DRAGOS | Deloitte. | servicenow

GP Georgia-Pacific | SUBZERO

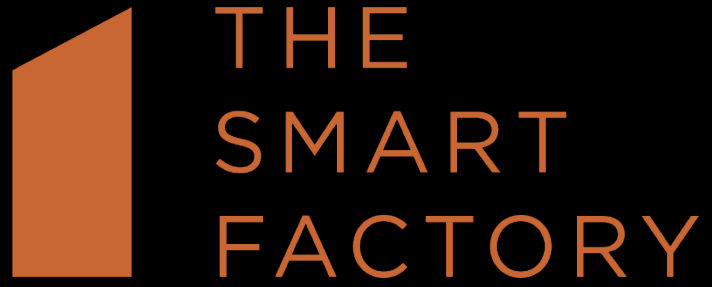
WEBINAR

Achieving Secure Digital Transformation in Manufacturing

Peter Vescuso
Marketing, Dragos

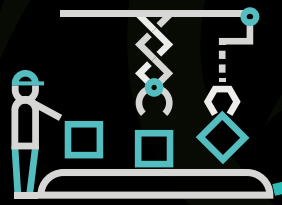
AGENDA

- Market Trends
- Deloitte Smart Factory
- Panel Discussion
- Dragos Platform

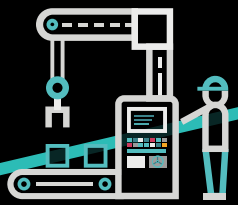


MANUFACTURING TRENDS

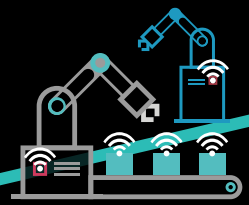
Growing investment in digital transformation and hyperconnectivity



STAND-ALONE



LOOSELY CONNECTED



HIGHLY CONNECTED

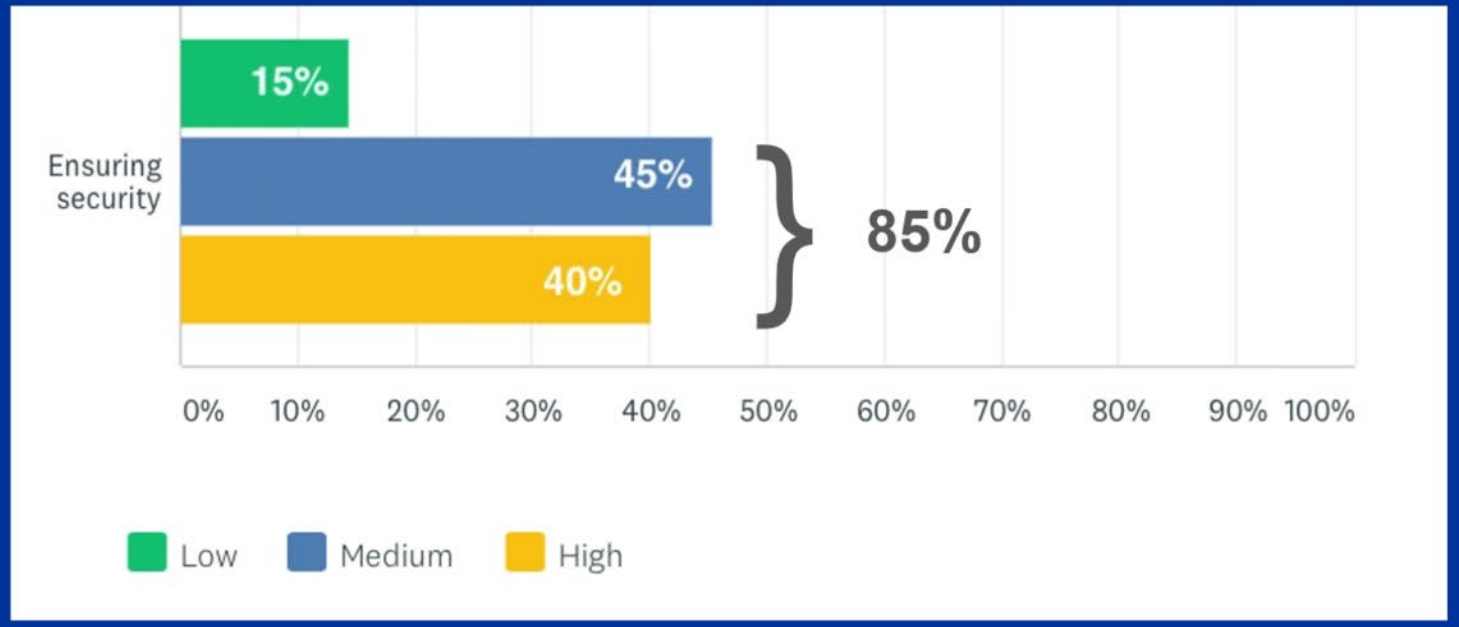
Greater exposure to malicious cyberthreats

