Microsoft

IoT Academy:

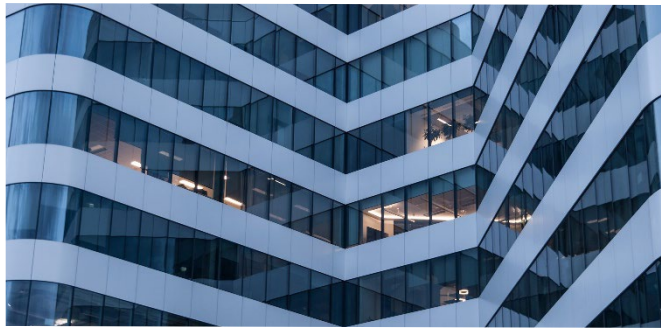
Azure Defender for IoT

Dan Frechette
Sr Technical Specialist GBB

How Gartner defines Operational Technology (OT) security

"The practices and technologies used to protect people, assets and information involved in the monitoring and/or control of physical devices, processes and events."

Manufacturing, energy & water utilities, smart buildings, chemicals, pharmaceuticals, oil & gas, transportation & logistics, mining, life sciences, retail, …



Differences between IT & OT security

IT Security	OT Security
Data confidentiality & privacy	Safety & availability
Standard protocols & devices	Specialized protocols, devices & legacy OS platforms
High levels of connectivity	Traditionally air-gapped
Multiple layers of controls & telemetry	Little or no visibility into IoT/OT risk

IoT/OT risk = business risk

Financial

Destructive malware shuts down factories worldwide, causing tens or hundreds of millions of dollars in losses (WannaCry, NotPetya, LockerGoga, Ekans, ...).

IP Theft

Adversaries compromise internet-connected devices to gain access to sensitive IP on corporate networks (discovered by Microsoft Security Research).

Safety

Malware exploits vulnerabilities in smart building access systems, actively targeting tens of thousands of devices every day in over 100 countries.

US CISA/NSA Advisory

"Cyber actors have demonstrated their continued willingness to conduct malicious cyber activity against critical infrastructure." **Organizations should**

- create an **accurate and detailed OT infrastructure map**
- use the **validated asset inventory** to investigate and **determine specific risks** associated with existing OT devices
- implement a continuous and vigilant system **monitoring program with anomaly detection**.

- Manufacturers are 8x more likely to be breached for theft of sensitive IP according to Verizon DBIR

Rapid deployment with zero performance impact

Deep Packet Inspection (DPI) with patented, OT-aware behavioral analytics

Sensor (virtual or physical appliance)

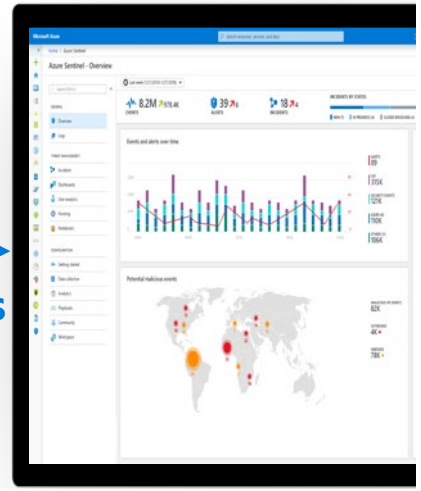
- **Assets**
- **Vulnerabilitie**
- **Threats**

Azure Defender for IoT

On-premises or cloud-connected

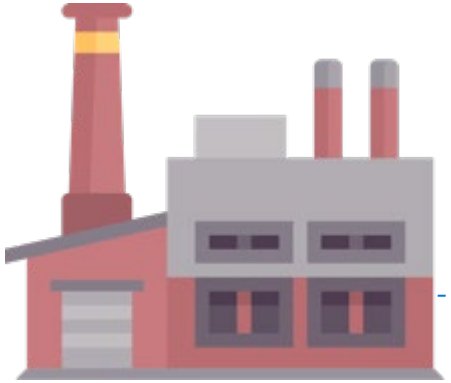
Alerts

Azure Sentinel



Also: Splunk, IBM QRadar, ServiceNow, etc.

