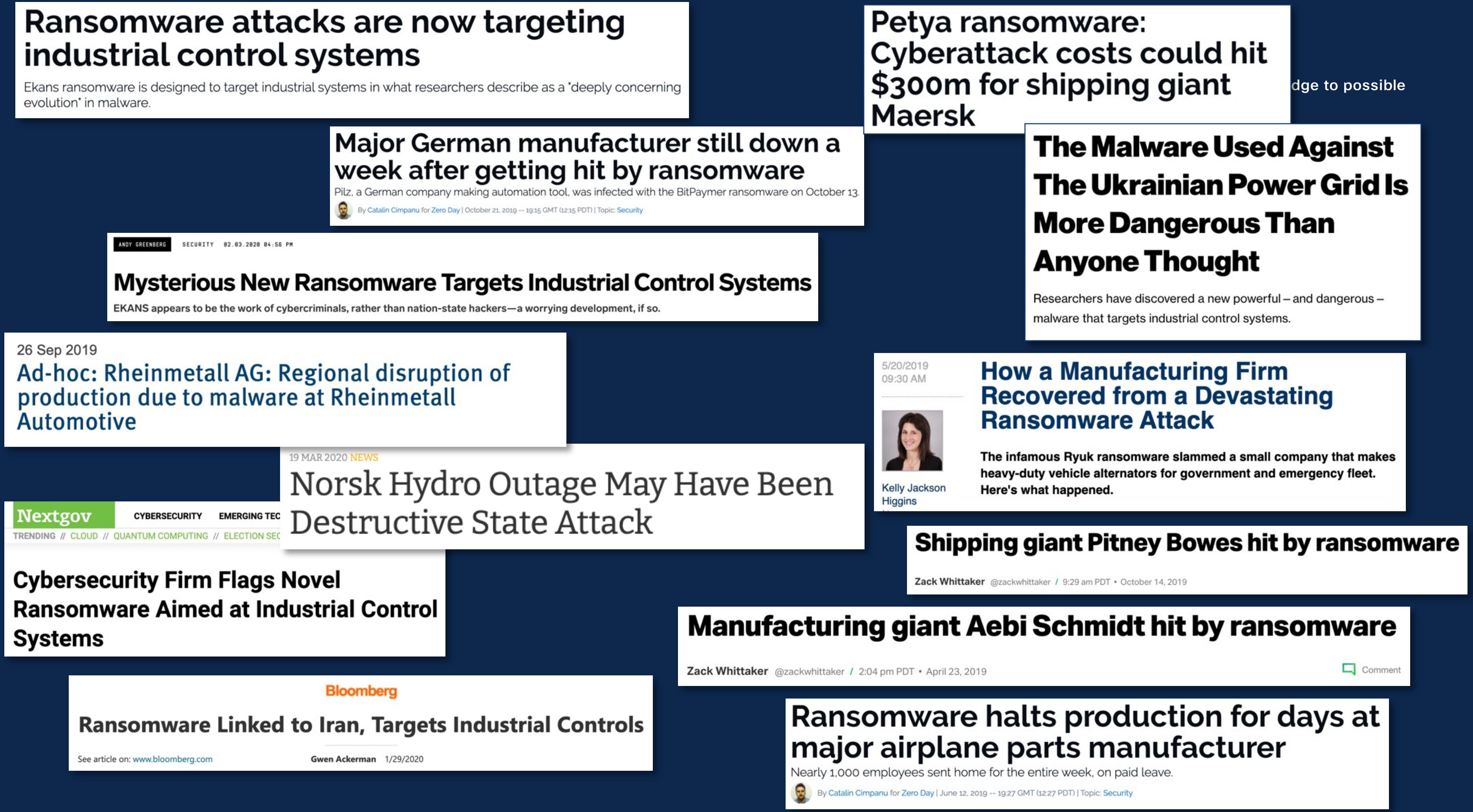
CISCO
SECURE

The bridge to possible

Cisco Industrial Threat Defense

Securing Industrial Control Systems

Laurentiu George



Ransomware attacks are now targeting industrial control systems

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

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

dge to possible

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

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

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

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.

