Kybernetická bezpečnost v prostředí IoT sítí

Jiří Rott

19.5.2020

Agenda

01 Why Cybersecurity in IoT

02 Architecture importance

03 Cisco Cyber Vision

© 2020 Cisco and/or its affiliates. All rights reserved.

Defining Operation Technology (OT)

OT is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events
(Source: Gartner)

Operation Technology Monitors Physical States

© 2020 Cisco and/or its affiliates. All rights reserved.

OT Components

Industrial Devices (aka “things”)

- Valves
- Pumps
- Sensors
- Thermostats
- Machines
- Robots
- Motors
- Boilers

and so much more

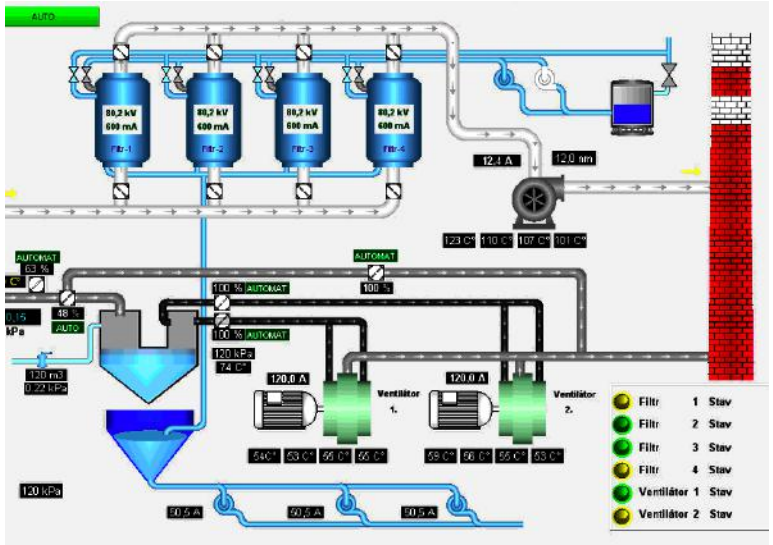
Industrial Control Systems

- Remote Terminal Units (RTU)
- Programmable Logic Controllers (PLC)
- Intelligent Electronic Devices (IED)
- Supervisory Control and Data Acquisition (SCADA)
- Distributed Control Systems (DCS)
- Human Machine Interfaces (HMI)

© 2020 Cisco and/or its affiliates. All rights reserved.

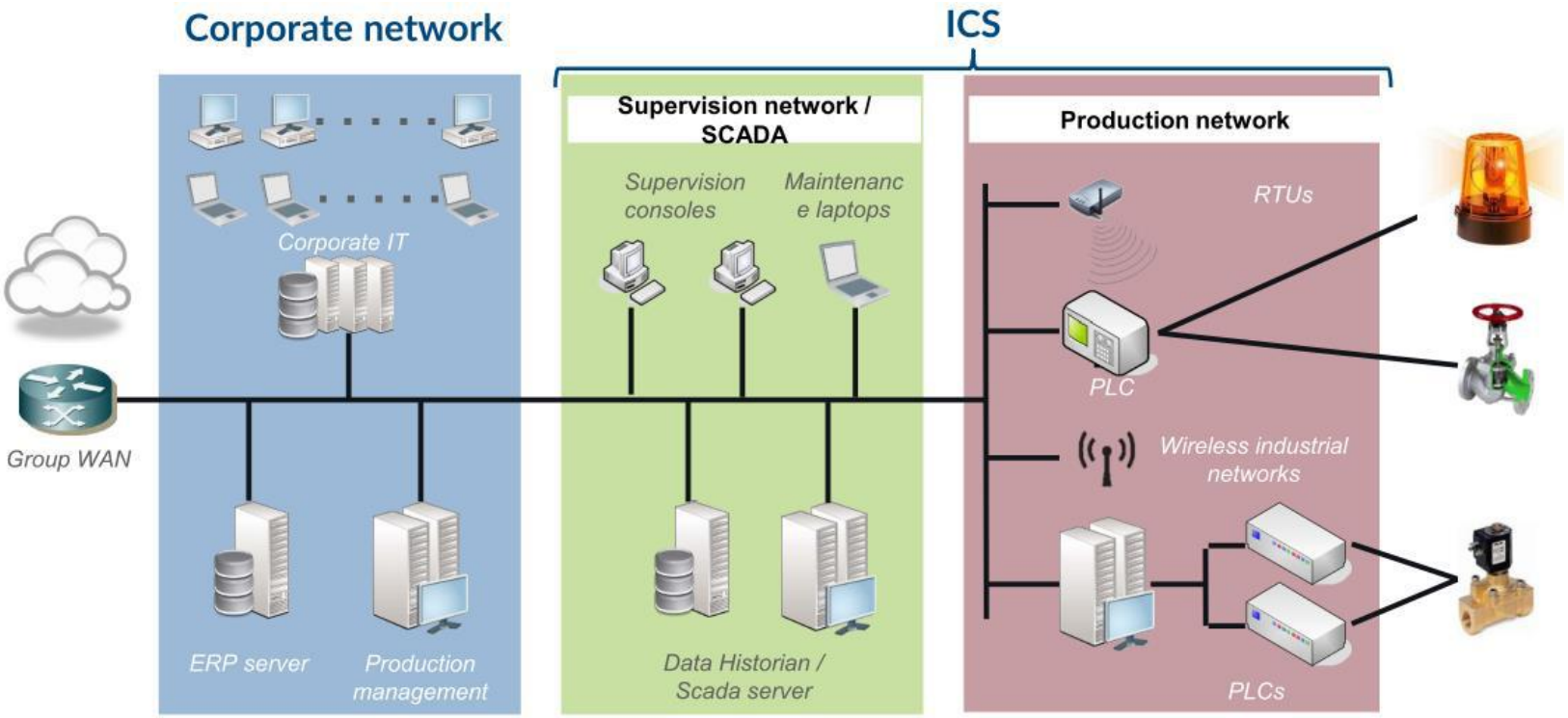
SCADA Systems

- SCADA: Supervisory Control And Data Acquisition
- Software platforms where control engineers monitor and manage processes
- This is only the supervision part but tends to be used as a synonym of ICS



© 2020 Cisco and/or its affiliates. All rights reserved.

Typical Industrial Control System (ICS)



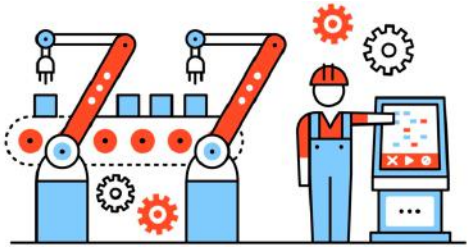
© 2020 Cisco and/or its affiliates. All rights reserved.

Customer Challenges

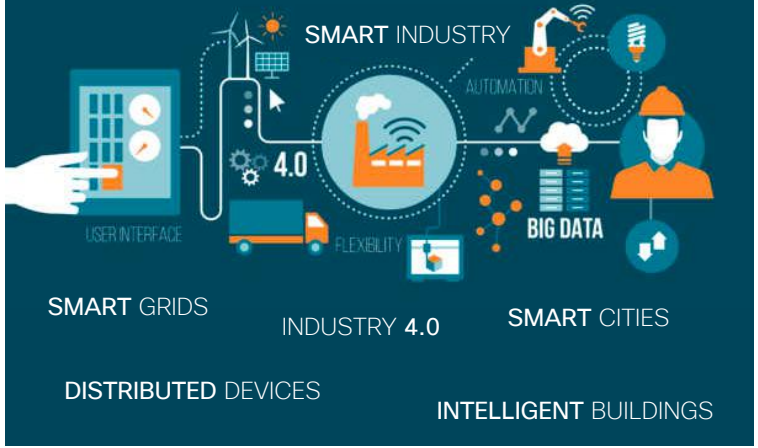
Industry **Digitization** Increases The **Attack Surface**

TODAY
Traditional automation systems

Energy, Manufacturing, Transportation, Process



TOMORROW
The Industrial Internet of Things



Industrial Control Systems are not designed for cybersecurity

© 2020 Cisco and/or its affiliates. All rights reserved.

OT & IT Have **Different Requirements**

- Security = Cybersecurity

(Knowhow is the heritage)

- IT teams manage data
- IT equipment are known, modern and controlled
- IT attacks can be well identified (virus, worms, DoS, etc.)

- Security = Safety *(Production 1st !!!)*
- OT teams manage processes that cannot be turned on/off easily
- OT assets are 10-20 years old
- OT attacks look like legitimate instructions to OT assets

Extending IT security to OT requires specific skills and features

© 2020 Cisco and/or its affiliates. All rights reserved.

Industrial systems are not designed for cybersecurity

What OT professionals tell us

What we see during assessments

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

© 2020 Cisco and/or its affiliates. All rights reserved.

Examples of Recent OT Attacks

2010

Stuxnet causes damages to Iran's nuclear program

2015

Ukrainian power grid is attacked, and almost 250k people are in the dark

2017

Ransomware attacks by Wannacry and NotPetya cause losses of more than $1B

2019

Norsk Hydro is shutdown because of ransomware

What's next ?

This is still a relatively new domain compared to IT security and attacks

© 2020 Cisco and/or its affiliates. All rights reserved.

Challenges of securing industrial networks

Skills Shortage

How to streamline OT cybersecurity tasks with existing OT and IT staff?

Growing Threats

53% of industrial companies have already suffered cyber attacks. Are you ready?

