You make **possible**

Securing Industrial Networks

Introduction to Cisco Cyber Vision

Fabien Maisl, Product Marketing Manager
Dan Berhens, Technical Marketing Engineer

PSOIOT-2555

Barcelona | January 27-31, 2020

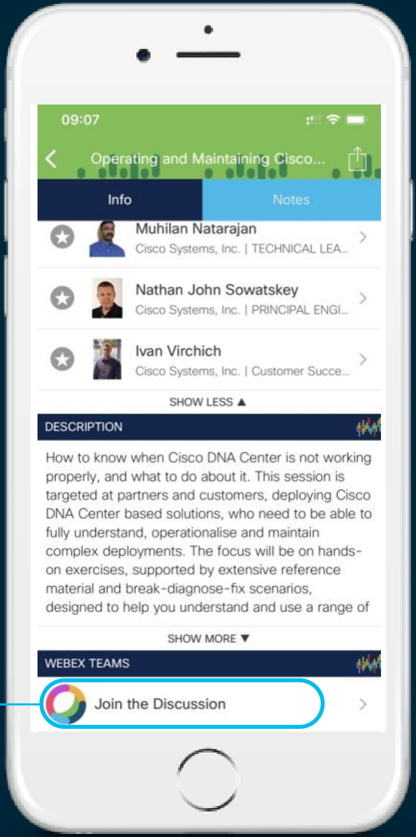
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat
with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



09:07

Operating and Maintaining Cisco...

Muhilan Natarajan
Cisco Systems, Inc. | TECHNICAL LEA...

Nathan John Sowatskey
Cisco Systems, Inc. | PRINCIPAL ENGI...

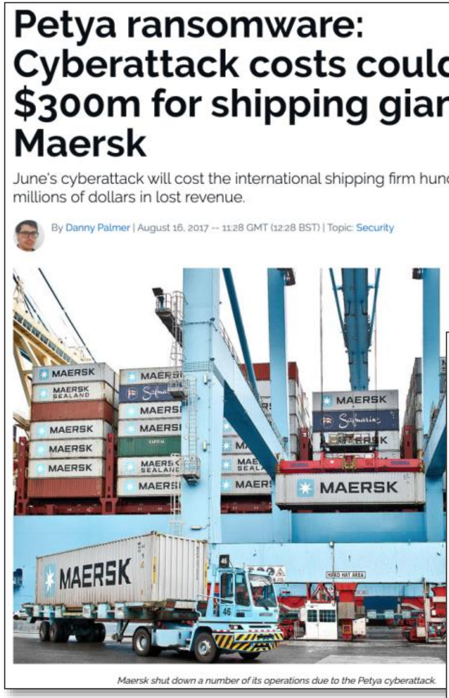
Ivan Virchich
Cisco Systems, Inc. | Customer Succe...

DESCRIPTION

How to know when Cisco DNA Center is not working properly, and what to do about it. This session is targeted at partners and customers, deploying Cisco DNA Center based solutions, who need to be able to fully understand, operationalise and maintain complex deployments. The focus will be on hands-on exercises, supported by extensive reference material and break-diagnose-fix scenarios, designed to help you understand and use a range of

WEBEX TEAMS

Industrial networks are a new target for hackers

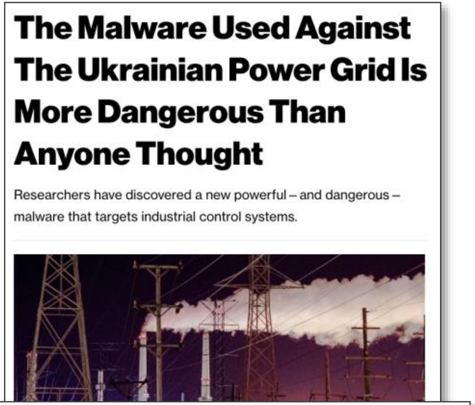


Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk

June's cyberattack will cost the international shipping firm hundreds of millions of dollars in lost revenue.

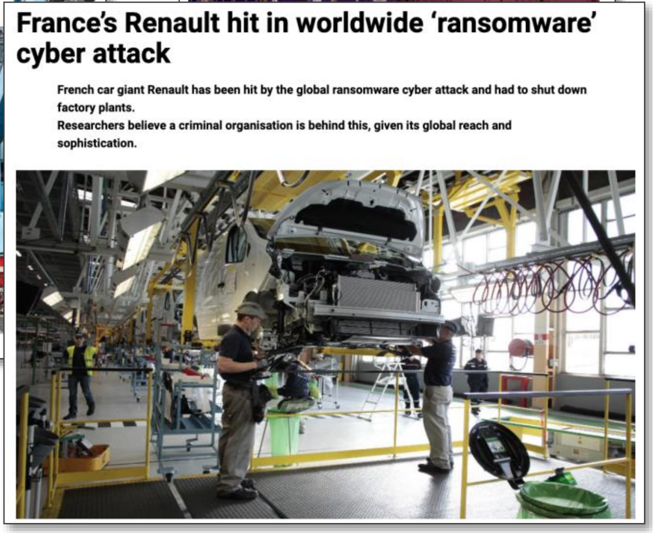
By Danny Palmer | August 16, 2017 -- 11:28 GMT (12:28 BST) | Topic: Security

Maersk shut down a number of its operations due to the Petya cyberattack



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

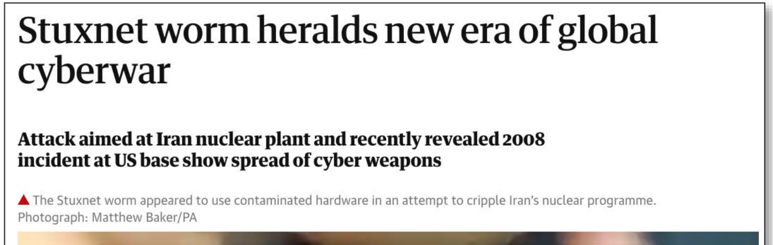
Researchers have discovered a new powerful – and dangerous – malware that targets industrial control systems.



France's Renault hit in worldwide 'ransomware' cyber attack

French car giant Renault has been hit by the global ransomware cyber attack and had to shut down factory plants.

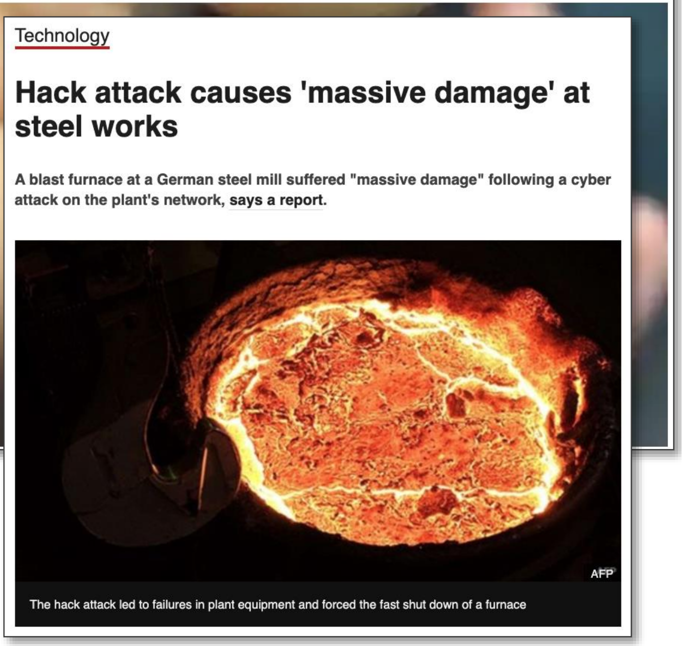
Researchers believe a criminal organisation is behind this, given its global reach and sophistication.