Passive Monitoring (Network Traffic Analysis or NTA)

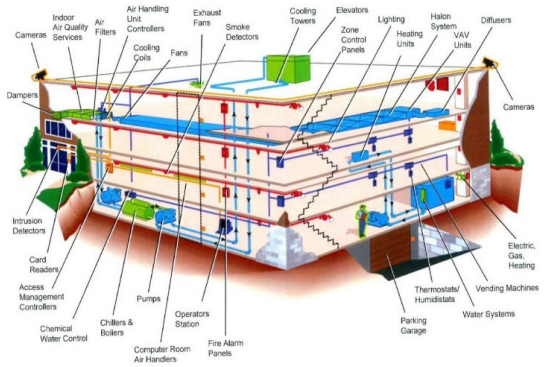


OT Network

SPAN port

Network switch

BMS Network



Protecting Your Enterprise of Things

Security Threat Intelligence

Defender for IoT

Microsoft Defender for Endpoint

Security Micro-Agent

Agentless Monitoring

Enterprise IoT

Dedicated IoT

Sensors, detectors, meters and purpose-built

OT/ICS

PLC/Indus. automation, embedded, proprietary

General-purpose IoT

Cameras, thermostats, smoke alarms, HVAC

Corporate IoT

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

Network

Routers, switches, APs

Endpoints

Servers, laptops, tablets, mobile

Greenfield

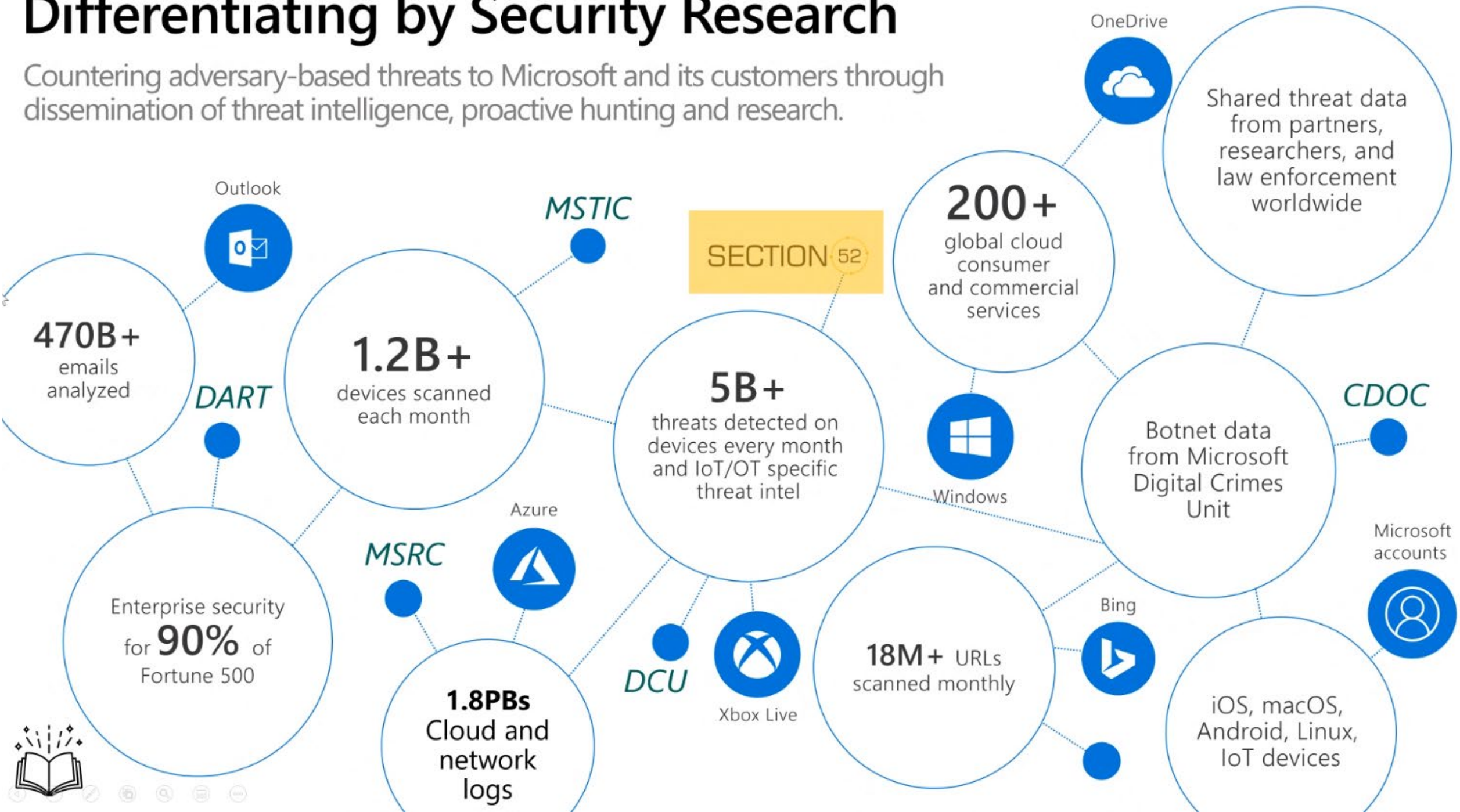
Industrial

Enterprise

Traditional

Differentiating by Security Research

Countering adversary-based threats to Microsoft and its customers through dissemination of threat intelligence, proactive hunting and research.