Source: IBM report 2017

Compliance

Must comply with new regulatory constraints (NERC CIP, EU-NIS...) and show shareholders that risks are under control

Agility

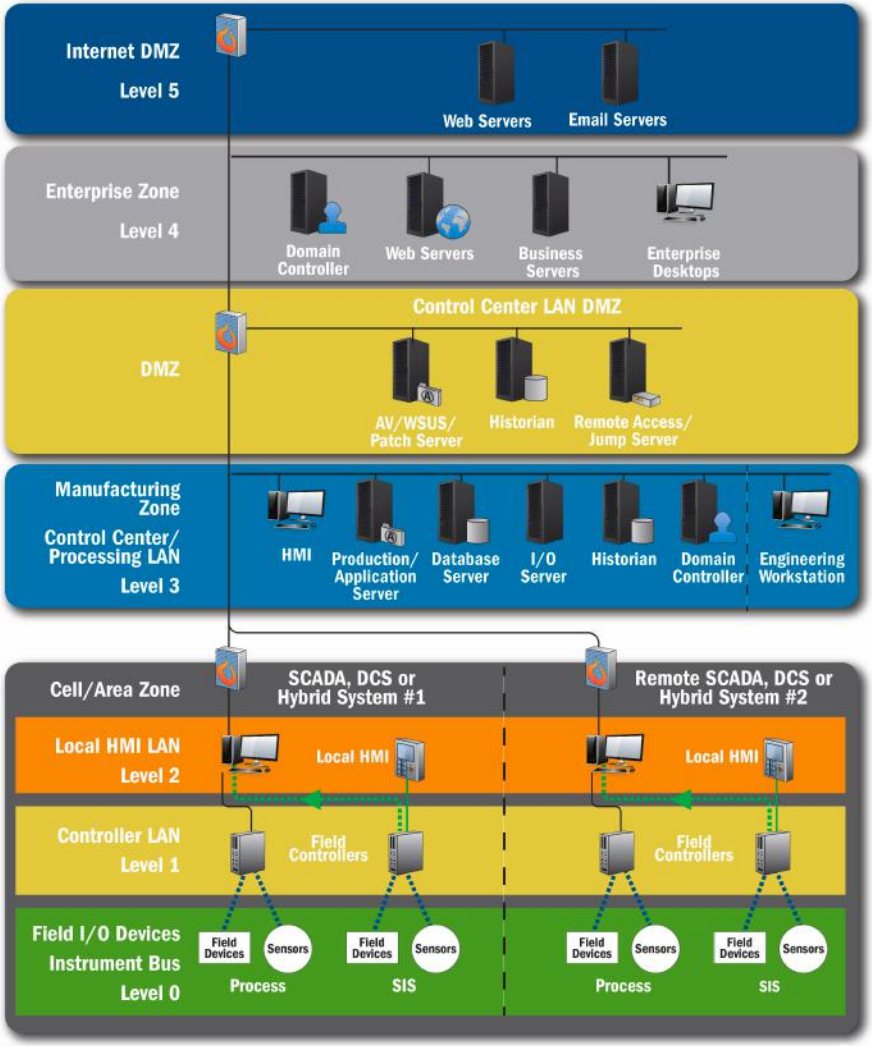
Converging OT & IT securely to capture the benefits of industry digitization

© 2020 Cisco and/or its affiliates. All rights reserved.

Architecture importance

Defining the Purdue Model

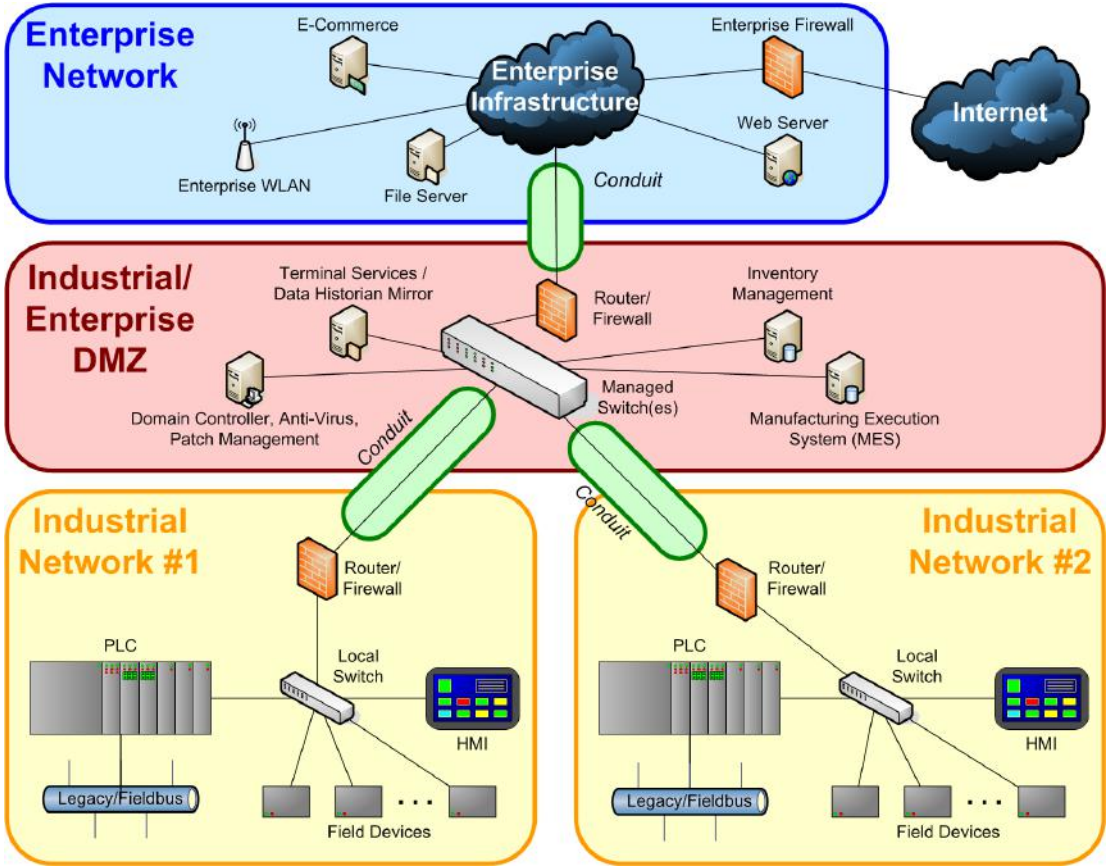
- Architecture of enterprise networks with industrial control systems
- Level 0 is the closest to the industrial process, level 5 is the closest to the IT network



© 2020 Cisco and/or its affiliates. All rights reserved.

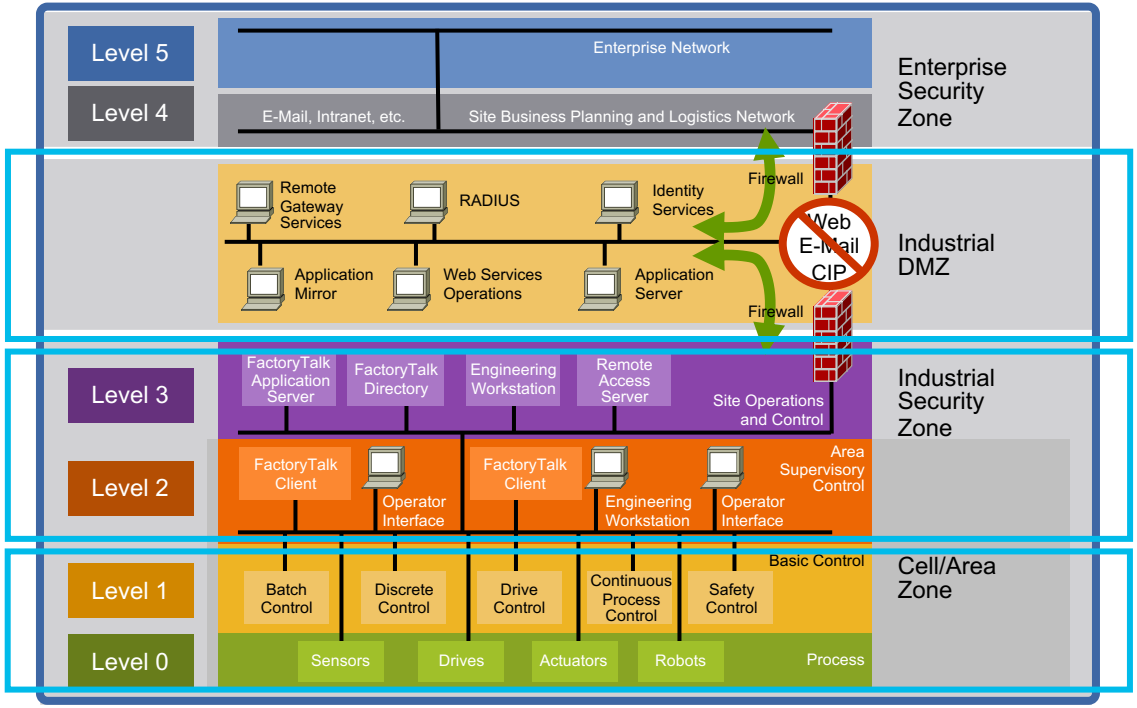
ISA-99/IEC-62443 Zones and Conduits

- A network & system segmentation technique
- Prevents the spread of an incident
- Provides a front-line set of defenses
- The basis for risk assessment in system design



© 2020 Cisco and/or its affiliates. All rights reserved.

