

Digitize IoT/OT Protect your Production

Dimitris Tsaktsiras
Cybersecurity Solution
Consultant, Networking Solutions

 **SPACE**

Classification ISO 27001: Public

MK-18022020-1

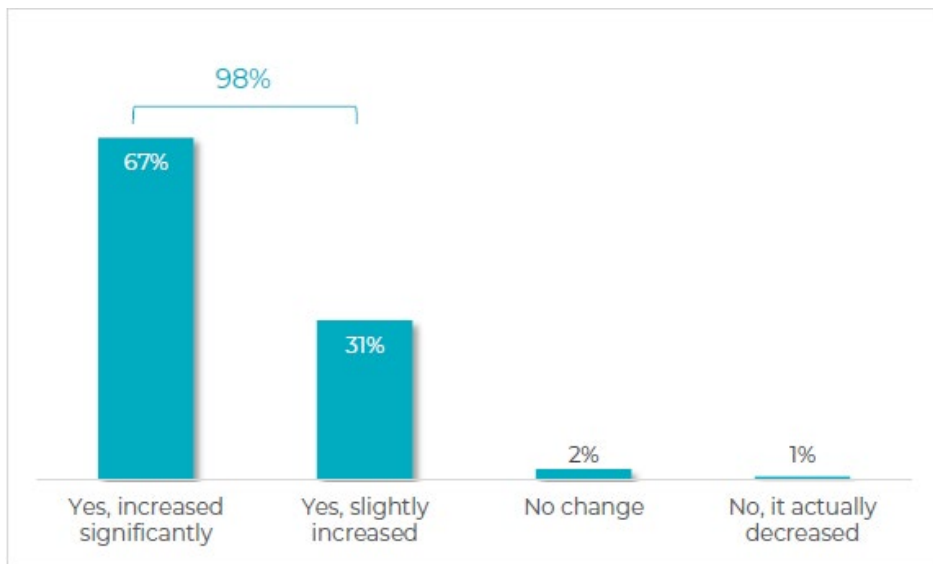


www.space.gr

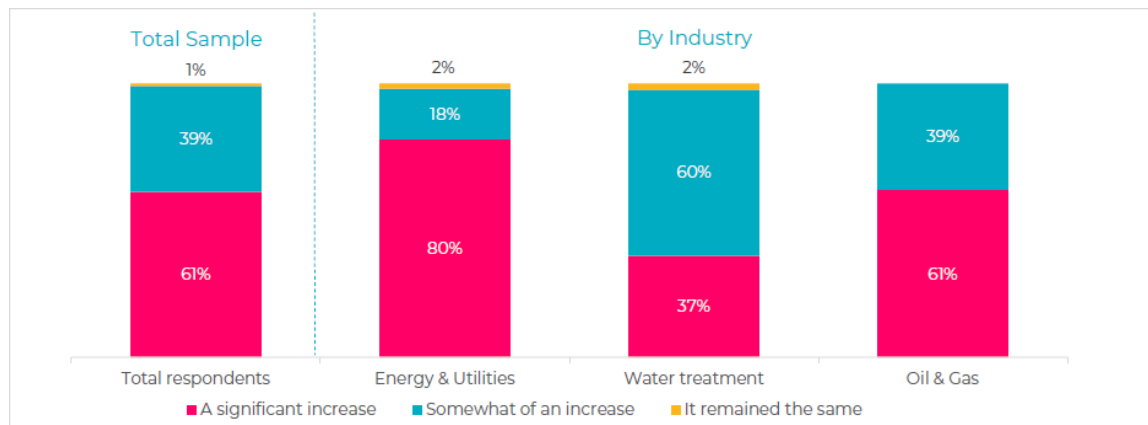
| Agenda

- Why IoT/OT Security
