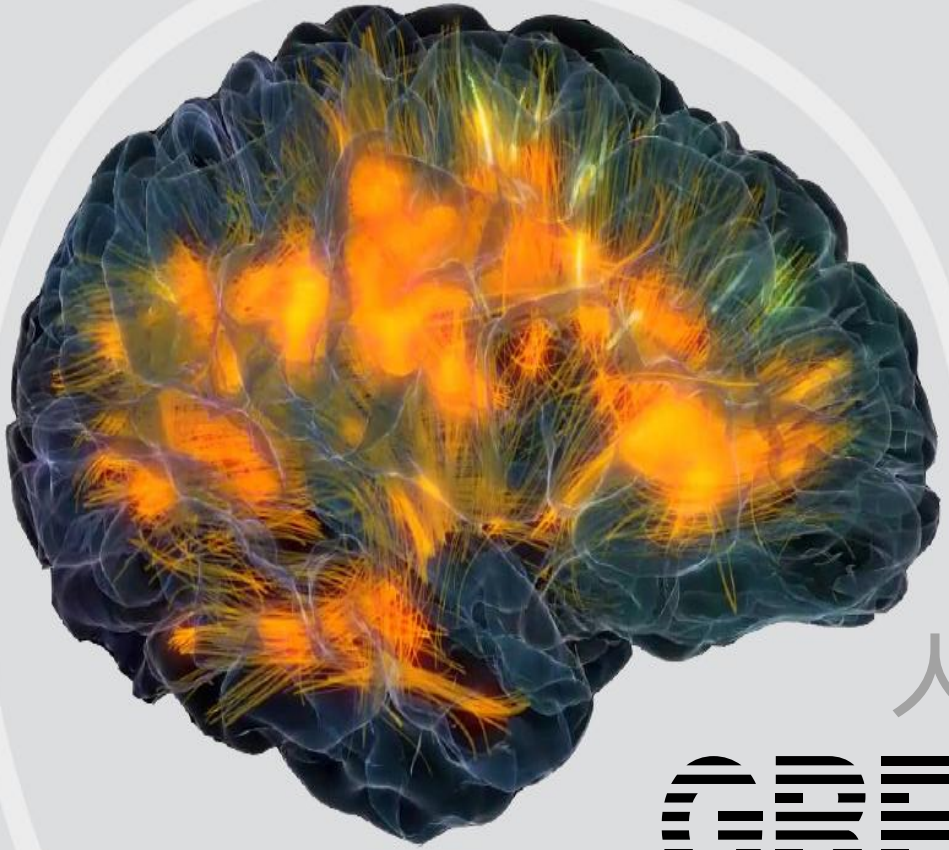
台灣獨家總代理

Version 2 台灣二版
www.version-2.com.tw



人工智慧監控軟體

GREYCORTEX

網路安全監控：APT入侵偵測與因應之道

Kenneth Lo 盧惠光 / 台灣二版 高級產品經理

2019 APT 攻擊分析

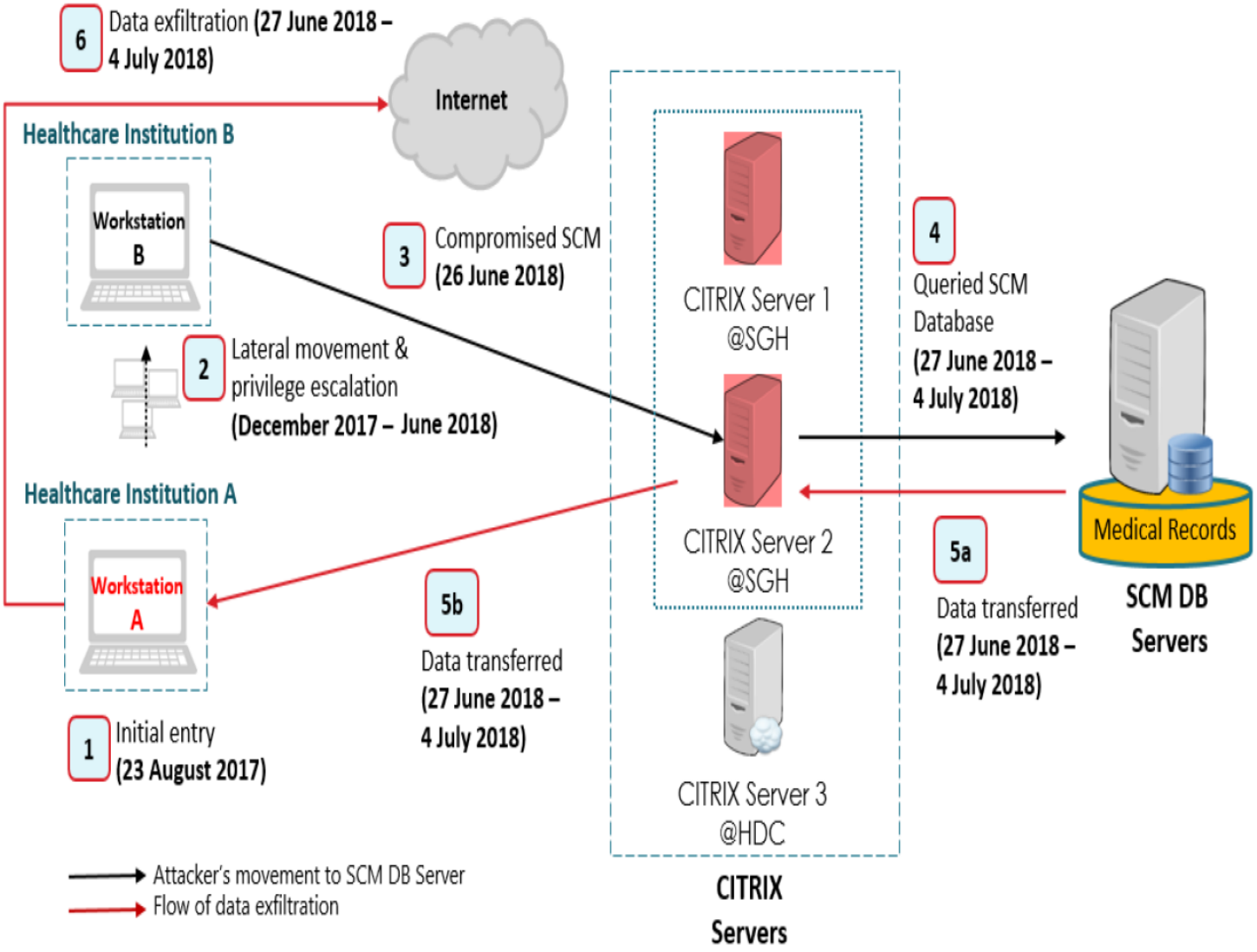
1. **“90%”的APT攻擊都在使用魚叉式網路釣魚且非常有效；成本大約為*2,000*美元(其中不包括零日漏洞利用的成本)。**

2. **滲透到內部網路後，”50%”的APT攻擊使用合法的管理工具和常用滲透測試軟體，軟體價格從*8,000*美元到*40,000*美元不等**

3. **根據估計，銀行攻擊所需工具的成本開始為*55,000*美元，網路間諜活動的成本要高得多，至少要*500,000*美元。**

*Source:https://www.ptsecurity.com/ww-en/analytics/advanced-persistent-threat-apt-attack-cost-report/

