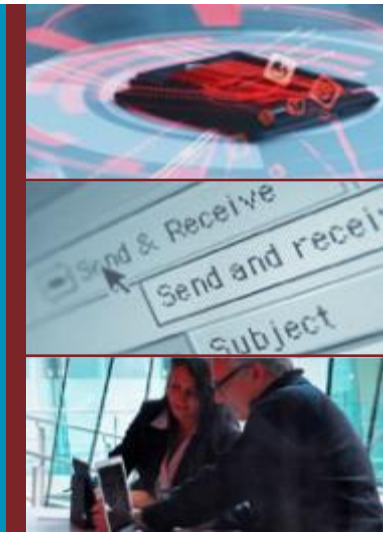
proofpoint

Proofpoint Threat Response

威脅應變管理平台產品介紹



2015年1月16日

threat protection | compliance | archiving & governance | secure communication

阿碼證點

攻擊發生迅速產生影響

滲漏迅速

46%

- 一旦攻擊發生**數分鐘**或**數秒鐘**內即開始發生滲漏現象。

應變緩慢

90%

- 從偵測到控制估計需要**數天**或**更長的時間**。

1 – Verizon 2014 Data Breach Report

資訊安全人才培養不易

62%
的組織
在2014年沒有增加安全培訓

1/3
的資安專家
不熟悉進階式持續性威脅(APT)

<2.4%
的應屆畢業生
持有電子計算機學位

1 Million
世界各地懸缺資訊安全工作

83%的企業
目前缺乏合適技能和人力資源以保護他們的IT資產

非營利組織 ISACA 2014 APT Survey
http://www.businesswire.com/news/home/20140708006700/en/ISACA-Global-Study-Organizations-Prepared-Advanced-Cyberthreats#.U4ewMBZnh4M

阿碼證點 proofpoint

企業面臨資安事件應變的挑戰

- 不斷上升的攻擊量
- 攻擊發生迅速產生衝擊
- 有經驗的資源非常難找

- 攻擊透不同系統擴散開來
- 現行處理流程過於人工化

當今事件應變處理過程

1

INVESTIGATE (調查)

2

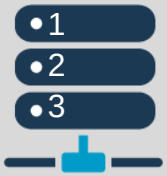
VERIFY (驗證)

重複
每一個
資安警示

4

CONTAIN (控制)

3



PRIORITIZE (排序)

人工處理所面臨的困境

- **資料收集→過程繁瑣**
  有效分析需要更多的事件背景資料，但這是個艱辛而緩慢的收集過程
- **誤報事件→徒勞無功**
  「誤報」造成IT單位、終端用戶必須付出龐大的成本及工作效率的影響
- **超量工作→疲於奔命**
  雖然先進檢測工具提高偵測量，但也增加了過度負荷團隊的工作量
- **冗長協調→效率不彰**
  網路與資安應變團隊的協調工作，有時候會延遲數小時、數天，甚至數週
- **設備配置→百般無奈**
  橫跨各種廠商資安專有設備的配置問題

Proofpoint 威脅應變管理平台

- 是一個內部部署(on-premise)的軟體平台，能夠讓IT資安團隊**即時**進行事件威脅應變管理：
  - 資安事件關聯的收集、驗證及分析
  - 事件的評估與訂定優先次序
  - 即時隔離、封鎖受感染的系統、及更新網路層級，以阻止對外通信
  - 「單一管理平台」能夠統一事件監看、威脅核分及牽制活動

自動關聯、優先次序及控制

〈檢測〉

proofpoint TAP

FireEye

ArcSight

paloalto NETWORKS

splunk>

Radar

proofpoint

關聯性及確認

Windows Server Active Directory · VIRUS TOTAL · who.is · URLVoid

自動化

評估

應變優先次序

持續性

控制

控制及隔離

立即性

〈防禦〉

CISCO

JUNIPER NETWORKS

Microsoft

paloalto NETWORKS

Check Point SOFTWARE TECHNOLOGIES LTD.