Typical Cyber security usecases



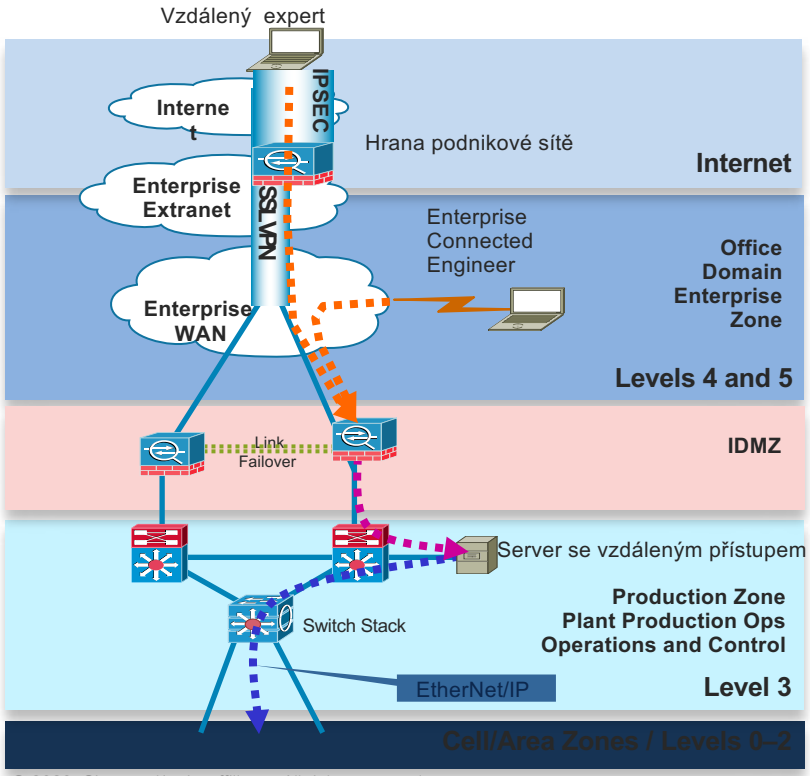
Connected Factory: IDMZ a Vzdálený přístup

Connected Factory: Identity Services

Connected Factory: NAT

© 2020 Cisco and/or its affiliates. All rights reserved.

Vzdálený přístup experta přes podnikovou síť



© 2020 Cisco and/or its affiliates. All rights reserved.

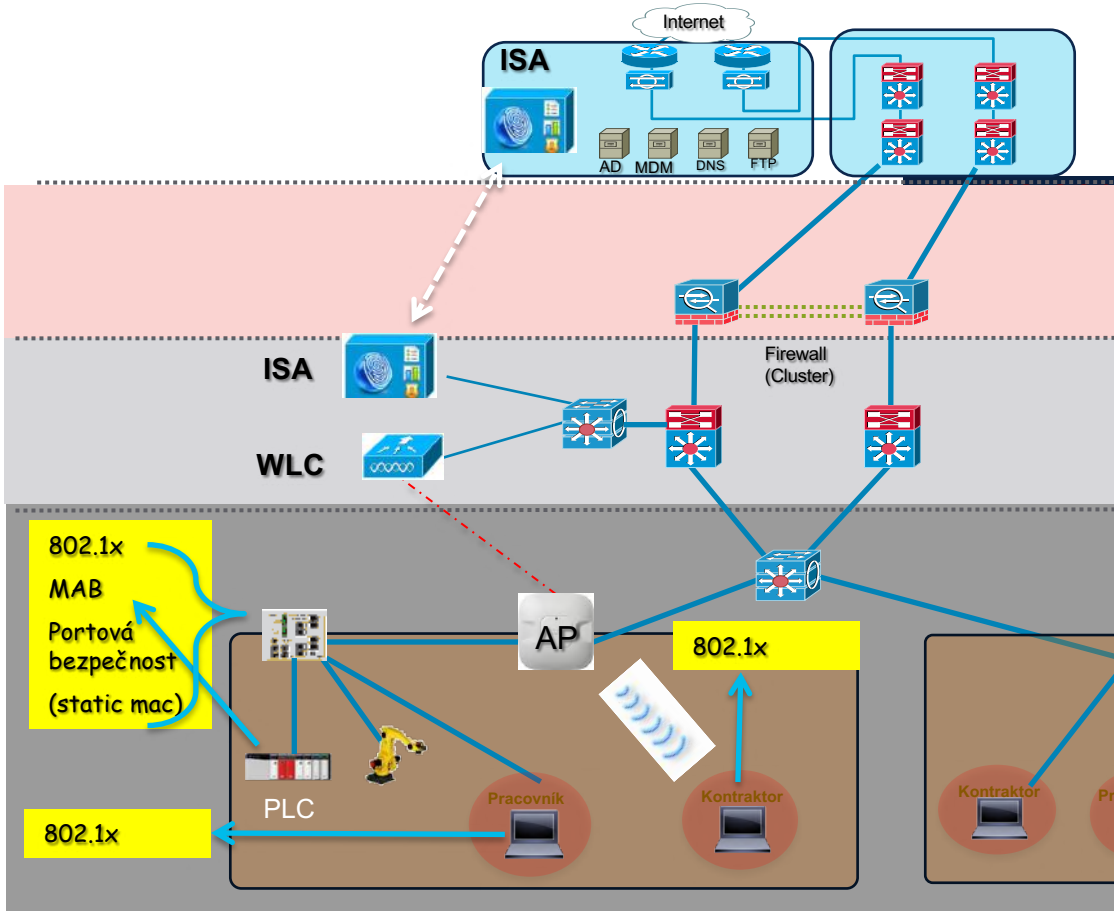
Proč ?

- Centrální zabezpečená hrana sítě
- Visibilita komunikace, logování
- Základní síťové bezpečnostní prvky FW, IPS
- Centralizovaná správa identit
- Dostupnost služby
- Škálování
- Omezení rizikových operací

Jak ?

- Správná pravidla DMZ i IDMZ
- Zabezpečený průchod sítí
- IT a OT efektivní komunikace
- Architekturní přístup

Zavedení Identity – 802.1x



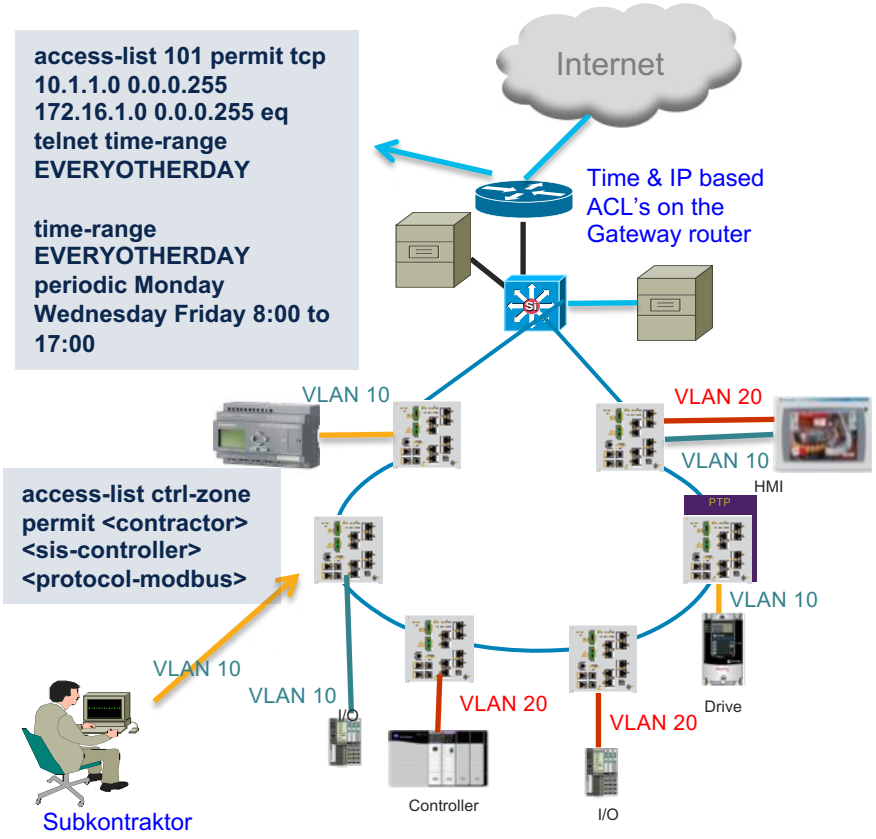
Proč Identita?

- Povolit pouze známá zařízení
- Omezit počet zařízení, které smí být připojeny k portu
- Zabránit přípojení neznámých zařízení

Jak ?

- Nastavit 802.1x ověření na portech přístupových přepínačů
- Použití MAB pro prvky (IoT) nedisponující suplikantem 802.1x
- Portová bezpečnost se statickou mac adresou pro statické koncové prvky

Omezení přístupu k síťovým zdrojům



Proč omezovat zdroje?

- Blokování přístupu zdrojů, které nejsou určeny pro správu – podniková síť, zařízení od jiných dodavatelů
- Blokování přístupu partnerů pro využití řídící sítě k přístupu do internetu

Jak?

