



Kybernetická bezpečnost v prostředí IoT sítí

Jiří Rott

19.5.2020

Agenda

01 Why Cybersecurity in IoT

02 Architecture importance

03 Cisco Cyber Vision

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

OT Components

Industrial Devices (aka “things”)

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

and so much more

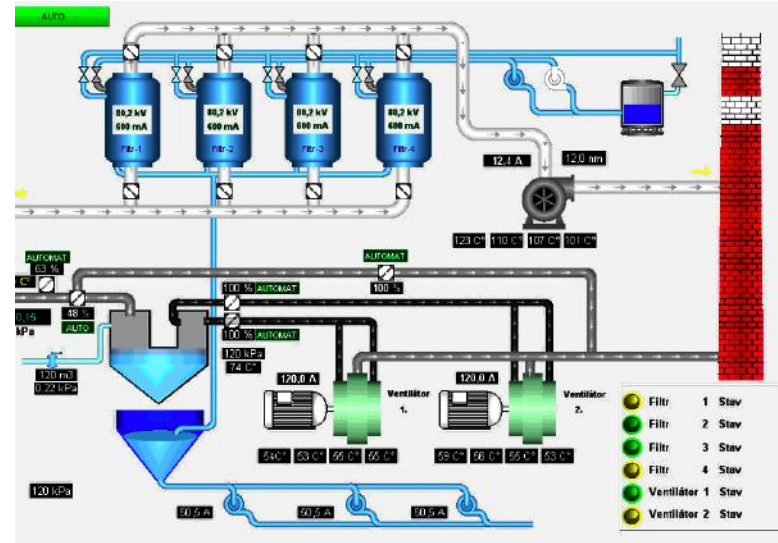


Industrial Control Systems

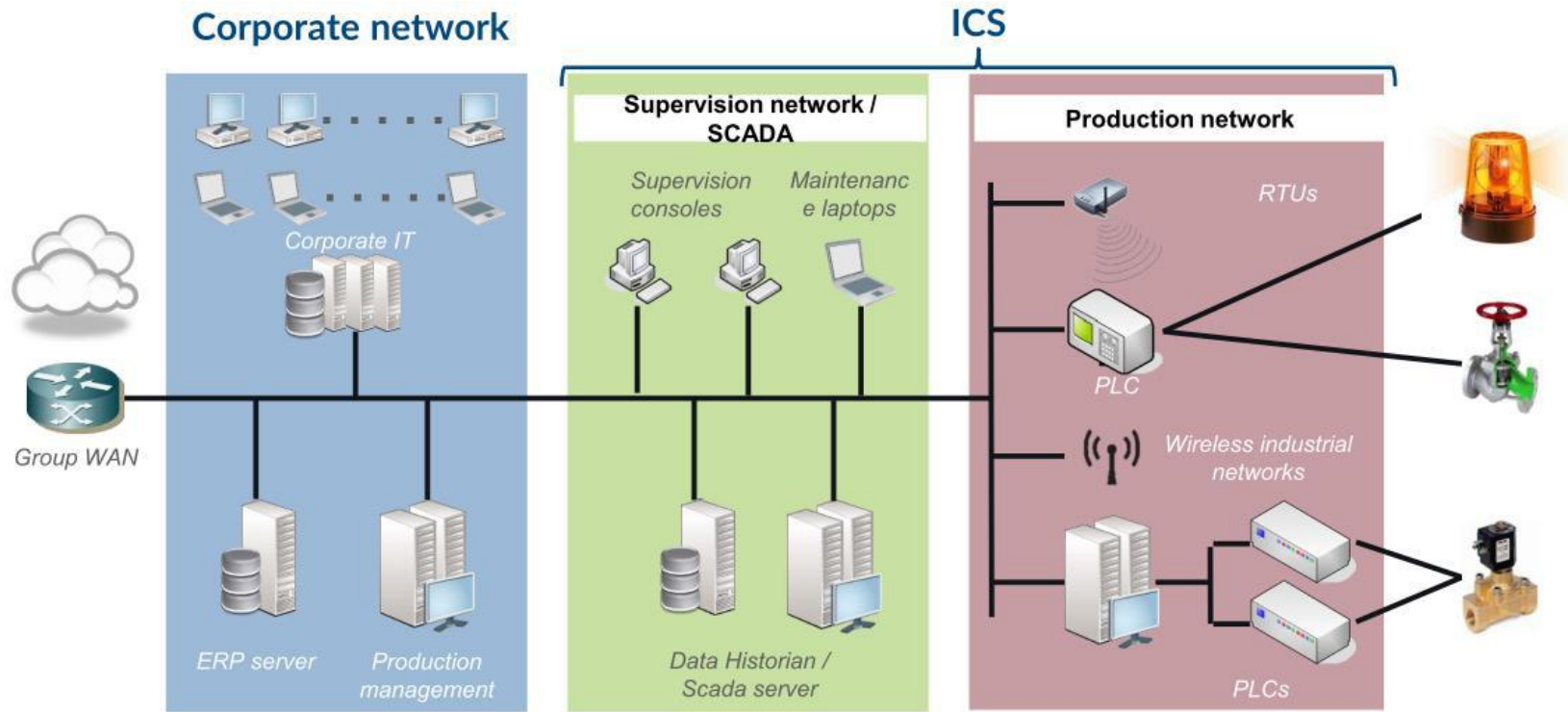
- Remote Terminal Units (RTU)
- Programmable Logic Controllers (PLC)
- Intelligent Electronic Devices (IED)
- Supervisory Control and Data Acquisition (SCADA)
- Distributed Control Systems (DCS)
- Human Machine Interfaces (HMI)

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



Typical Industrial Control System (ICS)

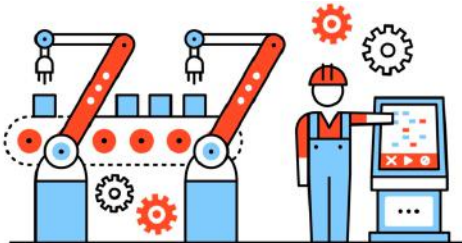


Customer Challenges

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

TODAY
Traditional automation systems


Energy, Manufacturing,
Transportation, Process



The illustration depicts a traditional industrial setting. On the left, two robotic arms with red joints and blue bases are positioned over a production line. In the center, a worker wearing a red hard hat and blue overalls stands next to a control panel with a screen displaying a grid of data. Several gears of various sizes are scattered around the scene, symbolizing mechanical processes.



TOMORROW
The Industrial Internet of Things



The illustration shows a complex, interconnected IIoT ecosystem. A hand on the left interacts with a 'USER INTERFACE' screen. A central factory icon is surrounded by '4.0' and 'SMART INDUSTRY' labels. Other elements include 'AUTOMATION' with a robotic arm, 'BIG DATA' with a server rack, and 'SMART CITIES' with a person icon. At the bottom, 'SMART GRIDS' and 'INDUSTRY 4.0' are connected to 'DISTRIBUTED DEVICES' and 'INTELLIGENT BUILDINGS'. A truck icon labeled 'FLEXIBILITY' is also present.

SMART GRIDS INDUSTRY 4.0 SMART CITIES

DISTRIBUTED DEVICES INTELLIGENT BUILDINGS

Industrial Control Systems are not designed for cybersecurity

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

Industrial systems are not designed for cybersecurity

What OT professionals tell us

Everything is fine!
My automation vendor has
very secured products...



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

Examples of Recent OT Attacks

2010

Stuxnet causes damages to Iran's nuclear program

2017

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

What's next ?

