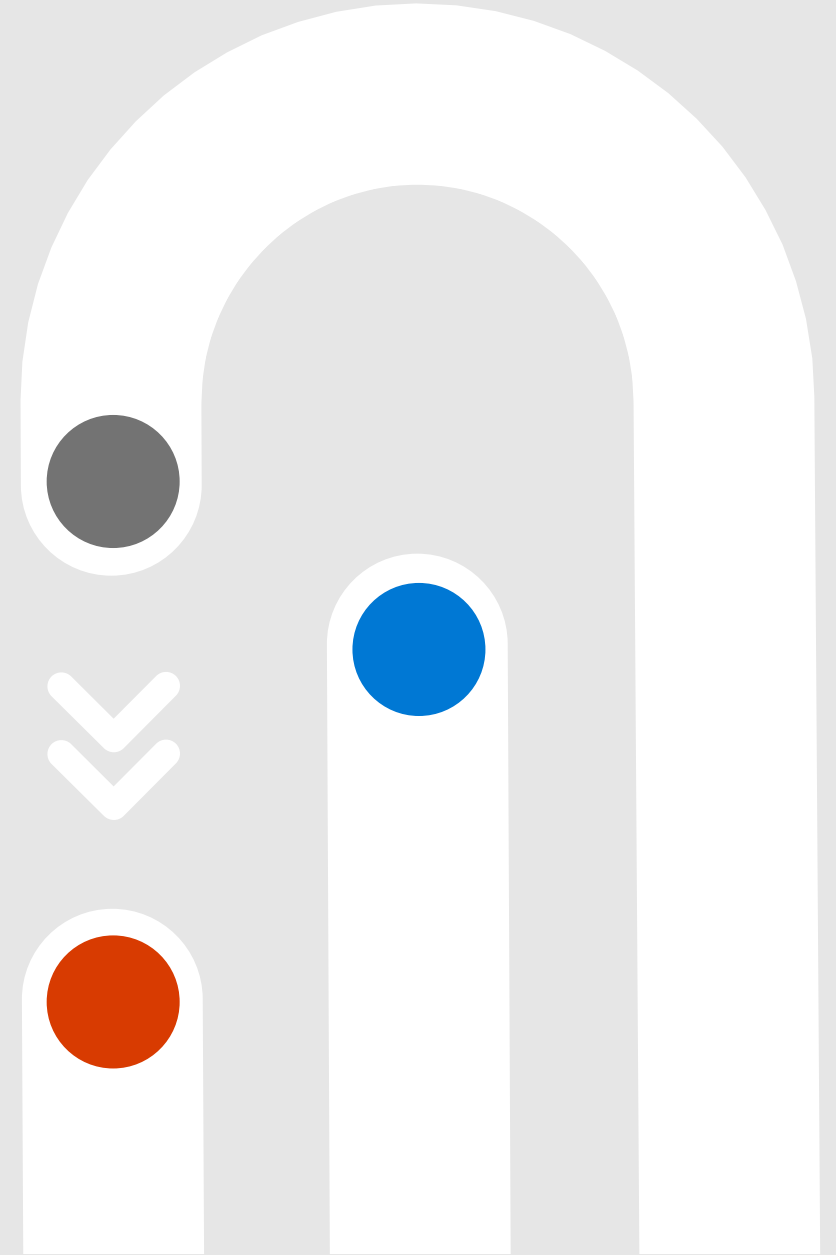


Defender for IoT

Angelica Faber



Today's agenda

- Defender for IoT Overview w/ Architecture
- Defender for IoT Demo
 - Sensor
 - Sentinel Integration



IoT/OT risk = business risk

Financial



Ransomware shuts down production leading to revenue losses of millions of dollars in downtime

IP Theft



Adversaries compromise IoT/OT to steal proprietary IP (designs, formulas, processes)

