OT資產之設定、變更、漏洞與合規管理 – Industrial Defender

研杰科技

Justin Chang

justin@youngtec.com.tw

Industrial Defender公司介紹

INDUSTRIAL DEFENDER®

- 成立於2006年，總部位於MA, USA
- 來自麻省理工學院的扎實控制系統工程專業知識
- OT資訊安全解決方案的創始者
- 曾與洛克希德·馬丁公司密切合作一段期間
- **10**多年前就通過ABB公司**800xA** DCS的測試與驗證
- 多年來持續獲得多種國際獎項

研杰科技
YOUNGTEC

- 成立於2001年
- 代理OT業界全球知名Kepware公司產品超過18年
- 2021年正式加入PTC公司的IIoT行銷體系
- 2021年正式代理Industrial Defender公司的OT資安軟體產品
- 專精於工業控制系統與企業資訊系統資料通訊問題處理
- 致力於協助製造業OT結合IT技術的軟體系統建置與問題排除

OT資安防護實施困難點

無資產清單
不知道生產環境中有哪些OT設備

弱點和風險
無從得知設備弱點曝露情形和風險程度

異動偵測
很難得知設備設定是否已被惡意更動

老舊設備
老舊OT設備資安防護能力有限

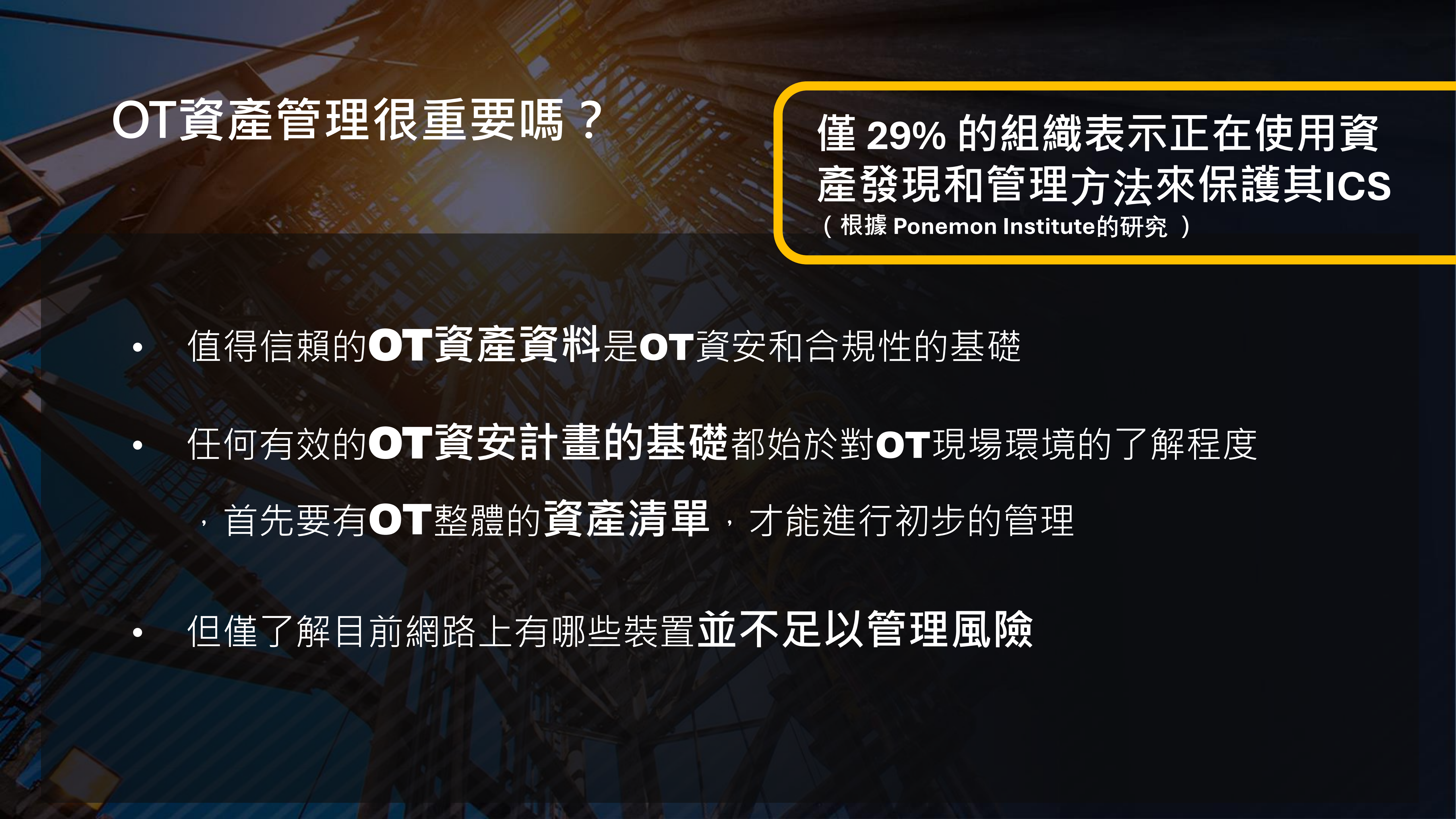
目前製造業對OT資安的普遍看法與措施

隔離　只要將工廠網路和企業網路隔絕 就萬無一失

單向傳輸　企業資訊網路資料不會進到工業生產網路

靠運氣　假設駭客不懂工業控制系統

有網路資安就足夠　與IT資安採用相同或類似的方案



OT資產管理很重要嗎？

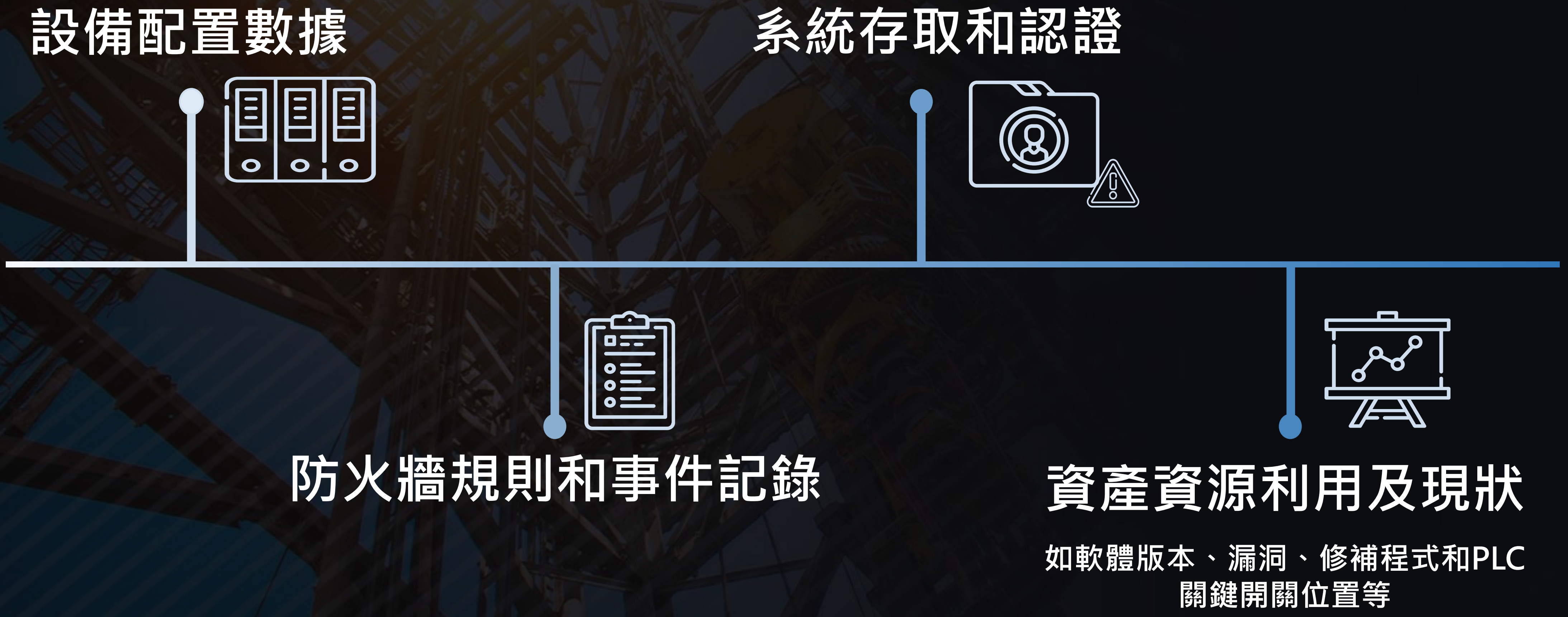
僅 29% 的組織表示正在使用資產發現和管理方法來保護其ICS
（根據 Ponemon Institute的研究 ）

- 值得信賴的**OT資產資料**是**OT**資安和合規性的基礎

- 任何有效的**OT資安計畫的基礎**都始於對**OT**現場環境的了解程度，首先要有**OT**整體的**資產清單**，才能進行初步的管理

- 但僅了解目前網路上有哪些裝置**並不足以管理風險**

Industrial Defender
管理的OT資產資料類型



設備配置數據

系統存取和認證

防火牆規則和事件記錄

資產資源利用及現狀

如軟體版本、漏洞、修補程式和PLC
關鍵開關位置等

Industrial Defender OT資產管理的優勢

- 建立高效率的**配置和變更管理**流程
- 支持更**全面的風險評估**並緩解風險
- 大量減少**修補風險的時間**
- 建立單一真實來源以**提高維護效率**
- 啟用持續的**漏洞和修補程式管理**
- 建立**備份和復原基礎**

一流的OT資安大數據收集方法

無代理程式溝通 (Agentless)

代理程式溝通 (Agent)

