Microsoft

Strengthen IoT/OT Zero Trust with Azure Defender for IoT: SecWise OT Detect

Koen Jacobs – SecWise

Nick Peeters- SecWise

Introduction SecWise

- Cyber Security & Information Protection consultancy & service
  - Identity & Access Management
  - Device Management
  - Threat Protection & Detection
  - Information & Data Protection
  - Managed Security Service (SecWise WATCH)
  - Azure IaaS / PaaS security
  - IoT/OT security
- Experts in Microsoft Cloud Security: act as a Trusted Advisor
- Part of The Cronos Group

SecWise

Context for Zero Trust

Our mission is to reduce the probability of material impact to our organization due to a cyber event.

A zero trust strategy assumes your network is already compromised and tries to limit material damage if it turns out to be true.

Global IoT/ICS Risk Report

Vulnerability data from 1,800+ industrial control system (ICS) networks

71%

Sites have outdated versions of Windows that no longer receive security patches

64%

Have unencrypted passwords facilitating compromise

66%

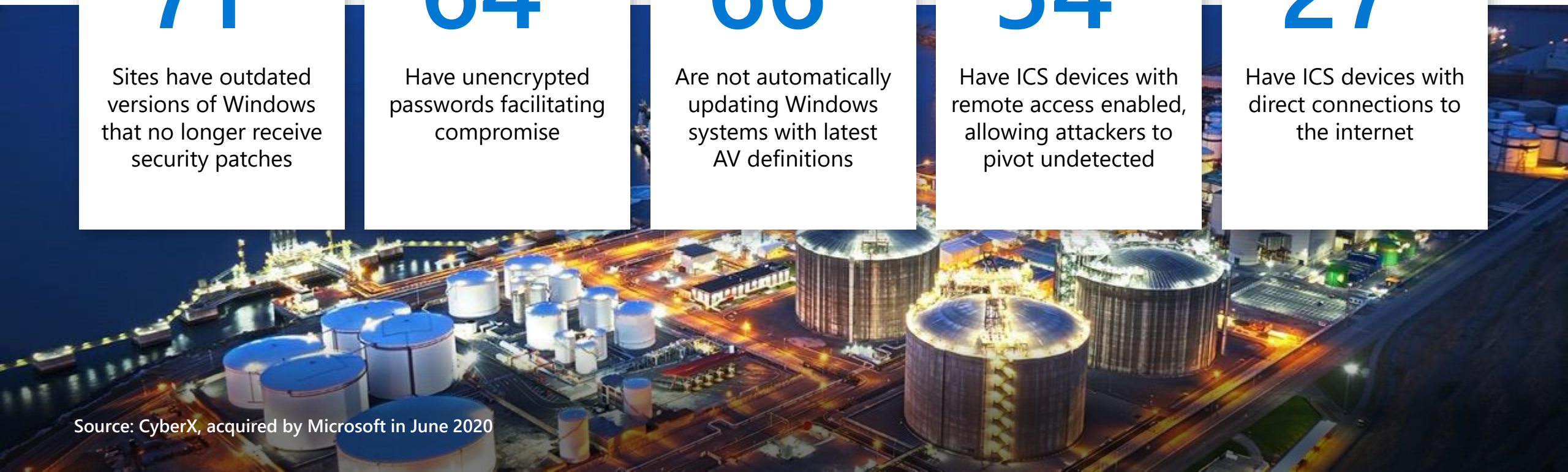
Are not automatically updating Windows systems with latest AV definitions

54%

Have ICS devices with remote access enabled, allowing attackers to pivot undetected

27%

Have ICS devices with direct connections to the internet



Source: CyberX, acquired by Microsoft in June 2020

IoT/OT risk = business risk

Financial

Destructive malware shuts down factories worldwide, causing billion of dollars in losses (WannaCry, NotPetya, LockerGoga, Ekans, …).

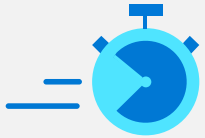
IP Theft

Manufacturers are 8x more likely to be attacked for theft of IP like proprietary formulas and designs than other verticals (DBIR).