Safety

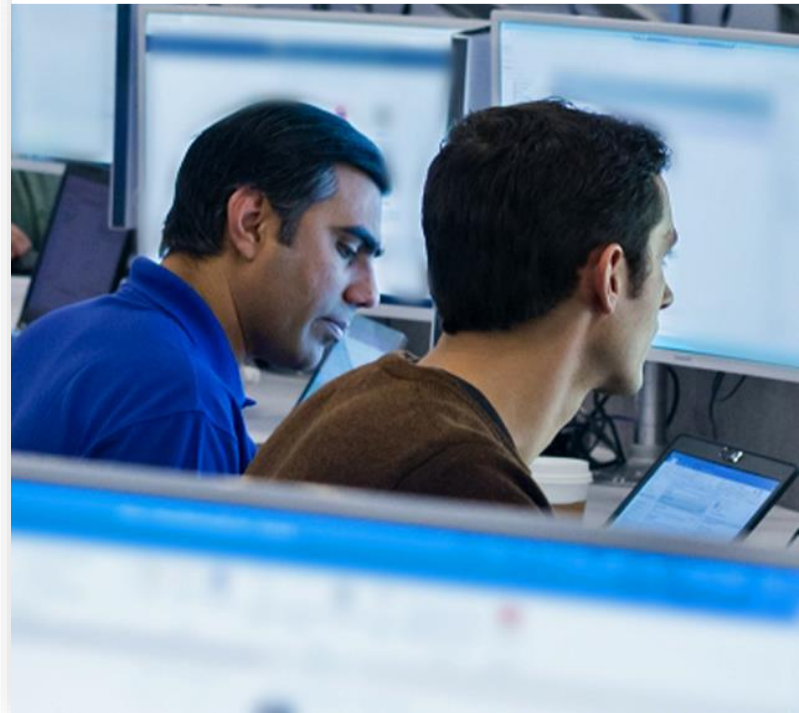


Attacks on electric grid, water utilities, gas compression facility, maritime ports, petrochemical facility, ...

Defender for IoT

Agentless Security for Unmanaged Devices

- Purpose-built OT security platform for Industrial IoT networks
- Deep knowledge of specialized OT protocols & devices across diverse OT suppliers (GE, Rockwell, Schneider, Emerson, Siemens, ABB, Yokogawa, etc.)
- Infused with IoT/OT specific Threat Intelligence
- Deploys in minutes with zero performance impact and 100% passive by default
- Native integration with existing IT security stacks (Sentinel, ServiceNow, etc.)



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 (pre-digital transformation)

Little or no visibility into IoT/OT risk

Better Together | Value Proposition

- CISOs of OT-oriented organizations need to cast light on their OT security blind spots, aiming to avoid attacker kill chain that aims to target their critical business processes
- Together, Microsoft Sentinel and Defender for IoT help bridge the gap between IT & OT security challenges and empower SOC teams with out-of-the-box capabilities to efficiently detect and respond to OT threats
- Unlike existing market alternatives, these two products provide a **converged IT & OT SOC team** to **reduce the time it takes to resolve OT incidents**



