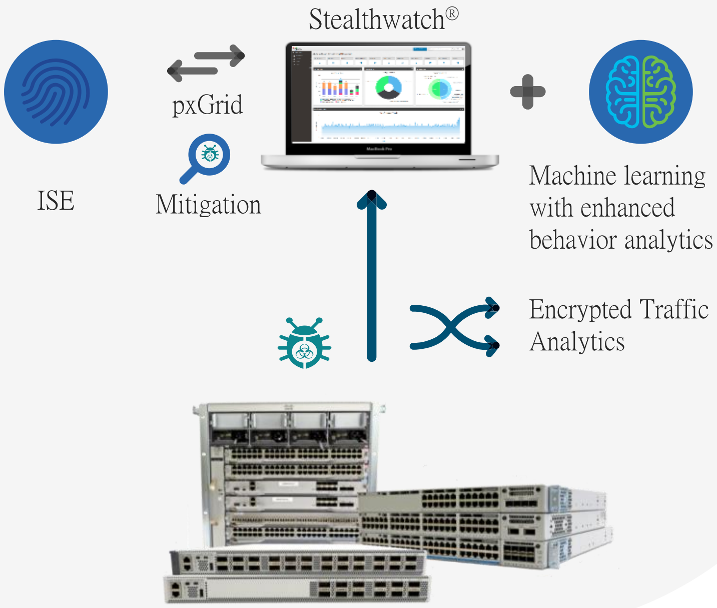
- Concern
- Recon
- C&C
- Exploitation
- Data hoarding
- Exfiltration
- DDoS target

RESPONSE

- Alarm table
- Host snapshot
- Email
- Syslog / SIEM
- Mitigation

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



Stealthwatch®

ISE

pxGrid

Mitigation

Machine learning with enhanced behavior analytics

Encrypted Traffic Analytics

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

Network telemetry based (no decryption)

Line-rate performance

Investment optimization

Simplified management

Globally correlated threat intel

TOMORROW starts here.