被動監聽網路流通封包

資料庫匯入

設備商自家通訊協定輪詢

手動輸入

為何深度配置可見性對於OT資安至關重要

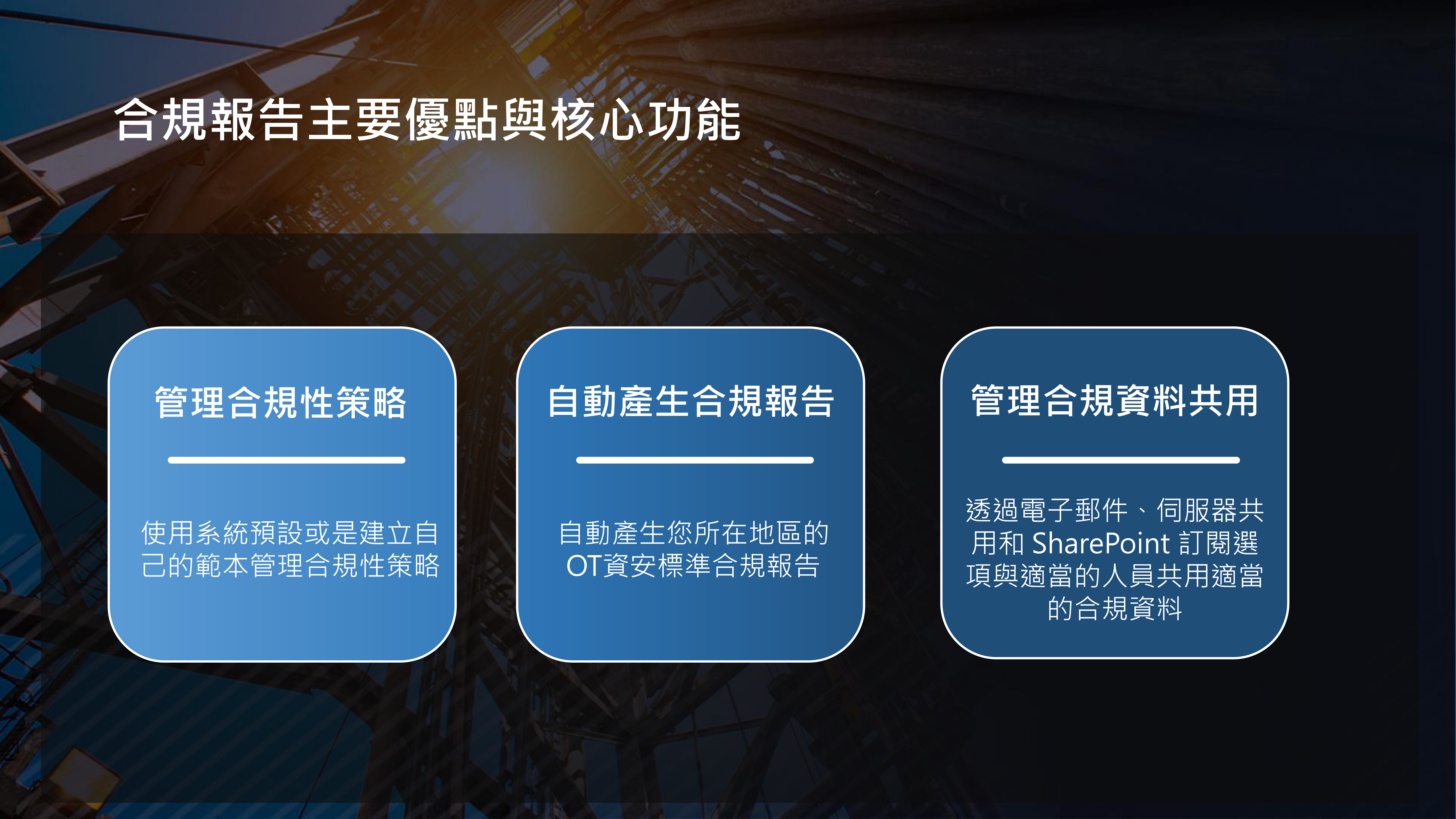
- 識別攻擊者的**潛在入口點**

- 未經授權的變更 - 導致**操作問題和系統不穩定**

- 不當的系統變更 - 可能會**引入錯誤配置和漏洞**

完整、準確、最新的漏洞資訊

- ◆ 為每個裝置建立漏洞輪廓檔
- ◆ 確保擁有最完整、最新的可用漏洞和修補程式訊息
- ◆ 不斷持續執行此操作
- ◆ 產出風險評分
- ◆ 與FoxGuard合作



合規報告主要優點與核心功能

管理合規性策略

使用系統預設或是建立自己的範本管理合規性策略

自動產生合規報告

自動產生您所在地區的OT資安標準合規報告

管理合規資料共用

透過電子郵件、伺服器共用和 SharePoint 訂閱選項與適當的人員共用適當的合規資料

NIST Cyber Security Framework

確認
Identify

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

防護
Protect

- Access Control
- Awareness and Training
- Data Security
- Info Protection Processes and Procedures
- Maintenance
- Protective Technology