- Použití VLAN's – konfigurace s přístupových portů do stejne VLAN
- Přístupové seznamy podle IP & VLAN na přístupových prepínačích dovolit přístup do příslušné VLAN nebo IP adresy
- Přístupové seznamy dle času & IP na přístupovém smerovači pro zabránění přístupu do internet/websites

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Cyber Vision

Acquisition of Sentryo

Cisco Cyber Vision

Asset Inventory & Security Platform for the Industrial IoT

ICS Visibility

Asset Inventory
Communication Patterns
Device Vulnerability

Operational Insights

Identify configuration changes
Record control system events
relevant to the integrity of the system

Threat Detection

Behavioral Anomaly Detection
Signature based IDS
Real-time alerting

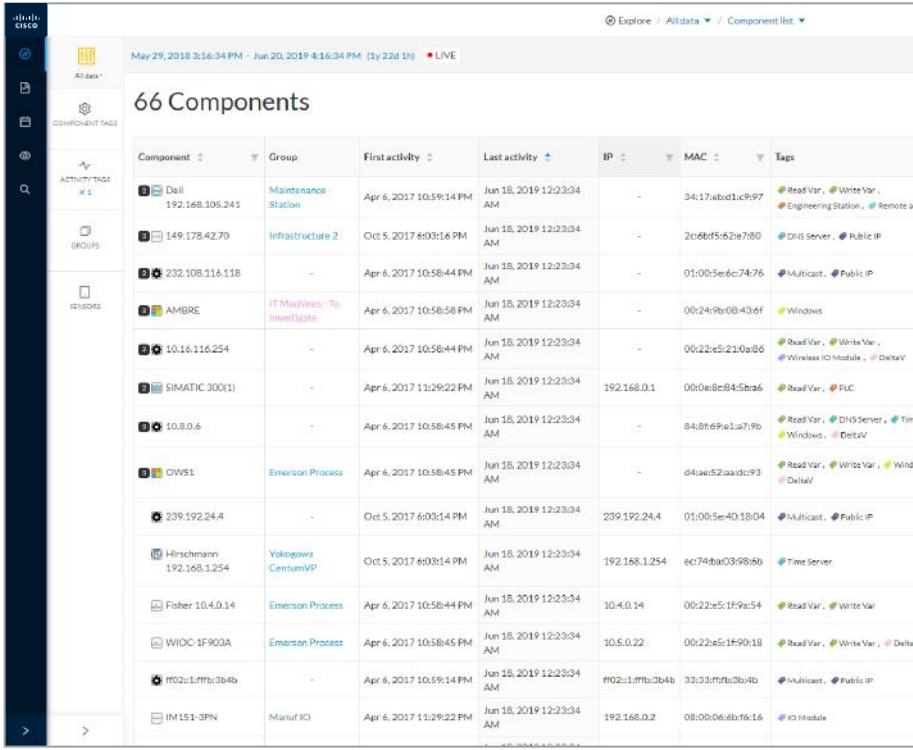
Cisco Cyber Vision helps companies protect
their industrial control systems against cyber risks

© 2020 Cisco and/or its affiliates. All rights reserved.

Visibility: Comprehensive **asset inventory**

- Automatically maintain a detailed list of all OT & IT equipment
- Immediate access to software & hardware characteristics
- Track rack-slot components
- Tags make it easily to understand asset functions and properties

Track the industrial assets to protect throughout their life cycles

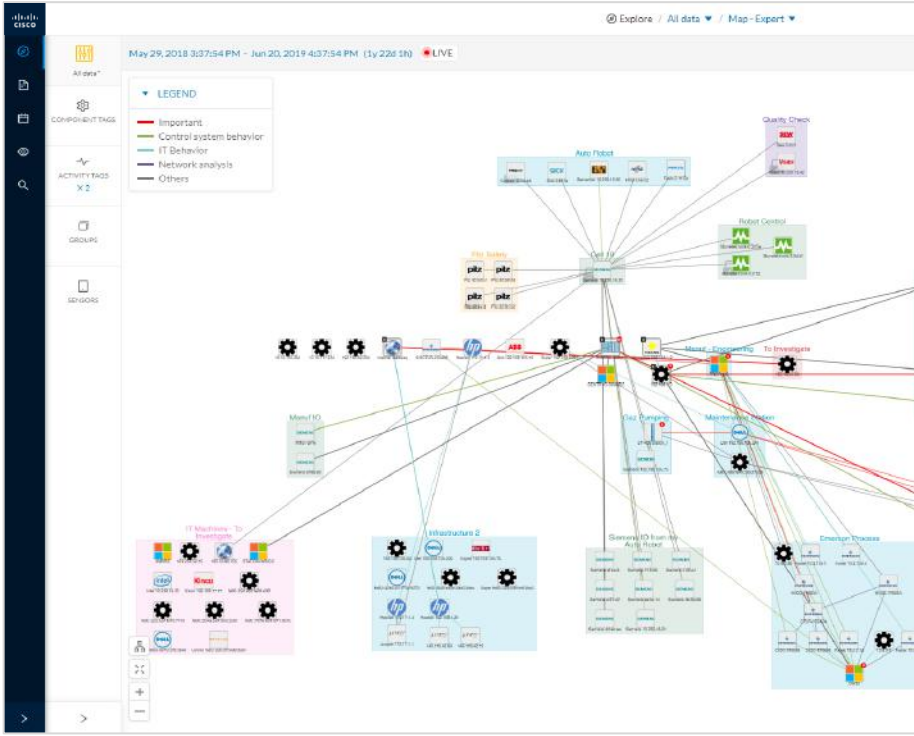


© 2020 Cisco and/or its affiliates. All rights reserved.

Visibility: Track **application flows**

- Identify all relations between assets including application flows
- Spot unwanted communications & noisy assets
- Tags make it easily to understand the content of each communication flow
- View live information or go back in time

Drive network segmentation and fine-tune configurations



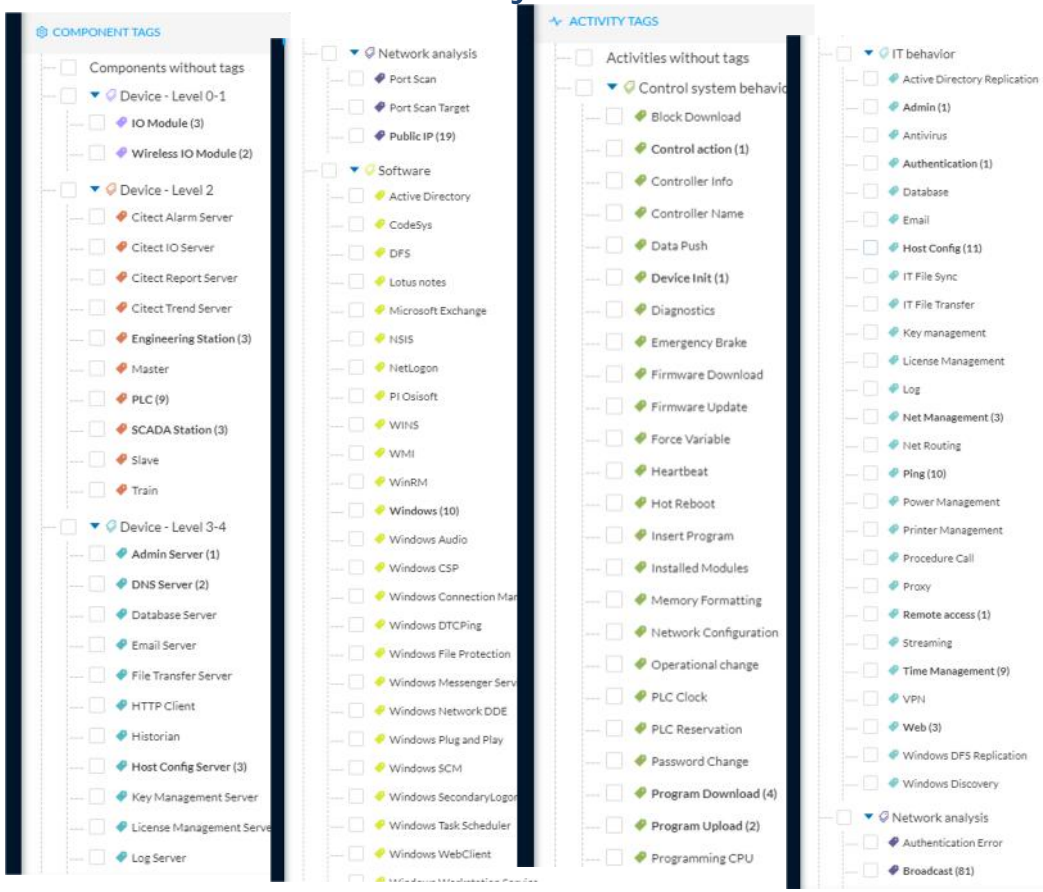
© 2020 Cisco and/or its affiliates. All rights reserved.

Cyber Vision tags to drive data analysis

Cyber Vision
Universal OT Language

- Asset characteristics and communications are translated to Tags any user can understand
- A common language, whatever the vendor reference
- Users do not need to be protocol experts to understand what is going on
- Automatically assigned based on behaviors and device information
- New tags can be added via RESTful API

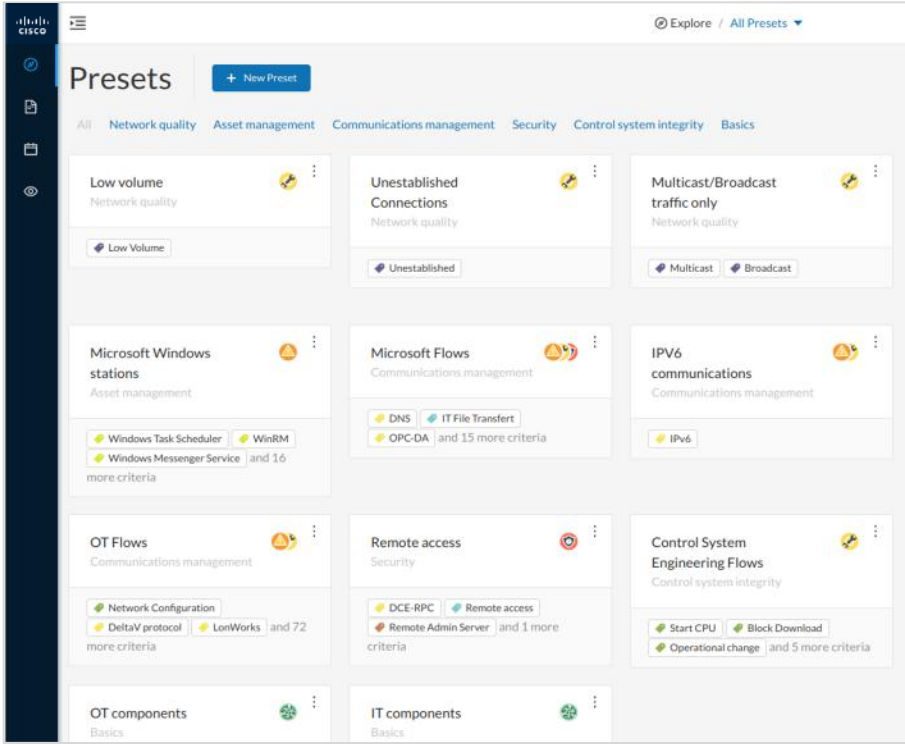
Quickly see asset and communication information in standard format



