ZERONE
零壹科技

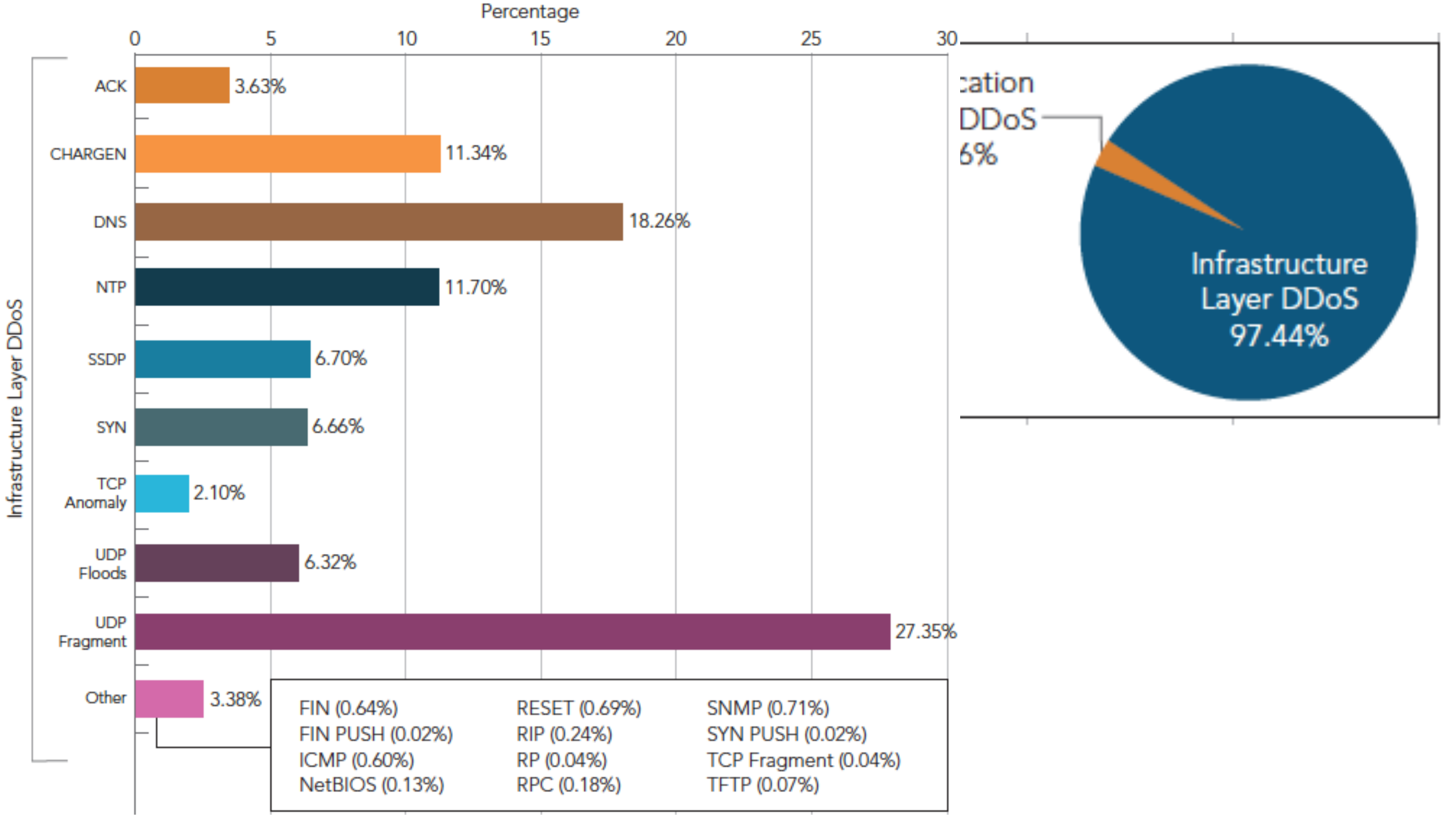
從數據分析談資訊安全

技術顧問
陳鳴豪 Bryant Chan

Agenda:

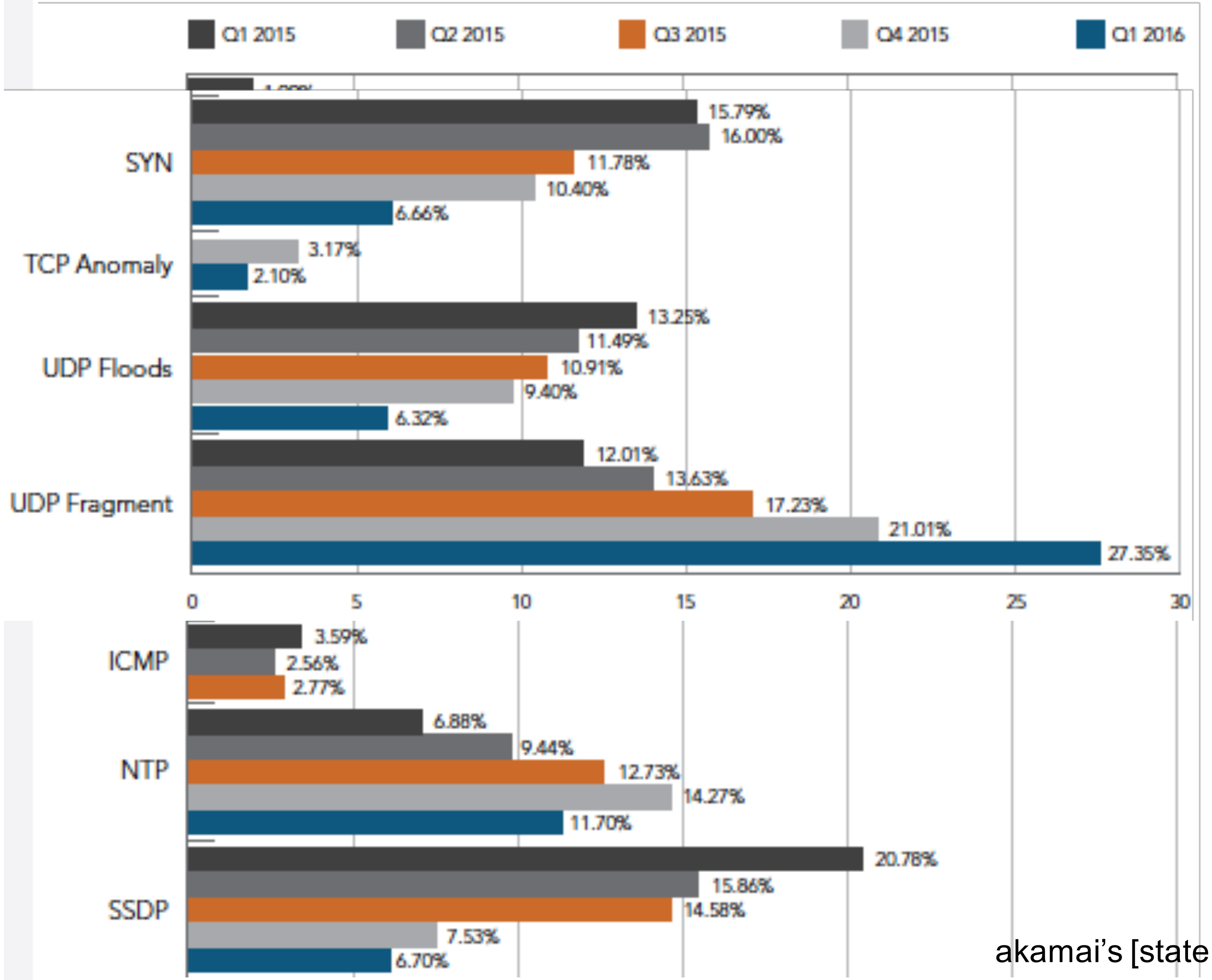
- 資安攻擊數據統計分享
- 案例分享
- 資訊安全調查
- 傳統事件處理
- 數據分析
- 共生互利系統