ANDY GREENBERG SECURITY 02.03.2020 04:56 PM

Mysterious New Ransomware Targets Industrial Control Systems

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

26 Sep 2019

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

5/20/2019
09:30 AM

Kelly Jackson Higgins

How a Manufacturing Firm Recovered from a Devastating Ransomware Attack

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

19 MAR 2020 NEWS

Norsk Hydro Outage May Have Been Destructive State Attack

Nextgov CYBERSECURITY EMERGING TEC

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

Cybersecurity Firm Flags Novel Ransomware Aimed at Industrial Control Systems

Shipping giant Pitney Bowes hit by ransomware

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

Manufacturing giant Aebi Schmidt hit by ransomware

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

Bloomberg

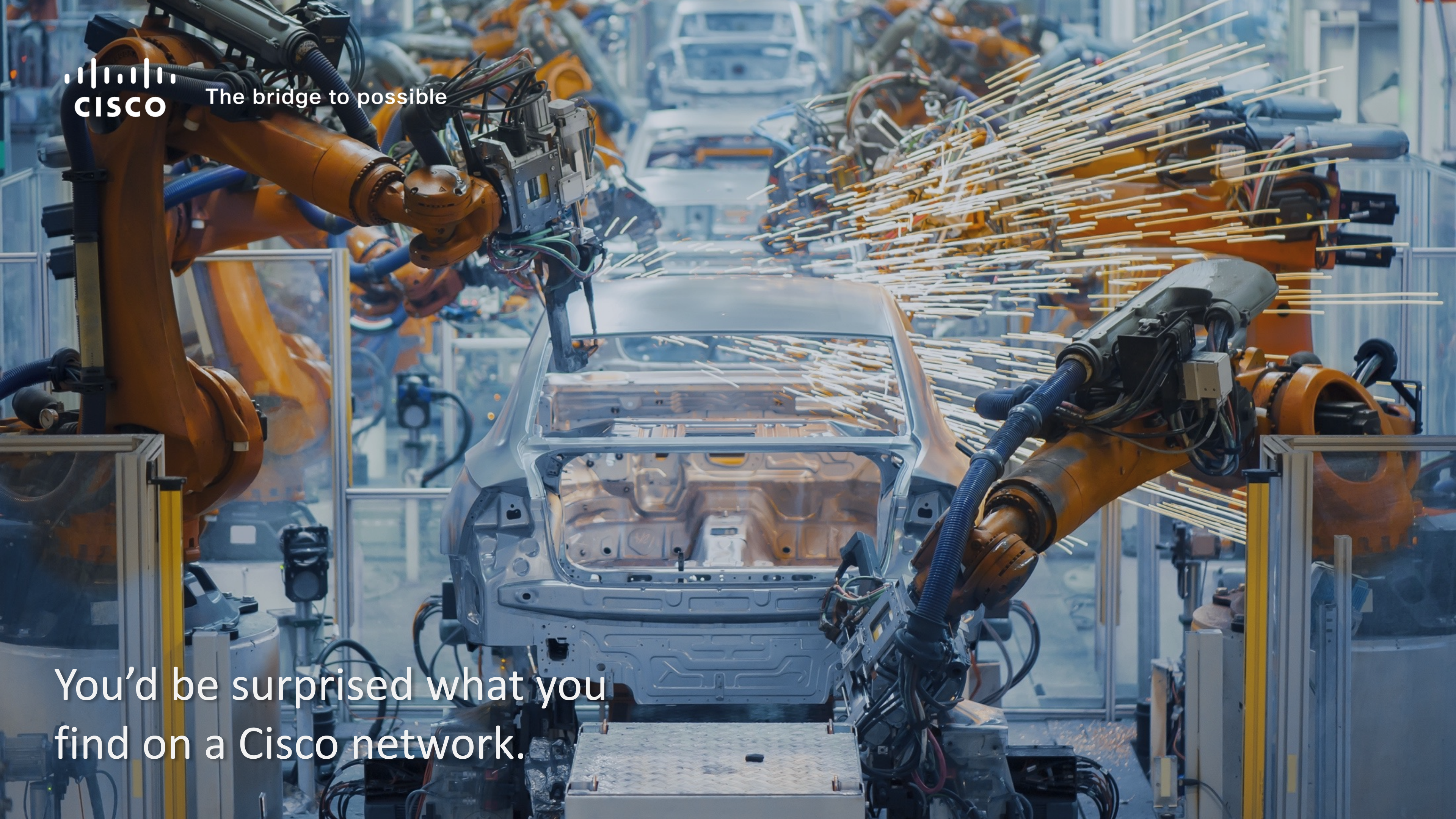
Ransomware Linked to Iran, Targets Industrial Controls