Visibility: **Guided data discovery** via presets

- Filtered views based on Tags you want to track
- Deep-dive into very large datasets with ease
- Share presets with other users to show your discoveries & enable collaboration
- System has predefined presets and the ability for users to create presets

Focus on what is most important to you

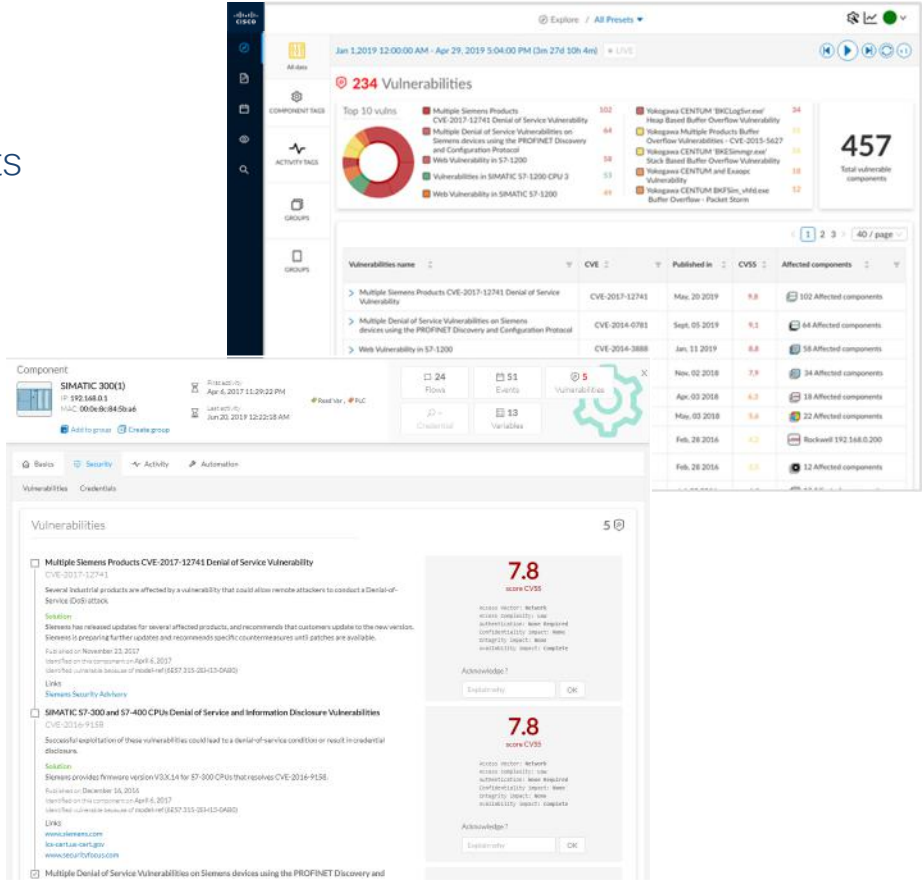


© 2020 Cisco and/or its affiliates. All rights reserved.

Visibility: Instantaneous **vulnerability** identification

- Automatically spot software & hardware vulnerabilities across all your industrial assets
- Access comprehensive information on vulnerability severities and solutions
- Built-in vulnerability database curated by Cisco Research Teams always up to date

Enforce cyber best practices

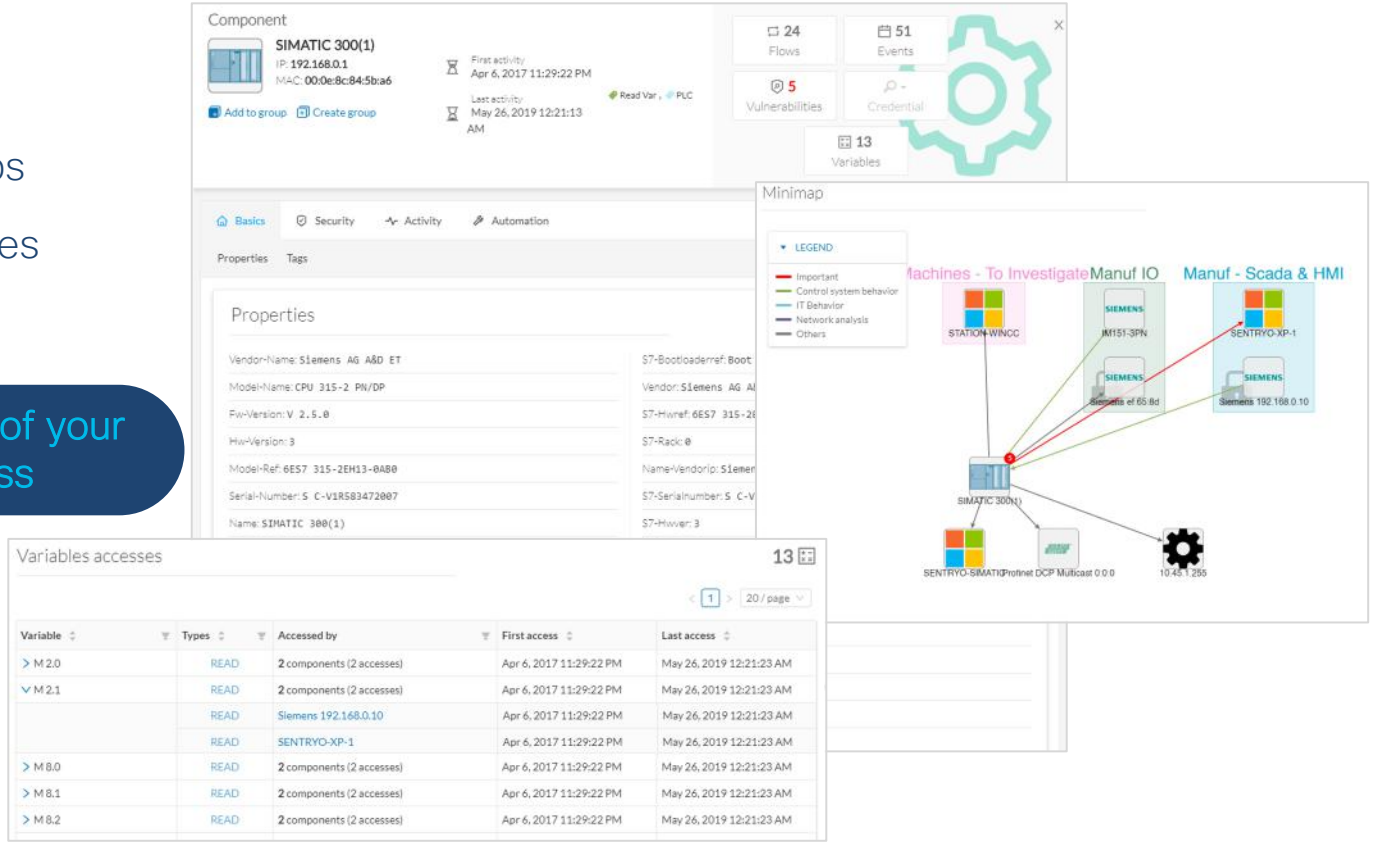


© 2020 Cisco and/or its affiliates. All rights reserved.

Operational insights: **Views for OT** teams

- Asset details
- Communication maps
- PLC program changes
- Variable accesses

Monitor the integrity of your industrial process



© 2020 Cisco and/or its affiliates. All rights reserved.

Operational insights: **Views for security leaders**

- Access the full history of all communication flows
- View detailed properties and content statistics for each flow
- View live information or go back in time for forensic search

Your ICS Flight Recorder

Flows

From	Source Port	To	Destination Port	First activity	Last activity	Tags	Packets	Bytes
Siemens 192.168.105.120	102	PLC_1	49158	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	No tags	0	0 B
PLC_1	102	Dell 192.168.105.241	1613	Apr 6, 2017 10:59:13 PM	May 26, 2019 12:21:13 AM	Program Upload, Start CPU, Stop CPU, Read Var, Write Var, ...1+	0	0 B
PLC_3	102	PLC_1	49159	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	No tags	0	0 B
Siemens 192.168.105.120	102	PLC_1	49158	Apr 6, 2017 10:59:13 PM	May 26, 2019 12:21:13 AM	No tags	0	0 B
Siemens 192.168.105.120	0	PLC_1	0	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	ARP	0	0 B
PLC_3	0	PLC_1	0	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	ARP	0	0 B
PLC_1	102	Dell 192.168.105.241	1611	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	Program Upload, Read Var, Write Var, S7Plus	0	0 B
PLC_1	102	Dell 19						
PLC_1	102	Dell 19						
PLC_1	102	Dell 19						
Siemens 192.168.105.150	49162	PLC_1						
Siemens 192.168.105.150	49163	PLC_1						
PLC_1	102	Dell 19						
Siemens 192.168.105.150	0	PLC_1						
PLC_1	0							

