iSecurity

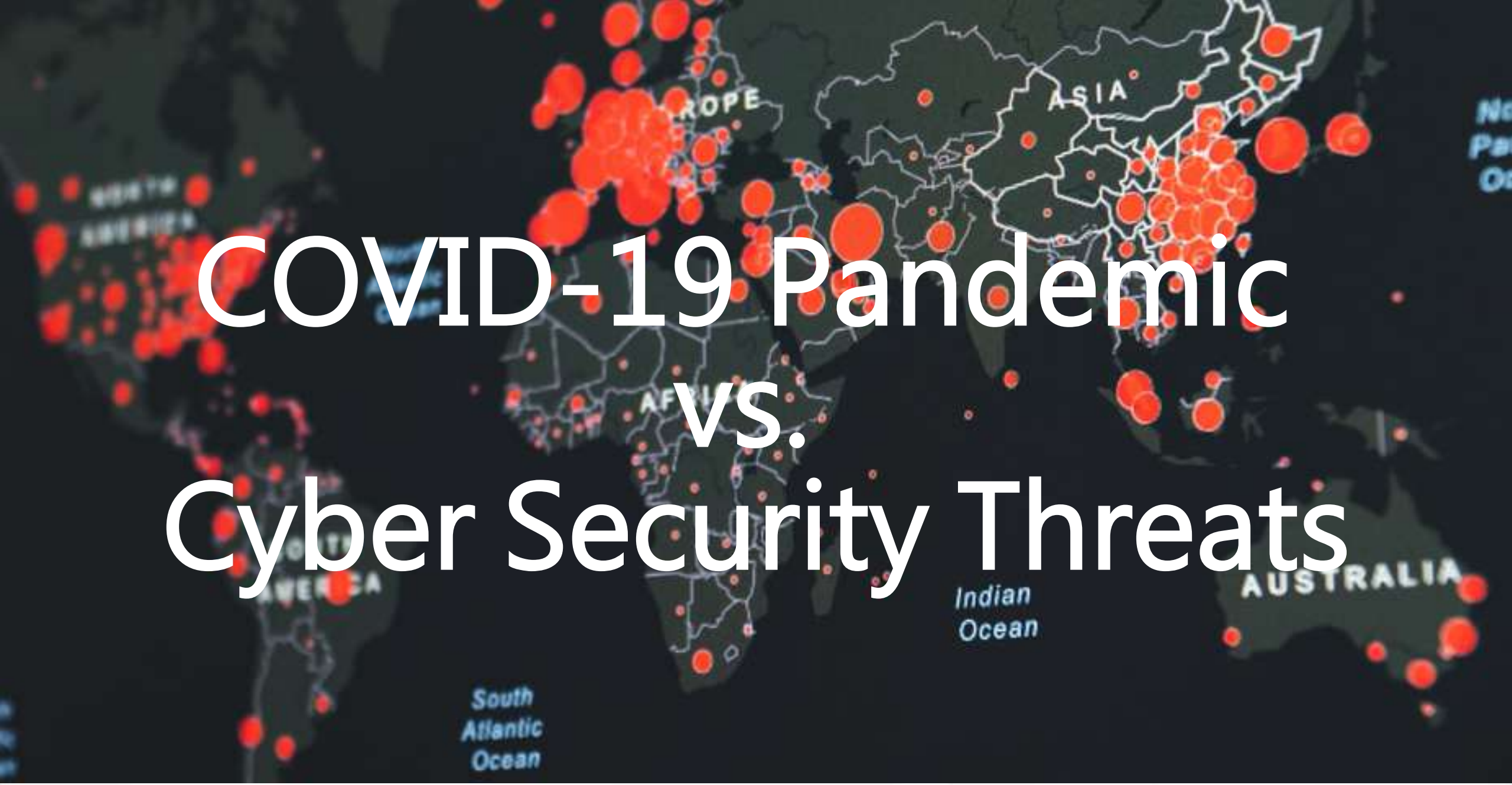
The Hub of Security Innovations

Reduce Breach Impact

阻絕擴散 降低損害

數位資安系統 | 陳建棠

COVID-19 Pandemic
vs.
Cyber Security Threats



iSecurity
The Hub of Security Innovations

世界各國因應COVID-19疫情相關措施

關閉邊境或對外停航	對外國人實施之簽證或境管措施	入境後隔離/檢疫措施
• 關閉國際航線 • 關閉邊境	• 禁止自有疫情之國家旅客入境 • 入境旅客須提供入境前72小時內核酸檢測陰性證明	• 自我隔離14天 • 社區隔離 • 縮小大型活動規模 • 禁止集會活動 • 強制配戴口罩與保持社交距離 • 進出公共場合及使用大眾運輸交通工具均須強制佩戴口罩

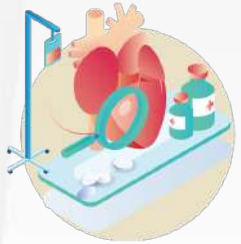
這些防疫措施
對照到
Cyber Security Framework
的防禦觀念

Identity Management & Access Control	Risk Management & Security Continuous Monitoring
身分識別管理&進出管控	風險管理&持續安全監控

NIST Cyber Security Framework

強化企業資安體質
為未知威脅做好準備

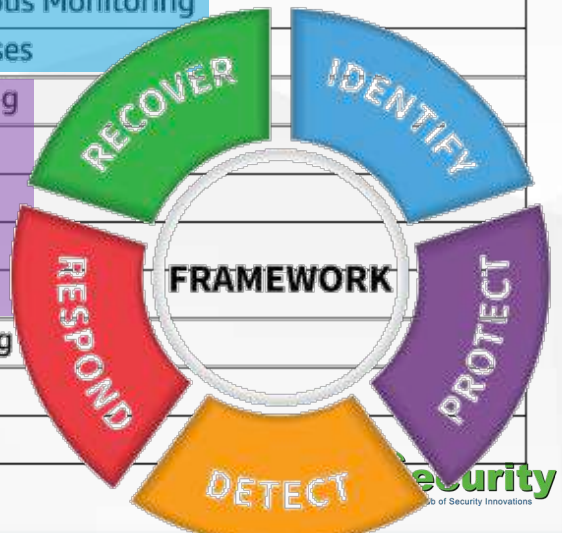
1 Stop More Attacks
超前部署，拒敵於境外



2&3 Find & Fix breaches faster
次世代資安維運中心

4 Reduce breach impact
阻絕擴散降低損害

Function		Code	Category
Identify	ID	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
Protect	PR	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
Detect	DE	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
Respond	RS	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
Recover	RC	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications



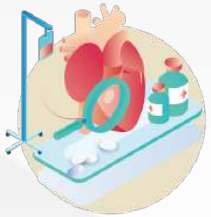
Cyber Secure Design Principles

National Cyber Security Centre

1. Establish the context before designing a system
   1.3 Understand the role of suppliers in establishing and maintaining system security
2. Make compromise difficult
   2.2 Reduce attack surface (減少被攻擊面)
3. Make disruption difficult
4. Make compromise detection easier
5. Reduce the impact of compromise (降低損害)
   5.1 Use a zoned or segmented network approach (阻絕擴散)