"Threat groups are rising 3X faster than they're declining…"

Source: Dragos 2020 YiR

The Cyber Challenge to 4.0 Transformation

How would you assess the following challenges related to adopting and using transformative M4.0 technologies?



85% say the cybersecurity challenge remains either a **high** or at least a **medium** obstacle to their adoption and use of transformational 4.0 technologies

MLC Transformative Technologies Survey: September 2021

Manufacturing Leadership Council

Deloitte Smart Factory @ Wichita State University

Jimmy Asher
Senior Manager
Deloitte Consulting LLP

THE SMART FACTORY

THE SMART FACTORY

9/30/21

The Smart Factory @ Wichita

The waiting game is over. Industry 4.0 is here.

Smart factory adoption is increasing, driving the evolution of smart and high-impact results.

A smart factory is a space where physical and digital solutions orchestrate to change the way manufacturers operate, enabling plant managers and factory workers to proactively manage short-term manufacturing challenges such as resources, physical assets, and schedule.

The Smart Factory @ Wichita marries advanced manufacturing techniques with the Internet of Things to create manufacturing systems that go beyond being interconnected. We are now able to demonstrate how to communicate, analyze, and use information to drive further intelligent action back in the physical world. And for companies like yours, that means using technologies that drive down costs, increase efficiencies, and position your organization for success.

Up to 20%
improved asset efficiency

Up to 35%
improved quality

Up to 30%
reduced costs

Up to 20%
enhanced agility

Overall equipment effectiveness (OEE) improvement

Up to 10%
improved safety and sustainability

Source: Deloitte analysis of the 2019 Deloitte and MAPI Smart Factory Study data

Behold the Smart Factory @ Wichita

Where the impossible becomes reality.

Isn't she a beauty? Construction is currently underway on nearly 60,000 square feet of super-smart, sustainable space for The Smart Factory @ Wichita. And we're working with Wichita State University to become a smart building on a smart grid.

This experiential space is your personal innovation playground, a workshop of sorts that allows visitors to immerse themselves in custom simulations to solve real business problems.

See? Told you it's super-smart.

How will the Smart Factory leverage Dragos?

OT AND IOT MONITORING

DIGITAL ASSEST MANAGEMENT

SOC CAPABILITIES

INCIDENT RESPONSE

What's next?

What will this look like within Smart Factory?