- Understanding OT
- Challenges
- The solution

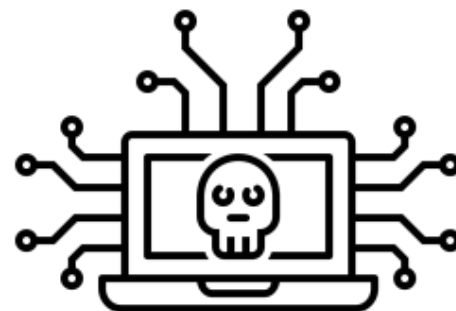
| Some Facts



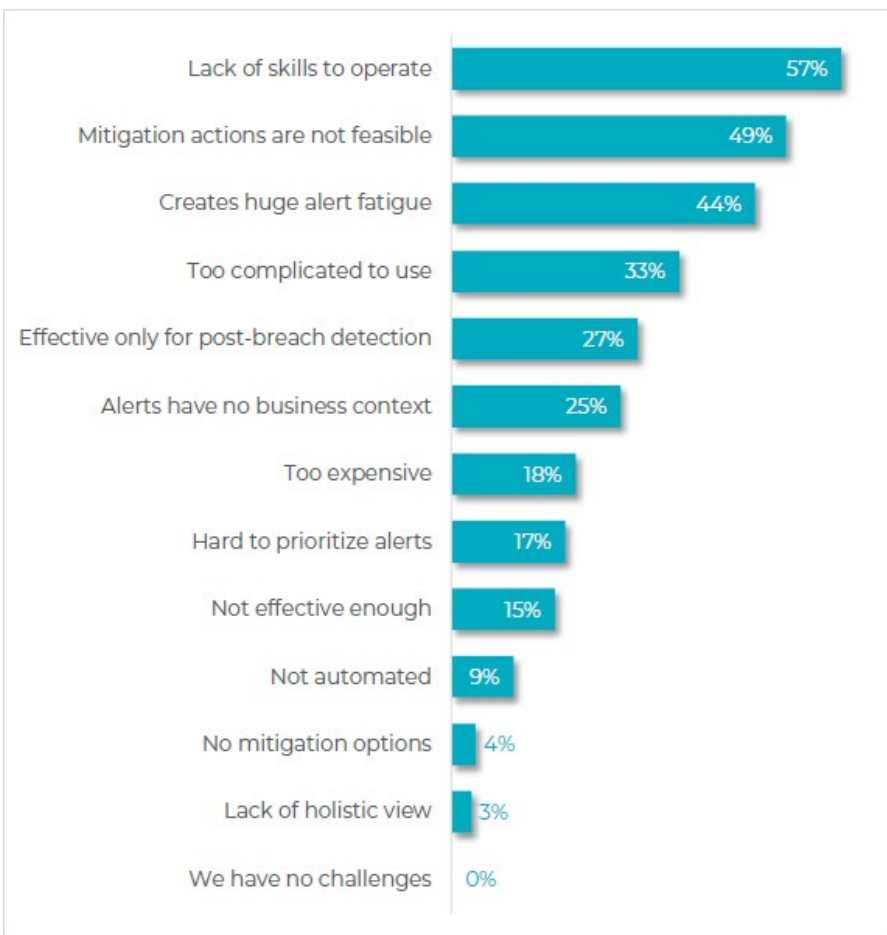
Increase in the Level of Digital and Cyber Risks (Past 3 Years)



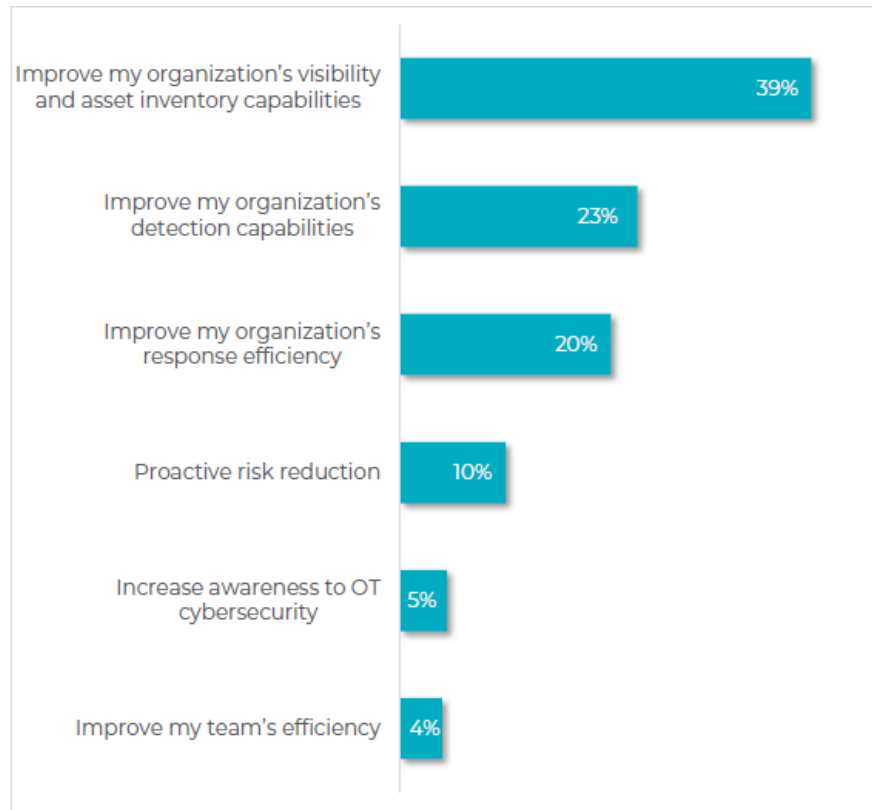
Changes in the Number of Regulations and Standards (Past 12 Months)