Better Together | Capabilities

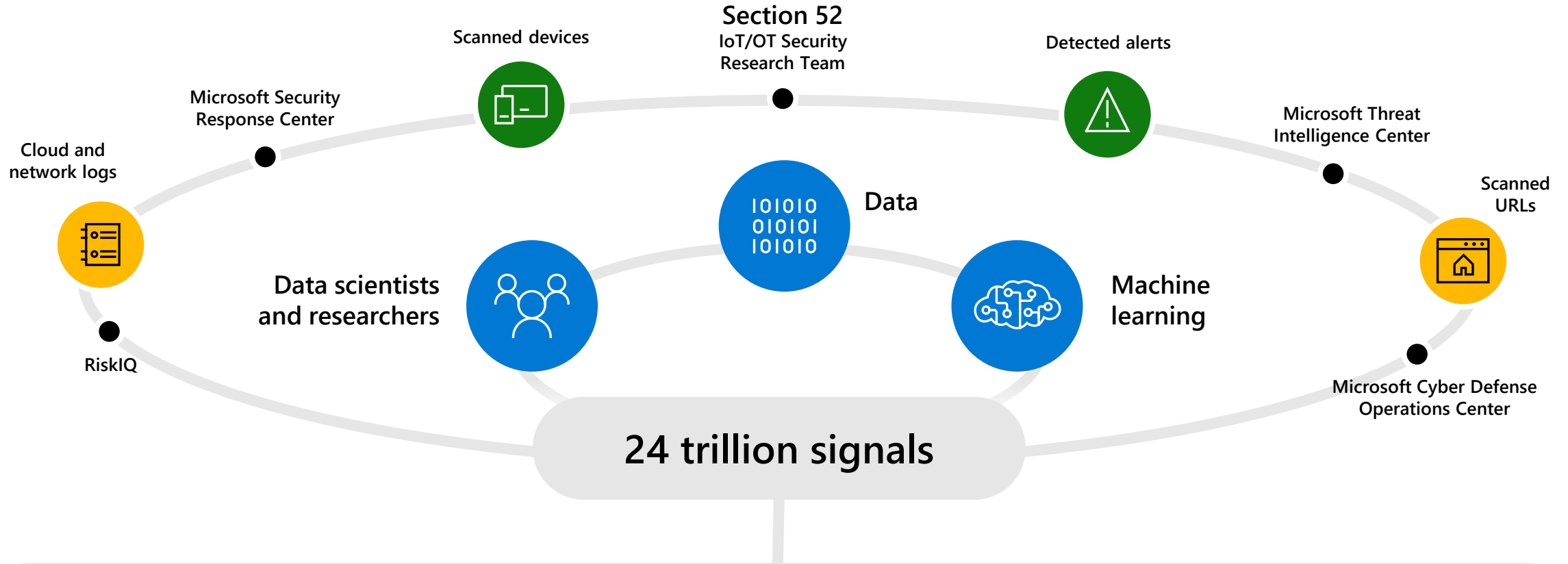
Converge your IT & OT SOC

- Single pane of glass for IT/OT incident management and response
- Insights on compromised OT assets and threats including vulnerabilities, risk score, and behavioral anomalies
- IT/OT holistic investigation experience that leverages additional data sources at zero cost (multistage attacks – fusion)
- Visibility into MITRE ATT&CK® for ICS

Shorten your OT incident's MTTR

- Comprehensive OT incident investigation that includes alerts, compromised assets, network connections/events and PCAP access
- Business impact mapping, to the level of the OT-centric organization site, line, and sensor
- Identification of OT crown jewels and the relevant OT persona to assign an incident to
- OOB OT solution of workbooks, analytic rules, and playbooks

World class threat expertise for IoT/OT



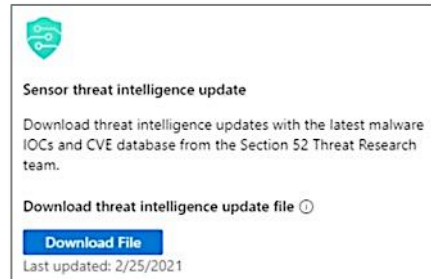
Section 52 and broader research teams leverage worlds richest threat intellect feed

Discover IoT/OT vulnerabilities, monitoring campaigns and creating unique detections

Results: #1 in detection visibility coverage in MITRE ATT&CK® for ICS evaluation

World-Class Threat Expertise

- Section 52: Former nation-state defenders, IoT/OT security researchers & data scientists
 - Proprietary vulnerability research
 - Reverse-engineering malware
 - Monitoring IoT/OT honeypots
 - Tracking adversaries & campaigns
- Continuous threat intelligence updates delivered via the cloud
 - Latest CVEs
 - Malware
 - Malicious DNS & other IOCs
- Recent threat intel packages
 - FireEye hacking tools
 - NOBELIUM campaign
- Integrated with Microsoft's global threat intelligence feed derived from 24+ trillion signals collected daily