2016 Q1 DDoS 類型統計



akamai's [state of the internet] / security / Q1 2016

十大DDoS類型趨勢



akamai's [state of the internet] / security / Q1 2016

多類型攻擊手段

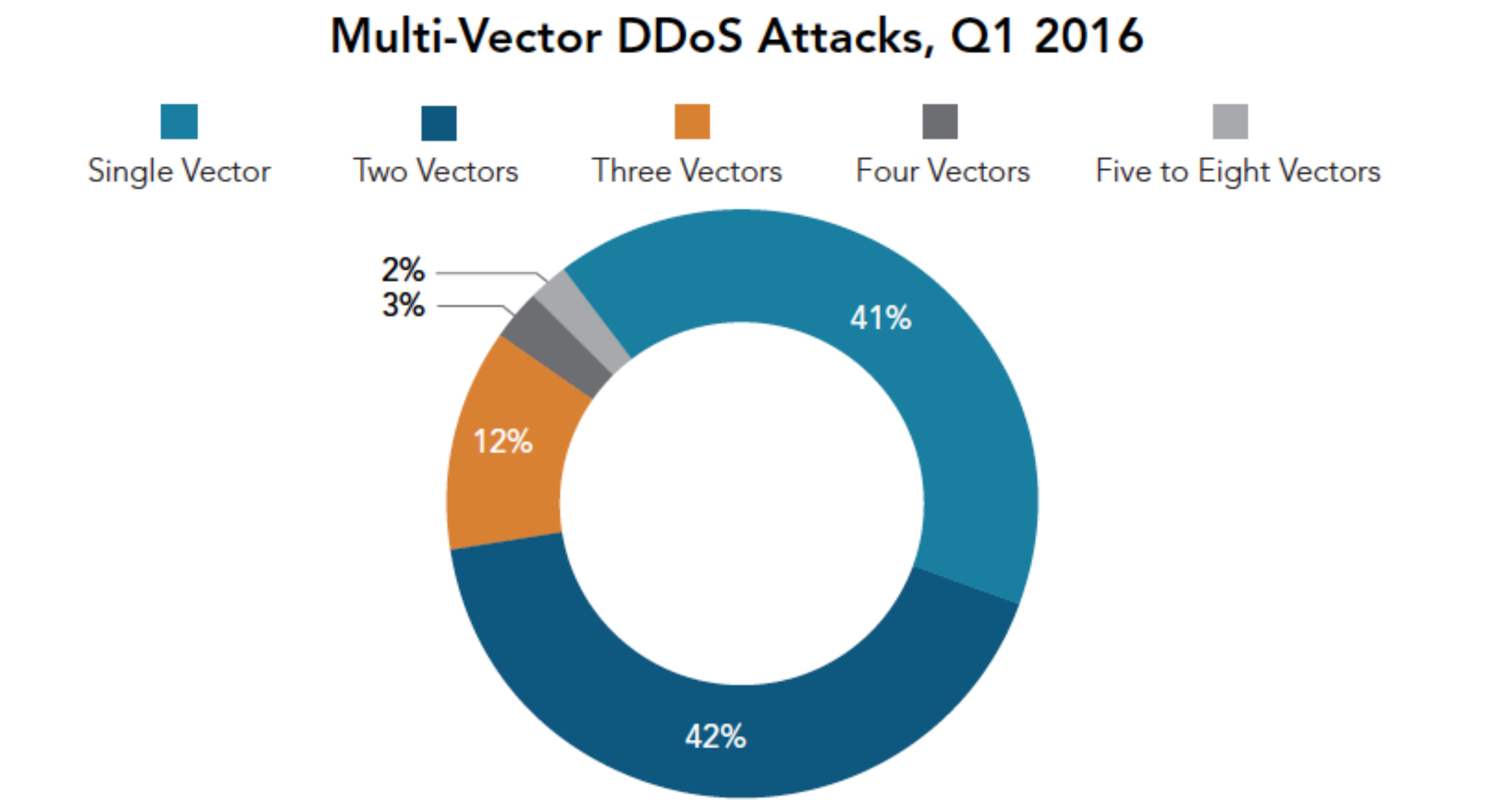
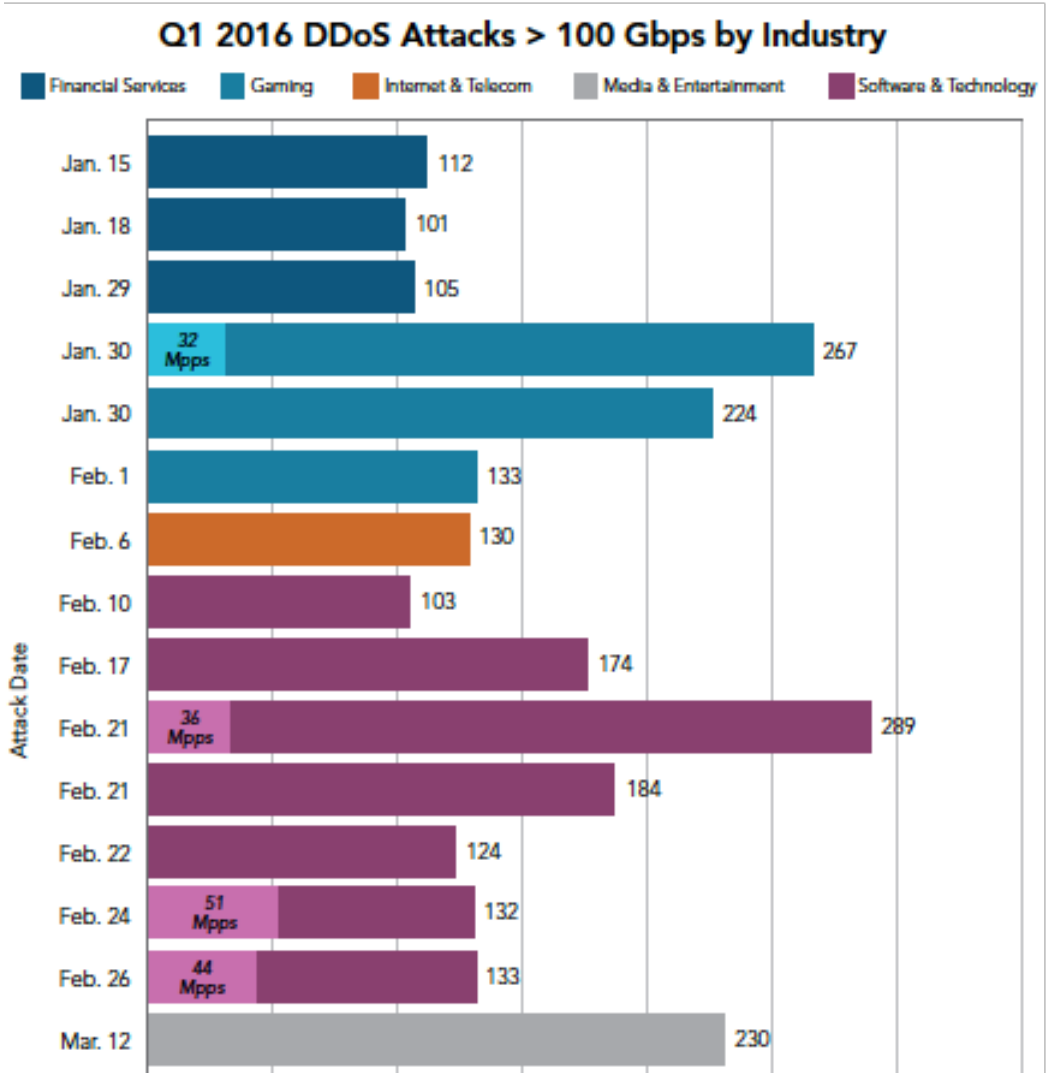