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

2015

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

2019

Norsk Hydro is shutdown because of ransomware

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



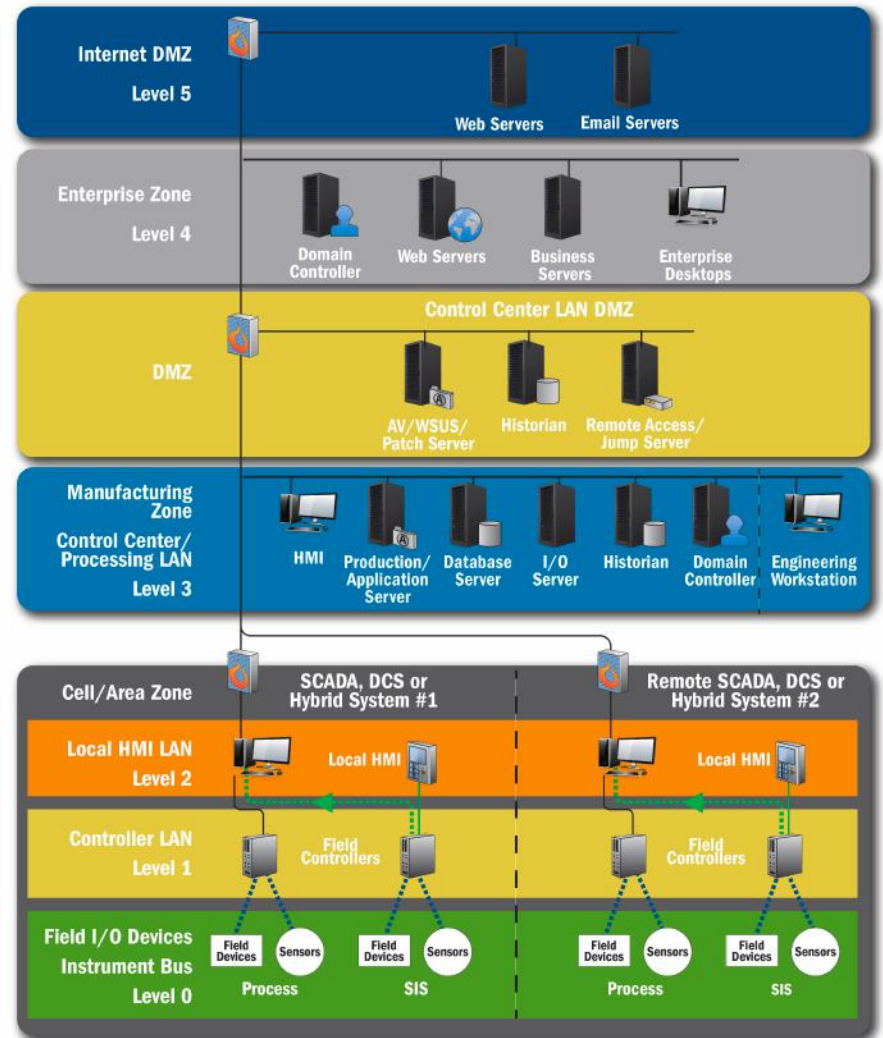
Agility

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

Architecture importance

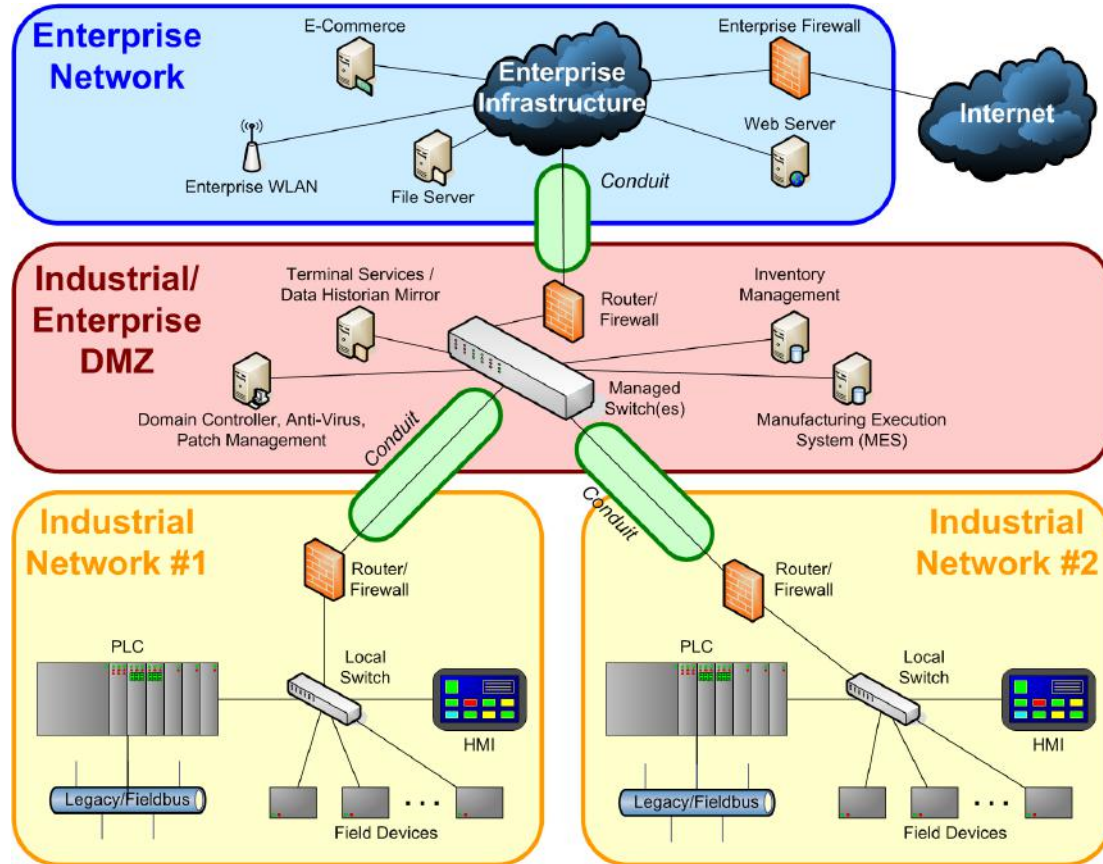
Defining the Purdue Model

- 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

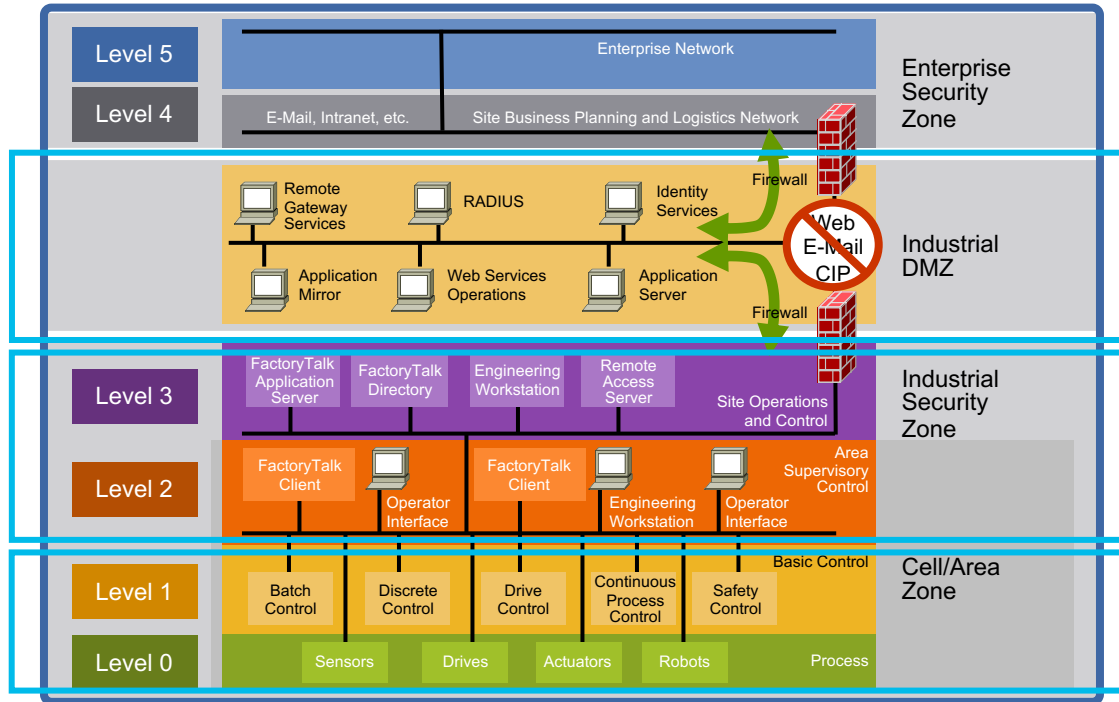


ISA-99/IEC-62443 Zones and Conduits

- 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



Typical Cyber security usecases

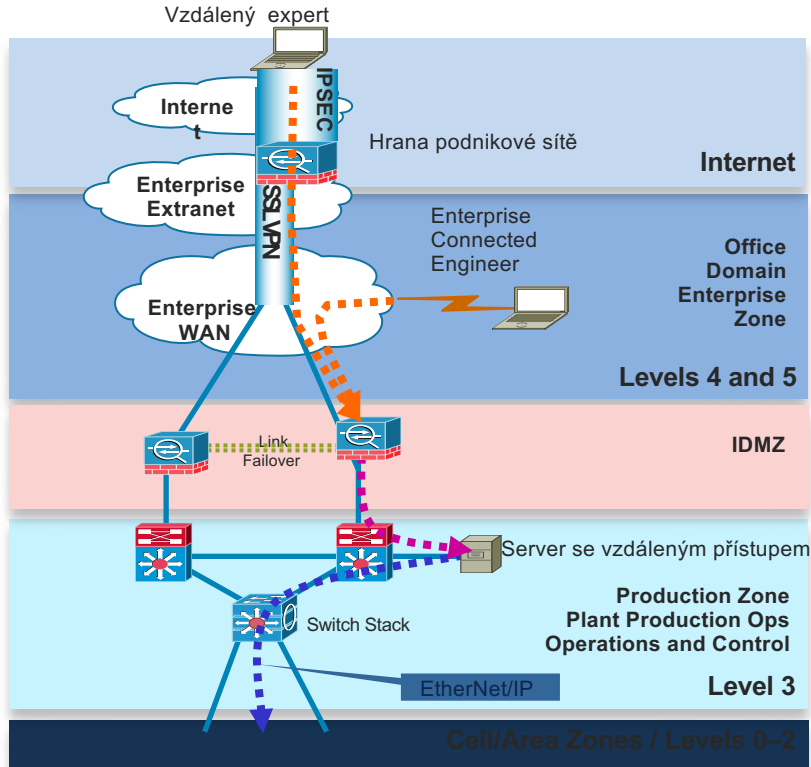


Connected Factory:
IDMZ a Vzdálený
přístup

Connected Factory:
Identity Services

Connected Factory:
NAT

