CYBERSEC 2021
臺灣資安大會

ORGANIZED BY iThome

TRUST:redefined

信 任 重 構

MAY 4-6 臺北南港展覽二館

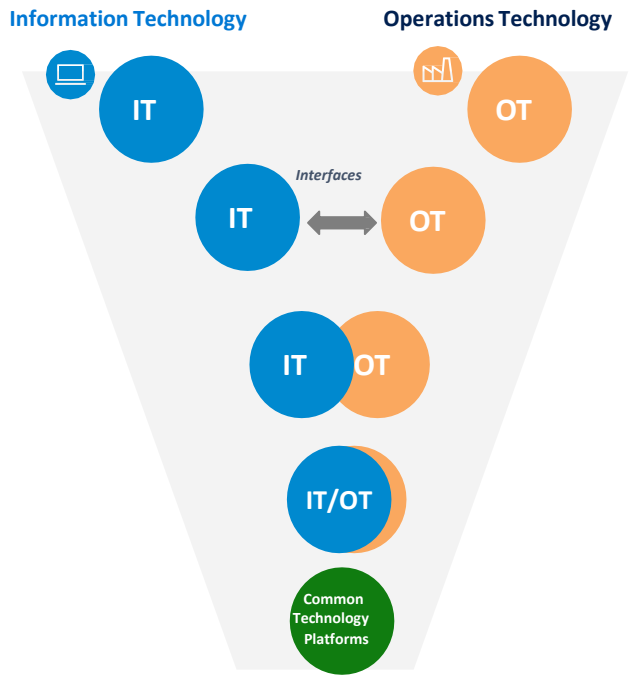
Microsoft

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

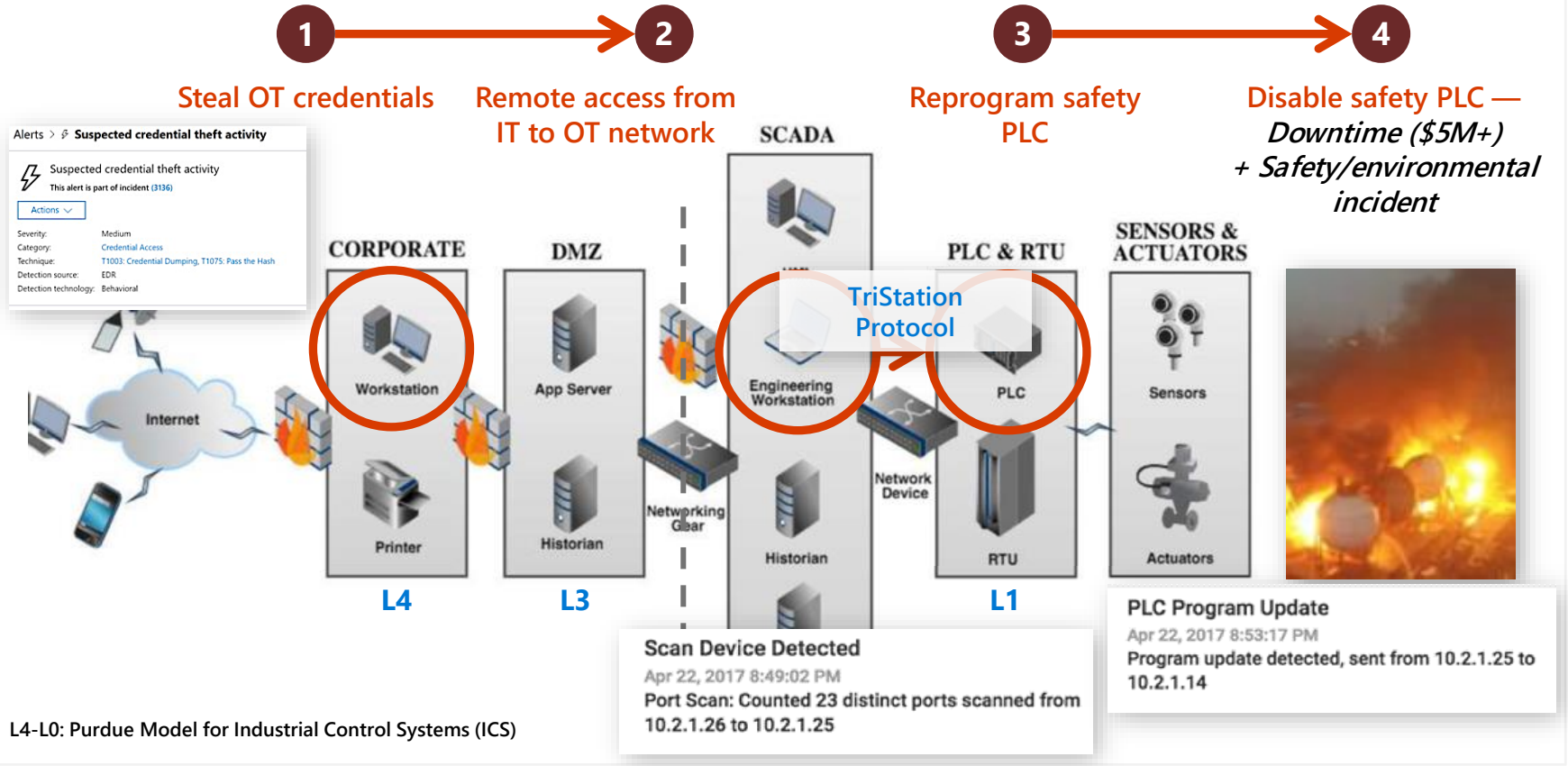
Safety & availability

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



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.

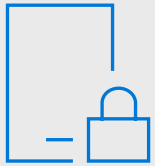