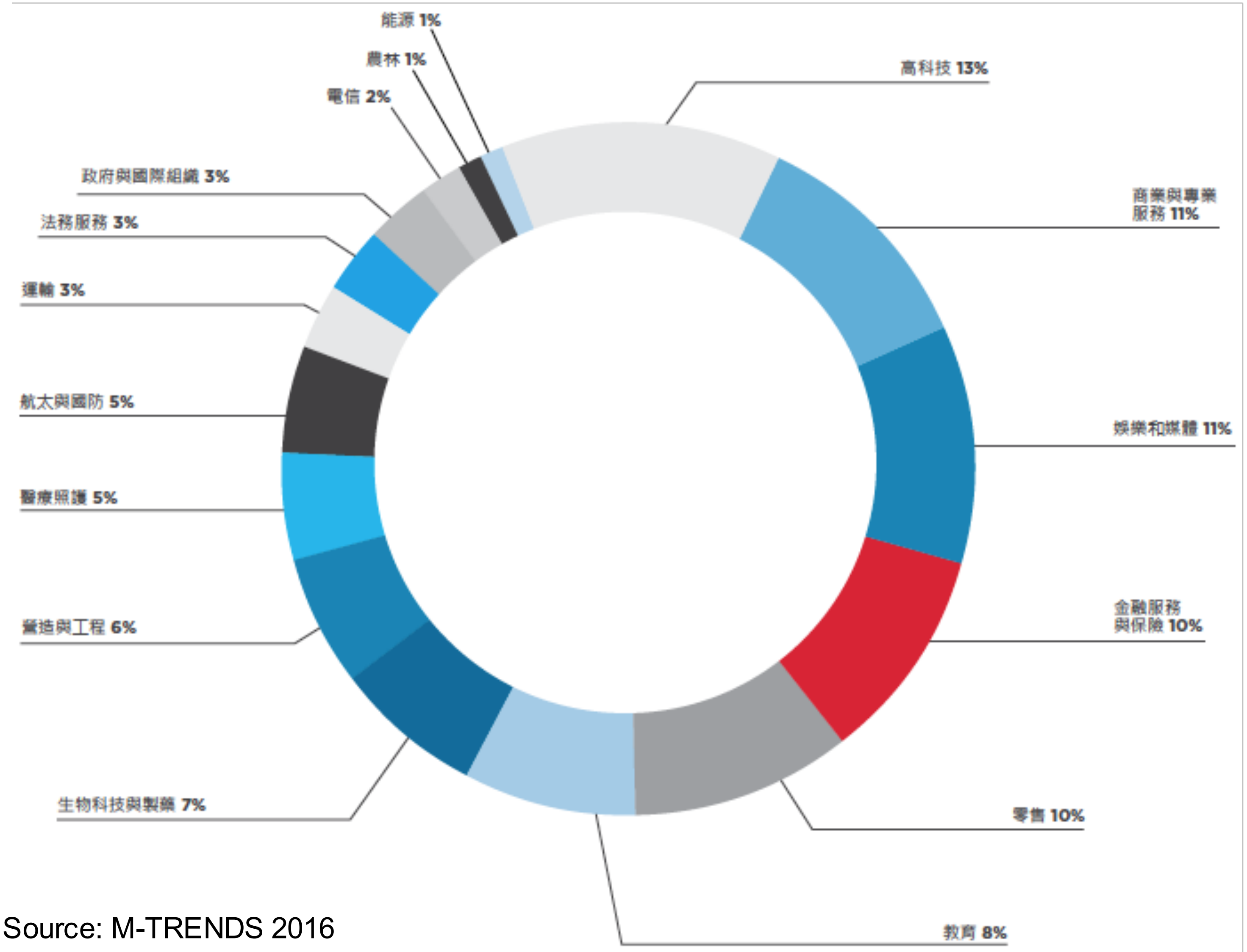
Figure 2-3: Multi-vector attacks accounted for 59% of DDoS activity in Q1 2016, reflecting a slight increase compared with last quarter (56%)

2016 Q1 DDoS 規模



akamai’s [state of the internet] / security / Q1 2016

APT事件數據



Source: M-TRENDS 2016

從被攻擊到發現需要…..