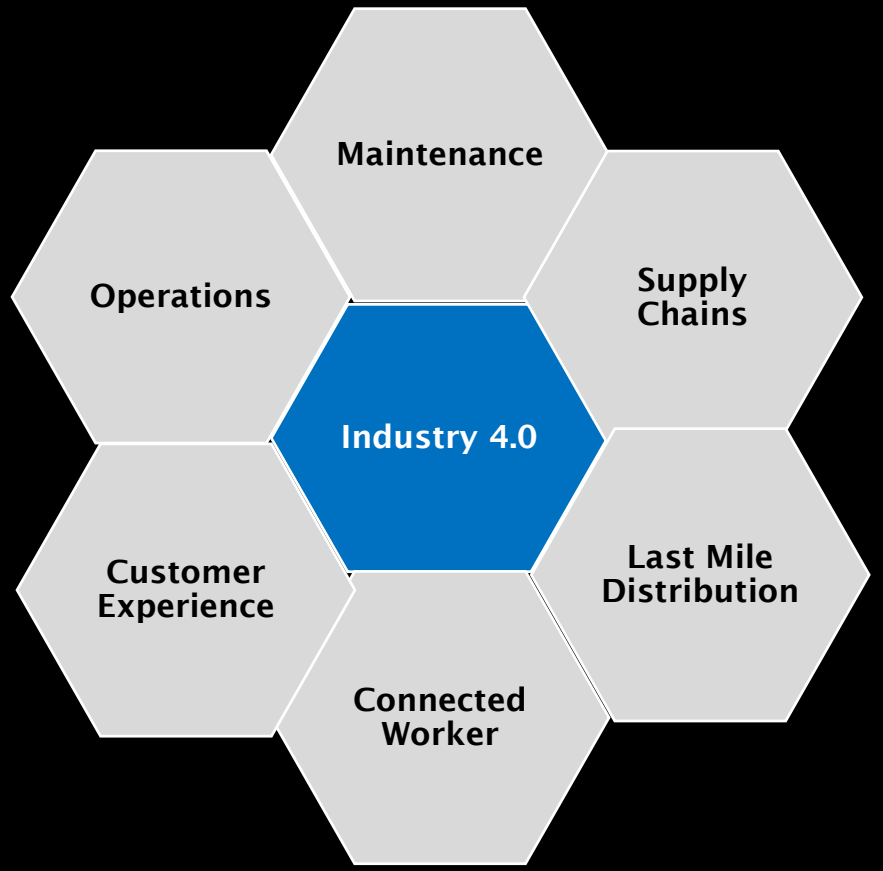
Dragos will be tightly coupled into the smart factory ecosystem and will actively monitor the network nodes for cyber scenarios such as spear-phishing, ransomware, third-party risk, etc.