Differentiating by Security Research

Countering adversary-based threats to Microsoft and its customers through dissemination of threat intelligence, proactive hunting and research.

OneDrive

Shared threat data from partners, researchers, and law enforcement worldwide

Outlook

MSTIC

SECTION 52

200+ global cloud consumer and commercial services

470B+ emails analyzed

DART

1.2B+ devices scanned

5B+

CDOC

About Section 52

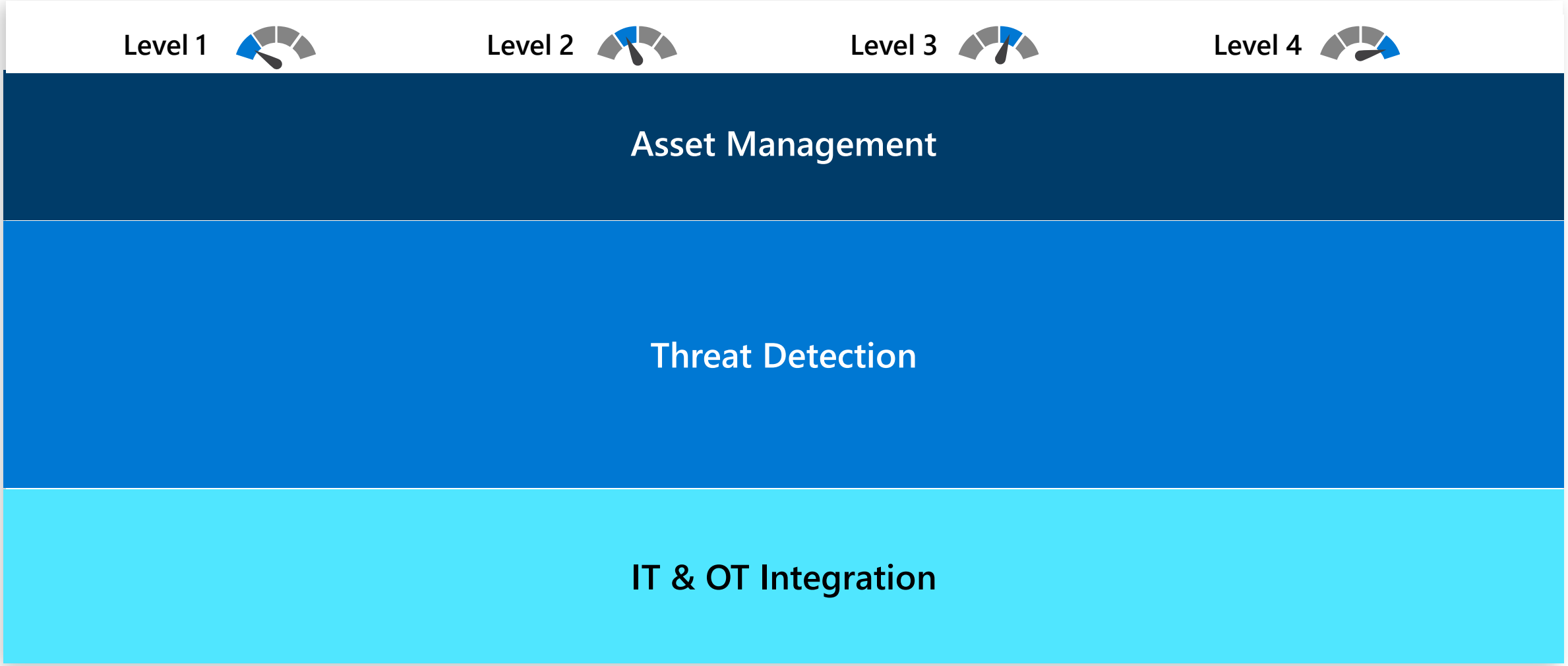
Microsoft's Section 52 is the security research group for Azure Defender for IoT. The group is comprised of security researchers and data scientists with deep domain expertise in IoT/OT threat hunting, malware reverse engineering, incident response, and data analysis. The group also provides ongoing threat intelligence updates to Azure Defender for IoT, enabling detection and mitigation of the most recent IoT/OT vulnerabilities and threats.