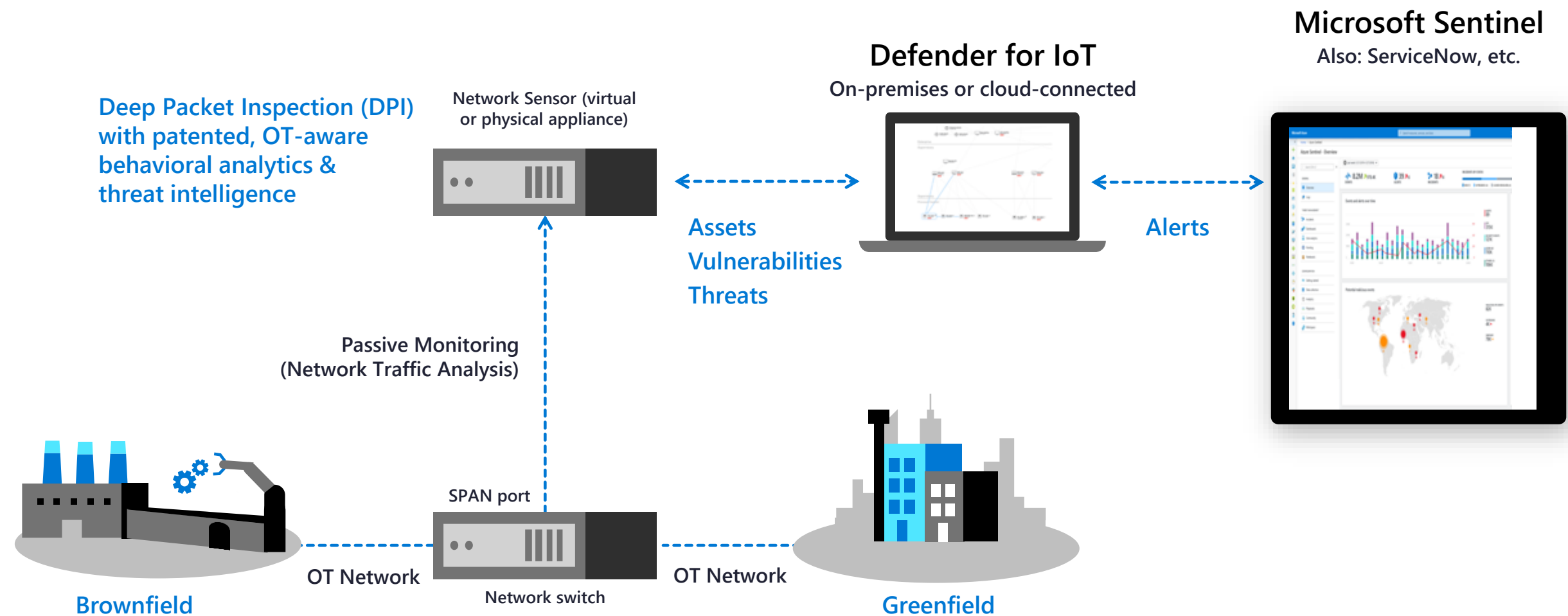
35+ zero-day vulnerabilities reported to CISA by Section 52

[BadAlloc vulnerabilities in widely-used RTOS/SDKs](#)
[Rockwell Automation Micrologix 1400 PLC Systems](#)
[Rockwell Automation CompactLogix 5370](#)
[Rockwell Automation MicroLogix 1100 PLC Overflow](#)
[Schneider Electric ConneXium Buffer Overflow Vulnerability](#)
[Schneider Electric Modicon M340 Buffer Overflow Vulnerability](#)
[Siemens Industrial Products](#)
[Emerson DeltaV DCS Workstations](#)
[GE CIMPLICITY](#)
[3S-Smart Software Solutions GmbH CODESYS](#)
[AVEVA InTouch](#)
[Paradox IP150 Building Security System](#)