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

Ransomware halts production for days at major airplane parts manufacturer

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

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



The bridge to possible

You’d be surprised what you find on a Cisco network.

Cisco Industrial Threat Defense

Industry digitization is accelerating movement of data across IT, OT, and Cloud

Cisco Industrial Threat Defense secures ICS networks, and provides visibility to the OT domain in the IT SOC

Visibility &
Threat Detection

Industrial Network
Segmentation

Threat Investigation &
Remediation

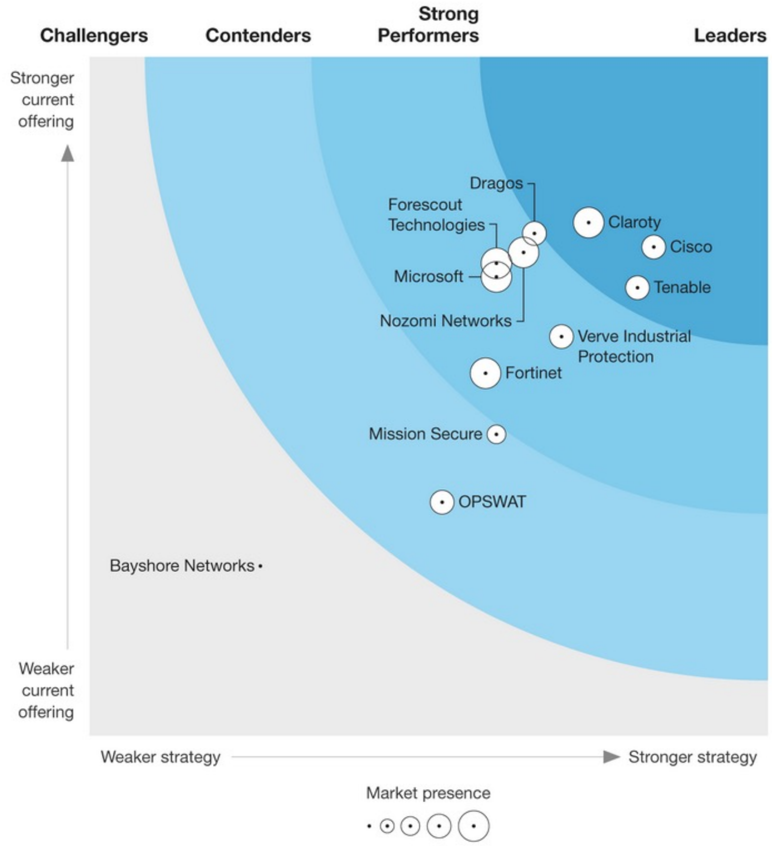
Cisco Named a Leader in IoT/OT Security

The Forrester Wave™: Industrial Control Systems (ICS) Security Solutions, Q4 2021