1.8PBs Cloud and network logs

Xbox Live

iOS, macOS, Android, Linux, IoT devices

IoT & ICS Security maturity model



IoT & ICS Security maturity model

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

Agentless security for unmanaged IoT/OT devices

IoT/OT Asset Discovery

What devices do we have & how are they communicating?

Operational Efficiency

How do we identify the root cause of malfunctioning or misconfigured equipment?

Risk & Vulnerability Management

What are risks & mitigations impacting our crown jewel assets?

Continuous IoT/OT Threat Monitoring, Incident Response & Threat Intelligence

How do we detect & respond to IoT/OT threats in our network?

Unified IT/OT Security Monitoring & Governance

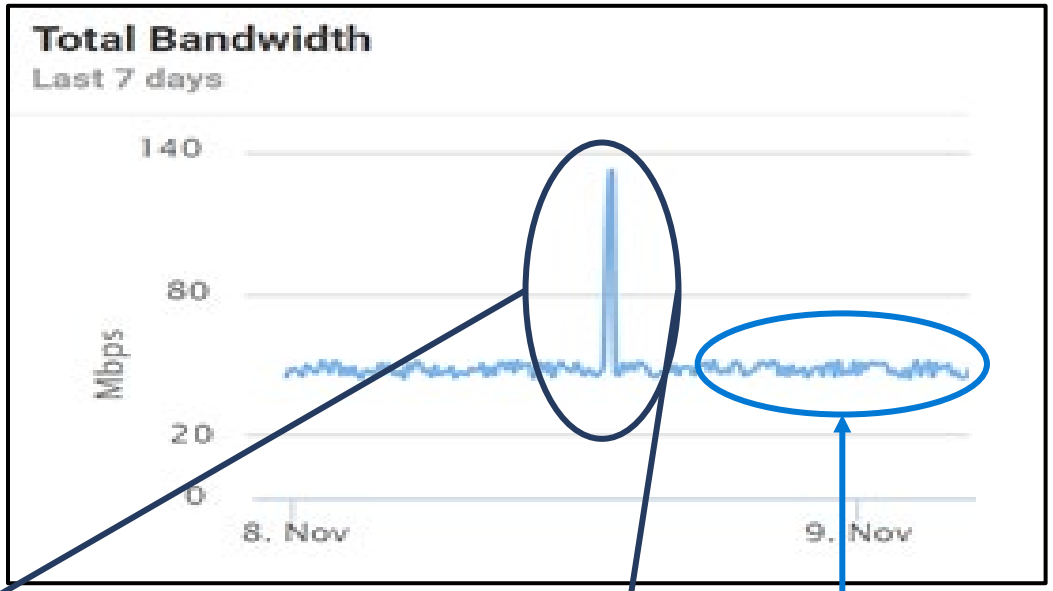
How do we break down IT/OT silos?

