



Securing your Operational Technology Networks

Cisco Gulf Region Webinar Series
May-June 2020

Speakers



Eddy Busaidy

IoT Product Sales Specialist
Cisco

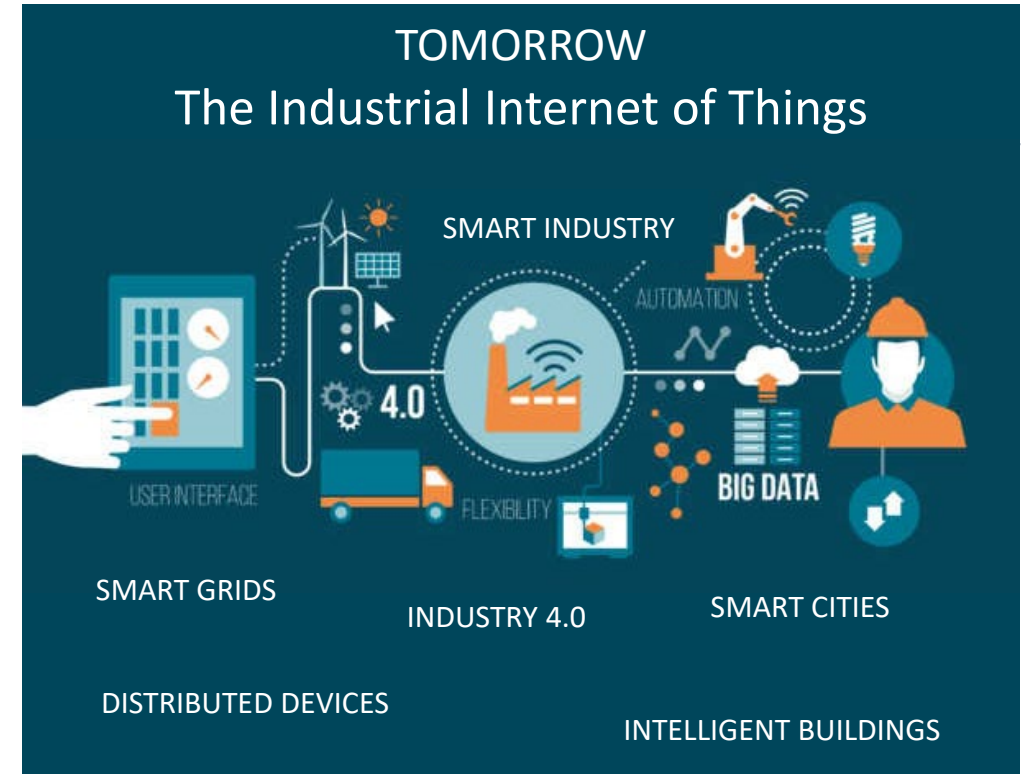
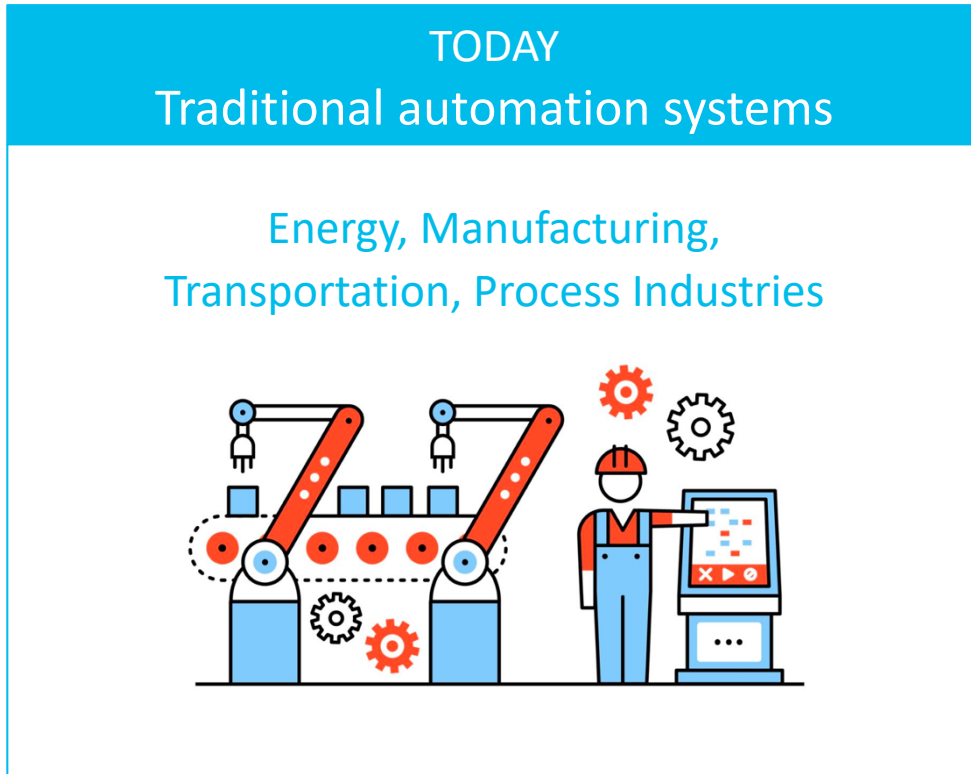
mbusaidy@cisco.com
www.cisco.com

***Securing Your Operational
Technology Networks***

Agenda

- ❑ Overview of Cisco Cyber Vision
- ❑ Cyber Vision Product Portfolio
- ❑ Cisco Services
- ❑ Demo
- ❑ Q&A