察覺
Detect

- Anomalies and Events
- Security Continuous Monitoring
- Detecting Processes

反應
Respond

- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

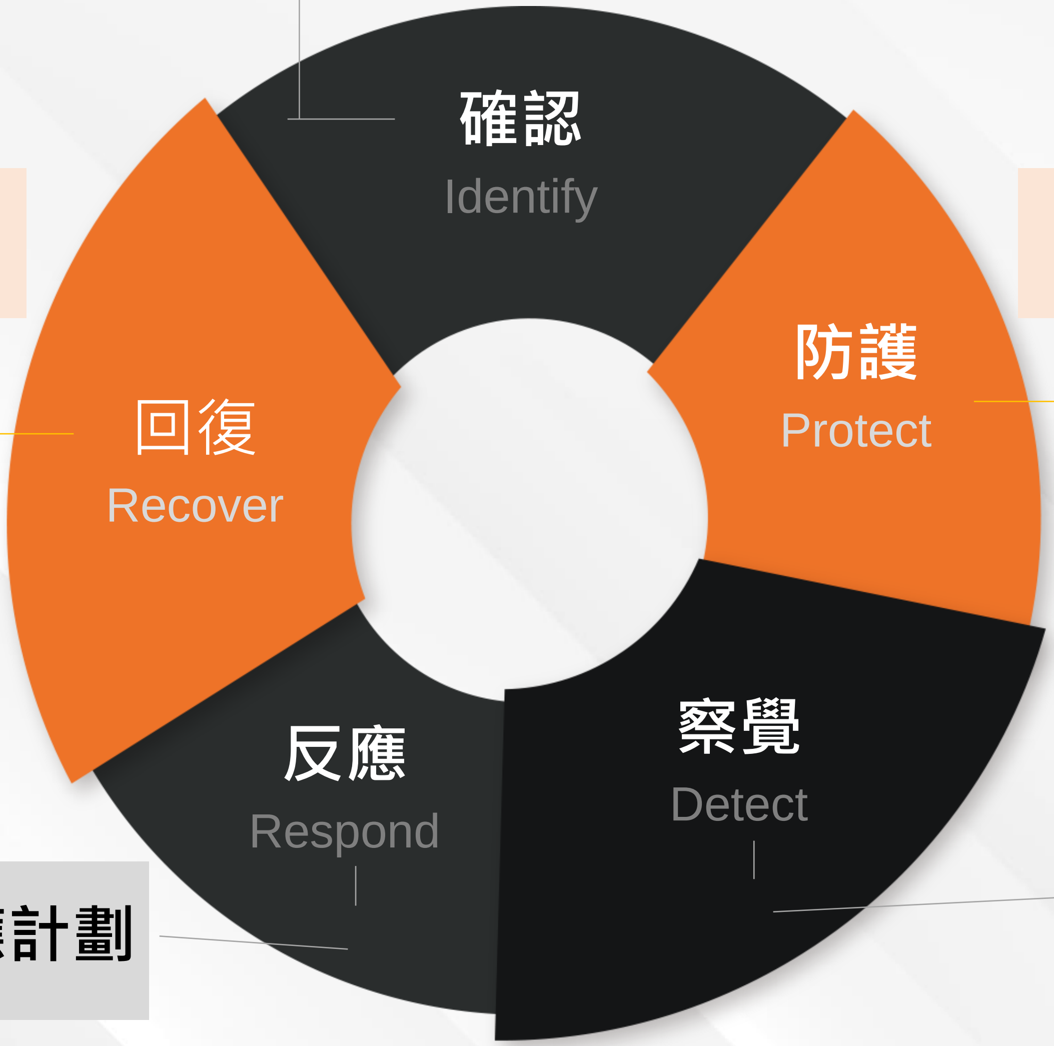
回復
Recover

- Recovery Planning
- Improvements
- Communications

了解你環境中的設備資產

恢復受損的能力或服務

制定適當的防護措施



實施適當的措施

制定並應用詳細的反應計劃

IDefender依據NIST CSF的實踐

綜合的資產識別方法

強大的資產管理能力

真正的OT漏洞/弱點管理

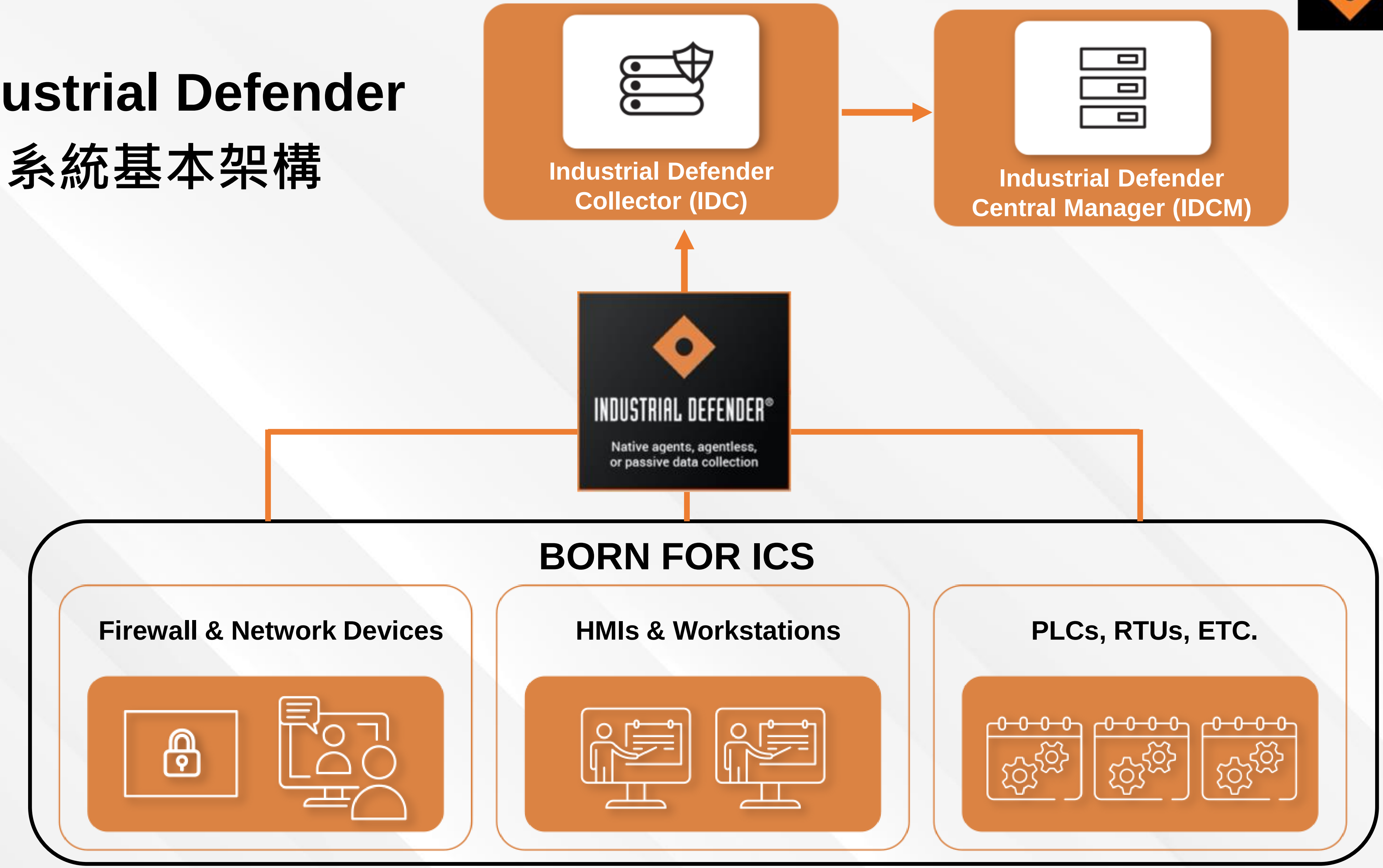
結合修補程式(Patch)
管理功能

能監視各種事件和變化

完整的事件回應支援

完善的與系統整合
及報告產出能力

Industrial Defender
系統基本架構



Industrial Defender Collector (IDC)

Industrial Defender Central Manager (IDCM)

INDUSTRIAL DEFENDER®

Native agents, agentless, or passive data collection

BORN FOR ICS

Firewall & Network Devices

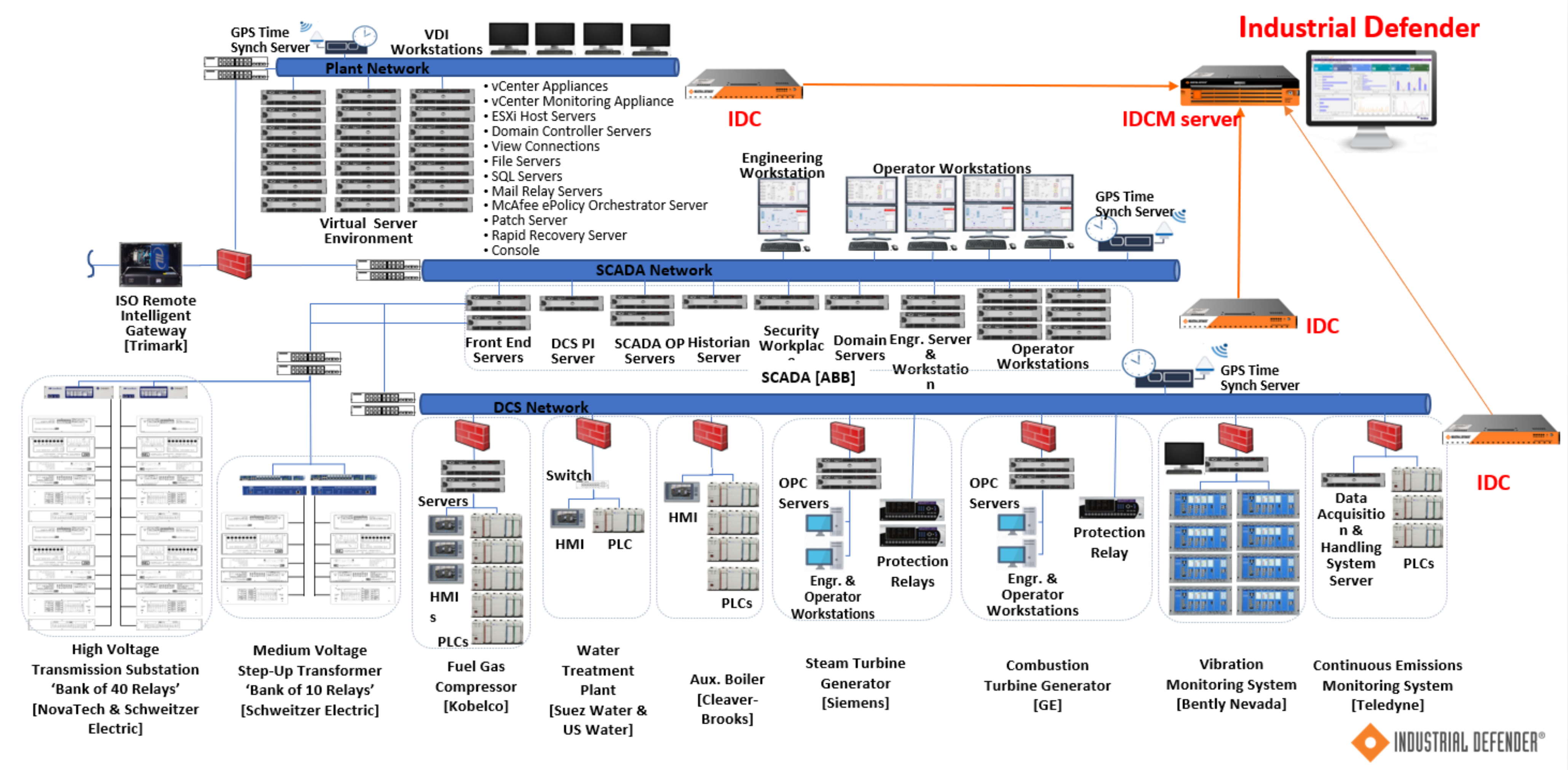
HMIs & Workstations

PLCs, RTUs, ETC.

Industrial Defender

實際應用架構範例

Powerplant with On Site Substation


GPS Time Synch Server
VDI Workstations
Plant Network
• vCenter Appliances
• vCenter Monitoring Appliance
• ESXi Host Servers
• Domain Controller Servers
• View Connections
• File Servers
• SQL Servers
• Mail Relay Servers
• McAfee ePolicy Orchestrator Server
• Patch Server
• Rapid Recovery Server
• Console
Virtual Server Environment
IDC
Industrial Defender
IDCM server
Engineering Workstation
Operator Workstations
GPS Time Synch Server
ISO Remote Intelligent Gateway [Trimark]
SCADA Network
Front End Servers
DCS PI Server
SCADA OP Servers
Historian Server
Security Workplac
Domain Servers
Engr. Server & Workstation
Operator Workstations
SCADA [ABB]
IDC
GPS Time Synch Server
DCS Network
Servers
HMIs
PLCs
Switch
HMI
PLC
HMI
PLCs
OPC Servers
Engr. & Operator Workstations
Protection Relays
OPC Servers
Engr. & Operator Workstations
Protection Relay
Data Acquisition & Handling System Server
PLCs
IDC
High Voltage Transmission Substation 'Bank of 40 Relays' [NovaTech & Schweitzer Electric]
Medium Voltage Step-Up Transformer 'Bank of 10 Relays' [Schweitzer Electric]
Fuel Gas Compressor [Kobelco]
Water Treatment Plant [Suez Water & US Water]
Aux. Boiler [Cleaver-Brooks]
Steam Turbine Generator [Siemens]
Combustion Turbine Generator [GE]
Vibration Monitoring System [Bently Nevada]
Continuous Emissions Monitoring System [Teledyne]
INDUSTRIAL DEFENDER

電力與石油、天然氣產業客戶群

NORTH AMERICAN ENERGY PROVIDERS

AMERICAN ELECTRIC POWER
Utility serves 5.5 million customers with electricity in 11 US states

Xcel Energy®
Gas & Electric Utility serves 3.5 million people in 8 US states

Exelon.
Gas & Electric Utility serves 10 million customers – active in 48 states

PSEG
Gas & Electric Utility serves the New York / New Jersey consumers

EDISON INTERNATIONAL®
Electric supply for over 15 million people in California

SaskPower Powering the future®
The electric supplier of the province of Saskatchewan, Canada

GRDA Grand River Dam Authority
Controls and maintains the Grand River waterway (Oklahoma) while producing electric power.

TALEN ENERGY
One of the largest competitive power generators in the USA with Fossil and Renewable sources

LA DWP Los Angeles Department of Water & Power
Los Angeles Department of Water and Power is the largest municipal utility in the US.

MULTINATIONAL RENEWABLE ENERGY COMPANIES

eDF renewables

AES we are the energy

engie

nationalgrid

LEADING SUPPLIERS OF ELECTRICITY AND NATURAL GAS IN EUROPE

SSE

RWE

NORTHERN POWERGRID

UK Power Networks

Skagerak Energi

eso

ESB

electric Ireland

LEADING SUPPLIERS OF ELECTRICITY IN AUSTRALIA

CITIPOWER

Powercor AUSTRALIA

TransGrid

EPSA Una empresa CELSIA
South American supplier of electricity via hydropower, combined cycle, photovoltaic, solar.

חברת החשמל
The largest company generating and supplying electricity in Israel.

其他關鍵基礎設施產業客戶群

Oil, LNG & Natural Gas

قطرغاز QATARGAS
DOLPHIN ENERGY دولفين للطاقة

UAE & Qatar

Santos
We have the energy

Australia

RRP
Rotterdam-Rijn Pijpleiding
ROTTERDAM ANTWERPEN PIJPLEIDING RAPL
PERN „Przyjaźń" S.A.