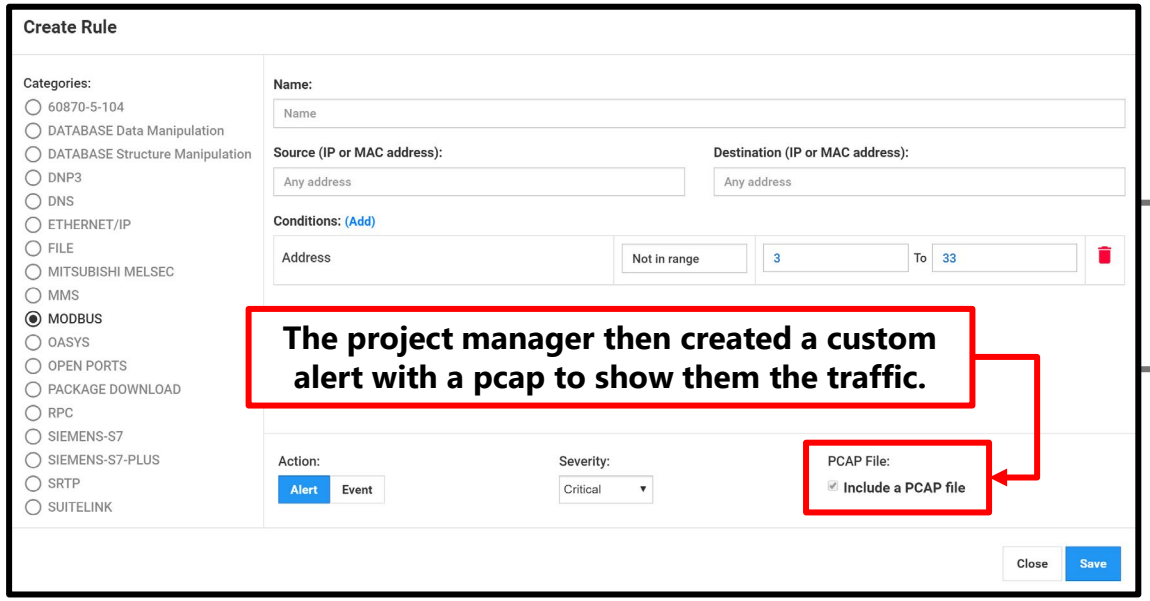
How do we leverage existing workflows & tools to centralize IT/OT security in our SOC?

How do we demonstrate to auditors that we have a safety and security-first environment?

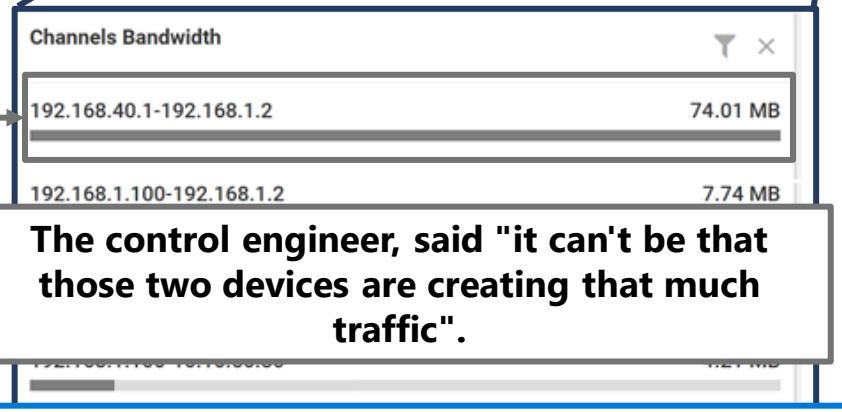
Misconfiguration In OT Network

- Customer decided to expand monitoring on one of the appliances
- They experienced a spike in measured bandwidth to 125mbs (a lot).
- Created the "busy channels" widget to look at details
- Discussed with the control engineer
- Identified the misconfiguration





The project manager then created a custom alert with a pcap to show them the traffic.



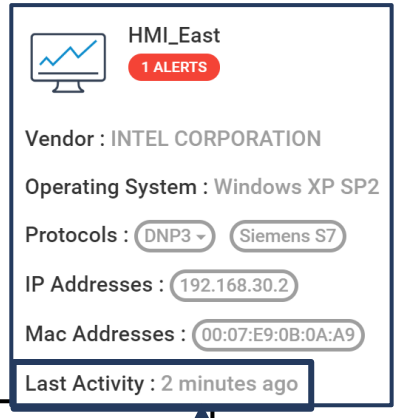
The control engineer, said "it can't be that those two devices are creating that much traffic".