BlueCoat

FORTINET

阿碼證點

proofpoint

自動關聯→自動化控制

安全警示

proofpoint

事件關聯

身分

使用者

群組

網路

IP地理位置

信譽

電腦感染指標(IOC)

應需收集器

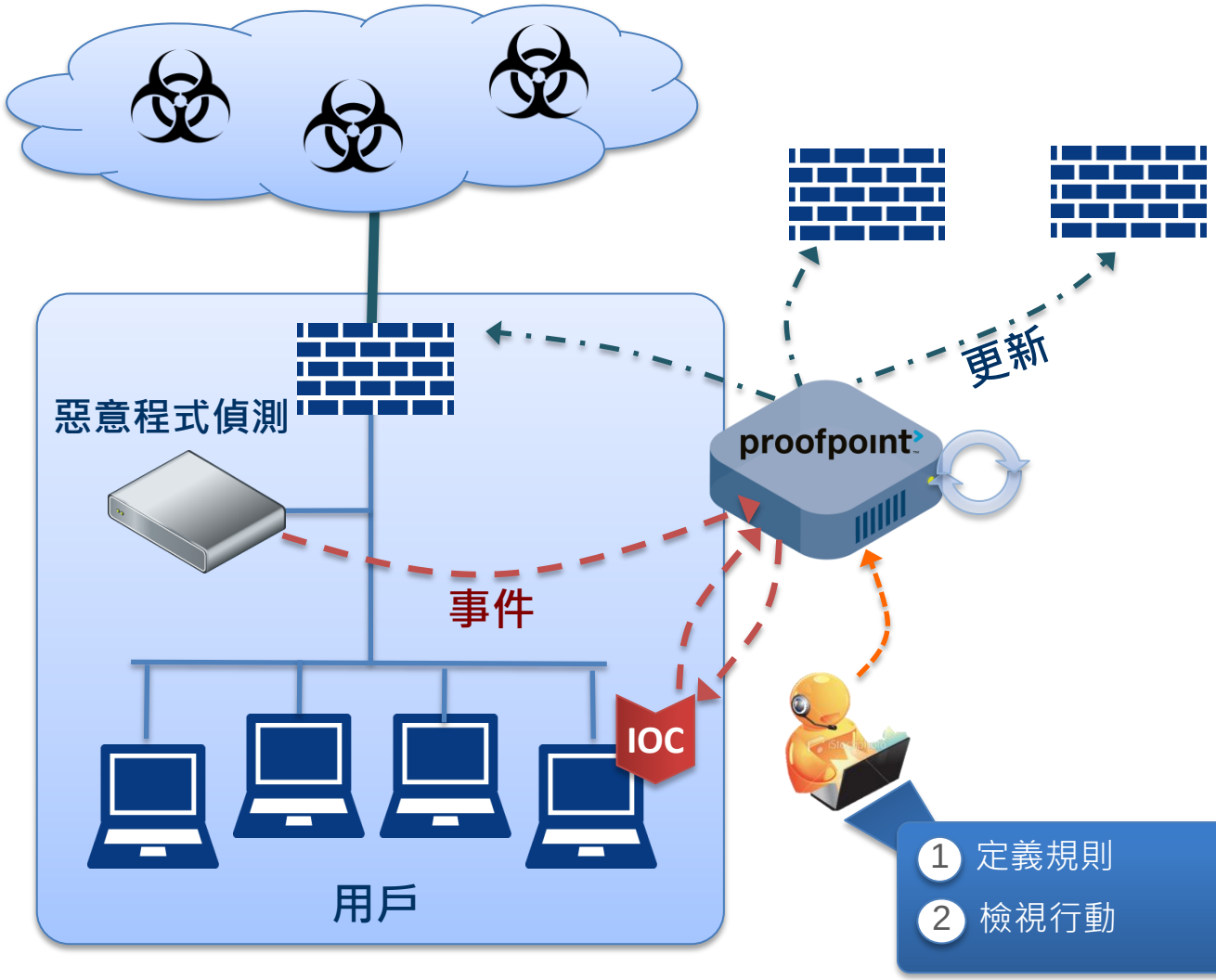
IOC
資料庫

自動化

業界邏輯

回應

大幅縮短偵測到控制的時間

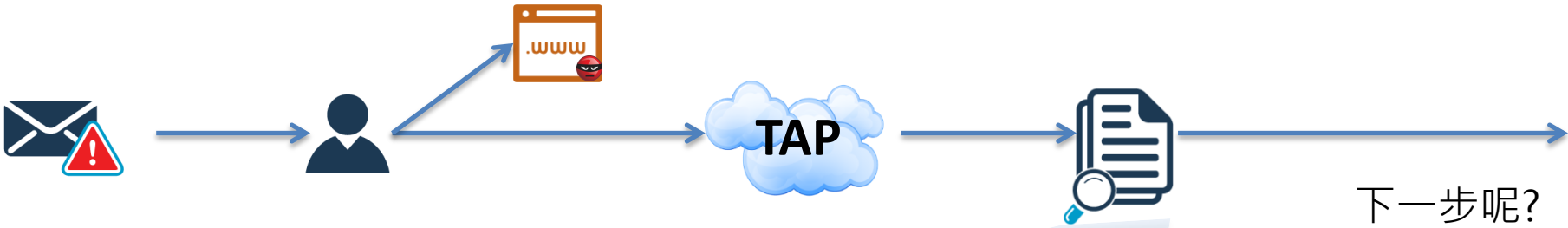


15個常見 IOC (Indicator of Compromise)

1	不尋常的出站網路流量
2	特權用戶帳戶異常活動
3	違反地理常規 (Geographical Irregularities)
4	其他登錄違規現象
5	資料庫讀取量驟升
6	HTML回覆大小(response size)
7	同一個檔案有大量的請求
8	不匹配的埠應用流量
9	可疑的註冊表或系統檔案變更
10	DNS請求異常
11	系統中非預期的修補
12	行動設備配置文件的更改
13	在錯誤的地方有大量的資料
14	非人性的網站流量
15	DDoS活動的徵象

Proofpoint TAP

是誰點擊惡意連結?

