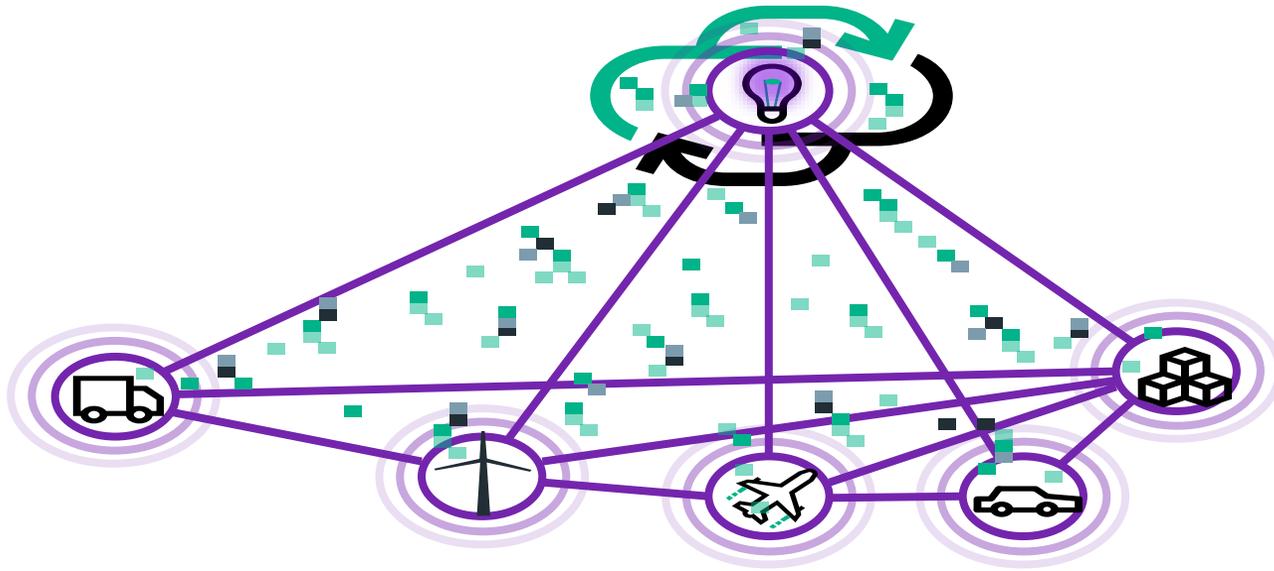


IoT補夢網

HPE 李柏厚 Bill Lee



什麼叫IoT就是Internet of Things(物聯網)



可以連上internet的設備及系統

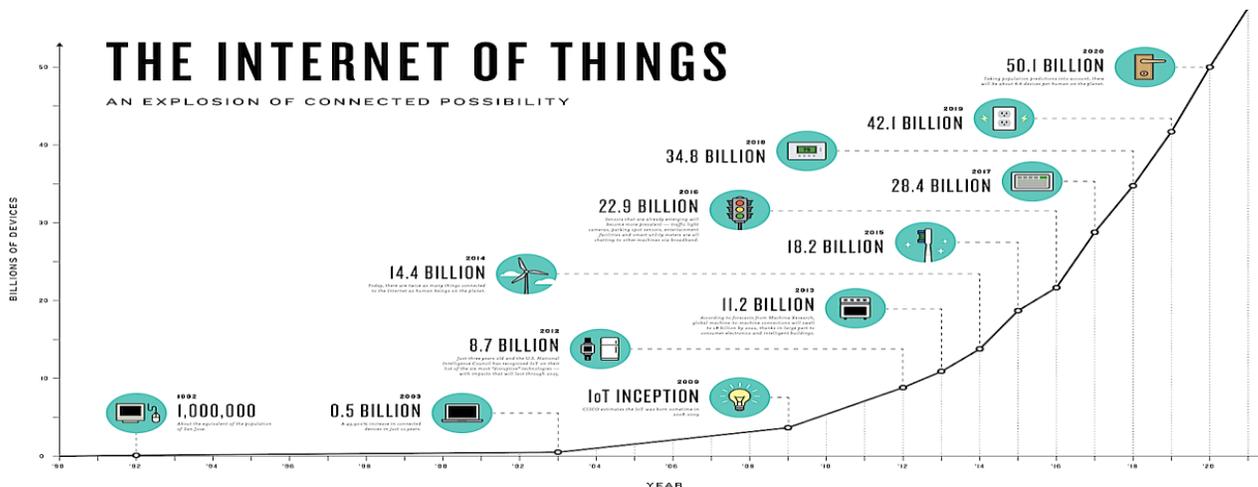
Gartner預估在2020年有260億個設備連上物聯網

在物聯網上的資料流量

IDC預估在2020年整個IoT上的資料佔所有資料流量的10%

在物聯網的新的資料

商業、工程及科學等資訊



IoT架構特性

- IoT的硬體及軟體不一定有標準
- 端點設備可能cpu及可寫入的空間大小不一
- IoT設備可能有儲存客戶機敏資料
- 整個網路可能跨過幾個地理區域，甚至是國家
- 功能面的要求可能造成安全的忽略，例如認證

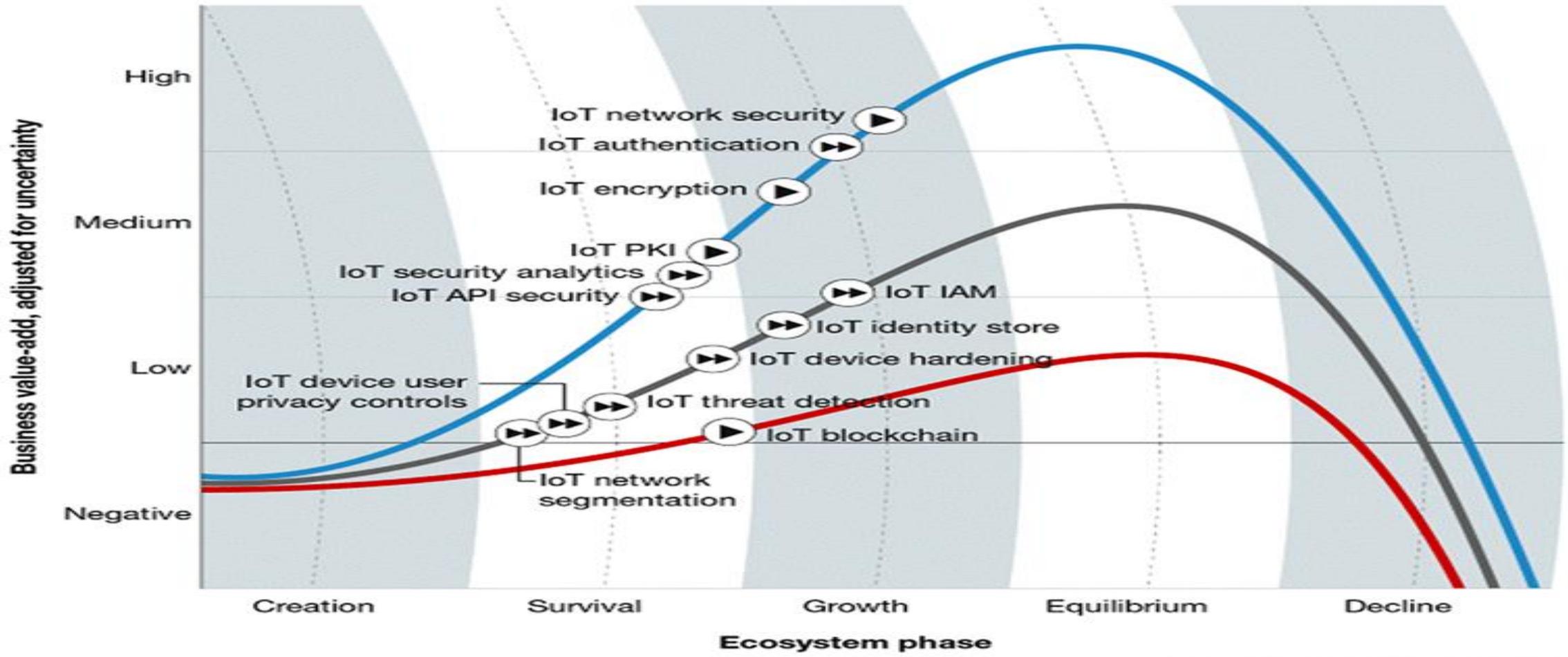
TechRadar™: Internet Of Things Security, Q1 '17

Trajectory:

- Significant success
- Moderate success
- Minimal success

Time to reach next phase:

- ▶▶ <1 year
- ▶ 1 to 3 years
- ▶ 3 to 5 years
- || 5 to 10 years
- >10 years



Source: Forrester Research, Inc.

在物聯網架構及考量資安的點?