Safety

Attacks on electric grid, water utilities, petrochemical facility, gas compression facility, blast furnaces, maritime ports, building automation systems, …

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 monitoring.

Detect unauthorized & compromised devices with behavioral anomaly detection.

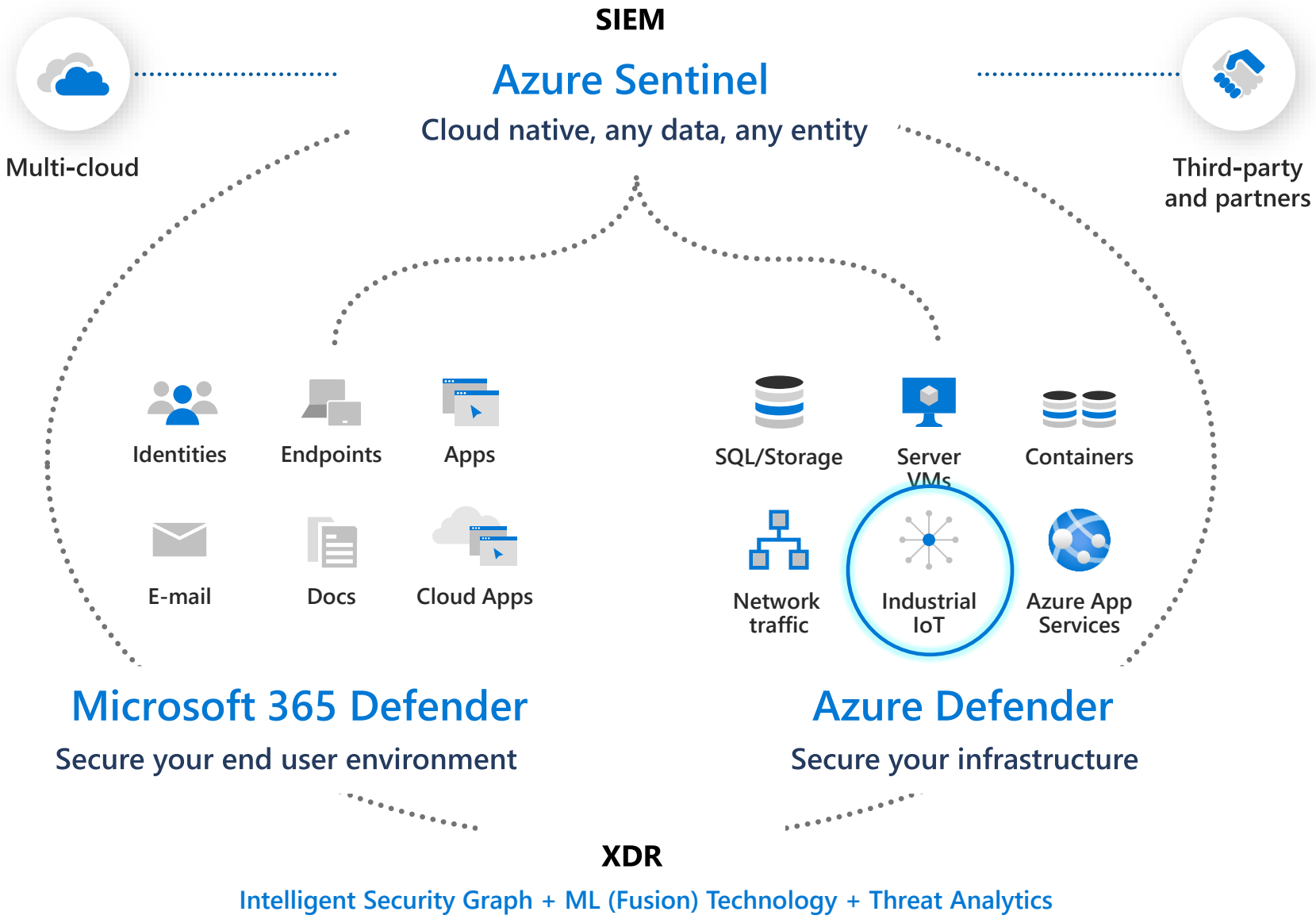
Implement network segmentation with asset discovery & network mapping.