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



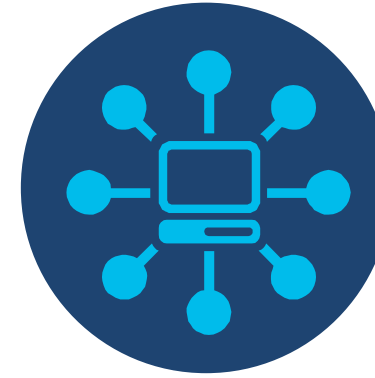
Industrial Control Systems are not designed for cybersecurity

You cannot secure what you don't know



Most customers don't have
accurate asset inventory

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

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



On June 6th, 2019 Cisco announced its intent to acquire Sentryo

Sentryo will become Cisco's worldwide expertise center for ICS cybersecurity

Sentryo will join Cisco's IoT business unit dedicated to industrial networks

Operation is expected to close before ~~October 26th, 2019~~

August 8th, 2019

Cisco IoT

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

Designed to meet the needs of all stakeholders



Security Leaders

Protect industrial operations
against cyber threats

Extend your SOC capabilities
to the OT domain

Enable collaboration
with OT teams



Industrial Operations

Ensure production continuity, integrity
and safety

Gain visibility on OT assets to implement
security best practices

Collect critical insights on OT processes to
ease day-to-day operations



Network Managers

Deploy industrial IoT at scale with
security and low TCO

Gain visibility to drive network
segmentation projects

Embed security into network equipment
for easy deployment

Cyber Vision

Control Center

SIEM or SOC Integration

Continuous Asset
Discovery &
Inventory

Configuration
Change Detection

Event Monitoring

Detection &
Alerting

Forensics Engine

Reporting Engine

Machine Learning ICS Behavioral Models

Hosts / Devices

Configuration, OS,
Firmware, Malfunctions

Network

Topology,
Malfunctions

Communication

Anomalies of traffic load, destinations,
protocols, timing, messages types, fields and
values