強化企業資安體質
為未知威脅做好準備
Cyber Resilience

1 Stop More Attacks
超前部署，拒敵於境外

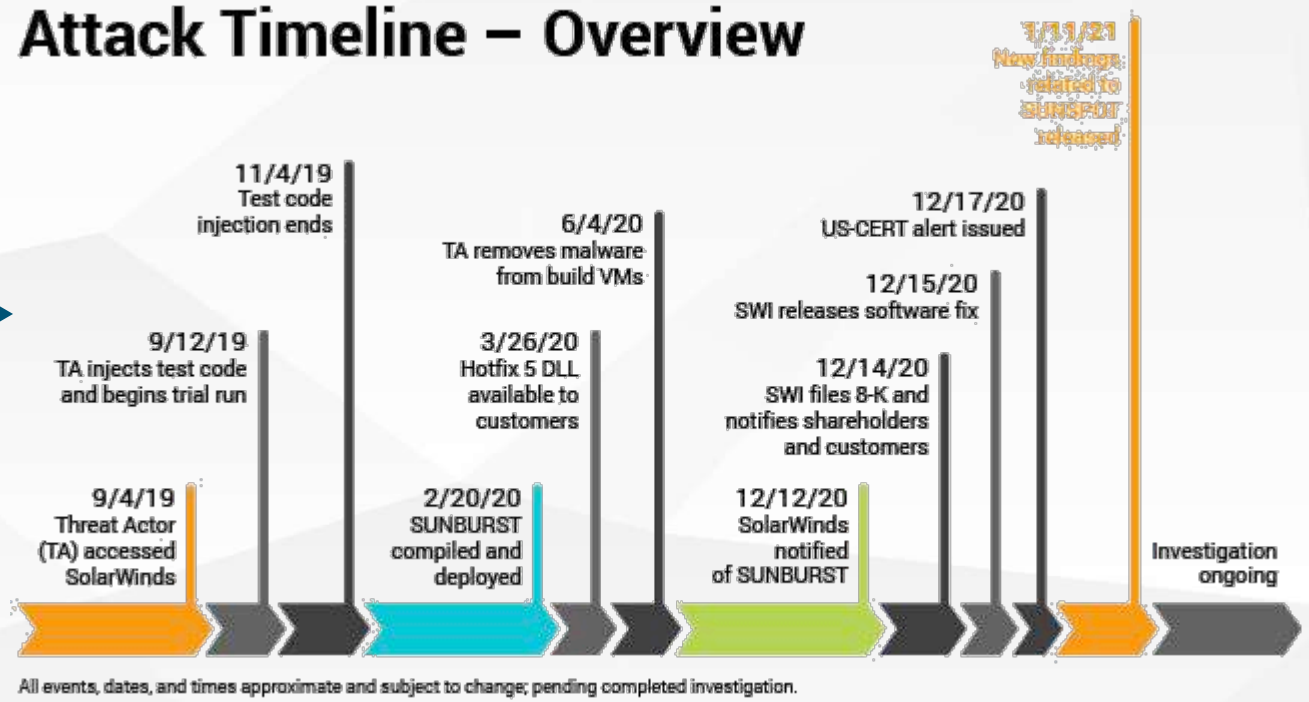


2&3 Find & Fix breaches faster
次世代資安維運中心

4 Reduce breach impact
阻絕擴散降低損害

iSecurity
The Hub of Security Innovations

SolarWinds Orion 供應鏈攻擊事件



iSecurity
The Hub of Security Innovations

iSecurity
The Hub of Security Innovations
←你以為的企業資產
←你所不知道的企業資產→
數位資產風險管理
(Digital Asset Risk Management)
RISKIQ

Improve Overall Situational Awareness

Discover Unknown Internet Assets

數位化的快速發展為企業的資安管理與其數位足跡(Digital Footprint)帶來威脅與隱憂

Investigate Threats

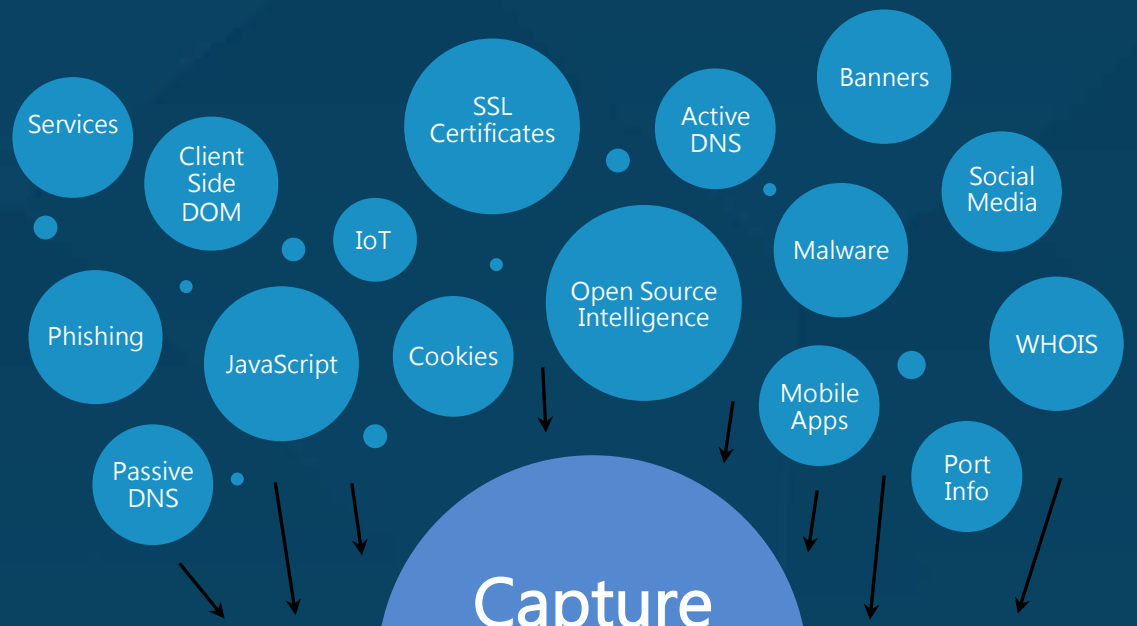
難以彙整所有相關數據來識別威脅並獲得真正可行的威脅情報 (Actionable Threat Intelligence) 來進行正確的響應動作

Incident Investigation and Intelligence

攻擊者(Threat Actors)持續將目標放在人性弱點這個攻擊層面(Human Attack Surface) 讓企業充滿壓力

iSecurity

Internet-Scale Collection



Capture
(Automated Discovery and Normalization)

10+
數十年的資料量
包含攻擊者的軌跡
與威脅情資

730B+
每年掃描超過
七千多億個網頁

300M+
收集超過三億筆
網域(DNS)資料

16M+
數千萬個APP的
分析資訊

- 250K New Domain Resolutions/ day
- 5.5M New Host Resolutions/day
- 106B+ Total Unique DNS Records

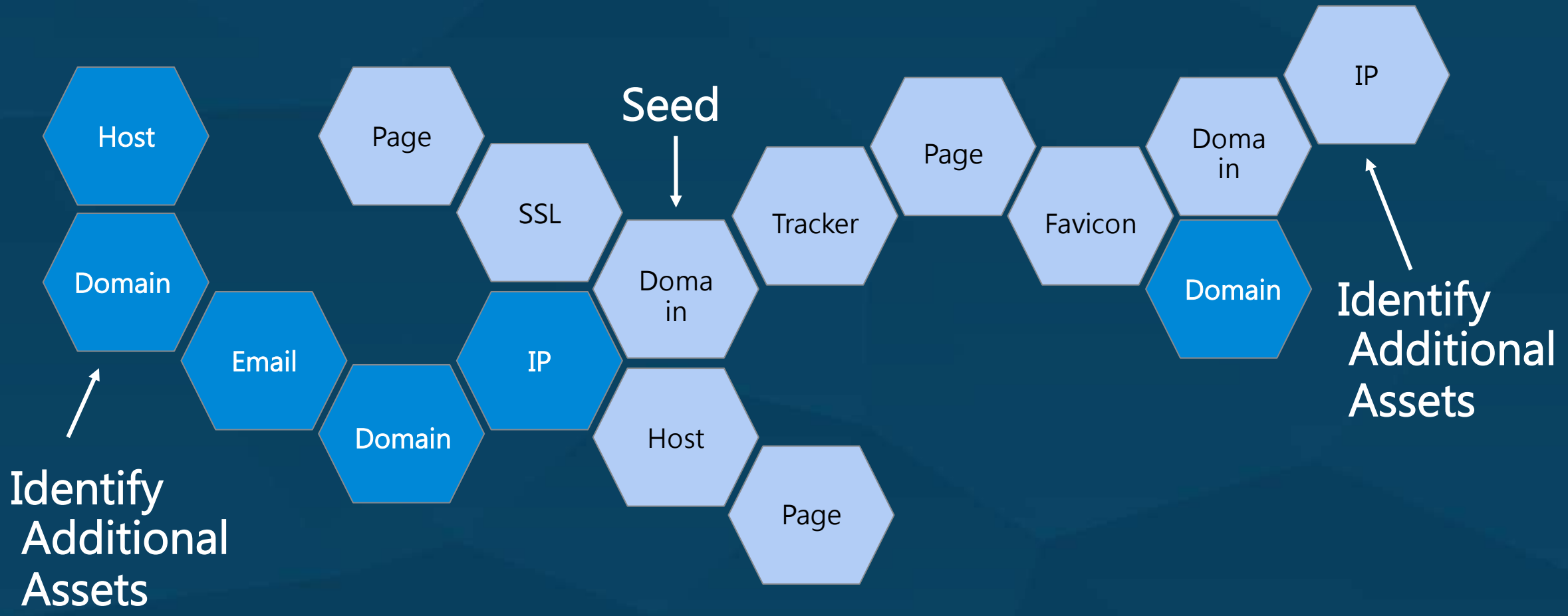
Advanced Internet Reconnaissance

RISKIQ

- 2B+ Crawls/ day
- 300K+ New Port Observations
- 300+ Mobile App Stores – 45M+ apps

iSecurity

Discovery – Infrastructure Chaining



RISKIQ

iSecurity

How can RiskIQ help you?