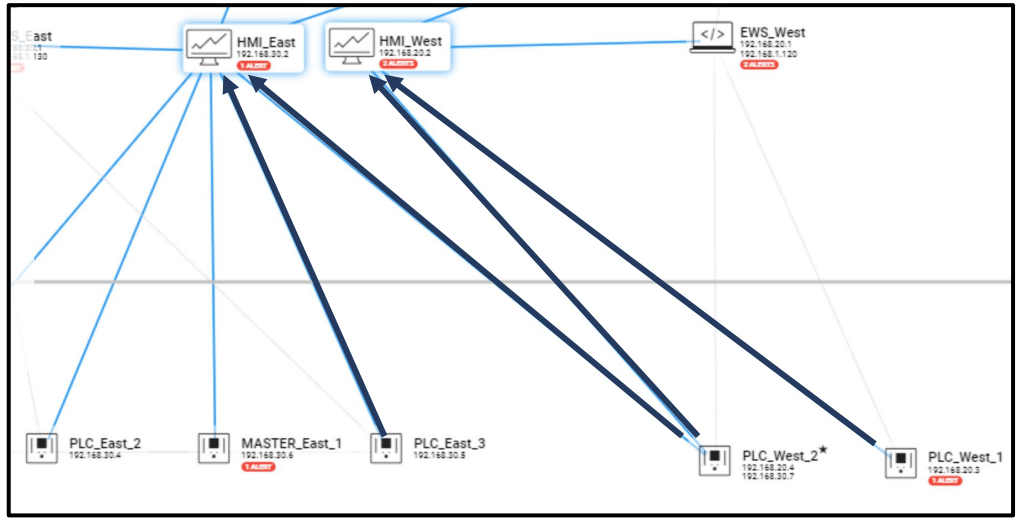
- **The end result was that those devices had a misconfiguration**
- **After fixing the issue, they dropped the bandwidth in the network from 125mbs to 60mbs.**

Network Visibility for Operational Insights

- Load balanced HMI's

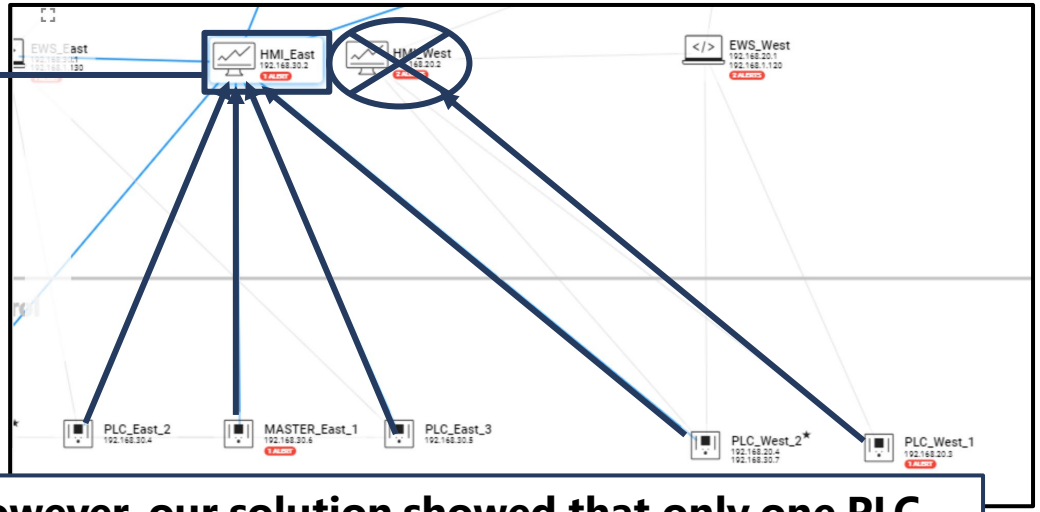
- Configured for round robin for setup





Open Ports per Connection

Server	Client	Port	Transport	Last Seen
EWS_East (192.168.30.1)	HMI_East (192.168.30.2)	SMB over IP (445)	TCP	15/11/2018 14:39:48
HMI_East (192.168.30.2)	Bob_Desktop (192.168.10.1)	Remote Desktop (3389)	TCP	15/11/2018 14:41:49
HMI_East (192.168.30.2)	EWS_East (192.168.30.1)	SMB over IP (445)	TCP	15/11/2018 14:42:03
HMI_West (192.168.20.2)	EWS_West (192.168.20.1)	SMB over IP (445)	TCP	15/11/2018 14:39:44
Historian (192.168.1.100)	HMI_East (192.168.30.2)	OSISoft PI Historian (5450)	TCP	15/11/2018 14:41:57
Historian (192.168.1.100)	HMI_East (192.168.30.2)	Oracle TNS (1521)	TCP	15/11/2018 14:40:31
Historian (192.168.1.100)	HMI_West (192.168.20.2)	OSISoft PI Historian (5450)	TCP	15/11/2018 14:40:07
Historian (192.168.1.100)	HMI_West (192.168.20.2)	Oracle TNS (1521)	TCP	15/11/2018 14:39:49
MASTER_East_1 (192.168.30.6)	HMI_East (192.168.30.2)	DNP3 (20000)	TCP	15/11/2018 14:39:57
PLC_East_1 (192.168.30.3)	HMI_East (192.168.30.2)	DNP3 (20000)	TCP	15/11/2018 14:40:14
PLC_East_2 (192.168.30.4)	HMI_East (192.168.30.2)	DNP3 (20000)	TCP	15/11/2018 14:41:05
PLC_East_3 (192.168.30.5)	HMI_East (192.168.30.2)	ISO Transport (102)	TCP	15/11/2018 14:39:42
PLC_West_2 (192.168.30.7)	HMI_East (192.168.30.2)	Ethernet/IP (44818)	TCP	15/11/2018 14:40:07
PLC_West_1 (192.168.20.3)	HMI_West (192.168.20.2)	Ethernet/IP (44818)	TCP	15/11/2018 14:40:24