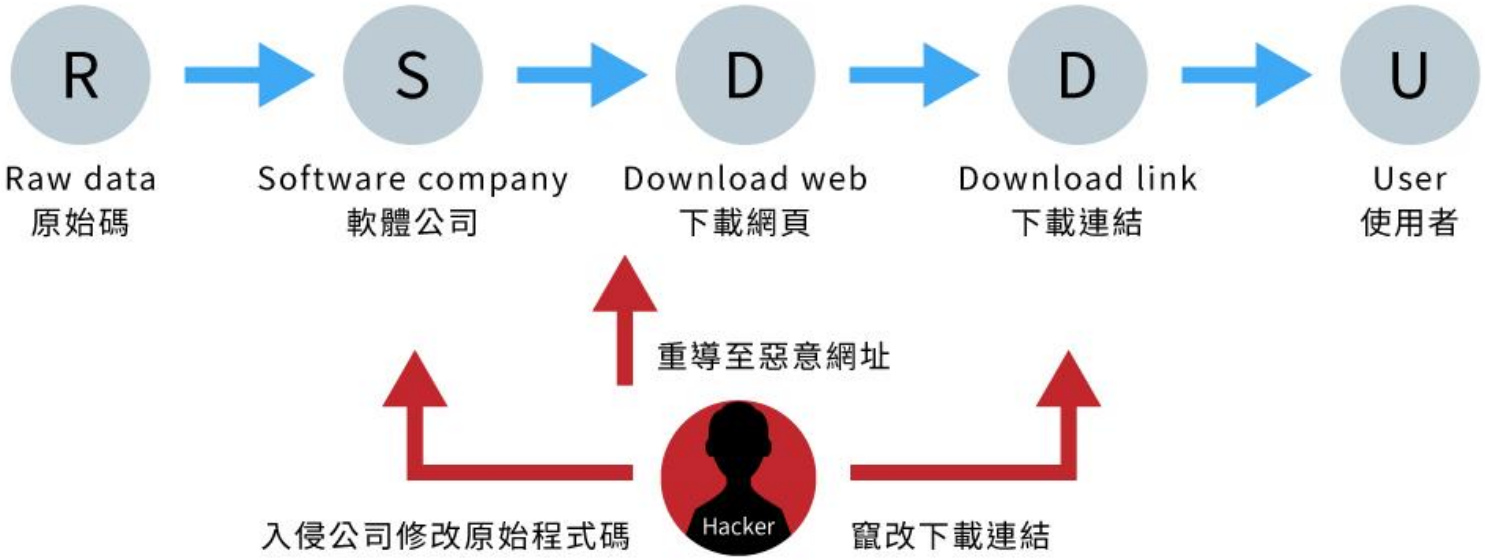
SINGHEALTH之駭客 APT 攻擊流程



從 APT 到供應鏈攻擊

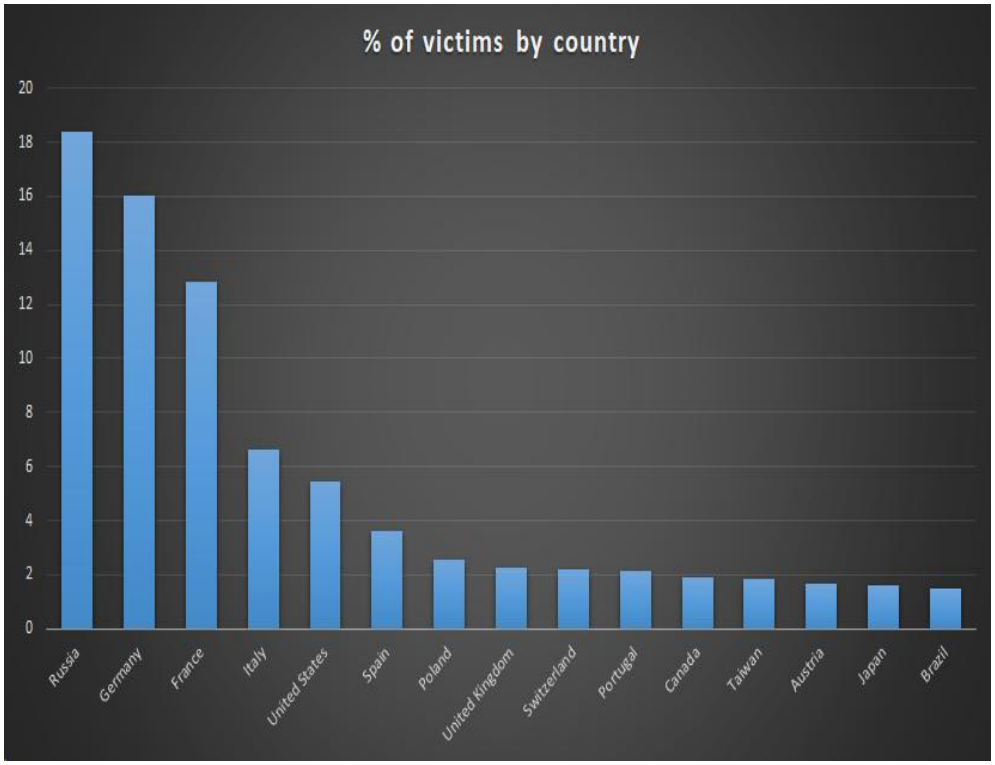
- 網路供應鏈原型 (參考來源: https://en.wikipedia.org/wiki/Supply_chain_attack)

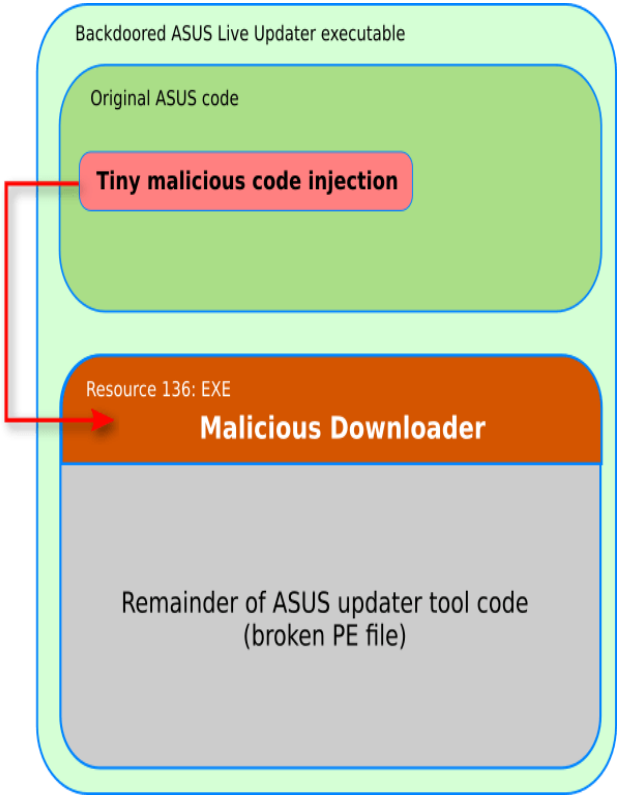
- 駭客攻擊有多種方式



***Source: http://www.cc.ntu.edu.tw/chinese/epaper/0044/20180320_4405.html**

知名品牌電腦的軟體更新伺服器遭供應鏈攻擊 (命名為SHADOWHAMMER 行動)





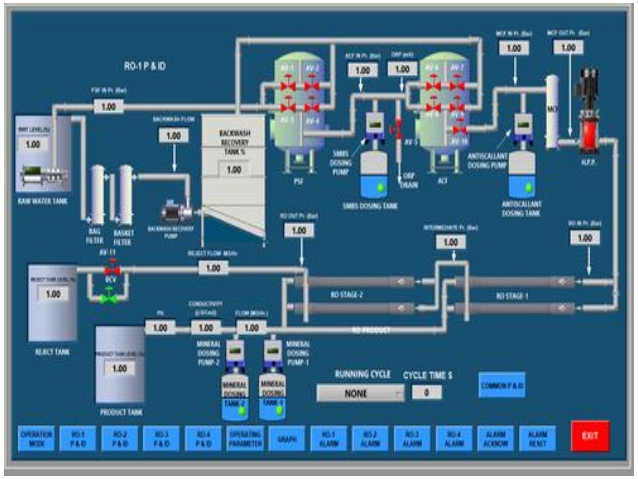
***Source:**
https://securelist.com/operation-shadowhammer/89992/
https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/
***軟體更新:**
https://www.asus.com/hk/support/FAQ/1018727/

建置GREYCORTEX MENDEL的目的在於...