Vzdálený přístup experta přes podnikovou síť



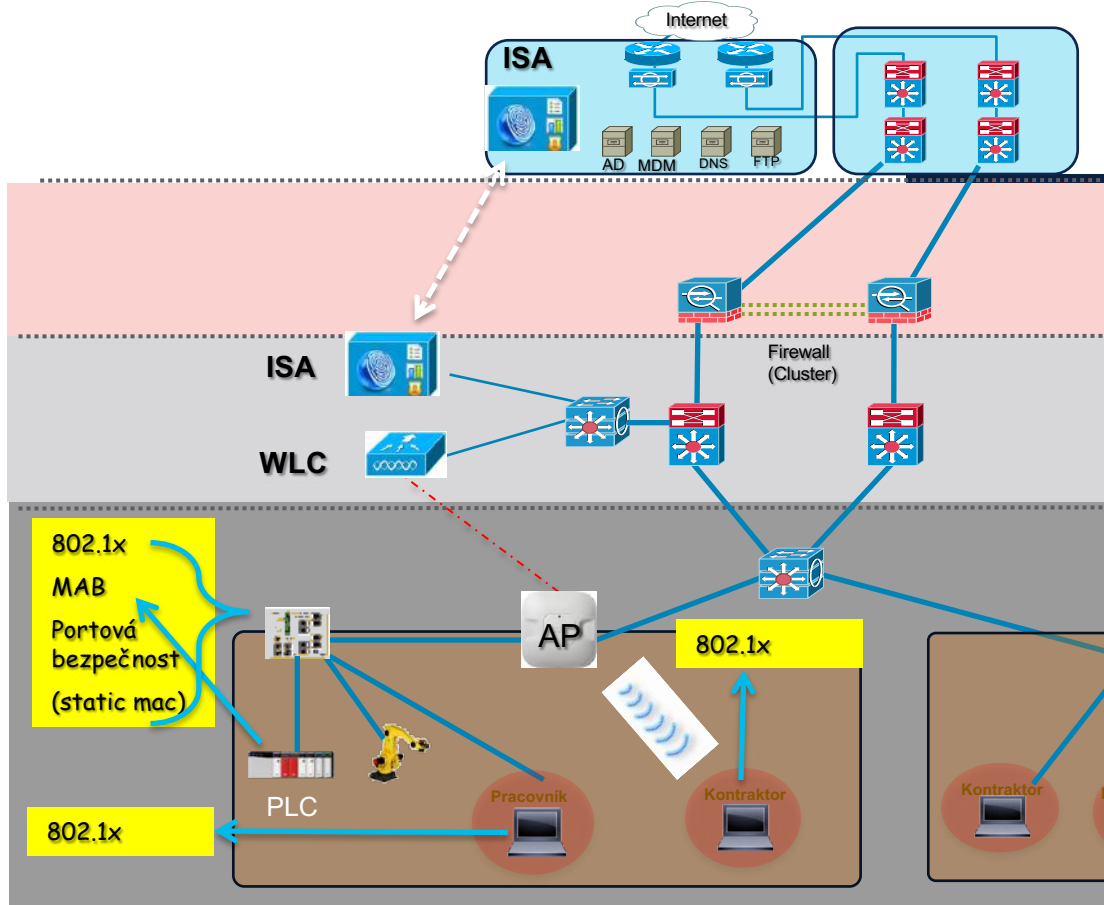
Proč ?

- 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 sítě
- 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 připojení neznámých zařízení

Jak ?

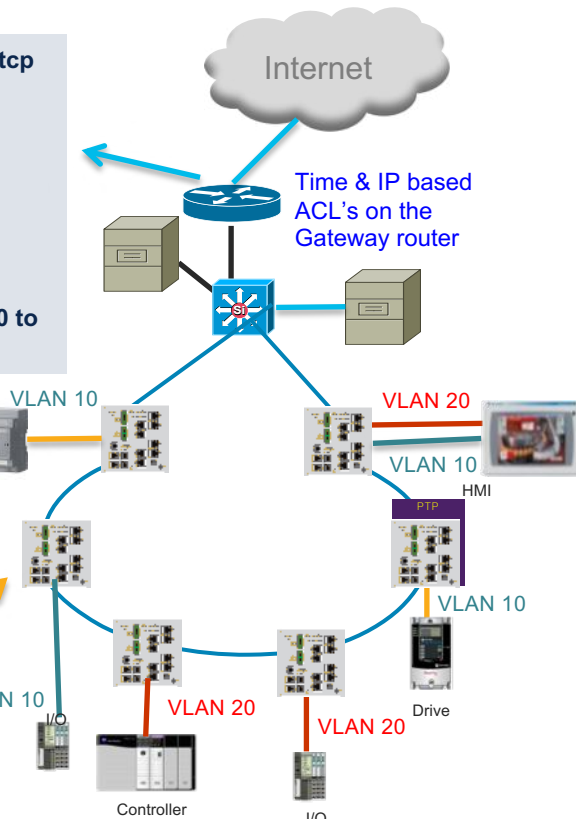
- Nastavit 802.1x ověření na portech přístupových přepínačů
- Použití MAB pro prvky (IoT) nedisponující suplikantem 802.1x
- Portová bezpečnost se statickou mac adresou pro statické koncové prvky

Omezení přístupu k síťovým zdrojům

```
access-list 101 permit tcp
10.1.1.0 0.0.0.255
172.16.1.0 0.0.0.255 eq
telnet time-range
EVERYOTHERDAY
```

```
time-range
EVERYOTHERDAY
periodic Monday
Wednesday Friday 8:00 to
17:00
```

```
access-list ctrl-zone
permit <contractor>
<sis-controller>
<protocol-modbus>
```



Proč omezovat zdroje?