“Hub and Spoke” networking model.

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.

Microsoft

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.

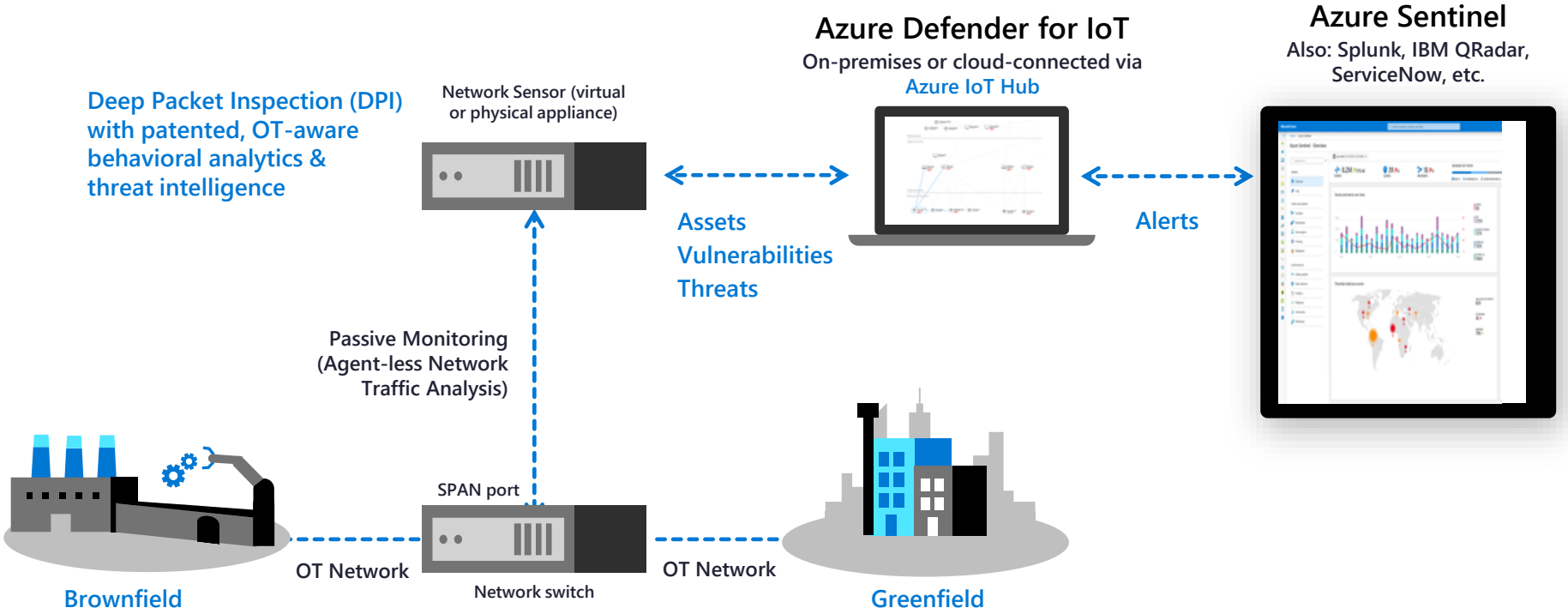
Detect unauthorized & compromised devices with behavioral anomaly detection.

Implement network segmentation with asset discovery & network mapping.

Unify IT & IoT/OT security monitoring in your SOC.

