"Security isn't something you buy, it's something we do, and it takes talented people to do it right"

How much Security is Enough ??

If its Connected, It must be Protected

Stop the Breach, Where IT and OT Meets

Vivek Porwal

October 2023

Security Challenges

Ineffective workflow between OT and IT

Limited visibility of OT assets

Lack of Segmentation

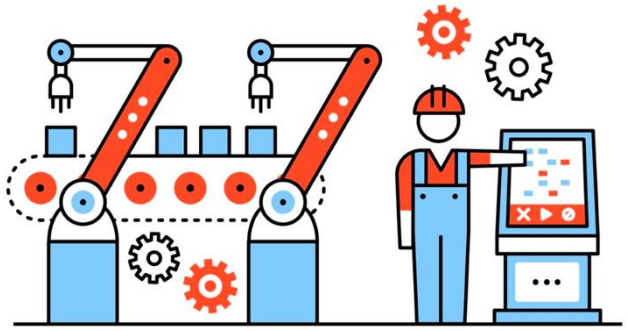
Malware is the killer

Many roadblocks towards success.
Industrial organizations need guidance.

The modern industry is even **more connected**

TODAY
Industrial Control Systems (ICS)

Energy, Manufacturing,
Transportation, Process Industries



TOMORROW
Industrial Internet of Things (IIoT)

Industry digitization increases the attack surface

Industrial operators think about safety, not security

What OT professionals are telling us

Everything is fine!
I have deployed high quality automation solutions and my operations are secure…

What we see during assessments

- Security patches not installed
- Firmware uploaded over FTP without signature
- Default credentials used to log into systems
- IT Vulnerability management
- Unauthorized remote accesses by subcontractors
- Decommissioned assets still connected
- OT network fully interconnected with IT
- Unnecessary network communications
- Windows XP, SMBv1

Securing Industrial must address various needs

OT

Gain **visibility** into assets and processes to keep production going and **reduce downtime**

IT

Reduce TCO by eliminating the need to invest in an ever-growing SPAN collection network

CSO

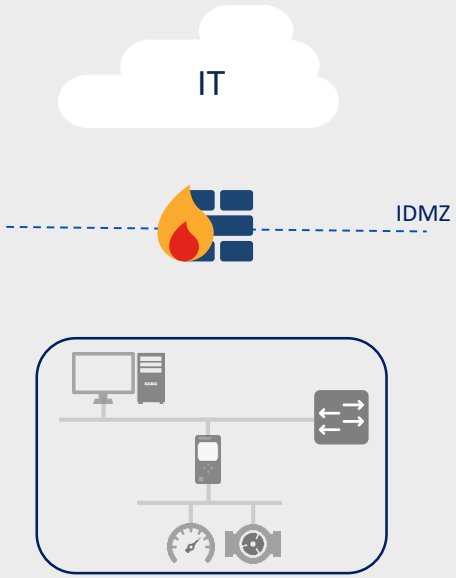
Feed **existing IT security tools** with OT context to build and **enforce OT security policies** that will not disrupt production

The bridge between the enterprise and the line of business

Industrial Security Guidelines

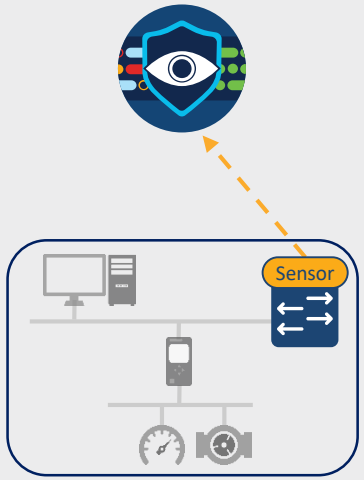
1 Build a Security Foundation

Define the IT/OT Boundary with Secure Firewall



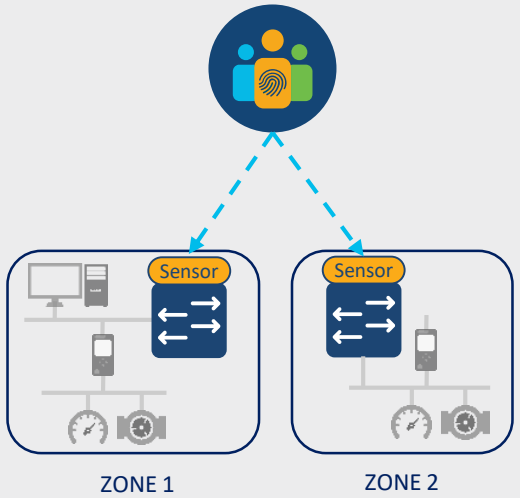
2 Gain Visibility & Device Posture

Using Network as a Sensor



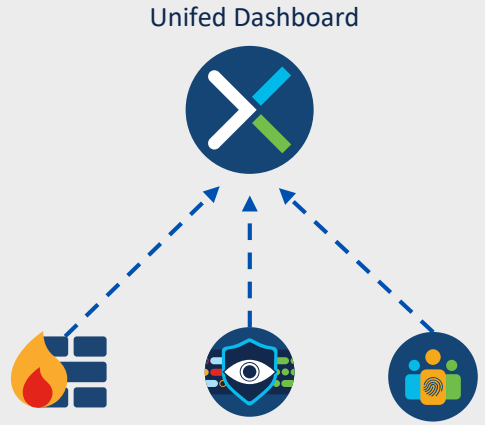
3 Segment network into smaller trust zones