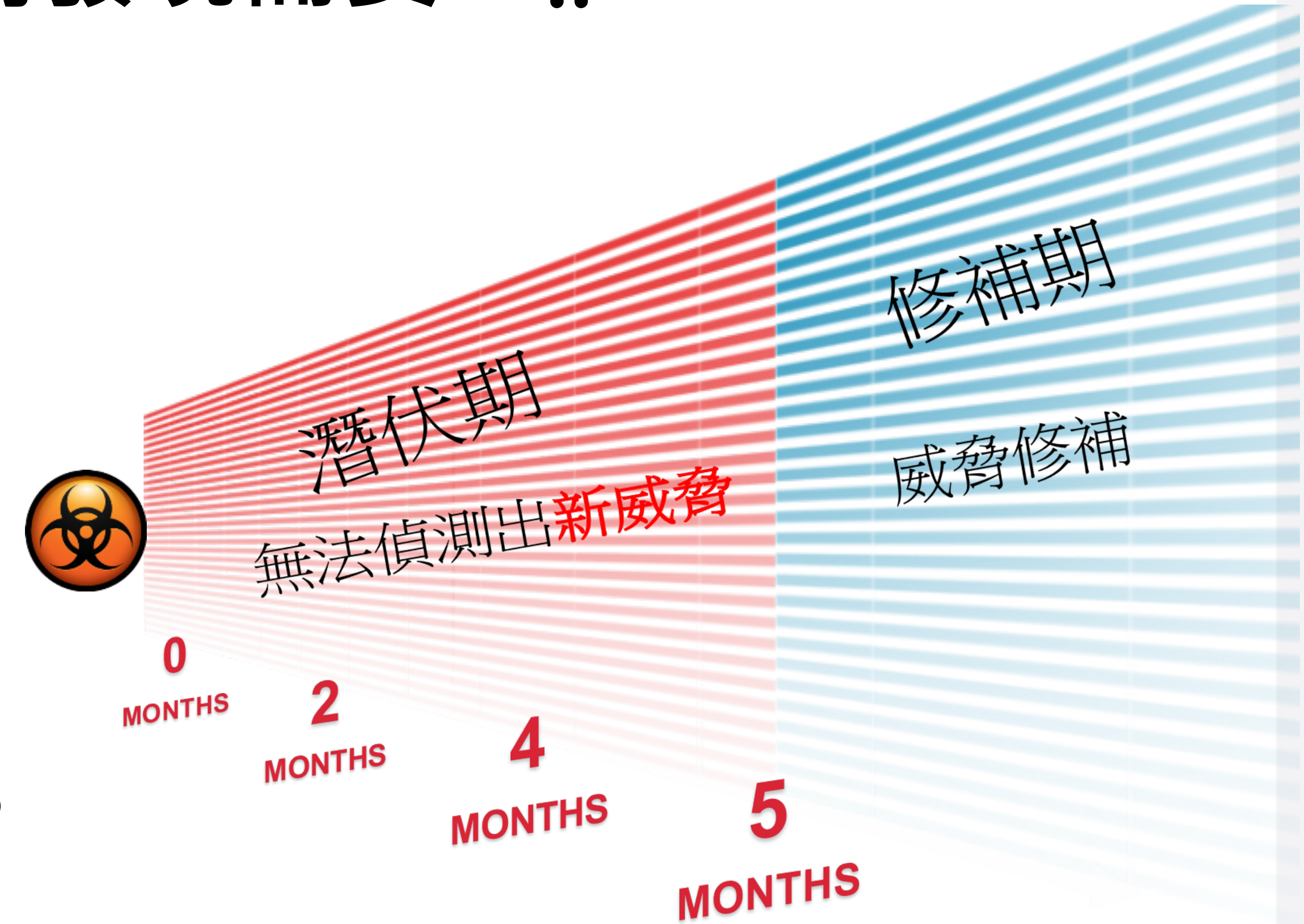
149 天
平均潛伏期

56 天
自行偵測遭受入侵

53%
經由第三方的通報得知

1600
由外部IR團隊協助受害單位
回復的平均處理時間（小時）

100%
受害者已安裝防火牆與
更新最新的防毒特徵碼



SOURCE: MANDIANT M-TRENDS REPORT, PONEMON COST OF DATA BREACH STUDY

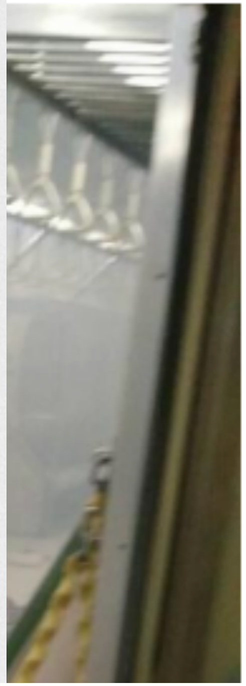
案例分享

松山火車站

【不斷更新】台鐵炸彈案緝凶關鍵：目擊指認　DNA露餡

（中央社記
車站今天晚
勢隨即撲滅
21人受傷，
救護車到現

台北市消防
站發生列車
車、11輛救
現場，並持



破案重點

1. 收集手上資訊
2. 資訊內容分析
3. 鎖定懷疑目標
4. 循線追蹤及情資比對
5. 收集重要證據
6. 作出推論
7. 結案

Source: www.google.com

資訊安全調查

數據中心或用戶端事件發生

傳統事件處理

- 各自看各自的內容
- 跨部門溝通
- 資料與資訊不完整
- 缺乏行為特徵分析
- 能做得更好嗎？