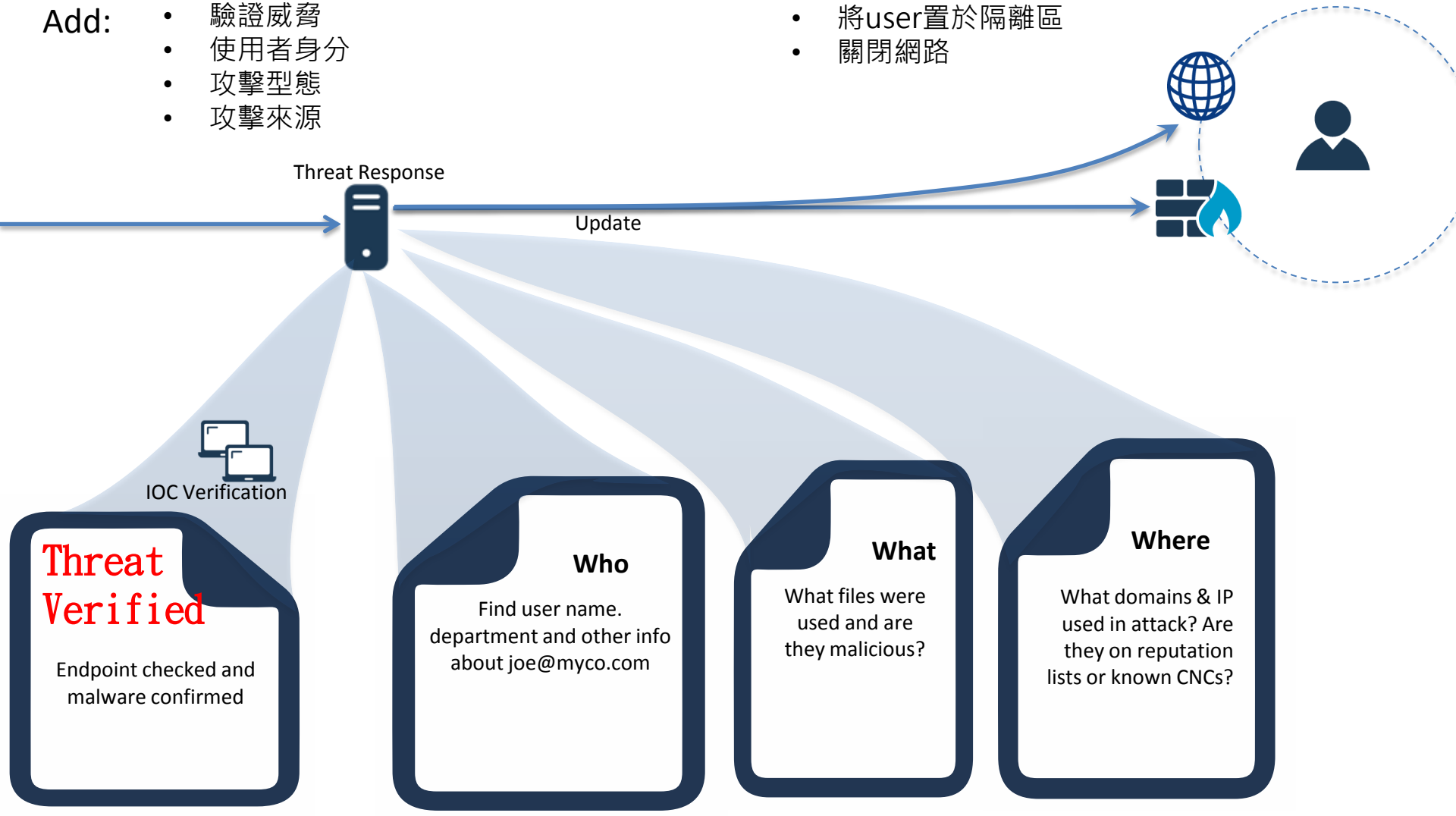


Email: joe@myco.com
Sender IP: 10.10.10.253
Clicked URL: http://waterhole.me?xy

Value Add: TAP+Threat Response

Add:

- 驗證威脅
- 使用者身分
- 攻擊型態
- 攻擊來源
- 將user置於隔離區
- 關閉網路



阿碼證點 proofpoint

Proofpoint 威脅應變管理作用

偵測 | 調查 | 驗證 | 排序 | 控制

FireEye
proofpoint TAP
paloalto NETWORKS

ArcSight
Radar
splunk>
LogRhythm

THREAT RESPONSE

MANDIANT

EnCase

CISCO
paloalto NETWORKS
Check Point SOFTWARE TECHNOLOGIES LTD.
BlueCoat
FORTINET
websense ESSENTIAL INFORMATION PROTECTION™
JUNIPER NETWORKS