Stuxnet worm heralds new era of global cyberwar

Attack aimed at Iran nuclear plant and recently revealed 2008 incident at US base show spread of cyber weapons

▲ The Stuxnet worm appeared to use contaminated hardware in an attempt to cripple Iran's nuclear programme. Photograph: Matthew Baker/PA



Technology

Hack attack causes 'massive damage' at steel works

A blast furnace at a German steel mill suffered "massive damage" following a cyber attack on the plant's network, says a report.

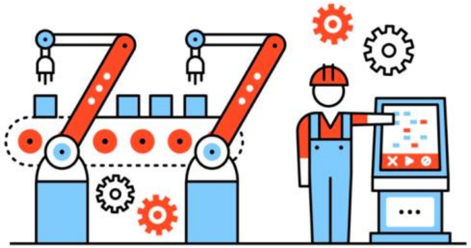
AFP

The hack attack led to failures in plant equipment and forced the fast shut down of a furnace

The modern industry is even **more connected**

TODAY
Industrial Control Systems (ICS)

Energy, Manufacturing, Transportation, Process



TOMORROW
Industrial Internet of Things (IIoT)

SMART GRIDS

INDUSTRY 4.0

SMART CITIES

DISTRIBUTED DEVICES

INTELLIGENT BUILDINGS

Industry digitization increases the attack surface

Agenda

1 The challenges of securing industrial systems

2 Why does the OT security architecture matter?

3 Benefits of converged OT-IT security operations

4 Cisco Cyber Vision demonstration

The challenges of securing industrial systems

68%

Security is the biggest challenge for Industrial IoT deployments

Source: *2018 ZK Research Network Purchase Intention Survey*

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

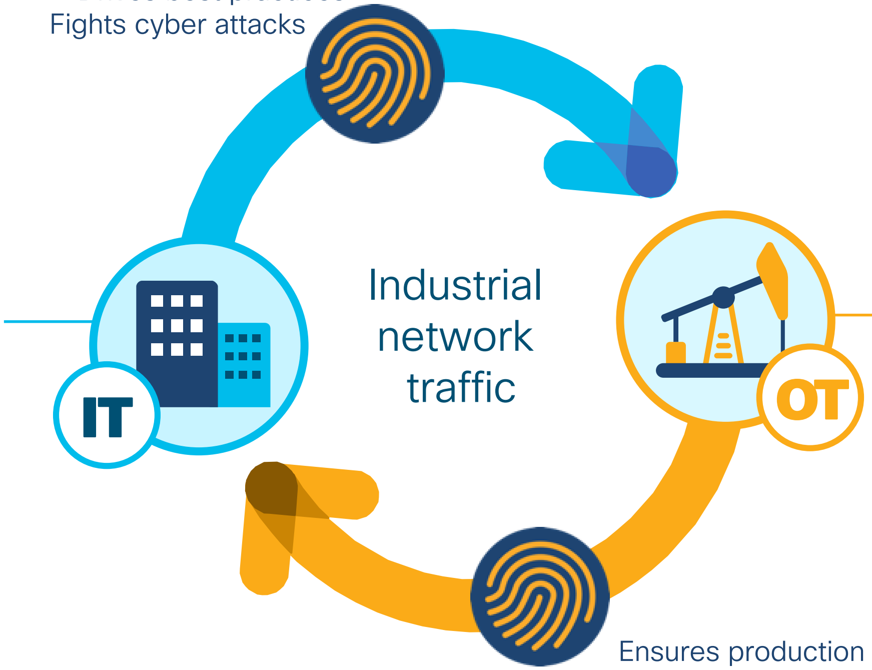
ICS equipment deployed over the years without strict security policies

Industrial control systems are not regular IT things

ABB
PHŒNIX CONTACT
Schneider Electric
GE
EMERSON
Rockwell Automation
SIEMENS
EATON
BECKHOFF
MITSUBISHI ELECTRIC
Honeywell
OMRON
YOKOGAWA

Proprietary industrial protocols your IT security tools don’t understand

IT-OT collaboration is vital for securing ICS



Drives best practices
Fights cyber attacks

Cybersecurity skills
Network hygiene
Security policies
Detection & Remediation

Industrial process skills
Operational events context
Asset criticality levels
Equipment configuration

Ensures production continuity
Defines behavioral baselines

Cisco Cyber Vision

Asset inventory & security platform for the Industrial IoT

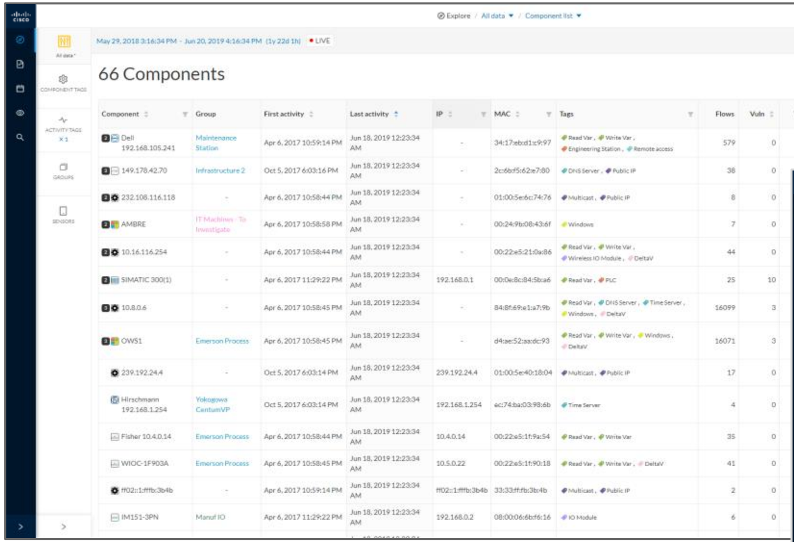
Protect your industrial control systems against cyber risks