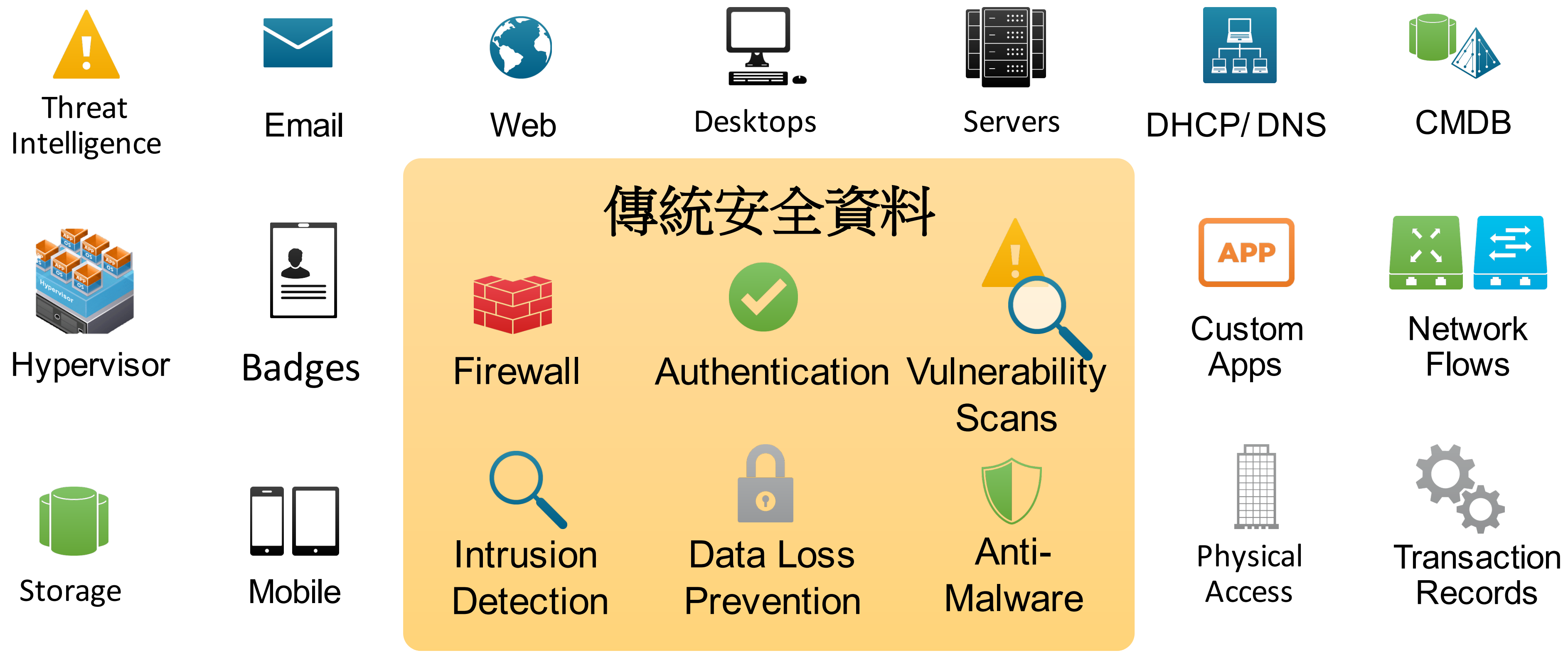
Source: www.google.com

來自機器的巨量資料

數量 ｜ 速度 ｜ 多樣性 | 變化性

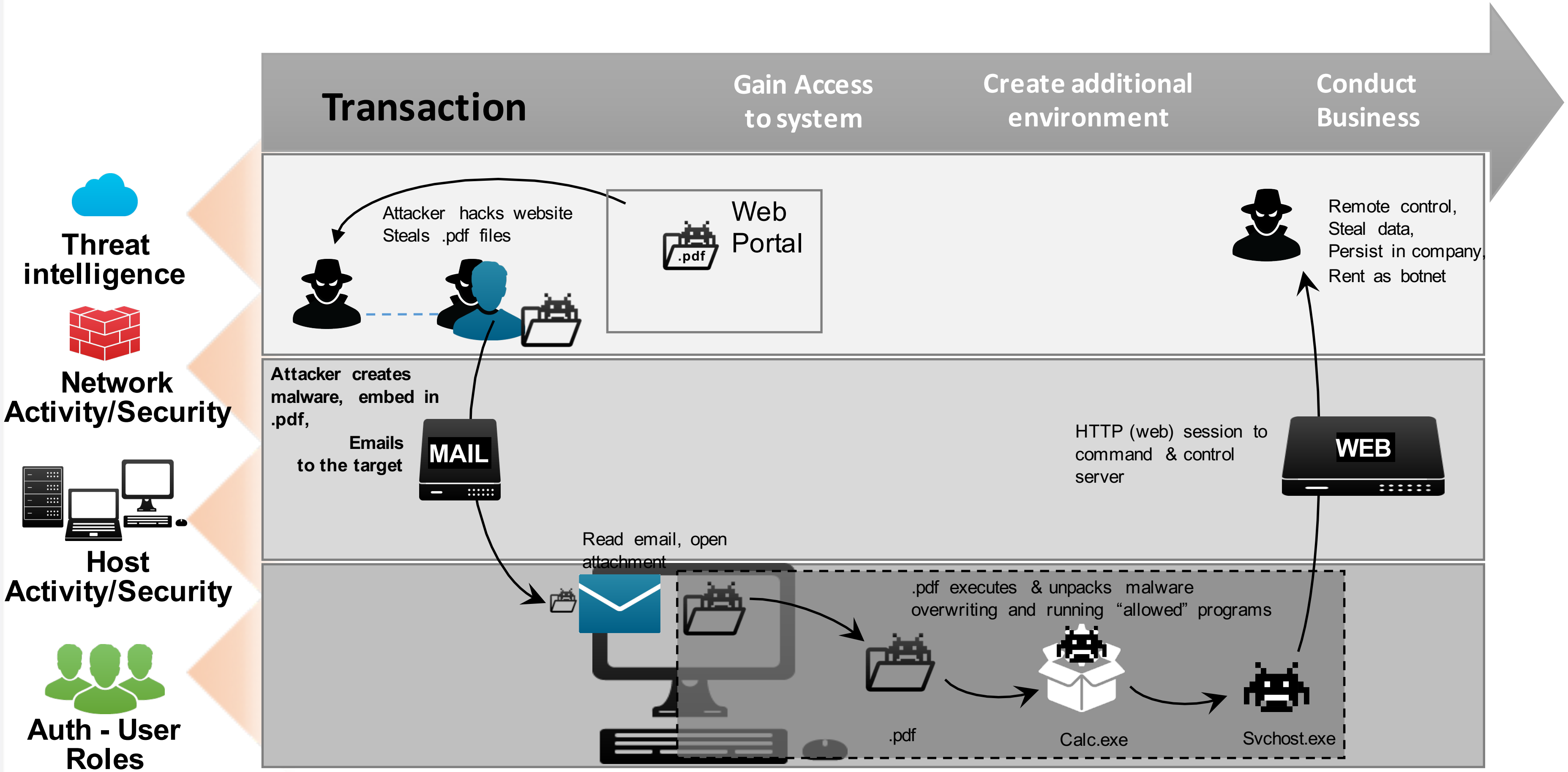
GPS,
RFID,
虛擬化監管程式,
網路伺服器,
電郵, 訊息,
點選流, 行動,
電話通訊, 互動式語音回應, 資料庫,
感測器, 車用電子, 儲存,
伺服器, 安全裝置, 桌上型電腦

資訊安全相關大數據

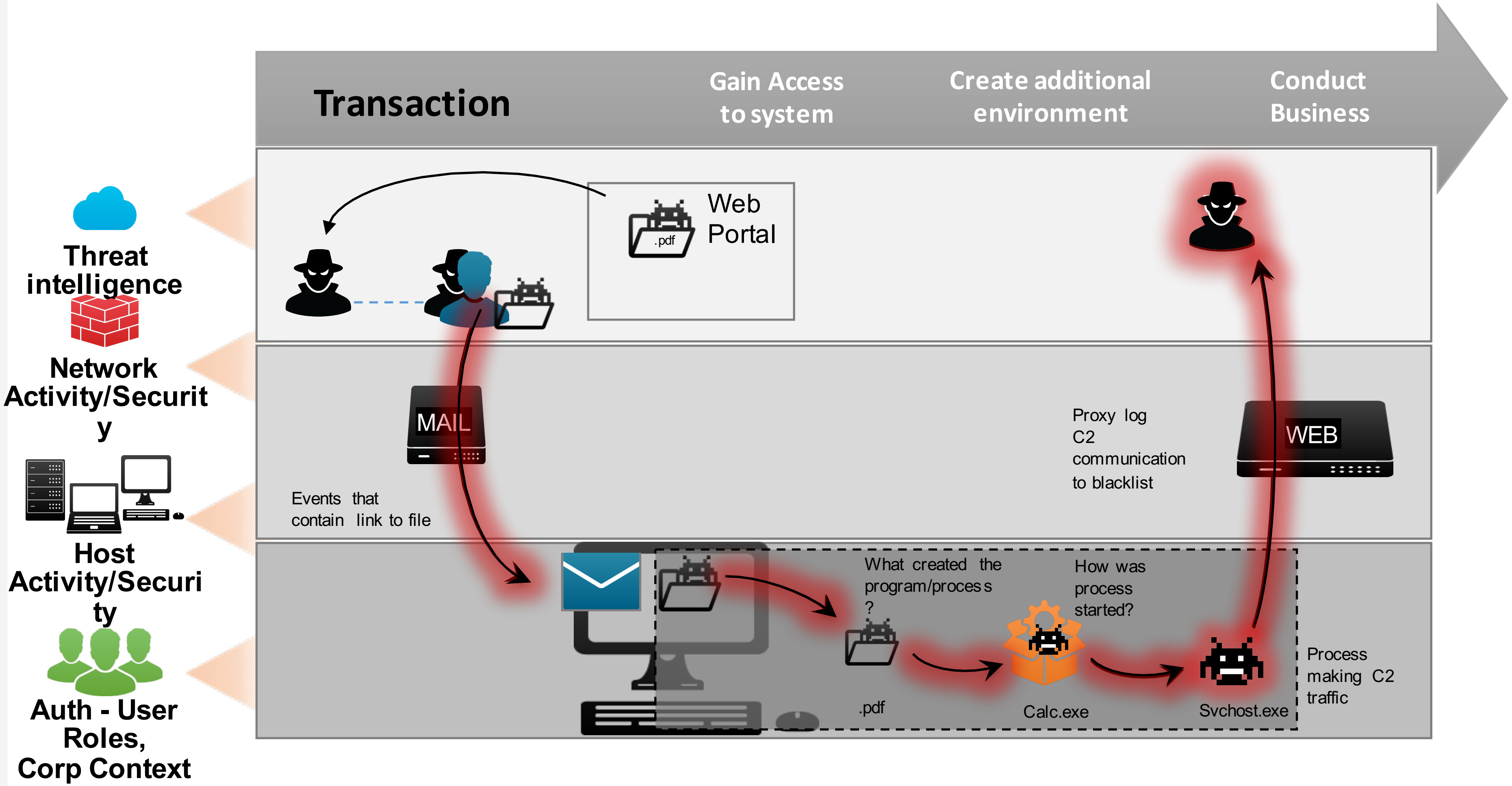


Threat Intelligence
Email
Web
Desktops
Servers
DHCP/ DNS
CMDB
傳統安全資料
Hypervisor
Badges
Firewall
Authentication
Vulnerability Scans
Custom Apps
Network Flows
Storage
Mobile
Intrusion Detection
Data Loss Prevention
Anti-Malware
Physical Access
Transaction Records