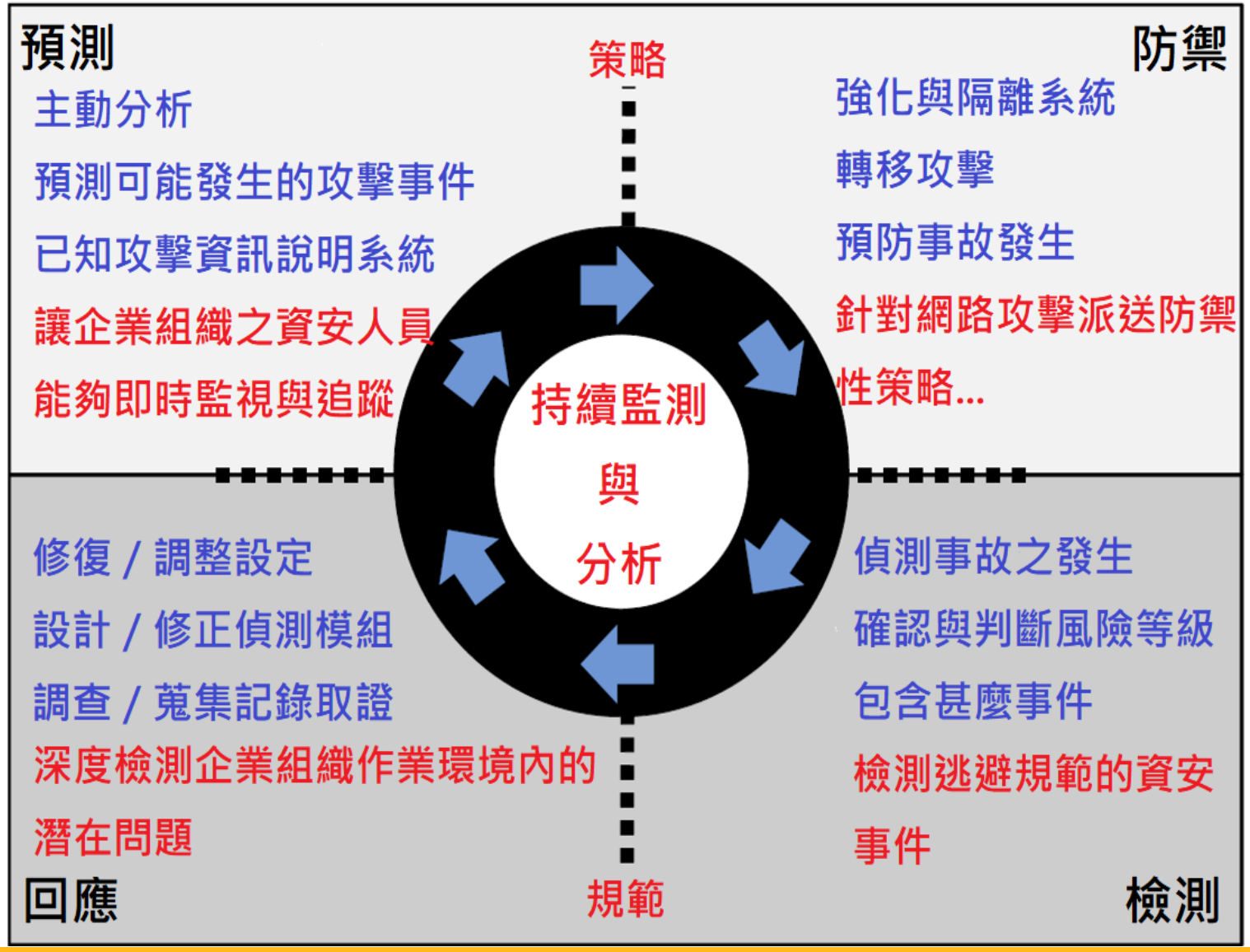
廣為流傳的
高級持續性
威脅(APT)

沒有網路
可視性

別忘了這些在您網路中之安全空隙...



SECURITY OPERATING CONTROLLER
應具備的偵防循環



Gartner NTA市場指南
5大網路安全要點

1. NTA在現代SOC中有著至關重要的作用
2. 行為是NTA的核心
3. 必須考慮可擴展性
4. 調查與偵查同等重要
5. 解密很重要

Gartner

Licensed for Distribution

Market Guide for Network Traffic Analysis

By Lawrence Orans, Jeremy D'Hoinne, Sanjit Ganguli

Published 28 February 2019 - ID G00381265 - 23 min read

Network traffic analysis is a new market, with many vendors entering since 2016. Here, we analyze the key NTA vendors to be considered by security and risk management leaders.

Overview

Key Findings

Recommendations

Market Definition

【Gartner Market Guide for NTA 2019】

Network Traffic Analysis is a new market, with many vendors entering since 2016. Gartner analyzed the key NTA vendors to be considered by security and risk management leaders.

***Source:**

https://www.forbes.com/sites/extrahop/2019/03/25/the-5-cybersecurity-takeaways-from-gartners-nta-market-guide/#1ebcffe570fd

https://www.gartner.com/en/documents/3902353/market-guide-for-network-traffic-analysis

外來和內部威脅！！！

- 企業內電腦或設備是否有被植入惡意程式？
- 企業內是否有內部攻擊或駭客行為？
- 有沒有駭客在偷取個資或商業機密？
- 企業內是否因設定錯誤而產生安全性漏洞？
- 如何保護各種 BYOD / IoT / 生產設備？

智能高效的網路監控？！

- 公司網內總共有多少台設備?
- 為什麼總有些內部系統很慢但找不出原因？
- 為什麼有些服務會塞車？
- 有沒有簡單易懂的網路效能報表？

架構

SPAN/MIRROR	威脅情報	LDAP/DC, DNS, DHCP	IDS 簽名, GEO IP, WHOIS

Signatures & DPI
Signatures & Deep Packet Inspection

基於簽名的檢測
- 已知惡意軟體
- 已知攻擊
- 已知漏洞
- 違法策略
- 高性能捕獲包

NBA
Network Behavior Analysis

基於行為的檢測
- 惡意軟體傳播活動，下載，垃圾郵件
- 攻擊者活動 - 掃描，暴力破解，試探
- C&C活動 - RAT，APT，AVT，僵屍，蠕蟲，rootkits ，資料洩露

Status
Network Statistics

可視性和性能
- 完整的網路可視性
- 應用性能
- 網路性能
- 應用程式和使用者意識

使用者介面, 報告 & 集成 (SIEM, Firewall, …)

1 企業內電腦或設備有否被植入惡意程式？

過度通訊 檢測到的威脅

該設備經常與2到8個網路服務進行通信及該設備試圖通過89項服務與全球142個節點進行通訊，包括中國，俄羅斯，歐盟，烏克蘭，美國和芬蘭

	Src Host	Src Subnet	Dst Host	Dst Subnet	Service
–	herishep (10.22.182.215)	WI-FI (10.22.180.0/22)			

Description

Anomalies caused by an excessive amount of communicating ports on the destination IP address (e.g. Port scan)

Recommendation

Check event details, please. In the case this is a legitimate communication, mark the event as False Positive.