Visibility
Know your assets

Insights
Track your processes

Detection
Trigger alerts

Cyber Vision **visibility**



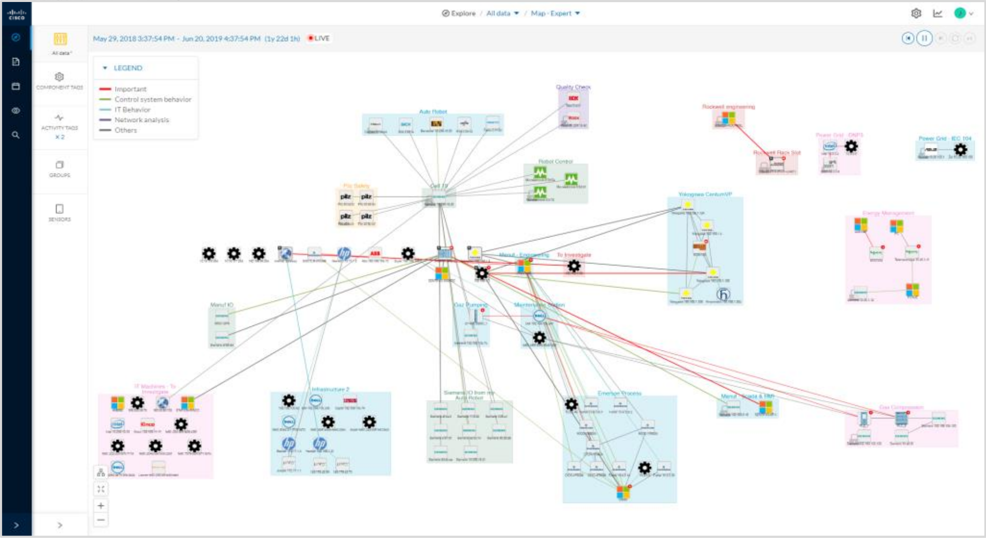
Explore / All data ▾ / Component list ▾
May 29, 2018 3:16:34 PM - Jun 20, 2019 4:16:34 PM (1y 22d 1h) ● LIVE
All data
COMPONENT TAGS
ACTIVITY TAGS × 1
GROUPS
SENSORS
< 1 2 3 4 > 20 / page

66 Components

Component	Group	First activity	Last activity	IP	MAC	Tags	Flows	Vuln	Var	Vendor	OS
Dell 192.168.105.241	Maintenance Station	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23:34 AM	-	34:17:eb:d1:c9:97	Read Var , Write Var , Engineering Station , Remote access	579	0	0	Dell Inc.	-
149.178.42.70	Infrastructure 2	Oct 5, 2017 6:03:16 PM	Jun 18, 2019 12:23:34 AM	-	2c:6b:f5:62:e7:80	DNS Server , Public IP	38	0			
232.108.116.118	-	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	-	01:00:5e:6c:74:76	Multicast , Public IP	8	0			
AMBRE	IT Machines - To Investigate	Apr 6, 2017 10:58:58 PM	Jun 18, 2019 12:23:34 AM	-	00:24:9b:08:43:6f	Windows	7	0			
10.16.116.254	-	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	-	00:22:e5:21:0a:86	Read Var , Write Var , Wireless IO Module , DeltaV	44	0			
SIMATIC 300(1)	-	Apr 6, 2017 11:29:22 PM	Jun 18, 2019 12:23:34 AM	192.168.0.1	00:0e:8c:84:5b:a6	Read Var , PLC	25	10			
10.8.0.6	-	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	-	84:8f:69:e1:a7:9b	Read Var , DNS Server , Time Server , Windows , DeltaV	16099	3			
OWS1	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	-	d4:ae:52:aa:dc:93	Read Var , Write Var , Windows , DeltaV	16071	3			
239.192.24.4	-	Oct 5, 2017 6:03:14 PM	Jun 18, 2019 12:23:34 AM	239.192.24.4	01:00:5e:40:18:04	Multicast , Public IP	17	0			
Hirschmann 192.168.1.254	Yokogowa CentumVP	Oct 5, 2017 6:03:14 PM	Jun 18, 2019 12:23:34 AM	192.168.1.254	ec:74:ba:03:98:6b	Time Server	4	0			
Fisher 10.4.0.14	Emerson Process	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	10.4.0.14	00:22:e5:1f:9a:54	Read Var , Write Var	35	0			
WIOC-1F903A	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	10.5.0.22	00:22:e5:1f:90:18	Read Var , Write Var , DeltaV	41	0			
ff02::1:fffb:3b4b	-	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23:34 AM	ff02::1:fffb:3b4b	33:33:ff:fb:3b:4b	Multicast , Public IP	2	0			
IM151-3PN	Manuf IO	Apr 6, 2017 11:29:22 PM	Jun 18, 2019 12:23:34 AM	192.168.0.2	08:00:06:6b:f6:16	IO Module	6	0			

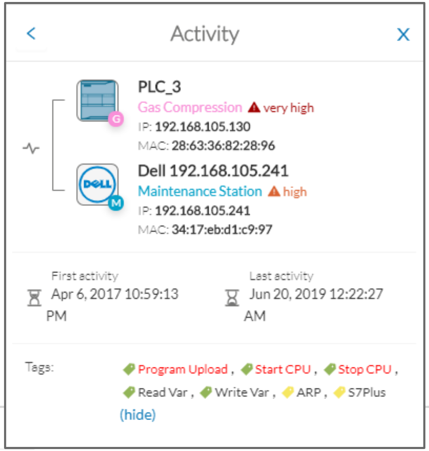
Comprehensive asset inventory

Dynamic communication map



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



Activity

PLC_3
Gas Compression ▲ very high
IP: 192.168.105.130
MAC: 28:63:36:82:28:96

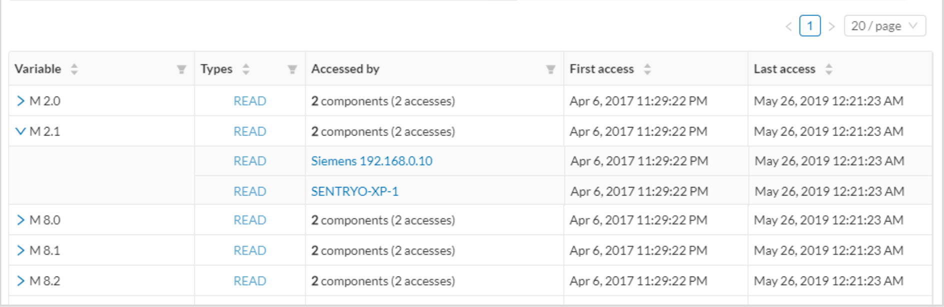
Dell 192.168.105.241
Maintenance Station ▲ high
IP: 192.168.105.241
MAC: 34:17:eb:d1:c9:97

First activity
Apr 6, 2017 10:59:13 PM

Last activity
Jun 20, 2019 12:22:27 AM

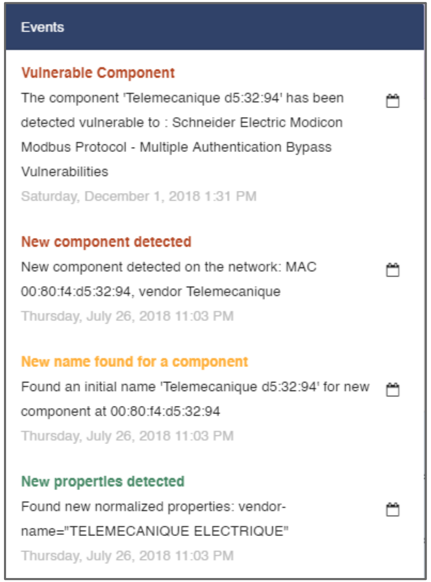
Tags: Program Upload , Start CPU , Stop CPU , Read Var , Write Var , ARP , S7Plus
(hide)