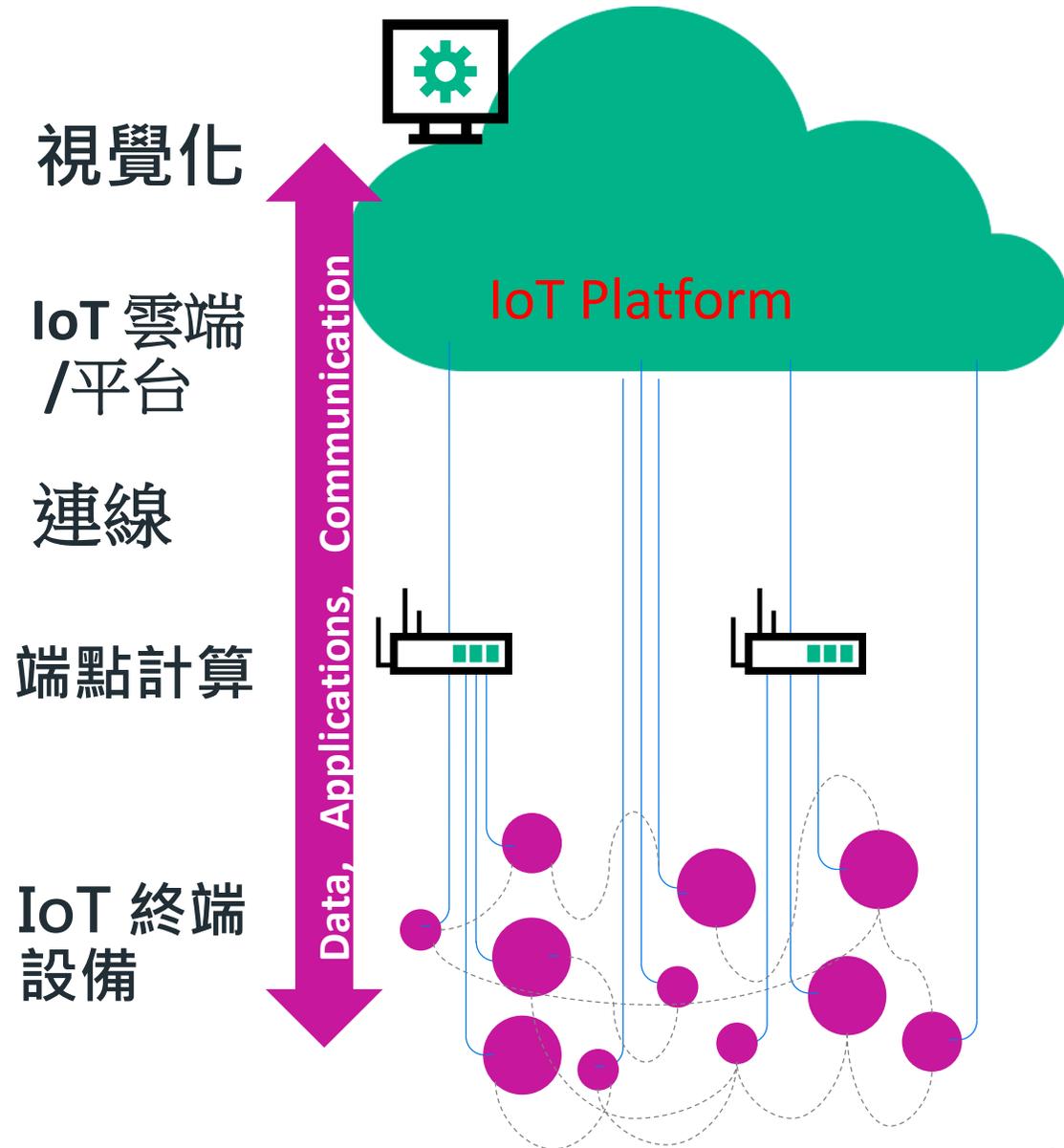
應用層-用於用視覺化的方式來讓管理者或來管理整個物聯網的運作

運作及控制IoT的架構-包含資料的儲存及大數據及機器學習做一個轉換。

連線層-用普遍，可靠及安全的連線方式來連接至端點或收集器的設備

收集器-主要是收集終端設備的資訊，例如是將運作的通訊協定(SCADA)轉成資訊的通訊協定(TCP/IP)，做資訊的擷取及轉換。

分散感應器及執行器-可能是行動或固定裝置，但常常連結於internet或private的網路，又稱M2M



在物聯網架構及考量資安的點?

破解端點及收集器

利用端點或收集器的弱點來安裝非經授權的人員，這會造成資料的外洩或是系統的運作問題。

入侵端點及收集器

利用設備上的軟體的弱點來入侵設備，尤其是那些較簡單或是沒有辦法即時修補的設備。

資料外洩

有些端點或收集器裏會有敏感性資料，例如帳號資訊。所以外洩這些資料會導致系統被入侵或個資外洩。

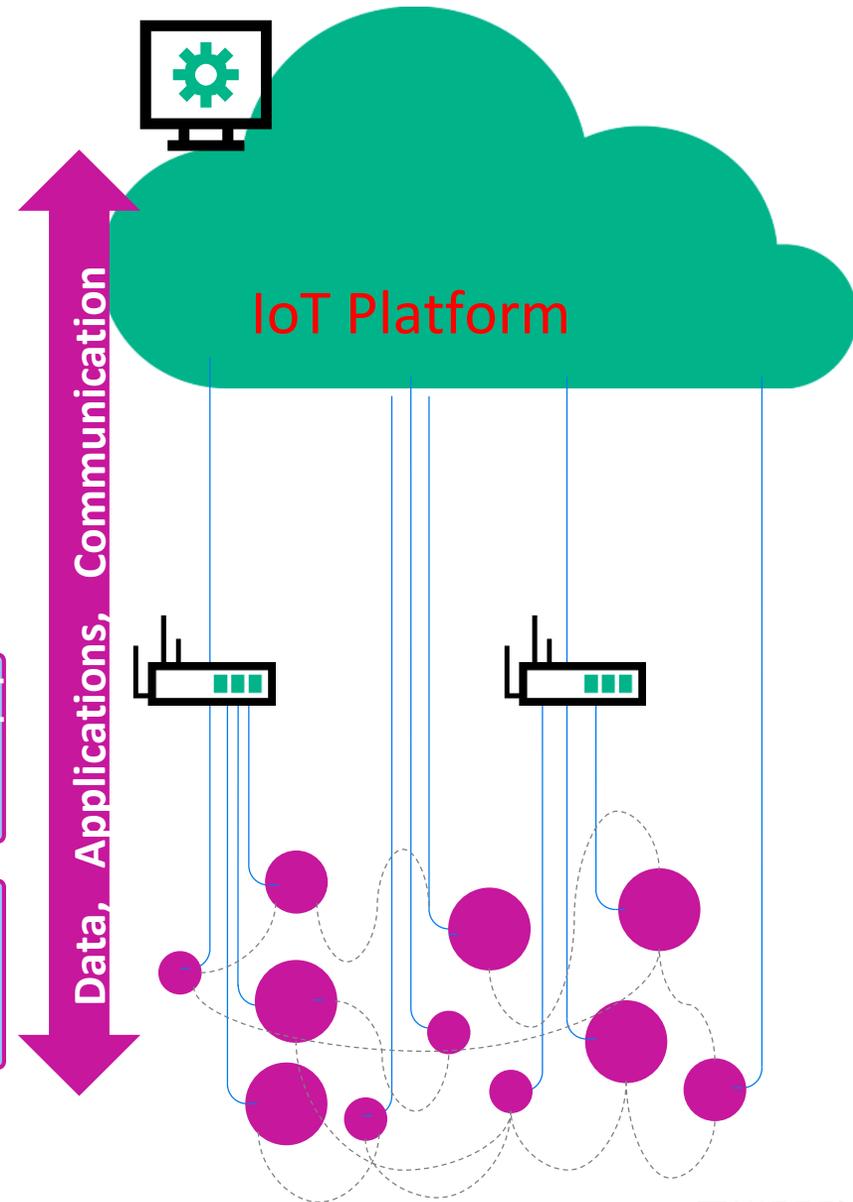
視覺化

IoT 雲端
/平台

連線

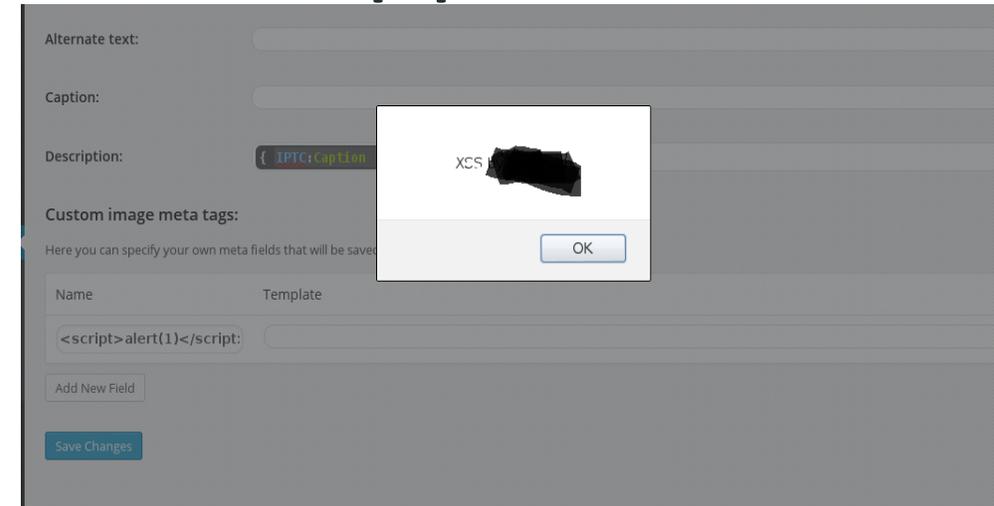
端點計算

IoT 終端
設備

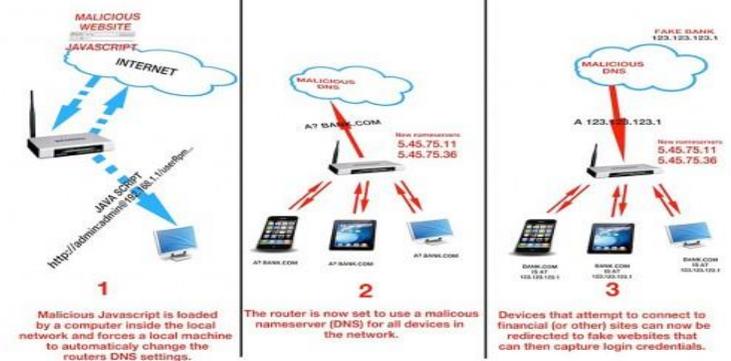


IoT入侵方式-利用Web界面做為進入點

- XSS-<https://www.youtube.com/watch?v=iMSUb9wq-qo>
- SQL injection
- CSRF
- Open source 已知風險



CSRF SOHO ROUTER ATTACK



在物聯網架構及考量資安的點?