Signature details

Signature ID: 3106
Created: 2015-05-
Class: Potentially
View Signa

- 5 outlier: Entropy (ports) at Host
- 5 outlier: Peers at Host
- 5 outlier: Data at Host
- 5 outlier: Flows at Host
- 5 p2p: BitTorrent peer sync
- 5 p2p: BitTorrent DHT ping request
- 5 p2p: BitTorrent DHT announce_peers request

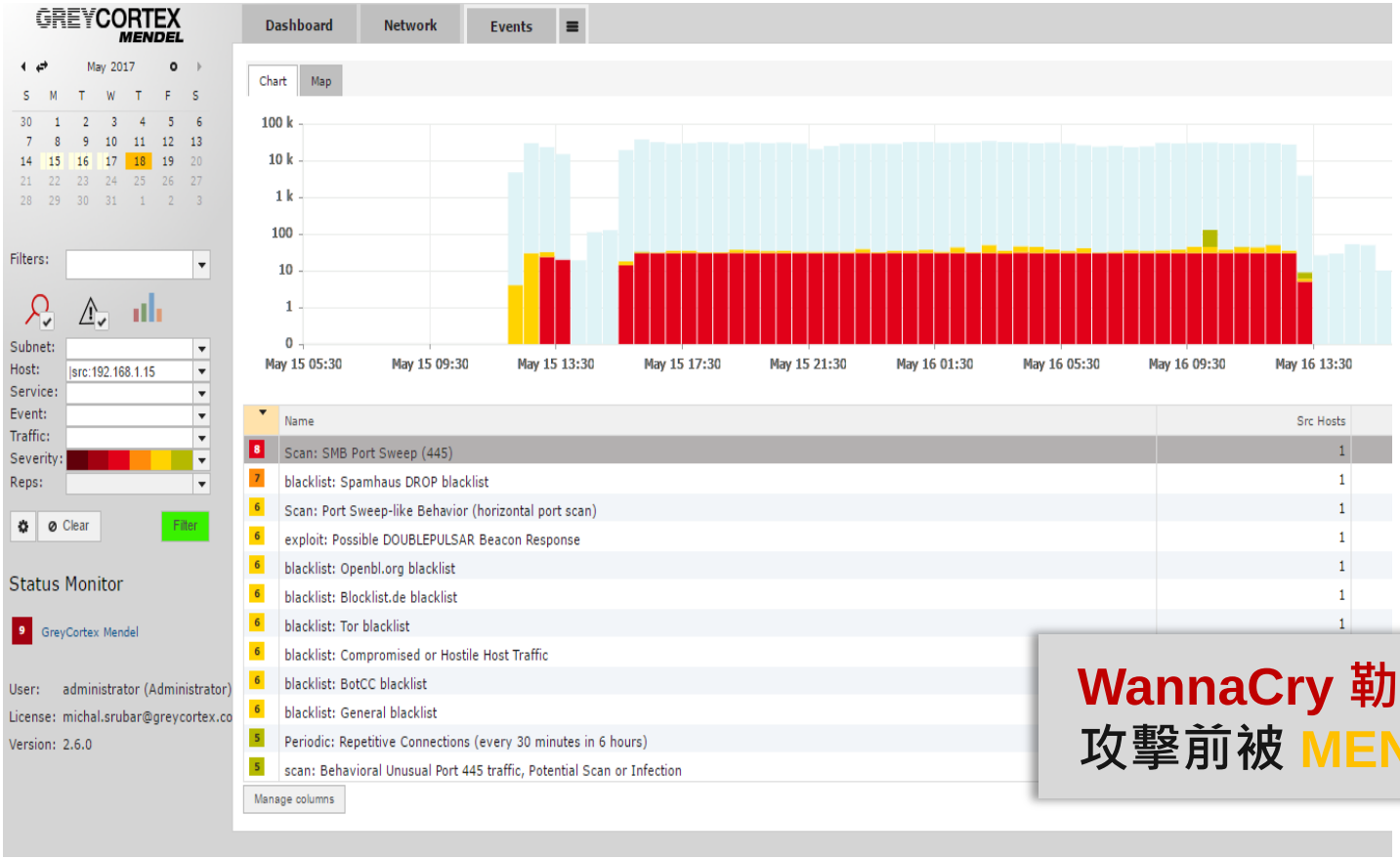
Events Stats | Current Model

Metric	Measured										All	
	All		In ⇩ ♀		In ⇩ ♂		Out ⇧ ♀		Out ⇧ ♂			
Flows	220	30x			44	117x					7.19	± 13.70
Peers	142	27x							133	28x	5.11	± 8.75
Ports	89	32x							83	35x	2.70	± 4.41

