

CYBERSEC 2021

臺灣資安大會

ORGANIZED BY **iThome**

TRUST:redefined

信任重構

M A Y 4 - 6 臺北南港展覽二館



當智慧製造遇上資安

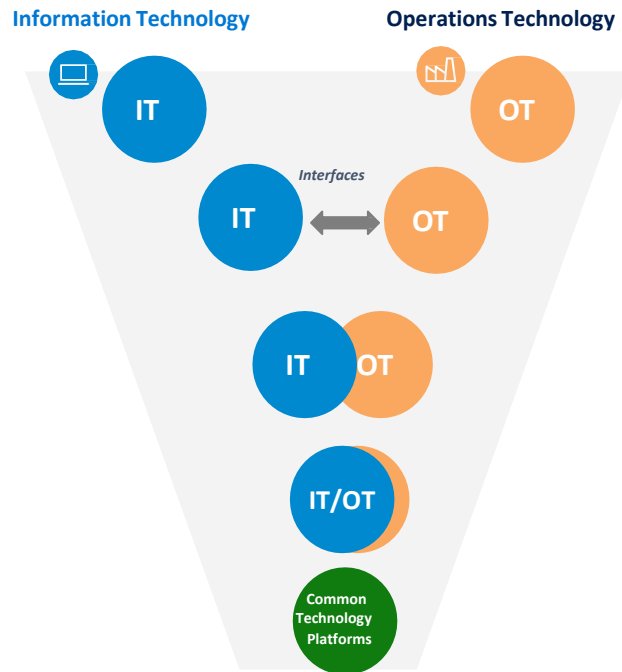
- OT/IT Security大哉問

葉怡君 Cathy Yeh
物聯網亞太創新中心 總經理
雲端暨人工智慧研發集團



當智慧製造遇上資安的常見問題

1. 不上雲就不會中毒了嗎？ OT 風險知多少？
2. 需要上Internet怎麼辦？
 - 需要支援平板手機嗎？
 - 客戶需要生產資料怎麼辦？
 - 設備廠商需要遠端維修怎麼辦？
 - 要出國設廠怎麼辦？
3. 生產資料放在雲端，會被Google到嗎？ 會不會被雲端業者拿去用？



Differences between IT & OT security



IT Security

Data confidentiality & privacy

Standard protocols & devices

High levels of connectivity

Multiple layers of controls & telemetry



OT Security

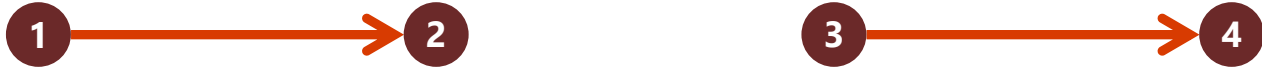
Safety & availability

Specialized protocols, devices & legacy OS platforms

Traditionally air-gapped, long patch cycle

Little or no visibility into IoT/OT risk

TRITON Attack on Safety Controllers in Petrochemical Facility

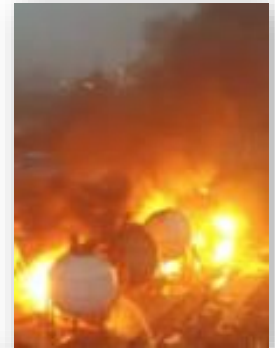
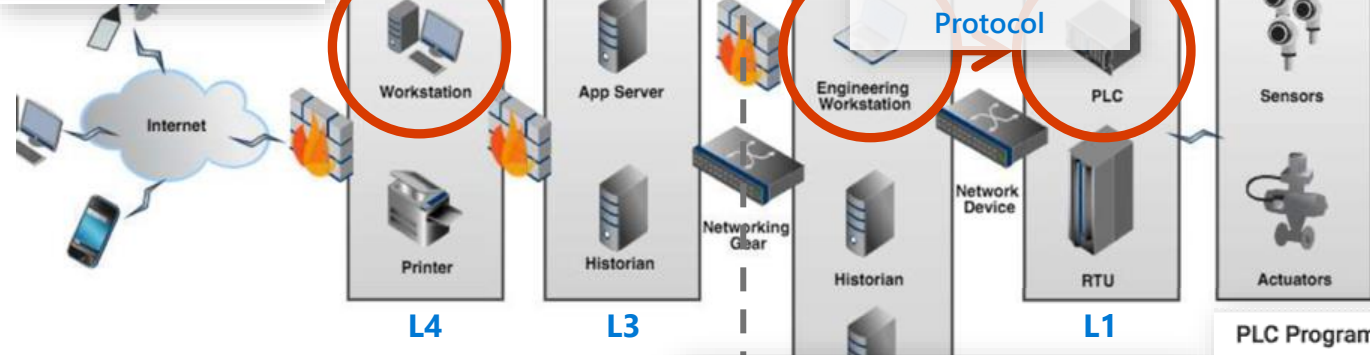