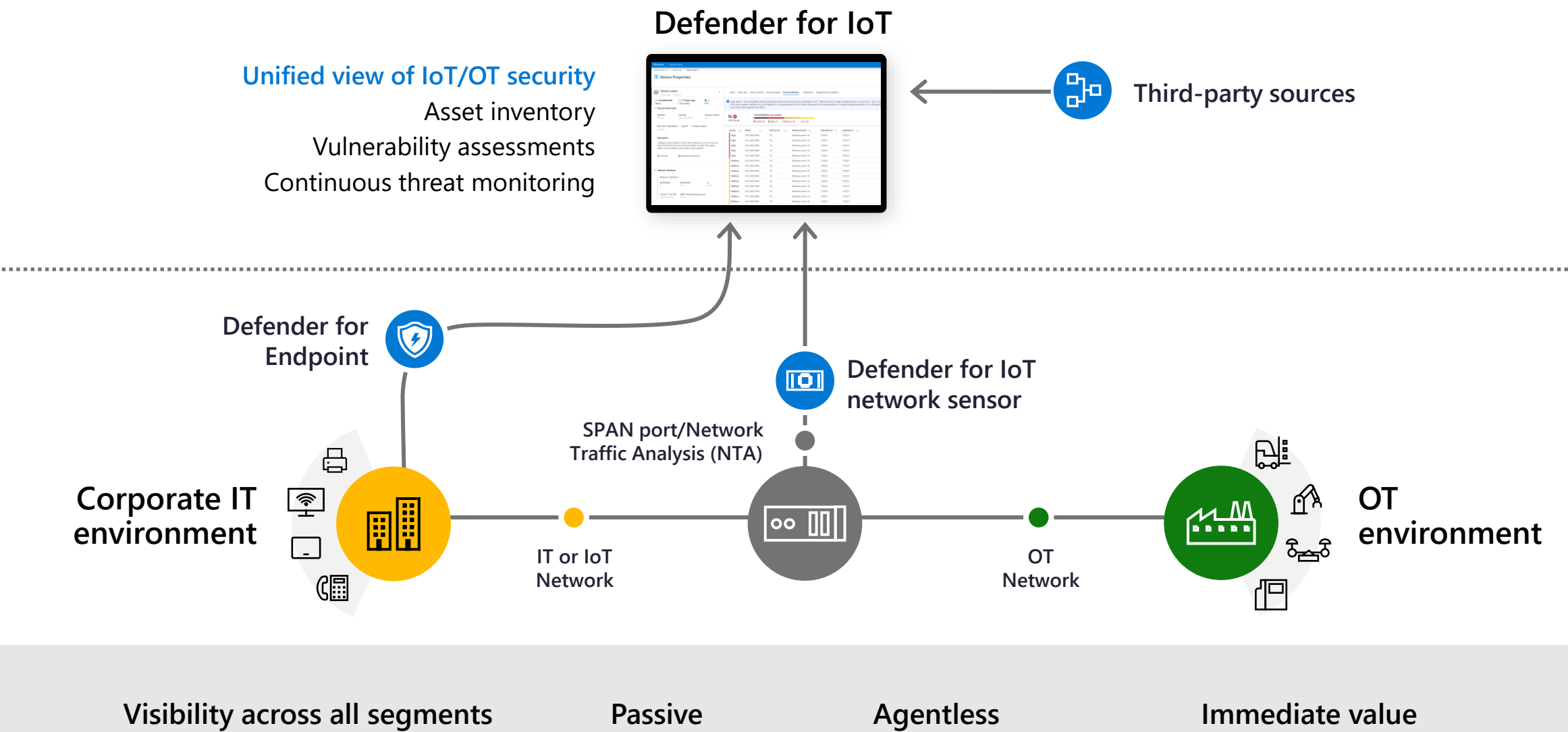
IoT/OT campaigns discovered by Section 52

[Operation BugDrop: Large-Scale Cyber-Reconnaissance Operation](#)
[Gangnam Industrial Style: APT Campaign Targets Supply Chain](#)
[RADIATION: DDoS for Hire Using Compromised CCTV Devices](#)

IoT/OT-aware Network Detection & Response (NDR)