1 企業內電腦或設備有否被植入惡意程式？

流量分析

檢測行為模式描述的威脅



WannaCry 勒索軟體, 在攻擊前被 MENDEL 發現

台灣獨家總代理

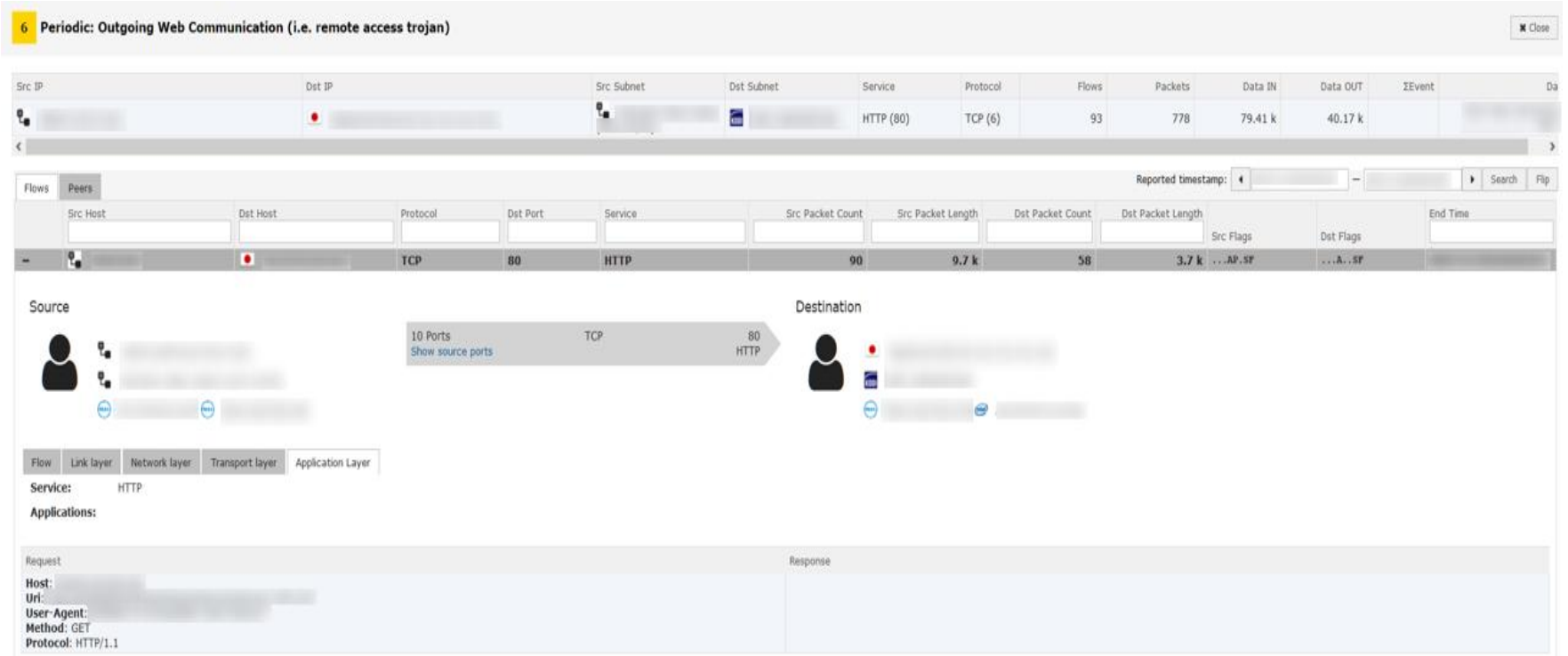
Version 2 台灣二版 www.version-2.com.tw

GREYCORTEX

1 企業內電腦或設備有否被植入惡意程式？

週期性通信

定期與可疑的IP位址進行通訊， 網路中繼資料被歸類為異常， 用戶可能安裝了未知惡意軟體



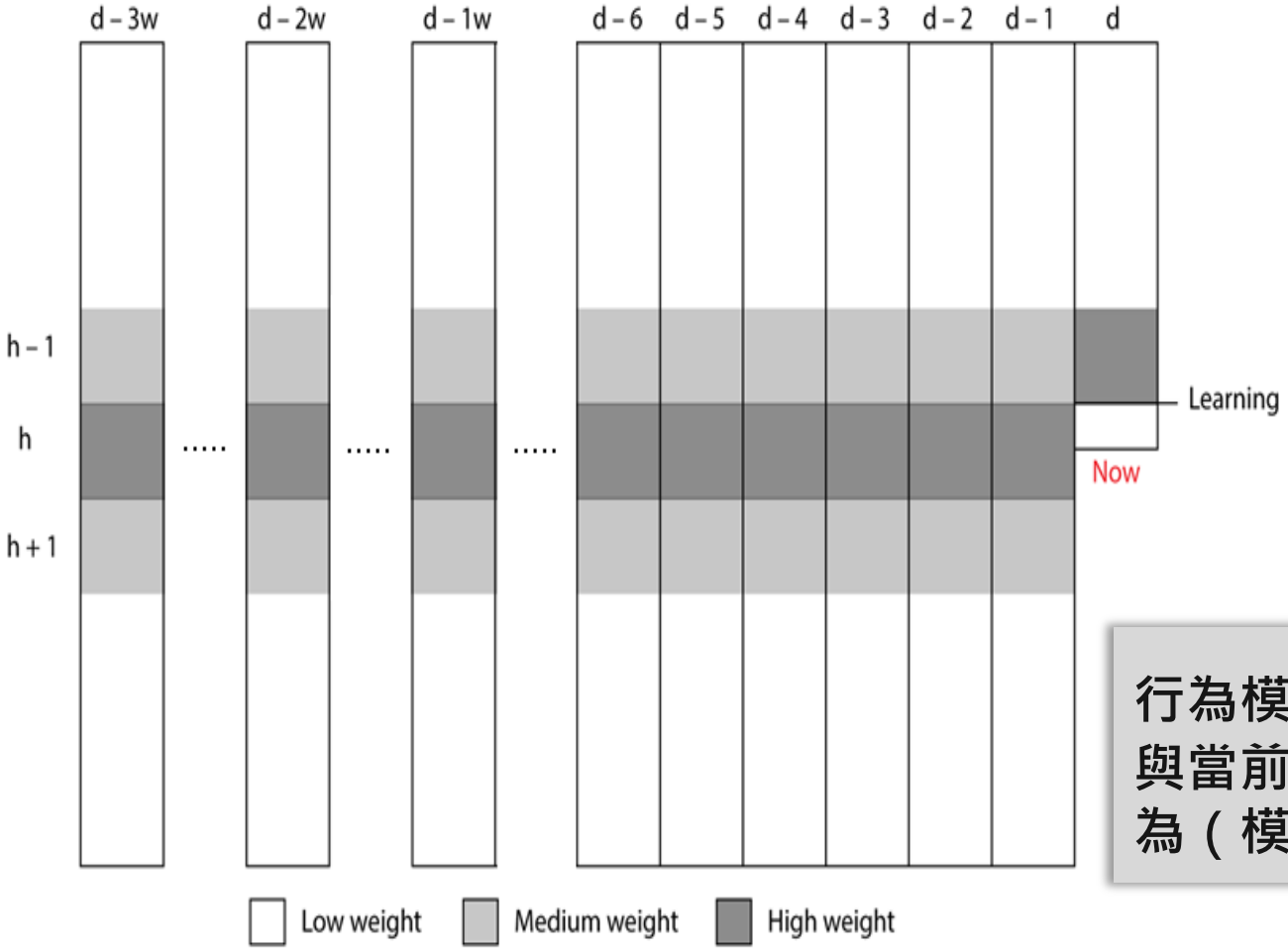
台灣獨家總代理

Version 2 台灣二版 www.version-2.com.tw

GREYCORTEX

企業內有否內部攻擊或駭客行為？

人工智慧機器學習

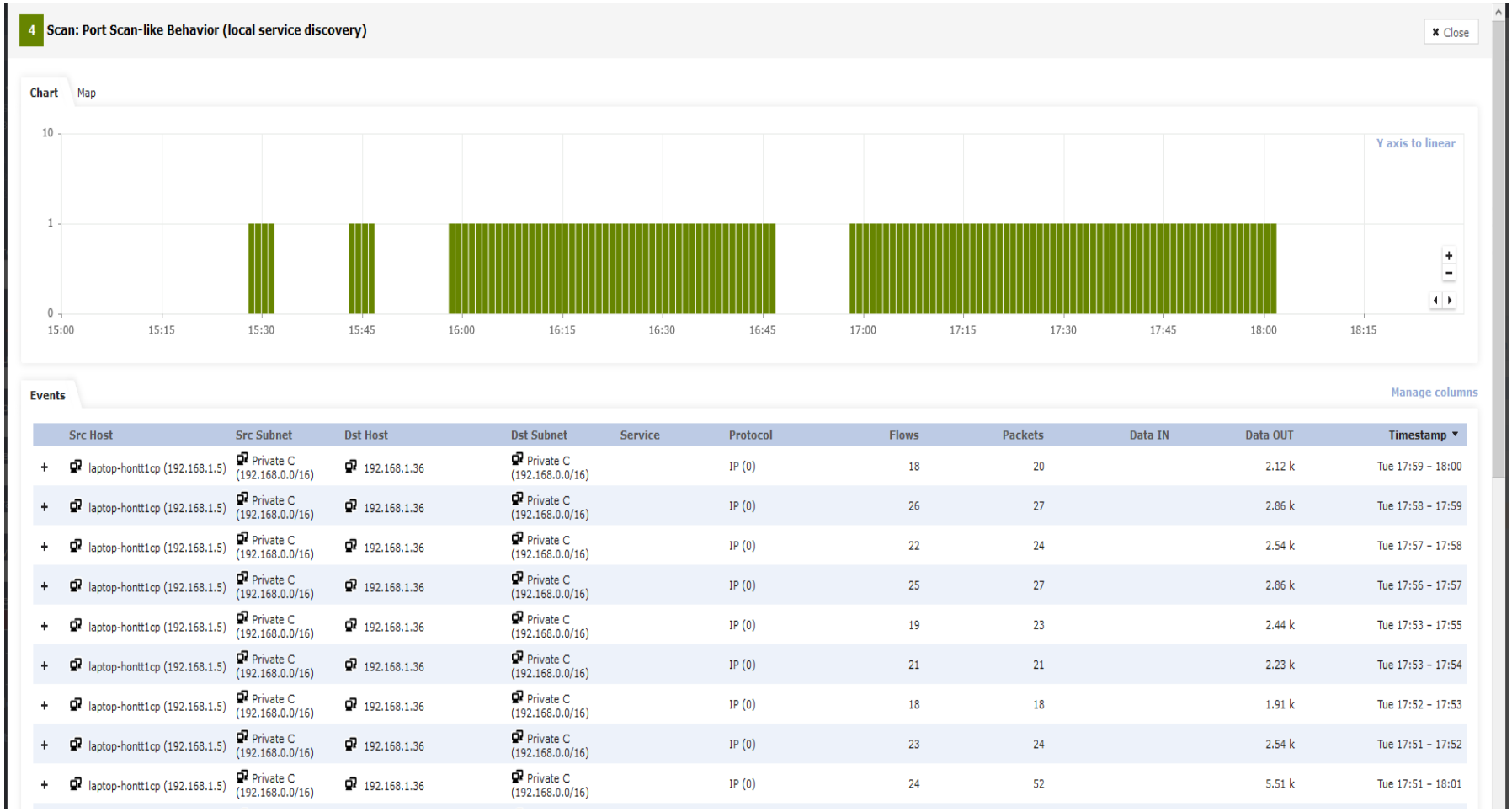


行為模型可存儲**30** 天並與當前流量及歷史學習行為（模型）進行比較

2 企業內有否內部攻擊或駭客行為？

掃瞄活動

通訊源正試著連接目標設備(機器)的多個端口



Src Host	Src Subnet	Dst Host	Dst Subnet	Service	Protocol	Flows	Packets	Data IN	Data OUT	Timestamp
laptop-hontt1cp (192.168.1.5)	Private C (192.168.0.0/16)	192.168.1.36	Private C (192.168.0.0/16)		IP (0)	18	20		2.12 k	Tue 17:59 - 18:00
laptop-hontt1cp (192.168.1.5)	Private C (192.168.0.0/16)	192.168.1.36	Private C (192.168.0.0/16)		IP (0)	26	27		2.86 k	Tue 17:58 - 17:59