中間人攻擊(MitM)

攻擊者偵測出端點或收集器到平台之間的內容，讓整個IoT的系統造成問題。

阻斷式攻擊(DoS)

讓IoT的雲端服務如Web API或VPN不能提供服務。

未經授權存取

利用模擬授權的端點來對系統獲取資訊或取得管理權限。

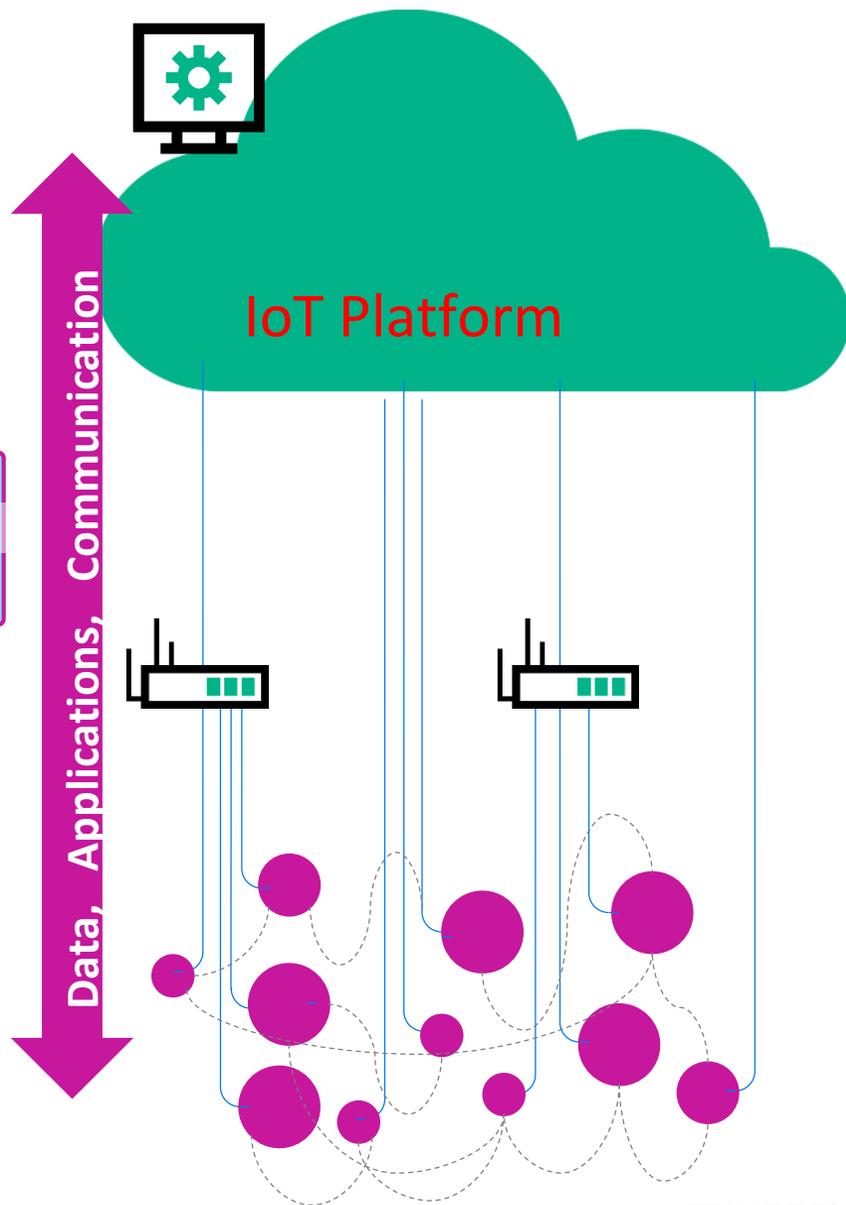
視覺化

IoT 雲端
/平台

連線

端點計算

IoT 終端
設備



網路服務商Dyn DDoS的攻擊事件

■ 時間-2016/10/21

■ 事件過程

- 透過惡意軟體「Mirai」，利用 IPCAM、CCTV、DVR、IoT 裝置等系統對Dyn這家網路服務公司進行 DDoS 攻擊。
- 事件是從10/21的早上7:00開始持續了兩個小時。造成上百萬的用戶無法上網。

■ 問題主因

- 主要是他們使用的DVR已經被植入了Mirai而造成問題



思科Elastic Services Controller問題

- 事件時間-2018/2/27
- 問題原因
 - 使用開放源碼
 - 主要是可以繞過web的認證，使用空白字元來登入

The screenshot shows a Cisco Security Advisory page for a critical vulnerability in Elastic Services Controller. The title is "思科Elastic Services Controller爆重大漏洞，免密碼就能取得管理員權限". The advisory ID is cisco-sa-20180221-esc, and the CVE is CVE-2018-0121. The severity is marked as "Critical" with a red circle. The page also includes a summary, a table of advisory details, and a sidebar with a "Cisco Security Vulnerability Policy" section. On the right, there is a banner for "Taiwan Cloud Edge Summit 2018" and an "iThome Security" logo.

新聞

思科Elastic Services Controller爆重大漏洞，免密碼就能取得管理員權限

當Elastic Services Controller服務入口頁彈出要求輸入管理員密碼時，駭客只要密碼欄留空送出，不須任何破解動作，便能輕鬆取得管理員權限，操作所有管理員能夠執行的命令。

文/ 李建興 | 2018-02-27 發表 讚 4.7 萬 按讚加入iThome粉絲團 讚 75 分享 G+

Home / Cisco Security / Security Advisories and Alerts

Cisco Security Advisory

Cisco Elastic Services Controller Service Portal Authentication Bypass Vulnerability

Advisory ID:	cisco-sa-20180221-esc	CVE-2018-0121	Download CVRF
First Published:	2018 February 21 16:00 GMT	CWE-287	Download PDF
Version 1.0:	Final		Email
Workarounds:	No workarounds available		
Cisco Bug IDs:	CSCvg29809		
CVSS Score:	Base 9.8		

Critical

Summary

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the [Security Vulnerability Policy](#). This document also contains instructions for

Taiwan Cloud Edge Summit 2018
2018年5月16日(三)
TICC 台北國際會議中心
[立即報名](#)

iThome Security
說這專頁讚 6202 按讚次數

在物聯網架構及考量資安的點?

有問題的網站應用程式及API

這會造成DoS或是資料流失或是被攻擊者控管整個系統。這也是OWASP 10列出需要被保護的風險。

有目地的攻擊

攻擊者會選擇有漏洞的設備的IoT的廠商進行攻擊。就如APT的攻擊一般選擇有目的廠商做攻擊。

視覺化

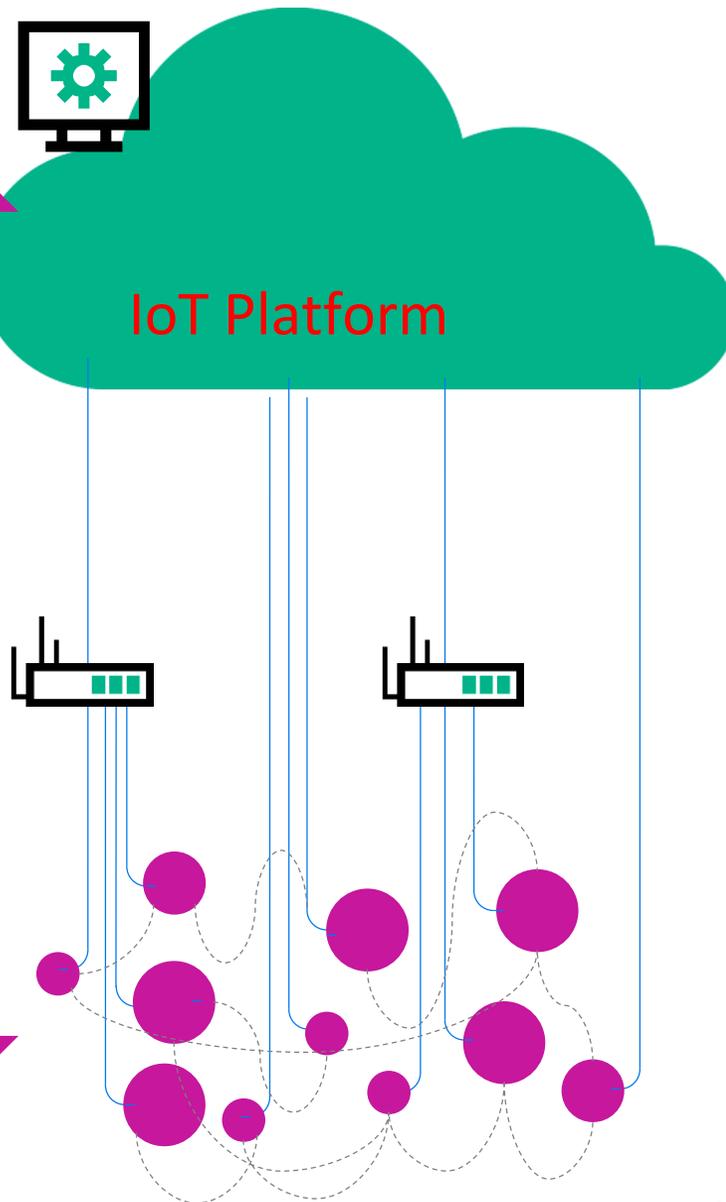
IoT 雲端
/平台

連線

端點計算

IoT 終端
設備

Data, Applications, Communication



SCADA烏克蘭電網攻擊事件

■ 時間-2015年12月

■ 事件過程

- 駭客攻擊了60座變電站，造成大規模的停電，這事件有人認為是俄羅斯主導

■ 事件原因

- 電力員工下載了惡意軟體“BlackEnergy”，然後駭客就利用軟體來切斷主控電腦及變電站連線。
- 在電腦裏植入病毒，在同時駭客對電力公司的通話進行干擾，導致停電的居民無法和電力公司進行聯絡。

IoT問題發生主因

■ IoT設備安全性問題

- 確認連線的IoT設備是合法授權及經過嚴格認證。
- 確保IoT設備本身沒有漏洞及安全。
- 確保IoT的存取的控管及認證。
- 確保IoT設備在各個連線上是否安全及加密。