Malicious Intent

Known attacks (signatures), spoofing,
poisoning, man-in-the-middle

Network Monitoring

Deep Packet Inspection (DPI) Engine, ICS-Proprietary Protocols

Field Bus / Serial Networks

IP Networks

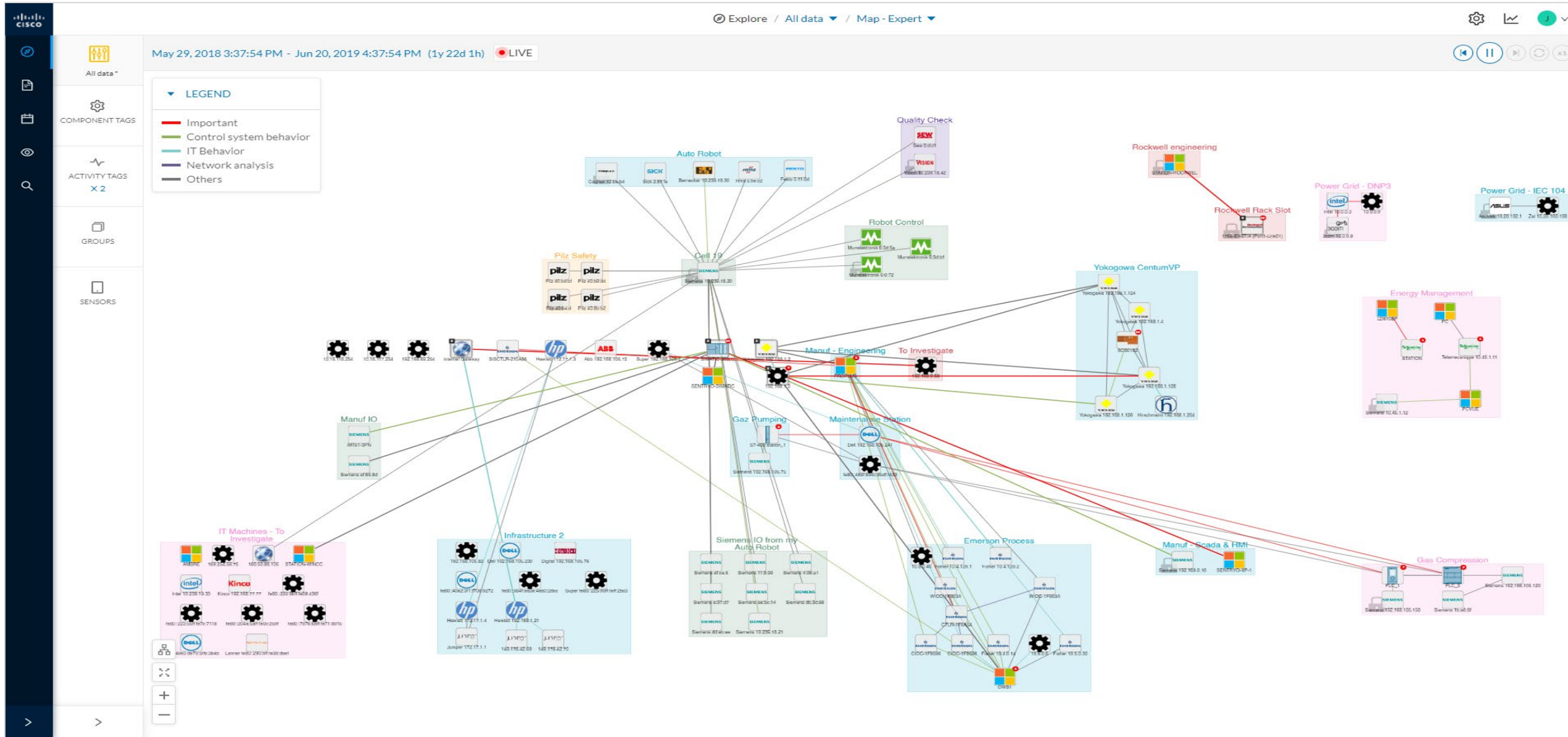
Cyber Vision Visibility

Comprehensive Asset Inventory

</

Cyber Vision Visibility

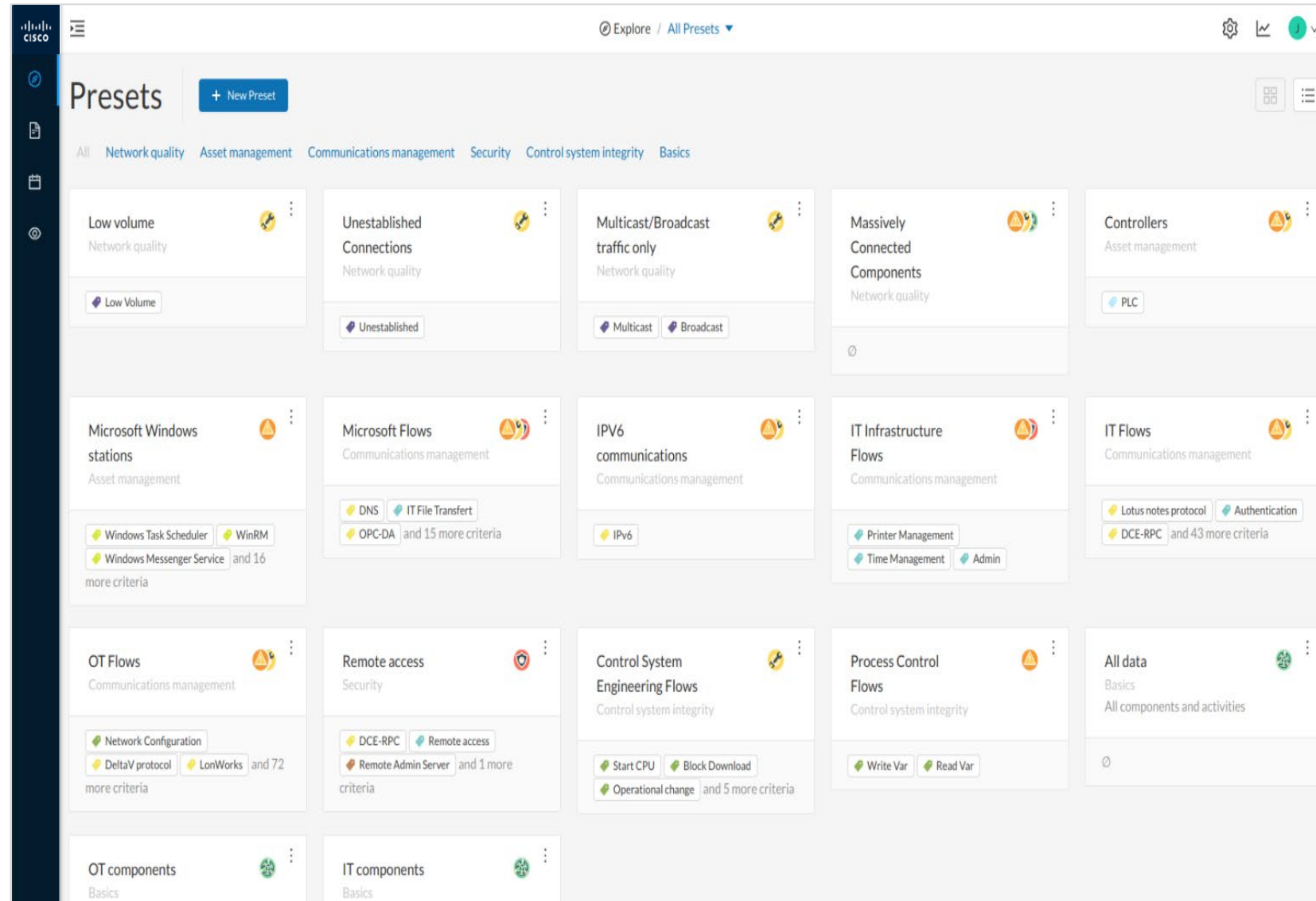
Dynamic Communication Map



Visibility: Guided Data Discovery

Focus on what is most important to you

- 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



Cyber Vision Operational Insights


- Asset functions and application flows are converted to Tags and Events:
Anyone can understand what is going on
- Track variable changes to monitor the integrity of your industrial process

Variables accesses						13
						< 1 > 20 / page
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		


<

Activity

X




PLC_3




Gas Compression ▲ very high

IP: 192.168.105.130
MAC: 28:63:36:82:28:96



Dell 192.168.105.241



Maintenance Station ▲ high

IP: 192.168.105.241
MAC: 34:17:eb:d1:c9:97

First activity

⌚ Apr 6, 2017 10:59:13 PM

Last activity

⌚ Jun 20, 2019 12:22:27 AM

Tags:

Program Upload

,

Start CPU

,

Stop CPU

,

Read Var

,

Write Var

,

ARP

,

S7Plus

(hide)