FORRESTER®

WAVE LEADER 2021

Industrial Control Systems (ICS) Security Solutions



Source: Forrester Research, Inc. Unauthorized reproduction, citation or distribution prohibited

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The 4-step journey to securing industrial networks

0 Industrial DMZ
- Secure Firewall

1 Asset Discovery
- Cyber Vision

2 Zone Segmentation
- Secure Industrial Firewall
- Identity Services Engine

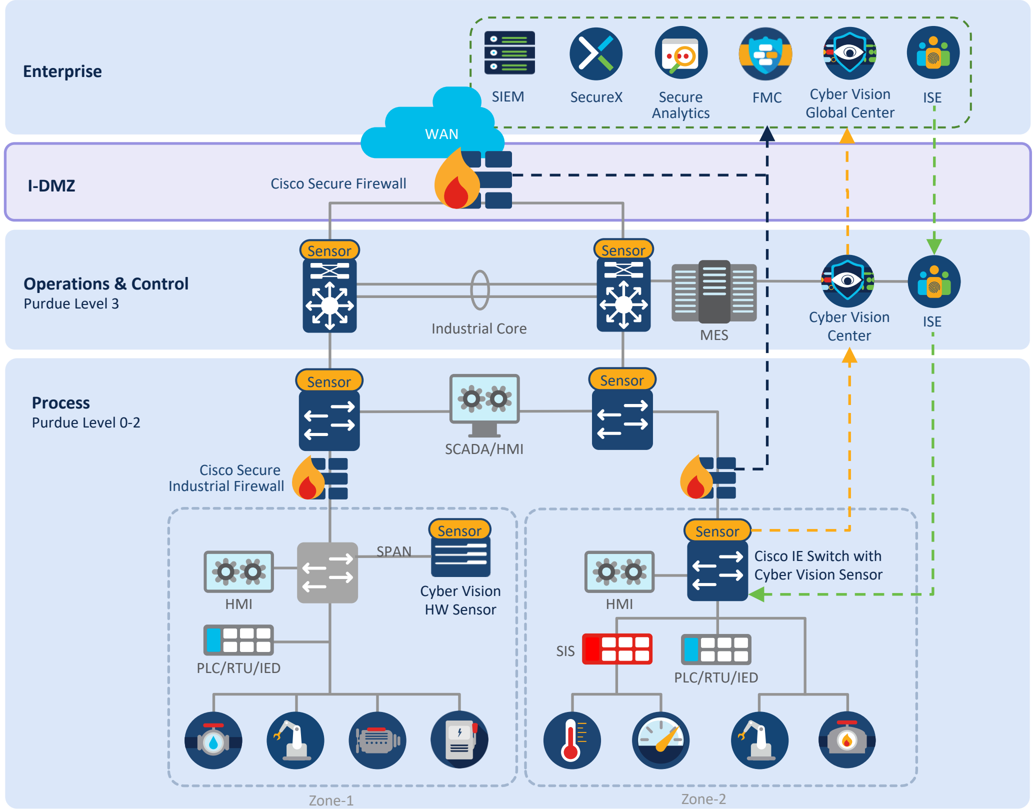
3 Threat Detection
- Secure Endpoint
- Cyber Vision
- Secure Industrial Firewall

4 Integrated IT/OT SOC
- SecureX

Powered by Talos Threat Intelligence

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Extend security operations to OT