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

Speed up detection and response with AI and automation.

Create a company-wide culture of OT/ICS security

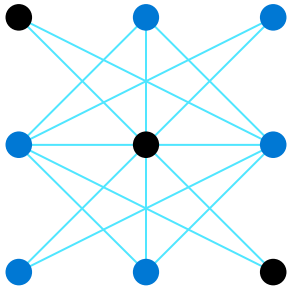
Stay ahead of attackers with a unified SecOps experience



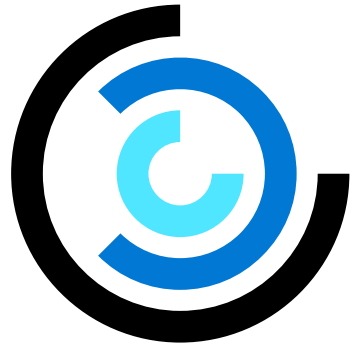
Azure Defender for IoT

Agentless security for Industrial IoT (IIoT) & Operational Technology (OT) devices

Agentless security.
Zero production impact.
Deployed in <1 day

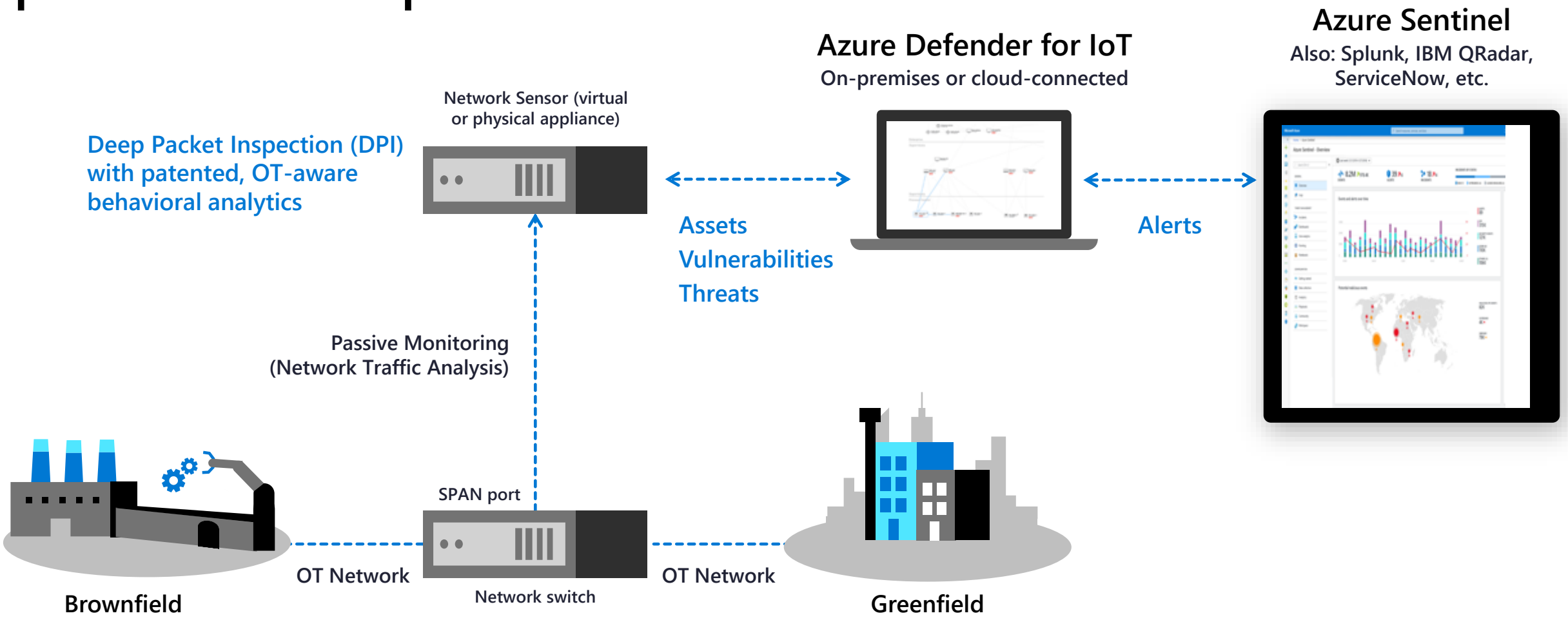


Continuous visibility into assets, cyber risk and operational issues — across legacy & proprietary IoT/OT devices