More Facts



Challenges with Existing OT Cybersecurity Solutions



Top OT Cybersecurity Focus

Source: OTORiO OT Cybersecurity Survey Report 2022



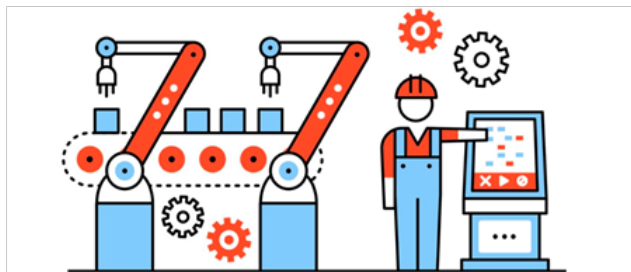
**Which
companies are
a target**

The modern industry is even more connected

TODAY

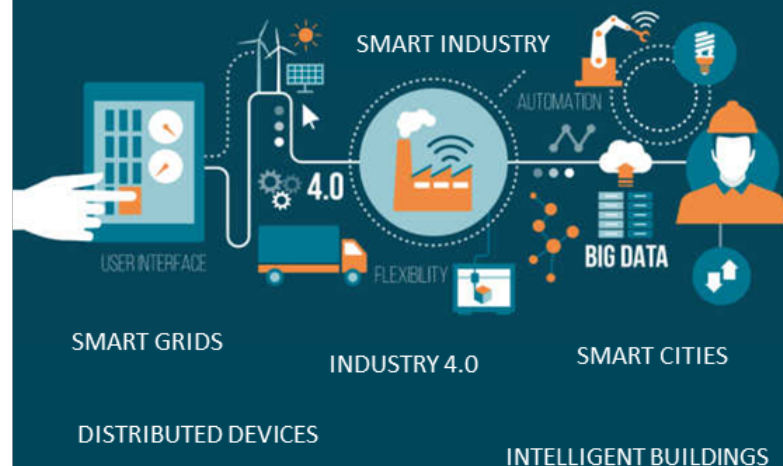
Industrial Control Systems (ICS)

Energy, Manufacturing,
Transportation, Process Industries



TOMORROW

Industrial Internet of Things (IIoT)



Industry digitization increases the attack surface



| Understanding OT

OT ≠ IoT ≠ IIoT ≠ ICS

IoT has become a generic name for everything that is not legacy IT, BUT:

- **IoT** is a technology to easily connect devices and increase datapoints at relative low cost
- **IIoT** is IoT technologies designed for industrial use cases
- **OT** devices control the physical world
- **ICS** (industrial control systems) orchestrate industrial processes through OT and IIoT devices

| OT & IT Have Different Requirements

	
Security = Cybersecurity	Security = Safety
IT teams manage data and care most about Confidentiality, Integrity and Availability	OT teams manage processes and care most about throughput and uptime
IT equipment are known, modern and controlled	OT devices can be 10-20+ years old and are often managed by third parties
IT networks are segmented	OT networks are flat
IT attacks can be well identified (virus, worms, DoS, etc.)	OT attacks look like legitimate instructions to industrial control systems

Extending IT security to OT requires specific skills and features

| Understanding “OT behaviors”



OT devices accessing the Internet is abnormal



Placing OT devices in quarantine can cause serious harm



Unconnected network segments are common



Unsupported OS, unpatched systems and outdated AV signatures are common



Machines and processes run 24/7/365

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

Building secure industrial operations is a journey

Visibility

Segmentation

Zero Trust

1. *People skills and training*
2. *Organizational processes*
3. *Network architecture & Security technologies*