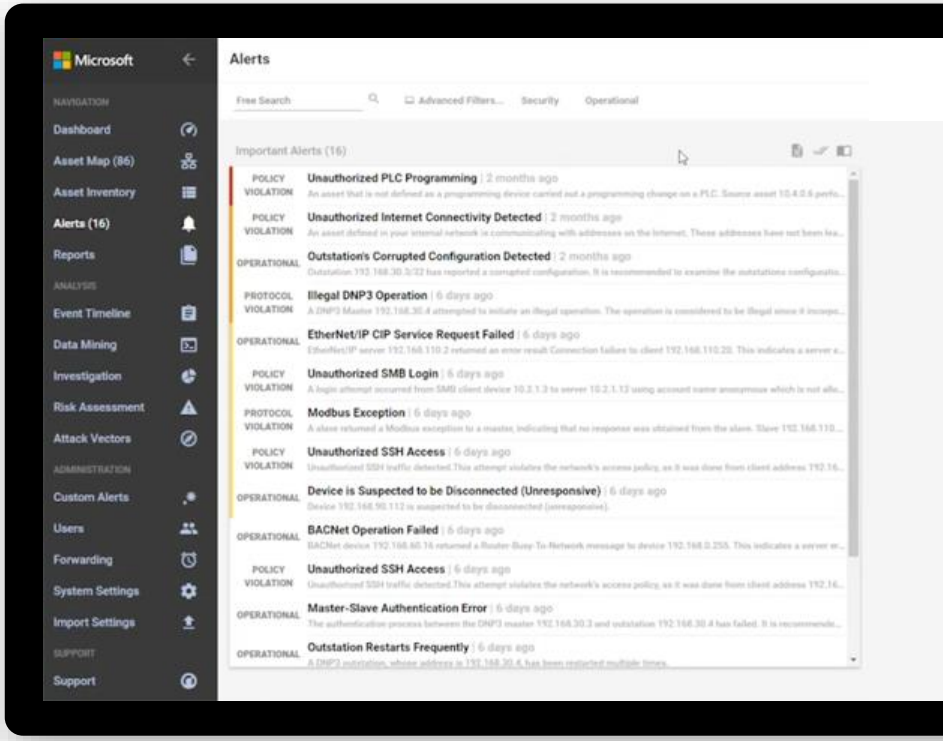
Speed up detection and response with AI and automation.

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

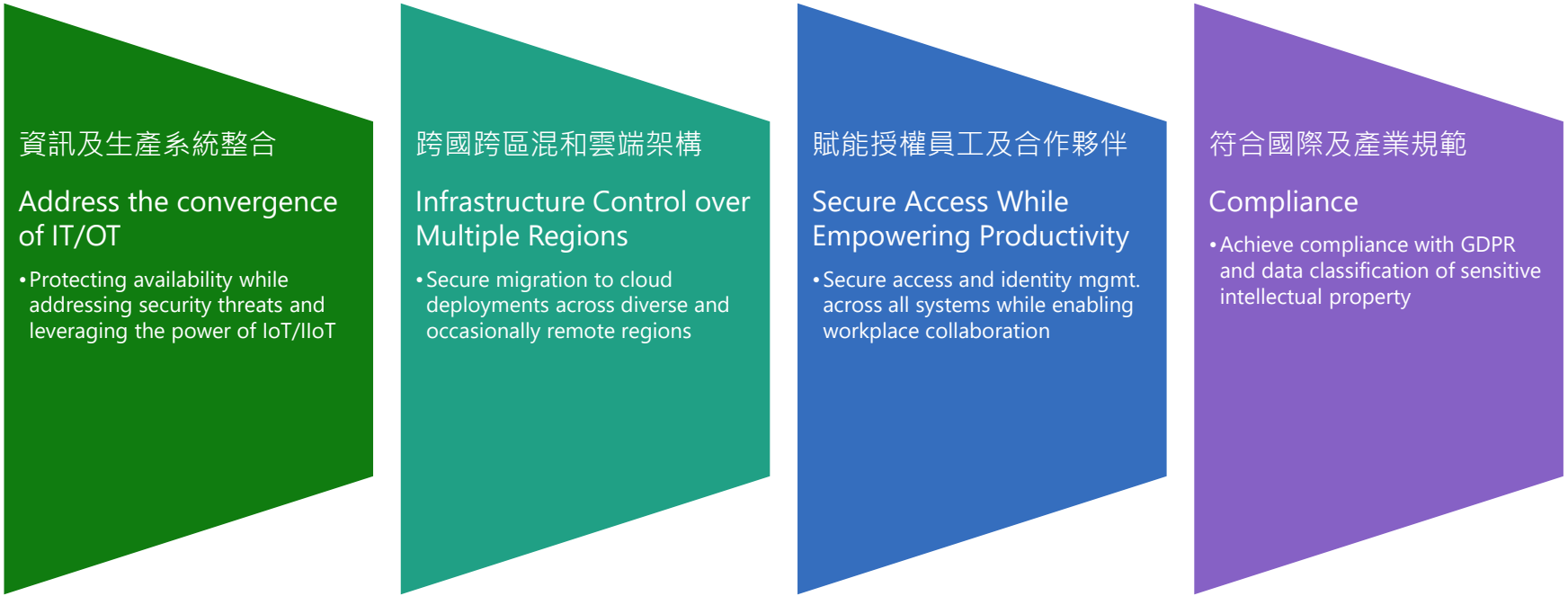
$3B auto parts manufacturer

- 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



TRUST:
redefined

Thank you!