Variables accesses



< 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



Events

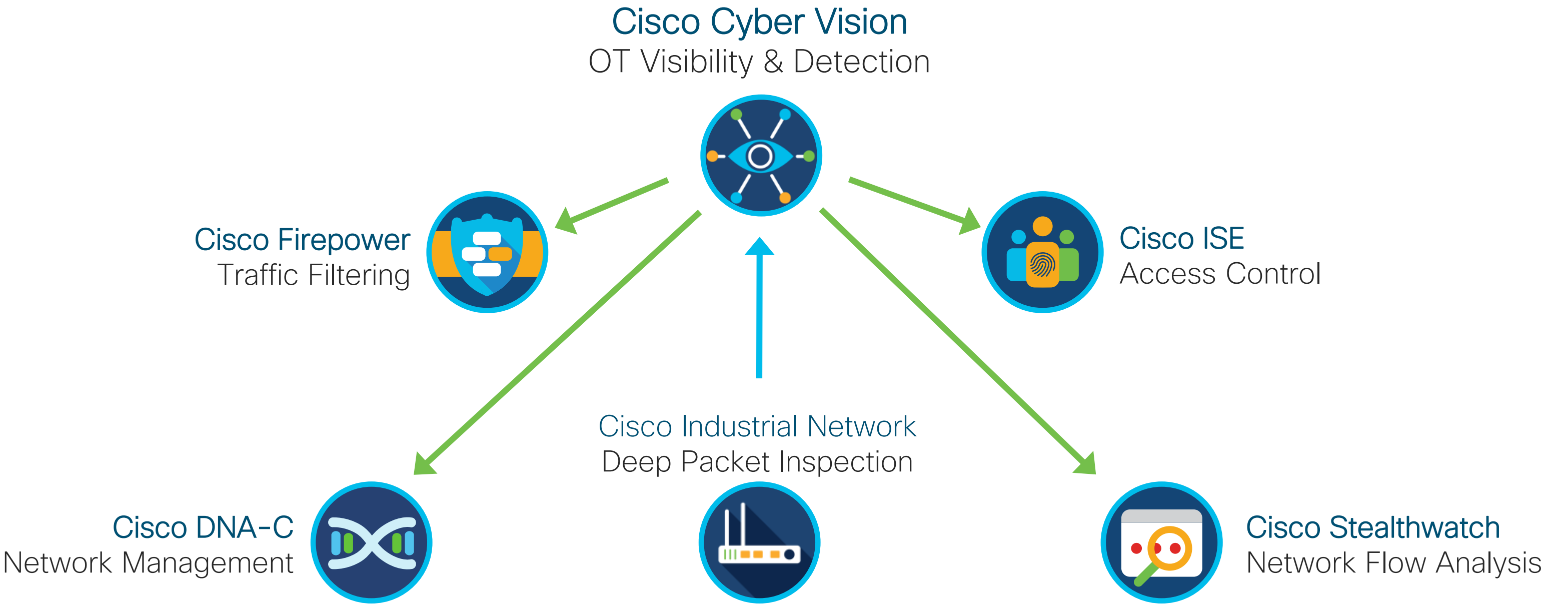
Vulnerable Component
The component 'Telemecanique d5:32:94' has been detected vulnerable to : Schneider Electric Modicon Modbus Protocol - Multiple Authentication Bypass Vulnerabilities
Saturday, December 1, 2018 1:31 PM

New component detected
New component detected on the network: MAC 00:80:f4:d5:32:94, vendor Telemecanique
Thursday, July 26, 2018 11:03 PM

New name found for a component
Found an initial name 'Telemecanique d5:32:94' for new component at 00:80:f4:d5:32:94
Thursday, July 26, 2018 11:03 PM

New properties detected
Found new normalized properties: vendor-name="TELEMECANIQUE ELECTRIQUE"
Thursday, July 26, 2018 11:03 PM

A fully integrated IT-OT security solution



Cisco Cyber Vision
OT Visibility & Detection

Cisco Firepower
Traffic Filtering

Cisco ISE
Access Control

Cisco Industrial Network
Deep Packet Inspection

Cisco DNA-C
Network Management

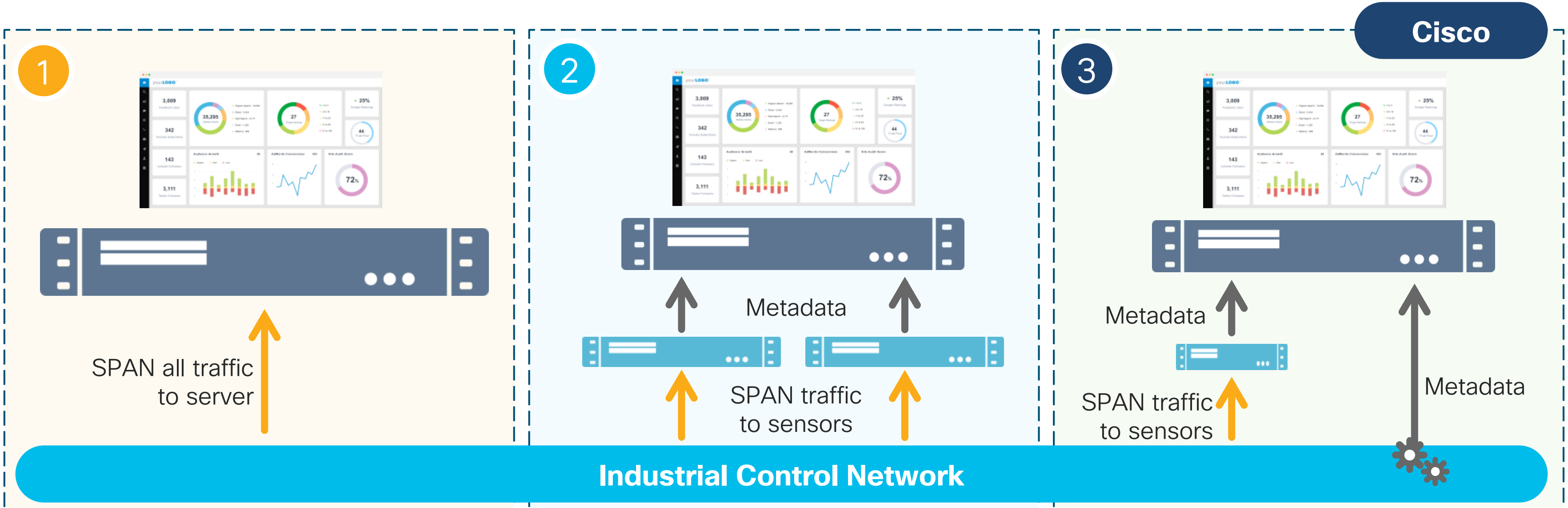
Cisco Stealthwatch
Network Flow Analysis

Working together to define and apply IoT security policies

Why does the OT security architecture matter?

