We securely connect everything to make anything possible.

CISCO

BECHTLE

cisco The bridge to possible

BECHTLE

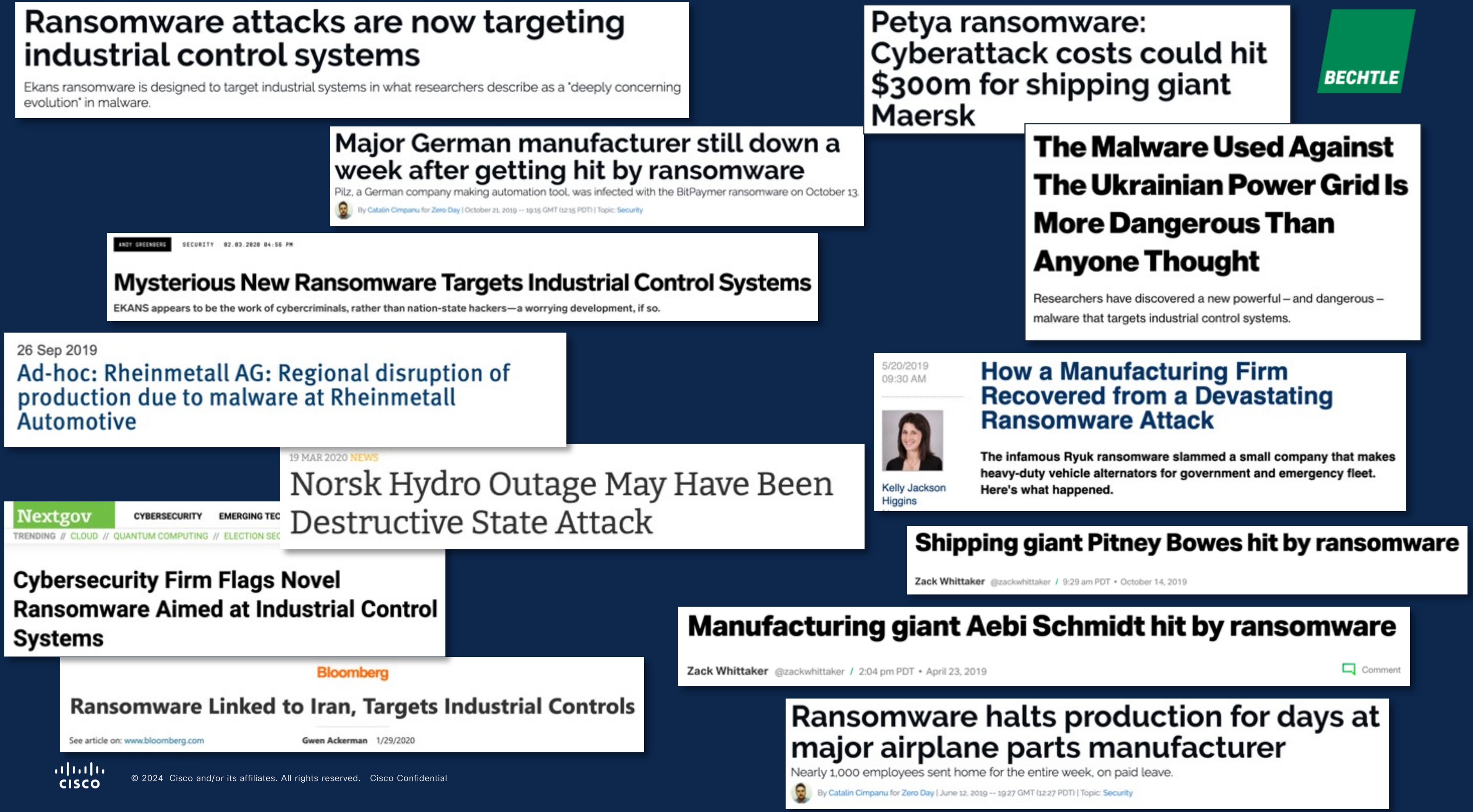
Journey to Securing Industrial Networks

Where to start?

Presenters: Christoph Koch, Cisco
Andreas Lustenberger, Bechtle

Agenda

- Introduction to OT Security
- Industrial Security Journey
- Conclusions



Ransomware attacks are now targeting industrial control systems

Ekans ransomware is designed to target industrial systems in what researchers describe as a 'deeply concerning evolution' in malware.

Major German manufacturer still down a week after getting hit by ransomware

Pilz, a German company making automation tool, was infected with the BitPaymer ransomware on October 13.

By Catalin Cimpanu for Zero Day | October 21, 2019 -- 19:15 GMT (12:15 PDT) | Topic: Security

ANDY GREENBERG SECURITY 02.03.2020 04:56 PM

Mysterious New Ransomware Targets Industrial Control Systems

EKANS appears to be the work of cybercriminals, rather than nation-state hackers—a worrying development, if so.

26 Sep 2019

Ad-hoc: Rheinmetall AG: Regional disruption of production due to malware at Rheinmetall Automotive

19 MAR 2020 NEWS

Norsk Hydro Outage May Have Been Destructive State Attack

Nextgov CYBERSECURITY EMERGING TEC

TRENDING // CLOUD // QUANTUM COMPUTING // ELECTION SEC

Cybersecurity Firm Flags Novel Ransomware Aimed at Industrial Control Systems

Bloomberg

Ransomware Linked to Iran, Targets Industrial Controls

See article on: www.bloomberg.com Gwen Ackerman 1/29/2020

Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk

BECHTLE

The Malware Used Against The Ukrainian Power Grid Is More Dangerous Than Anyone Thought

Researchers have discovered a new powerful – and dangerous – malware that targets industrial control systems.

5/20/2019 09:30 AM

Kelly Jackson Higgins

How a Manufacturing Firm Recovered from a Devastating Ransomware Attack

The infamous Ryuk ransomware slammed a small company that makes heavy-duty vehicle alternators for government and emergency fleet. Here's what happened.

Shipping giant Pitney Bowes hit by ransomware

Zack Whittaker @zackwhittaker / 9:29 am PDT • October 14, 2019

Manufacturing giant Aebi Schmidt hit by ransomware

Zack Whittaker @zackwhittaker / 2:04 pm PDT • April 23, 2019 Comment

Ransomware halts production for days at major airplane parts manufacturer

Nearly 1,000 employees sent home for the entire week, on paid leave.

By Catalin Cimpanu for Zero Day | June 12, 2019 -- 19:27 GMT (12:27 PDT) | Topic: Security

The Landscape

Typical Issues Found in Industrial Networks

Unauthorized remote access by third parties

OT network fully connected to IT

Default credentials to log into systems

Security Patches not installed

Unknown devices

Bad Firewall or Switch configuration

Firmware uploaded over FTP without Signature

Multiple Time Servers

DNS queries to Amazon

Windows XP SMBv1

Unnecessary network communications

Decommissioned assets still connected

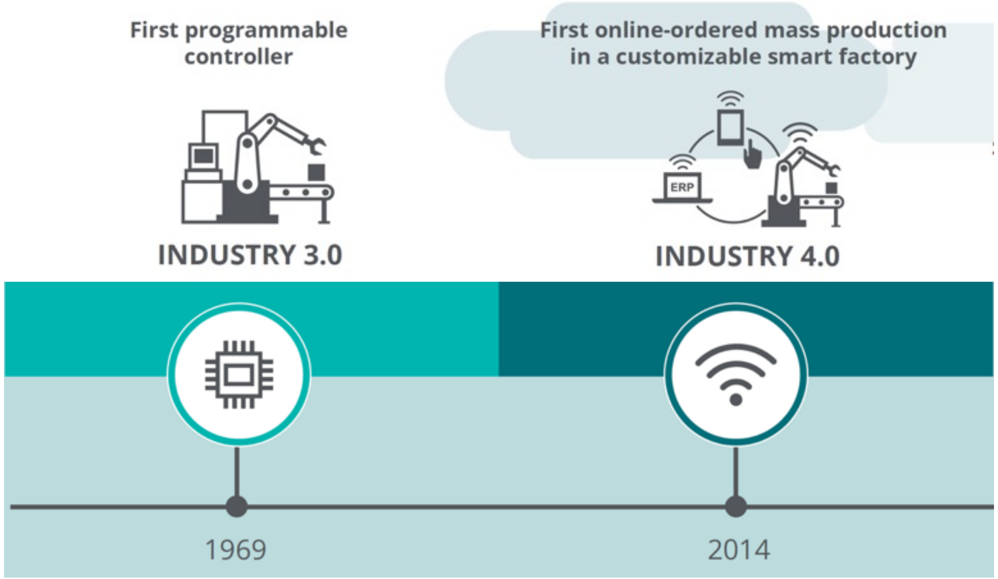
IPv6 traffic in IPv4 networks

Devices in the wrong VLAN

Malware or Virus activities

Program Upload over VPN during the night

Why is interconnected OT so hard to protect?