Network as an Enforcer



4 Develop an Incident Investigation & Response plan

Investigate threats & orchestrate response



Thanks

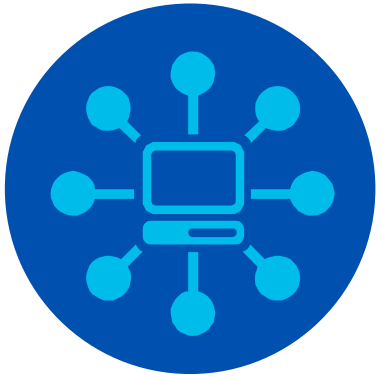
- Ask us for a session on Industrial Security
- Request an Assessment of your OT Security


CISCO

You cannot secure what you don’t know

Most customers don’t have accurate asset Visibility

55% have no or low confidence that they know all devices in their network



Blind to what their assets are communicating with

ICS equipment deployed over the years without strict security policies

Cisco Cyber Vision

Visibility & Security Platform for the Industrial IoT

Visibility
Asset inventory
Communication patterns

Security Posture
Device vulnerabilities
Risk scoring

Operational Insights
Track process/device modifications
Record control system events

Context and insights that are foundational to securing OT networks

Cisco Named a Leader in IoT/OT Security

The Forrester Wave™: Industrial Control Systems (ICS) Security Solutions, Q4 2021

FORRESTER®
WAVE LEADER 2021
Industrial Control Systems (ICS) Security Solutions

Source: Forrester Research, Inc. Unauthorized reproduction, citation or distribution prohibited

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

Benefits for IT: Visibility drives OT security

Segment OT Networks

Know your OT assets to implement access policies without disrupting production

Converge Security Operations

Get OT context and events in the SOC to build and enforce the right security policies

Reduce the Attack Surface

Identify risks to take corrective actions and implement best practices

Drive IT/OT Collaboration

Share a common understanding of the situation to build security policies together

Leverage your existing Cisco network to gain visibility over your OT and secure the whole enterprise

Benefits for OT: Visibility drives efficiency

Improve Network Performance

Identify network configuration issues, unnecessary traffic and old devices

Reduce Downtime

Spot device problems and configuration issues before they disrupt production

Troubleshoot Issues Faster

Record all OT events for root cause analysis when ICS components have issues

Monitor Contractor Activities

Track remote access sessions and all changes done by vendors to your ICS

Your Cisco industrial network gives you comprehensive visibility so you can improve operational efficiency

Bring Cisco scale and simplicity to industrial security

Cisco Industrial Networks

Connect anything anywhere

Cisco Security

Comprehensive IT/OT cybersecurity

Cisco Validated Designs

State-of-the-art architecture guides

Cisco Customer Services

Human skills to enable deployments

All working together for successful industrial security deployments

Case study: Energy

Natural gas distributor in Europe

Business drivers

- 5000 kms of gas pipes
- 600 gas compression stations and gas storage sites
- Low bandwidth network connections to central control room
- Predominantly Rockwell PLCs and devices
- Needed consolidated OT visibility to HQ and IT SOC integration

Solutions

- Cyber Vision Sensors deployed across the entire infrastructure to monitor 2,500 industrial control devices
- Lightweight data sent to Cyber Vision Center in HQ to save bandwidth
- Integration with RSA NetWitness for IT SOC visibility

Results

- Cyber Vision was deployed in phases starting with a risk assessment to target high priority risks, then real-time anomaly detection and IT SOC integration
- IT and OT teams now have accurate asset inventory and vulnerability data
- Cyber Vision reports incorporated into Operations maintenance plans
- Delivered cybersecurity training to OT over lifetime of the project

Case study: Utilities

A major power utility in EMEAR

Business drivers

- 1000 substations to monitor and secure
- Limited space to install equipment in substations
- Strong support of IEC-61850 (MMS/GOOSE)
- Integration with firewalls required

Solutions

- One Cyber Vision Sensor installed in each substation
- One Cyber Vision Center in the control room
- Integration with IBM QRadar (SIEM)
- Integration with Cisco FTD & Fortinet firewalls

Results

- Phase 1 deployment includes 52 substations
- Cyber Vision integrated into the SOC
- Edge architecture for limited substation equipment space and lower hardware costs


CISCO