Europe

SaskEnergy TransGas
Gibsons
GIBSON ENERGY
SOUTHWEST GAS
BGE
EVERSOURCE ENERGY
Piedmont Natural Gas
Xcel Energy®
PSEG

North America

Chemical Processing

Westlake Chemical

US

Chevron Phillips Chemical Company LP

Worldwide

S-Chem

Saudi Arabia

QAPCO

Qatar

Water Treatment + Buildings & Critical Infrastructure

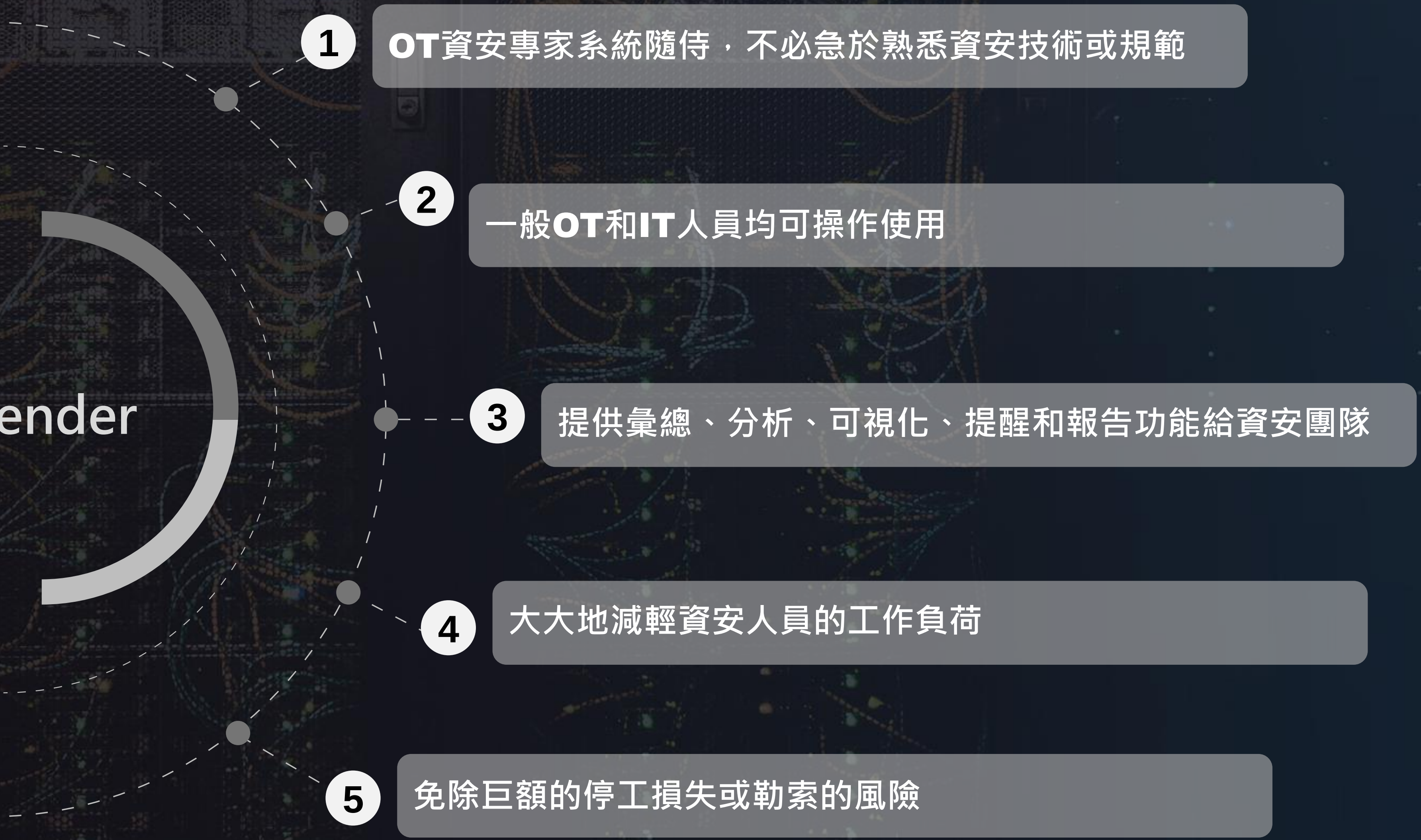
QUEENSLAND UrbanUtilities

Australia

HARVARD
Energy & Facilities

US Research & Educational University

採用 Industrial Defender 的效益



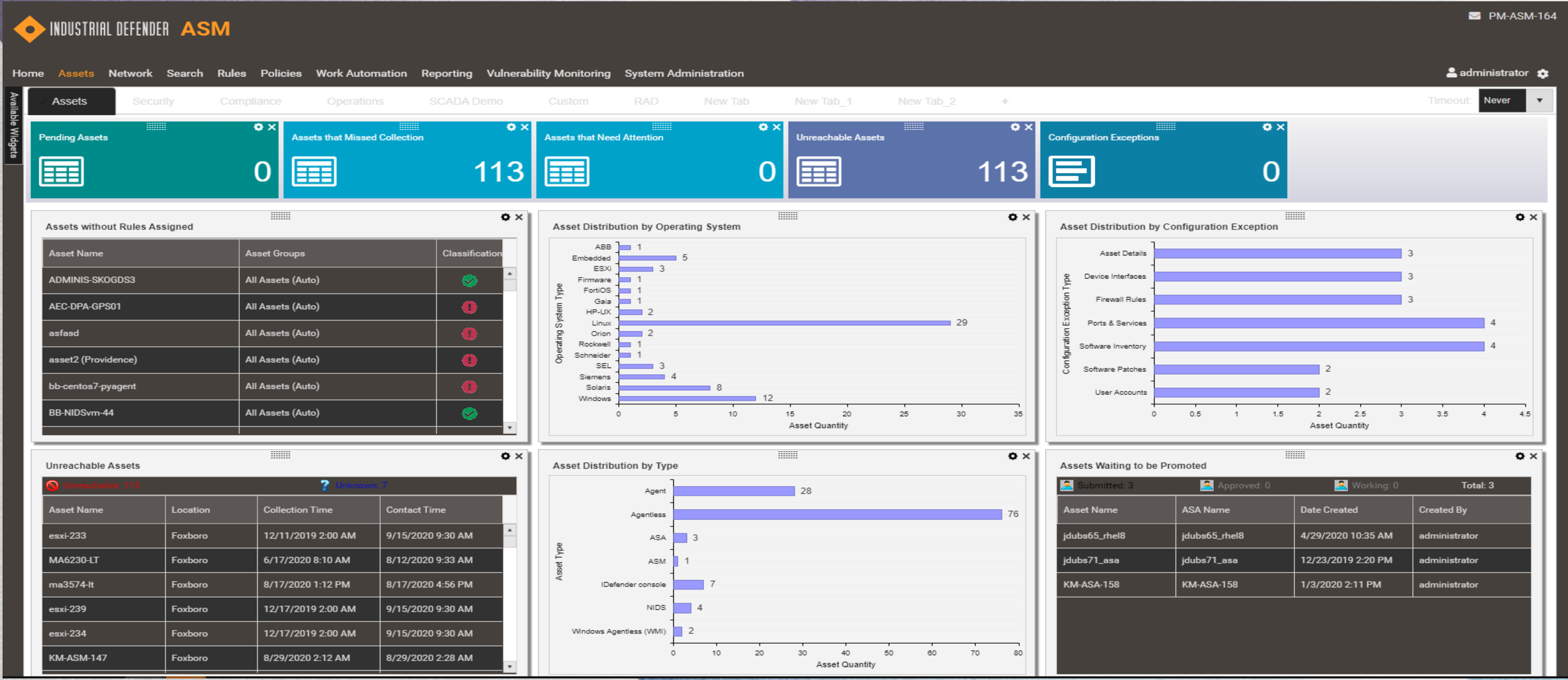
1. OT資安專家系統隨侍，不必急於熟悉資安技術或規範
2. 一般OT和IT人員均可操作使用
3. 提供彙總、分析、可視化、提醒和報告功能給資安團隊
4. 大大地減輕資安人員的工作負荷
5. 免除巨額的停工損失或勒索的風險

Industrial Defender具備功能

- 資產管理
- 安全事件管理
- 設定管理
- 弱點管理
- 政策管理
- 風險分析
- 網路分析
- 自動合規分析和報告
- 企業資訊整合

資產盤點

從多種資料收集方法（Agent、Agentless、Passive）得出的資產清單



Assets without Rules Assigned

Asset Name	Asset Groups	Classification
ADMINIS-SKOGDS3	All Assets (Auto)	✓
AEC-DPA-GPS01	All Assets (Auto)	!
asfasd	All Assets (Auto)	!
asset2 (Providence)	All Assets (Auto)	!
bb-centos7-pyagent	All Assets (Auto)	!
BB-NIDSvm-44	All Assets (Auto)	✓

Asset Distribution by Operating System

Asset Distribution by Configuration Exception

Unreachable Assets

Unreachable: 113 Unknown: 7

Asset Name	Location	Collection Time	Contact Time
esxi-233	Foxboro	12/11/2019 2:00 AM	9/15/2020 9:30 AM
MA6230-LT	Foxboro	6/17/2020 8:10 AM	8/12/2020 9:33 AM
ma3574-lt	Foxboro	8/17/2020 1:12 PM	8/17/2020 4:56 PM
esxi-239	Foxboro	12/17/2019 2:00 AM	9/15/2020 9:30 AM
esxi-234	Foxboro	12/17/2019 2:00 AM	9/15/2020 9:30 AM
KM-ASM-147	Foxboro	8/29/2020 2:12 AM	8/29/2020 2:28 AM