■ IoT平台安全性問題

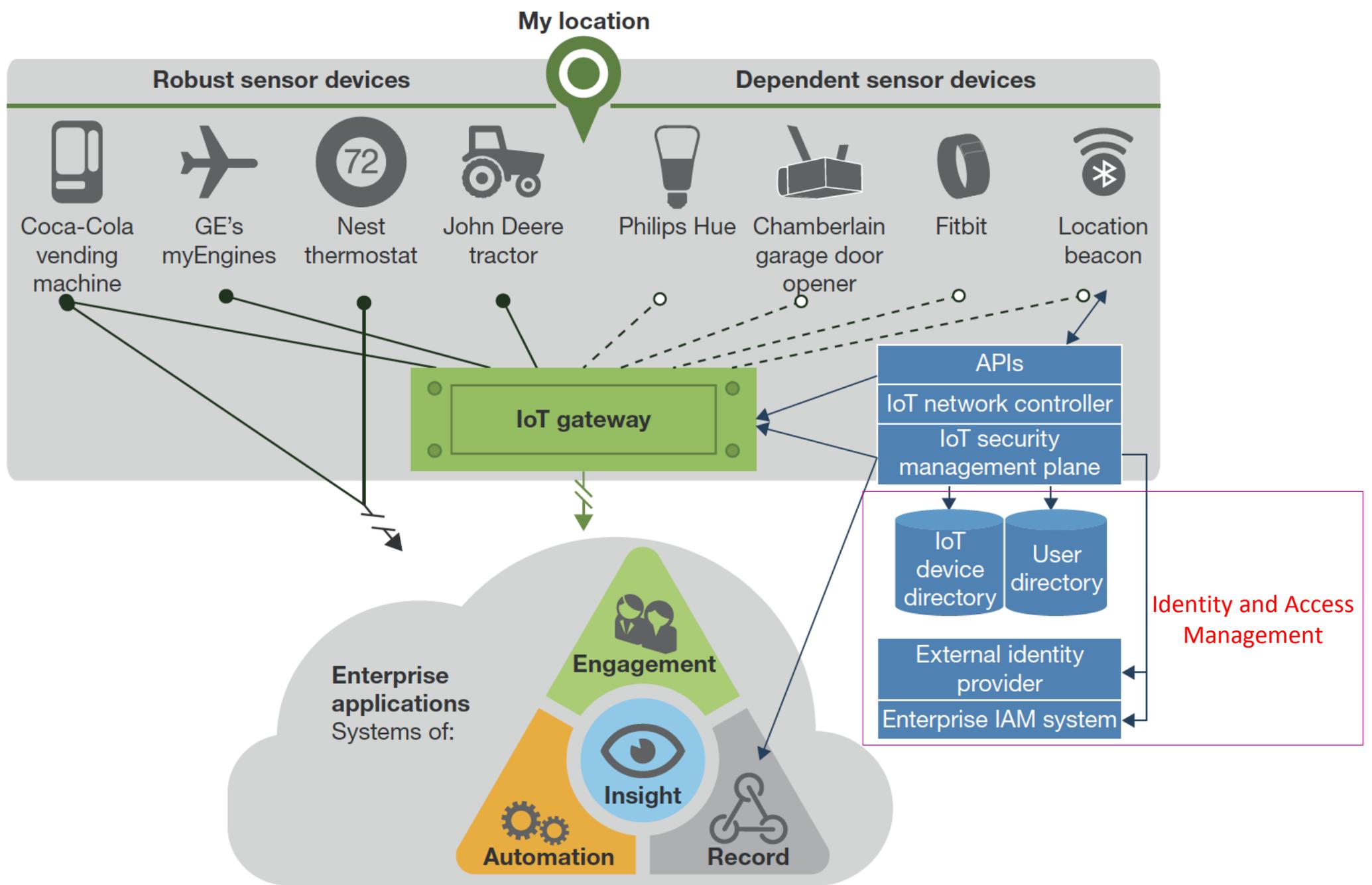
- 確保存取的控管及認證。
- 確保儲存的資料安全，例如資料加密。

確保IoT安全可用到的技術

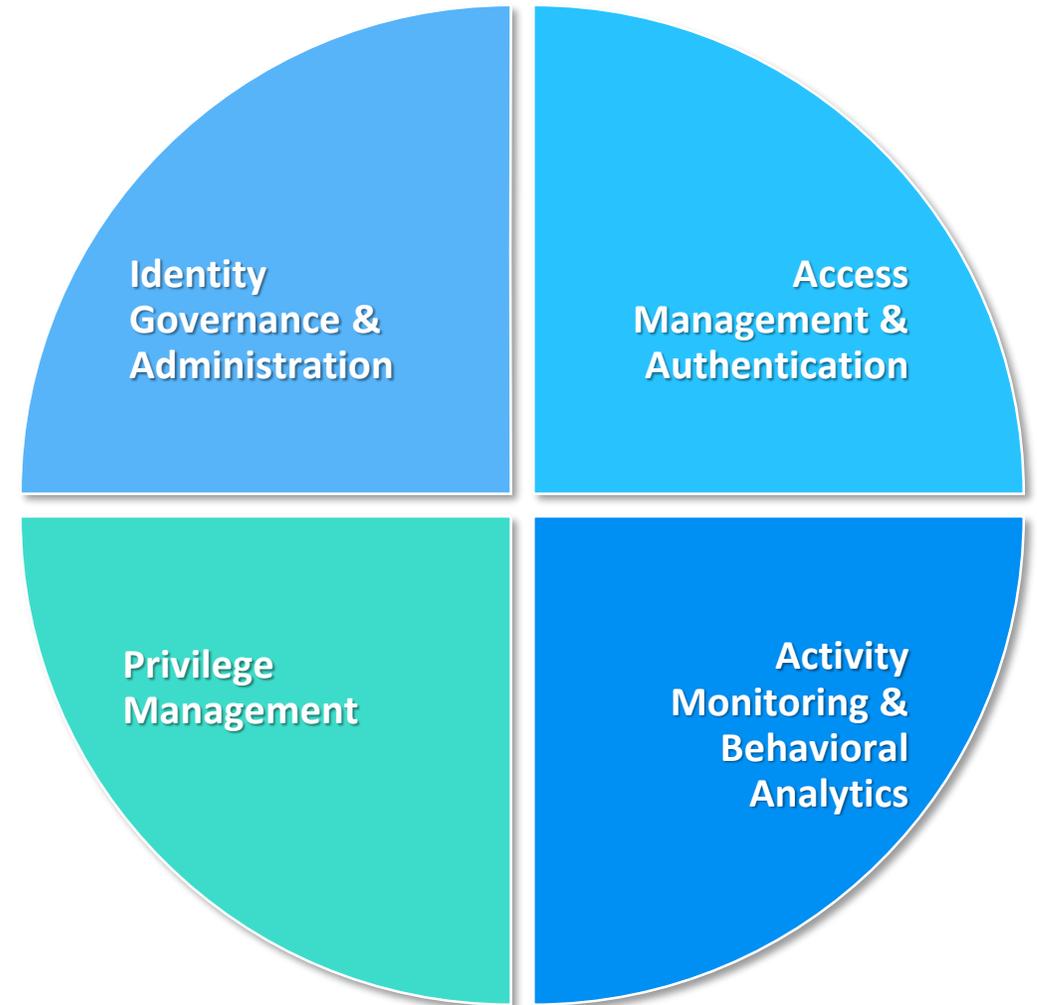
- 身份認證
- 預防應用程式的問題
 - 源碼掃描(白箱測試)
 - 網站滲透(黑箱測試)
- 資安事件稽核
 - 非法攻擊
 - 合法人員的非法行為
- 加密
 - 儲存資料加密
 - 連線加密
 - 應用程式加密

IoT身份驗證的重點

- 連線設備的確認
- 提供對的人對的存取在對的時間
- 認證的三因因素
 - 使用者有什麼(Something you have)
 - 使用者知道什麼(Something you know)
 - 使用者之生物辨識(Something you are)
- 認證的技術
 - 挑戰及回應
 - 一次性密碼
 - 憑證
 - 帳號及密碼
- 認證架構
 - 先集中再依狀況來做適當認證設計



Simplicity Through Intelligence



預防應用程式的問題-(白箱)-OpenWRT

Summary | Audit Guide | Scan | Reports

Filter Set: Security Auditor View My Issues

1871 6540 0 7954 ... 16365

Critical (1871)

Group By: Category

- > Buffer Overflow - [0 / 1299]
- > Buffer Overflow: Format String - [0 / 70]
- > Buffer Overflow: Off-by-One - [0 / 4]
- > Command Injection - [0 / 34]
- > Key Management: Hardcoded Encryption Key - [0 / 34]
- > Path Manipulation - [0 / 452]

Advanced...

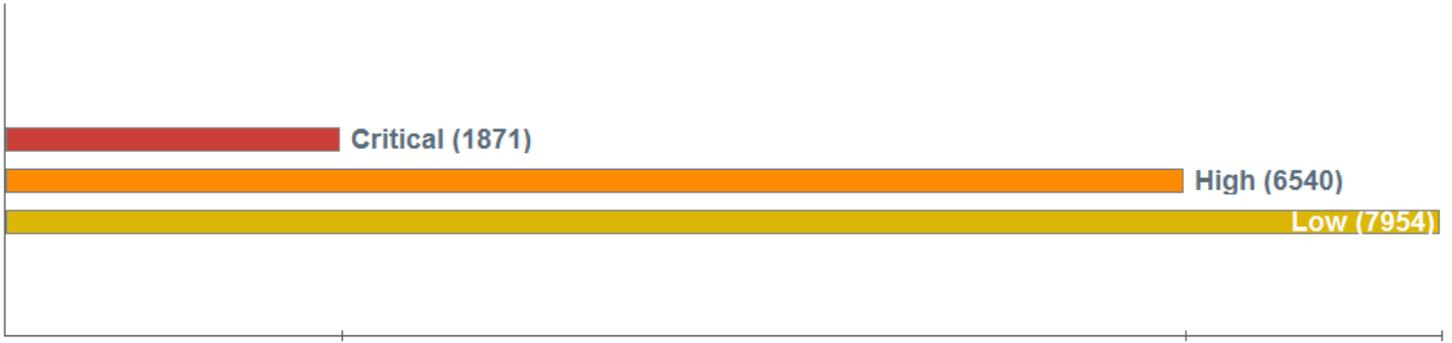
Project Summary

Summary | Certification | Runtime Analysis | Build Information | Analysis Information