First programmable controller
INDUSTRY 3.0
First online-ordered mass production in a customizable smart factory
ERP
INDUSTRY 4.0
1969
2014

- Data + device proliferation
- Cloud adoption
- Increasing IT software usage
- Converging IT-OT networks

And now?

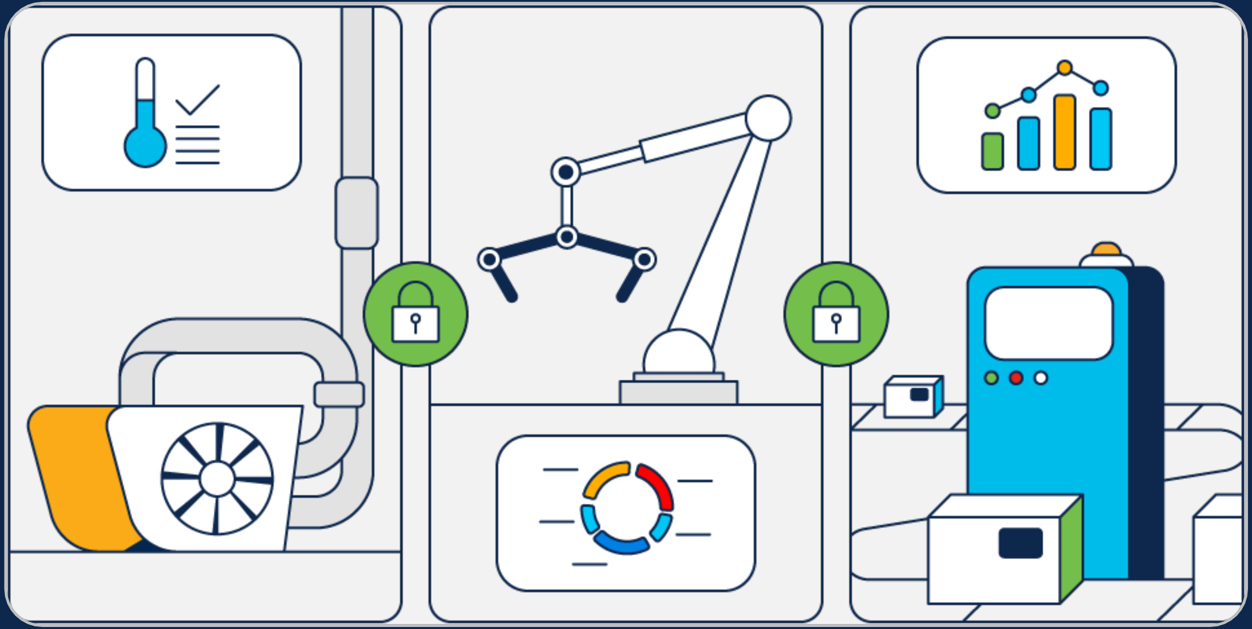
The golden ”OT Security” question

‘We need to converge our IT and OT networks, where do we start with securing our Operational Network?’

Primary Drivers

- Business demanding visibility from OT plant for efficiency and flexibility gains
- Historically ‘air-gapped’ systems are now more connected – exposing many new risks to the revenue earning parts of the business
- Systems are in place for potentially multiple decades exposing a large and weak attack surface
  - Vulnerabilities across plant and aging control systems (Windows 7 and potentially older)
- Regulations and standards to fulfill e.g.: ISA/IEC62443 or NIS2