Deloitte Smart Factory: Infor and Dragos

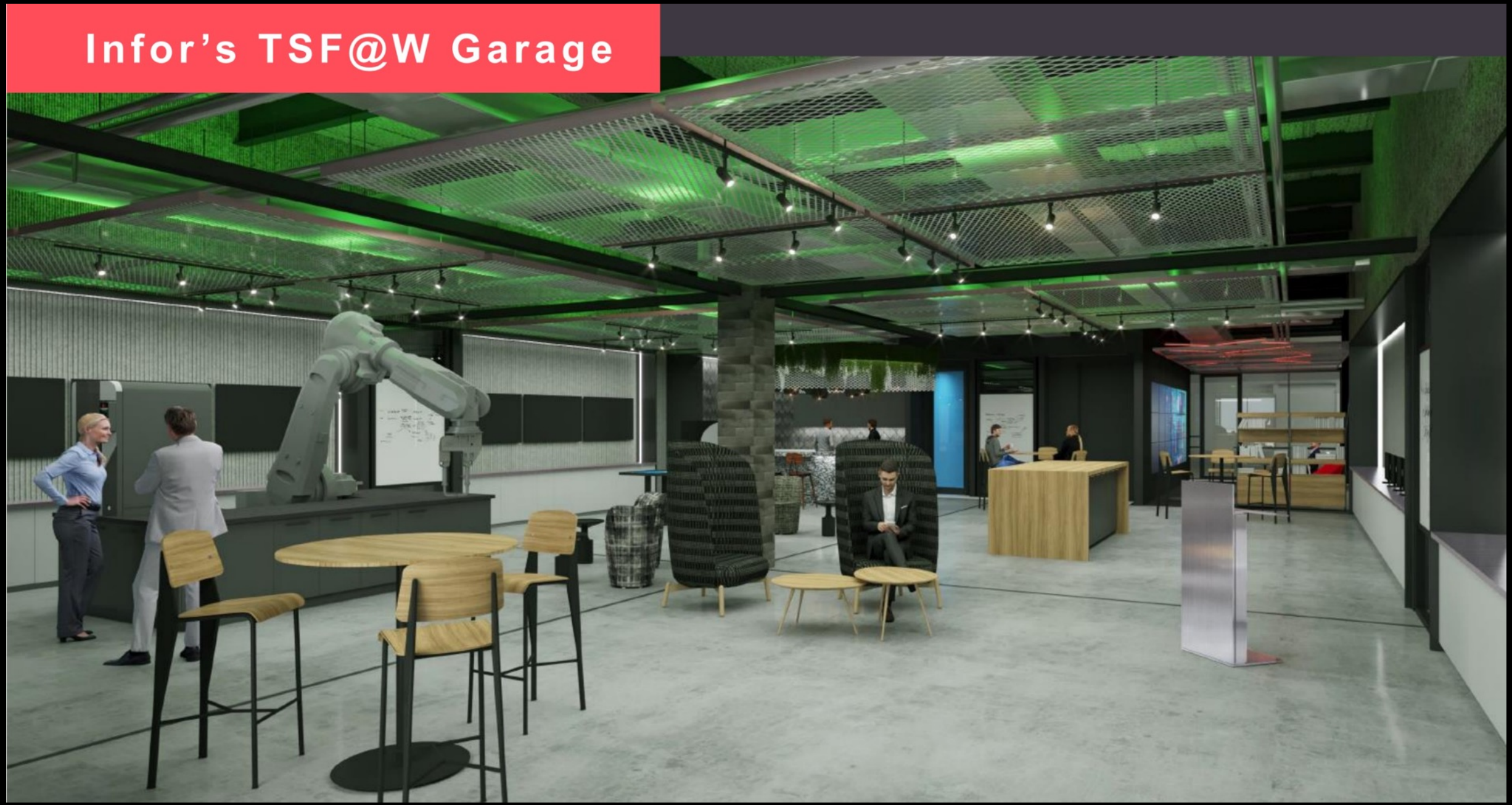
The future of manufacturing is here

Infor Industry 4.0 engages with strategic clients to connect people, processes, “things,” and businesses to:

- Drive measurable business outcomes
- Make operations more nimble
- Enable businesses to be more efficient
- Provide the power to respond to volatile supply chains



Infor's TSF@W Garage



Panel Discussion

Panel Session

Moderator

- Steve Applegate
  - Dragos CISO

Panelists

- Fran Cioffi
  - CISO, Georgia Pacific
- Jeremy Korger
  - OT Cybersecurity lead, Sub-Zero
- James Destro
  - Head of Manufacturing Industry Products, ServiceNow

Dragos Platform

Jimmy Graham

Senior Director of Product Management, Dragos

THE DRAGOS PLATFORM

FOR INDUSTRIAL CYBERSECURITY

NEIGHBORHOOD KEEPER
Collective defense & community-wide visibility

DRAGOS PLATFORM

OT WATCH
Managed ICS/OT network visibility, threat hunting, & incident triage

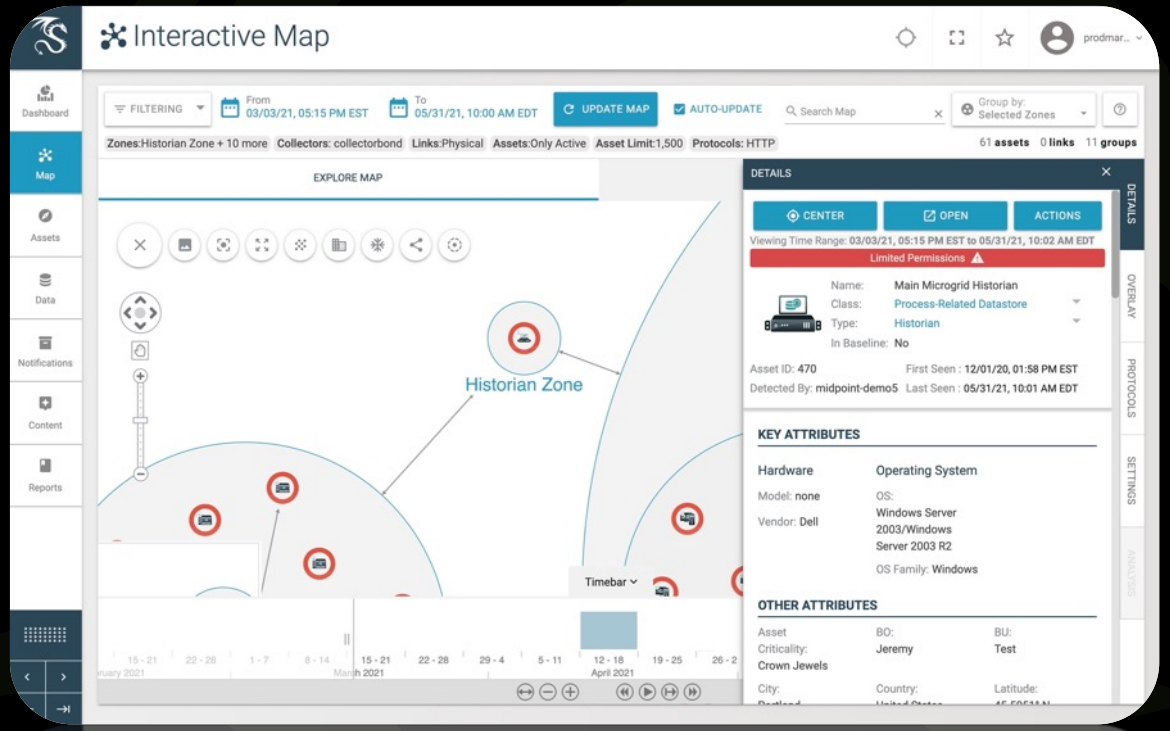
- ASSET VISIBILITY & INVENTORY
- THREAT DETECTION
- INVESTIGATION & RESPONSE
- VULNERABILITY MANAGEMENT