Broad coverage from diverse data sources

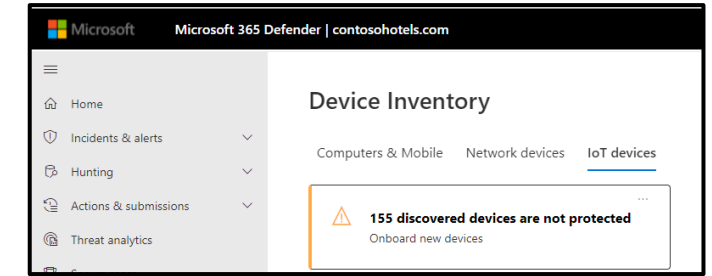
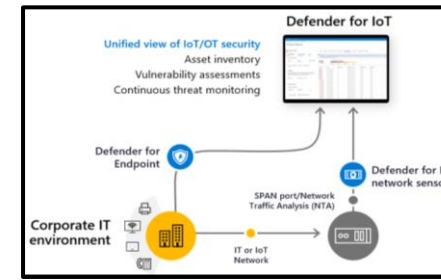


MDE Discovers eloT Devices: Solves Asset Inventory Problem

- Integrated with E5/MDE
- MDE Passive Discovery for eloT Devices

The screenshot shows the Microsoft 365 Defender interface. A red arrow points to the 'IoT devices' tab in the 'Device Inventory' section. A red box highlights the 'Device inventory' link in the left sidebar. Below the tabs, a warning states '155 discovered devices are not protected'. A summary bar shows 61 total devices, 0 high risk, 0 high exposure, and 0 newly discovered. A table of discovered devices is shown below.

IP	Device type	Vendor	Model	Name	Risk level	Exposure level	OS distribution	OS version	Last device update
10.121.89.70	Printer	HP			No known risks	Medium	Linux	Other	Feb 28, 2022 4:15 AM
10.121.88.59	Miscellaneous	Actiontec Ele...			No known risks	Low	OpenWRT	Other	Feb 28, 2022 4:13 AM
10.121.89.48	Miscellaneous	Actiontec Ele...			No known risks	Low	OpenWRT	Other	Feb 28, 2022 5:16 AM
10.121.88.58	Printer	Xerox	WorkCentre 7855	XR9C934E95F767	No known risks	Low	Other	075.040.001.01210	Feb 19, 2022 3:51 PM
10.121.89.48	Printer	Xerox	WorkCentre 7855	XR9C934E95F74D	No known risks	Low	Other	075.040.001.01210	Feb 19, 2022 4:17 PM
10.121.88.57	Printer	Xerox	WorkCentre 7855	XR9C934E95FA83	No known risks	Low	Other	075.040.001.01210	Feb 19, 2022 10:14 PM
10.121.88.62	Printer	Xerox	7855	9c934e95eb43	No known risks	Low	Linux	075.040.001.01210	Feb 28, 2022 5:21 AM