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

Jak?

- Použití VLAN's – konfigurace s přístupových portů do stejné 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

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

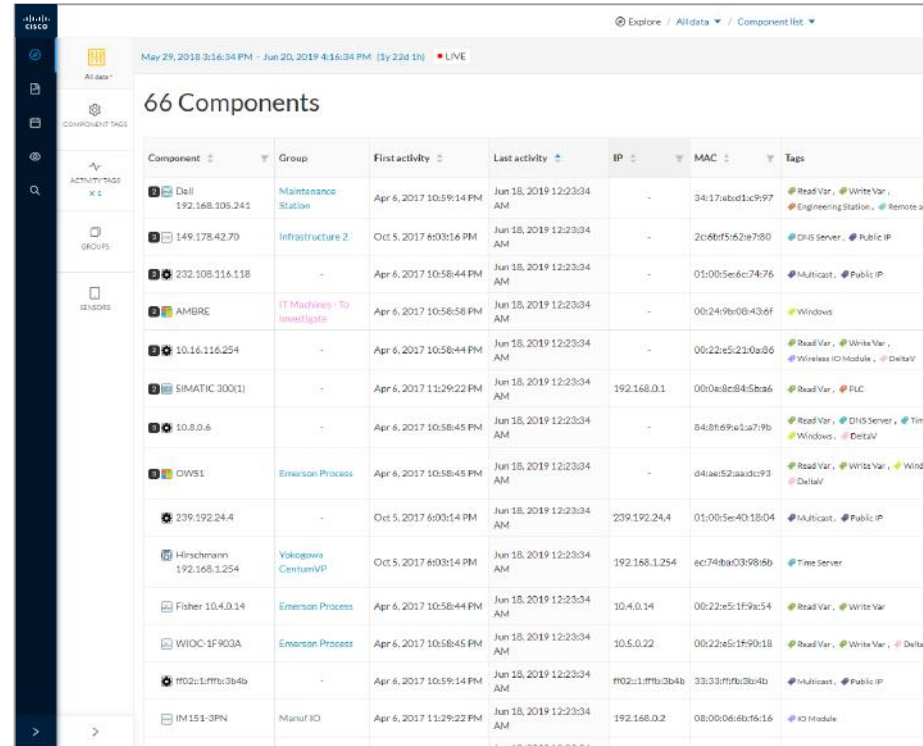
Behavioral Anomaly Detection
Signature based IDS
Real-time alerting

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

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 easy to understand asset functions and properties

Track the industrial assets to protect throughout their life cycles



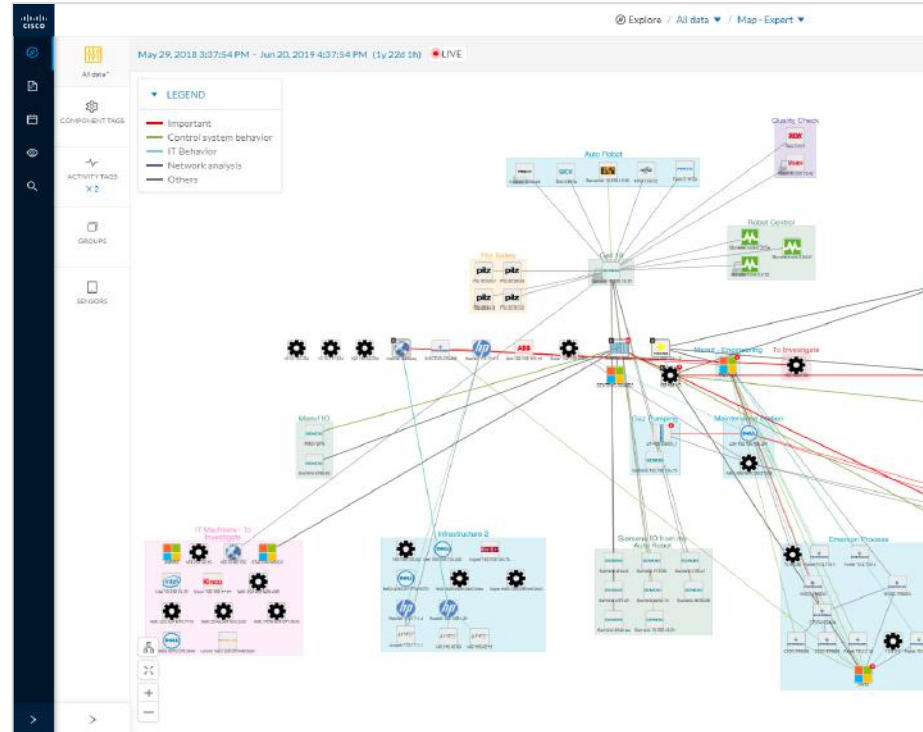
The screenshot displays the Cisco Asset Manager interface. The main content area shows a table titled "66 Components". The table has the following columns: Component, Group, First activity, Last activity, IP, MAC, and Tags. The data rows include various components such as Dell, AMBRE, SIMATIC 300(1), OWSE, Hirschmann, Fisher, WI0C-1F903A, and IM151-3PN, each with associated activity dates and tags like "Maintenance Station", "Infrastructure 2", "IT Machines - To investigate", "Emerson Process", "Yokogawa CentumVP", "Emerson Process", and "Manufacturing".

Component	Group	First activity	Last activity	IP	MAC	Tags
Dell 192.168.105.241	Maintenance Station	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23:04 AM	-	34:17:ab:d1:c9:97	Read Var, Write Var, Engineering Station, Remote
149.178.42.70	Infrastructure 2	Oct 5, 2017 6:03:16 PM	Jun 18, 2019 12:23:04 AM	-	2c:6b:f5:62:e7:80	DNS Server, Public IP
232.108.116.118	-	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:04 AM	-	01:00:5e:6c:74:76	Multicast, Public IP
AMBRE	IT Machines - To investigate	Apr 6, 2017 10:58:58 PM	Jun 18, 2019 12:23:04 AM	-	00:24:9b:08:43:6f	Windows
10.16.116.254	-	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:04 AM	-	00:22:e5:21:0a:06	Read Var, Write Var, Wireless I/O Module, DeltaV
SIMATIC 300(1)	-	Apr 6, 2017 11:29:22 PM	Jun 18, 2019 12:23:04 AM	192.168.0.1	00:0e:8c:84:5b:a6	Read Var, PLC
10.8.0.6	-	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:04 AM	-	84:8d:69:e1:a7:9b	Read Var, DNS Server, Time Server, Windows, DeltaV
OWSE	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:04 AM	-	d4:0e:52:aa:dc:93	Read Var, Write Var, Windows, DeltaV
239.192.24.4	-	Oct 5, 2017 6:03:14 PM	Jun 18, 2019 12:23:04 AM	239.192.24.4	01:00:5e:40:18:04	Multicast, Public IP
Hirschmann 192.168.1.254	Yokogawa CentumVP	Oct 5, 2017 6:03:14 PM	Jun 18, 2019 12:23:04 AM	192.168.1.254	ec:74:8a:03:98:8b	Time Server
Fisher 10.4.0.14	Emerson Process	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:04 AM	10.4.0.14	00:22:e5:1f:9a:54	Read Var, Write Var
WI0C-1F903A	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:04 AM	10.5.0.22	00:22:e5:1f:9b:18	Read Var, Write Var, DeltaV
#f02:1:fffb:3b4b	-	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23:04 AM	#f02:1:fffb:3b4b	33:03:fffb:3b4b	Multicast, Public IP
IM151-3PN	Manufacturing	Apr 6, 2017 11:29:22 PM	Jun 18, 2019 12:23:04 AM	192.168.0.2	08:00:06:60:f6:16	I/O Module