Alerts > Suspected credential theft activity

Suspected credential theft activity
This alert is part of incident (3136)

Actions ▾

Severity: Medium
Category: Credential Access
Technique: T1003: Credential Dumping, T1075: Pass the Hash
Detection source: EDR
Detection technology: Behavioral



Disable safety PLC —
Downtime (\$5M+)
+ Safety/environmental incident

Scan Device Detected
Apr 22, 2017 8:49:02 PM
Port Scan: Counted 23 distinct ports scanned from 10.2.1.26 to 10.2.1.25

PLC Program Update
Apr 22, 2017 8:53:17 PM
Program update detected, sent from 10.2.1.25 to 10.2.1.14

L4-L0: Purdue Model for Industrial Control Systems (ICS)

建構安全智慧製造系統五大支柱

5 pillars of OT/ICS Security Controls for manufacturers



Governance

OT-level security risk assessment.

Identity critical assets and security priorities.

Establish a security Program.

Align governance aspects of OA/OT.



Boundary Protection

Isolation between OT and IT environments.

“Hub and Spoke” networking model.

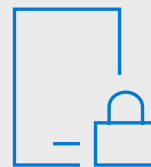


Identity

Provide a secure identity platform.

Protect privileged identities against compromise.

Ensure clean source path for management.



Security Configuration

Establish a strategic program for security configuration baselines.

Define update management process and tools.



Monitoring

Integrate OT security monitoring with SOC.

Use advanced threat protection technologies to rapid detection and response.

Establish response process and recovery procedures in partnership with IT and plant engineering.

Zero trust for IoT/OT



Verify explicitly.
Implement least privileged access.
Assume compromise.



Apply basic hygiene.
Patch where possible.
Implement MFA.
Train employees.

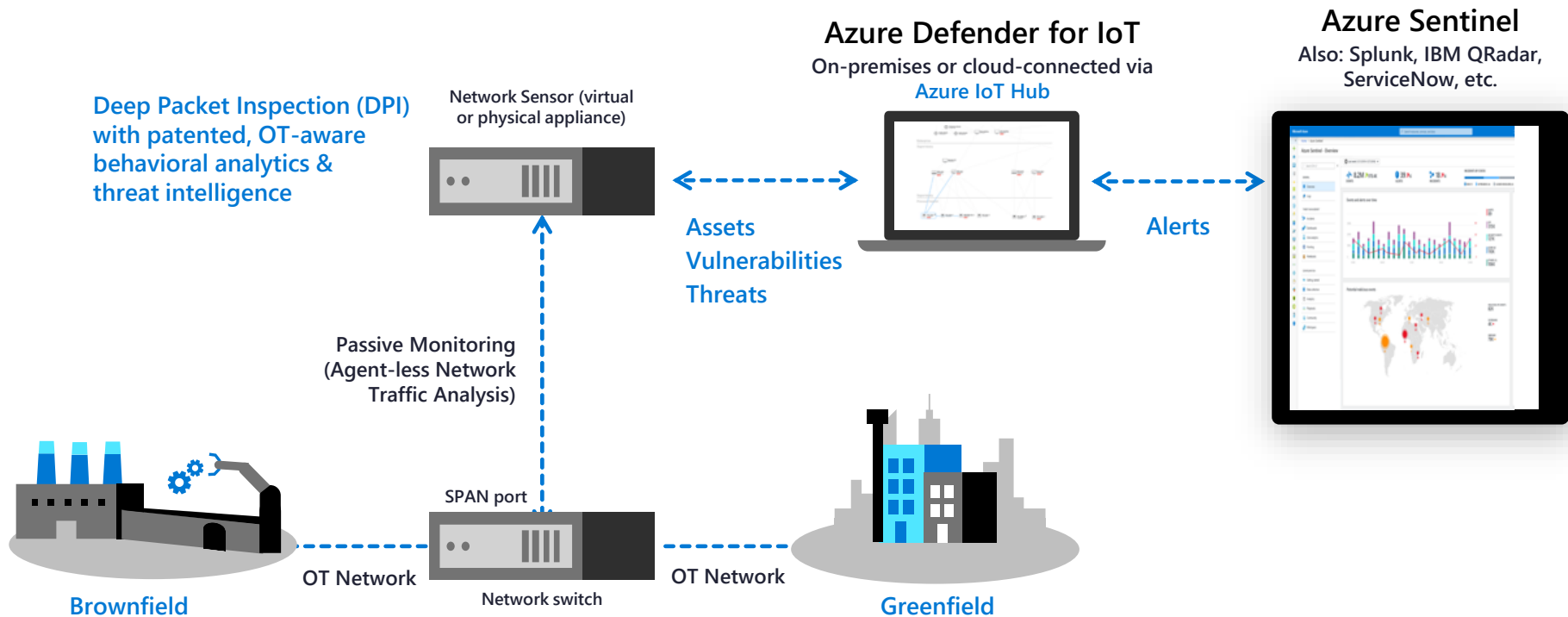


Implement continuous, active monitoring.
Detect unauthorized & compromised devices with behavioral anomaly detection.
Implement network segmentation with asset discovery & network mapping.