YOUR DIGITAL PRESENCE

	Web	Mobile	Social
Known Assets accounted for and owned by the organization through personnel or technical controls	Defacement Account Compromise Unauthorized Content Phishing	Compliance & Monitoring Unauthorized Connectivity	Ad Delivery 3rd-Party Code Redirections Partner Compromise
Unknown Assets unknown and unaccounted for by the organization, but have an association	Shadow IT Mergers & Acquisitions Orphaned IT Internet of Things	Shadow IT Mergers & Acquisitions Application Sprawl Unauthorized Partners	Unauthorized Accounts Mergers & Acquisitions Partner IP/Brand Auditing Legacy Accounts Unclaimed Accounts
Rogue Assets created by nefarious or malicious entities to harm the organization	Malware & Deception IP/Brand Infringement Credential Theft Phishing Fraud/Counterfeit	App Modification Fake/Infringing Apps Malware & Deception Credential Theft Copycat Apps	Fraud Malware Brand/Reputation Infringement

iSecurity
The Hub of Security Innovations

RISKIQ ATTACK INTELLIGENCE DASHBOARD

VISIBLE GLOBAL DASHBOARDS

- Digital Footprint Summary
- External Threats Summary
- RiskIQ Attack Intelligence Dashboard
- FireEye Red Team Tools Vulnerabilities
- Javascript Threats Summary

VISIBLE TEMPLATE DASHBOARDS

- Antiquated Assets & Decommissioning Insights
- Files Insights
- MITRE Attack
- National Security Agency | Cybersecurity Advisory
- Third Party Risk Insights

HIDDEN GLOBAL DASHBOARDS

- Andy: Test
- BM_GB
- BMG_N2
- BMG-1
- CISO Insights
- first - updated
- GDPR Compliance

RISKIQ ATTACK INTELLIGENCE DASHBOARD

Global Inventory

Dashboard Overview

Surface relevant and timely detections related to new vulnerabilities and the threat actors leveraging them in an effort to provide customers with visibility into potentially impacted devices in their Digital Footprint.

ATTACK INTELLIGENCE SUMMARY

Attack Surface: Summarized Asset Counts

ISC BIND 365	Internet Printing Protocol (IPP) 167	WebLogic Server 81	F5 Big-IP 80	Fortinet FortiGate 55
SonicWall 53	FortiGate Default Certificates 44	Exim Internet Mailer 44	Citrix NetScaler Gateway 44	Palo Alto GlobalProtect 35
SonarQube 28	Pulse Secure Connect 18	Microsoft SharePoint 10	SMBv1 8	Others 5

LATEST ATTACK INTELLIGENCE

0 SolarWinds Orion

RISKIQ

iSecurity

Panorays

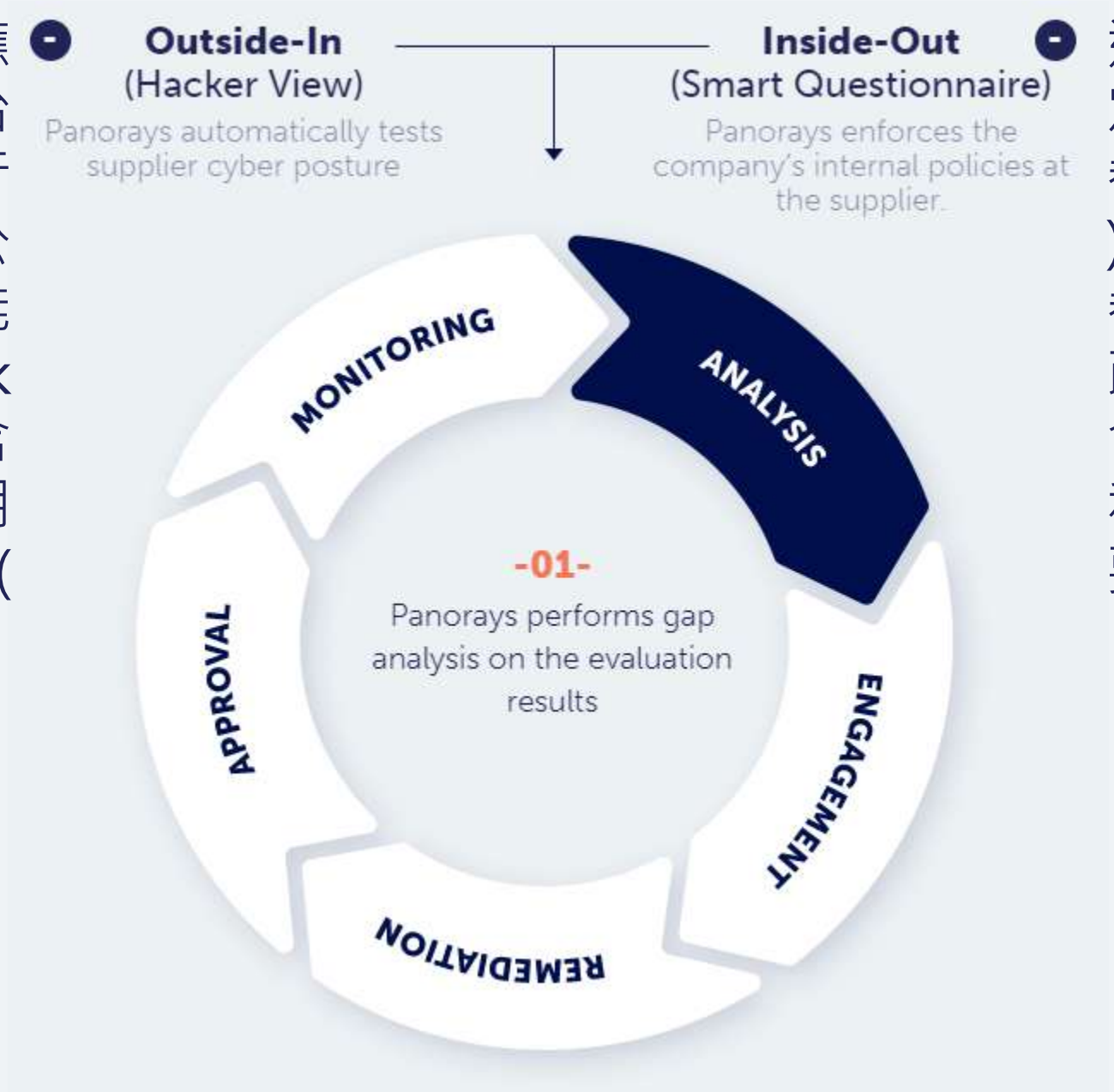
供應鏈風險管理
Supply Chain (3rd Party Vendor) Risk Management