Defender for IoT

Defender for Endpoint

Enterprise IoT- Agentless Monitoring

Agent

Corporate IoT

IP cameras, printers, smart TVs, VoIP phones, smart appliances

Network

Routers, switches, APs

Endpoints

Servers, laptops, tablets, mobile

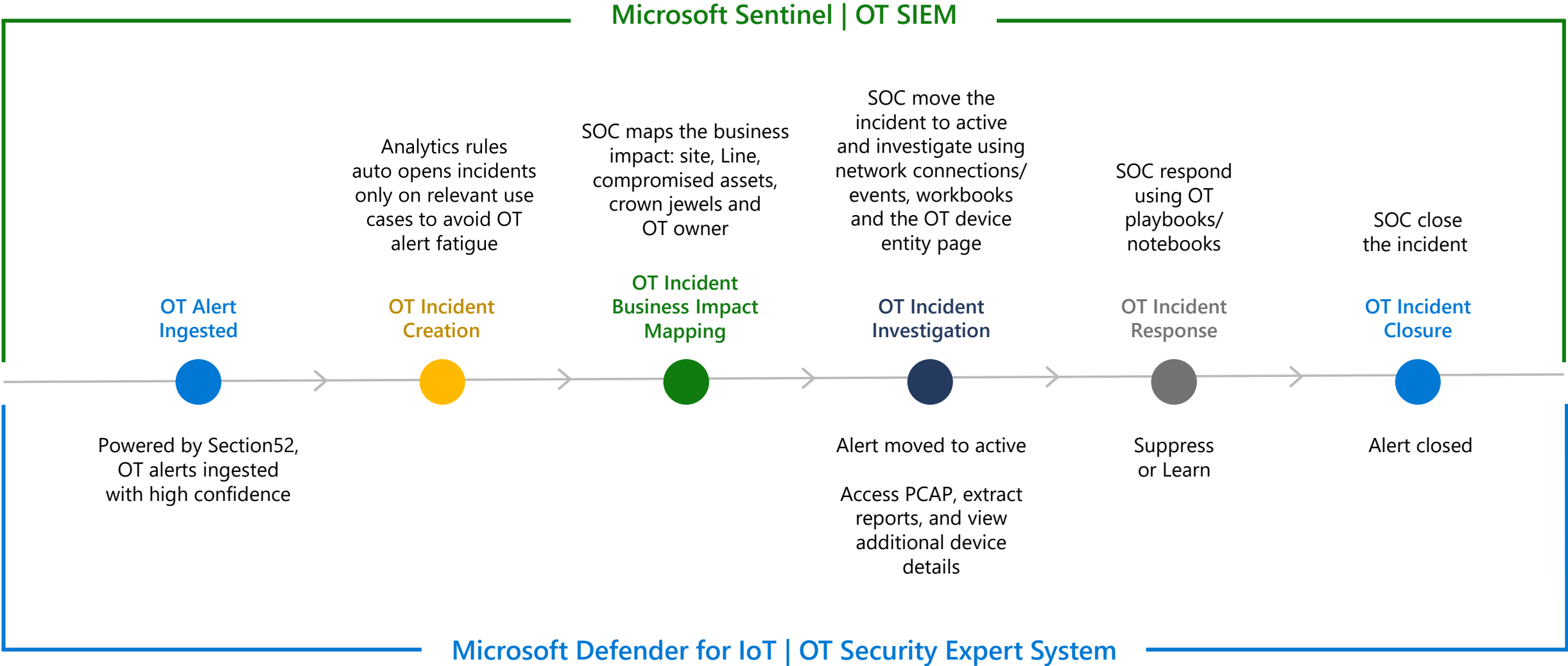
Two questions...

- How are you securing your enterprise network from growing IoT attack surface?
- Do you know all the IoT devices that are connected to your network now?

Enterprise

Traditional

Better together | User experience





Solution Content

Guide: ☐ Yes ☒ No Subscription: All Workspace: All Time Range: Last 30 days

Please take time to answer a quick survey. [click here.](#)

IoT/OT Threat Monitoring with Defender for IoT

Welcome to the IoT/OT Threat Monitoring with Defender for IoT Workbook. This workbook provides a guided investigation for entities based on open incidents, alerts sign-ins and activity for IT/OT assets. This workbook is ATT&CK for ICS, and designed to enable SecOps Analysts, Security Engineers, and MSSPs to gain situational awareness for IT/OT security posture.