ICS visibility and detection solution types

What is really going on under the hood



Central server

- DPI
- Analytics
- Visualization

Midweight sensor

- DPI
- Analytics

Server

- Additional analytics
- Visualization

Lightweight sensor

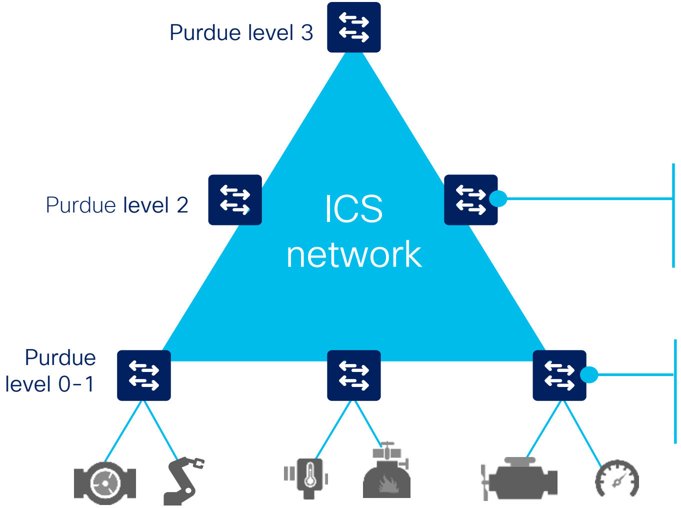
- DPI

Server

- Analytics
- Visualization

cisco Live!

Why is a network sensor important?



Suboptimal location

Most control traffic is local to the cell

Expensive

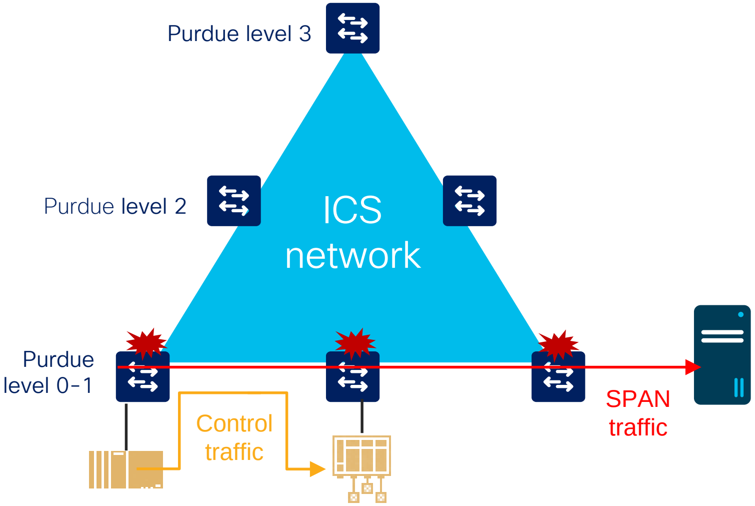
Additional Hardware, cabling for out-of-band SPAN network

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?



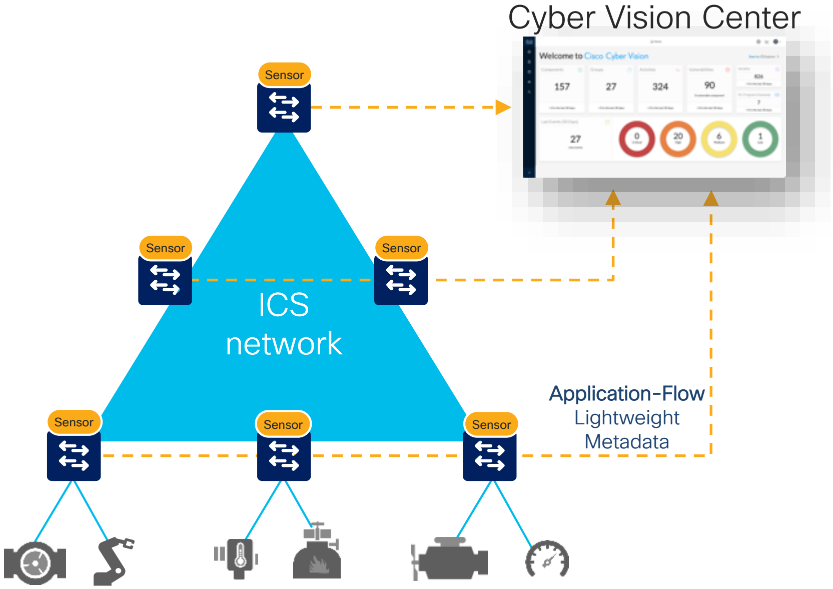
RSPAN introduces Jitter!

- 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

Cisco Cyber Vision

Visibility & detection built into your network infrastructure

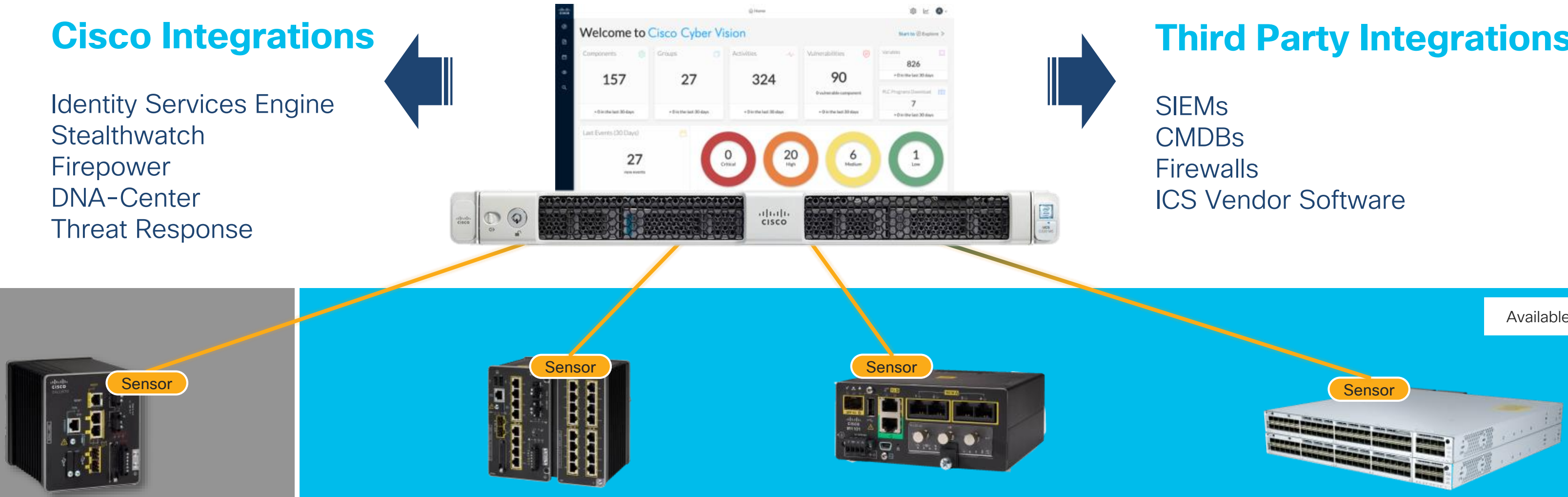


Monitoring at the edge

- **No additional hardware**: Cyber Vision Sensors embedded into industrial network equipment
- **Reduce costs**: No need for an out-of-band monitoring network
- **Built for IT and OT**: integrates with IT security workflow, provides context OT needs

CISCO OT cybersecurity at the edge from the World leader in industrial networking