iSecurity
The Hub of Security Innovations

Panorays

Automating Self-Assessment and Vendor Risk Management
自動化供應鏈廠商風險自評管理

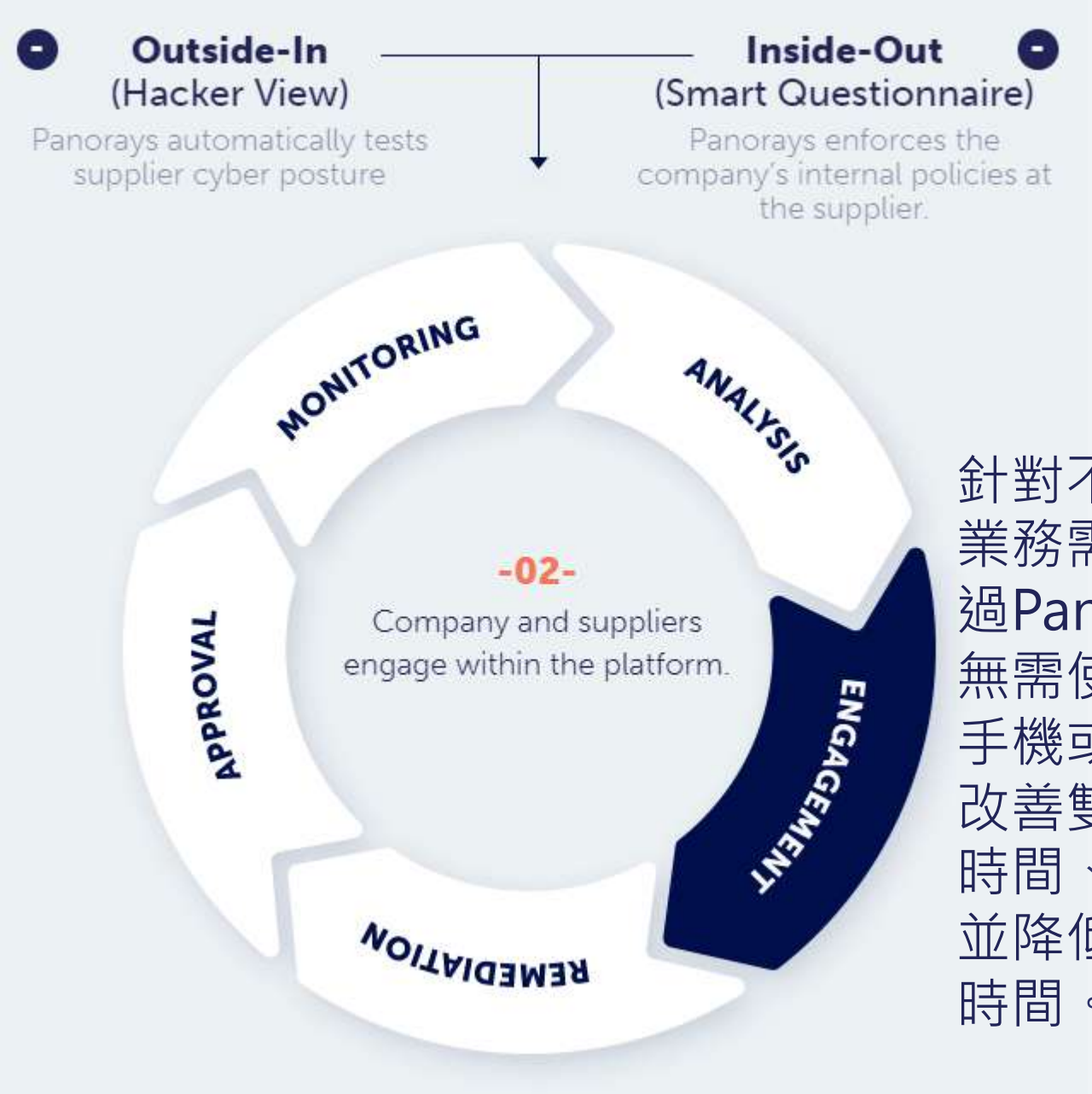
Panorays的供應鏈風險管理平台模擬駭客進行偵察，以發現公司和供應商可能的被攻擊面(Attack Surface)，包含網路、IT、應用層以及人員層(員工、承包商、客戶、供應商)



透過Panorays制定及管理調查問卷(Questionnaires)的平台，這些問卷包含公司內部政策，同時符合GDPR、CCPA和NYDFS等法規要求

Panorays

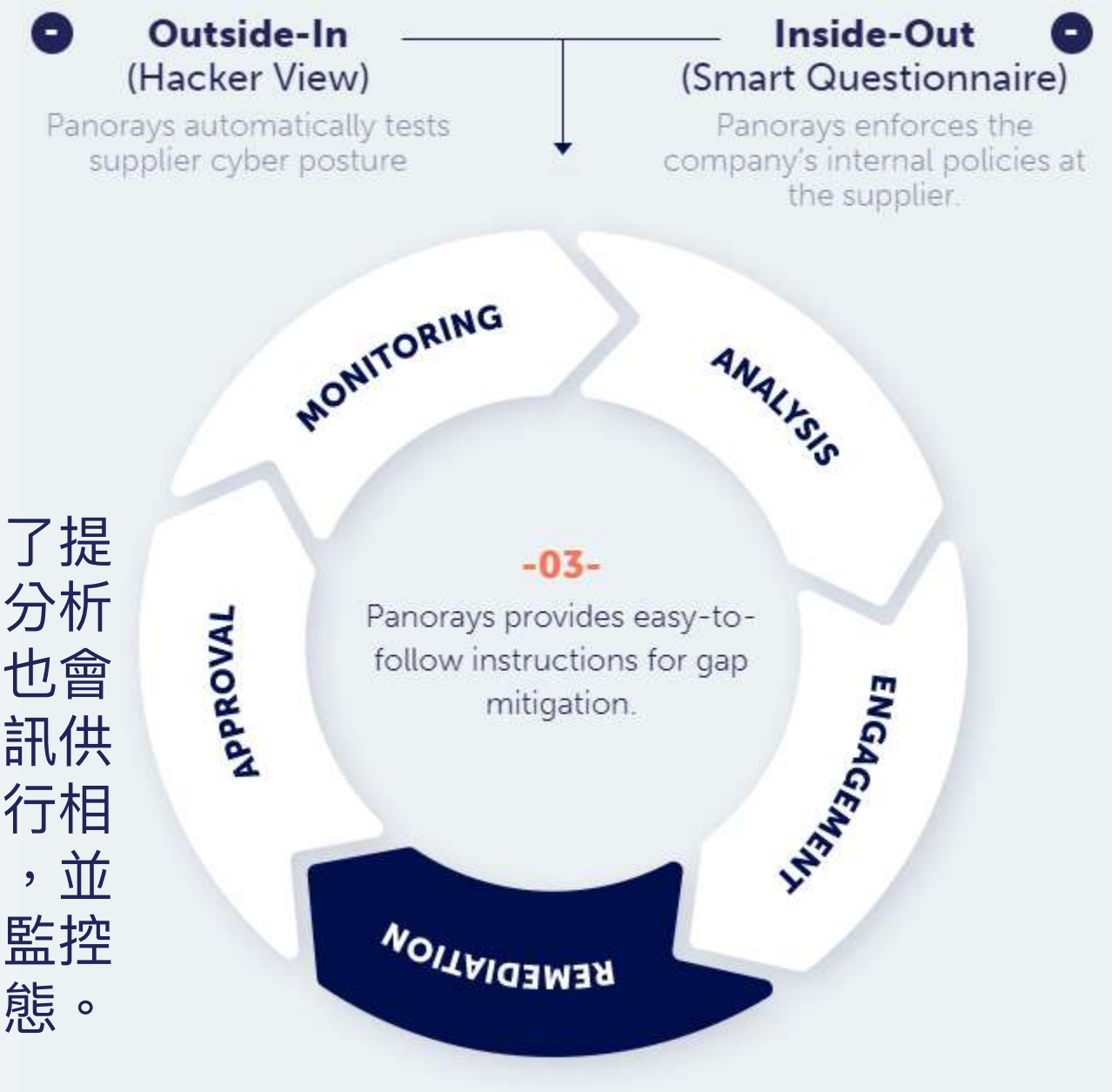
iSecurity
The Hub of Security Innovations