Proofpoint 威脅應變管理平台的價值

快速應變

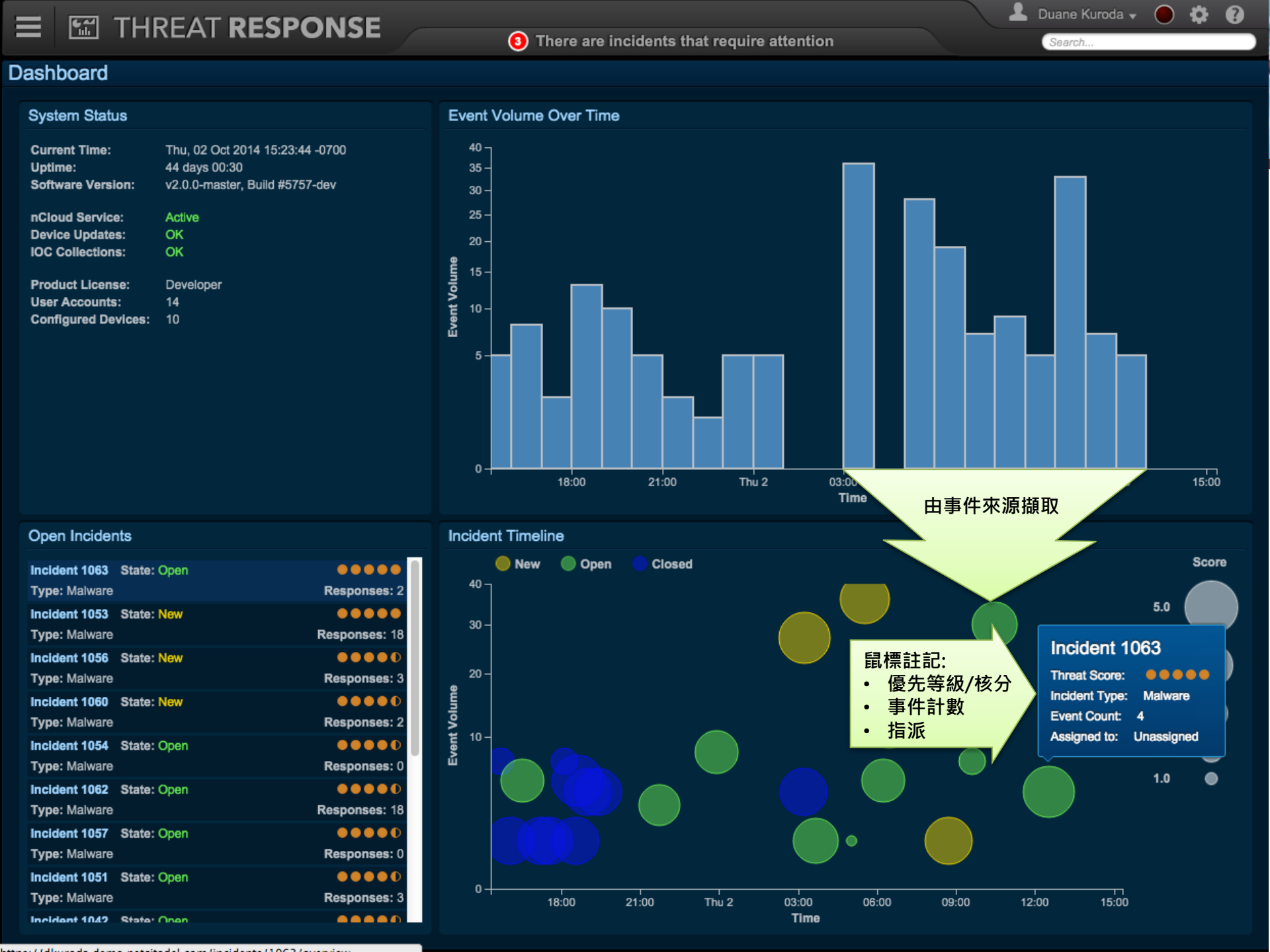
- 減少50%的調查時間
- 減少95%以上牽制及隔離的時間

資源應用更有效率

- 避免資訊超載(Alert-overload)
- 提高資安分析師應變能力
- 使初階資安人員在專業領域更有信心

提高信賴度及準確性

- 從多個不同來源的關聯性、威脅識別確認，以減少誤報避免浪費時間


THREAT RESPONSE
Duane Kuroda
3 There are incidents that require attention
Search...
Dashboard
System Status
Current Time: Thu, 02 Oct 2014 15:23:44 -0700
Uptime: 44 days 00:30
Software Version: v2.0.0-master, Build #5757-dev
nCloud Service: Active
Device Updates: OK
IOC Collections: OK
Product License: Developer
User Accounts: 14
Configured Devices: 10
Event Volume Over Time
Event Volume
Time
18:00
21:00
Thu 2
15:00
由事件來源擷取
Open Incidents
Incident 1063 State: Open
Type: Malware Responses: 2
Incident 1053 State: New
Type: Malware Responses: 18
Incident 1056 State: New
Type: Malware Responses: 3
Incident 1060 State: New
Type: Malware Responses: 2
Incident 1054 State: Open
Type: Malware Responses: 0
Incident 1062 State: Open
Type: Malware Responses: 18
Incident 1057 State: Open
Type: Malware Responses: 0
Incident 1051 State: Open
Type: Malware Responses: 3
Incident Timeline
New
Open
Closed
Score
5.0
1.0
Event Volume
Time
18:00
21:00
Thu 2
03:00
06:00
09:00
12:00
15:00
鼠標註記:
• 優先等級/核分
• 事件計數
• 指派
Incident 1063
Threat Score:
Incident Type: Malware
Event Count: 4
Assigned to: Unassigned


THREAT RESPONSE
There are incidents that require attention
Duane Kuroda
Search...
« Incidents List
Details for Incident 1063
Threat Score: 5.0/5.0
Assigned to: Unassigned
Assign...
Close Incident
Overview
Threat Info
PC Data
IP Details
Identity
History
Tanium
1 Proofpoint event
3 PANOS events
Source Information
Source: 10.10.124.164
Host: EBRACKM-WIN7-01.demo.netci...
Computer Name: EBRACKM-WIN7-01