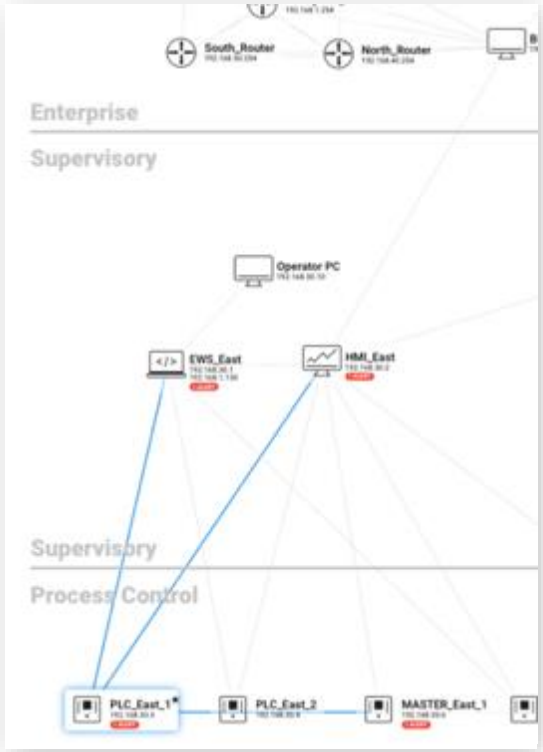
Integration with Azure Sentinel & other SOC tools for unified IT/OT governance