Alerts Incidents MITRE ATT&CK for ICS Device Inventory

Alerts

Alerts Summary

HIGH	MEDIUM
152	120

(1) IoT/OT Threat Monitoring Workbook Assessment & Reporting

391 Active rules

Rules by severity

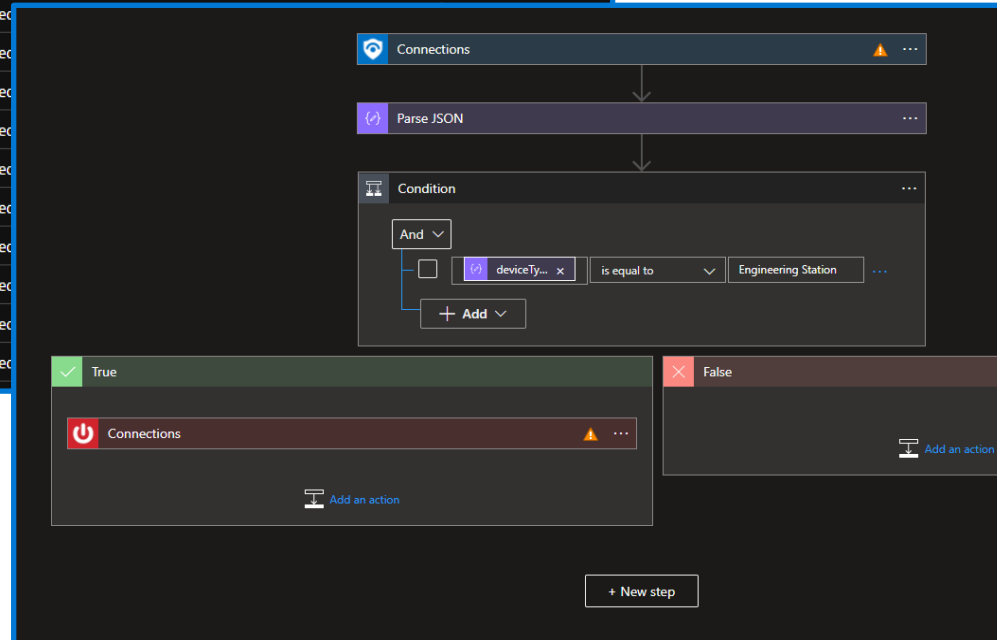
High (121)	Medium (198)	Low (29)	Informational (43)
------------	--------------	----------	--------------------

Active rules Rule templates

Search: Severity: All Rule Type: All Status: All Tactics: All





<input type="checkbox"/>	Severity <input type="text" value="↑↓"/>	Name <input type="text" value="↑↓"/>	Rule type <input type="text" value="↑↓"/>	Status <input type="text" value="↑↓"/>
<input type="checkbox"/>	High	Create incidents based		
<input type="checkbox"/>	High	Create incidents based		
<input type="checkbox"/>	High	Create incidents based		
<input type="checkbox"/>	High	Create incidents based		
<input type="checkbox"/>	High	Create incidents based		
<input type="checkbox"/>	High	Create incidents based		
<input type="checkbox"/>	High	Create incidents based		
<input type="checkbox"/>	High	Create incidents based		
<input type="checkbox"/>	High	Create incidents based		
<input type="checkbox"/>	High	Create incidents based		
<input type="checkbox"/>	High	Create incidents based		
<input type="checkbox"/>	High	Create incidents based		

(14) IoT/OT Threat Monitoring Analytics Rules Monitoring



(4) IoT/OT Threat Monitoring Playbooks Response

IoT & ICS Security maturity model

	Level 1 	Level 2 	Level 3 	Level 4 
Asset Mgt	<p>Asset documentation Spreadsheet</p> <p>Static network map</p>	<p>Dynamic Asset documentation</p> <p>Accurate spreadsheet with IPs</p>	<p>Alerting when new assets appear and retire</p> <p>Accurate network map with all assets in network topology</p>	<p>Integration with Asset Inventory database (CMDB)</p> <p>Automated network topology with device communications & protocol visibility</p>
Threat Detection	<p>No Anomaly Detection (AD)</p> <p>No incident response</p> <p>No risk & vulnerability assessment</p>	<p>AD via manual log review & signature-based alerts (IDS)</p> <p>Manual incident response</p> <p>Yearly risk & vulnerability assessment</p>	<p>AD via continuous monitoring with behavioral analytics using self-learning</p> <p>Automated incident response & threat hunting. Reviewed occasionally</p> <p>Automated risk & vulnerability assessment</p>	<p>AD via continuous monitoring with behavioral analytics using self-learning and remediation processes</p> <p>Automated incident response & threat hunting with supporting processes and dedicated personal</p> <p>Automated risk & vulnerability assessment with prioritized remediation</p>
IT & OT Integration	<p>No threat modeling</p> <p>No alignment between security & operational teams</p>	<p>Manual threat modeling</p> <p>Planning alignment between security & operational teams</p>	<p>Automated threat modeling</p> <p>Basic integration of SOC for OT environment</p>	<p>Automated threat modeling and proactive remediation efforts</p> <p>Integrated SOC for OT environment with process and procedures fully defined and operational while sharing VA information</p>



Demo



Thank you!