KNOWLEDGE PACKS
Regular updates for asset visibility, threat and vulnerability detection, and response playbooks

- ICS/OT THREAT INTELLIGENCE
- ICS/OT FRONTLINE EXPERIENCE

THE DRAGOS PLATFORM

ASSET VISIBILITY & ANOMALY DETECTION



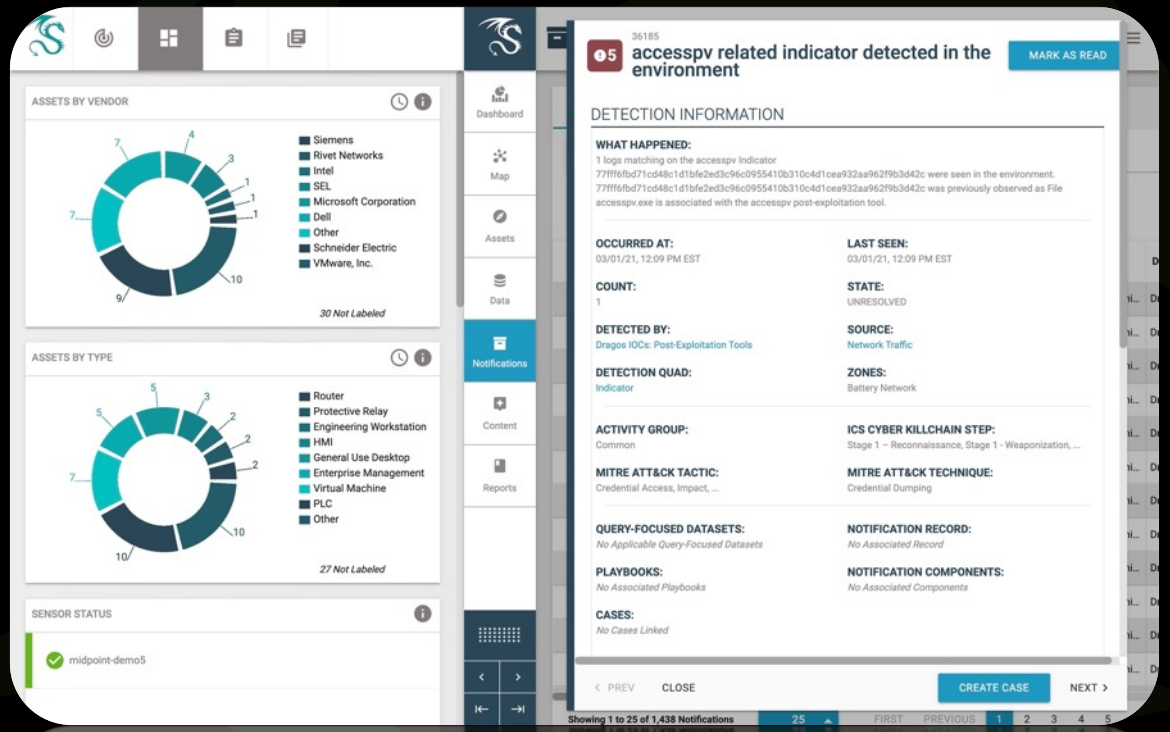
- ✓ See OT network traffic and assets
- ✓ Timeline and historical views
- ✓ Highly customizable zoning
- ✓ In-depth asset details including device type, vendor, firmware, model, and more