Industrial Security Journey



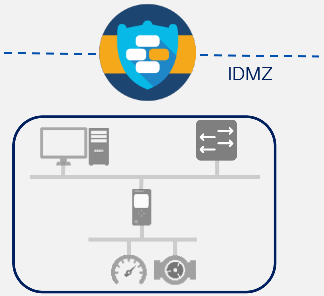
The Journey

The 4-Step Journey to Securing Industrial Networks

1 Build a Security **Foundation**

Define the IT/OT boundary with Cisco Secure Firewall

Firewall

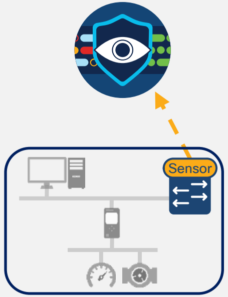


Detect, Protect, Respond

2 Gain **Visibility** & Device Posture

Network as a Sensor with Cisco Cyber Vision

Cisco Cyber Vision

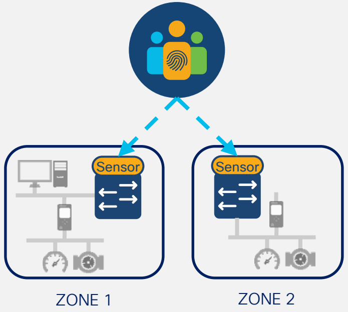


Identify, Detect

3 **Segment** Network into Smaller Zones of Trust

Network as an Enforcer with Cisco ISE

Cisco Identity Services Engine

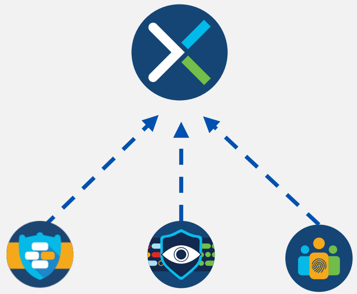


Segment, Protect, Respond

4 Integrated Incident **Investigation**

Investigate threats & orchestrate response with Cisco XDR

Cisco XDR



Investigate, Respond

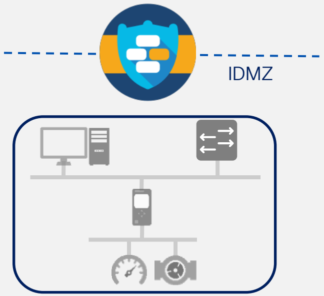
The Journey

The 4-Step Journey to Securing Industrial Networks

1 Build a Security **Foundation**

Define the IT/OT boundary with Cisco Secure Firewall

Firewall

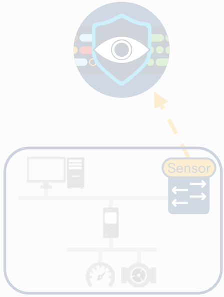


Detect, Protect, Respond

2 Gain Visibility & Device Posture

Network as a Sensor with Cisco Cyber Vision

Cisco Cyber Vision

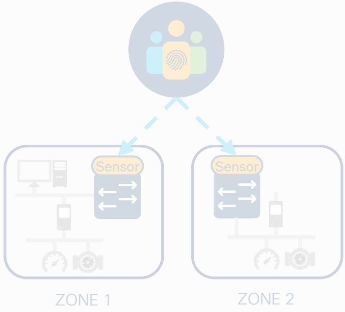


Identify, Detect

3 Segment Network into Smaller Zones of Trust

Network as an Enforcer with Cisco ISE

Cisco Identity Services Engine

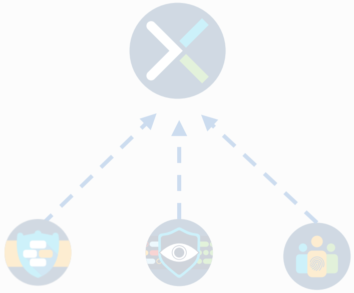


Segment, Protect, Respond

4 Integrated Incident Investigation

Investigate threats & orchestrate response with Cisco XDR

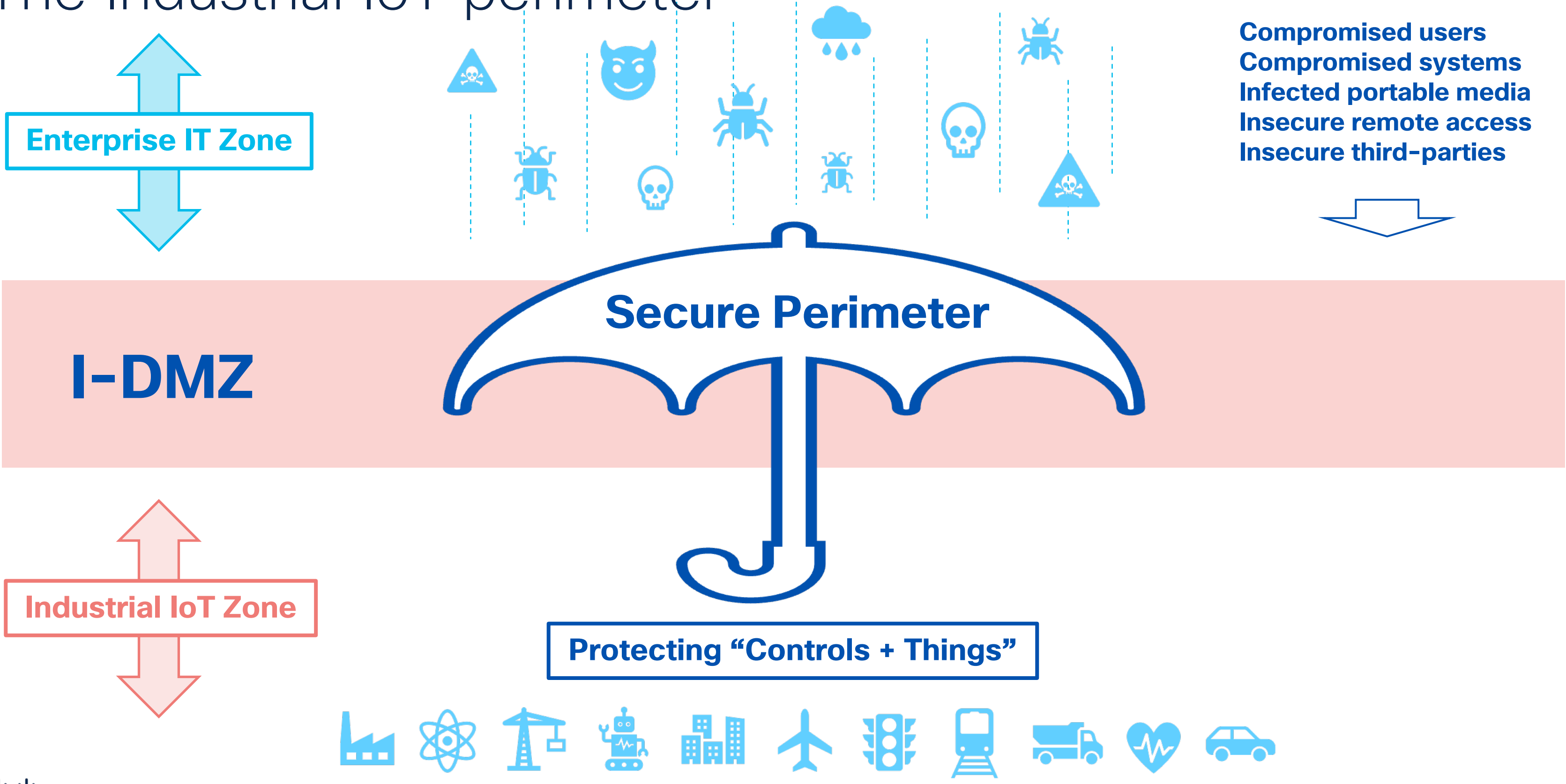
Cisco XDR



Investigate, Respond

Journey Step 1

The Industrial IoT perimeter



Compromised users
Compromised systems
Infected portable media
Insecure remote access
Insecure third-parties

Enterprise IT Zone

I-DMZ

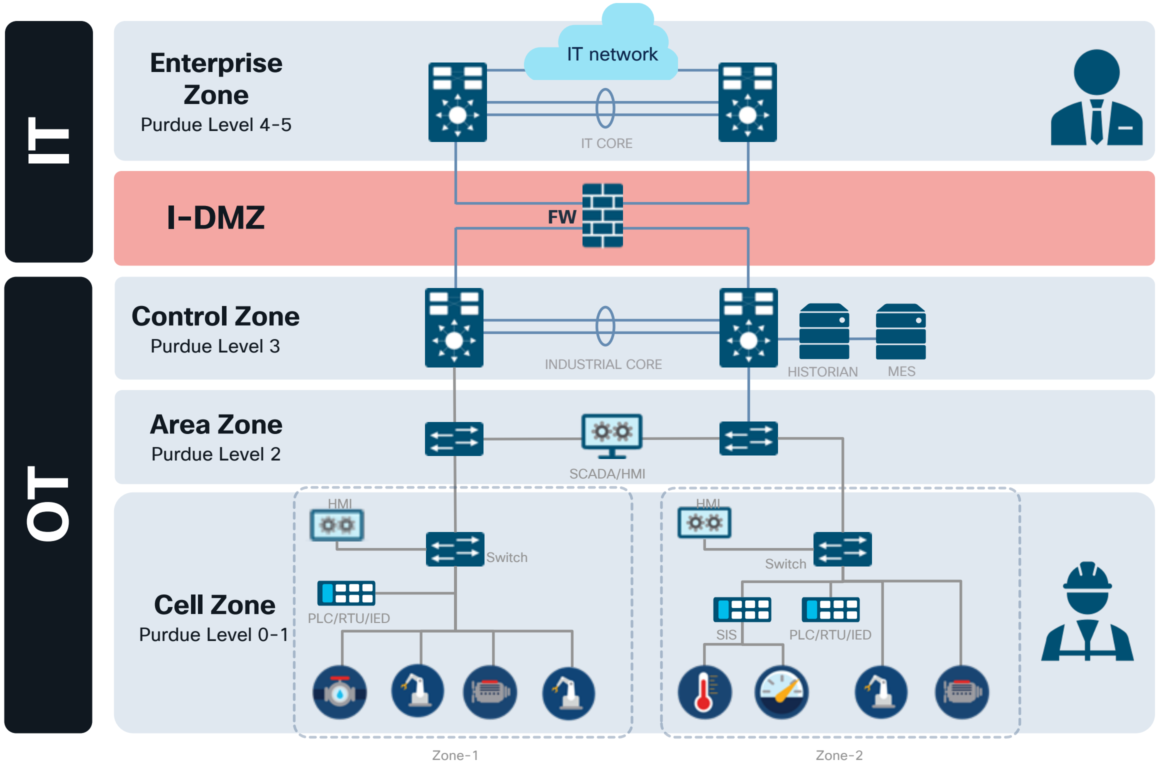
Secure Perimeter

Industrial IoT Zone

Protecting “Controls + Things”

Journey Step 1

The ISA95 model concept



How do we secure this environment that has minimal security with just an IDMZ?