APT追蹤及分析案例

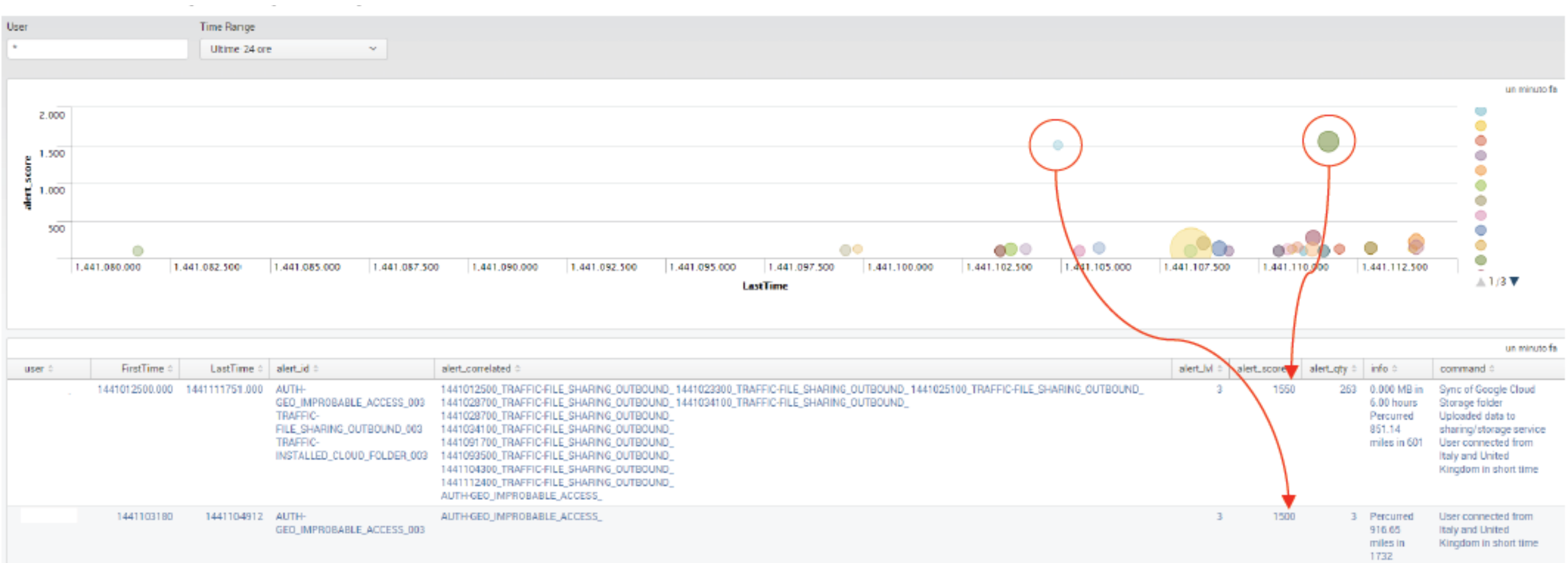

Transaction
Gain Access to system
Create additional environment
Conduct Business
Threat intelligence
Network Activity/Security
Host Activity/Security
Auth - User Roles
Attacker hacks website
Steals .pdf files
Web Portal
.pdf
Remote control,
Steal data,
Persist in company,
Rent as botnet
Attacker creates malware, embed in .pdf,
Emails to the target
MAIL
HTTP (web) session to command & control server
WEB
Read email, open attachment
.pdf executes & unpacks malware overwriting and running "allowed" programs
.pdf
Calc.exe
Svchost.exe

風險追蹤偵辦及回應


Transaction
Gain Access to system
Create additional environment
Conduct Business
Threat intelligence
Network Activity/Security
Host Activity/Security
Auth - User Roles, Corp Context
Web Portal
.pdf
MAIL
Events that contain link to file
Proxy log C2 communication to blacklist
WEB
What created the program/process ?
How was process started?
.pdf
Calc.exe
Svchost.exe
Process making C2 traffic

追蹤及主動通報

- 疑似行為發現
- 追蹤及主動通報



user	FirstTime	LastTime	alert_id	alert_correlated	alert_lvl	alert_score	alert_qty	info	command
	1441012500.000	1441111751.000	AUTH-GEO_IMPROBABLE_ACCESS_003 TRAFFIC-FILE_SHARING_OUTBOUND_003 TRAFFIC-INSTALLED_CLOUD_FOLDER_003	1441012500_TRAFFIC-FILE_SHARING_OUTBOUND_ 1441023300_TRAFFIC-FILE_SHARING_OUTBOUND_ 1441025100_TRAFFIC-FILE_SHARING_OUTBOUND_ 1441028700_TRAFFIC-FILE_SHARING_OUTBOUND_ 1441034100_TRAFFIC-FILE_SHARING_OUTBOUND_ 1441028700_TRAFFIC-FILE_SHARING_OUTBOUND_ 1441034100_TRAFFIC-FILE_SHARING_OUTBOUND_ 1441091700_TRAFFIC-FILE_SHARING_OUTBOUND_ 1441093500_TRAFFIC-FILE_SHARING_OUTBOUND_ 1441104300_TRAFFIC-FILE_SHARING_OUTBOUND_ 1441112400_TRAFFIC-FILE_SHARING_OUTBOUND_ AUTH-GEO_IMPROBABLE_ACCESS_	3	1550	263	0.000 MB in 6.00 hours Percurred 851.14 miles in 601	Sync of Google Cloud Storage folder Uploaded data to sharing/storage service User connected from Italy and United Kingdom in short time
	1441103180	1441104912	AUTH-GEO_IMPROBABLE_ACCESS_003	AUTH-GEO_IMPROBABLE_ACCESS_	3	1500	3	Percurred 916.65 miles in 1732	User connected from Italy and United Kingdom in short time

監控與稽核

Sources

Example Correlation – Data Loss

Windows Authentication

20130806041221.000000Caption=ACME-2975EB\Administrator Description=Built-in account for administering the computer/domain Domain=ACME-2975EB InstallDate=NULL LocalAccount = IP: 10.11.36.20 TrueName=Administrator SID =S-1-5-21-1715567821-926492609 Status=D ype=UserAccounts