Domain: SALESDEMO
MAC Address: 00:16:3e:38:10:34
View User Details...
檢視User
Event Information
Incident Created 10-02-2014
4
3
2
1
0
03:00
06:00
09:00
12:00
15:00
提供事件之履歷資訊
IP Details
re-calculated every 2 min
SRC
1
0% are on reputation list
0% already on a list
Add to List...
DEST
2
0% are on reputation list
0% already on a list
Add to List...
CNC
25
68% are on reputation list
Add to List...
阻斷威脅明細
OTHER
1
0% are on reputation list
0% already on a list
Add to List...
URL
0% are on reputation list
Threat Info
Category: Malware
Name: Trojan.Win32.Genome
Type: Trojan
Filename: xMiner.exe
MD5: 31063125e41c5f3df2d5c363c1...
Virus Total: Aware - 34 out of 51 AVs
View Malware Details...
Indicators of Compromise
Suspicious processes detected
Suspicious registry keys detected
2 Suspicious mutex detected
2 Suspicious file matches
Matches Found
驗證目前系統之感染狀況
Collected Thu, Oct 2 2014 12:32
Recent Incident History
System Administrator created a response
2 hours ago
Added 3 URL(s) to list Dangerous URLs
"Adding URLs to block list to help protect other users from getting infected."
Show details...
System Administrator created a response
2 hours ago
Added 1 User(s) to list Suspicious Users
"Adding Earline to the Suspicious User list for 24 hours while investigation continues."
Show details...
System Administrator added a comment
2 hours ago
"Initial investigation underway"
Show details...
System
3 hours ago
Incident was created
Add Response...

結語

- 當所有的企業的MIS & IT 還在辛苦的備份資安設備與分析
- Proofpoint 已將資安鑑識專家的智慧放入我們的最新產品---威脅應變管理平台
- 完整的APT防禦，需要多種技術相互組合，PTR 擁有獨特的事件分析與應變機制，正符合台灣資安界所需
- 請您給阿碼證點

  為台灣資安界貢獻一個機會

proofpoint

Q&A

threat protection | compliance | archiving & governance | secure communication