Cyber Vision provides visibility & insights that are foundational to securing OT networks

| 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

Asset Visibility



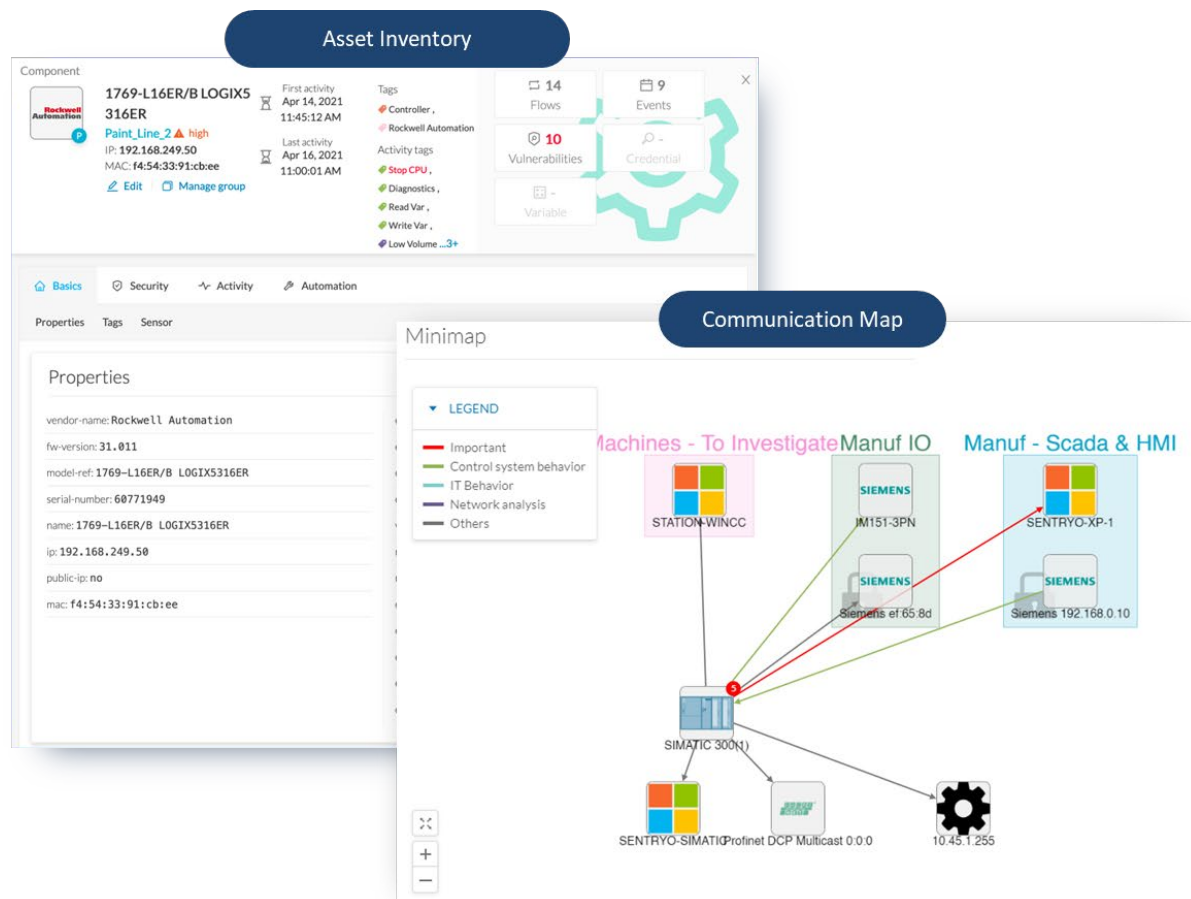
Asset Inventory

Comprehensive up to date inventory of all assets in your environment