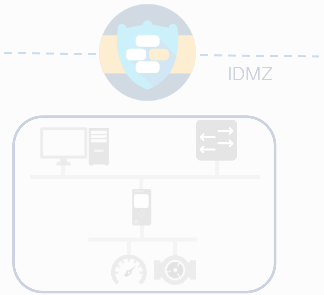
The Journey

The 4-Step Journey to Securing Industrial Networks

1 Build a Security Foundation

Define the IT/OT boundary with Cisco Secure Firewall

Firewall

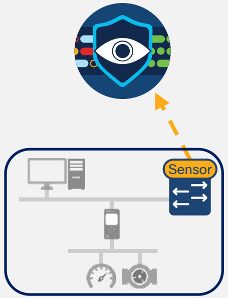


Detect, Protect, Respond

2 Gain **Visibility** & Device Posture

Network as a Sensor with Cisco Cyber Vision

Cisco Cyber Vision

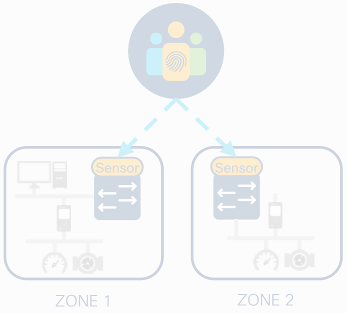


Identify, Detect

3 Segment Network into Smaller Zones of Trust

Network as an Enforcer with Cisco ISE

Cisco Identity Services Engine

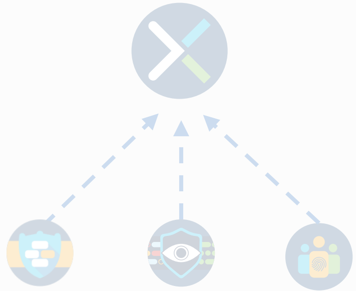


Segment, Protect, Respond

4 Integrated Incident Investigation

Investigate threats & orchestrate response with Cisco XDR

Cisco XDR



Investigate, Respond

Cisco Cyber Vision

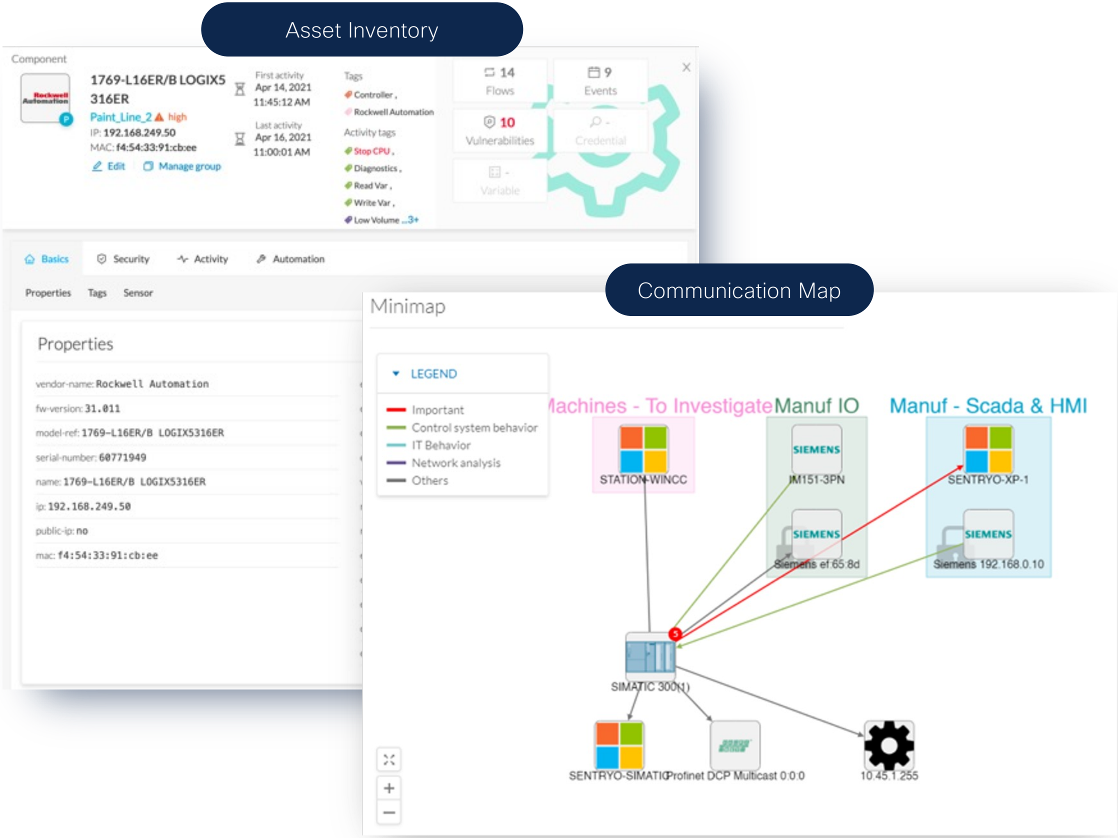
Asset Visibility

Asset Inventory

Comprehensive up to date inventory of all assets in your environment

Communication Patterns

Dynamic communication map with detailed application flow level information



Asset Inventory

Component

1769-L16ER/B LOGIX5316ER
Paint_Line_2 ⚠ high
IP: 192.168.249.50
MAC: f4:54:33:91:cb:ee

First activity Apr 14, 2021 11:45:12 AM
Last activity Apr 16, 2021 11:00:01 AM

Tags: Controller, Rockwell Automation
Activity tags: Stop CPU, Diagnostics, Read Var, Write Var, Low Volume ...3+

14 Flows
9 Events
10 Vulnerabilities
- Credential
- Variable

Properties

vendor-name: Rockwell Automation
fw-version: 31.011
model-ref: 1769-L16ER/B LOGIX5316ER
serial-number: 60771949
name: 1769-L16ER/B LOGIX5316ER
ip: 192.168.249.50
public-ip: no
mac: f4:54:33:91:cb:ee

Communication Map

LEGEND
- 🟥 Important
- 🟩 Control system behavior
- IT Behavior
- Network analysis
- Others

Cisco Cyber Vision

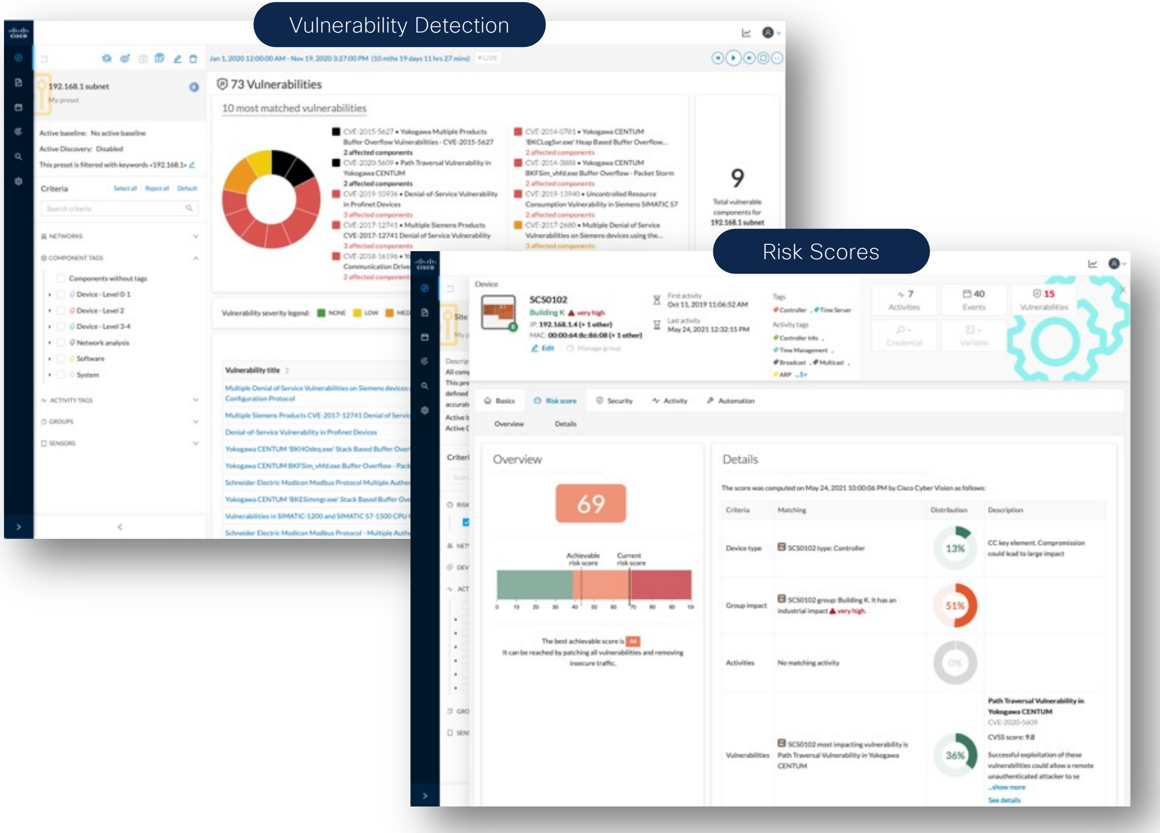
Security Posture

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



Jan 1, 2020 12:00:00 AM - Nov 19, 2020 3:27:00 PM (10 mths 19 days 11 hrs 27 mins) • LIVE

192.168.1 subnet
My preset

Active baseline: No active baseline

Active Discovery: Disabled

This preset is filtered with keywords «192.168.1»

Criteria — Select all | Reject all | Default

Search criteria

NETWORKS

COMPONENT TAGS

- □ Components without tags
- □ Device - Level 0-1
- □ Device - Level 2
- □ Device - Level 3-4
- □ Network analysis
- □ Software
- □ System