1 Visibility built into your industrial network to identify assets and flows

2 Level-2 Zone-segmentation using industrial firewalls to protect against malware and threats with Snort IDS/IPS

3 Micro-segmentation at the access switch where assets connect to the network

4 Detect attempts to modify industrial processes using anomaly detection built into the industrial network

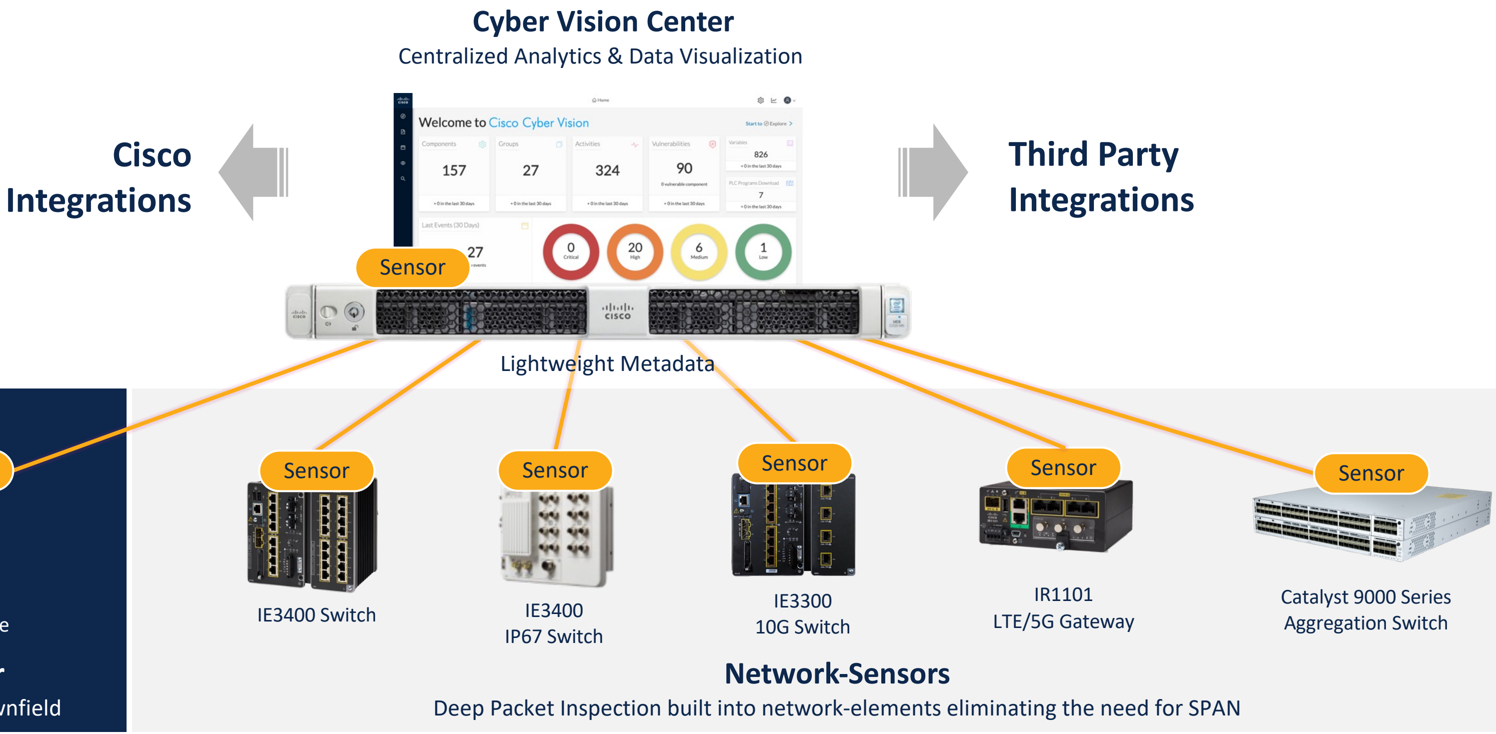
5 Investigate and remediate across IT-OT domains with aggregated threat intelligence and integrated security technologies

CISCO SECURE

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Security that scales with your infrastructure

Visibility and threat detection built into your industrial network



Cyber Vision Center

Centralized Analytics & Data Visualization

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

0 Critical

20 High

6 Medium

1 Low

Cisco Integrations

Third Party Integrations

Sensor

Lightweight Metadata

Sensor

IC3000 Industrial Compute

Hardware-Sensor

DPI via SPAN to support brownfield

Sensor

IE3400 Switch

Sensor

IE3400
IP67 Switch

Sensor

IE3300
10G Switch

Sensor

IR1101
LTE/5G Gateway

Sensor

Catalyst 9000 Series
Aggregation Switch

Network-Sensors

Deep Packet Inspection built into network-elements eliminating the need for SPAN

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Talos, the industry-leading threat intel group

Threat Intelligence

Discovering 200+ vulnerabilities every year.
Superior ICS/OT reverse engineering expertise.
The official developer of Snort rules.