Communication Patterns

Dynamic communication map with detailed application flow level information



Security Posture



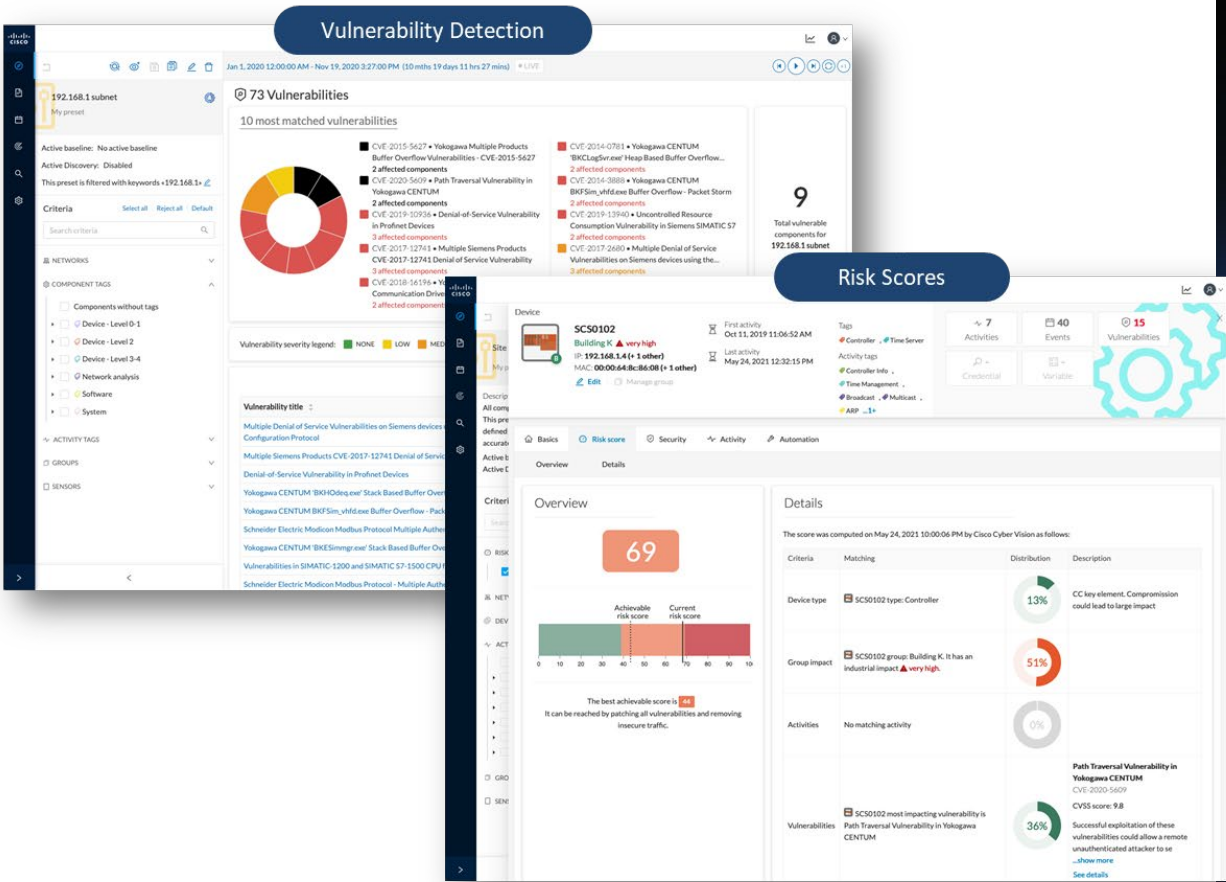
Vulnerability Detection

Identify known asset vulnerabilities so you can patch them before they are exploited