針對不同供應鏈的業務需求，統一透過Panorays平台且無需使用人工方式(手機或E-mail等)，改善雙方作業等待時間、提升參與度並降低解決問題的時間。

Panorays

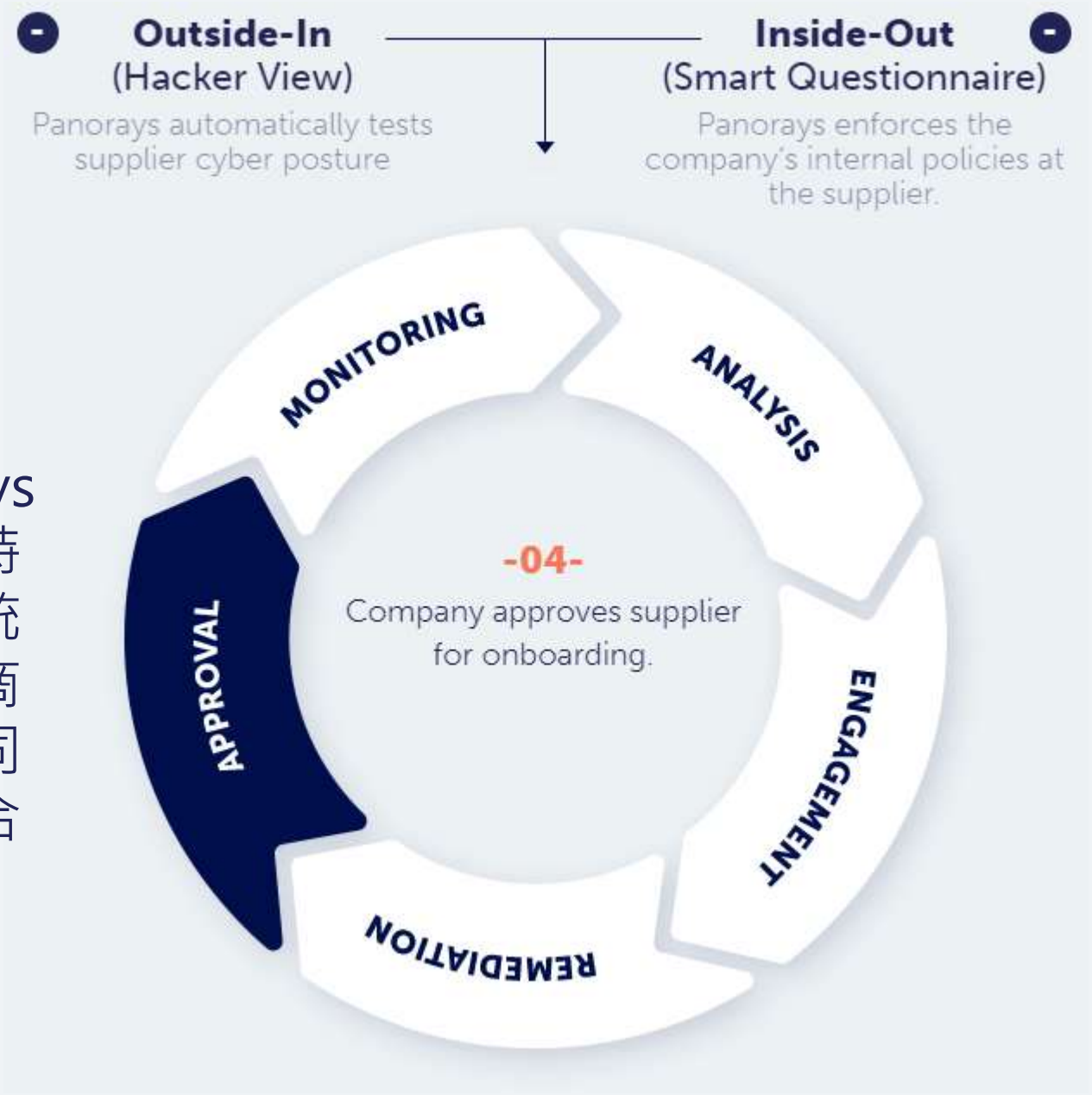
iSecurity
The Hub of Security Innovations



Panorays除了提供網路安全分析與評比外，也會提供相關資訊供資安人員進行相關問題修復，並於後續持續監控網路安全狀態。

Panorays

iSecurity
The Hub of Security Innovations



透過Panorays平台可於短時間內驗證與統一控管供應商是否符合公司內部制定的合規性政策。

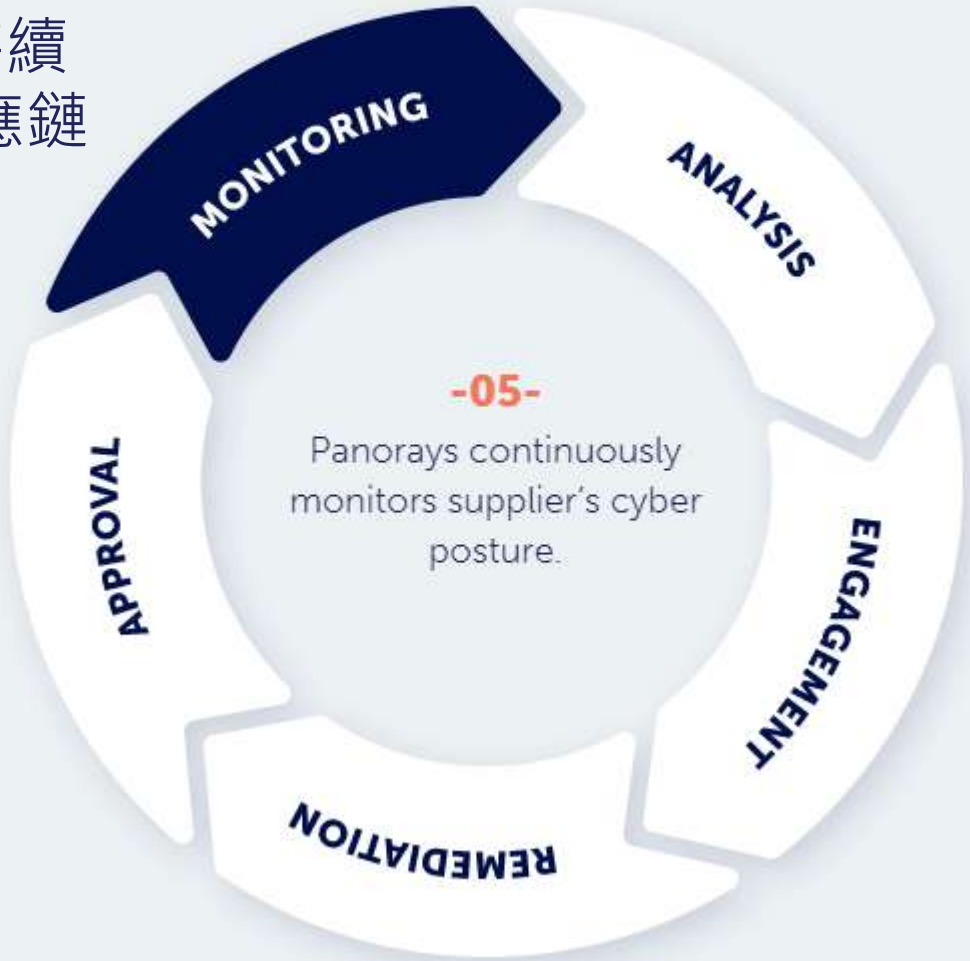
Panorays

iSecurity
The Hub of Security Innovations

Outside-In
(Hacker View)
Panorays automatically tests supplier cyber posture

Inside-Out
(Smart Questionnaire)
Panorays enforces the company's internal policies at the supplier.

透過Panorays 7*24持續性的監控，可確保供應鏈的資安狀態並於偵測到網路危害時發送告警通知，提醒相關人員進行修補。



Panorays

iSecurity
The Hub of Security Innovations

CYBER ASSESSMENT

Risk Rating

Poor

Business Im

MINIMAL

Remediation Plan

[redacted] has to improve its risk rating in order to comply with [redacted]'s policies.

Portfolio Overview

25
Suppliers

Posture Rating Distribution

Inquiry Rating Distribution

No Results

Inquiry Status

Suppliers Assets Geolocation

2
Inquiries Sent

Ø
Average days to answer

Ø
Average Inquiry Rating

No Results
Approved Suppliers

No Results
Rejected Suppliers

25
Pending Approval

Top 10 Industries by Count

Financial Services
Computer Hardware
Internet Software & Services
Insurance
Investment Banking
Investment Management
Management Consulting
Airlines
Research & Consulting Services
Airlines/Aviation

Suppliers

Industry vs Portfolio Ratings

Average Industry Rating
Portfolio Industry Rating

GDPR Compliance Level

No Results

Business Impact Distribution

Minimal
Significant
Business Impact

Relationships by Count

GDPR
On Premise Solution
Permanently Holds Sensitive Data
Holds Credentials
Web Access
Managed Service Provider
Provides Mobile App
Temporarily Holds Sensitive Data

Suppliers

Self Assessment

[redacted]

Cyber Posture Rating

NETWORK AND IT

77

79

80

88

0-55
56-79
80-100

+ Add Findings

Status
2 Open issues

Status
2 Open issues

SHARE

Panorays

iSecurity
The Hub of Security Innovations

目前一般泛用的管理方案

定期安全調查表 (Periodic Security Surveys)

- 昂貴並耗時
- 立即過期
- 缺乏覆蓋範圍和規模

Instructions: Check the appropriate column to indicate the application's security capabilities. Please provide any additional responses or detailed explanations of either compensating controls as comments. Please number your comments in the appropriate column, and match the comment number with your detailed explanations at the end of this form. This questionnaire currently applies to healthcare applications and does not address the operating system or hardware controls.