Visibility: Track **application flows**

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

Drive network segmentation and fine-tune configurations



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

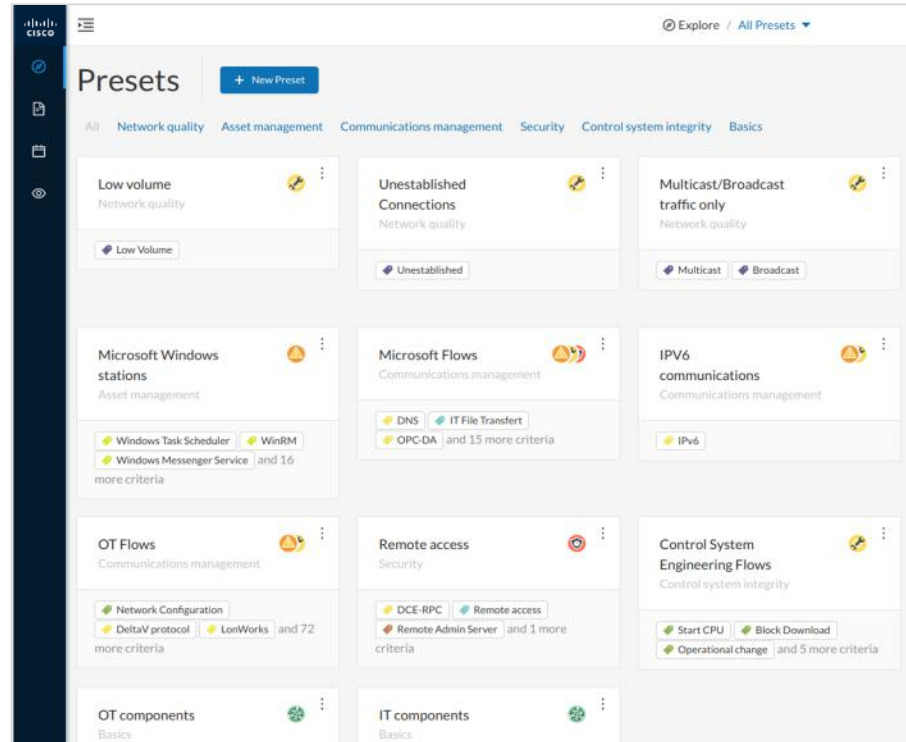
Quickly see asset and communication information in standard format

The image displays two side-by-side screenshots of the Cyber Vision interface. The left screenshot, titled 'COMPONENT TAGS', shows a hierarchical tree structure. It includes categories like 'Components without tags', 'Device - Level 0-1' (with sub-items: IO Module (3), Wireless IO Module (2)), 'Device - Level 2' (with sub-items: Citect Alarm Server, Citect IO Server, Citect Report Server, Citect Trend Server, Engineering Station (3), Master, PLC (9), SCADA Station (3), Slave, Train), and 'Device - Level 3-4' (with sub-items: Admin Server (1), DNS Server (2), Database Server, Email Server, File Transfer Server, HTTP Client, Historian, Host Config Server (3), Key Management Server, License Management Server, Log Server). The right screenshot, titled 'ACTIVITY TAGS', shows another hierarchical tree structure. It includes categories like 'Activities without tags', 'Control system behavior', and 'IT behavior'. The 'IT behavior' category is expanded to show a long list of activities such as Active Directory Replication, Admin (1), Antivirus, Authentication (1), Database, Email, Host Config (11), IT File Sync, IT File Transfer, Key management, License Management, Log, Net Management (3), Net Routing, Ping (10), Power Management, Printer Management, Procedure Call, Proxy, Remote access (1), Streaming, Time Management (9), VPN, Web (3), Windows DFS Replication, Windows Discovery, Network analysis, Authentication Error, and Broadcast (81).

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

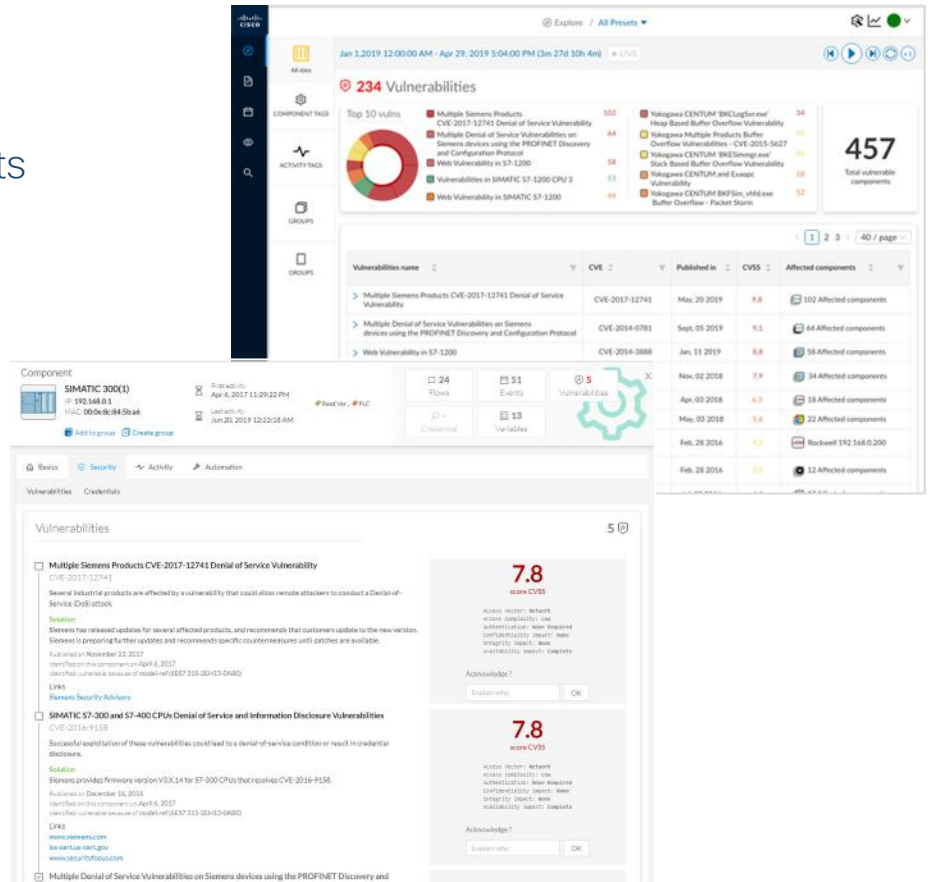
Focus on what is most important to you



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



Operational insights: **Views for OT** teams

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

Monitor the integrity of your industrial process

The screenshot displays a comprehensive view of an industrial asset, specifically a SIMATIC 300(1) PLC. The interface is divided into several key sections:

- Component Details:** Shows the asset name 'SIMATIC 300(1)', IP address '192.168.0.1', and MAC address '00:0e:8c:84:5bra6'. It also tracks activity, such as the first activity on 'Apr 6, 2017 11:29:22 PM' and the last activity on 'May 26, 2019 12:21:13 AM'. Summary statistics include 24 Flows, 51 Events, 5 Vulnerabilities, and 13 Variables.
- Properties:** A detailed list of hardware and software specifications, including Vendor (Siemens AG A&D ET), Model (CPU 315-2 PN/DP), Firmware (V 2.5.0), and various serial and rack information.
- Variables accesses:** A table showing the history of variable reads. The table has columns for Variable, Types, Accessed by, First access, and Last access.
- Minimap:** A network diagram showing the PLC's connections to other systems like 'STATION WINCC', 'Manuf IO', and 'Manuf - Scada & HMI'. A legend identifies connection types like 'Important', 'Control system behavior', and 'IT Behavior'.