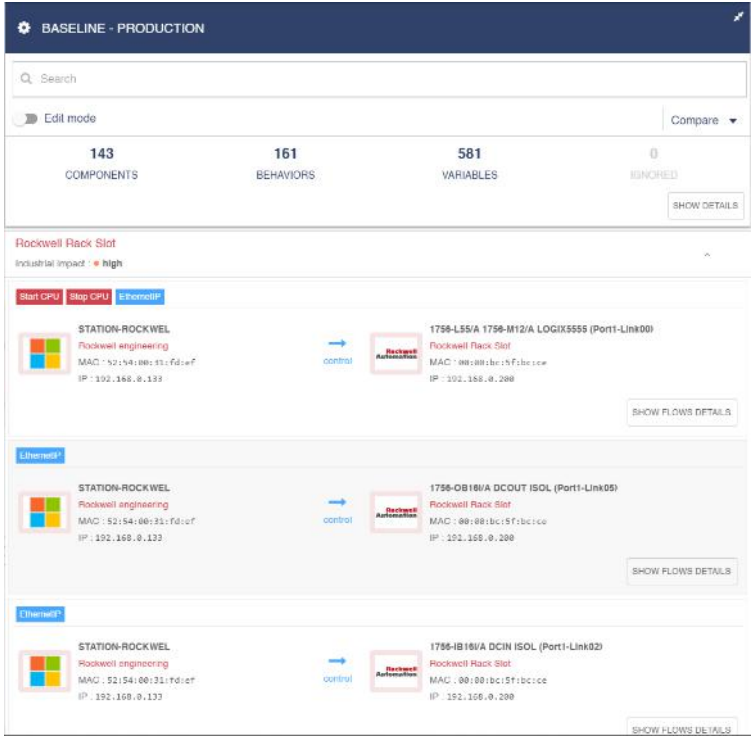
Content Statistics

Property	Value	Occurences
emerson-udp-event	setvar	7
emerson-udp-function	KeepAlive	1
emerson-udp-function	Message	7
emerson-udp-var-name	PID1/MODE	1
emerson-udp-var-name	PID1/SP	6
emerson-udp-var-scope	CV	6
emerson-udp-var-scope	TARGET	1
emerson-udp-var-value	49.52	1
emerson-udp-var-value	49.97	1
emerson-udp-var-value	69.97	1
emerson-udp-var-value	70	1
emerson-udp-var-value	70.41	1
emerson-udp-var-value	72	1
emerson-udp-var-value	AUTO	1
ipv4-ttl	128	1
ipv4-ttl	64	1

© 2020 Cisco and/or its affiliates. All rights reserved.

Threat detection: **Behavioral analytics**

- Create Baselines to define normal behaviors and configurations
- Behavior modeling automatically triggers alerts on deviations to the baselines
- Import IoC to detect known malicious behaviors
- Continuously improve detection with classification of new events



Detect unknown attacks and malfunctions

© 2020 Cisco and/or its affiliates. All rights reserved.

Threat detection: **Signature-based IDS**

- Snort based Intrusion Detection
- Immediately identify known attacks:
  - Lateral Movement via exploits
  - Command and Control (C&C) callbacks
  - OT Malwares
  - Bad IT behaviors (ex: repeated logon failure on SMB)
  - IT Denial of Services (DoS)
- Frequently updated signatures curated by cybersecurity specialists focused on hunting threats to industrial networks

© 2020 Cisco and/or its affiliates. All rights reserved.

Cyber Vision integrates with your existing security platforms

Access Control

Identity Service Engine

Firewalls

Firepower NGFW

CMDB

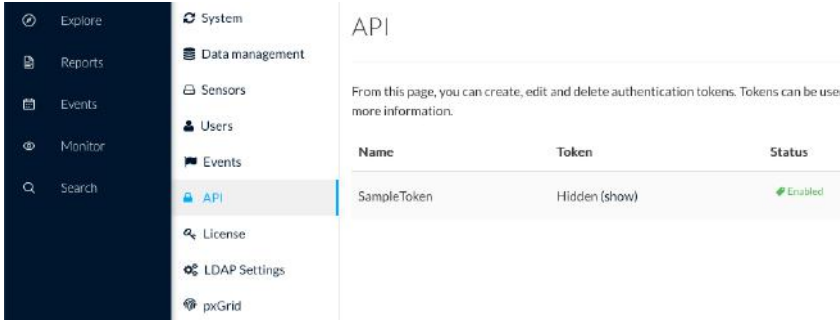
SOC

Stealthwatch

© 2020 Cisco and/or its affiliates. All rights reserved.

Integrations and customization via **RESTful API**

- Access data about components and communication flows available in Cyber Vision
- Leverage sandboxed application hosting to automate functions and integrations
- Modify tag assignment, presets and groups programmatically
- Define custom analyzers for unknown traffic in environment



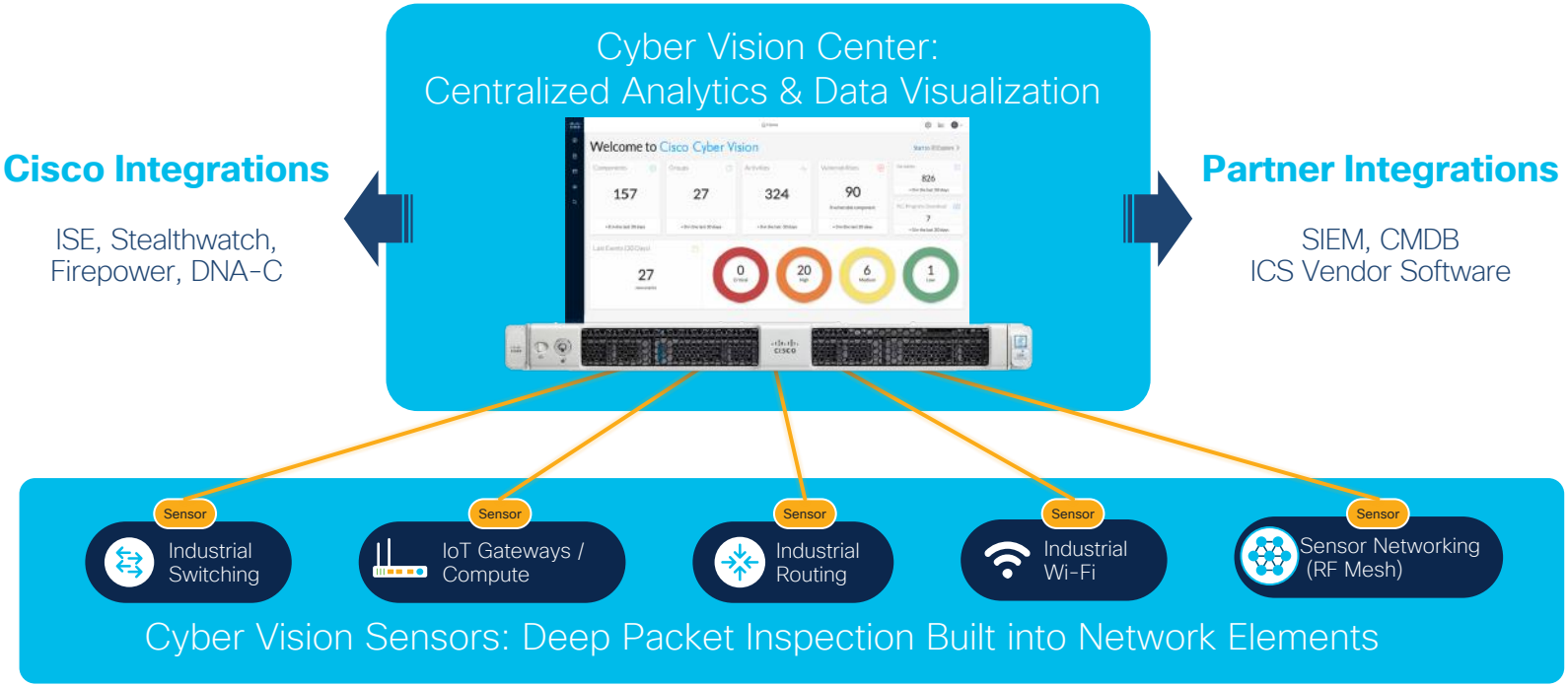
Integrate data from Cyber Vision into additional tools

© 2020 Cisco and/or its affiliates. All rights reserved.

Best architecture ?