ACTIVITY TAGS

GROUPS

SENSORS

73 Vulnerabilities

10 most matched vulnerabilities

- CVE-2015-5627 • Yokogawa Multiple Products Buffer Overflow Vulnerabilities - CVE-2015-5627 — 2 affected components
- CVE-2020-5609 • Path Traversal Vulnerability in Yokogawa CENTUM — 2 affected components
- CVE-2019-10936 • Denial-of-Service Vulnerability in Profinet Devices — 3 affected components
- CVE-2017-12741 • Multiple Siemens Products CVE-2017-12741 Denial of Service Vulnerability — 3 affected components
- CVE-2018-16196 • Y… Communication Drive… — 2 affected component…
- CVE-2014-0781 • Yokogawa CENTUM 'BKCLogSvr.exe' Heap Based Buffer Overflow… — 2 affected components
- CVE-2014-3888 • Yokogawa CENTUM BKFSim_vhfd.exe Buffer Overflow - Packet Storm — 2 affected components
- CVE-2019-13940 • Uncontrolled Resource Consumption Vulnerability in Siemens SIMATIC S7 — 2 affected components
- CVE-2017-2680 • Multiple Denial of Service Vulnerabilities on Siemens devices using the… — 3 affected components

9
Total vulnerable components for 192.168.1 subnet

Vulnerability severity legend: 🟩 NONE 🟨 LOW 🟧 MED…

Vulnerability title

- Multiple Denial of Service Vulnerabilities on Siemens devices… Configuration Protocol
- Multiple Siemens Products CVE-2017-12741 Denial of Servic…
- Denial-of-Service Vulnerability in Profinet Devices
- Yokogawa CENTUM 'BKHOdeq.exe' Stack Based Buffer Over…
- Yokogawa CENTUM BKFSim_vhfd.exe Buffer Overflow - Pack…
- Schneider Electric Modicon Modbus Protocol Multiple Authe…
- Yokogawa CENTUM 'BKESimmgr.exe' Stack Based Buffer Ove…
- Vulnerabilities in SIMATIC-1200 and SIMATIC S7-1500 CPU…
- Schneider Electric Modicon Modbus Protocol - Multiple Auth…

Device

SCS0102
Building K ▲ very high
IP: 192.168.1.4 (+ 1 other)
MAC: 00:00:64:8c:86:08 (+ 1 other)
Edit | Manage group

First activity: Oct 11, 2019 11:06:52 AM
Last activity: May 24, 2021 12:32:15 PM

Tags: Controller, Time Server
Activity tags: Controller Info, Time Management, Broadcast, Multicast, ARP …1+

7 Activities | 40 Events | 15 Vulnerabilities | - Credential | - Variable

Basics | Risk score | Security | Activity | Automation

Overview | Details

Overview

69

Achievable risk score — Current risk score

The best achievable score is 44
It can be reached by patching all vulnerabilities and removing insecure traffic.

Details

The score was computed on May 24, 2021 10:00:06 PM by Cisco Cyber Vision as follows:

Criteria	Matching	Distribution	Description
Device type	SCS0102 type: Controller	13%	CC key element. Compromission could lead to large impact
Group impact	SCS0102 group: Building K. It has an industrial impact ▲ very high.	51%	
Activities	No matching activity	0%	
Vulnerabilities	SCS0102 most impacting vulnerability is Path Traversal Vulnerability in Yokogawa CENTUM	36%	**Path Traversal Vulnerability in Yokogawa CENTUM** CVE-2020-5609 CVSS score: 9.8 Successful exploitation of these vulnerabilities could allow a remote unauthenticated attacker to se …show more See details