Variable	Types	Accessed by	First access	Last access
> M.2.0	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
▼ M.2.1	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
	READ	Siemens 192.168.0.10	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
	READ	SENTRYO-XP-1	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
> M.8.0	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
> M.8.1	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
> M.8.2	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM

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

The screenshot displays two main components of a network flow analysis tool. The top component is a table titled "Flows" with columns for From, Source Port, To, Destination Port, First activity, Last activity, and Tags. The bottom component is a "Content Statistics" view showing a table of properties and their occurrences.

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 6:04:42 PM	May 26, 2019 12:21:13 AM	@ NetMap	0	0 B
PLC_1	102	Dest 192.168.105.241	1653	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 6:04:42 PM	May 26, 2019 12:21:13 AM	@ NetMap	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	@ NetMap	0	0 B
Siemens 192.168.105.120	0	PLC_1	0	Aug 20, 2018 6:04:42 PM	May 26, 2019 12:21:13 AM	APP	0	0 B
PLC_3	0	PLC_1	0	Aug 20, 2018 6:04:42 PM	May 26, 2019 12:21:13 AM	APP	0	0 B
PLC_1	102	Dest 192.168.105.241	1651	Aug 20, 2018 6:04:42 PM	May 26, 2019 12:21:13 AM	Program Upload, @Read Var, @Write Var, @SPut	0	0 B
PLC_1	102	Dest 19						
PLC_1	102	Dest 19						
PLC_1	102	Dest 19						
Siemens 192.168.105.100	49162	PLC_1						
Siemens 192.168.105.150	49163	PLC_1						
PLC_1	102	Dest 19						
Siemens 192.168.105.150	0	PLC_1						
PLC_1	0							

Property	Value	Occurrences
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

Your ICS Flight Recorder

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

The screenshot displays a network management interface titled "BASELINE - PRODUCTION". It features a search bar, an "Edit mode" toggle, and a "Compare" dropdown. Below these are summary statistics: 143 COMPONENTS, 161 BEHAVIORS, 581 VARIABLES, and 0 IGNORED. A "SHOW DETAILS" button is present. The main content area shows a "Rockwell Rack Slot" with an industrial impact of "high". It includes a "Start CPU" button and a "Stop CPU" button. The interface displays three network flows, each with a "control" button and a "SHOW FLOWS DETAILS" button. The flows are:

- Flow 1: STATION-ROCKWEL (Rockwell engineering, MAC: 52:54:00:31:fd:1f, IP: 192.168.0.133) to 1758-L55/A 1758-M12/A LOGIX5555 (Port1-Link00) (Rockwell Rack Slot, MAC: 00:00:bc:5f:bc:0c, IP: 192.168.0.200).
- Flow 2: STATION-ROCKWEL (Rockwell engineering, MAC: 52:54:00:31:fd:1f, IP: 192.168.0.133) to 1758-OB18/A DCOUT ISOL (Port1-Link05) (Rockwell Rack Slot, MAC: 00:00:bc:5f:bc:0c, IP: 192.168.0.200).
- Flow 3: STATION-ROCKWEL (Rockwell engineering, MAC: 52:54:00:31:fd:1f, IP: 192.168.0.133) to 1758-IB18/A DCIN ISOL (Port1-Link02) (Rockwell Rack Slot, MAC: 00:00:bc:5f:bc:0c, IP: 192.168.0.200).

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

Cyber Vision integrates with your existing security platforms

Access Control



Identity Service Engine

Firewalls



Firepower NGFW



CMDB



SOC

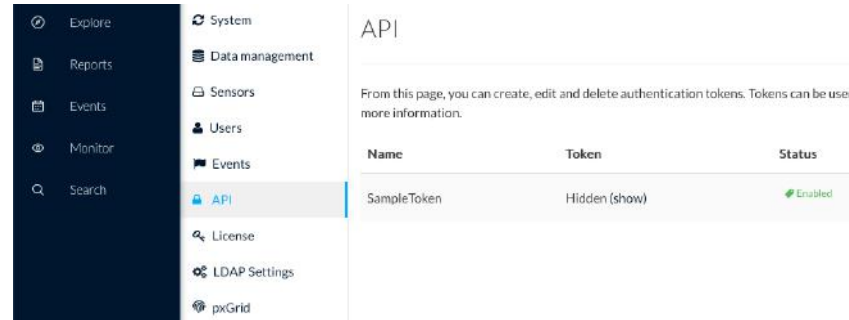


Stealthwatch



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

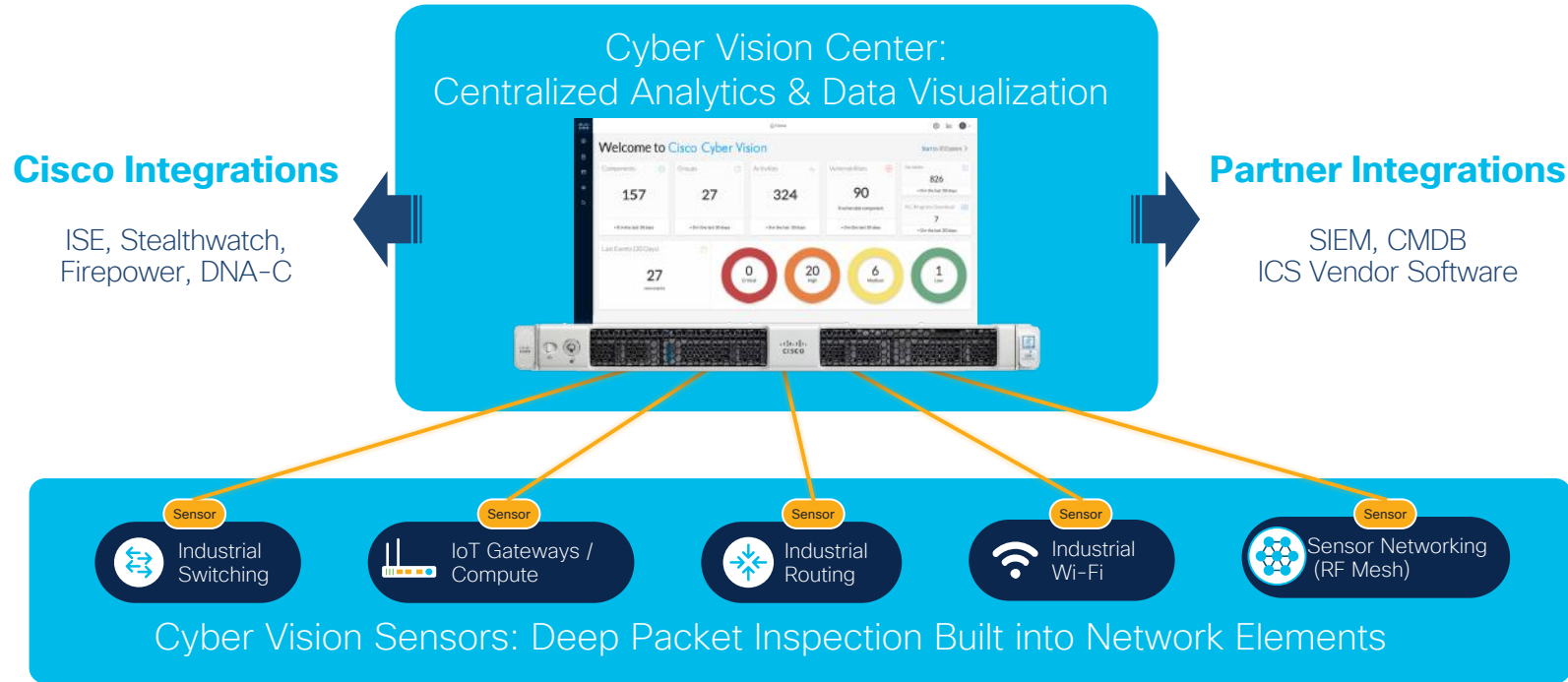


Integrate data from Cyber Vision
into additional tools

Best architecture ?