Risk Scoring

Asset risk scoring based on impact and likelihood to help you improve compliance



Operational Insights



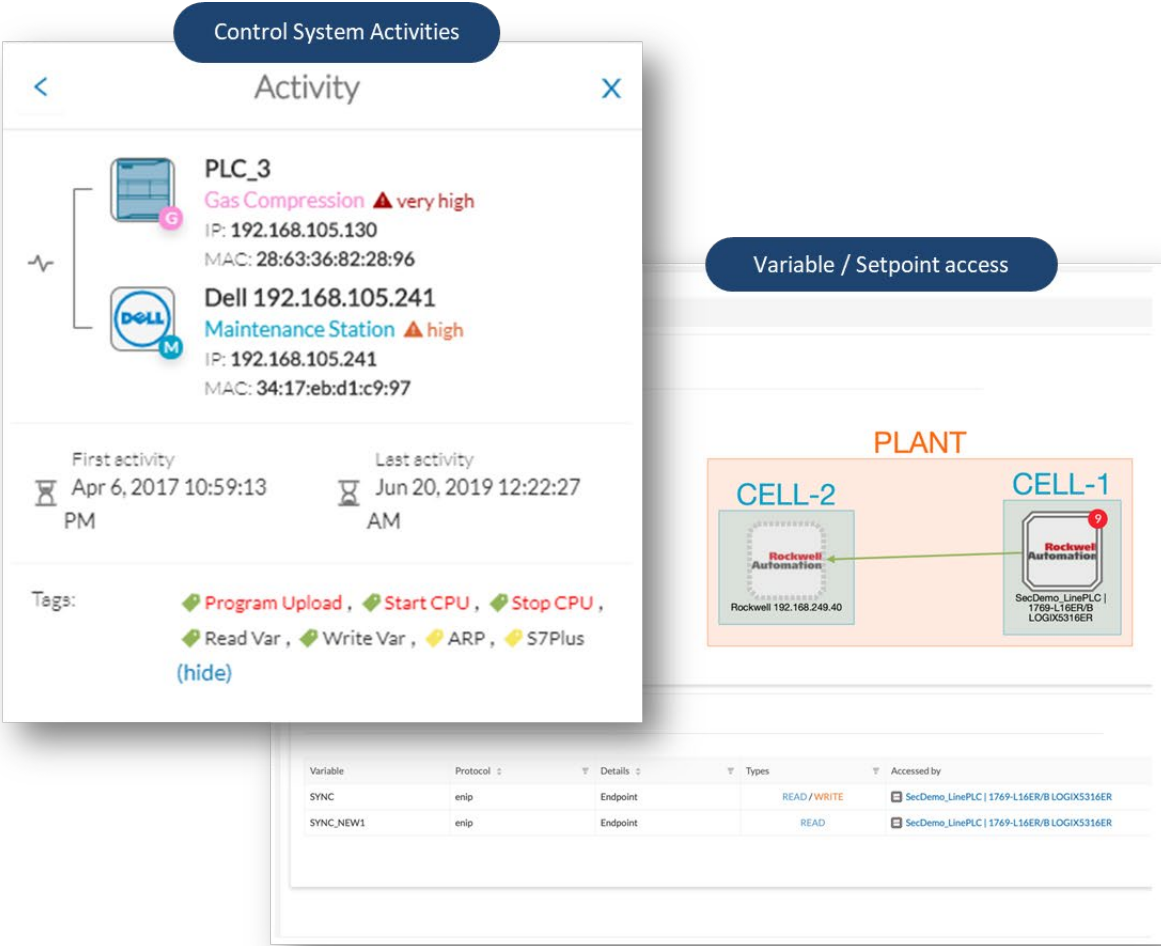
Control System Activities

Track process modifications
Identify configuration changes
Record control system events