Visibility: Instantaneous Vulnerability Identification

- Automatically spot software vulnerabilities across all your industrial assets
- Access comprehensive information on vulnerability severities and solutions
- Built-in vulnerability database always up to date

The screenshot displays the Siemens SIMATIC Manager interface, specifically the 'Vulnerabilities' section. At the top, a 'Component' header shows 'SIMATIC 300(1)' with IP '192.168.0.1' and MAC '00:0e:8c:84:5b:a6'. It also indicates 'First activity' on Apr 6, 2017, and 'Last activity' on Jun 20, 2019. A 'Vulnerabilities' badge shows 5 vulnerabilities. Below this, a navigation bar includes 'Basics', 'Security' (selected), 'Activity', and 'Automation'. The 'Vulnerabilities' tab is active, showing a list of vulnerabilities. Two vulnerabilities are visible, both with a CVSS score of 7.8. The first is 'Multiple Siemens Products CVE-2017-12741 Denial of Service Vulnerability', and the second is 'SIMATIC S7-300 and S7-400 CPUs Denial of Service and Information Disclosure Vulnerabilities'. Both entries include a description, a solution, publication date, identification date, and links to Siemens security advisories. To the right of each vulnerability entry is a detailed CVSS score breakdown, including Access Vector, Access Complexity, Authentication, Confidentiality impact, Integrity impact, and Availability impact. At the bottom, a third vulnerability entry is partially visible: 'Multiple Denial of Service Vulnerabilities on Siemens devices using the PROFINET Discovery and'.

Component

SIMATIC 300(1)
IP: 192.168.0.1
MAC: 00:0e:8c:84:5b:a6

First activity
Apr 6, 2017 11:29:22 PM

Last activity
Jun 20, 2019 12:22:18 AM

Read Var , PLC

Add to group Create group

24 Flows
51 Events
13 Variables
- Credential

Vulnerabilities 5

Basics Security Activity Automation

Vulnerabilities Credentials

Vulnerabilities

☐ **Multiple Siemens Products CVE-2017-12741 Denial of Service Vulnerability**
CVE-2017-12741

Several industrial products are affected by a vulnerability that could allow remote attackers to conduct a Denial-of-Service (DoS) attack.

Solution
Siemens has released updates for several affected products, and recommends that customers update to the new version. Siemens is preparing further updates and recommends specific countermeasures until patches are available.

Published on November 23, 2017
Identified on this component on April 6, 2017
Identified vulnerable because of model-ref (6ES7 315-2EH13-0AB0)

Links
[Siemens Security Advisory](#)

☐ **SIMATIC S7-300 and S7-400 CPUs Denial of Service and Information Disclosure Vulnerabilities**
CVE-2016-9158

Successful exploitation of these vulnerabilities could lead to a denial-of-service condition or result in credential disclosure.

Solution
Siemens provides firmware version V3.X.14 for S7-300 CPUs that resolves CVE-2016-9158.

Published on December 16, 2016
Identified on this component on April 6, 2017
Identified vulnerable because of model-ref (6ES7 315-2EH13-0AB0)

Links
[www.siemens.com](#)
[ics-cert.us-cert.gov](#)
[www.securityfocus.com](#)

☒ **Multiple Denial of Service Vulnerabilities on Siemens devices using the PROFINET Discovery and**

7.8
score CVSS

Access Vector: Network
Access Complexity: Low
Authentication: None Required
Confidentiality impact: None
Integrity impact: None
Availability impact: Complete

Acknowledge ?

7.8
score CVSS

Access Vector: Network
Access Complexity: Low
Authentication: None Required
Confidentiality impact: None
Integrity impact: None
Availability impact: Complete

Acknowledge ?