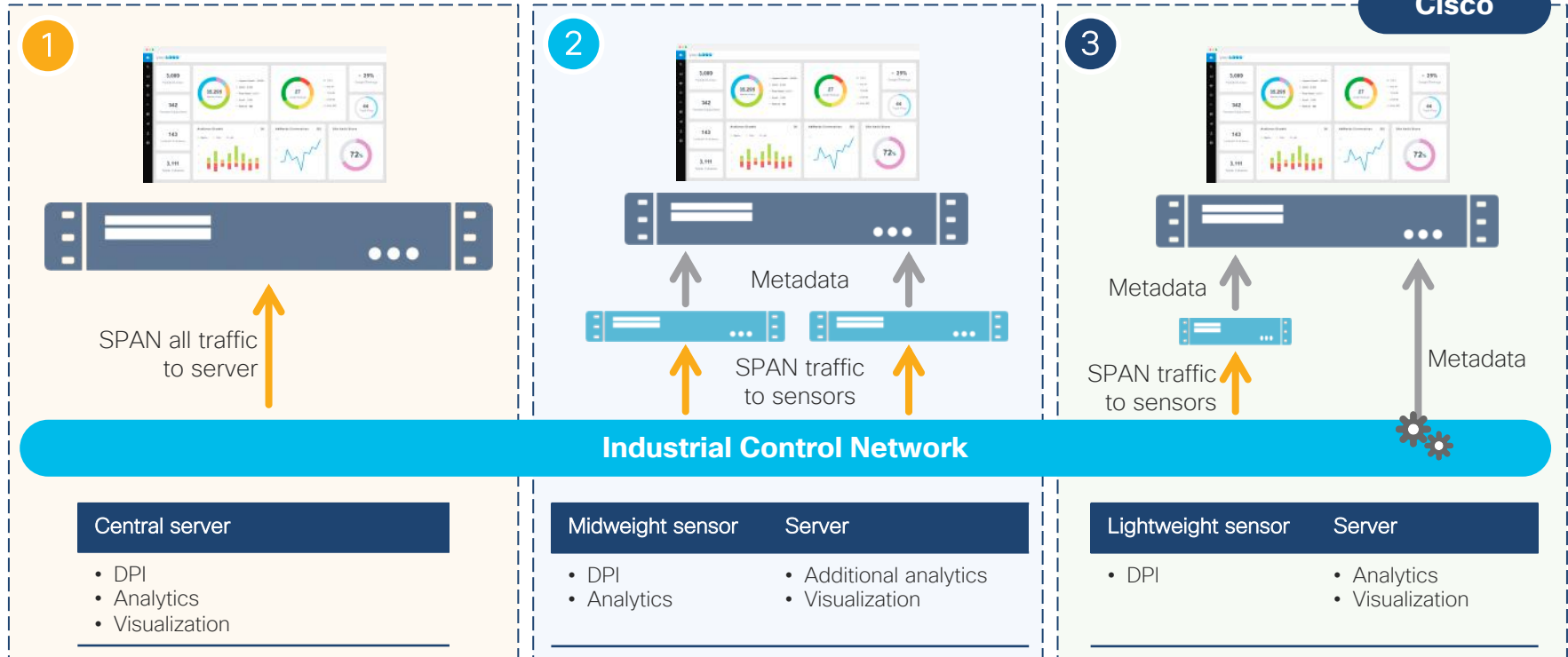
Cisco Cyber Vision

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

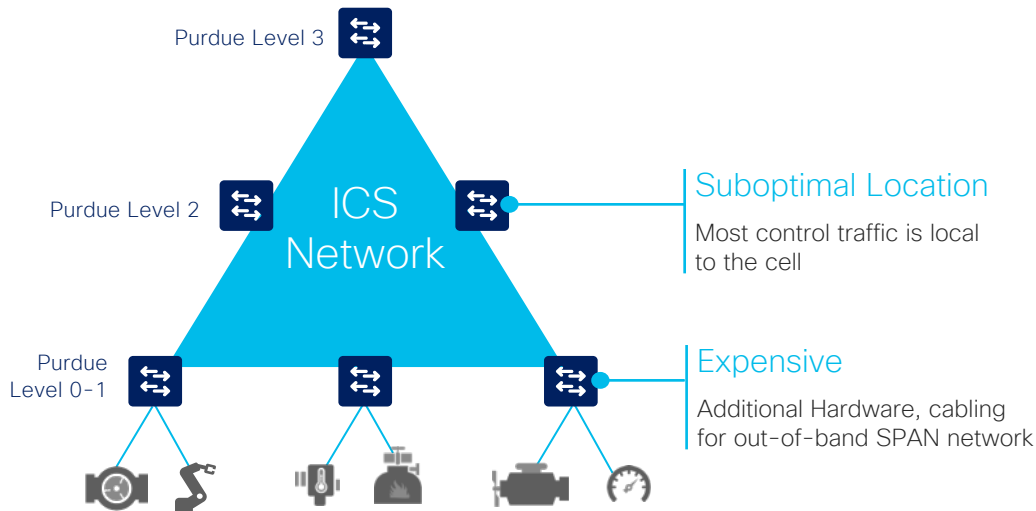


ICS visibility and detection solution types

What is really going on under the hood



Why is a network-sensor important?

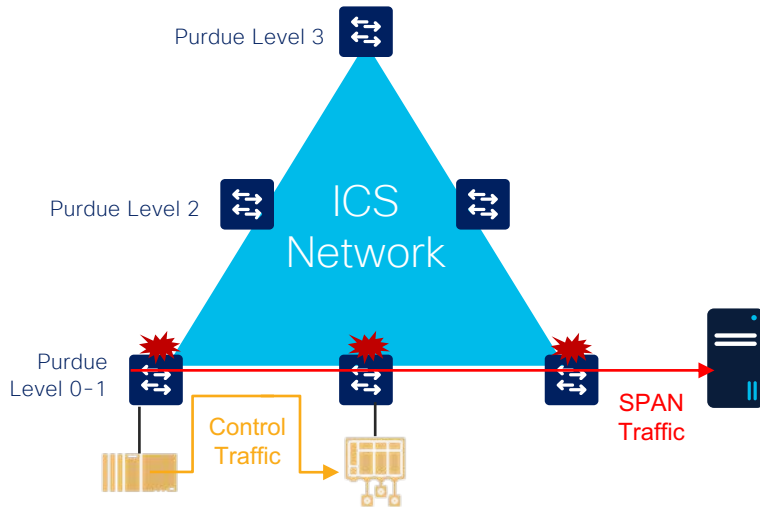


DPI Location Matters!

- 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

Why is a network-sensor important?



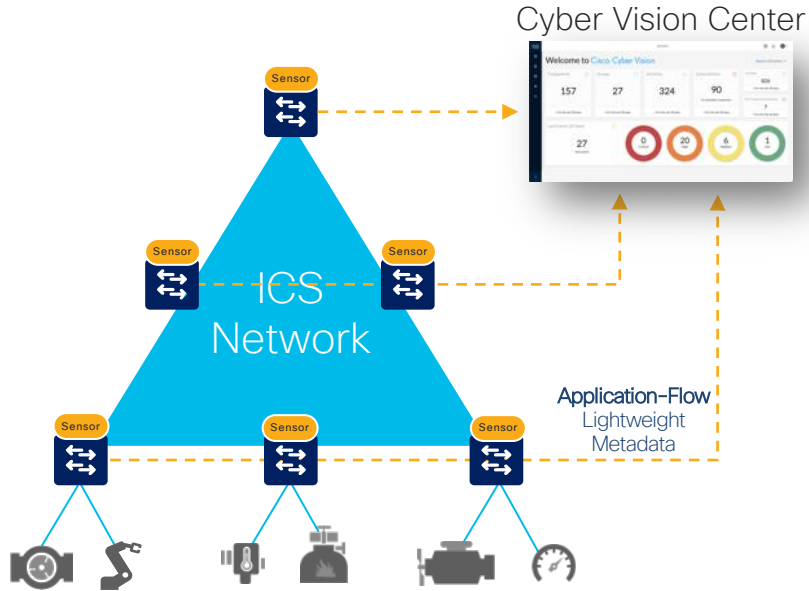
RSPAN introduces Jitter!