However, our solution showed that only one PLC was communicating with a SINGLE HMI within the network traffic from a Siemens application

Economic Benefit for Defender for IoT

"Our reputation of delivering when the customer is expecting it is one of our most important assets. In the event of a ransomware event, the cost of the ransom will not even compare to the reputational cost of disrupting our customer's business flow. It may be un-recoverable."

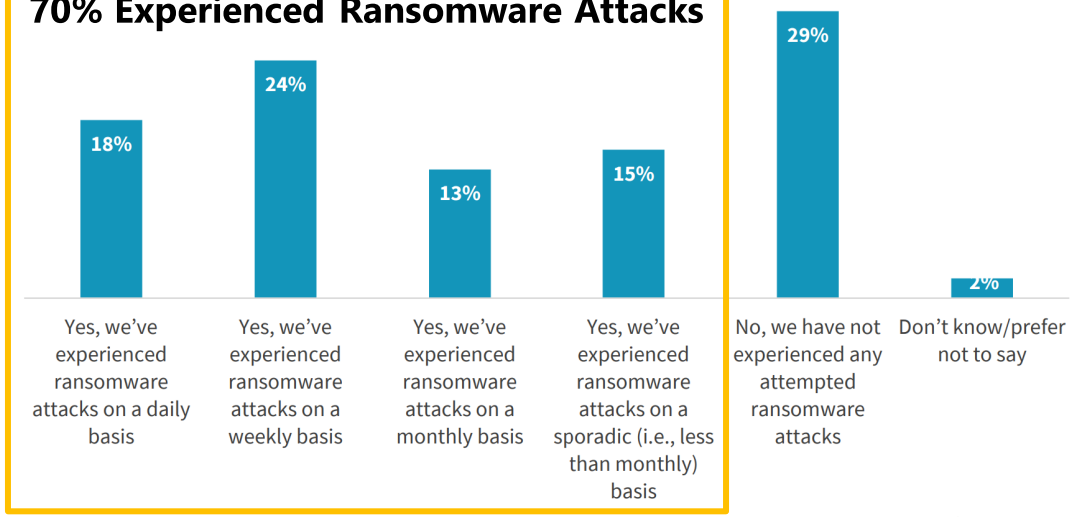
At the conclusion of this report, ESG presents an economic model showing that a typical $1.3 billion organization can realize potential cost avoidance and cost savings of $11.8 million per year, based on a software investment of less than $600,000 per year.

44%
Experienced cyber-attacks where IoT/OT devices were involved

60%
Say IoT/OT is one of the least secured parts of their infrastructure

63%
Expect the volume of sttacks on IoT/OT to increase

70% Experienced Ransomware Attacks



Source: Enterprise Strategy Group

"When deploying Defender for IoT, we found many devices that we did not know were there, many in an open state. We also found older protocols that we were unaware were still running on our systems."

"If an OT security event causes even 5 minutes of downtime, it will back up our delivery trucks, causing a cascade of problems, customer delays, and possibly fines. This quickly spins into hundred of thousands to millions of dollars of impact off a single delay.

"During our corporate security review, we were able to give a clear and concise view of current risk in our OT environment. Without the solution, we would have to run a truck out to each site. Doing this would require far more time and cost and would result in data that was subjective and dependent on the knowledge level of the person visiting each site."

– OT/ICS Cybersecurity Consultant

"1 hour of downtime is more costly than the entire annual cost of Defender for IoT. The solution pays for itself many times over."

-CISO, Manufacturing

Microsoft

Thank you!