Operational Insights: Views for Security Leaders

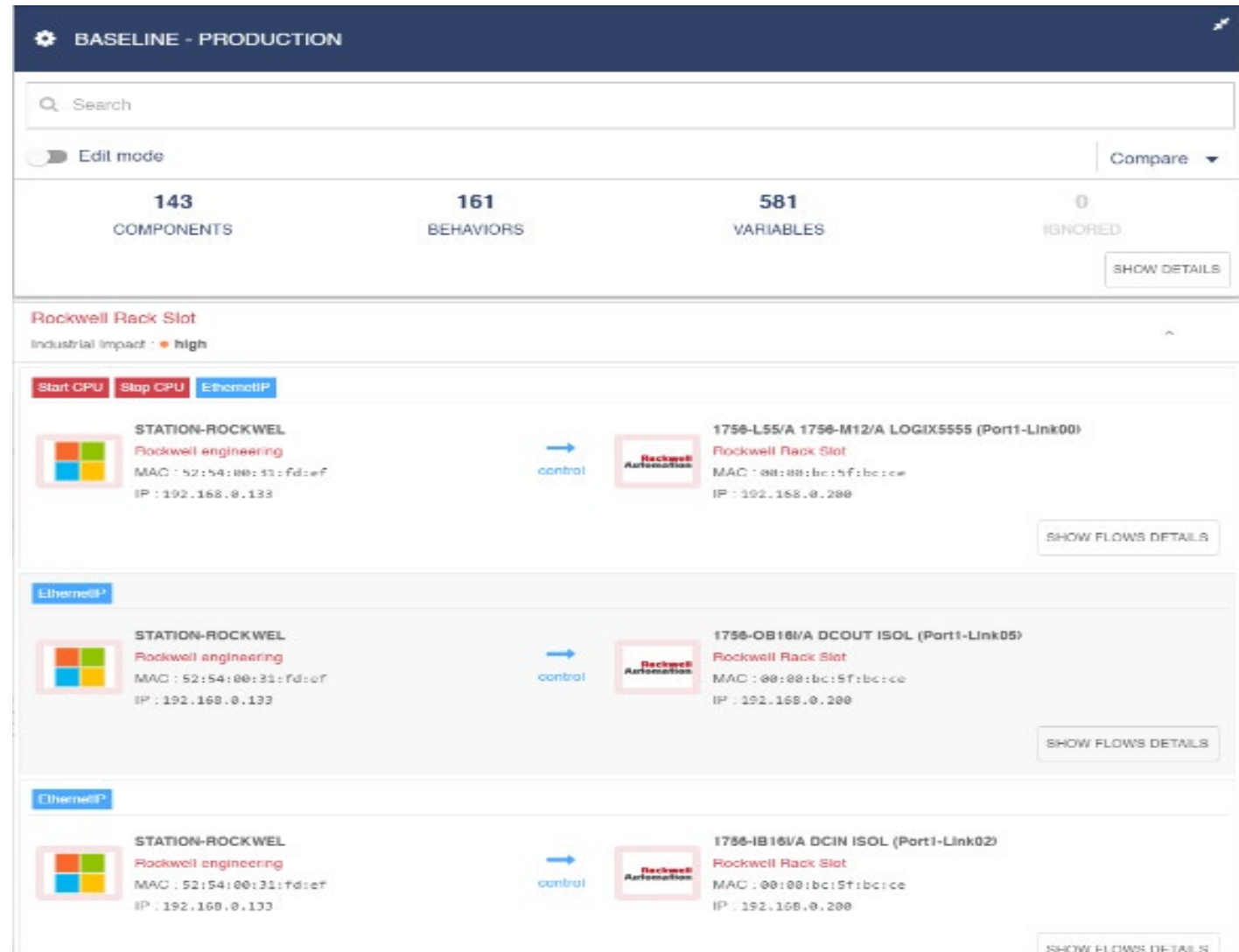
- Access the full history of all communication flows
- View detailed properties and content statistics for each flow
- View live information or go back in time for forensic search

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	No tags	0	0 B
PLC_3	0	PLC_1	0	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	1611	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	1614	Apr 6, 2017 10:59:13 PM	May 26, 2019 12:21:13 AM	No tags	0	0 B
PLC_1	102	Dell 192.168.105.241	1612	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	1614	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	No tags	0	0 B
Siemens 192.168.105.150	49162	PLC_1	102	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	No tags	0	0 B
Siemens 192.168.105.150	49163	PLC_1	102	Apr 6, 2017 10:59:13 PM	May 26, 2019 12:21:13 AM	No tags	0	0 B
PLC_1	102	Dell 192.168.105.241	1613	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	No tags	0	0 B
Siemens 192.168.105.150	0	PLC_1	0	Aug 20, 2018 6:34:42 PM	May 26, 2019 12:21:13 AM	No tags	0	0 B
PLC_1	0	PLC_1	0	Apr 6, 2017 10:59:13 PM	May 26, 2019 12:21:13 AM	No tags	0	0 B

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

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



Cyber Vision understands ICS protocols you use



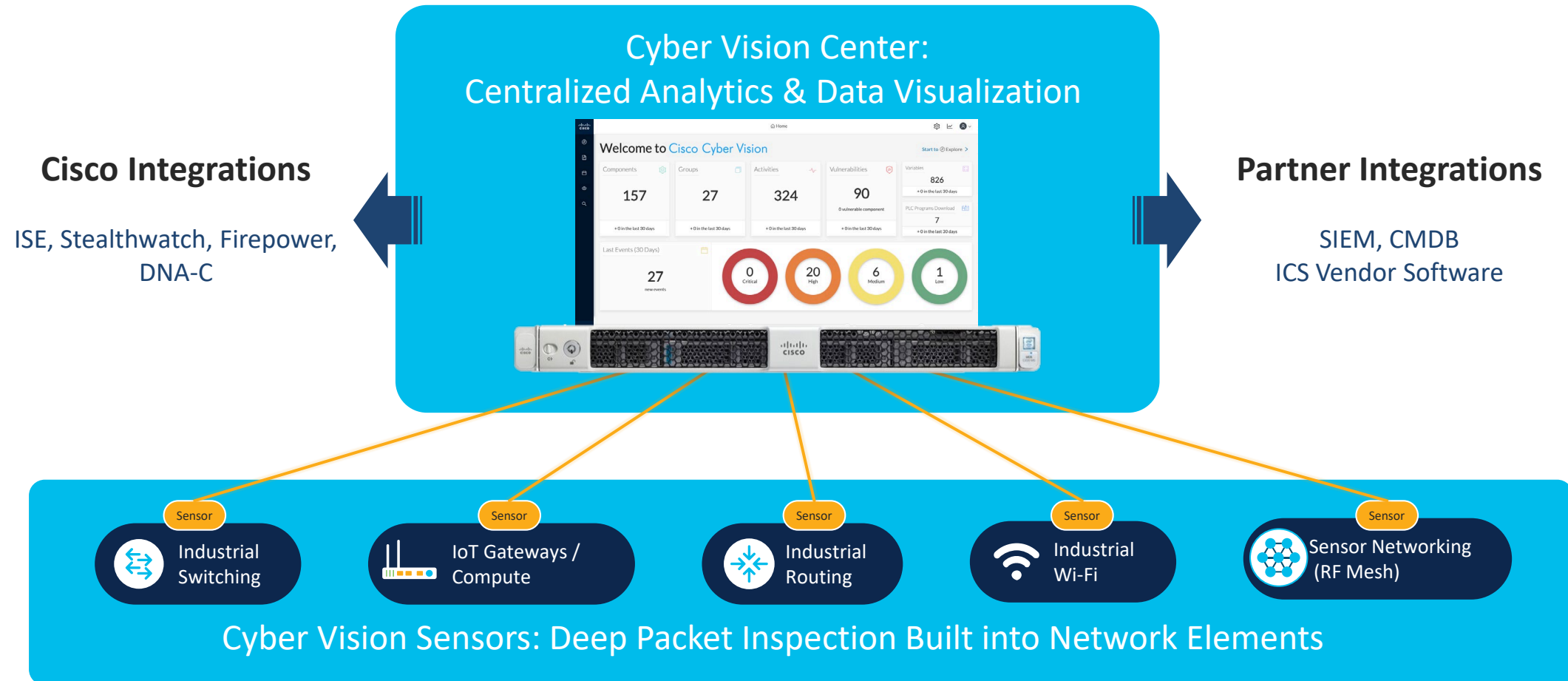
Cisco's Deep Packet Inspection understands all process information
even when using proprietary protocols