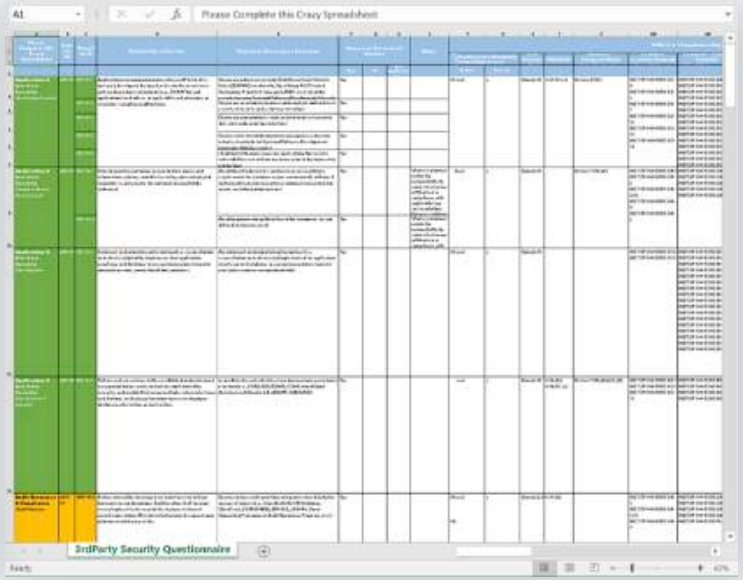
Application Security Questionnaire

Application Name	Vendor	Version	Release Date
Application supports the following business functions:			

Vendor Representative Contact Information	Name	Title	Department
	Company Name	Telephone #	e-mail

#	ACCESS MANAGEMENT	Yes	No	N/A	Comment #
1.1	Does the application support integration with the enterprise identity management system?				
	a. If yes, indicate the alert (such as Directory Services, LDAP, Kerberos, etc.): _____				
1.2	Is user authentication controlled by means other than user account and password or PIN?				
	a. If yes, indicate what other mechanisms are used (e.g. certificates, token, biometric, etc.):				
	Questions 1.3 through 1.8 apply to the use of passwords				
1.3	Does the application force "new" users to change their password upon first login into the application?				
1.4	Can the user change their password at any time?				
1.5	Can the system administrator enforce password policy and/or complexity such as minimum length, numbers and alphabet requirements, and upper and lower case constraint, etc.?				
1.6	Can the application force password expiration and prevent users from reusing a password?				
1.7	Is password transmission and storage encrypted and unreadable even to the system administrators?				
1.8	Can the application be set to automatically lock a user's account after a predetermined number of consecutive unsuccessful logon attempts?				
1.9	Does the application prohibit users from logging into the application on more than one workstation at the same time with the same user ID?				
1.10	Can the application be set to automatically log a user off the application after a predefined period of inactivity?				

© 2007, HIMSS. All rights reserved. Version 2.3 (Feb. 07) Page 1 of 7



Please Complete this Crazy Spreadsheet

3rdParty Security Questionnaire

費時費力但所獲得的稽核調查結果不是最即時的，而且覆蓋範圍與規模很低！

Panorays

iSecurity
The Hub of Security Innovations

安全性問題集 Security Inquiries Questionnaire

選擇您自己的問卷

您可以使用標準的SIG或Panorays的內置安全調查表。上傳您自己定義的內部政策，並建立某些條件性問題以澄清答案。也可以執行法規政策，例如GDPR和NYDFS。以下為參考範本。

問題分類

問題內容

可調問題權重

可以要求供應商提供補充說明

評估者(業主)視角

[redacted] > Security Inquiry

Security Inquiry

Displaying Inquiry: Apr 4, 2020

Request To Update

Security Inquiry Rating	GDPR Compliance Level	Status	Contact Person (1)
47	--	Done	j[redacted]@[redacted].com
Out of 100	Not Applicable	Submitted on: Apr 4, 2020	

評分
為47分

表示
已經
完成

Inquiry (91/129 answered)

129個問題
中已回覆9
1個

- HIPAA
- ENISA
- British Standard 7799 Part 3
- ISF Standard of Good Practice
- ISAE3402
- Other

If you selected "Other", please elaborate:

none

If you selected "Other", please attach:

No file attached

Are you ISO 27001 Certified?*

More Information

Which of the following standards and regulations do you adhere to or comply with?

☐ ISO-22307	10
☑ NIST	10
☐ COBIT	10
☐ COSO	10
☐ ITIL	10
☐ HIPAA	10
☐ ENISA	10
☐ British Standard 7799 Part 3	10
☐ ISF Standard of Good Practice	10

權重weight

Activity

線上直接與
供應商互動

Me. 19 hours ago.
If you do not mind it, would you please share with us why there is no other standard being compliant? Can you have HIPPA and ISO-22307?

Messages 1 Message

Type a message

Panorays

Smart Questionnaire for SolarWinds Event

[redacted] > Smart Questionnaire™

Smart Questionnaire™

17 10/10 answered

CATEGORIES

SolarWinds - Supply Chain Attack Awa...
10 questions 17

QUESTIONS

SolarWinds - Supply Chain Attack Awareness Questionnaire

At this time, is there any known exposure of your company's data or systems that you or your critical vendors may host in support of your company or the services you provide to our company?*

- ○ Yes
- ◉ No

Relationship

Do you have the Orion product implemented with version 2019.4 through 2020.2.1 found here?*

- ○ Yes
- ◉ No

Panorays

iSecurity
The Hub of Security Innovations

SolarWinds Orion 供應鏈攻擊事件帶給我們的啟發

- 做好企業數位資產的管理與追蹤
- 瞭解您的第三方/第四方合作廠商
- 充分掌握聯絡窗口
- 緊急開關 (Kill-Switch) 的設置
- 通報系統的自動化
- 持續性不中斷的監控

iSecurity
The Hub of Security Innovations

美國佛羅里達州淨水處理廠網路攻擊事件

- Windows 7
- Weak Password
- Shared Password
- TeamViewer
- No Firewall on the host

Photo source: Florida Water Daily @ flickr

iSecurity
The Hub of Security Innovations

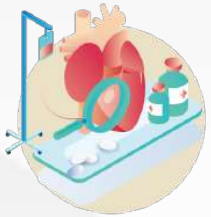
Cyber Secure Design Principles

National Cyber Security Centre

1. Establish the context before designing a system
   1.3 Understand the role of suppliers in establishing and maintaining system security
2. Make compromise difficult
   2.2 Reduce attack surface (減少被攻擊面)
3. Make disruption difficult
4. Make compromise detection easier
5. Reduce the impact of compromise (降低損害)
   5.1 Use a zoned or segmented network approach (阻絕擴散)