Numerous 0-days disclosed (VPNfilter, TemplateAPT, etc)
Track record of discovering ICS vuln (and creating Snort rules)

Incident Response

Proactive and emergency services delivered worldwide. Help prepare, respond and recover from a breach.
Strong presence in industrial verticals.

Provided first ever incident command in DOE ICS
Recognized by US DOJ for Ukraine work

CISCO SECURE © 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Industrial Threat Defense

Supporting Products

Building converged IT/OT security is a journey

Zero Trust
Foundation
IDMZ

1. *People skills and training*
2. *Organizational processes*
3. *Network architecture & Security technologies*

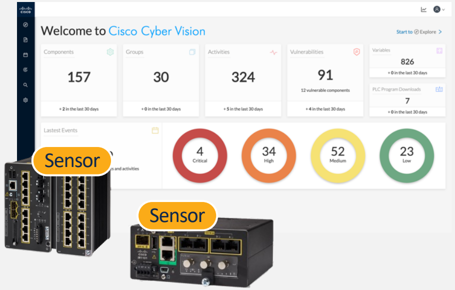
Cisco Industrial Threat Defense is a modular solution to enable OT security at scale

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Foundational Components of Industrial Security

Detect

Cisco Cyber Vision



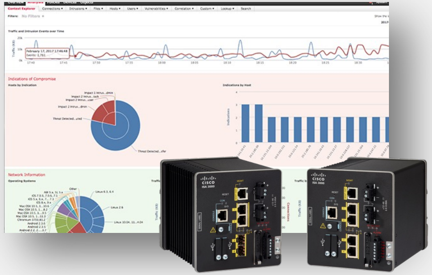
OT asset inventory

Track industrial processes

Detect attempts to modify assets

Protect

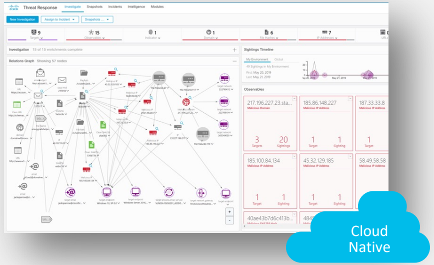
Cisco Industrial Firewall



Segment network and prevent threat propagation with best of breed industrial protocol IPS/IDS

Investigate & Respond

Cisco SecureX



Enable security experts to investigate industrial threats and orchestrate response with playbooks

Powered by Cisco Talos threat intelligence

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Moving Towards Zero Trust for ICS

Secure Endpoint

Protects endpoints from malware, tracks process changes, tracks files across network with retrospective

ISE

Network Access Control – users, endpoint state, and more. Automates ICS micro-segmentation

Duo

Verify user trust, Establish device trust, Enforce adaptive policies for zero trust security

AnyConnect

Enterprise class MFA based VPN with deep integration with with Secure Endpoint, Umbrella, ISE

Secure Network Analytics

Scalable visibility and security analytics using telemetry from your network infrastructure