Asset Distribution by Type

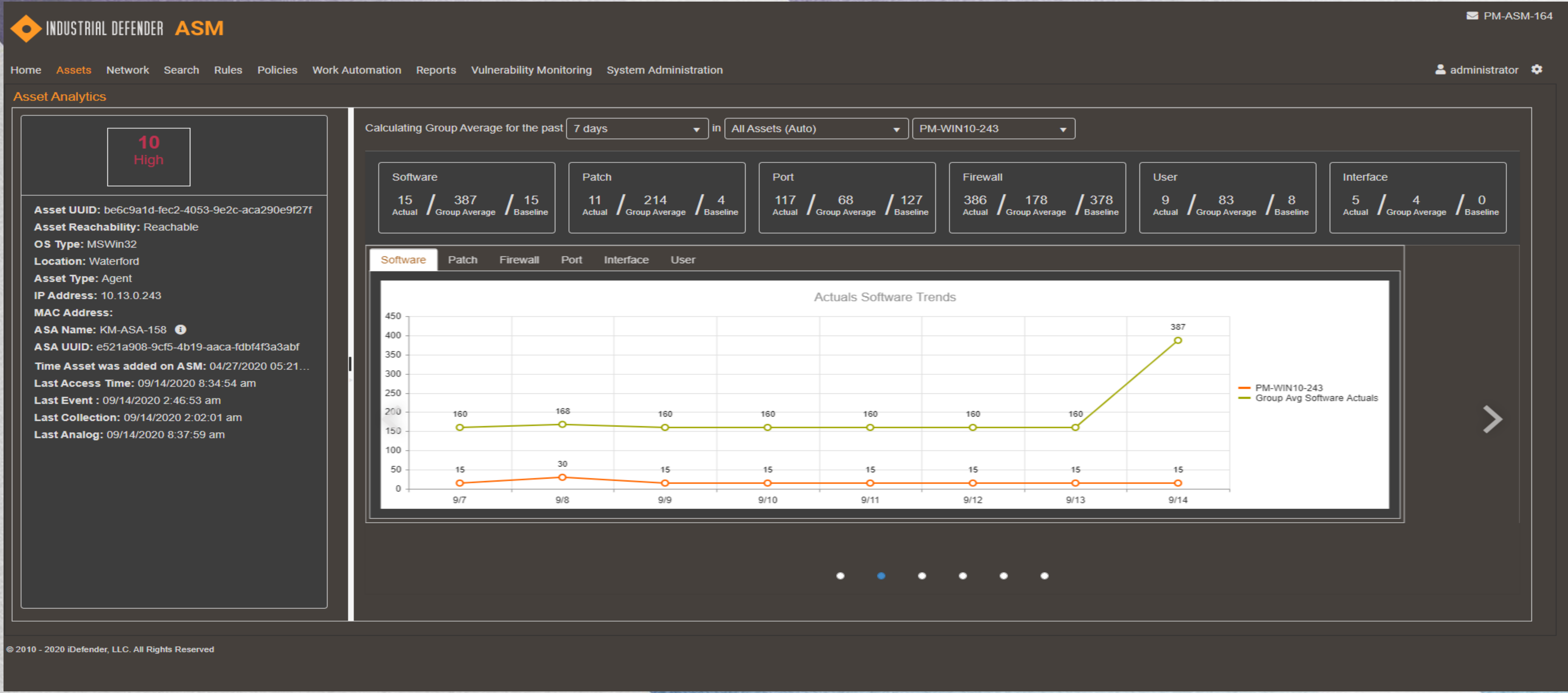
Assets Waiting to be Promoted

Submitted: 3 Approved: 0 Working: 0 Total: 3

Asset Name	ASA Name	Date Created	Created By
jdubs65_rhel8	jdubs65_rhel8	4/29/2020 10:35 AM	administrator
jdubs71_asa	jdubs71_asa	12/23/2019 2:20 PM	administrator
KM-ASA-158	KM-ASA-158	1/3/2020 2:11 PM	administrator

資產趨勢

詳細了解您的資產如何隨時間變化



INDUSTRIAL DEFENDER ASM

✉ PM-ASM-164

Home Assets Network Search Rules Policies Work Automation Reports Vulnerability Monitoring System Administration

administrator

Asset Analytics

10
High

Asset UUID: be6c9a1d-fec2-4053-9e2c-aca290e9f27f
Asset Reachability: Reachable
OS Type: MSWin32
Location: Waterford
Asset Type: Agent
IP Address: 10.13.0.243
MAC Address:
ASA Name: KM-ASA-158
ASA UUID: e521a908-9cf5-4b19-aaca-fdbf4f3a3abf
Time Asset was added on ASM: 04/27/2020 05:21...
Last Access Time: 09/14/2020 8:34:54 am
Last Event : 09/14/2020 2:46:53 am
Last Collection: 09/14/2020 2:02:01 am
Last Analog: 09/14/2020 8:37:59 am

Calculating Group Average for the past 7 days in All Assets (Auto) PM-WIN10-243

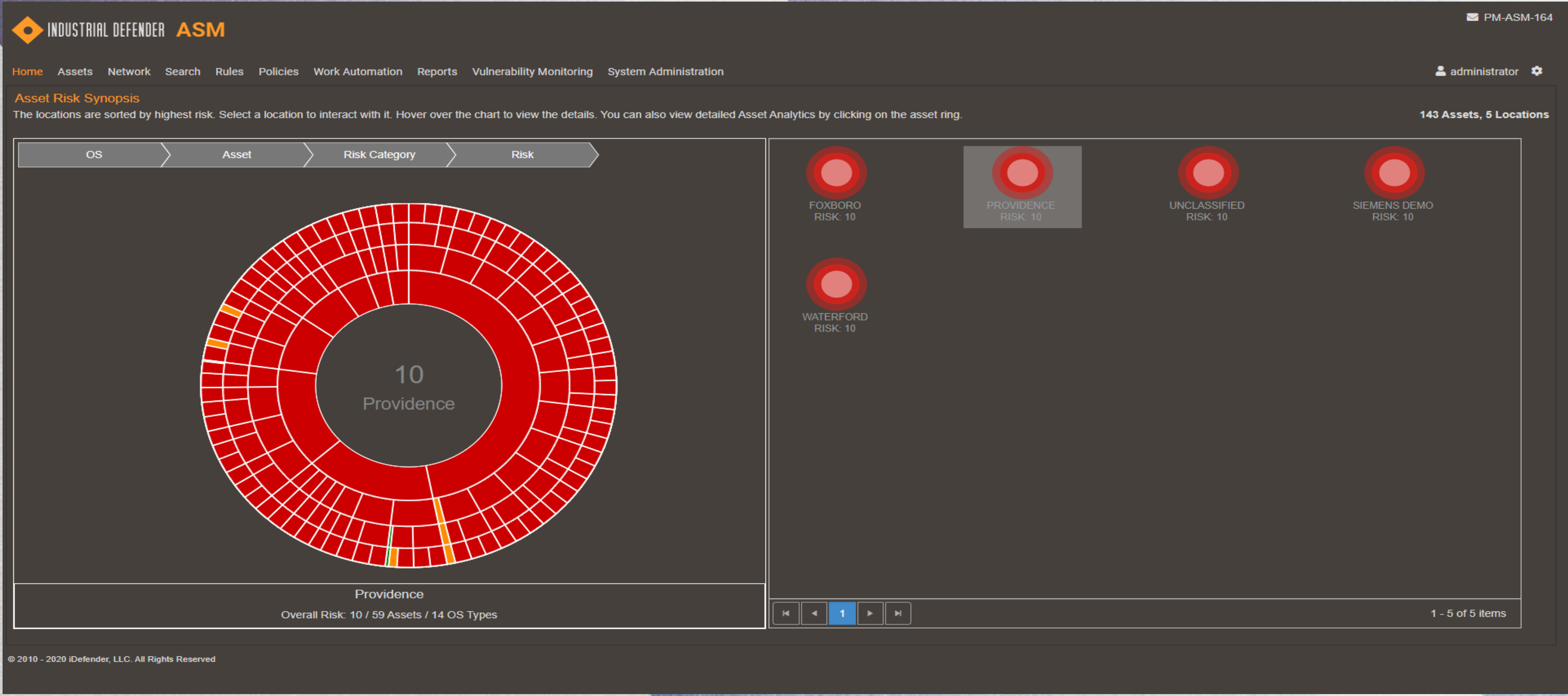
	Actual	Group Average	Baseline
Software	15	387	15
Patch	11	214	4
Port	117	68	127
Firewall	386	178	378
User	9	83	8
Interface	5	4	0

Software Patch Firewall Port Interface User

© 2010 - 2020 iDefender, LLC. All Rights Reserved

風險分析

以種類區分的儀表板可突顯出資產的風險



Asset Risk Synopsis

The locations are sorted by highest risk. Select a location to interact with it. Hover over the chart to view the details. You can also view detailed Asset Analytics by clicking on the asset ring.

143 Assets, 5 Locations

Providence

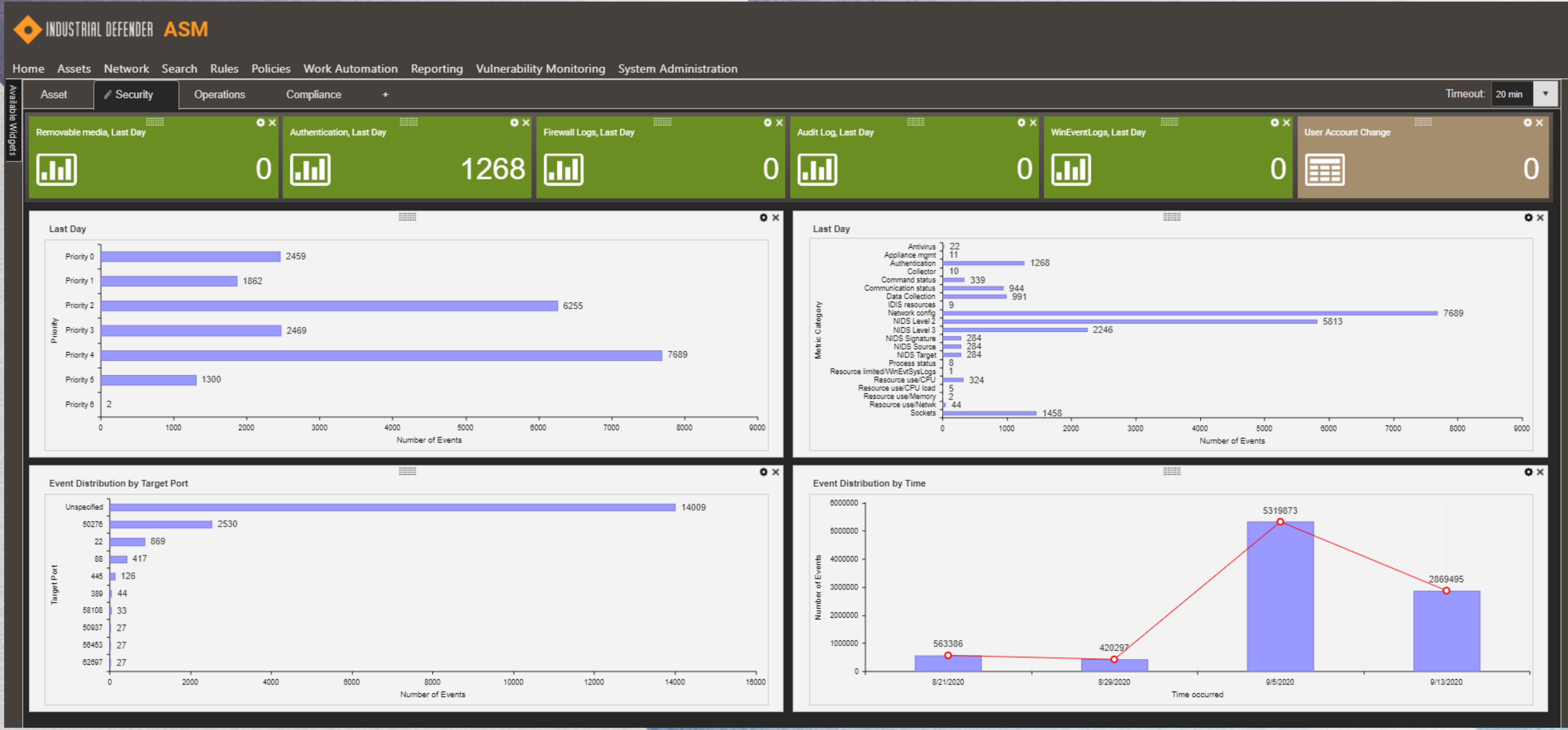
Overall Risk: 10 / 59 Assets / 14 OS Types