Default Admin Account

Source IP

Endpoint Security

Aug 08 06:09:13 acmesep01.acmetech.com Aug 09 06:17:24 SymantecServer acmesep01: Virus found,Computer name ACME-002,Source: Real Time Scan,Risk name: Hackertool.rootkit,Occurrences: 1,C:/Documents and Settings/smithe/Local Settings/Temp/evil.tmp "",Actual action: Quarantined,Requested action: Cleaned, time: 2009-01-23 03:19:12,Inserted: 2009-01-23 03:20:12,End: 2009-01-23 03:19:12,Domain: Default Group: My Company\ACME Remote,Server: acmesep01,User: smithe,Source computer: ,Source IP: 10.11.36.20

Malware Found

Source IP

Intrusion Detection

Aug 08 08:26:54 snort.acmetech.com {TCP} 10.11.36.20:5072 -> 10.11.36.26:443 itsec snort[18774]: [1:100000:3] [Classification: Potential Privacy Violation] Credit Card Number Detected in Clear Text [Priority: 2]:

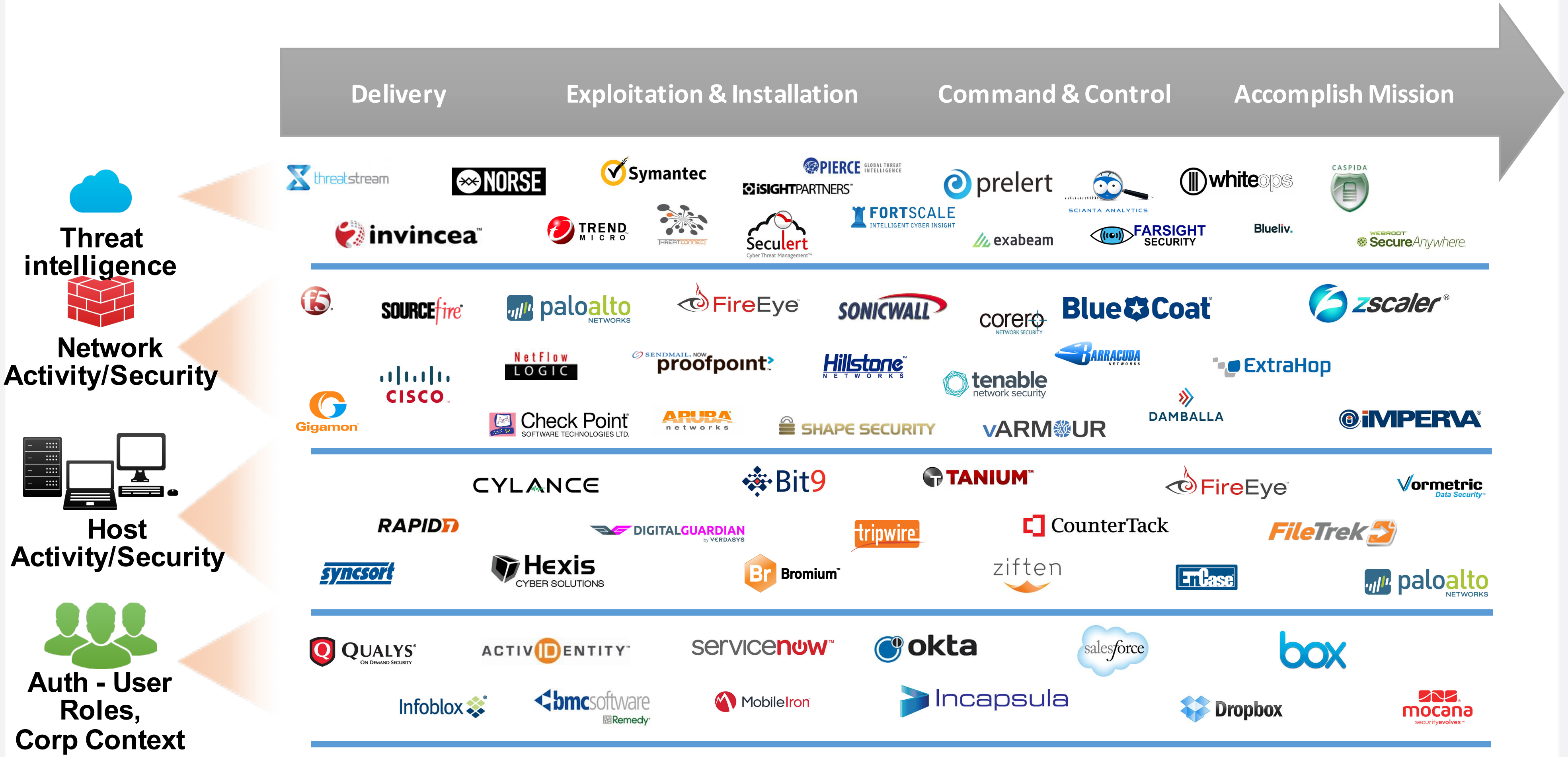
Source IP

Data Loss

Time Range

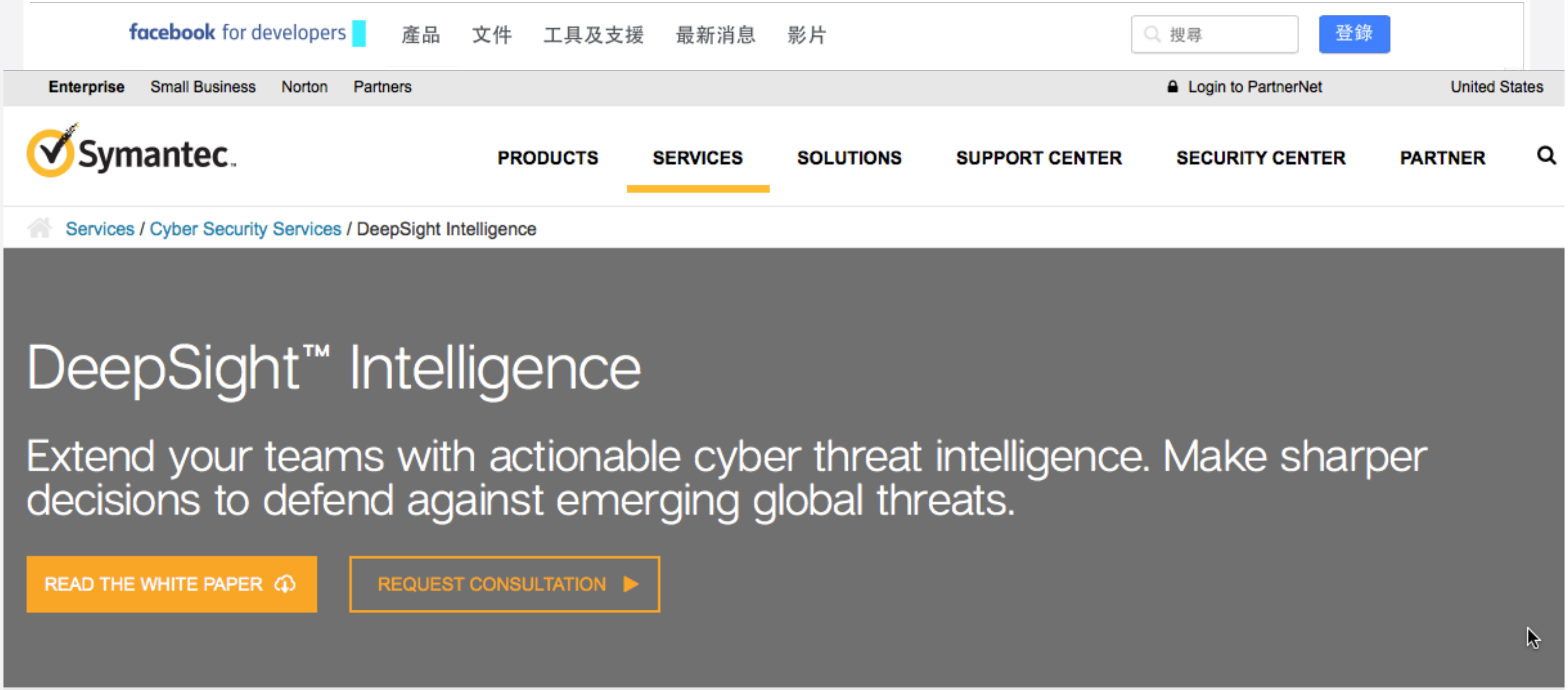
All three occurring within a 24-hour period