- 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

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

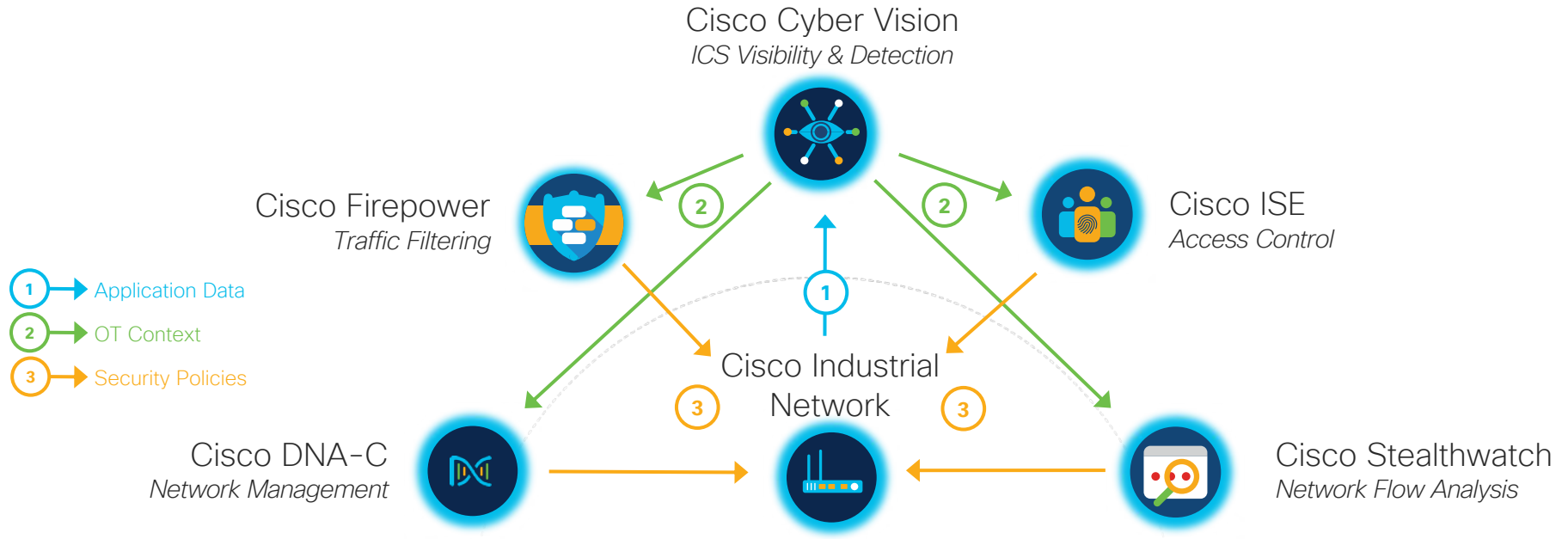


is the only vendor on the market with an edge strategy for OT cybersecurity

”Magic pill” ?

The Only Fully Integrated OT Security Solution

Working together to define & apply IoT security policies



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

ICS Visibility



Cisco Industrial Network Provides Visibility and Enforces Security Policy



TrustSec



Industrial Switching



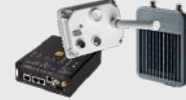
Industrial Wireless



Industrial Routing



IoT Gateways



Mesh / LoRA



Industrial Firewalls



Embedded

Cisco Stealthwatch Integration

Speed up incident response and forensics



ICS Visibility



PLC



IO



DRIVE



CONTROLLER



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

Cisco Firepower Integration

OT context for creating rules, remediation, and impact assessment



ICS Visibility



PLC



IO



DRIVE



CONTROLLER



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

Splunk Integration

Unified IT/OT security events management in SIEM



ICS Visibility



Syslog

splunkenterprise App: Search & Reporting

Search > Analytics > Datasets > Reports > Alerts > Dashboards

New Search

source="udp:514" sourcetype="syslog"

2 events (before 11/12/19 5:42:44.000 PM) No Event Sampling

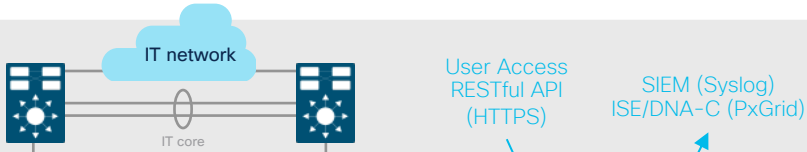
Time	Event
11/12/19 5:42:33.000 PM	Nov 12 17:42:33 10.1.100.10 Nov 12 17:42:28 rsyslogd cybervision[2]: CEP:0 sentry cybervision 1.0 token_new Cyber Vision API token added licat-Cyber Vision Administration msgToken test has been added by admin admin user=admin@cisico.com spriv=Administrator SCVEventType=token SCVTokenId=df578372-01ad-4e21-af37-e61582a4559b SCVTokenName=test SCVTokenEnable=true SCVTokenAction=add SCVAuthorId=477d2bf-475f-4ab6-b23b-4264a368487f host = 10.110010 source = udp:514 sourcetype = syslog
11/12/19 5:40:49.000 PM	Nov 12 17:40:49 10.1.100.10 Nov 12 17:40:44 rsyslogd cybervision[2]: Id="351e61d5-6ba8-4258-9559-78be32a9cc31" type="Software" severity="Medium" category="Cyber Vision Administration" family="Cyber vision" description="admin admin has changed Syslog configuration to local3.A" udp10.1.100.8:514 host = 10.110010 source = udp:514 sourcetype = syslog

Architecture with Cybersecurity?

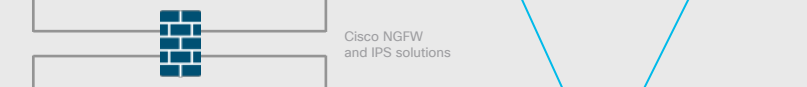
Converged Industrial Architectures

Enterprise Zone

Purdue Level 4



DMZ



Industrial Zone

Purdue Level 3



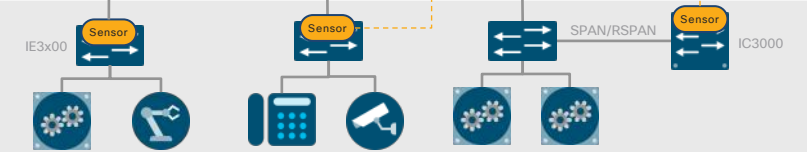
Area Zone

Purdue Level 2



Cell Zone

Purdue Level 0-1



User Access RESTful API (HTTPS)

SIEM (Syslog) ISE/DNA-C (PxGrid)



Cisco Components

Industrial DMZ	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> AAA identity services Network management Asset inventory Anomaly detection Plant-wide services Traffic enforcement (plant to IDMZ, north/south)
Area zone	<ul style="list-style-type: none"> Traffic Enforcement (Cell to Cell, East/West) QoS Prioritization SXP Netflow
Inter-cell (ISA3000)	<ul style="list-style-type: none"> Industrial deep packet inspection (DPI) Stateful firewall and intrusion prevention (IPS) Hardware bypass
Cell zone	<ul style="list-style-type: none"> 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)

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



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>