強化企業資安體質
為未知威脅做好準備
Cyber Resilience

1 Stop More Attacks
超前部署，拒敵於境外



2&3 Find & Fix breaches faster
次世代資安維運中心

4 Reduce breach impact
阻絕擴散降低損害

iSecurity
The Hub of Security Innovations

WATERFALL®
Stronger Than Firewalls

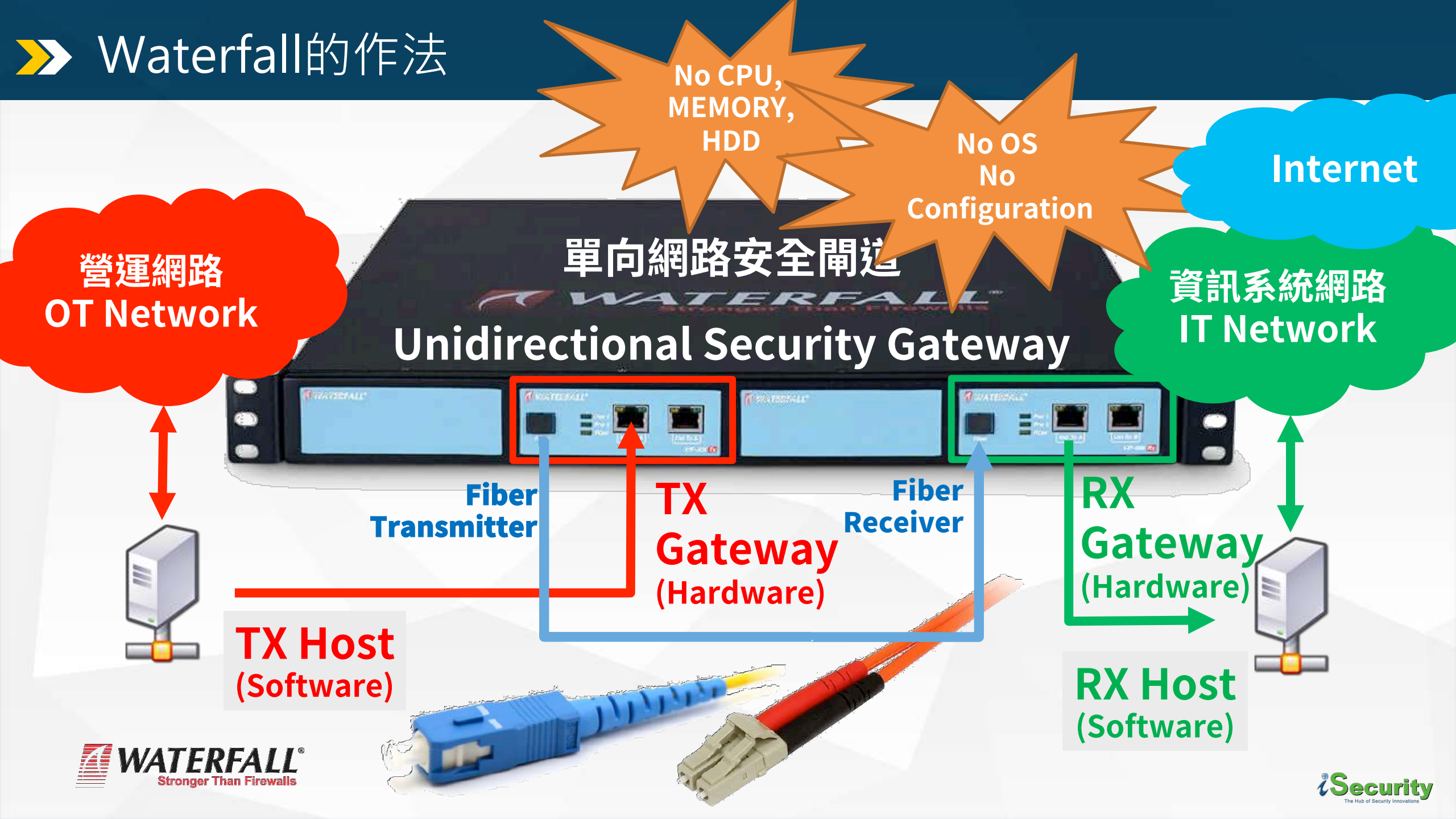
iSecurity
The Hub of Security Innovations

實體隔離網路架構
資料單向傳輸
解決方案

Why Firewall is not enough?

- 連接防火牆的實體網路是雙向的通訊，無論是以光或是電為傳輸媒介。
- 防火牆是一個作業系統，有軟體就有BUG或是漏洞的可能，有漏洞就有被入侵的可能。
- 若被入侵則防火牆政策形同虛設。
- 人為設定(Misconfiguration)的疏忽！
- 防火牆管理者的人性弱點！