SecWise OT Detect: Rapid agentless deployment with zero performance impact

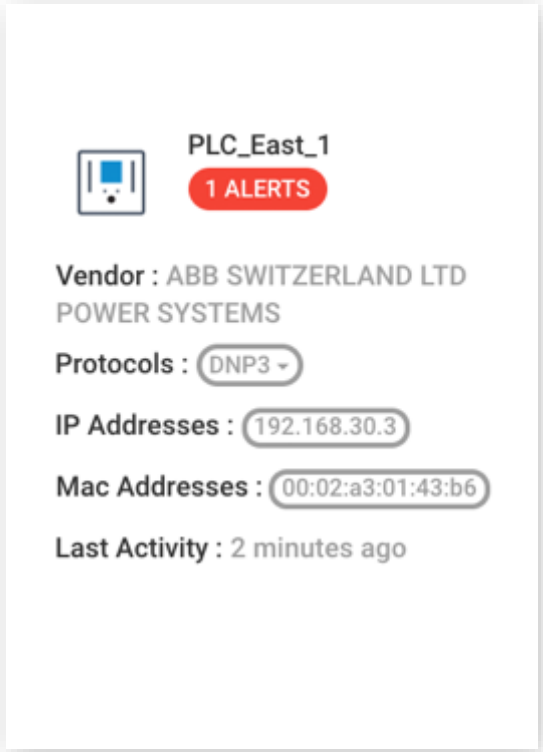


Azure Defender for IoT screenshot examples

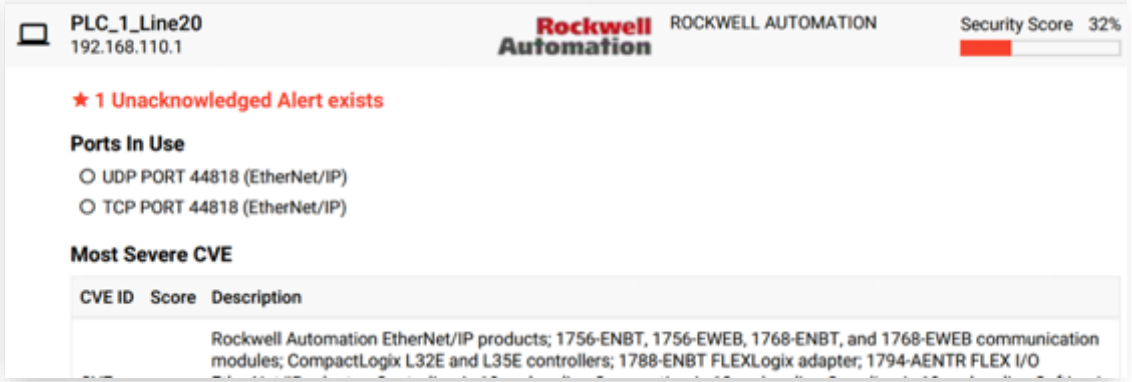
Asset discovery & network topology mapping