Build ID: openwrt1
Scan Date: 2017/6/19
Warnings: None

Scanned: 2,050 files, 107,632 LOC (Executable)
Total Issues: 16,365
Certification: Results Certification Valid

All Issues by Folder



Severity	Count
Critical	1871
High	6540
Low	7954

預防應用程式的問題-(黑箱)-wireless router

Site

- http://192.168.1.1/
 - /
 - calendar
 - require
 - switcherplugin
 - <script>alert('TRACE');</script>
 - <script>alert('TRACK');</script>
 - AdaptiveQoS_Bandwidth_Monitor
 - Advanced_DSL_Content.asp
 - Advanced_IPv6_Content.asp
 - Advanced_Modem_Content.asp
 - Advanced_OperationMode_Conte
 - Advanced_VPN_PPTP.asp
 - Advanced_WAN_Content.asp
 - Advanced_WAN_Content.asp
 - AIProtection_HomeSecurity.asp
 - ajax_status.xml
 - ajax_status.xml
 - ajax_status.xml
 - ajax_status.xml

Scan Info

- Dashboard
- Traffic Monitor
- Attachments
- False Positives

Session Info

Host Info

- P3P Info
- AJAX
- Certificates
- Comments
- Cookies
- E-mails
- Forms
- Hiddens
- Scripts
- Broken Links
- Offsite Links
- Parameters

Scan Dashboard

- Crawled: 190 of 190
- Audited: 139 of 139
- Smart Audited: 139 of 139
- Verified: 99 of 99
- Reflection Audited: 0 of 0

Network

Network	0.00B

Analysis

Analysis	0

Vulnerabilities

Vulnerability Type	Count
Critical	27
High	7
Medium	1
Low	7
Info	0
Best Practices	36

Attack Type

Attack Type	Attacks	!	●	●	●	●
Manipulation	4,761	27	1	0	0	0
Exploratory	4,438	0	3	0	3	0
Other	1,158	0	3	1	4	0

Scan

- Type: Site
- Status: Completed
- Agent: Not Detected
- Client: FF
- Duration: 2:22:04:23
- Policy: OWASP Top 10...
- Deleted Items: 0

Crawl

- Hosts: 1
- Sessions: 9

Audit

- Attacks Sent: 10,357
- Issues: 78

Network

- Total Requests: 14,000
- Failed Requests: 30
- Script Includes: 11
- Macro Requests: 96
- 404 Probes: 1,087
- 404 Check Redirects: 392
- Verify Requests: 0
- Logouts: 1,247
- Macro Playbacks: 1,257

開放源碼檢查(已知問題)

SampleApp - 2016-10-05 - Build Report

Summary Policy Violations Security Issues License Analysis

FILTER: All Exact Similar Unknown Proprietary VIOLATIONS: Summary All Waived

Policy Threat	Component	Filename	Popu...	Age	Release History
Security-High	commons-httpclient : commons-httpclient : 3.1	commons-httpclie...		9.1 y	
	org.apache.geronimo.framework : geronimo-sec...	geronimo-security...		8.6 y	

Component Info Policy Similar Occurrences Licenses Vulnerabilities Labels Audit Log

Group: org.apache.geronimo.framework
Artifact: geronimo-security
Version: 2.1
Declared License: Apache-2.0
Observed License: No Sources
Effective License: Apache-2.0
Highest Policy Threat: 9 within 3 policies
Highest Security Threat: 9.4 within 3 security issues
Cataloged: 8 years ago
Match State: exact
Identification Source: Sonatype

Popularity License Risk Security Alerts

Older This Version Newer

2.1.8

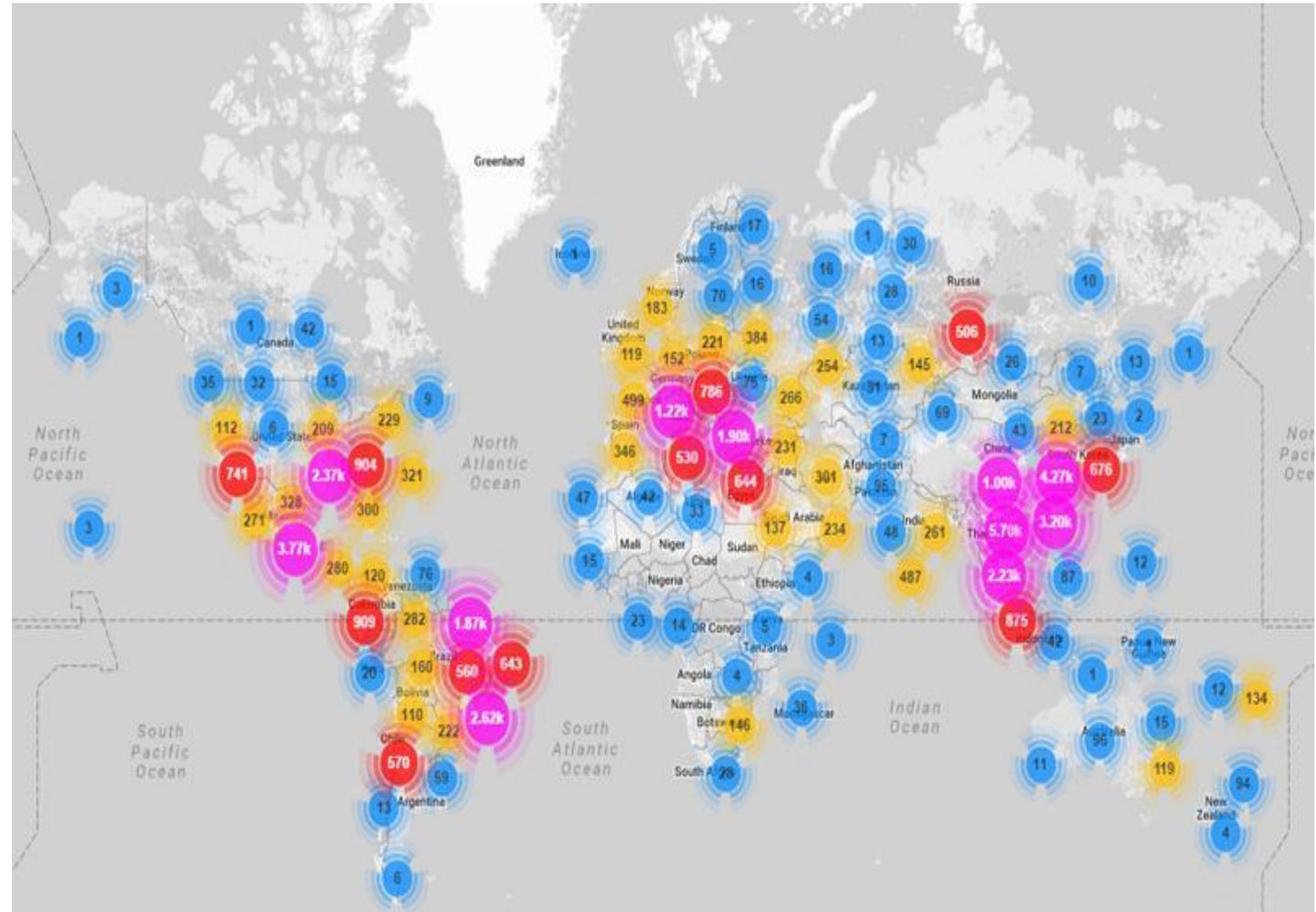
新本上沒有
風險

IoT事件稽核– Mirai Botnet

```
log /home/vac/logs/vac.log-last | egrep "pps\|.....
bps" | awk '{print $1,$2,$3,$6}' | sed "s/ /|/g" | cut -f
1,2,3,7,8,10,11 -d '|' | sed "s/.....bps/Gbps/" | sed
"s/.....pps/Mpps/" | cut -f 2,3,4,5,6,7 -d ":" | sort | g
rep "gone" | sed "s/gone|/"
```

Sep 18	10:49:12	tcp_ack	20Mpps	232Gbps
Sep 18	10:58:32	tcp_ack	15Mpps	173Gbps
Sep 18	11:17:02	tcp_ack	19Mpps	224Gbps
Sep 18	11:44:17	tcp_ack	19Mpps	227Gbps
Sep 18	19:05:47	tcp_ack	66Mpps	735Gbps
Sep 18	20:49:27	tcp_ack	81Mpps	360Gbps
Sep 18	22:43:32	tcp_ack	11Mpps	136Gbps
Sep 18	22:44:17	tcp_ack	38Mpps	442Gbps
Sep 19	10:13:57	tcp_ack	10Mpps	117Gbps
Sep 19	11:53:57	tcp_ack	13Mpps	159Gbps
Sep 19	11:54:42	tcp_ack	52Mpps	607Gbps
Sep 19	22:51:57	tcp_ack	10Mpps	115Gbps
Sep 20	01:40:02	tcp_ack	22Mpps	191Gbps
Sep 20	01:40:47	tcp_ack	93Mpps	799Gbps
Sep 20	01:50:07	tcp_ack	14Mpps	124Gbps
Sep 20	01:50:32	tcp_ack	72Mpps	615Gbps
Sep 20	03:12:12	tcp_ack	49Mpps	419Gbps
Sep 20	11:57:07	tcp_ack	15Mpps	178Gbps
Sep 20	11:58:02	tcp_ack	60Mpps	698Gbps
Sep 20	12:31:12	tcp_ack	17Mpps	201Gbps
Sep 20	12:32:22	tcp_ack	50Mpps	587Gbps
Sep 20	12:47:02	tcp_ack	18Mpps	210Gbps
Sep 20	12:48:17	tcp_ack	49Mpps	572Gbps
Sep 21	05:09:42	tcp_ack	32Mpps	144Gbps
Sep 21	20:21:37	tcp_ack	22Mpps	122Gbps
Sep 22	00:50:57	tcp_ack	16Mpps	191Gbps