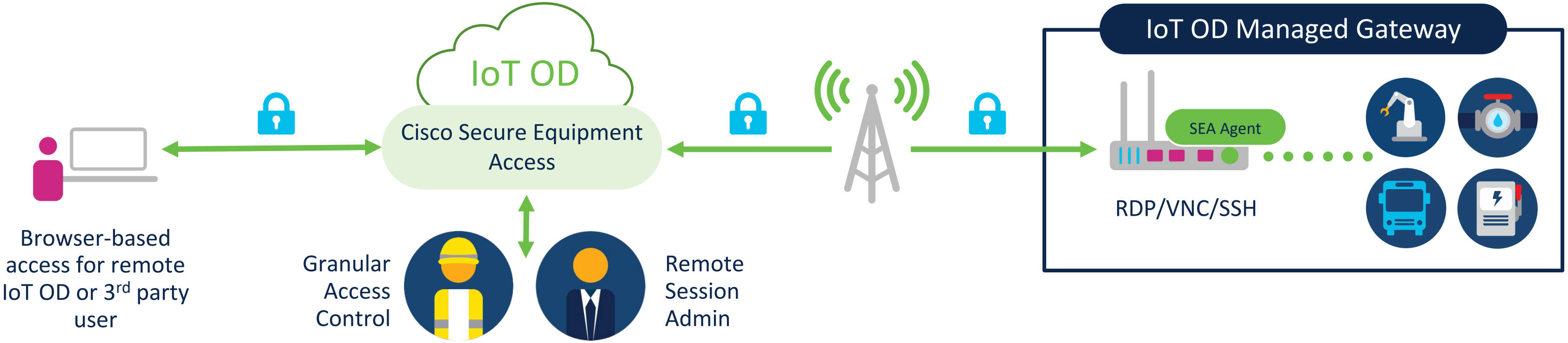
Umbrella

SASE for internet exposed devices and services

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Secure Equipment Access

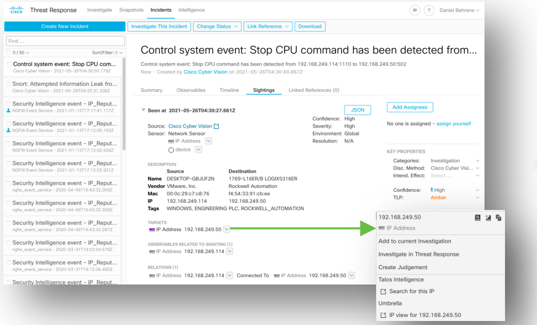
Cisco's cloud solution designed for OT/IT to easily and securely monitor and perform critical day-to-day operations of remote industrial equipment



© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Investigation & Response Orchestration

Manage Incident



Control system event: Stop CPU com...
Cisco Cyber Vision · 2021-05-26T04:30:50.179Z

Snort: Attempted Information Leak fro...
Cisco Cyber Vision · 2021-05-26T04:25:31.208Z

Security Intelligence event - IP_Reput...
NGFW Event Service · 2021-01-12T17:17:41.117Z

Security Intelligence event - IP_Reput...
NGFW Event Service · 2021-01-12T17:12:05.193Z

Security Intelligence event - IP_Reput...
NGFW Event Service · 2021-01-12T17:12:02.934Z

Security Intelligence event - IP_Reput...
NGFW Event Service · 2021-01-12T17:12:02.931Z

Security Intelligence event - IP_Reput...
ngfw_event_service · 2020-04-06T16:43:32.309Z

Security Intelligence event - IP_Reput...
ngfw_event_service · 2020-04-06T16:43:32.309Z

Security Intelligence event - IP_Reput...
ngfw_event_service · 2020-04-06T16:43:32.287Z

Security Intelligence event - IP_Reput...
ngfw_event_service · 2020-03-31T19:23:04.678Z

Security Intelligence event - IP_Reput...
ngfw_event_service · 2020-03-31T19:12:34.460Z

Security Intelligence event - IP_Reput...

Control system event: Stop CPU command has been detected from...