Cisco Cyber Vision

extends IT security to your OT domain through
seamless integration with your SOC and
easy deployment in your industrial network

Cisco Cyber Vision

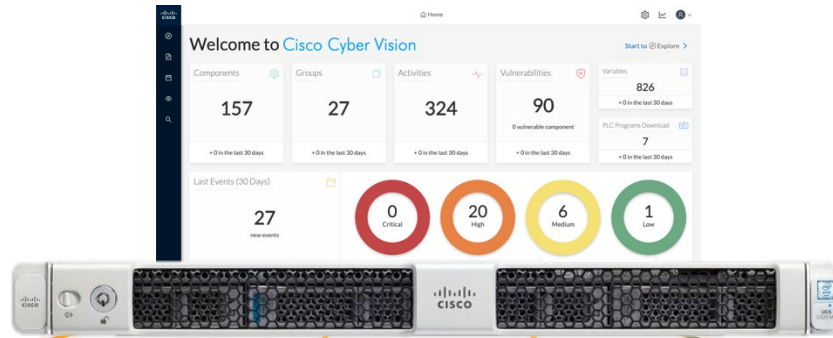
A 2-tier edge monitoring architecture that integrates with your SOC



Cisco Cyber Vision

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

Cyber Vision Center Centralized Analytics & Data Visualization



Cisco Integrations

ISE, Stealthwatch, Firepower,
DNA-C

Partner Integrations

SIEM, CMDB
ICS Vendor Software



IC3000 Industrial Compute
Hardware-Sensor
To support brownfield



IE 3400 Switch



IR 1101 Gateway

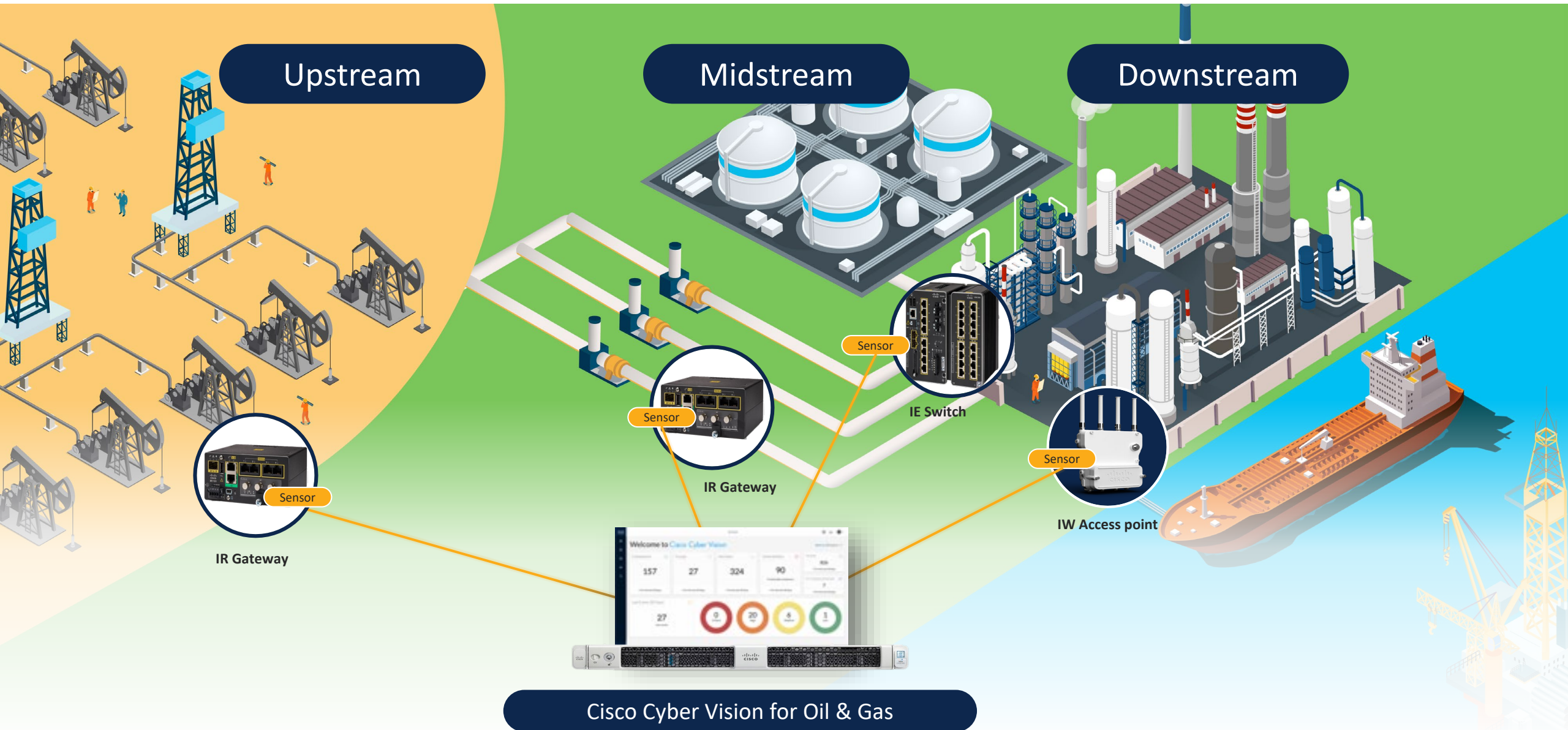


Catalyst 9300

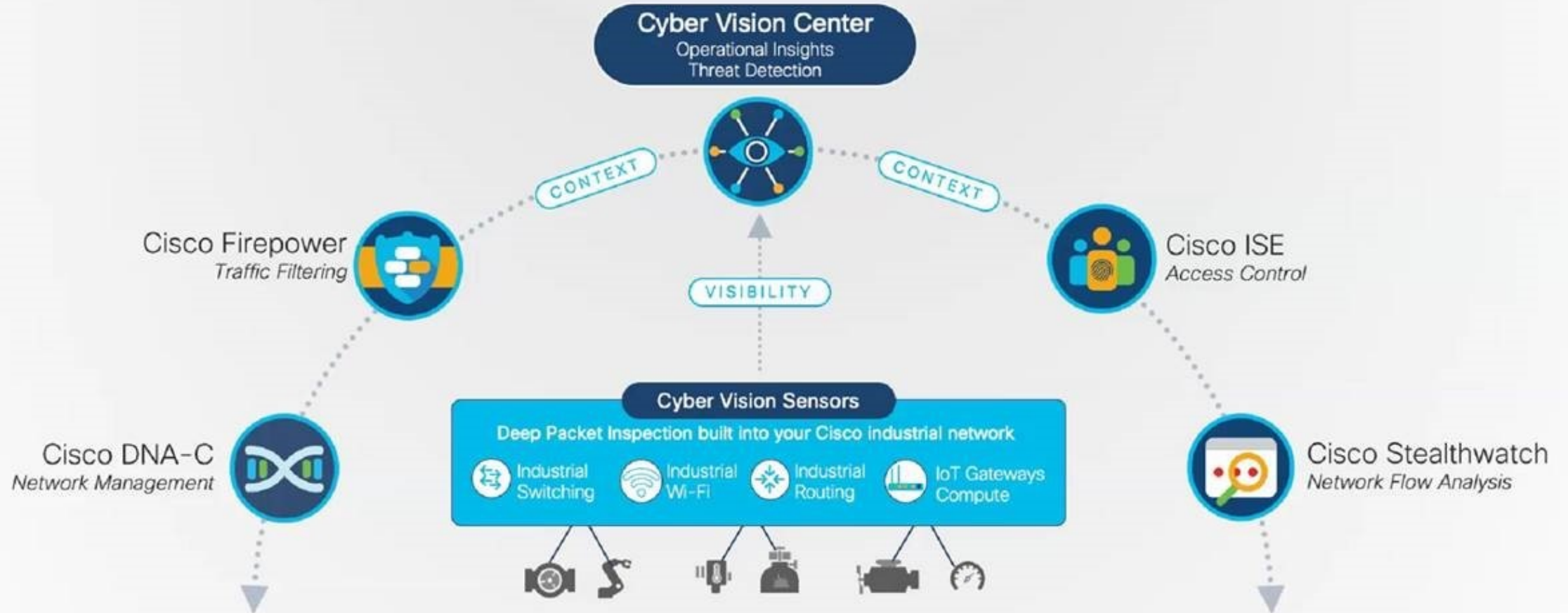
Network-Sensors

Deep Packet Inspection built into network elements

Security that can be deployed at scale



The only fully integrated IT-OT security solution



Cisco Security for Industrial IoT

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



I/O



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

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 SOC

Access Control



Firewalls



CMDB

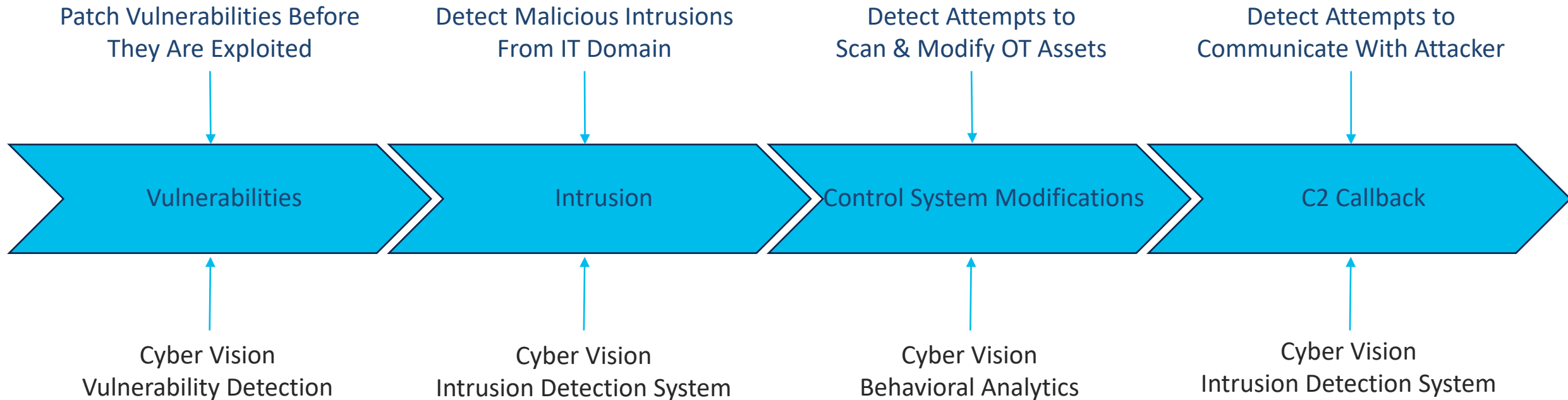


SIEM