Cisco Cyber Vision

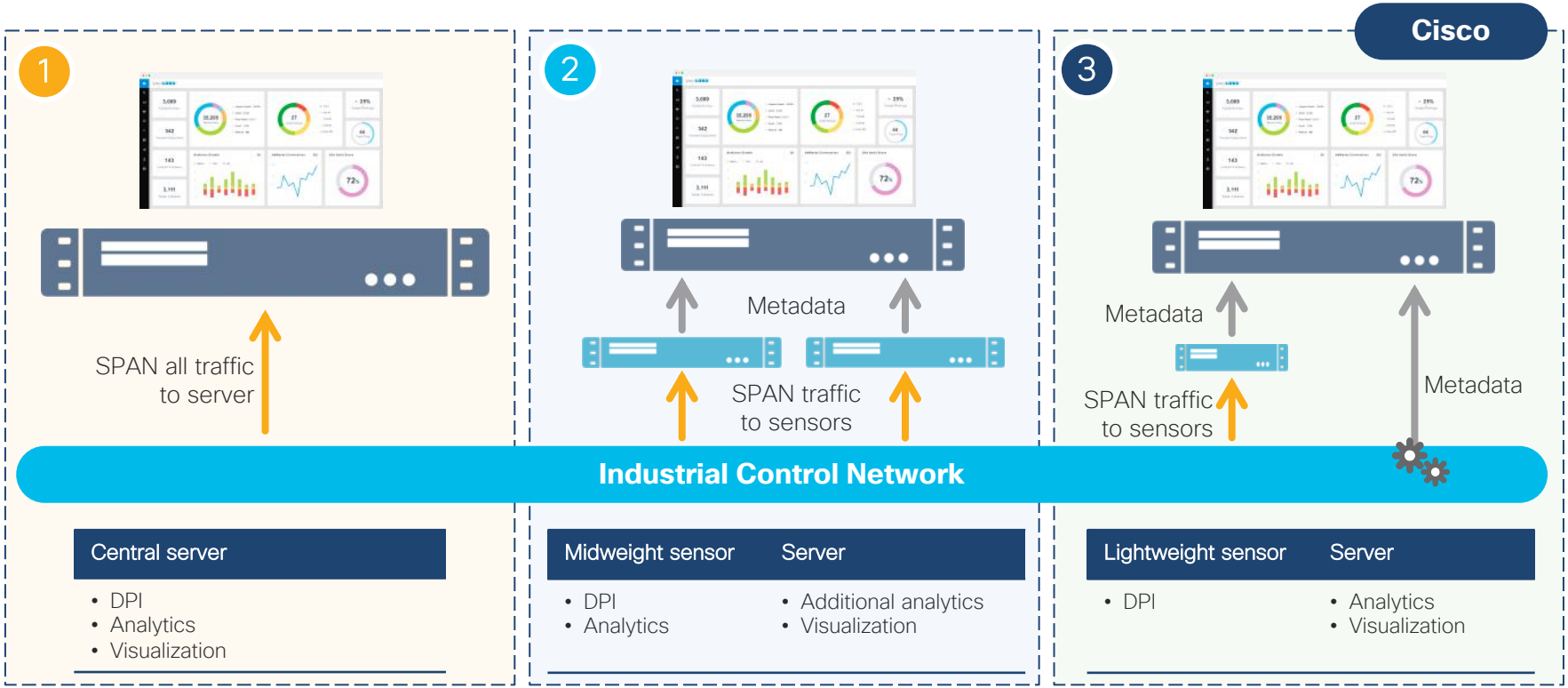
A 2-tier edge architecture that integrates with your existing security solutions



© 2020 Cisco and/or its affiliates. All rights reserved.

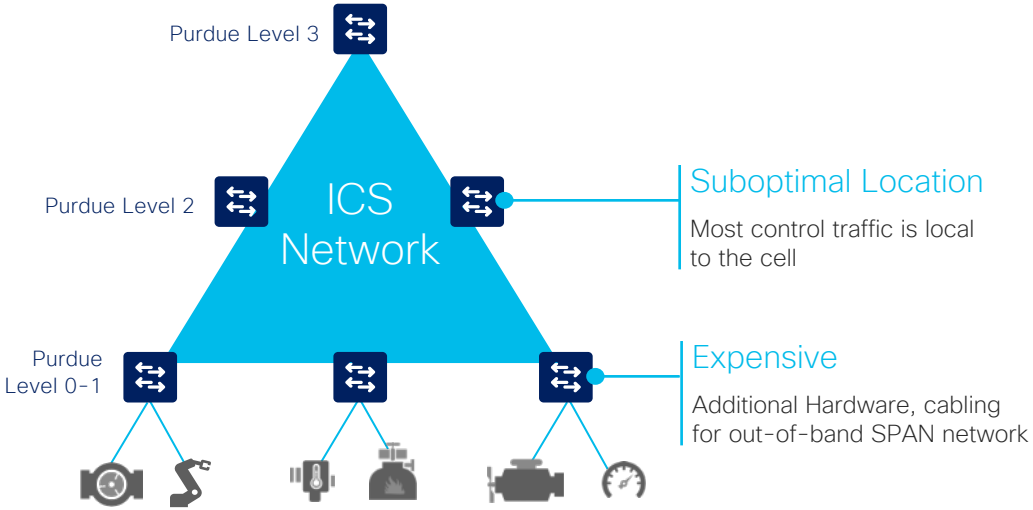
ICS visibility and detection solution types

What is really going on under the hood



© 2020 Cisco and/or its affiliates. All rights reserved.

Why is a network-sensor important?



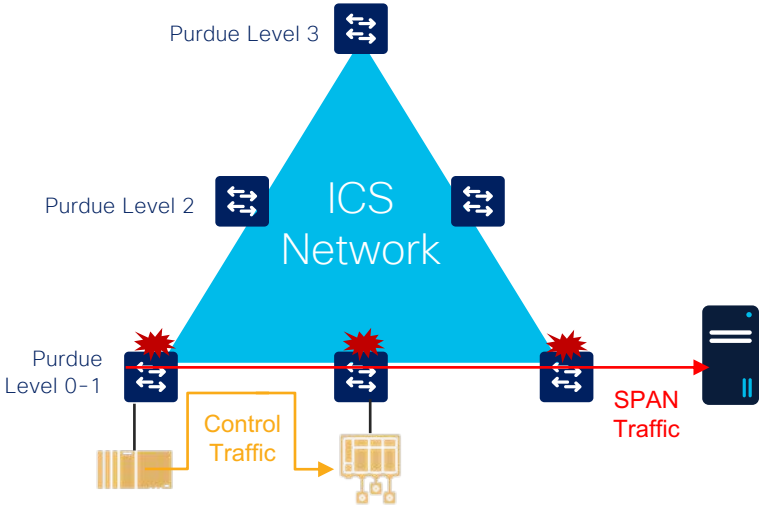
DPI Location Matters!

- Mirroring traffic in at the aggregation layer results in visibility to only North-South traffic
- Mirroring traffic at the cell layer requires an expensive out-of-band SPAN network

Sensor embedded in the network sees everything that attaches to it

© 2020 Cisco and/or its affiliates. All rights reserved.

Why is a network-sensor important?



RSPAN introduces Jitter!

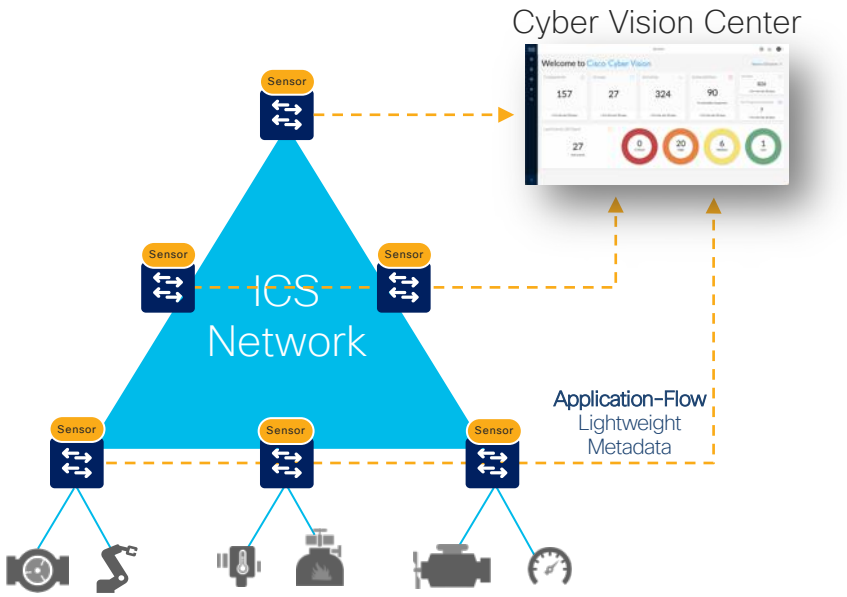
- Head-of-line blocking caused by Inline SPAN traffic negatively impacts time-sensitive control loop
- RSPAN in LANs is detrimental to control system performance

Sensor embedded in the network generates lightweight metadata that does not congest QoS queues

© 2020 Cisco and/or its affiliates. All rights reserved.

Visibility Using your Network Infrastructure

The Cisco industrial network lets you see everything that connects to it



Monitoring at the Edge

- Cyber Vision Sensors embedded into industrial network equipment
- No additional hardware needed
- No need for an out-of-band monitoring network

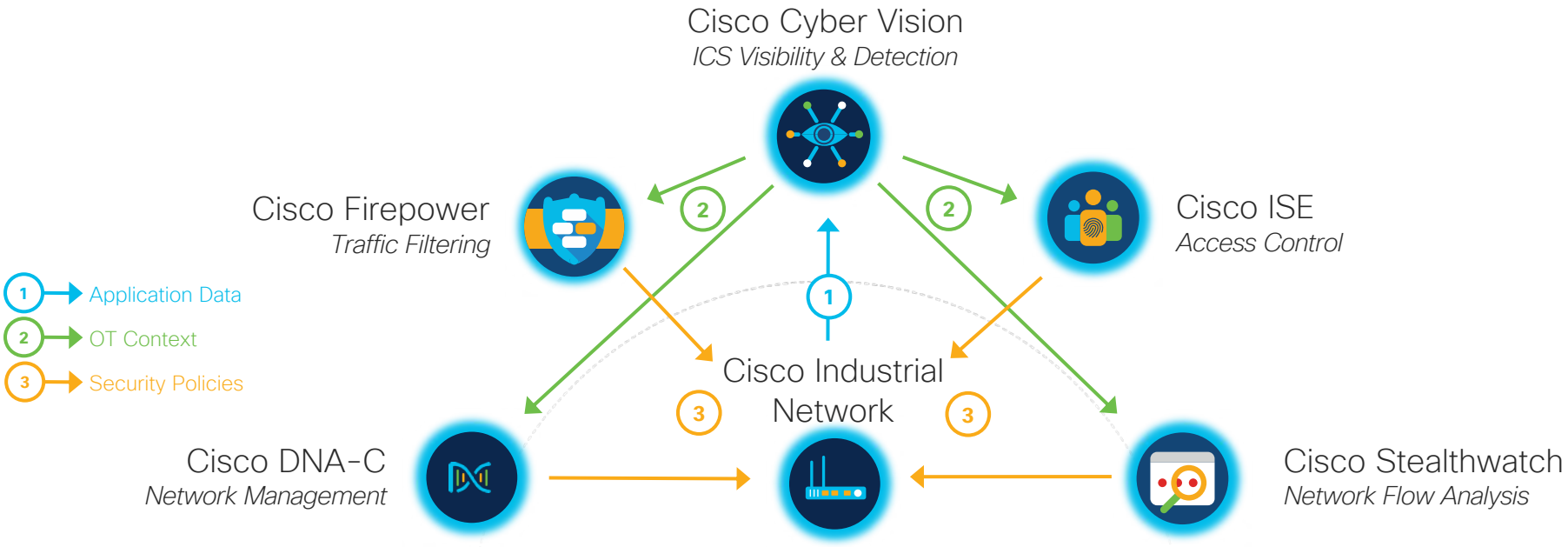
Easy deployment
Low TCO

CISCO is the only vendor on the market with an edge strategy for OT cybersecurity

”Magic pill” ?