You have new mail in /var/mail/root



2016-09-21 DDoS vis Flooding, DNS AMP and GRE
Flooding Attack

49,657 unique IPs which hosted Mirai-infected devices

SCADA網路監控

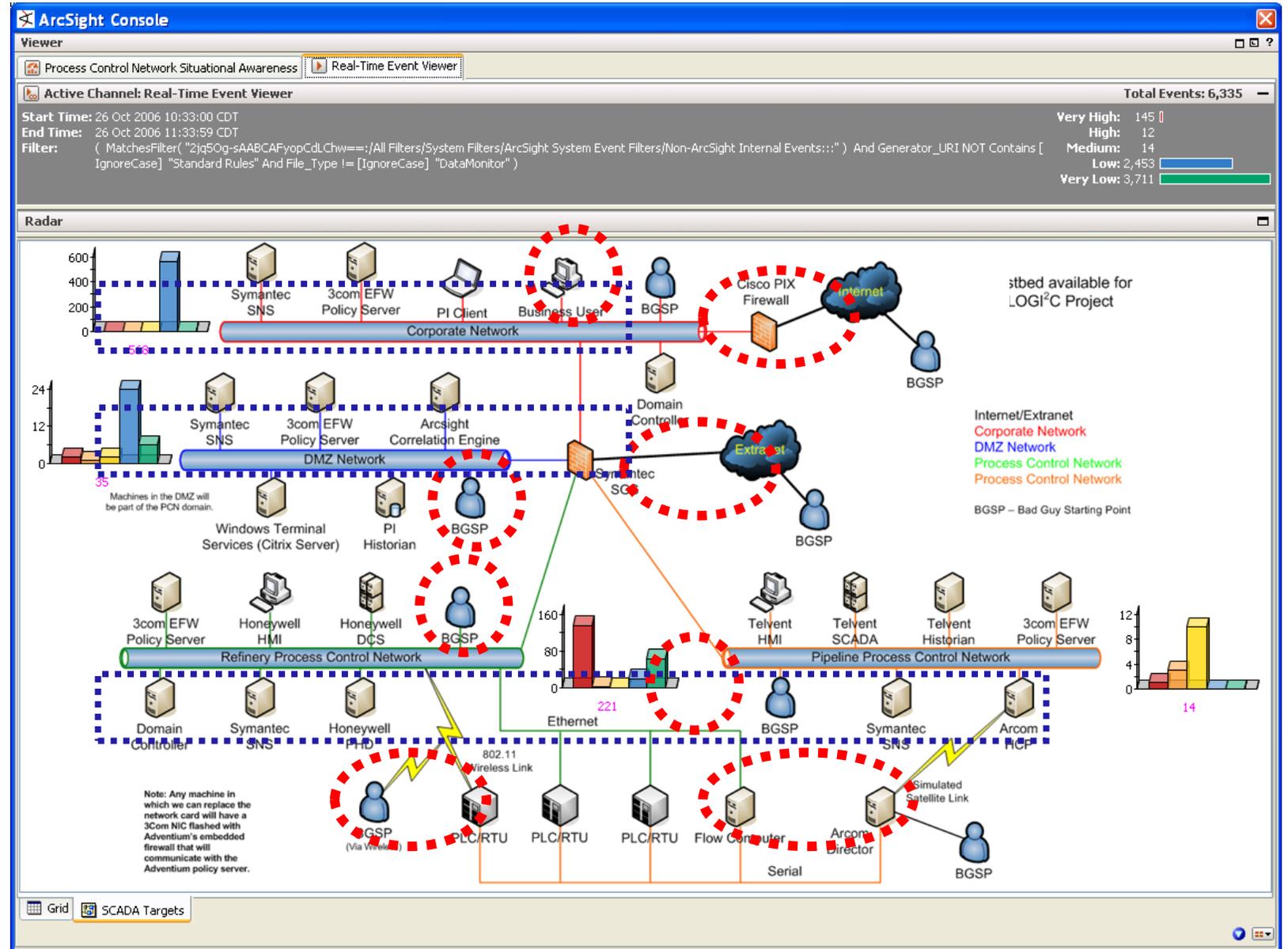
企業及控制系統監控

► 攻擊因素

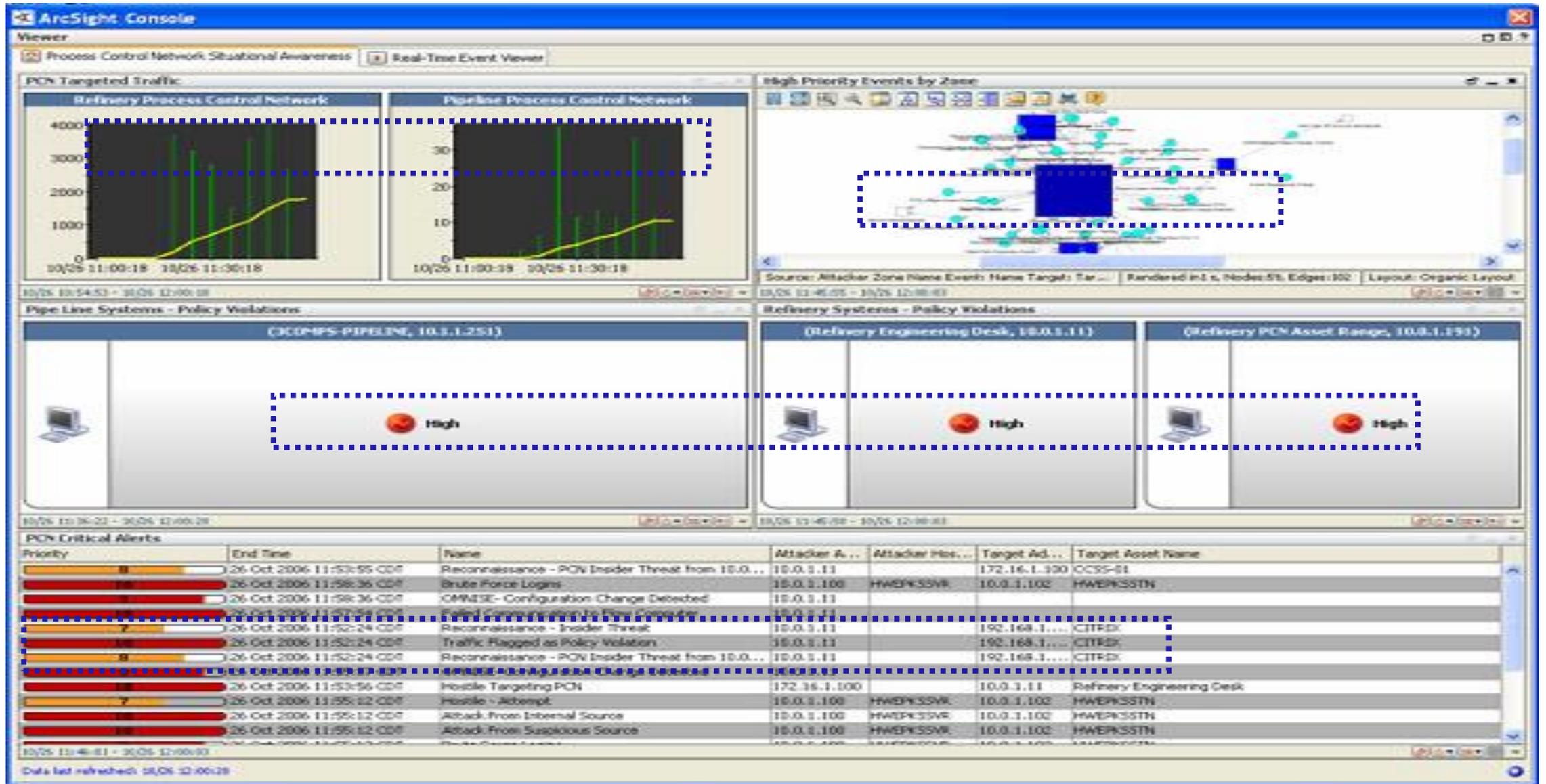
- 內部網路
- 外部網路
- 無線網路
- 衛星網路

► 企業網路狀況

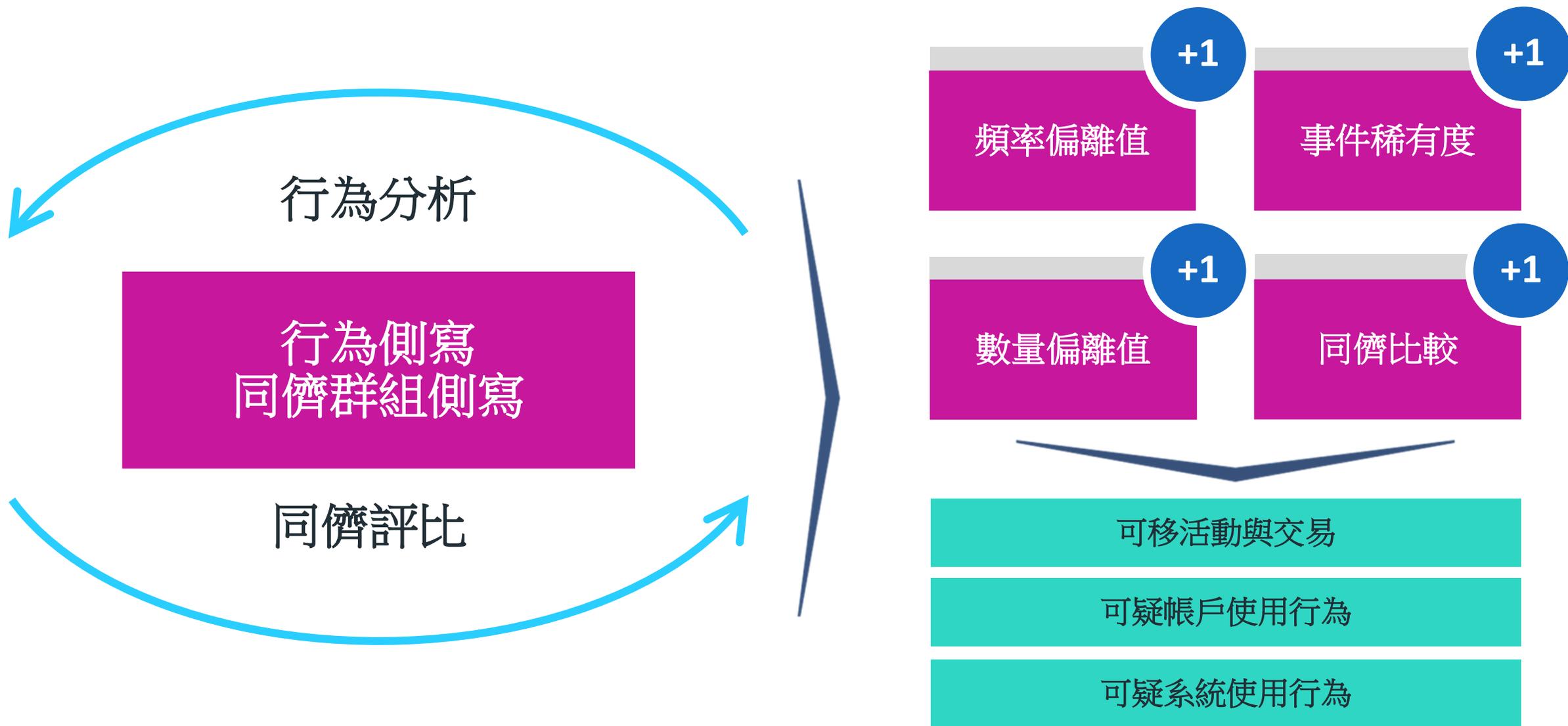
► DMZ狀況



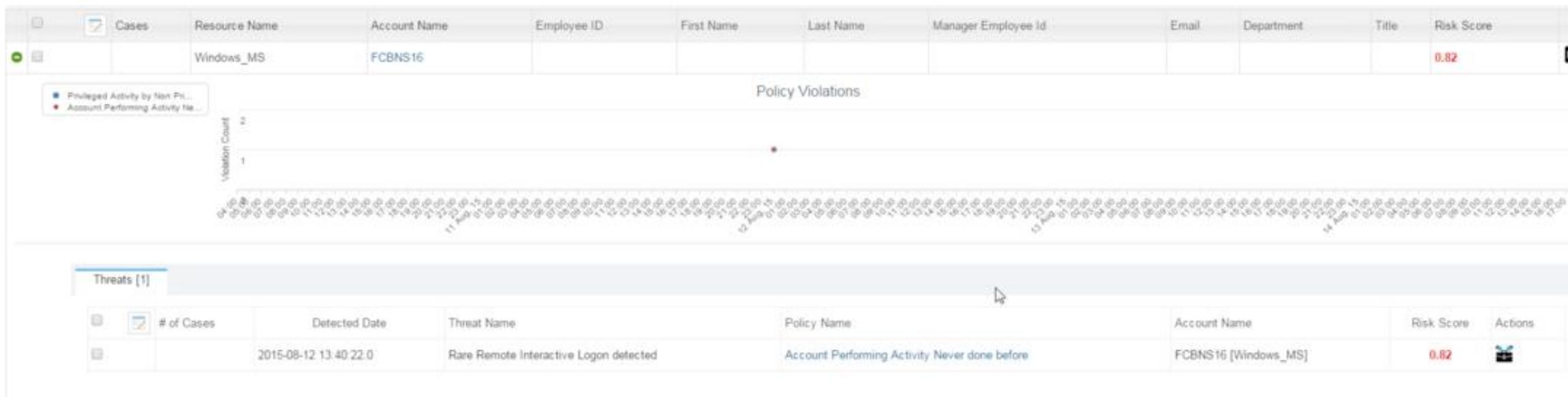
SCADA網路監控-案例