1 - 5 of 5 items

© 2010 - 2020 iDefender, LLC. All Rights Reserved

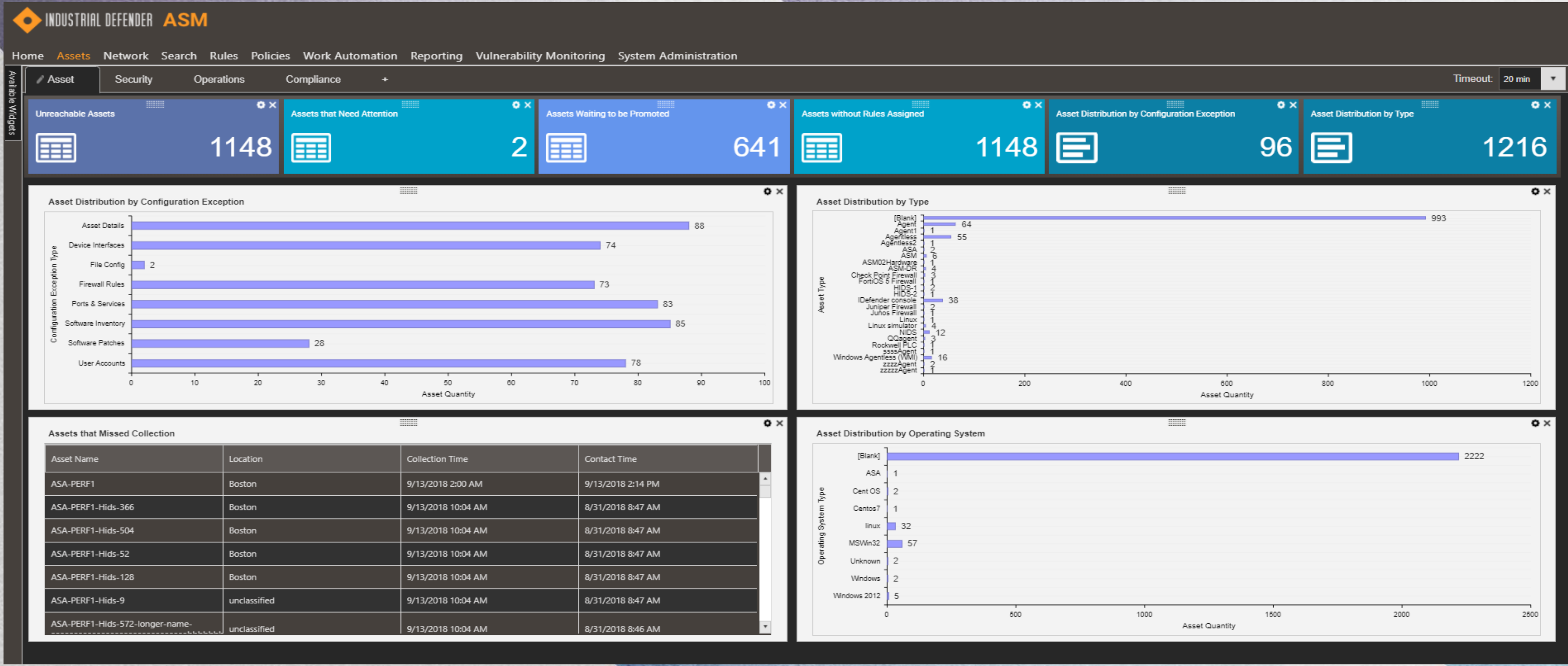
安全事件管理

來自工業控制系統的有用事件資訊



設定管理

監視和管理 OT 端點設定變更



Unreachable Assets 1148

Assets that Need Attention 2

Assets Waiting to be Promoted 641

Assets without Rules Assigned 1148

Asset Distribution by Configuration Exception 96

Asset Distribution by Type 1216

Asset Distribution by Configuration Exception

Asset Distribution by Type

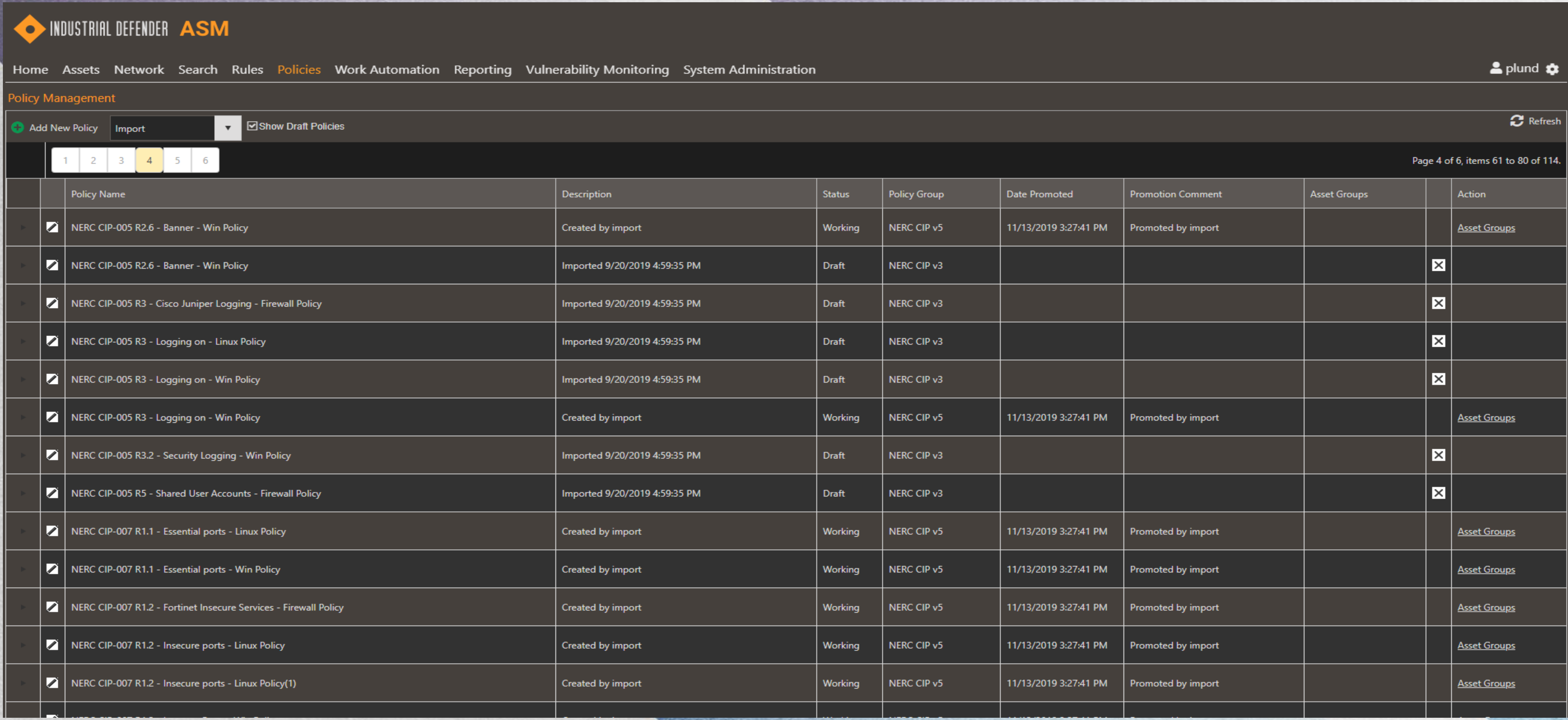
Assets that Missed Collection

Asset Name	Location	Collection Time	Contact Time
ASA-PERF1	Boston	9/13/2018 2:00 AM	9/13/2018 2:14 PM
ASA-PERF1-Hids-366	Boston	9/13/2018 10:04 AM	8/31/2018 8:47 AM
ASA-PERF1-Hids-504	Boston	9/13/2018 10:04 AM	8/31/2018 8:47 AM
ASA-PERF1-Hids-52	Boston	9/13/2018 10:04 AM	8/31/2018 8:47 AM
ASA-PERF1-Hids-128	Boston	9/13/2018 10:04 AM	8/31/2018 8:47 AM
ASA-PERF1-Hids-9	unclassified	9/13/2018 10:04 AM	8/31/2018 8:47 AM
ASA-PERF1-Hids-572-longer-name-	unclassified	9/13/2018 10:04 AM	8/31/2018 8:46 AM