Control system event: Stop CPU command has been detected from 192.168.249.114:1110 to 192.168.249.50:502
New · Created by Cisco Cyber Vision on 2021-05-26T04:30:49.867Z

Seen at 2021-05-26T04:30:27.661Z

Source: Cisco Cyber Vision
Sensor: Network Sensor
IP Address
device

Confidence: High
Severity: High
Environment: Global
Resolution: N/A

No one is assigned - assign yourself

DESCRIPTION

	Source	Destination
Name	DESKTOP-GBJUF2N	1769-L16ER/B LOGIX5316ER
Vendor	VMware, Inc.	Rockwell Automation
Mac	00:0c:29:c7:c8:76	f4:54:33:91:cb:ee
IP	192.168.249.114	192.168.249.50
Tags	WINDOWS, ENGINEERING PLC, ROCKWELL_AUTOMATION	

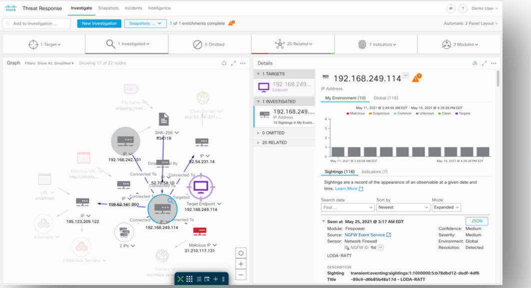
TARGETS
IP Address 192.168.249.50

OBSERVABLES RELATED TO SIGHTING (1)
IP Address 192.168.249.114

RELATIONS (1)
IP Address 192.168.249.114 Connected To IP Address 192.168.249.50

KEY PROPERTIES
Categories: Investigation
Disc. Method: Cisco Cyber Visi...
Intend. Effect: Select ...
Confidence: High
TLP: Amber

Investigate with Enrichment



Sightings are a record of the appearance of an observable at a given date and time. Learn More

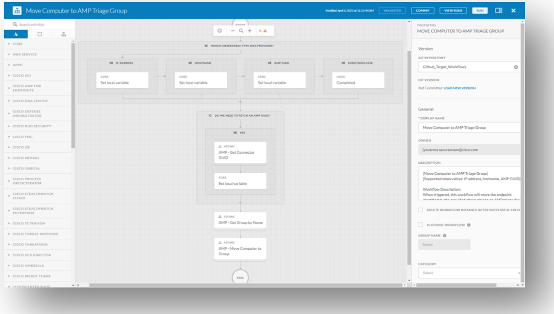
Seen at May 25, 2021 @ 3:17 AM EDT
Module: Firepower
Source: NGFW Event Service
Sensor: Network Firewall
NGFW ID ftd

Confidence: Medium
Severity: Medium
Environment: Global
Resolution: Detected

LODA-RATT

DESCRIPTION
Sighting Title transient:eventing:sightings:1:1000000:5:b78dbd12-dedf-4df6-89c9-d6b85b48a17d - LODA-RATT

Playbook Orchestration



GIT REPOSITORY: Github_Target_Workflows

GIT VERSION: Not Committed LOAD NEW VERSION

* DISPLAY NAME: Move Computer to AMP Triage Group

OWNER: jyoverma securexnam@cisco.com

DESCRIPTION:
[Move Computer to AMP Triage Group]
[Supported observables: IP address, hostname, AMP GUID]
Workflow Description:
When triggered, this workflow will move the endpoint

Promote events from Level-2 for incident management

Event observables are enriched by Cisco and 3rd party products

Run playbooks with custom workflows to automate response across cloud and on-prem assets

Cyber Vision event “PLC stop command issued from operator workstation” promoted to SecureX incident manager

SecureX enrichment shows workstation is communicating with external IP flagged by AMP, Talos, and Umbrella

Playbook takes AMP GUID and requests tier-2 approval from OT operator to enable host isolation of workstation

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Bring Cisco scale and simplicity to industrial security

Cisco Industrial Networks

Connect anything anywhere

Cisco Security

Comprehensive IT/OT cybersecurity

Cisco Validated Designs

State-of-the-art architecture guides

Cisco Customer Services

Human skills to enable deployments

All working together for successful industrial security deployments

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

cisco SECURE