合法人員的非法行為-使用者行為分析技術



合法人員非法行為案例 – 用戶進行從未見過的遠端登入行為

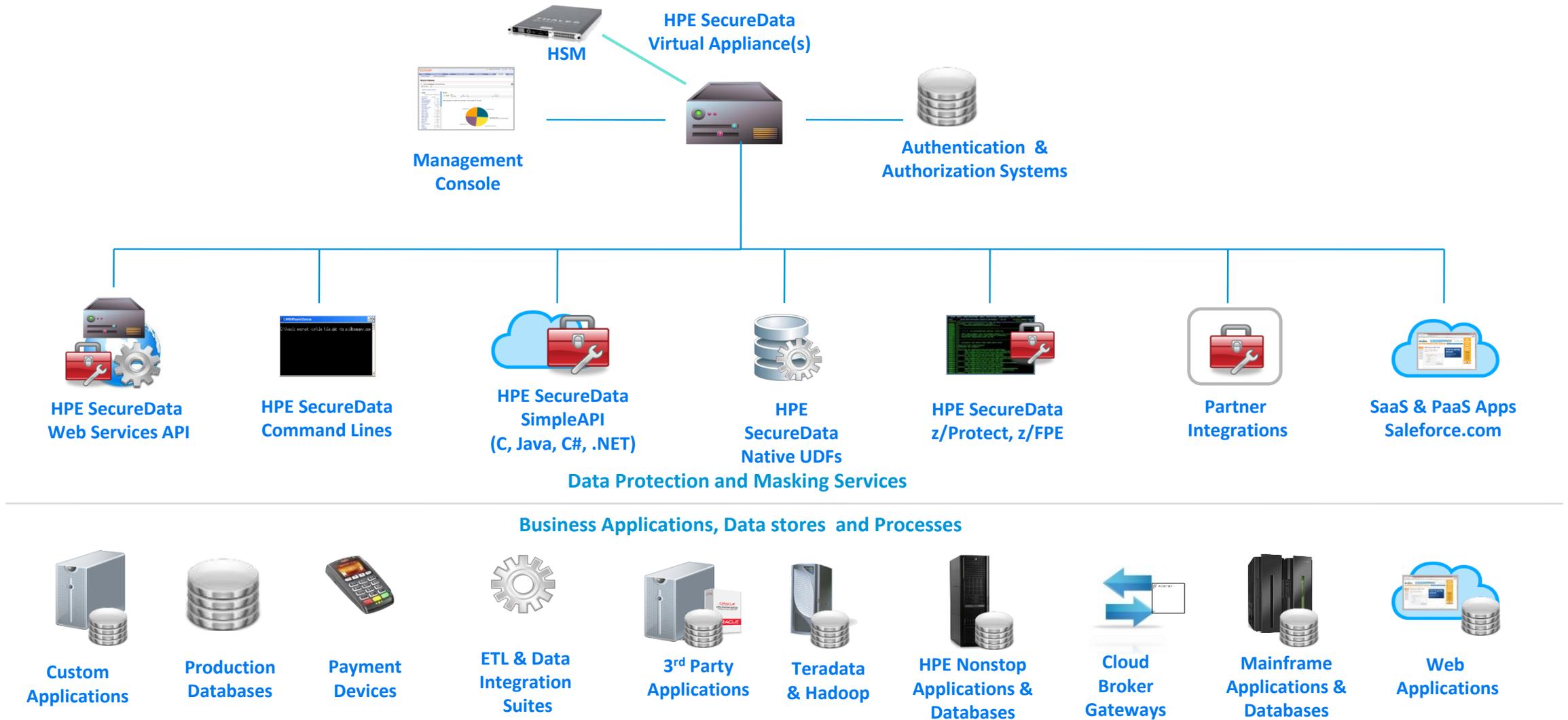


Case ID	Threat Indicator	Transaction	Event Date/Time	Datasource	Resource Name	Account	Employee Id	First Name	Last Name	Raw Score	Network Address
	Rare Remote Interactive Logon detected	Message: An account was successfully logged on	Fri Jul 31 18:15:34 EDT 2015	Windows_MS	Windows_MS	FCBNS16				0.82	10.52.140.33