Asset Distribution by Operating System

資安政策管理

輕鬆建立、設定和審核政策



Policy Management

☑ Show Draft Policies

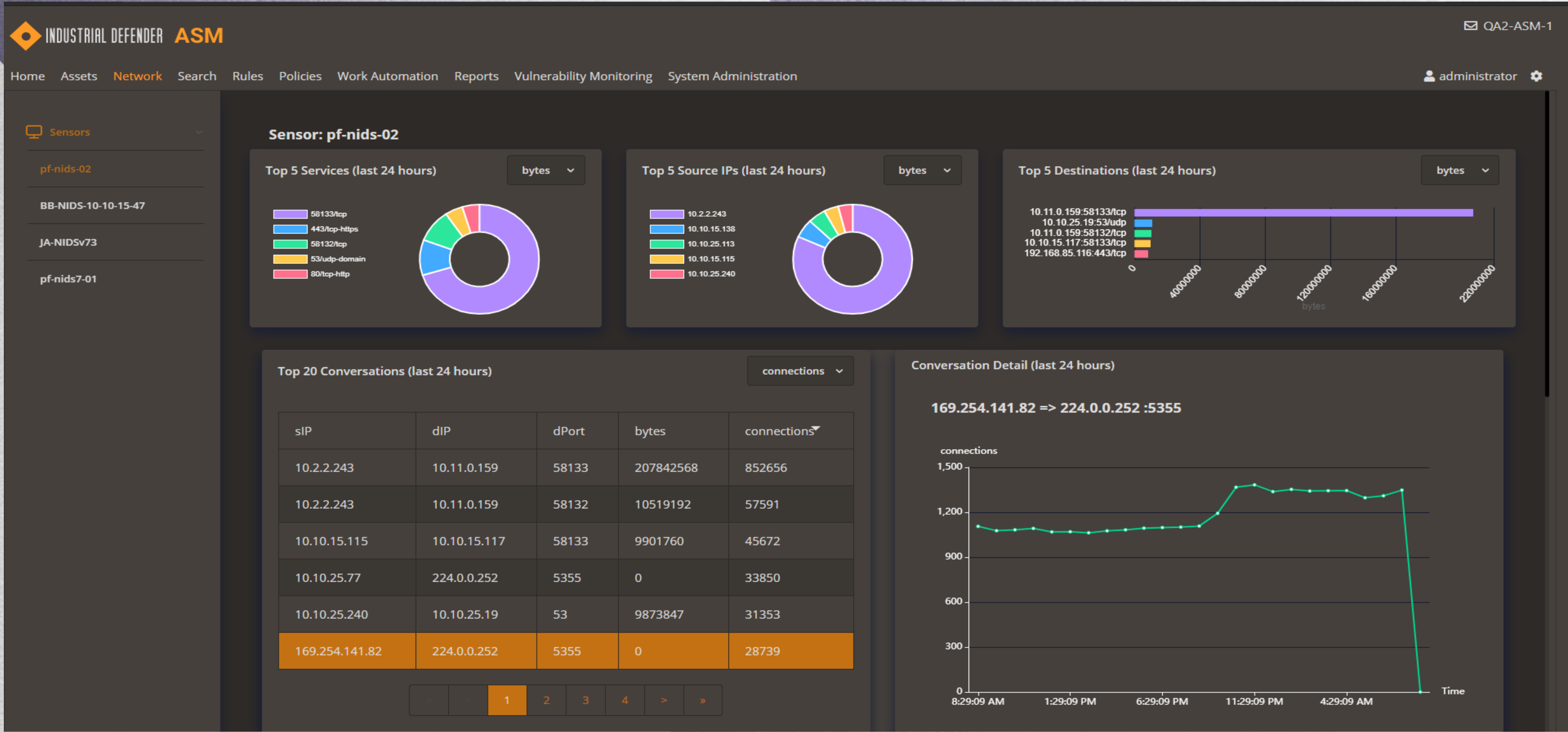
Page 4 of 6, items 61 to 80 of 114.

Policy Name	Description	Status	Policy Group	Date Promoted	Promotion Comment	Asset Groups		Action
NERC CIP-005 R2.6 - Banner - Win Policy	Created by import	Working	NERC CIP v5	11/13/2019 3:27:41 PM	Promoted by import			Asset Groups
NERC CIP-005 R2.6 - Banner - Win Policy	Imported 9/20/2019 4:59:35 PM	Draft	NERC CIP v3				☒	
NERC CIP-005 R3 - Cisco Juniper Logging - Firewall Policy	Imported 9/20/2019 4:59:35 PM	Draft	NERC CIP v3				☒	
NERC CIP-005 R3 - Logging on - Linux Policy	Imported 9/20/2019 4:59:35 PM	Draft	NERC CIP v3				☒	
NERC CIP-005 R3 - Logging on - Win Policy	Imported 9/20/2019 4:59:35 PM	Draft	NERC CIP v3				☒	
NERC CIP-005 R3 - Logging on - Win Policy	Created by import	Working	NERC CIP v5	11/13/2019 3:27:41 PM	Promoted by import			Asset Groups
NERC CIP-005 R3.2 - Security Logging - Win Policy	Imported 9/20/2019 4:59:35 PM	Draft	NERC CIP v3				☒	
NERC CIP-005 R5 - Shared User Accounts - Firewall Policy	Imported 9/20/2019 4:59:35 PM	Draft	NERC CIP v3				☒	
NERC CIP-007 R1.1 - Essential ports - Linux Policy	Created by import	Working	NERC CIP v5	11/13/2019 3:27:41 PM	Promoted by import			Asset Groups
NERC CIP-007 R1.1 - Essential ports - Win Policy	Created by import	Working	NERC CIP v5	11/13/2019 3:27:41 PM	Promoted by import			Asset Groups
NERC CIP-007 R1.2 - Fortinet Insecure Services - Firewall Policy	Created by import	Working	NERC CIP v5	11/13/2019 3:27:41 PM	Promoted by import			Asset Groups
NERC CIP-007 R1.2 - Insecure ports - Linux Policy	Created by import	Working	NERC CIP v5	11/13/2019 3:27:41 PM	Promoted by import			Asset Groups
NERC CIP-007 R1.2 - Insecure ports - Linux Policy(1)	Created by import	Working	NERC CIP v5	11/13/2019 3:27:41 PM	Promoted by import			Asset Groups

INDUSTRIAL DEFENDER®

網路流量分析

視覺化網路監視資料



Sensor: pf-nids-02

Top 5 Services (last 24 hours)

Top 5 Source IPs (last 24 hours)

Top 5 Destinations (last 24 hours)

Top 20 Conversations (last 24 hours)

sIP	dIP	dPort	bytes	connections
10.2.2.243	10.11.0.159	58133	207842568	852656
10.2.2.243	10.11.0.159	58132	10519192	57591
10.10.15.115	10.10.15.117	58133	9901760	45672
10.10.25.77	224.0.0.252	5355	0	33850
10.10.25.240	10.10.25.19	53	9873847	31353
169.254.141.82	224.0.0.252	5355	0	28739

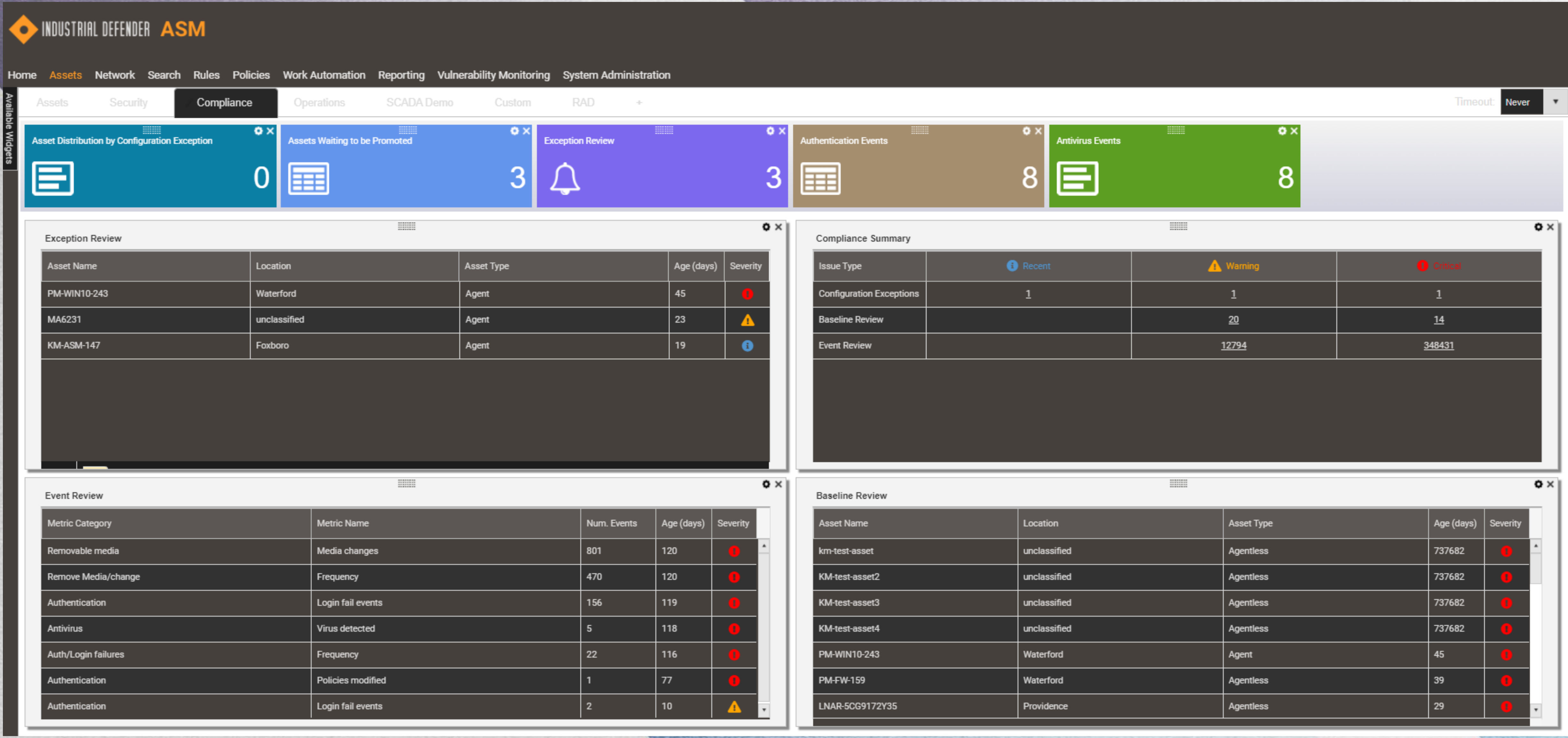
Conversation Detail (last 24 hours)

169.254.141.82 => 224.0.0.252 :5355

研杰科技 YOUNGTEC

合於資安規範的儀表板

合於資安規範的即時可見性



Asset Distribution by Configuration Exception 0

Assets Waiting to be Promoted 3

Exception Review 3

Authentication Events 8

Antivirus Events 8

Exception Review

Asset Name	Location	Asset Type	Age (days)	Severity
PM-WIN10-243	Waterford	Agent	45	❗
MA6231	unclassified	Agent	23	⚠
KM-ASM-147	Foxboro	Agent	19	ℹ

Compliance Summary

Issue Type	ℹ Recent	⚠ Warning	❗ Critical
Configuration Exceptions	1	1	1
Baseline Review		20	14
Event Review		12794	348431