laptop-hontt1cp (192.168.1.5)	Private C (192.168.0.0/16)	192.168.1.36	Private C (192.168.0.0/16)		IP (0)	22	24		2.54 k	Tue 17:57 - 17:58
laptop-hontt1cp (192.168.1.5)	Private C (192.168.0.0/16)	192.168.1.36	Private C (192.168.0.0/16)		IP (0)	25	27		2.86 k	Tue 17:56 - 17:57
laptop-hontt1cp (192.168.1.5)	Private C (192.168.0.0/16)	192.168.1.36	Private C (192.168.0.0/16)		IP (0)	19	23		2.44 k	Tue 17:53 - 17:55
laptop-hontt1cp (192.168.1.5)	Private C (192.168.0.0/16)	192.168.1.36	Private C (192.168.0.0/16)		IP (0)	21	21		2.23 k	Tue 17:53 - 17:54
laptop-hontt1cp (192.168.1.5)	Private C (192.168.0.0/16)	192.168.1.36	Private C (192.168.0.0/16)		IP (0)	18	18		1.91 k	Tue 17:52 - 17:53
laptop-hontt1cp (192.168.1.5)	Private C (192.168.0.0/16)	192.168.1.36	Private C (192.168.0.0/16)		IP (0)	23	24		2.54 k	Tue 17:51 - 17:52
laptop-hontt1cp (192.168.1.5)	Private C (192.168.0.0/16)	192.168.1.36	Private C (192.168.0.0/16)		IP (0)	24	52		5.51 k	Tue 17:51 - 18:01