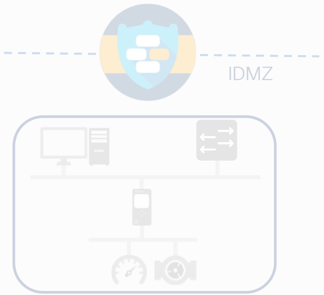
The Journey

The 4-Step Journey to Securing Industrial Networks

1 Build a Security Foundation

Define the IT/OT boundary with Cisco Secure Firewall

Firewall

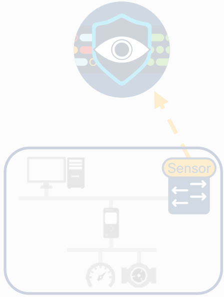


Detect, Protect, Respond

2 Gain Visibility & Device Posture

Network as a Sensor with Cisco Cyber Vision

Cisco Cyber Vision

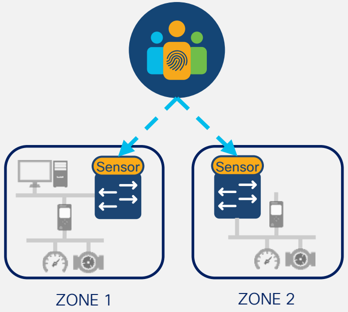


Identify, Detect

3 **Segment** Network into Smaller Zones of Trust

Network as an Enforcer with Cisco ISE

Cisco Identity Services Engine

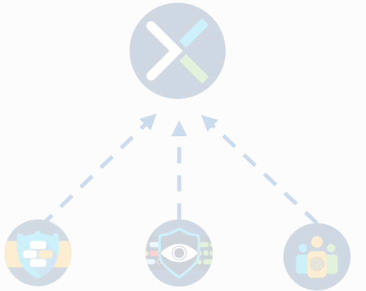


Segment, Protect, Respond

4 Integrated Incident Investigation

Investigate threats & orchestrate response with Cisco XDR

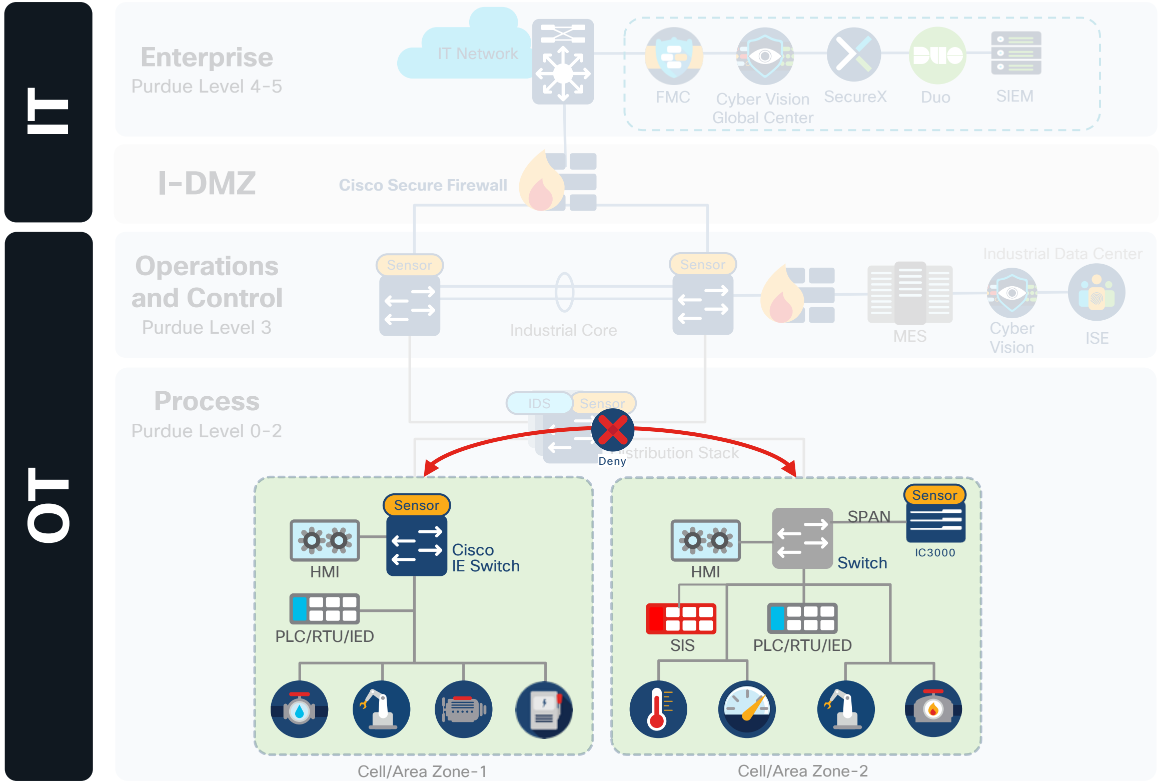
Cisco XDR



Investigate, Respond

Journey Step 3

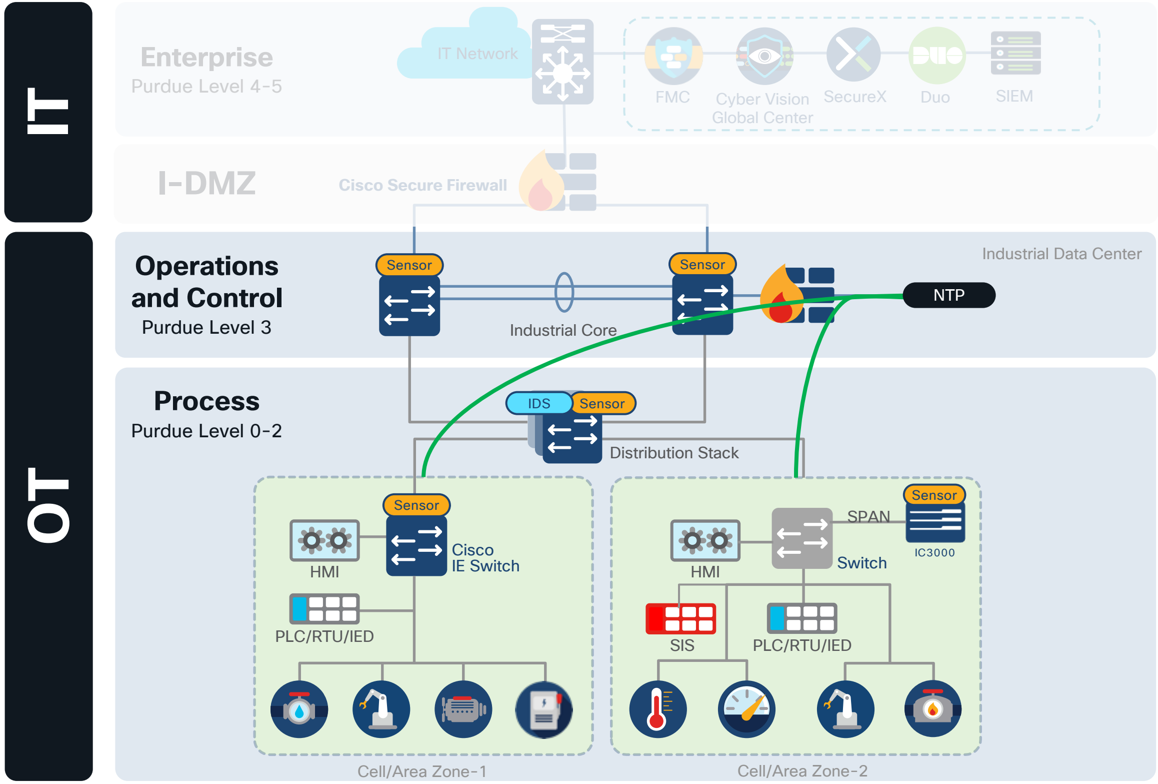
Use Case 1: Cell/Area Zone to Cell/Area Zone



- Network location has purpose in Industrial Networks
- Connectivity over Security WITHIN the zone
- Least Privilege across zones (conduit)
- Visibility in the zone is key

Journey Step 3

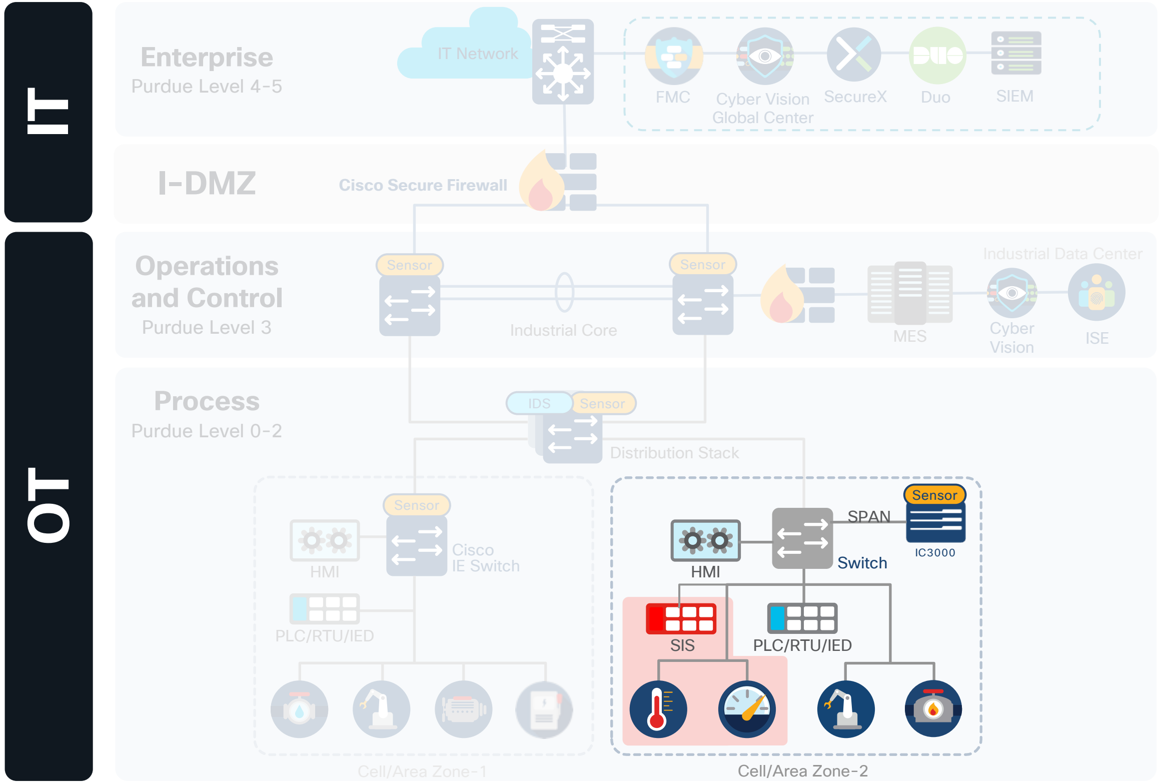
Use Case 2: Infrastructure Services in Cell/Area Zone



- Make sure to allow communication to Infrastructure Services!
- There will be a minimum set of services ALL zones need access to!
- Switch Management should be on a dedicated subnet with access to ISE for example

Journey Step 3

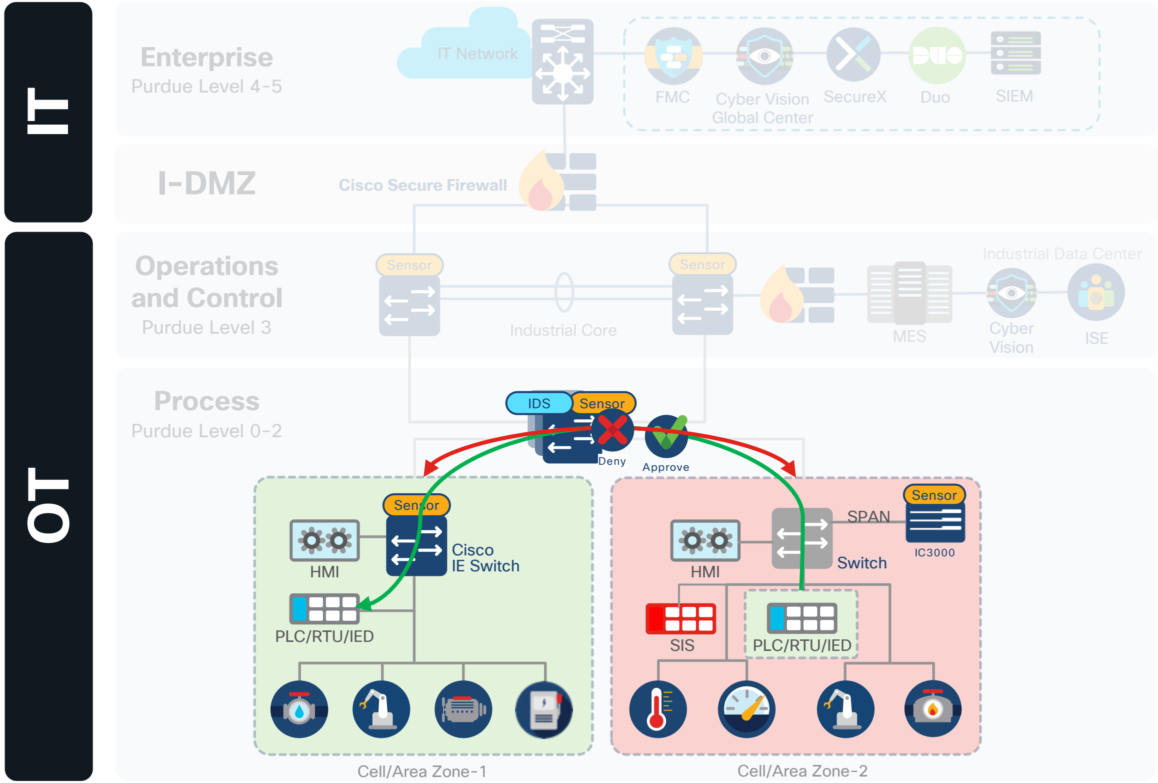
Use Case 3: Safety network air-gapped or segmented