Event Review

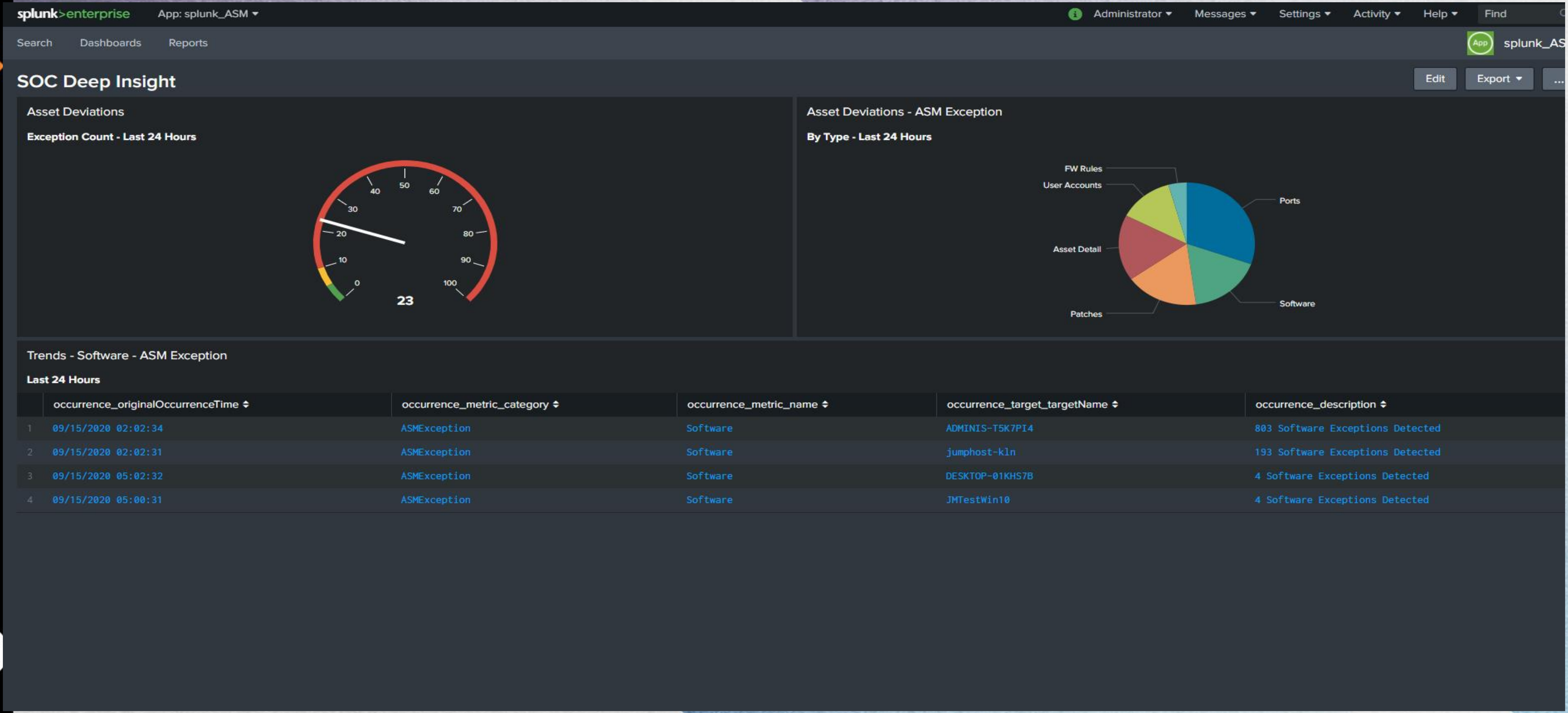
Metric Category	Metric Name	Num. Events	Age (days)	Severity
Removable media	Media changes	801	120	❗
Remove Media/change	Frequency	470	120	❗
Authentication	Login fail events	156	119	❗
Antivirus	Virus detected	5	118	❗
Auth/Login failures	Frequency	22	116	❗
Authentication	Policies modified	1	77	❗
Authentication	Login fail events	2	10	⚠

Baseline Review

Asset Name	Location	Asset Type	Age (days)	Severity
km-test-asset	unclassified	Agentless	737682	❗
KM-test-asset2	unclassified	Agentless	737682	❗
KM-test-asset3	unclassified	Agentless	737682	❗
KM-test-asset4	unclassified	Agentless	737682	❗
PM-WIN10-243	Waterford	Agent	45	❗
PM-FW-159	Waterford	Agentless	39	❗
LNAR-5CG9172Y35	Providence	Agentless	29	❗

API-Enabled整合

將資料輸入到企業資訊系統和資安管理自動化系統中



SOC Deep Insight

Asset Deviations

Exception Count - Last 24 Hours

Asset Deviations - ASM Exception

By Type - Last 24 Hours

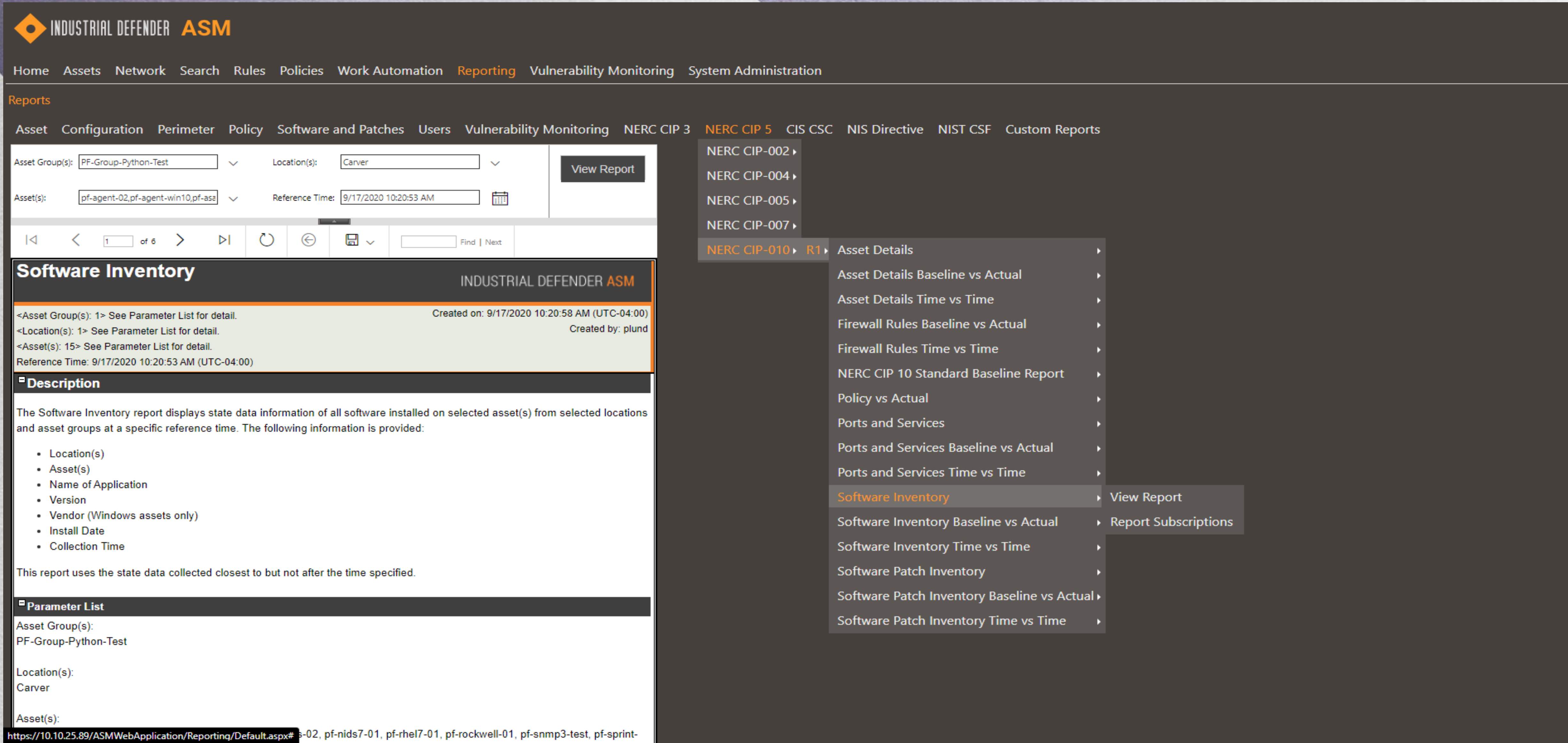
Trends - Software - ASM Exception

Last 24 Hours

	occurrence_originalOccurrenceTime ⬍	occurrence_metric_category ⬍	occurrence_metric_name ⬍	occurrence_target_targetName ⬍	occurrence_description ⬍
1	09/15/2020 02:02:34	ASMException	Software	ADMINIS-T5K7PI4	803 Software Exceptions Detected
2	09/15/2020 02:02:31	ASMException	Software	jumphost-kln	193 Software Exceptions Detected
3	09/15/2020 05:02:32	ASMException	Software	DESKTOP-01KHS7B	4 Software Exceptions Detected
4	09/15/2020 05:00:31	ASMException	Software	JMTestWin10	4 Software Exceptions Detected

強大的報表模組

開箱即用的內建標準和客製化報表



Asset Group(s): PF-Group-Python-Test

Location(s): Carver

Asset(s): pf-agent-02,pf-agent-win10,pf-asa

Reference Time: 9/17/2020 10:20:53 AM

Software Inventory

<Asset Group(s): 1> See Parameter List for detail.
<Location(s): 1> See Parameter List for detail.
<Asset(s): 15> See Parameter List for detail.
Reference Time: 9/17/2020 10:20:53 AM (UTC-04:00)

Created on: 9/17/2020 10:20:58 AM (UTC-04:00)
Created by: plund

Description

The Software Inventory report displays state data information of all software installed on selected asset(s) from selected locations and asset groups at a specific reference time. The following information is provided:

- Location(s)
- Asset(s)
- Name of Application
- Version
- Vendor (Windows assets only)
- Install Date
- Collection Time

This report uses the state data collected closest to but not after the time specified.

Parameter List

Asset Group(s):
PF-Group-Python-Test

Location(s):
Carver

Asset(s):
https://10.10.25.89/ASMWebApplication/Reporting/Default.aspx# s-02, pf-nids7-01, pf-rhel7-01, pf-rockwell-01, pf-snmp3-test, pf-sprint-

感謝您的聆聽

研杰科技

-IoT & Industry 4.0 Software Solution Provider

張振忠

justin@youngtec.com.tw