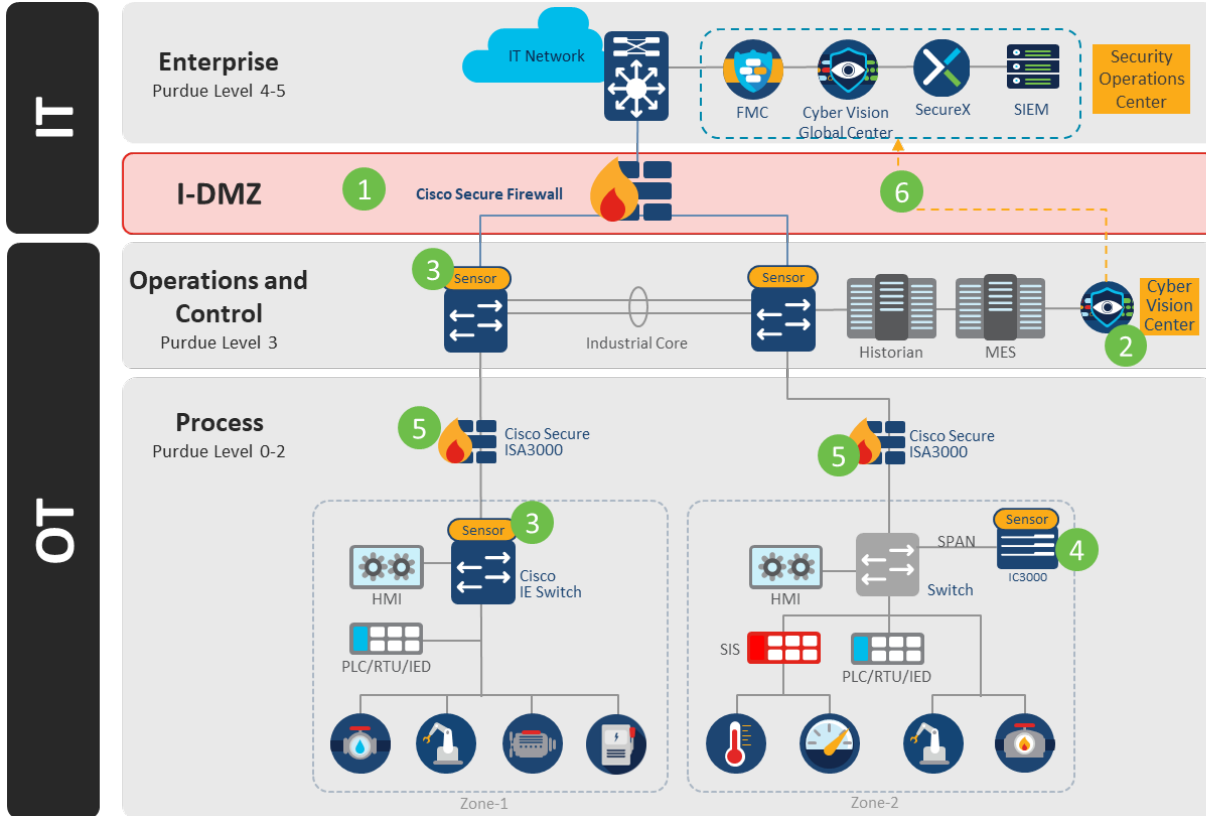


Variable Access

See which variables, objects,
setpoints are being accessed or
modified



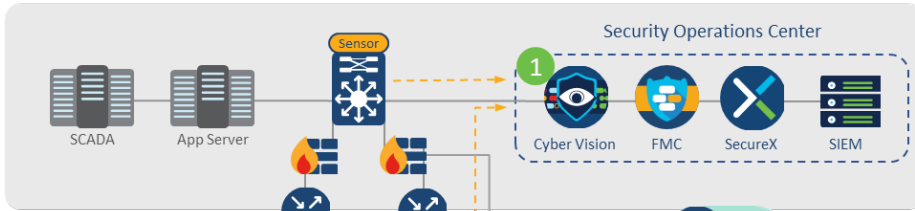
Foundational Security Architecture in Manufacturing



1. Isolate IT and OT by installing an industrial DMZ with Cisco Secure FW
2. Install Cyber Vision Sensors and Center to gain visibility on OT
3. Cyber Vision Sensors embedded on IE3400 and Catalyst 9300 switches
4. Cyber Vision hardware-sensors deployed via one-hop SPAN to gain visibility on non-Cisco switches
5. Deploy Cisco Secure ISA3000 to isolate production zones
6. Cyber Vision shares details on OT devices and events with SOC to build informed security policies and investigate threats across domains

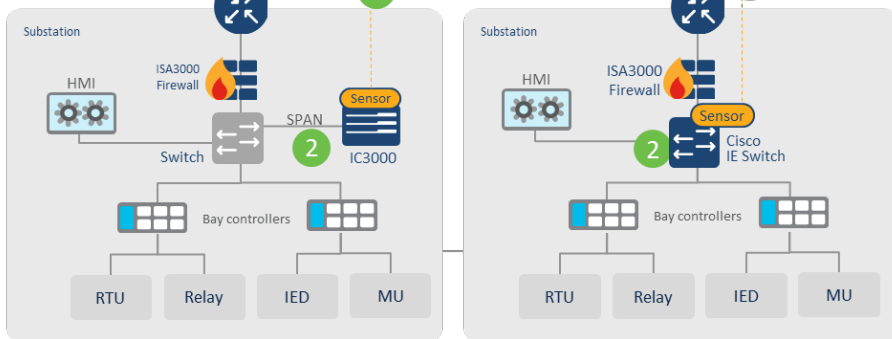
Foundational Security Architecture in Electric Utilities

Data Center / Control Center

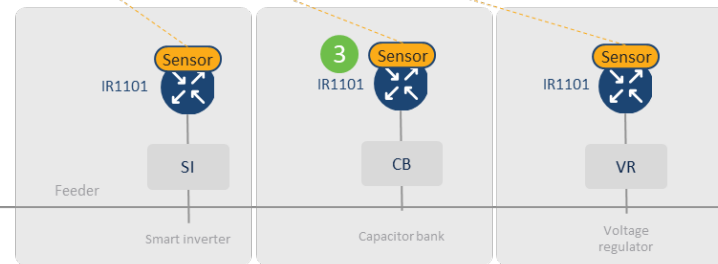


- 1 Cyber Vision Center deployed at Control center
- 2 Cyber Vision Sensor embedded in IE3400 switches or deployed via one-hop SPAN on IC3000 in transmission substations
- 3 Cyber Vision Sensor embedded in IR1101 gateways in the distribution grid
- 4 Application-flow streamed from sensors to center over utility private WAN connecting transmission substations and over cellular backhaul from the distribution grid