3 員工有否有意或無意間洩漏個資或商業機密？

TOR管道

可能透過TOR網路和其他通道傳輸洩漏資料

台灣獨家總代理

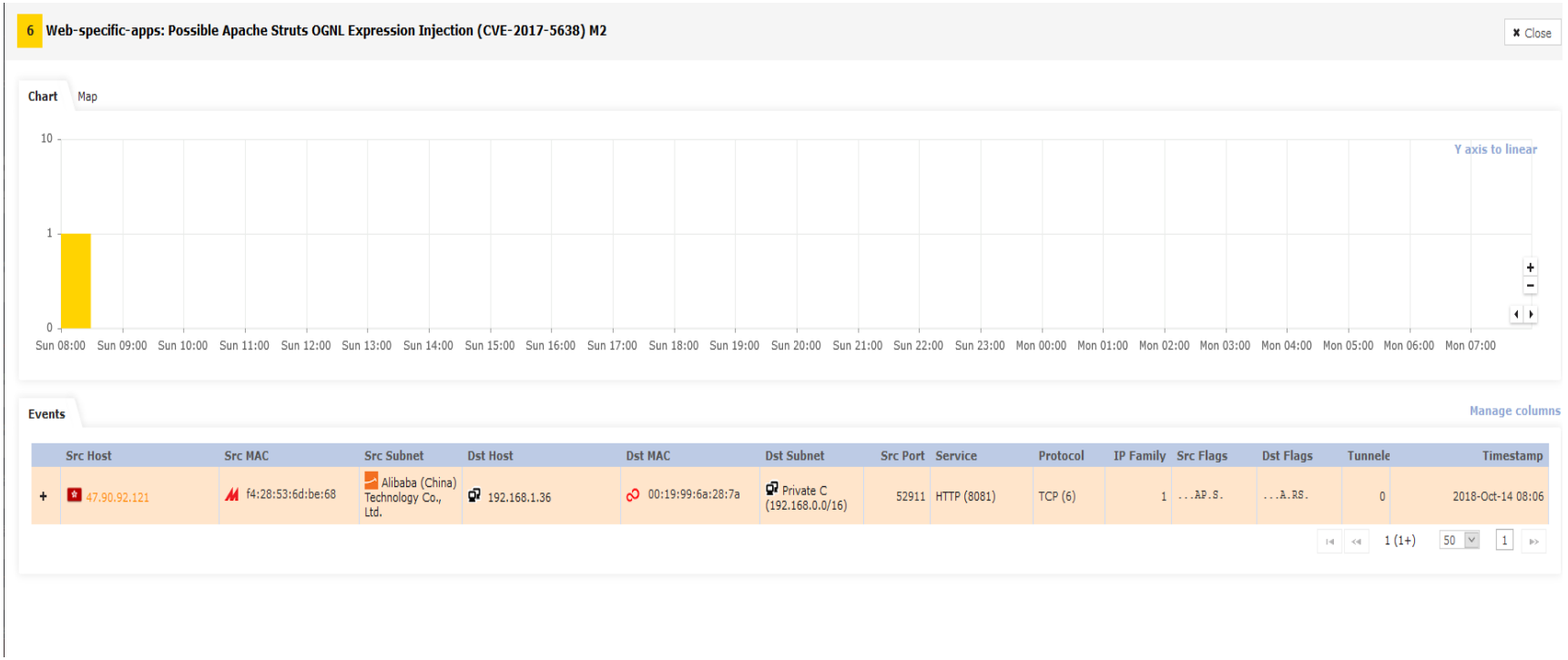
Version 2 台灣二版 www.version-2.com.tw

GREYCORTEX

企業內有否設定錯誤而產生安全性漏洞？

漏補/錯誤設置伺服器

未修補的系統不僅可以存在於PC和服務器上，還可以存在於物聯網設備和客戶機上



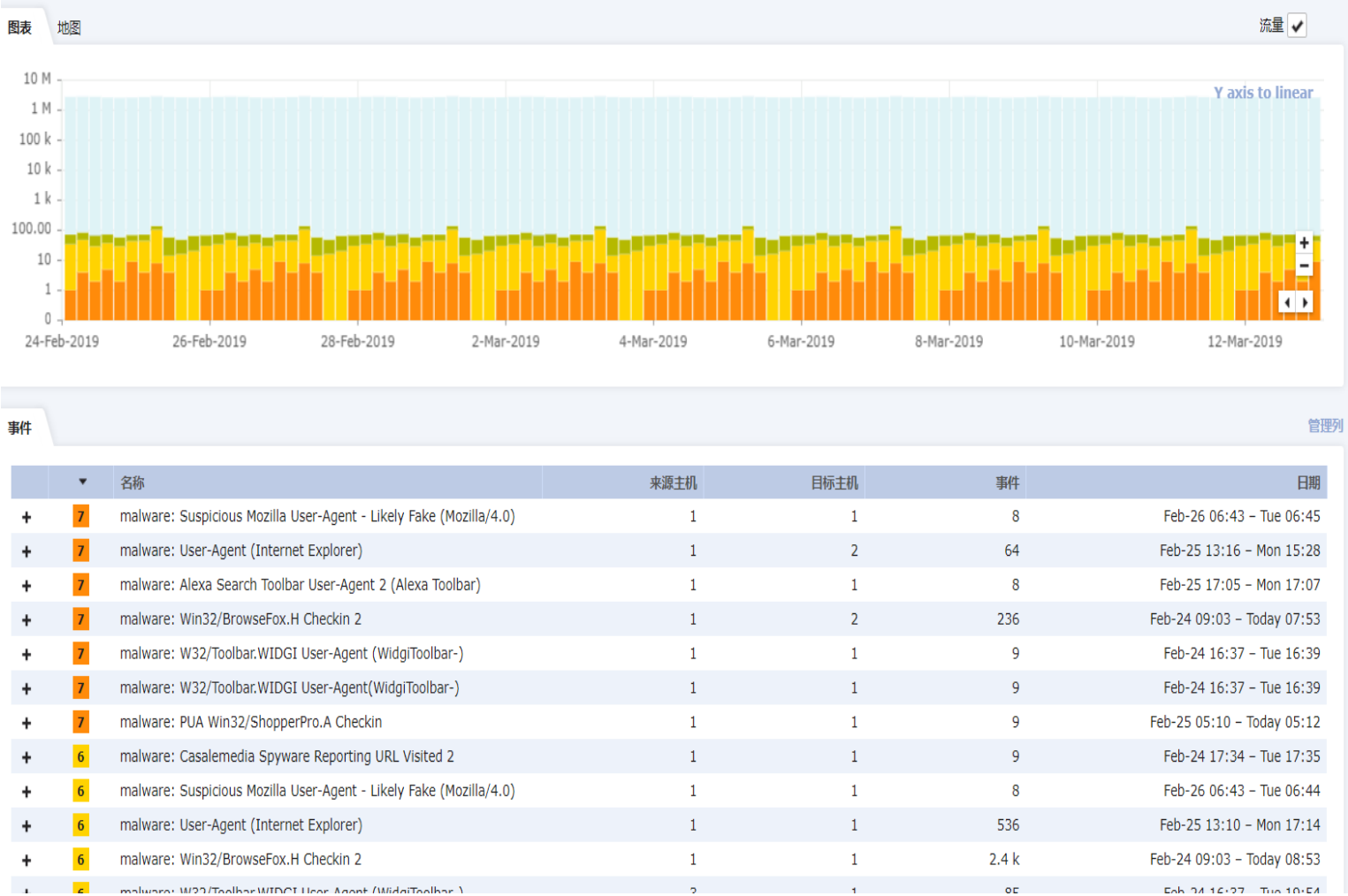
台灣獨家總代理

Version 2 台灣二版 www.version-2.com.tw

GREYCORTEX

如何保護各種 BYOD / IoT 設備 ??

受感染移動設備



		名称	来源主机	目标主机	事件	日期
+	7	malware: Suspicious Mozilla User-Agent - Likely Fake (Mozilla/4.0)	1	1	8	Feb-26 06:43 – Tue 06:45
+	7	malware: User-Agent (Internet Explorer)	1	2	64	Feb-25 13:16 – Mon 15:28
+	7	malware: Alexa Search Toolbar User-Agent 2 (Alexa Toolbar)	1	1	8	Feb-25 17:05 – Mon 17:07
+	7	malware: Win32/BrowseFox.H Checkin 2	1	2	236	Feb-24 09:03 – Today 07:53
+	7	malware: W32/Toolbar.WIDGI User-Agent (WidgiToolbar-)	1	1	9	Feb-24 16:37 – Tue 16:39
+	7	malware: W32/Toolbar.WIDGI User-Agent(WidgiToolbar-)	1	1	9	Feb-24 16:37 – Tue 16:39
+	7	malware: PUA Win32/ShopperPro.A Checkin	1	1	9	Feb-25 05:10 – Today 05:12
+	6	malware: Casalemedia Spyware Reporting URL Visited 2	1	1	9	Feb-24 17:34 – Tue 17:35
+	6	malware: Suspicious Mozilla User-Agent - Likely Fake (Mozilla/4.0)	1	1	8	Feb-26 06:43 – Tue 06:44
+	6	malware: User-Agent (Internet Explorer)	1	1	536	Feb-25 13:10 – Mon 17:14
+	6	malware: Win32/BrowseFox.H Checkin 2	1	1	2.4 k	Feb-24 09:03 – Today 08:53