- Safety is another Macro Zone in the network
- Logical Segmentation is possible, but ensure all routes are blocked
- Still recommended to Air-Gap from rest of network to avoid misconfiguration errors propagation

Journey Step 3

Use Case 4: Select devices, such as interlocking PLCs



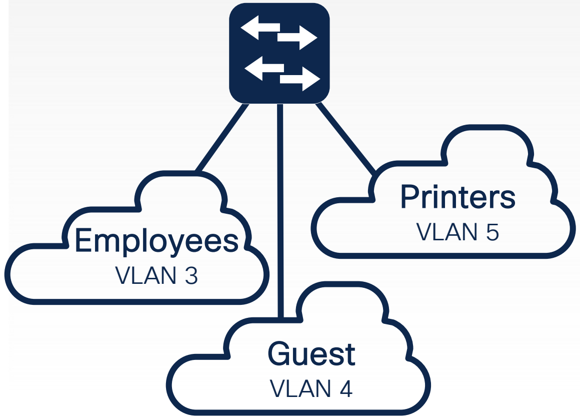
- Use cases occur where we can no longer apply policy to a Zone, but to individual devices
- Example, PLC in Cell/Area 1 sends data to PLC in Cell/Area 2
- By default, this communication would be denied

Journey Step 3

Segmentation Technologies

VLANs

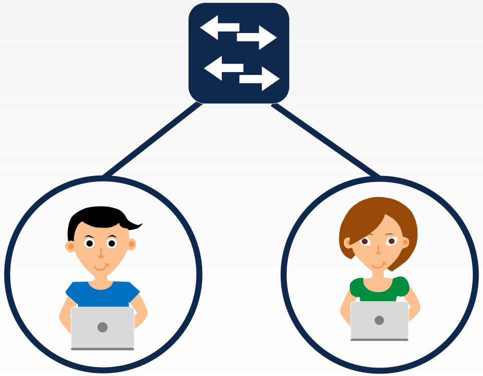
Dynamic VLAN Assignments



Per port / Per Domain / Per MAC

ACLs: DL, Named, DNS

Downloadable ACL (Wired) or
Named ACL (Wired + Wireless)



Employee

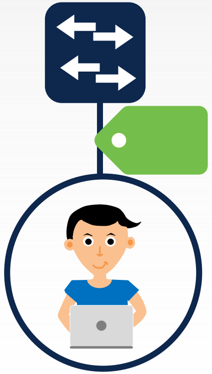
```
permit ip any any
```

Contractor

```
deny ip host <critical>
permit ip any any
```

Security Group Tags

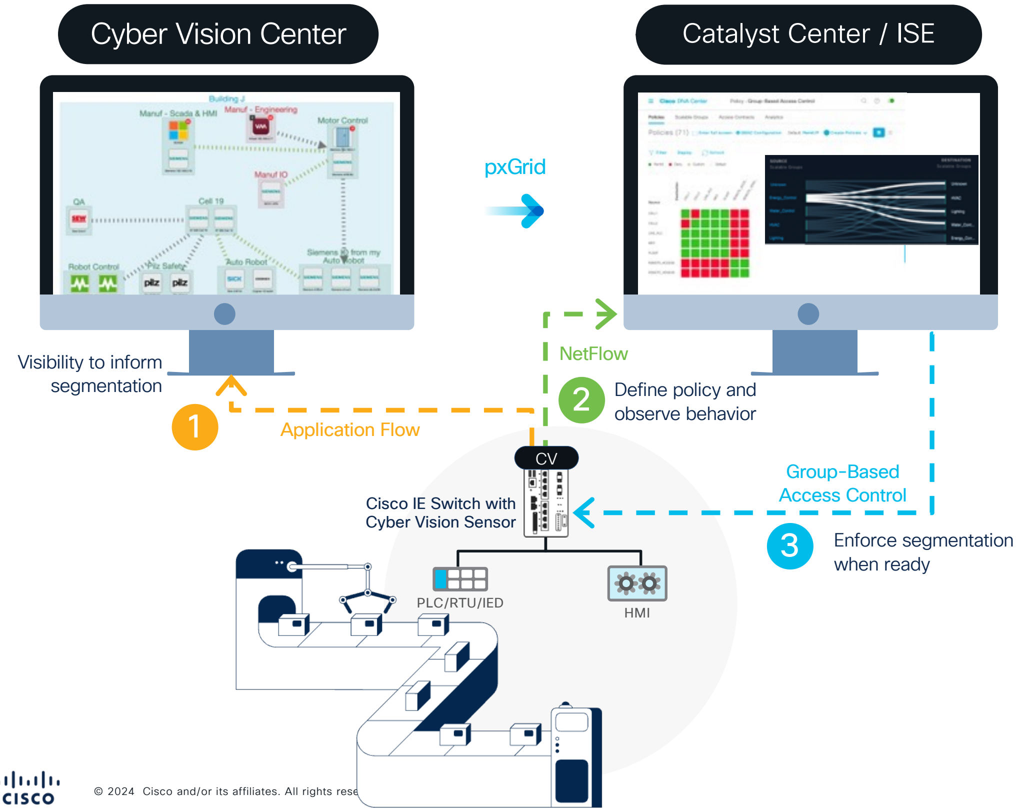
Cisco Group-Based Policy



16-bit SGT assignment and
SGT based Access Control

Journey Step 3

Use visibility to influence segmentation



Cyber Vision Center

Catalyst Center / ISE

pxGrid

NetFlow

Visibility to inform segmentation

1 Application Flow

2 Define policy and observe behavior

3 Enforce segmentation when ready

Group-Based Access Control

CV

Cisco IE Switch with Cyber Vision Sensor

PLC/RTU/IED

HMI

Visualize Zones & Conduits

visualize aggregated flows as conduits to inform segmentation policy

Dynamic SGT Mapping

Cyber Vision grouping results in dynamic Group-based policy assignment to endpoints through ISE

Monitor Before Enforcement

Visualize Group-based network behavior in Catalyst Center and enable enforcement when confident after monitoring