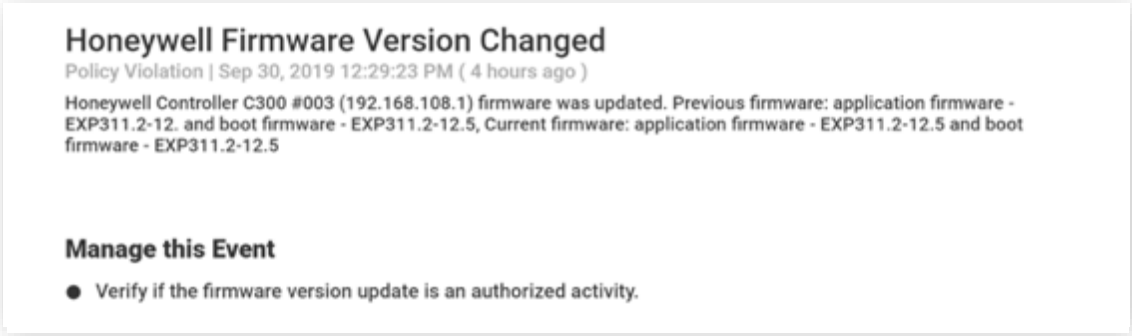
Device details



Vulnerability management

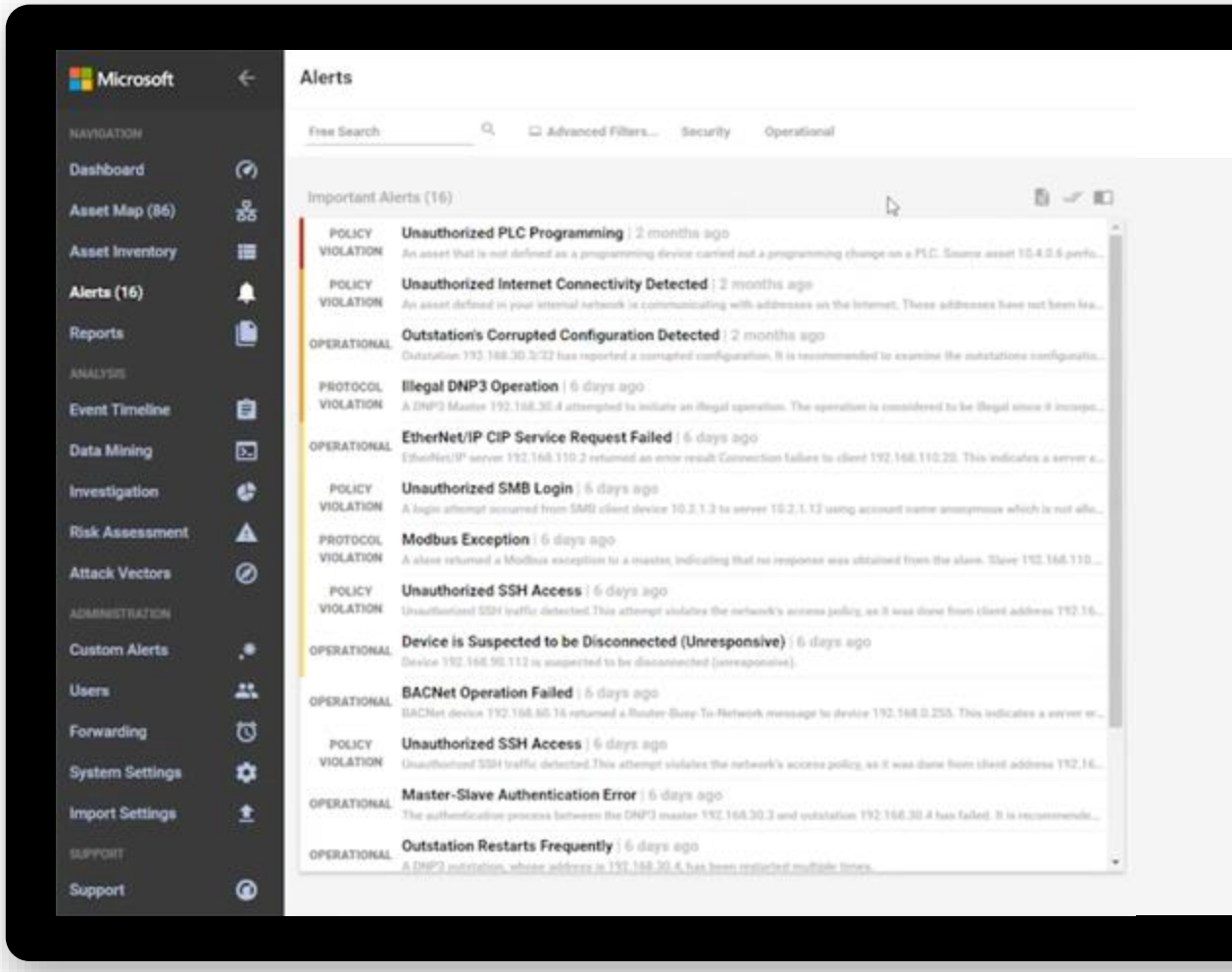


Security alert



Real-time IoT/OT threat alerts

- Unauthorized device connected to the network
- Known malware detected (e.g., EternalBlue)
- Unauthorized connection to the internet
- Unauthorized remote access
- 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
- BACnet operation failed
- Illegal DNP3 operation
- Master-slave authentication error
- Unauthorized SMB login



Azure Sentinel

Cloud-native SIEM/SOAR, deeply integrated with Azure Defender for IoT

Native functionality

Converged IT/OT visibility — modernizing the corporate SOC

ML combined with continuously-updated threat intelligence from trillions of signals collected daily