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



Cyber Vision Center
Centralized Analytics & Data Visualization

Cisco Integrations

Identity Services Engine
Stealthwatch
Firepower
DNA-Center
Threat Response

Third Party Integrations

SIEMs
CMDBs
Firewalls
ICS Vendor Software

Available Spring 2020

IC3000 Industrial Compute

Hardware-Sensor
DPI via SPAN ports

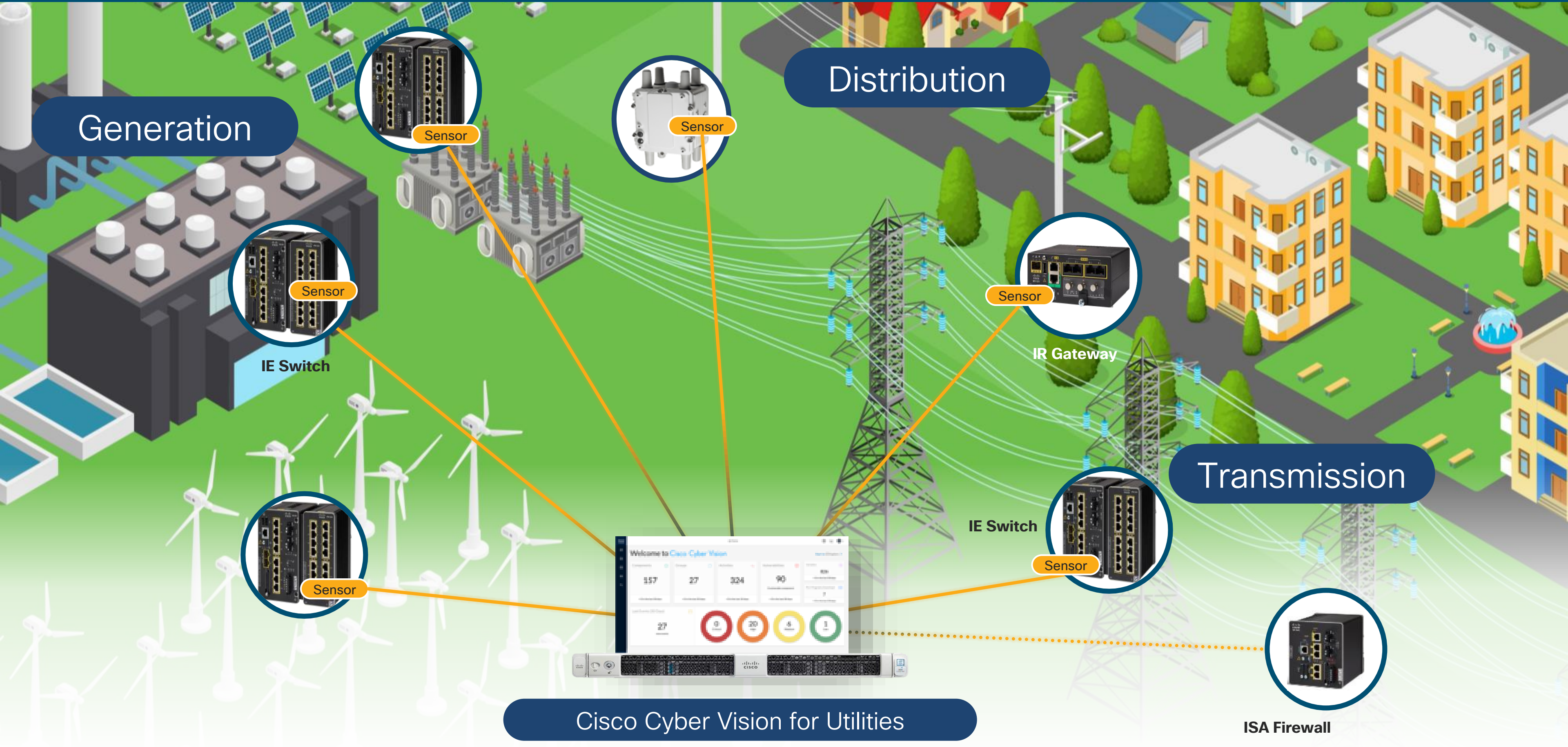
IE 3400 Switch

IR 1101 Gateway

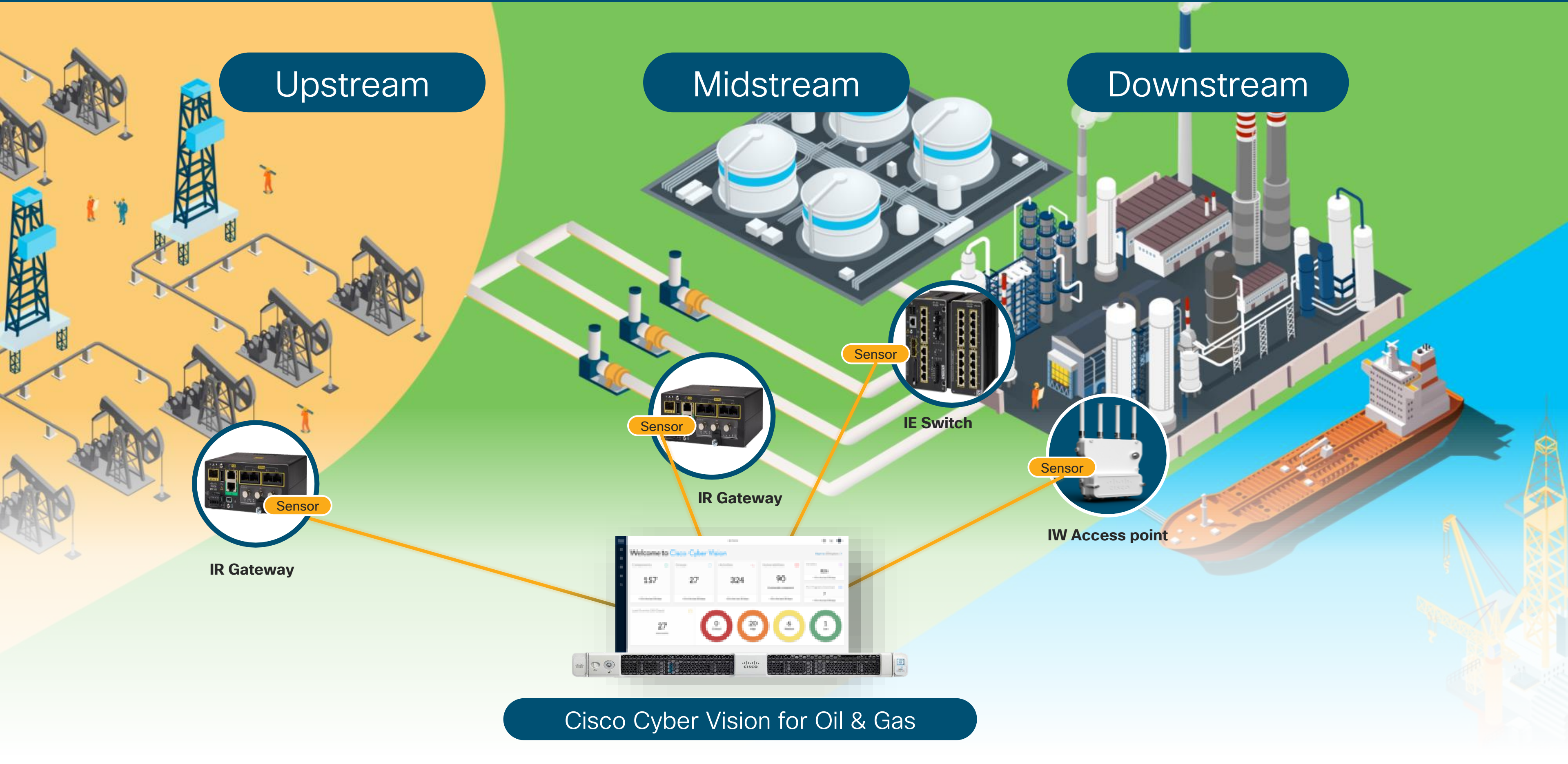
Catalyst 9000 Series Switch

Network-Sensors
Deep Packet Inspection built into network elements

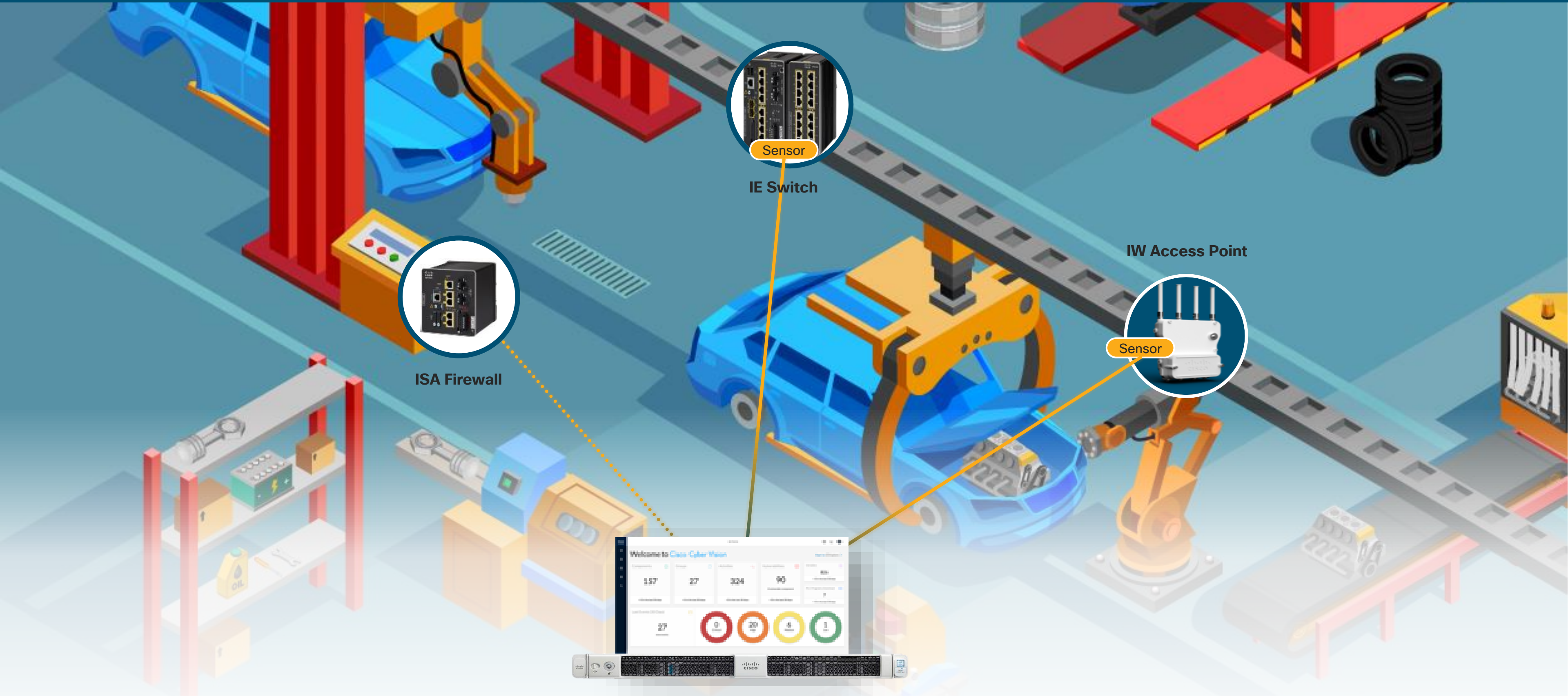
Industrial cybersecurity that can be **deployed at scale**