Bottom Line:

Dragos has the richest asset visibility solution in the industry with fine grained filtering and historical “point in time” precision that lets teams quickly separate signal from noise

THE DRAGOS PLATFORM

THREAT ANALYTICS MAPPED TO MITRE ATT&CK for ICS



- ✓ Continuous threat monitoring
- ✓ Context rich threat detection
- ✓ Mapped to MITRE ATT&CK for ICS
- ✓ Unique adversary Indicators and Tactics, Techniques, and Procedures (TTP)

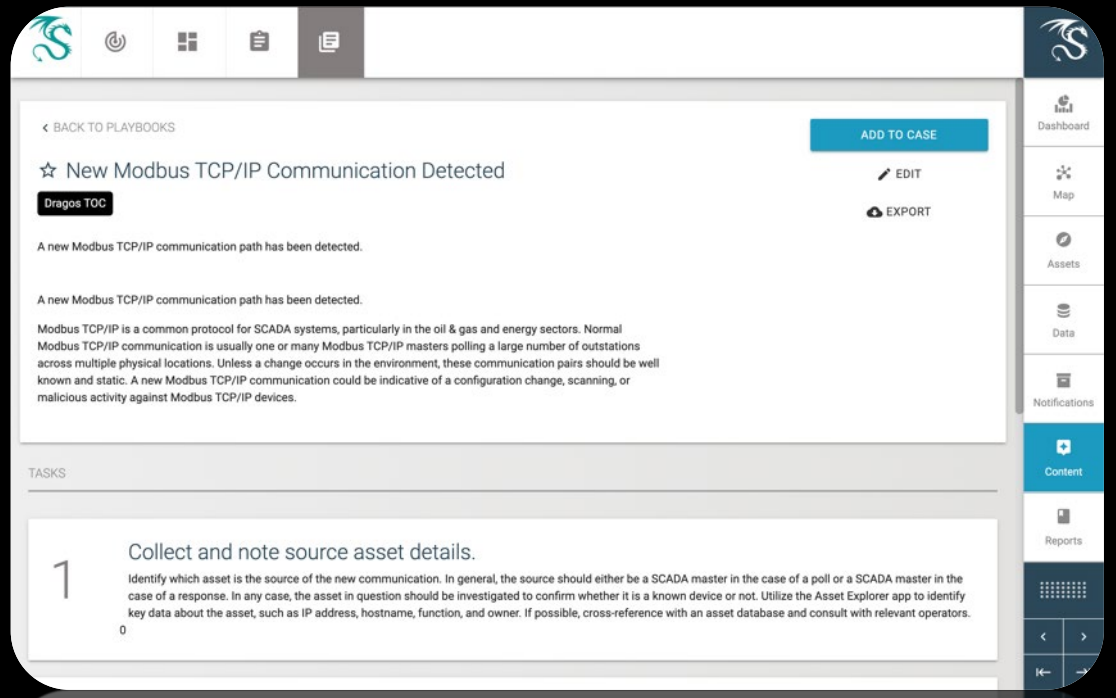
Bottom Line:

Dragos's unique threat analytics are the most effective way to detect real ICS threats, and we provide actionable perspective based on unique, globally sourced intelligence.