Transmission Grid



Distribution Grid



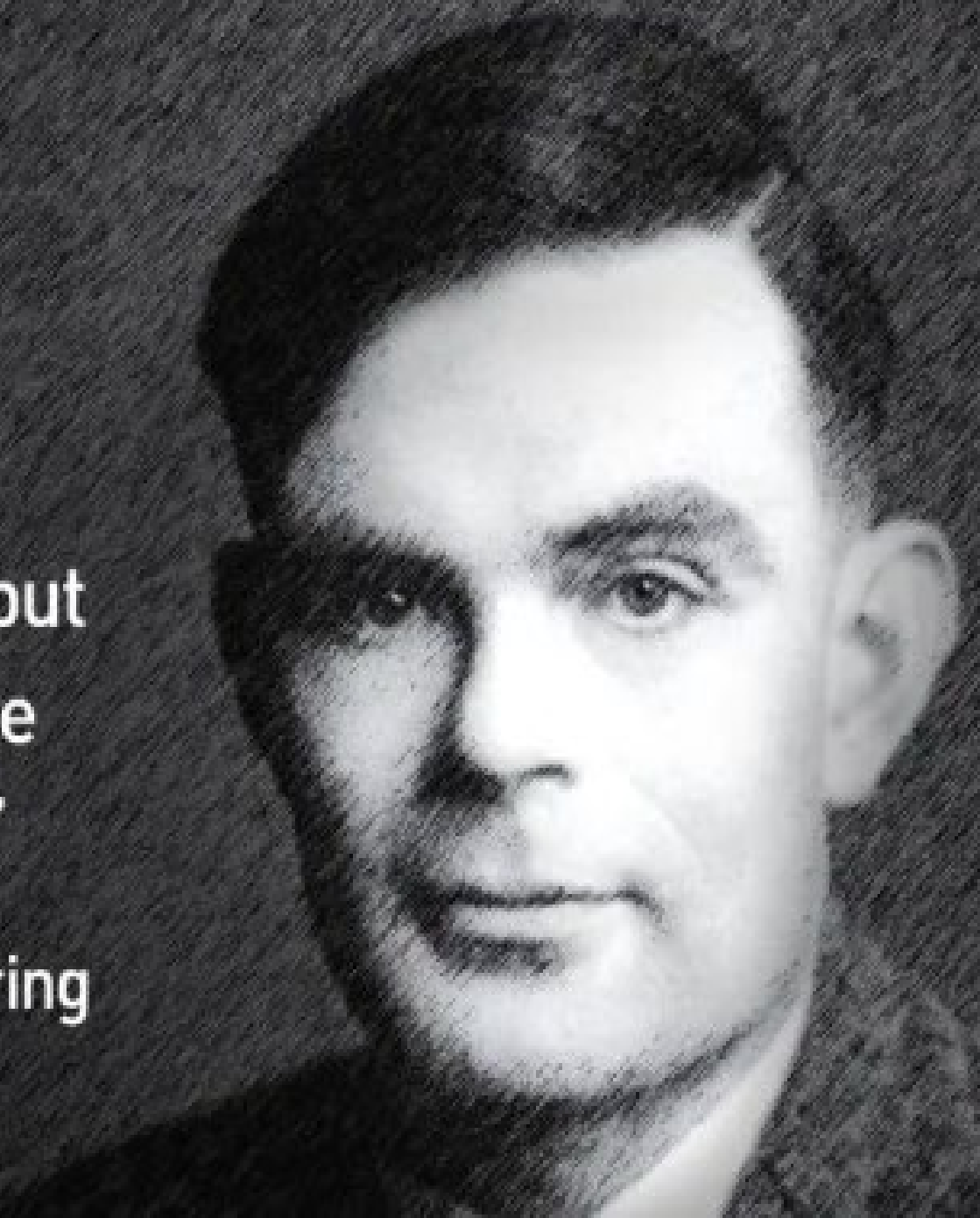
| Why Space for Partner

- 35+ years in the market
- Cisco Gold Partner
- Financially healthy ('longevity')
- Customer loyalty
- Integrated Security (holistic approach)
- Experience, know-how



“We can only see a short distance ahead, but we can see plenty there that needs to be done.”

- Alan Turing



Empowering

Your Digital Transformation Journey

Thank you for your attention

 **SPACE**

Classification ISO 27001: Public



www.space.gr