Waterfall的作法



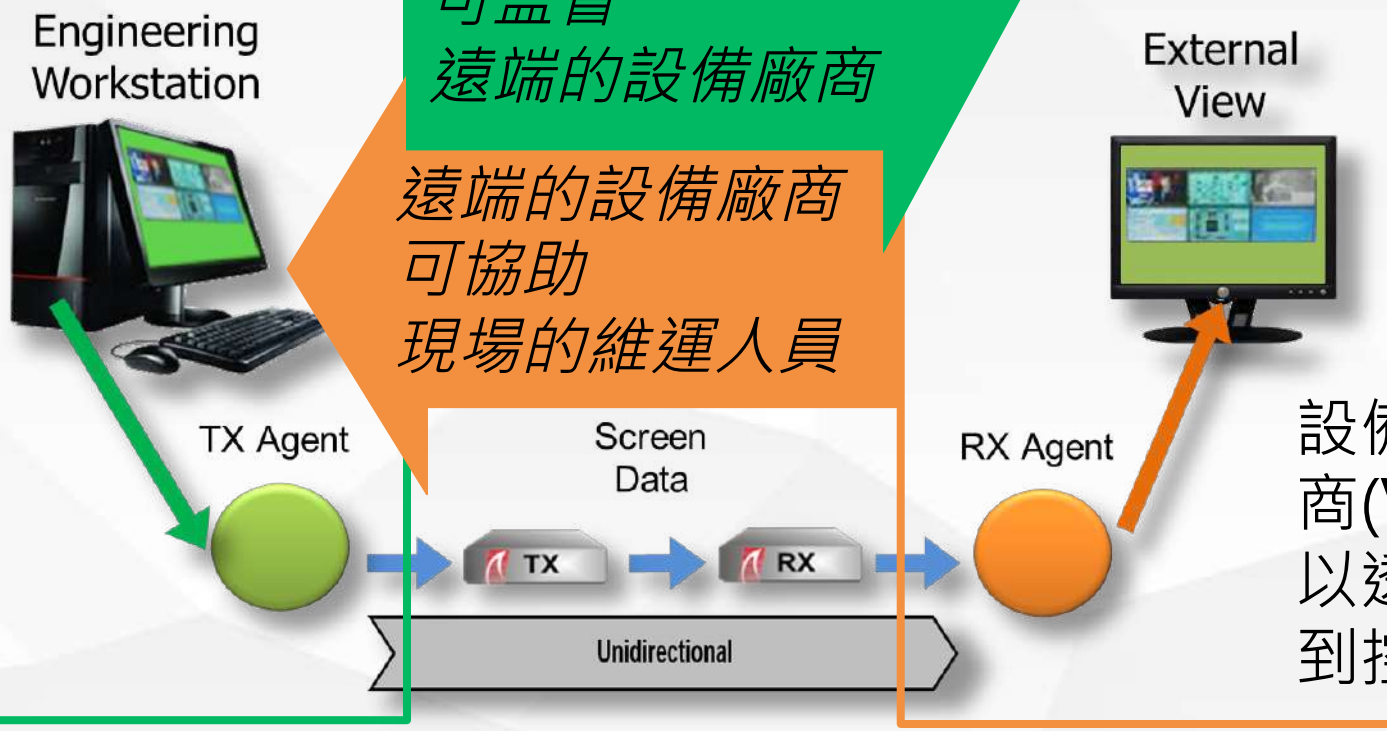
Remote Access：Remote Screen View

現場工作環境

遠端監視環境

現場的維運人員可監督遠端的設備廠商

遠端的設備廠商可協助現場的維運人員



維運人員(OP)能夠在現場控制系統並透過電話與設備廠商溝通

設備廠商(Vendors)可以透過瀏覽器看到控制系統的畫面

所有的系統狀況及異動皆可讓設備廠商清楚了解並即時的協助維運人員處理現場問題

WATERFALL® Stronger Than Firewalls

iSecurity The Hub of Security Innovations

兩種單向佈署方向皆可阻擋網路攻擊

資料由Safe Zone傳至Unsafe Zone

資料由Unsafe Zone傳至Safe Zone

WATERFALL® Stronger Than Firewalls

iSecurity The Hub of Security Innovations

工控威脅偵測

radiflow
Secure your Assets

iSecurity
The Hub of Security Innovations

階段性檢視整體工控資安防護層級

1 Assessment

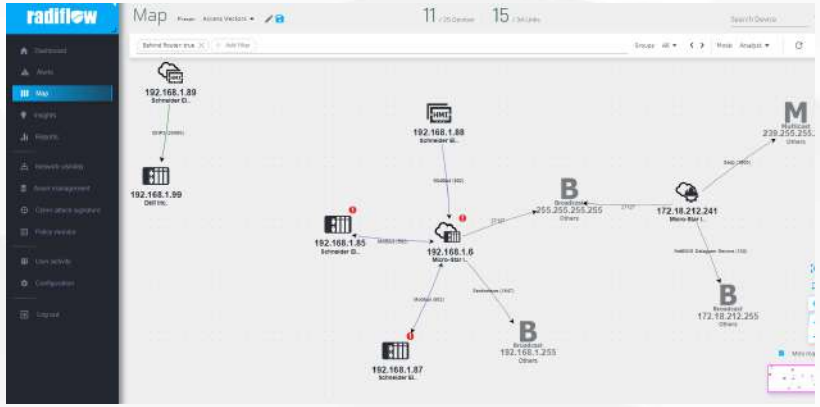
百分百被動模式, 容易佈署

2 Detection(iSID)

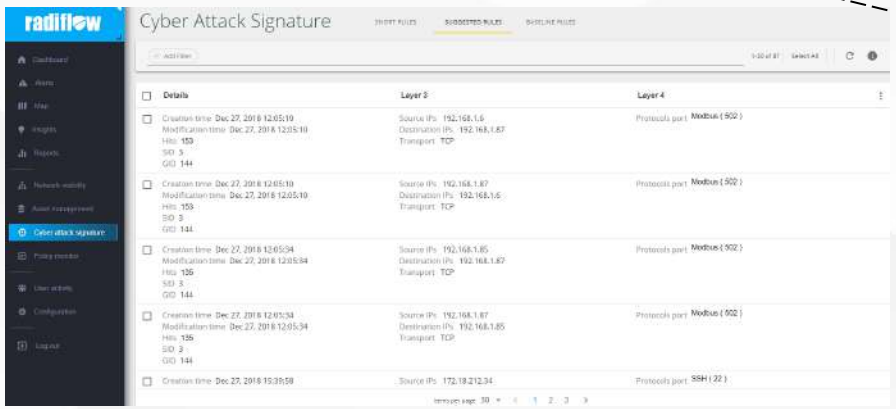
用 port mirroring (或 iSAP Smart Collector)將流量導向至iSID, 不會有停機時間

Prevention 3

分析工控網路流量



呈現網路拓樸架構



未授權/異常活動告警

radiflow
Secure your Assets

iSecurity
The Hub of Security Innovations

多層次工控安全資安防護引擎

透過被動掃描(Passive Scanning)來檢視所有OT網路流量，將所有設備、網路通訊協定及連線數據建立視覺化網路拓樸，甚至是普渡(Purdue)模型

比對網路攻擊威脅數據，亦可自訂SNORT規則

可驗證網路通訊中的特定指令（例如：寫入控制器）和操作範圍（如：不可將渦輪機轉速設置高於800轉）

深度封包解析(Deep Packet Inspection ,DPI)每一個網路連線，判斷網路行為是否異常

當特定設備在特定時間內的維護工作進行時，可透過設定來限制維護期間的網路暴露風險。當維護階段完成後，可產生所有維護工作的活動日誌報告

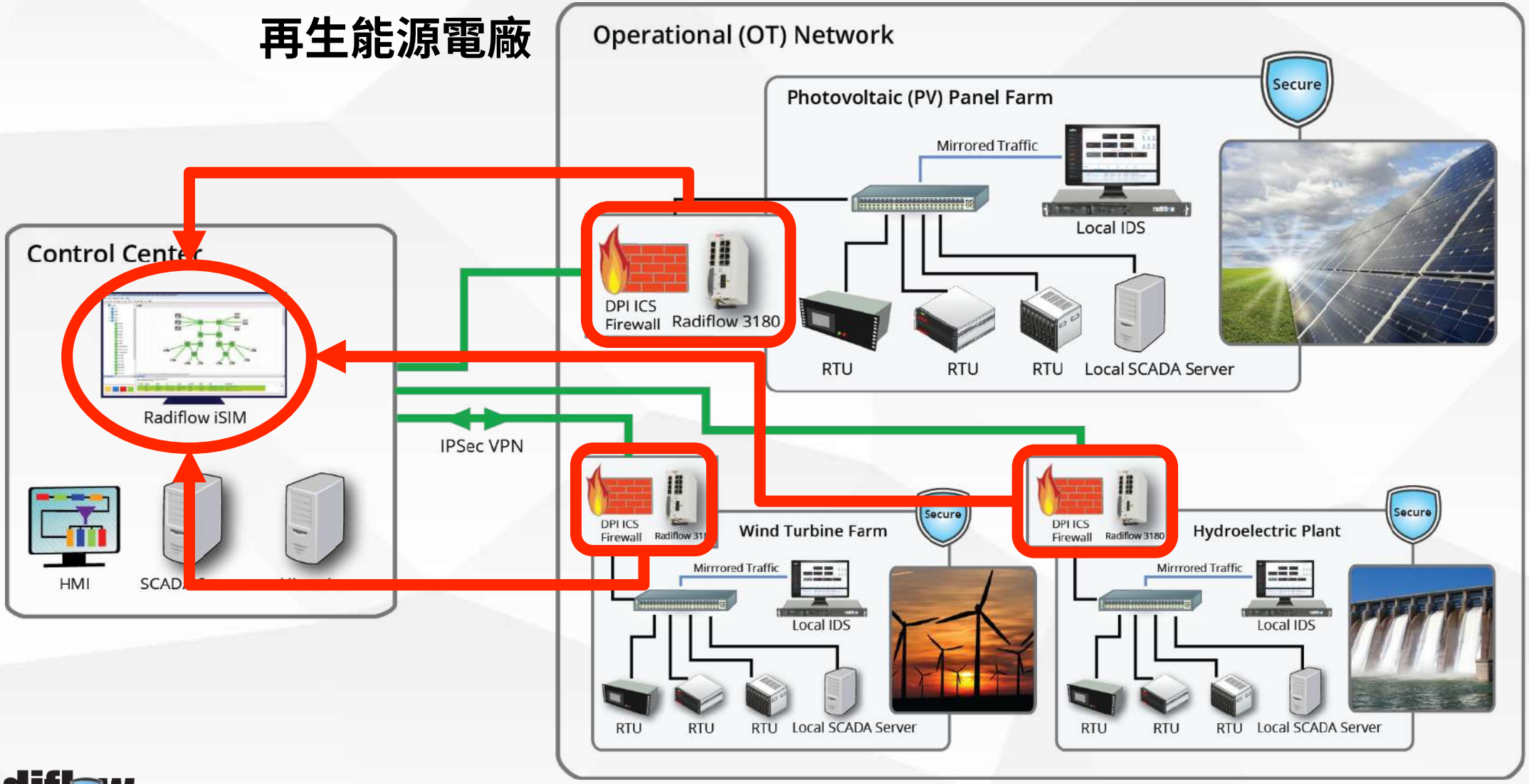
監視和稽核外部站點設備（PLC, RTU & IED）的運作管理，並可發出韌體變更或配置修改（如：軟體更新或是開啟/關閉了設備）以及活動紀錄的告警

radiflow
Secure your Assets

iSecurity
The Hub of Security Innovations

實際應用案例

再生能源電廠



radiflow
Secure your Assets

iSecurity
The Hub of Security Innovations

回顧

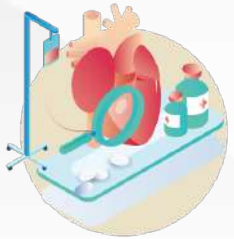
Cyber Resilience

Reduce Breach Impact

- 掌握企業數位資產
  做好風險威脅管控
- 瞭解供應鏈廠商
  並做好風險管控
- 依重要性區隔網路
  做好網路存取管控
- 持續監視重要網路
  及時告警及早因應

強化企業資安體質
為未知威脅做好準備
Cyber Resilience

1 **Stop More Attacks**
超前部署，拒敵於境外



2&3 **Find & Fix breaches faster**
次世代資安維運中心

4 **Reduce breach impact**
阻絕擴散降低損害

iSecurity
The Hub of Security Innovations