The Only Fully Integrated OT Security Solution

Working together to define & apply IoT security policies



© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco ISE Integration

Extend security policies to your industrial network

pxGrid

Cisco ISE

- ISE endpoints are enriched with context from Cyber Vision
- Use ICS attributes (PLC, Siemens, Cell-1) to define profiling policy
- Segment your network to prevent malware and ransomware from spreading

TrustSec

ICS Visibility

Cisco Industrial Network Provides Visibility and Enforces Security Policy

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Stealthwatch Integration

Speed up incident response and forensics

REST API

Cisco Stealthwatch

- Stealthwatch flows enriched with context from Cyber Vision
- Use ICS attributes (PLC, Siemens, Cell-1) to define host-group policy
- Pinpoint ICS assets when Stealthwatch raises alarms at Level-3 for north-south traffic from industrial network to the Enterprise

ICS Visibility

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Firepower Integration

OT context for creating rules, remediation, and impact assessment

ICS Visibility

Cisco Firepower

- Map ICS device IP to named objects (PLC, IO, Drive) in Firepower for use in access policy*
- Map ICS device vulnerabilities to Hosts in Firepower for use in correlation policy*
- Identify anomalous flows in Cyber Vision and kill FTD Firewall sessions

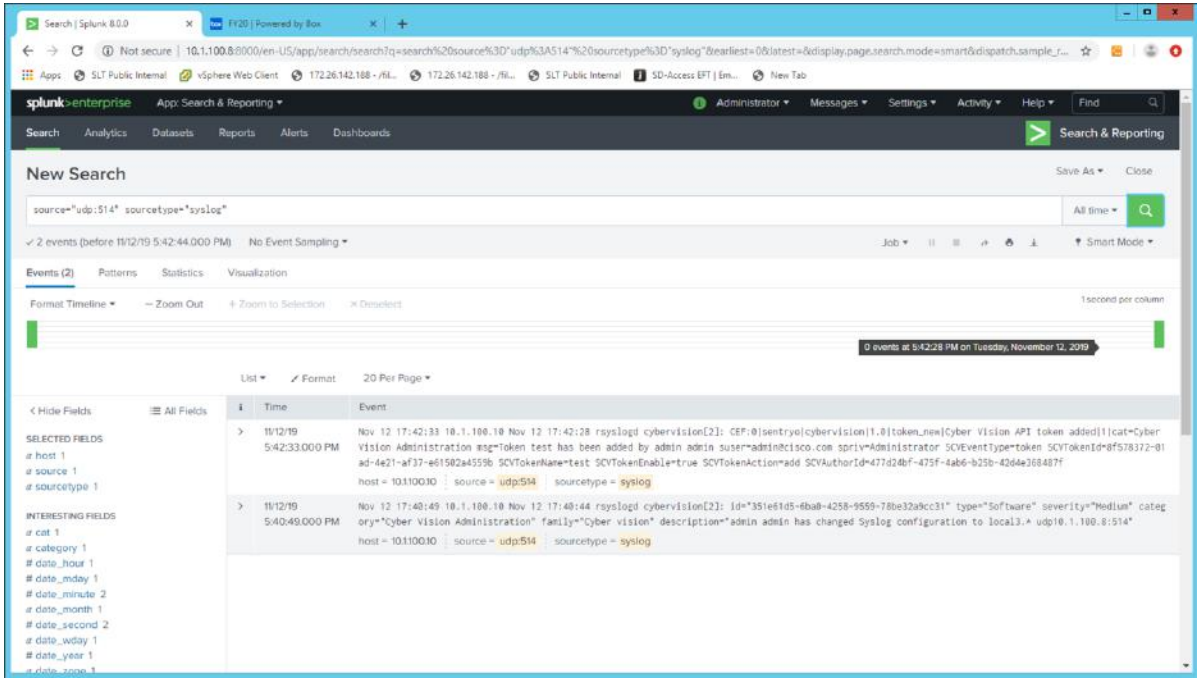
* Spring 2020

© 2020 Cisco and/or its affiliates. All rights reserved.

Splunk Integration

Unified IT/OT security events management in SIEM

Syslog

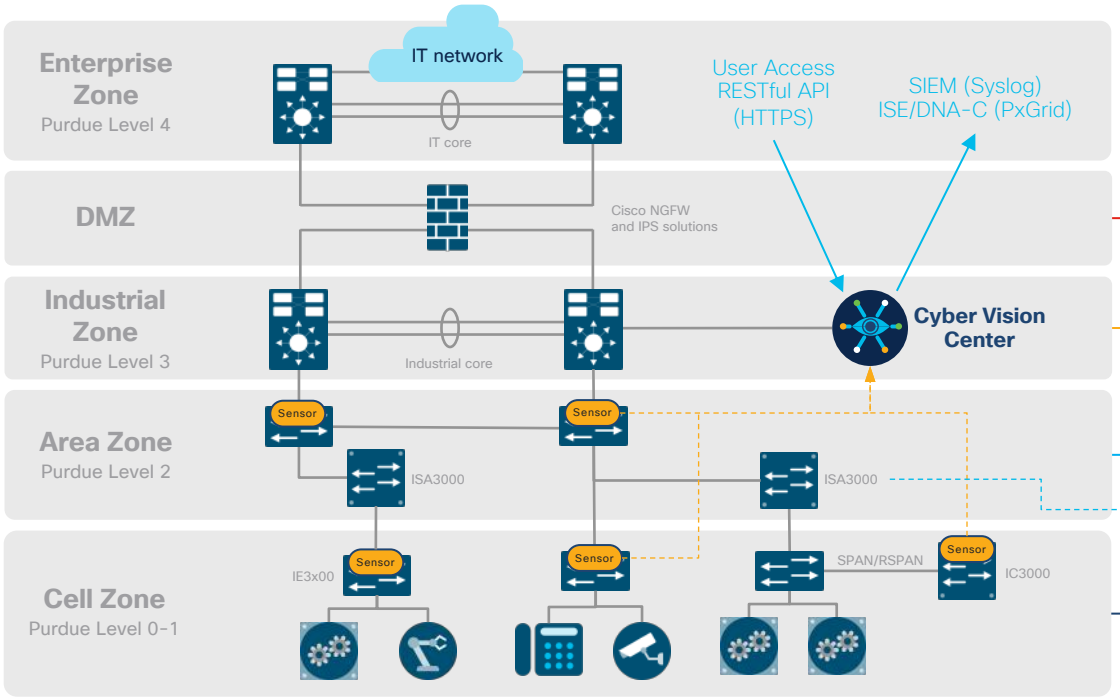


ICS Visibility

© 2020 Cisco and/or its affiliates. All rights reserved.

Architecture with Cybersecurity?

Converged Industrial Architectures



Cisco Components	
Industrial DMZ	• Access control lists (ACLs) • Intrusion detection systems (IDS) and intrusion prevention systems (IPS) • VPN services • Portal and remote desktop services • Application and data mirrors
Industrial zone	• AAA identity services • Network management • Asset inventory • Anomaly detection • Plant-wide services • Traffic enforcement (plant to IDMZ, north/south)
Area zone	• Traffic Enforcement (Cell to Cell, East/West) • QoS Prioritization • SXP • Netflow
Inter-cell (ISA3000)	• Industrial deep packet inspection (DPI) • Stateful firewall and intrusion prevention (IPS) • Hardware bypass
Cell zone	• PoE/PoE+ • Layer 2 NAT • 802.1X • MAC Authentication Bypass (MAB) • Quality of Service marking • Netflow (IE3x00 and IE4000 only) • TrustSec tagging (IE3x00 and IE4000 only) • Edge compute (IE3x00 only)

© 2020 Cisco and/or its affiliates. All rights reserved.

Conclusion

- OT network is vulnerable to attacks
- Architecture approach (IDMZ, Segmentation, …)
- Cisco Cybervision :
  - Can help in many directions (visibility, flows, …)
  - Provides data usable for OT specialists (easy tags)
  - Can help to enforce best practices
  - Perfect architecture
  - Open integrations via APIs

© 2020 Cisco and/or its affiliates. All rights reserved.

Resources

Literatura

Cisco IoT Security:
https://www.cisco.com/c/en/us/solutions/internet-of-things/iot-security.html

Cisco Cyber Vision:
https://www.cisco.com/c/en/us/products/security/cyber-vision/index.html

Cisco Cyber Vision Datasheet:
https://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/datasheet-c78-743222.html

Cisco Cyber Vision Center Hardware Appliance Data Sheet:
https://www.cisco.com/c/en/us/products/collateral/security/cyber-vision/datasheet-c78-743481.html

© 2020 Cisco and/or its affiliates. All rights reserved.

CISCO