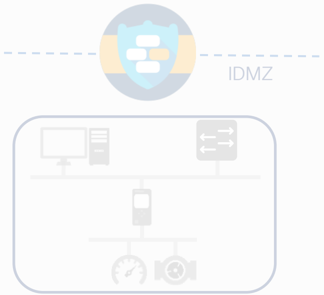
The Journey

The 4-Step Journey to Securing Industrial Networks

1 Build a Security Foundation

Define the IT/OT boundary with Cisco Secure Firewall

Firewall

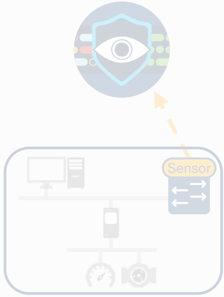


Detect, Protect, Respond

2 Gain Visibility & Device Posture

Network as a Sensor with Cisco Cyber Vision

Cisco Cyber Vision

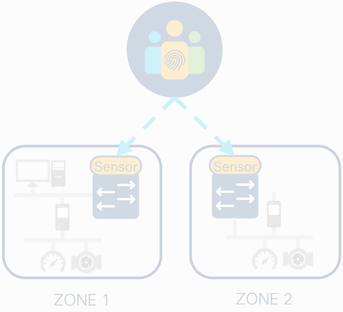


Identify, Detect

3 Segment Network into Smaller Zones of Trust

Network as an Enforcer with Cisco ISE

Cisco Identity Services Engine

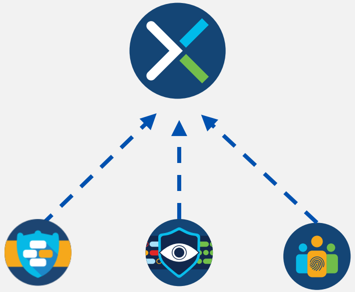


Segment, Protect, Respond

4 Integrated Incident **Investigation**

Investigate threats & orchestrate response with Cisco XDR

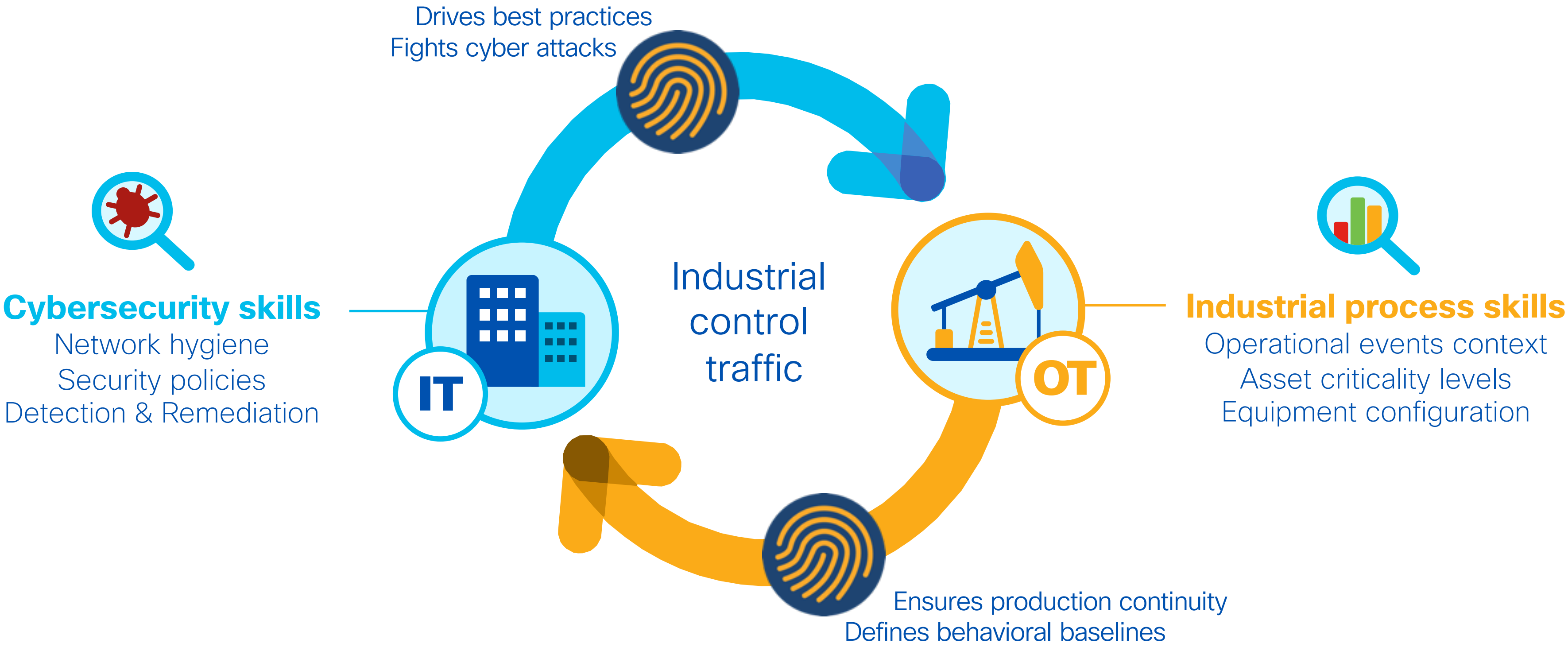
Cisco XDR



Investigate, Respond

Journey Step 4

IT – OT collaboration is vital to ICS security



Closing

What Bechtle and Cisco can do for you?

Closing

All steakholders need OT visibility

OT

Gain **visibility** into assets and processes to **reduce downtime**

IT

Identify **risks** to drive **segmentation** and reduce the **attack surface**

CSO

Get **OT context** so IT security tools can **enforce security policies**

Visibility drives segmentation, operational efficiency, and converged security

Closing

Need Help with OT Security

Organizational

- Operational Maturity & Technical Security Assessments
- Security Architecture Framework
- Security Strategy, Risk and Compliance Services

Technical

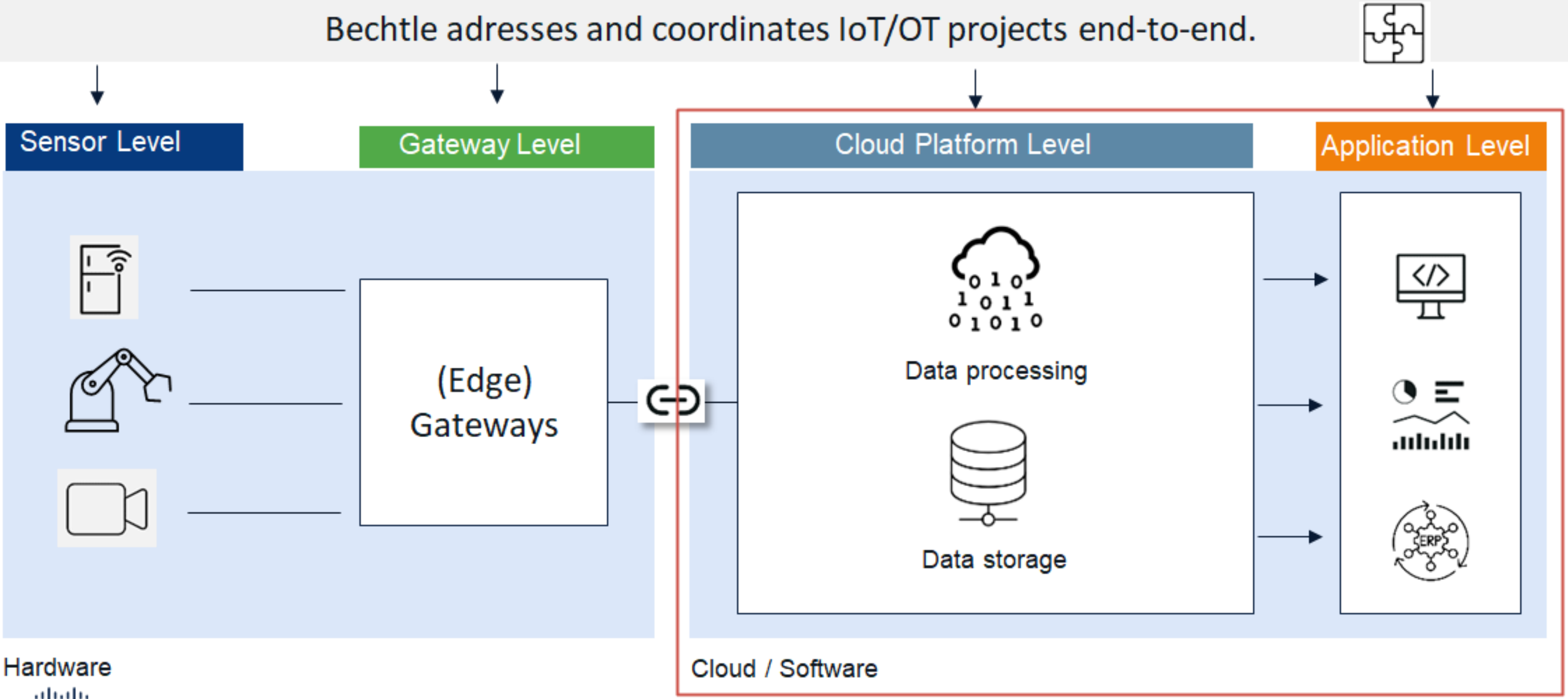
- Network segmentation design and implement Services
- Design and implement zero-trust infrastructures Services
- Cisco IIoT security solution planning, design and implementation Services

Operational

- Incident Response Services
- Cybersecurity operations optimization services
- Continuous post-deployment assessment and solution maintenance Services

IoT/OT Projects: We focus on platform and application levels

Bechtle adresses and coordinates IoT/OT projects end-to-end.



Our Offer

Consultancy and planning - Implementation of workshops.

Integration of existing and new systems.

Operation and maintenance/services.

Education and training.

Resources for consumption

Best practices & Design guides

Cisco Validated Design

Tested Implemented Proven

Networking and Security in Industrial Automation Environments Design and Implementation Guide

Cisco DNA Center for Industrial Automation Design Guide

Industrial Security Design Guide

End-End Architecture

CVDs start with the customer use cases and architecture from the edge device to the application, validating the key Cisco and 3rd party components

Best Practices

Document best practices so you can confidently set performance expectations

Reliability

Reduce risk products won't work together or perform as promised

Comprehensive

Provide tested system designs and configuration instructions

The bridge to possible

Thank you