Cyber Vision Threat Detection

Holistic Threat Detection Techniques



Cisco Services

(aka Customer Experience - CX)

Maximize your Cyber Vision investment with Cisco CX



1

Project Enablement

A set of service offers to help customers plan and kick start their OT security projects

Security Assessment

Asset Inventory and Mapping



2

Delivery

IoT CX proven delivery methodology to ensure successful deployments and delighted customers

OT Specific Project Methodology

Cisco Cross Platform Integration



3

Optimization

Ongoing optimization & services to assure product usage, maximize performance and identify expansion opportunities

Ongoing Consultation Services

User & Partner Training



4

Support

Multiple flavors of support to drive customers towards faster resolution of issues, maintain reliability and maximize ROI

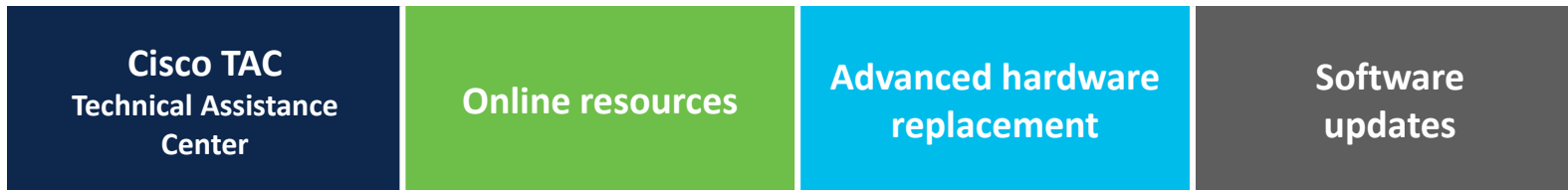
Software Support Services (SWSS)

Solution Support

Cisco Smart Net Total Care



Technical Support Capabilities



Award-winning technical support

HTTS Locations



Cyber Vision Demo

Processing Monitoring Data at the Edge



Leverage Your Existing
Network Equipment



Simplify Your
Monitoring Network



Reduce Your Costs