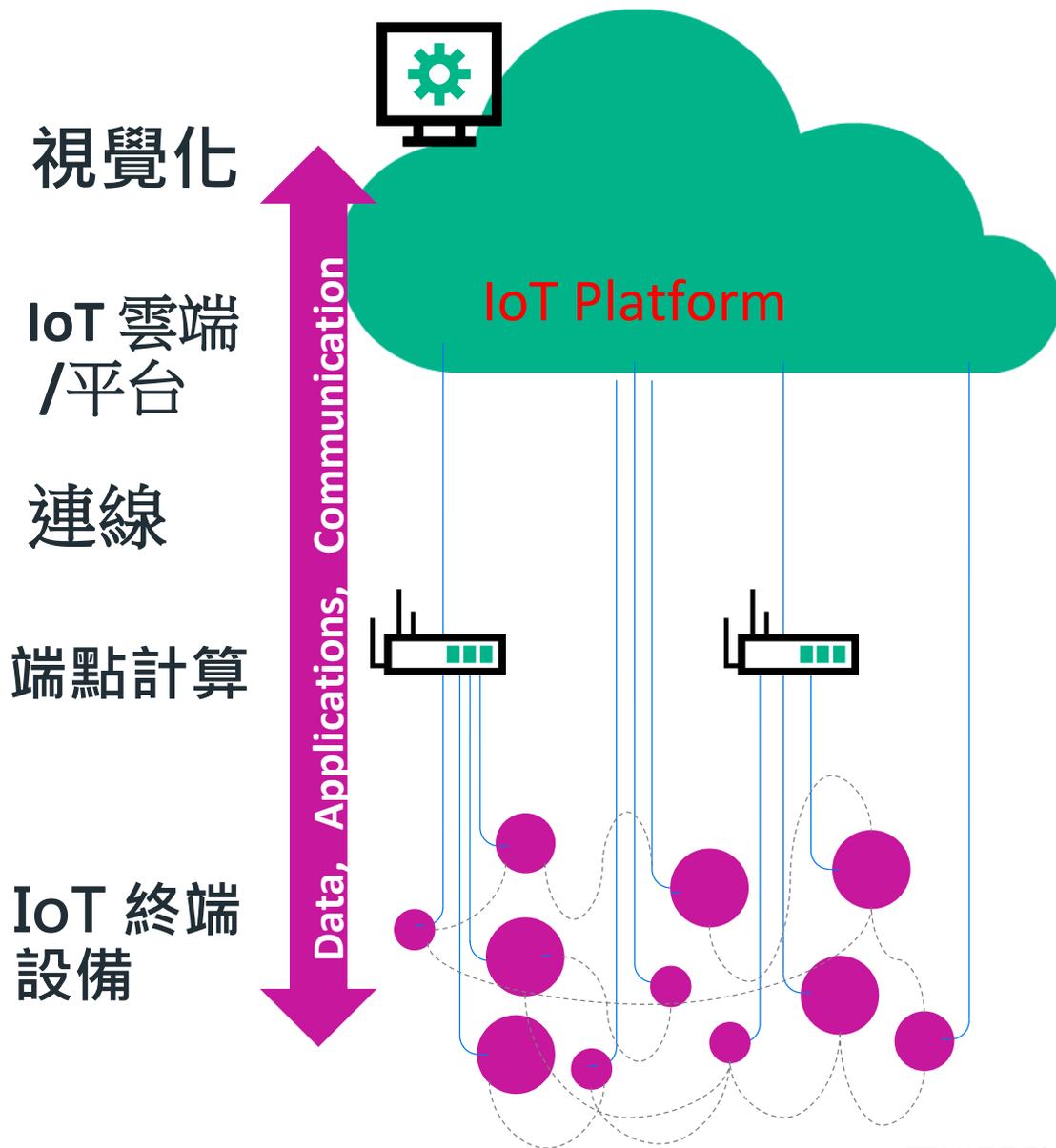
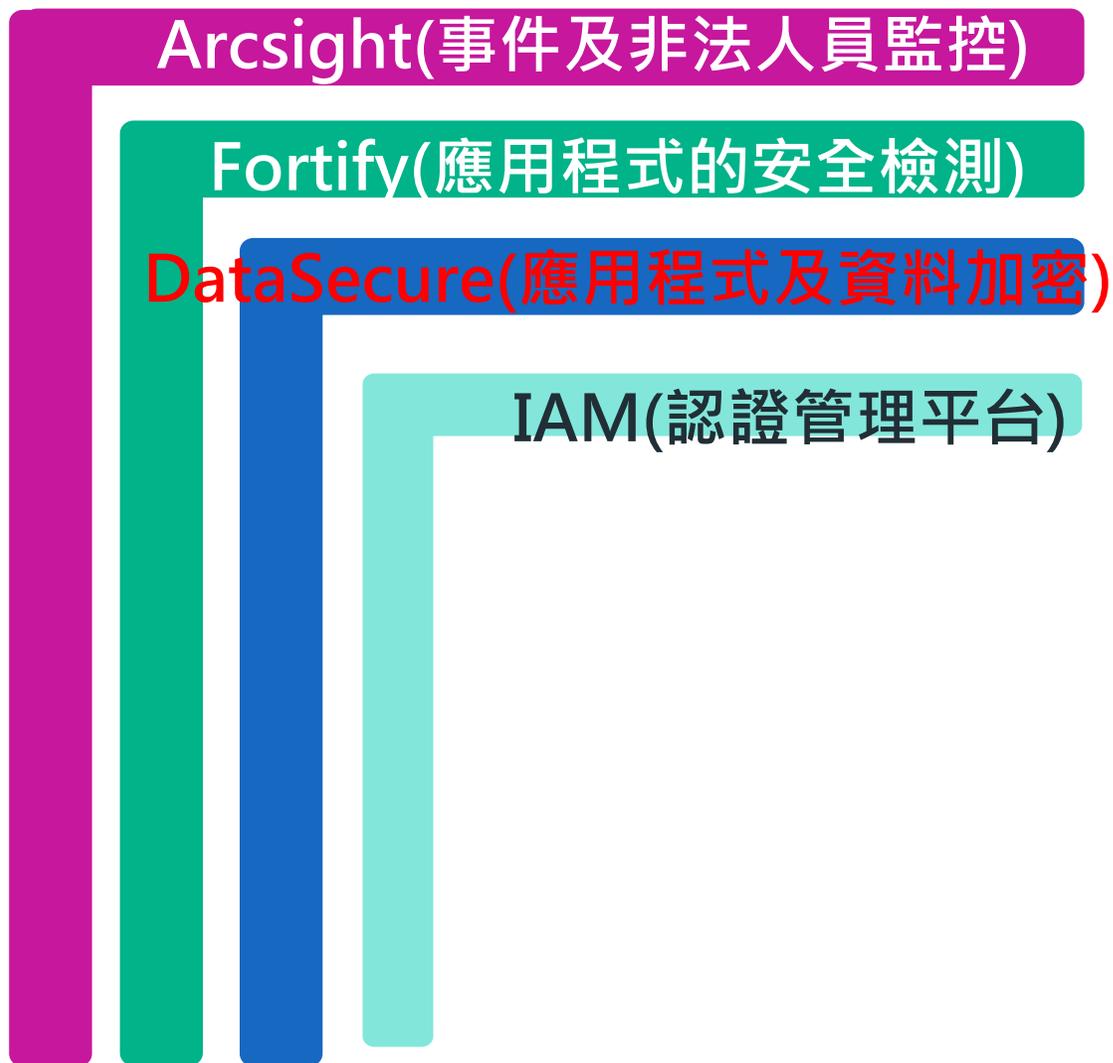
Check Name	Frequency	Baseline	Raw Score	Generated Date	View Violations	Number of Days in the resource
Account performing activity never conducted before	1	0	0.82	2015-08-12 13:40:22.0	View Violations	10

ComputerName	EventCode	Message	TargetAccount	TargetAccountDomain	LoginType	SourcePort	Account Name	Network Address	Last Performed Date/Time	Geolocation		Frequency
										Computed	Commercial	
TORKBNS4.bns.bns	4624	An account was successfully logged on			10	1561	FCBNS16	10.52.140.33	Fri Jul 31 18:15:34 EDT 2015			1

應用程式的加密



Microfocus產品對應



Microfocus 資安產品介紹

產品方案	應用程式	資料	連線
ArcSight	事件交叉及資安事件通知(ArcSight Data Platform, ESM – Security Information and Event Management, AppView) 資安分析 (ArcSight Interactive Discovery, DNS Malware Analytics, User Behavior Analytics)		
Fortify	源碼掃描 (Source Code Scanning) 網站掃描 (Black-Box Scanning of Web-Applications) 即時應用程式及網站保護- (RASP)		
IAM	登入認證 設備認證 認證管理		
Voltage	端點對端點的保護敏感資料-資料遮罩、格式保留加密技術及記號化等技術		
Atalla	Enterprise Secure Key Management (ESKM – Public Key Infrastructure)		

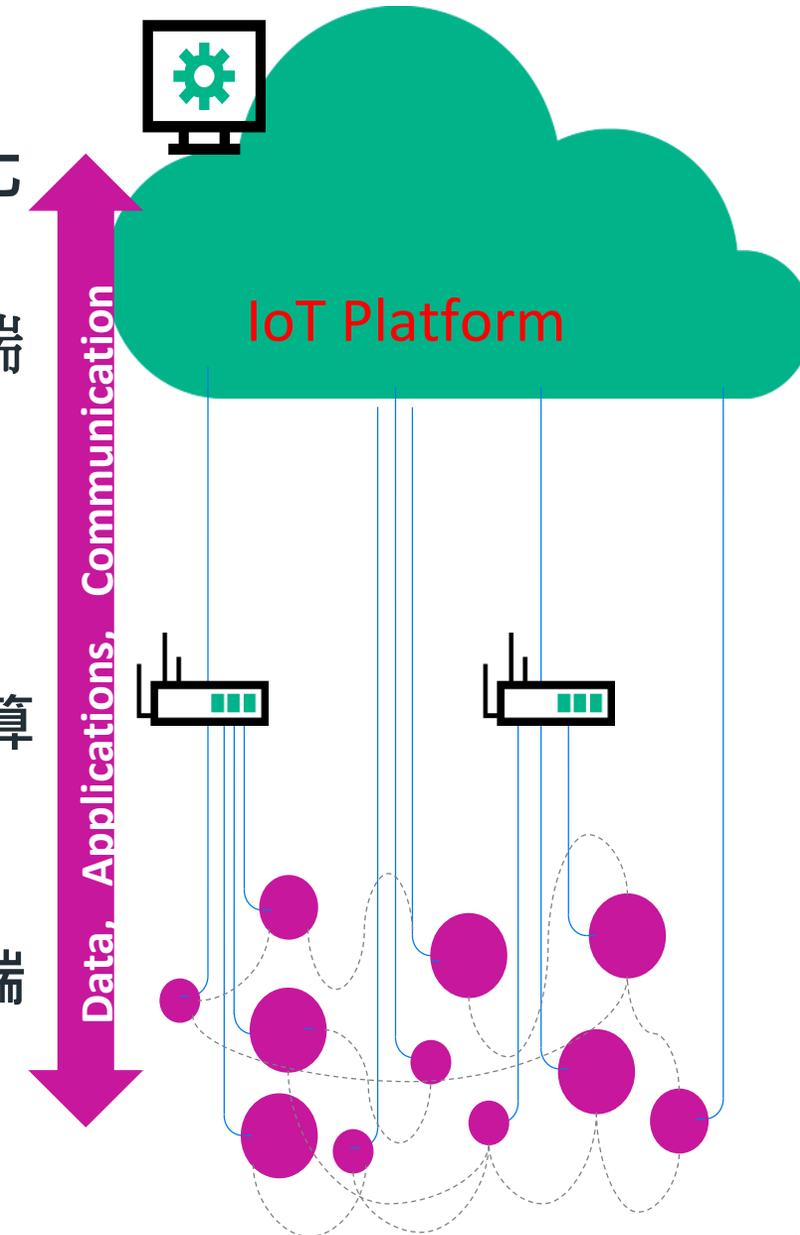
視覺化

IoT 雲端
/平台

連線

端點計算

IoT 終端
設備



Thank you.

www.microfocus.com