Scalability of cloud-based service

Reduced complexity & TCO

OT specific

Deep OT/IoT contextual information via Azure Defender for IoT

OT/IoT-specific threat intelligence via Section 52 research team

OT/IoT-specific SOAR playbooks

Zero Trust Scenarios

Authorized devices

Alert new device

Cross subnet traffic

Attack Vector - 192.168.110.1

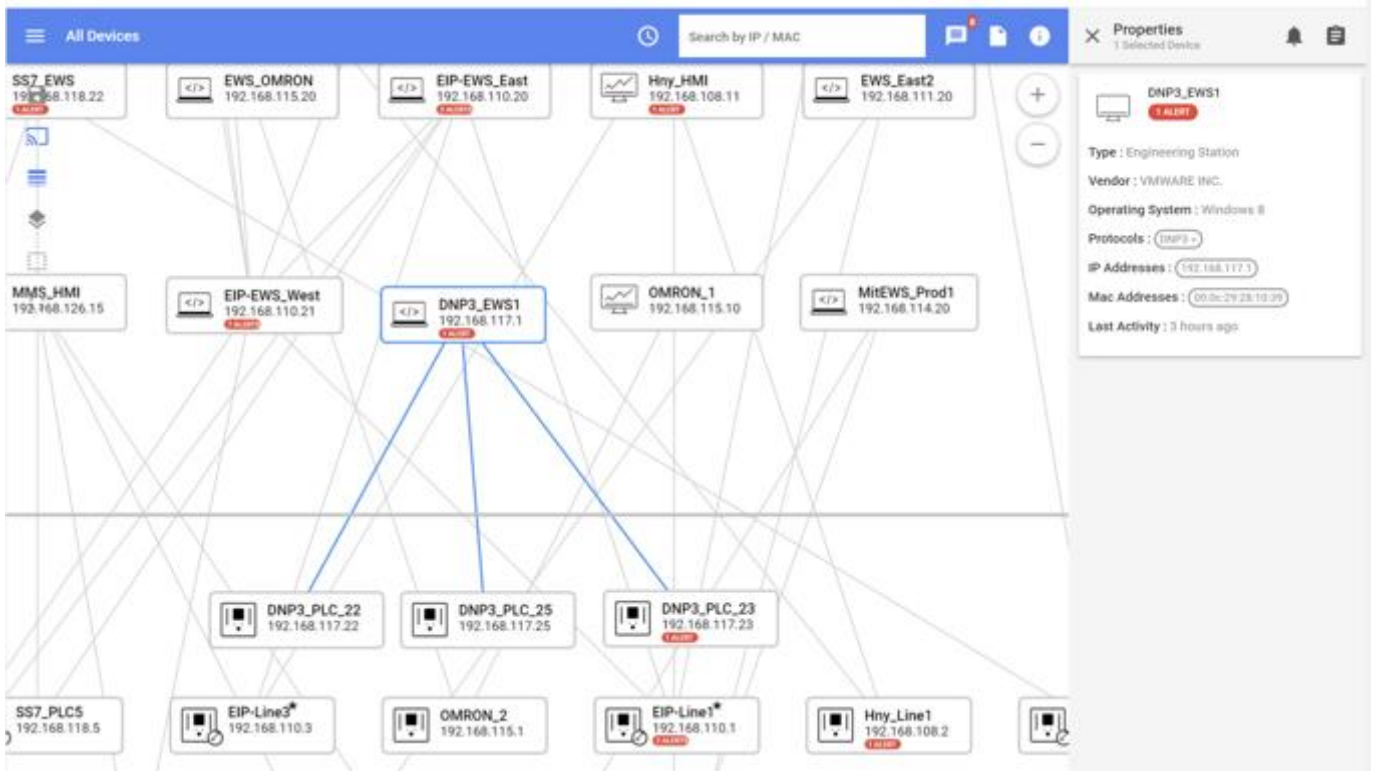
Visibility

Protection

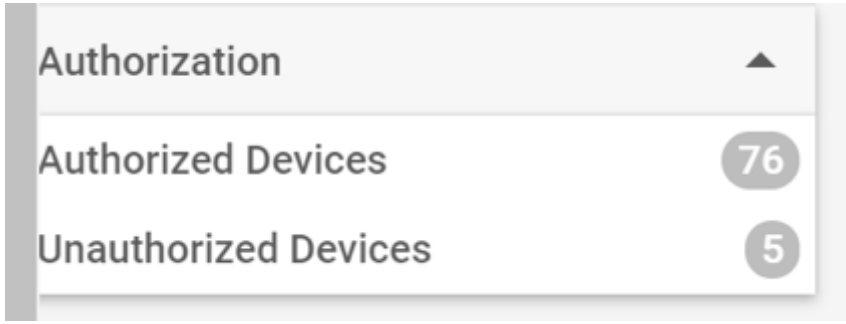
Monitoring

Authorized Devices

- Do you know what devices are on your network?
- Do you know who they communicate with?
- If you do, then these can be “authorized” devices…



Do you know what device are “Un-Authorized”?



- How quickly can you identify them?
- How do you know what they are doing?

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, IBM 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
- Multiple generation sites (electrical, LNG, renewable energy)
- Had no visibility into OT assets/risk
- "It's not just for security – it also helps fix operational issues."

een) -

Thank You!

contact: koen.jacobs@secwise.be

SecWise