Ready to Scale



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

Follow up with us!

Speaker Details:

Eddy Busaidy (mbusaidy@cisco.com)

Cisco Cyber Vision:

<https://www.cisco.com/c/en/us/products/security/cyber-vision/index.html>

Cisco Security Portfolio:

<https://www.cisco.com/c/en/us/products/security/index.html>

Cisco Oil & Gas Portfolio Explorer:

https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-oil-and-gas.html





IoT Portfolio

Industrial Switching



IE 1K, 2K, 3K, 3200, 3300, 3400, 3400H, 4K, 5K, CGS

IoT Gateways / Compute



819-MNA, IR807, IR809, IR829, IR1101, IC3000

Industrial Routing



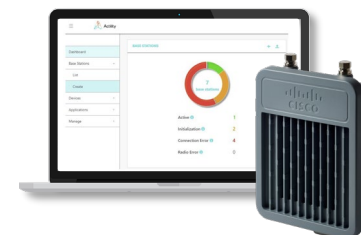
ASR 902U/903U/920U, CGR 1000, CGR 2000

Cisco Resilient Mesh



IR500, DevNet

Low Power Wide Area Wireless



LoRaWAN IXM Gateway

Industrial Wireless



AP1552, IW3702, IW6300

Industrial Security



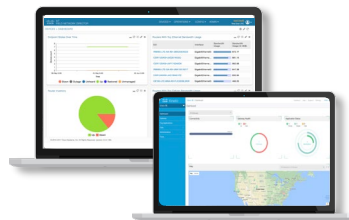
ISA 3000 Cyber Vision

Embedded IoT



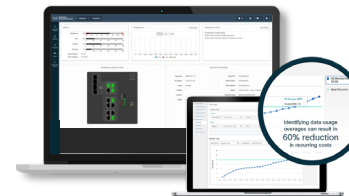
ESS, ESR, ESW

Edge Computing Software



IOx

Management & Automation



Field Network Director
Industrial Network Director
Control Center & GMM

Cisco Vision



Dynamic Signage Director
Digital Media Players