Industrial cybersecurity that can be **deployed at scale**



Industrial cybersecurity that can be **deployed at scale**

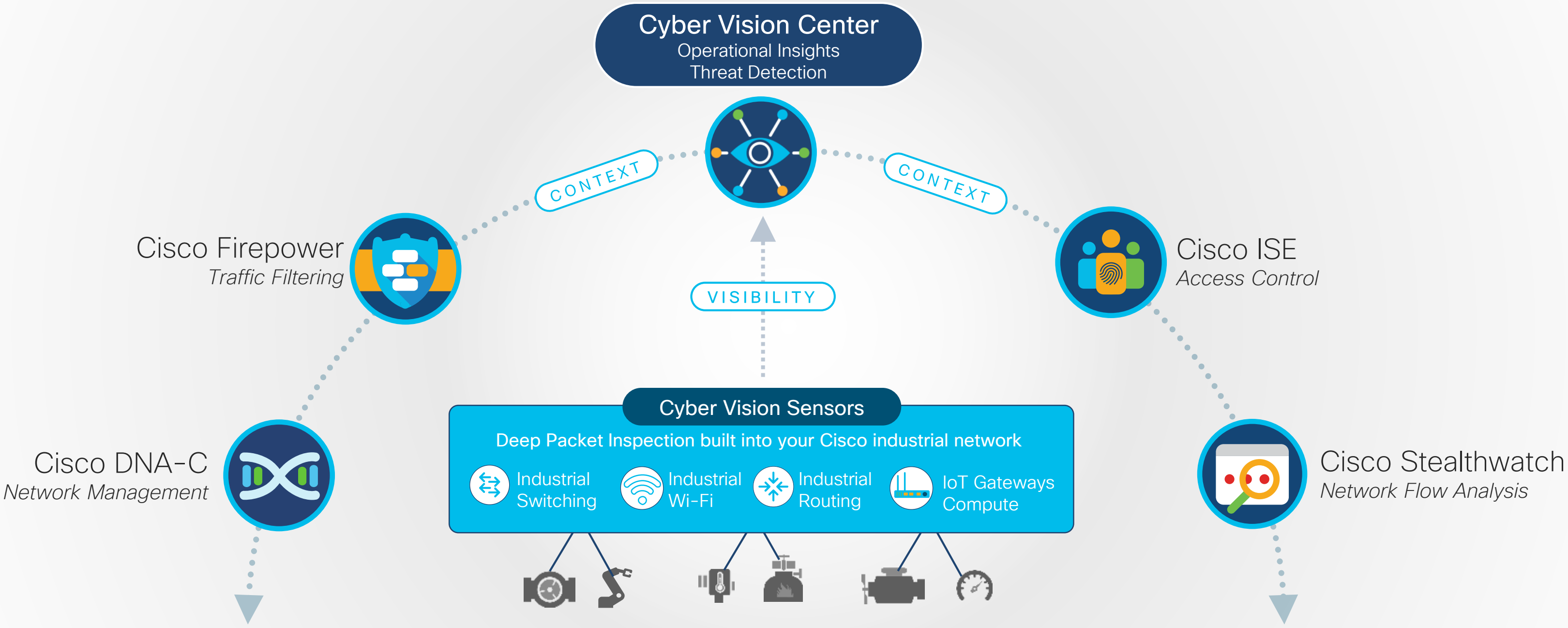


Cisco Cyber Vision for Manufacturing

Benefits of converged OT-IT security operations

A fully **integrated IT-OT security** solution

Working together to define & apply IoT security policies



Cyber Vision Center

Operational Insights

Threat Detection

Cisco Firepower

Traffic Filtering

Cisco ISE

Access Control

Cisco DNA-C

Network Management

Cisco Stealthwatch

Network Flow Analysis

Cyber Vision Sensors

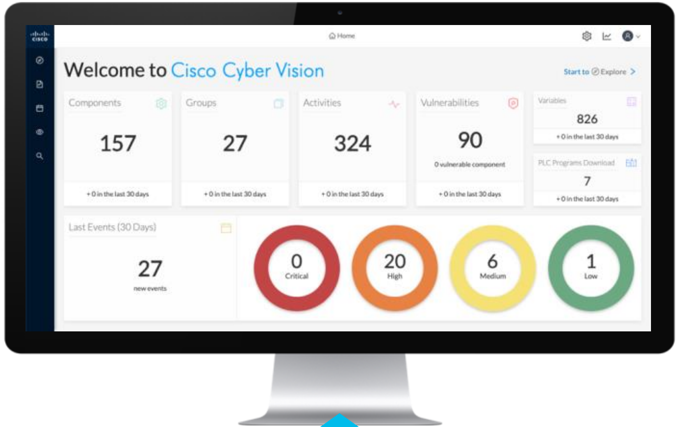
Deep Packet Inspection built into your Cisco industrial network

- Industrial Switching
- Industrial Wi-Fi
- Industrial Routing
- IoT Gateways Compute

Cisco Security for Industrial IoT

Cyber Vision + Cisco ISE

Automate segmentation and extend security policies to your OT



Home

Welcome to Cisco Cyber Vision

Start to Explore >

Components 157 +0 in the last 30 days

Groups 27 +0 in the last 30 days

Activities 324 +0 in the last 30 days

Vulnerabilities 90 0 vulnerable component +0 in the last 30 days

Variables 826 +0 in the last 30 days

PLC Programs Download 7 +0 in the last 30 days

Last Events (30 Days) 27 new events

0 Critical

20 High

6 Medium

1 Low

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

Cyber Vision Sensor

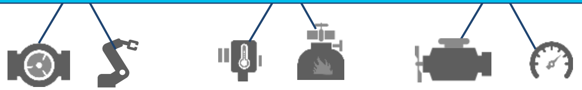
Cisco industrial network provides visibility and enforces security policy

Industrial Switching

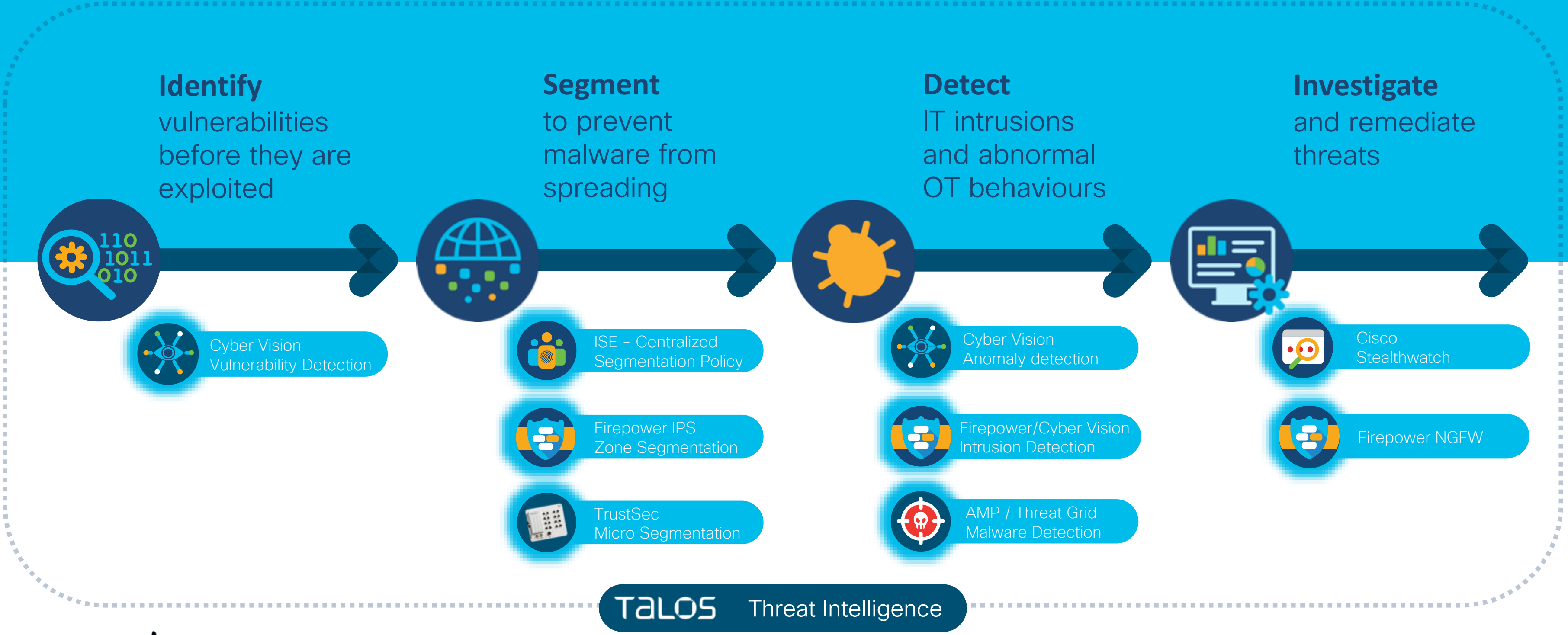
Industrial Wi-Fi

Industrial Routing

IoT Gateways / Compute



Securing industrial networks with Cisco



Identify vulnerabilities before they are exploited

- Cyber Vision Vulnerability Detection

Segment to prevent malware from spreading

- ISE - Centralized Segmentation Policy
- Firepower IPS Zone Segmentation
- TrustSec Micro Segmentation

Detect IT intrusions and abnormal OT behaviours

- Cyber Vision Anomaly detection
- Firepower/Cyber Vision Intrusion Detection
- AMP / Threat Grid Malware Detection

Investigate and remediate threats

- Cisco Stealthwatch
- Firepower NGFW

TALOS Threat Intelligence

Integrations for the real world

Access Control

cisco
Identity Service Engine

Firewalls

cisco
Firepower NGFW

FORTINET

paloalto NETWORKS

STORMSHIELD

Check Point SOFTWARE TECHNOLOGIES LTD.

CMDB

servicenow

bmc REMEDY

SOC

cisco
Stealthwatch

IBM QRadar

RSA SECURITY

ALIEN VAULT

McAfee
Together is power.

splunk>

Key takeaways

1. ICS visibility & detection requires new tools

2. Network sensors is the only scalable solution

3. Cyber Vision extends your SOC to secure OT

Demo

Questions?

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

Thank you

You make **possible**