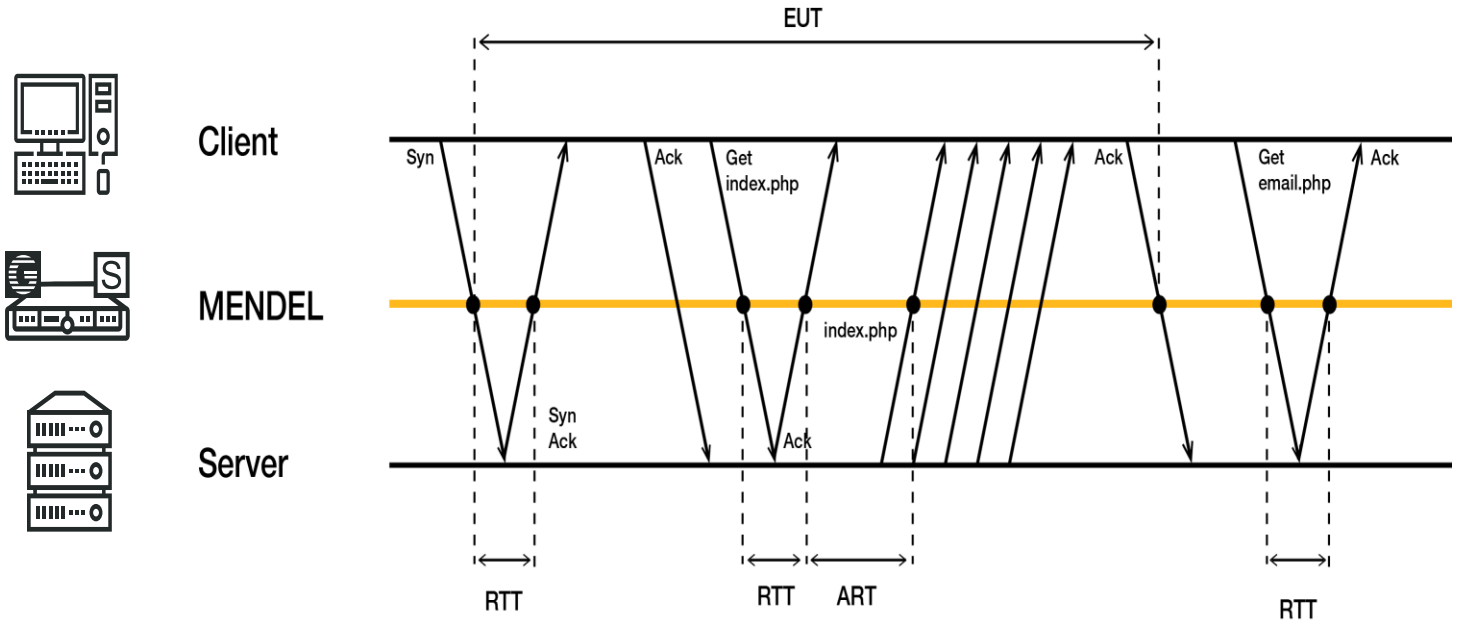
1 為什麼總有些內部系統很慢但找不出原因？

網絡監控

網路和應用程式的性能（全系列埠(port) 0 – 65535）

使用應用程式中繼資料識別應用程式

監控當前和平均頻寬，用戶和伺服器回應時間，網路回應時間，使用中的埠(port)，連接節點等



2 為什麼有些服務會塞車？

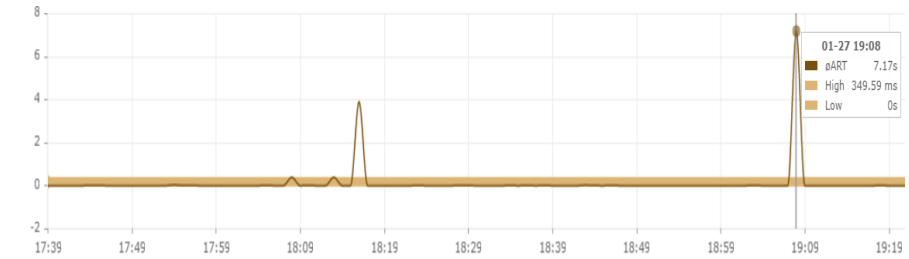
MS-SQL性能異常

MS-SQL的異常過度回應時間為30s

2 為什麼有些服務會塞車？

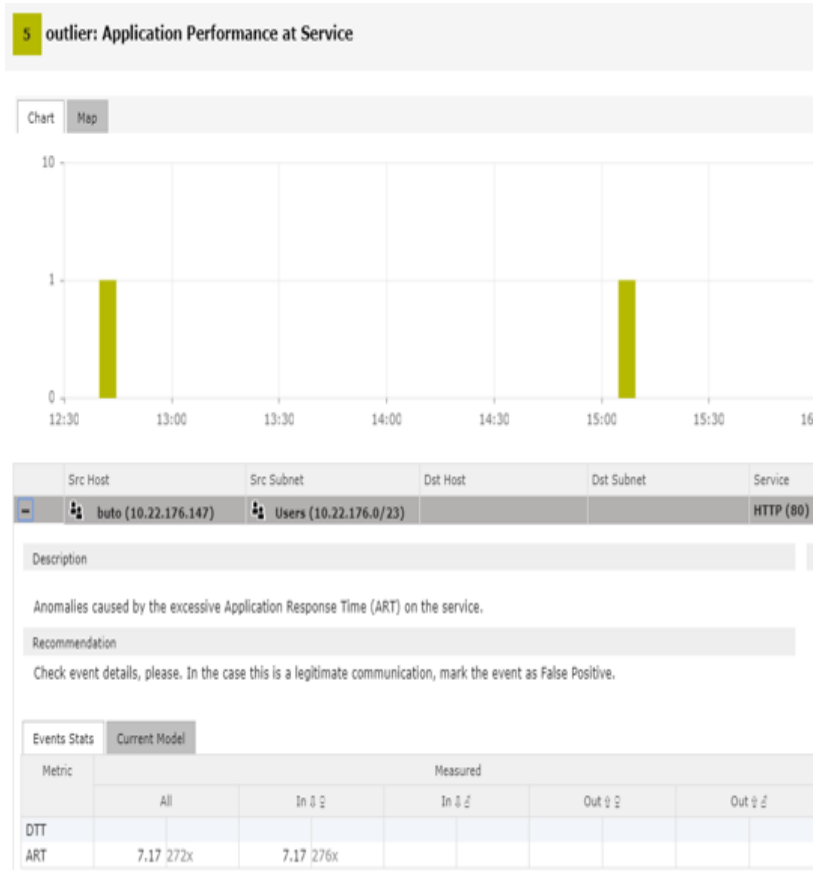
HTTP性能異常

HTTP的異常過度回應時間為7秒，比該伺服器的平常回應高272倍



Sum | Current | Model

Service	Port	Service Type	Protocol	Flows	Packets	Data [B]	Data ⇩ [B]
HTTP	80	LOCAL	TCP (6)	1.45 k	338.09 k	351.72 M	16.71 M
HTTP	80	REMOTE	TCP (6)	2	2	128	128



台灣獨家總代理

Version 2 台灣二版 www.version-2.com.tw

GREYCORTEX

快速部署 快速掌握

MENDEL快速偵測

1 分鐘- 6 小時

MENDEL 的平均偵測時間

設定快速的部署

30 - 60 Minutes

MENDEL 的平均部署時間

監控效能與視覺化網路

網路可靠性

過度連線

新加入的設備

有漏洞的程式

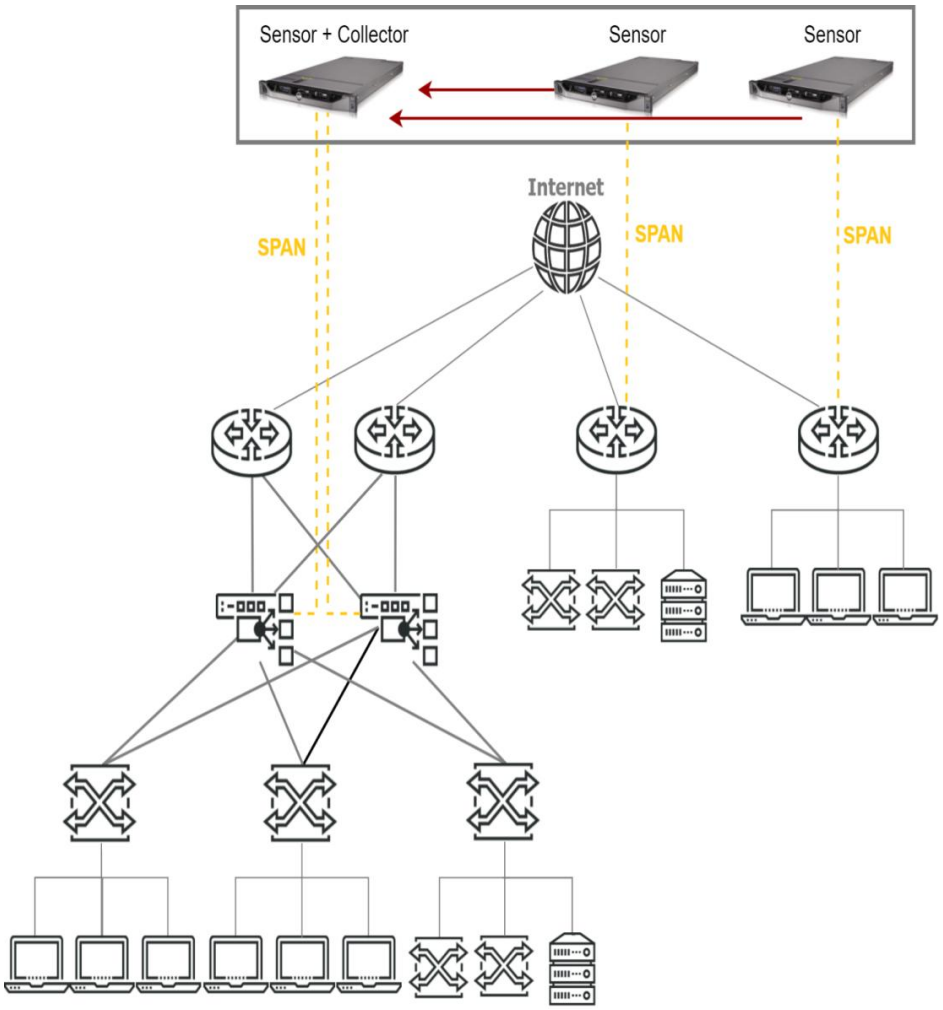
直覺式的操作界面

事件過濾

自訂介面

簡易偵測

部署



探測器

- 核心交換機/TAP的鏡像
- ASNM 輸出(= 0,5% - 1% 流量)
- 高達 10Gbps/探測器

收集器

- 1 收集器= 10+ 探測器
- 聚合輸入高達 40Gbps+
- 集中收集所有事件

設備

- 被動的
- 前置的
- 硬體或虛擬化部署(VMware ESXi, Hyper-V, KVM…)

GREYCORTEX MENDEL

深入的 威脅檢測

應用程式及網路的 性能監控

詳細 網路的可視性

台灣獨家總代理

Version 2 台灣二版
www.version-2.com.tw

人工智慧監控軟體

GREYCORTEX

感謝聆聽

歡迎至【台灣二版攤位】洽詢