THE DRAGOS PLATFORM

ANALYST WORKBENCH WITH INVESTIGATION PLAYBOOKS

- ✓ Case management and workbench
- ✓ Pre-made queries for alert triaging
- ✓ Playbooks for each threat analytic
- ✓ Step-by-step guides to investigations

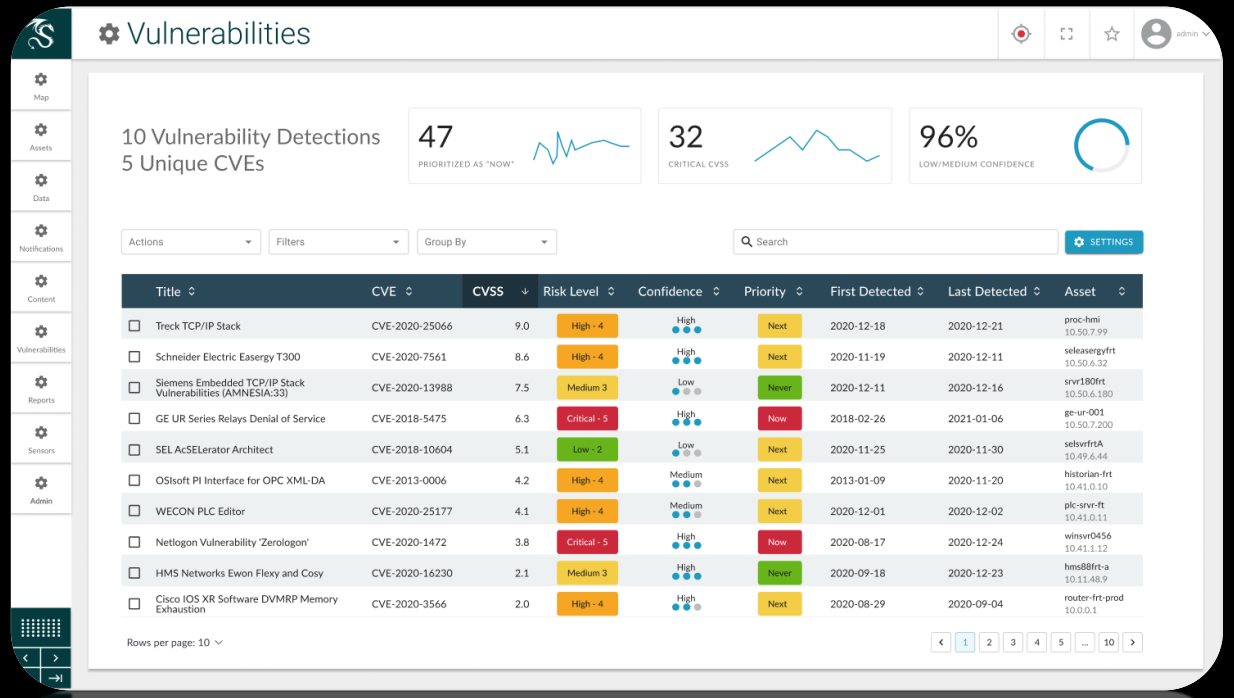


Bottom Line:
Dragos provides highly differentiated, expert-authored playbooks with clear, prescriptive guidance. Our distinct expertise and field experience are unmatched.