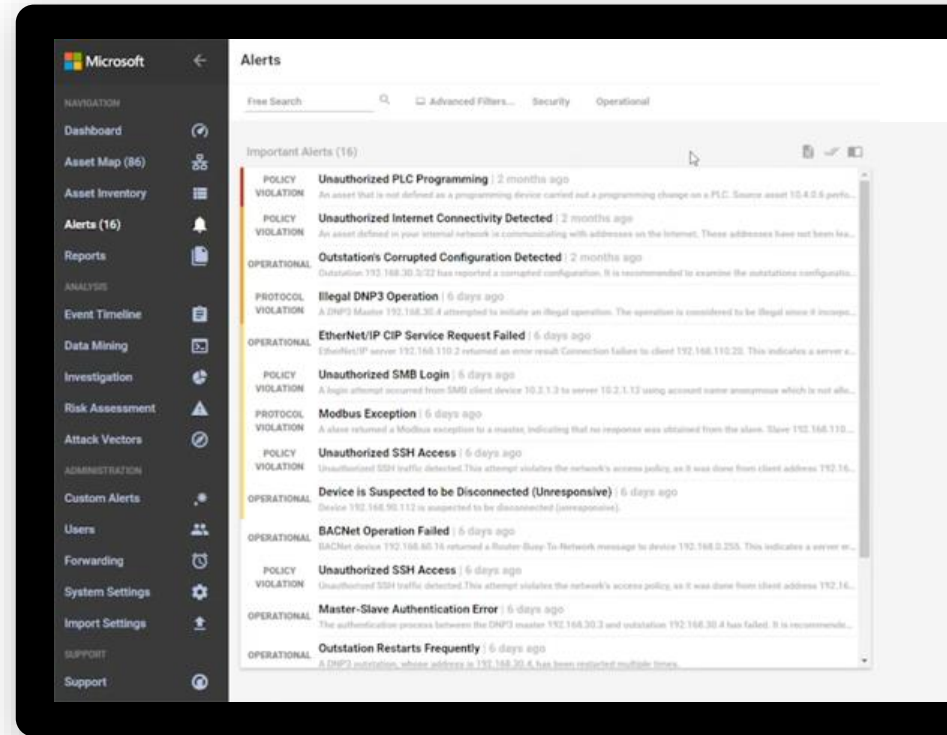
Unify IT & IoT/OT security monitoring in your SOC.
Speed up detection and response with AI and automation.

Rapid deployment with zero production impact



Real-time IoT/OT threat alerts (examples)

- Unauthorized device connected to the network
- Known malware detected (e.g., EternalBlue)
- Unauthorized connection to the internet
- Unauthorized remote access
- BACnet operation failed
- Network scanning operation detected
- Unauthorized PLC programming
- Changes to firmware versions
- “PLC Stop” and other potentially malicious commands
- Device is suspected of being disconnected
- Ethernet/IP CIP service request failure
- Illegal DNP3 operation
- Master-slave authentication error
- Unauthorized SMB login



Proven in the world's most complex IoT/OT environments



Top 3 global pharmaceutical

- Monitoring 50,000 OT devices in 65+ sites worldwide
- Diverse OT (Rockwell, Schneider, Siemens, GE, ABB, Yokogawa, ...)
- Centrally managed via 3 SOCs
- Integrated with Splunk, QRadar, ServiceNow CMDB & ticketing



\$3B auto parts manufacturer

- Monitoring 35,000 OT devices
- Deployed in 1 week in multiple plants across several continents
- Immediately detected WannaCry
- Integrated with Splunk



Top 5 US energy utility

- Monitoring 35,000 OT devices in multiple generation sites (electrical, LNG, renewable energy)
- CISO: "In the past, if equipment went down, we had no idea if it was a security issue or equipment malfunction."
- OT: "Now we can also quickly diagnose operational issues."

您可以從四個維度思考 Top Manufacturing & Resources Use Cases

資訊及生產系統整合

Address the convergence
of IT/OT

- Protecting availability while addressing security threats and leveraging the power of IoT/IIoT

跨國跨區混和雲端架構

Infrastructure Control over
Multiple Regions

- Secure migration to cloud deployments across diverse and occasionally remote regions

賦能授權員工及合作夥伴

Secure Access While
Empowering Productivity

- Secure access and identity mgmt. across all systems while enabling workplace collaboration

符合國際及產業規範

Compliance

- Achieve compliance with GDPR and data classification of sensitive intellectual property

CYBERSEC 2021
臺灣資安大會

ORGANIZED BY
iThome

Thank you!

TRUST:
redefined

M A Y 4 - 6 臺 北 南 港 展 覽 二 館