資訊安全共生系統



Delivery
Exploitation & Installation
Command & Control
Accomplish Mission
Threat intelligence
threatstream
NORSE
Symantec
PIERCE
iSIGHT PARTNERS
prelert
SCIANTA ANALYTICS
whiteops
CASPIDA
invincea
TREND MICRO
THREATCONNECT
Seculert
FORTSCALE
exabeam
FARSIGHT SECURITY
Blueliv.
Webroot SecureAnywhere
Network Activity/Security
f5
SOURCEfire
paloalto NETWORKS
FireEye
SONICWALL
corero
Blue Coat
zscaler
NetFlow LOGIC
cisco
proofpoint
Hillstone NETWORKS
tenable network security
BARRACUDA
ExtraHop
Gigamon
Check Point SOFTWARE TECHNOLOGIES LTD.
ARUBA networks
SHAPE SECURITY
vARMOUR
DAMBALLA
IMPERVA
Host Activity/Security
CYLANCE
Bit9
TANIUM
FireEye
Vormetric
RAPID7
DIGITALGUARDIAN
tripwire
CounterTack
FileTrek
syncsort
Hexis CYBER SOLUTIONS
Bromium
ziften
EnCase
paloalto NETWORKS
Auth - User Roles, Corp Context
QUALYS
ACTIVIDENTITY
servicenow
okta
salesforce
box
Infoblox
bmcsoftware Remedy
MobileIron
Incapsula
Dropbox
mocana

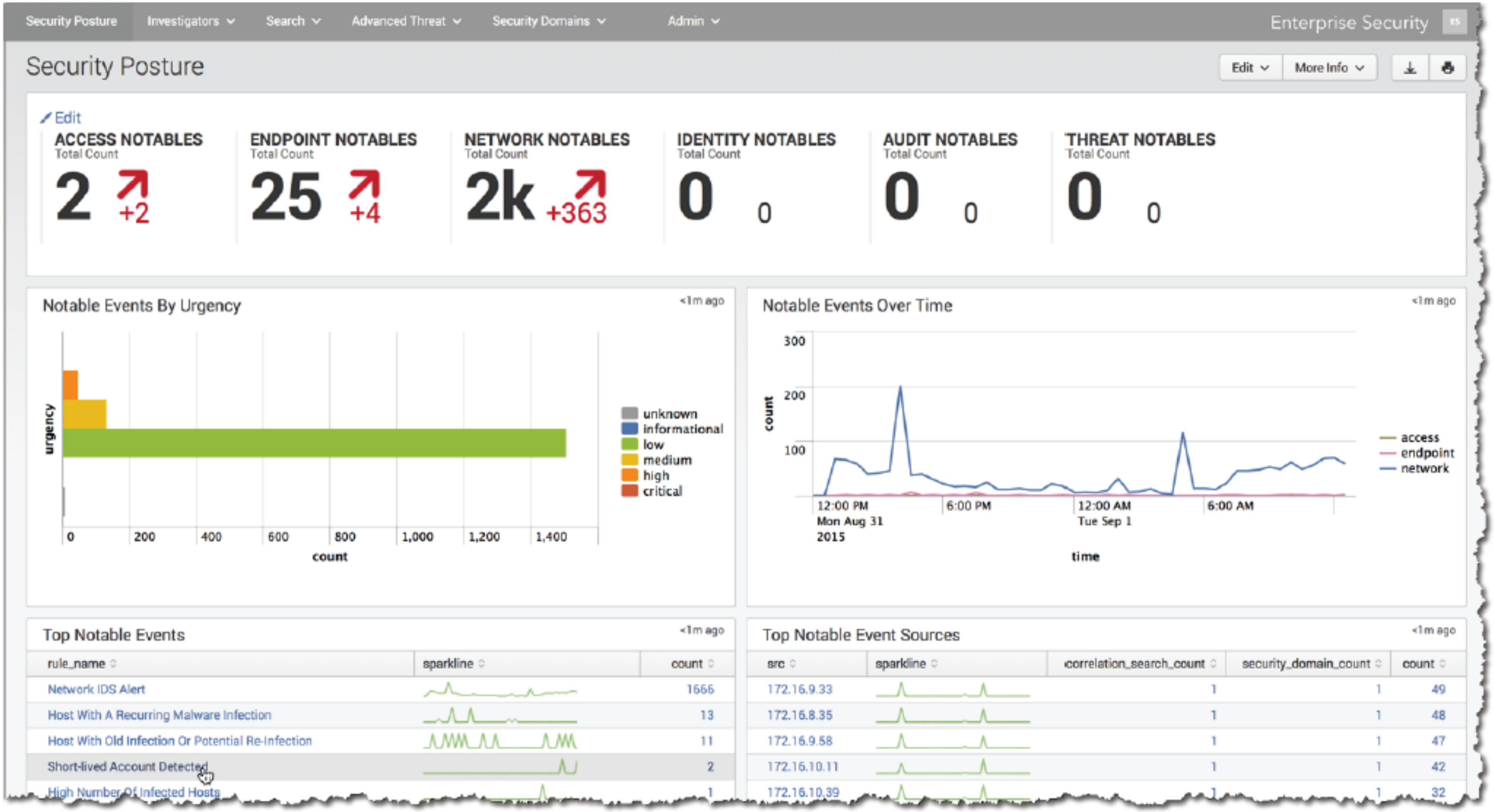
威脅情報分享及交換


facebook for developers
產品
文件
工具及支援
最新消息
影片
搜尋
登錄
Enterprise
Small Business
Norton
Partners
Login to PartnerNet
United States
Symantec.
PRODUCTS
SERVICES
SOLUTIONS
SUPPORT CENTER
SECURITY CENTER
PARTNER
Services / Cyber Security Services / DeepSight Intelligence
DeepSight™ Intelligence
Extend your teams with actionable cyber threat intelligence. Make sharper decisions to defend against emerging global threats.
READ THE WHITE PAPER
REQUEST CONSULTATION

工具及平台比較

- Free of Charge vs Free of Cost
- SoC vs SIEM
- Integrity 完整性
- Reliability 可依賴
- Scalability 延展性
- Accessible & Speedy 存取快速

資料處理及分析平台的重要性



專業服務 追求卓越

We Commit To Excellence