THE DRAGOS PLATFORM

VULNERABILITY MANAGEMENT

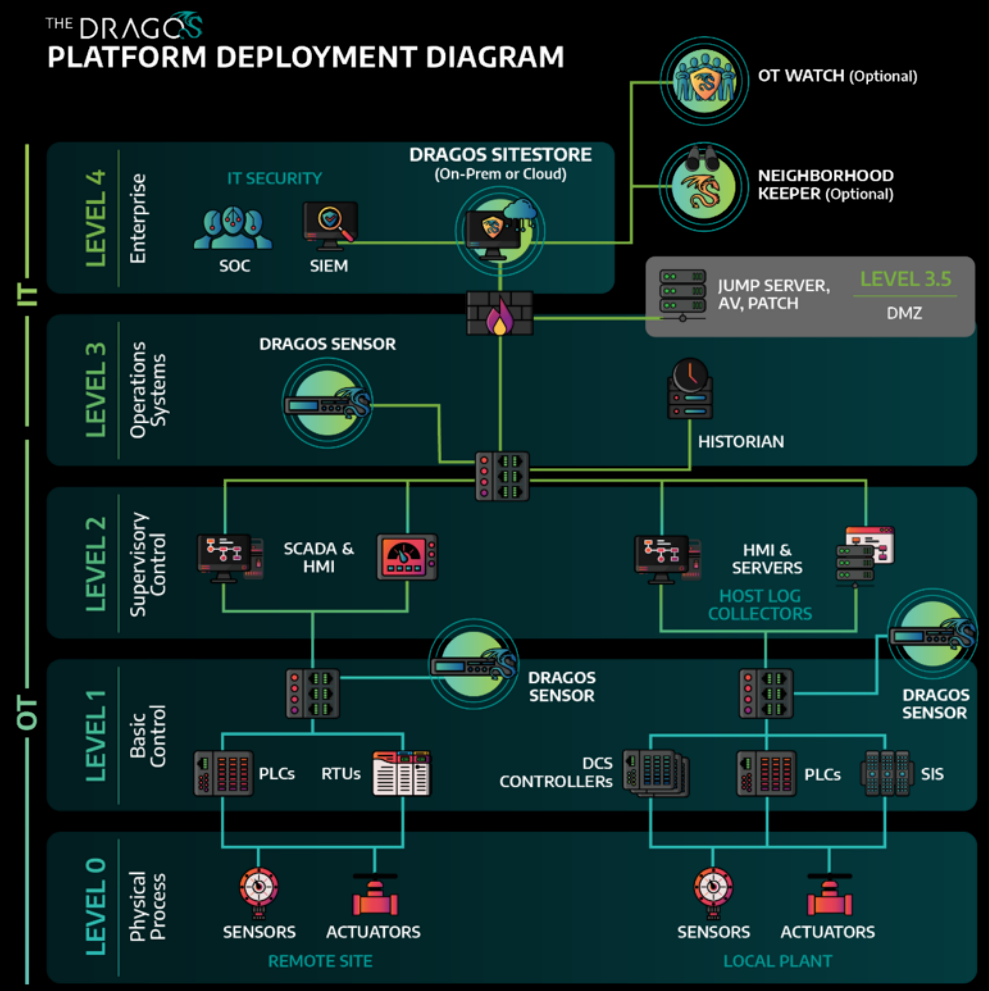
- ✓ Purpose built for OT, uses our own vulnerability knowledge base
- ✓ Vulnerability Intelligence – we add unique guidance to vulnerabilities beyond ICS-Cert
- ✓ Vulnerability Management Process: *now, next, never*



Bottom Line:

Dragos's vuln management solutions provide the most accurate and complete information available; focused effort on highest priority issues mitigates risk and minimizes wasted time

PLATFORM DEPLOYMENT



Dragos SiteStore

Deployable on-premise or in AWS cloud
Managed Hunting option available for cloud.

Traffic Collection

Dragos sensors are primarily deployed via network span or tap as DIN-Rail mounted, ruggedized, and enterprise-class options

Logs and/or PCAPS

Consume network traffic and logs such as Windows Events and Syslog

Integrations

Utilize existing infrastructure, systems, devices, and tools

Dragos Sensors

- Passive collection
- Multiple form factors
- Ruggedized
  - DIN Rail
  - SEL-3355
- Virtual Sensors

25 Mbps
Rugged / Industrial Rated
DIN Rail / Wall Mount

100 Mbps
Rugged / Industrial Rated
3U Rackmount
(SEL-3355)

100 Mbps
Desktop / 1U Rack Mount Kit

1 Gbps
1U Rackmount

THE DRAGOS PLATFORM

WORKFLOW INTEGRATIONS

SIEM

splunk>

McAfee

FORTINET

IBM QRadar

MICRO FOCUS

LogRhythm

Firewall and Network

FORTINET

SEL SCHWEITZER ENGINEERING LABORATORIES

WATERFALL Stronger Than Firewalls

OWL Cyber Defense

GARLAND TECHNOLOGY *

KEYSIGHT TECHNOLOGIES *

aruba * a Hewlett Packard Enterprise company

CMDB

servicenow

AXONIUS *

Historian

AVEVA + OSIsoft

Endpoint

CROWDSTRIKE *

McAfee *

SOAR

SWIMLANE *

Threat Intelligence Integrations

CROWDSTRIKE

splunk>

ThreatConnect

ANOMALI

CYWARE

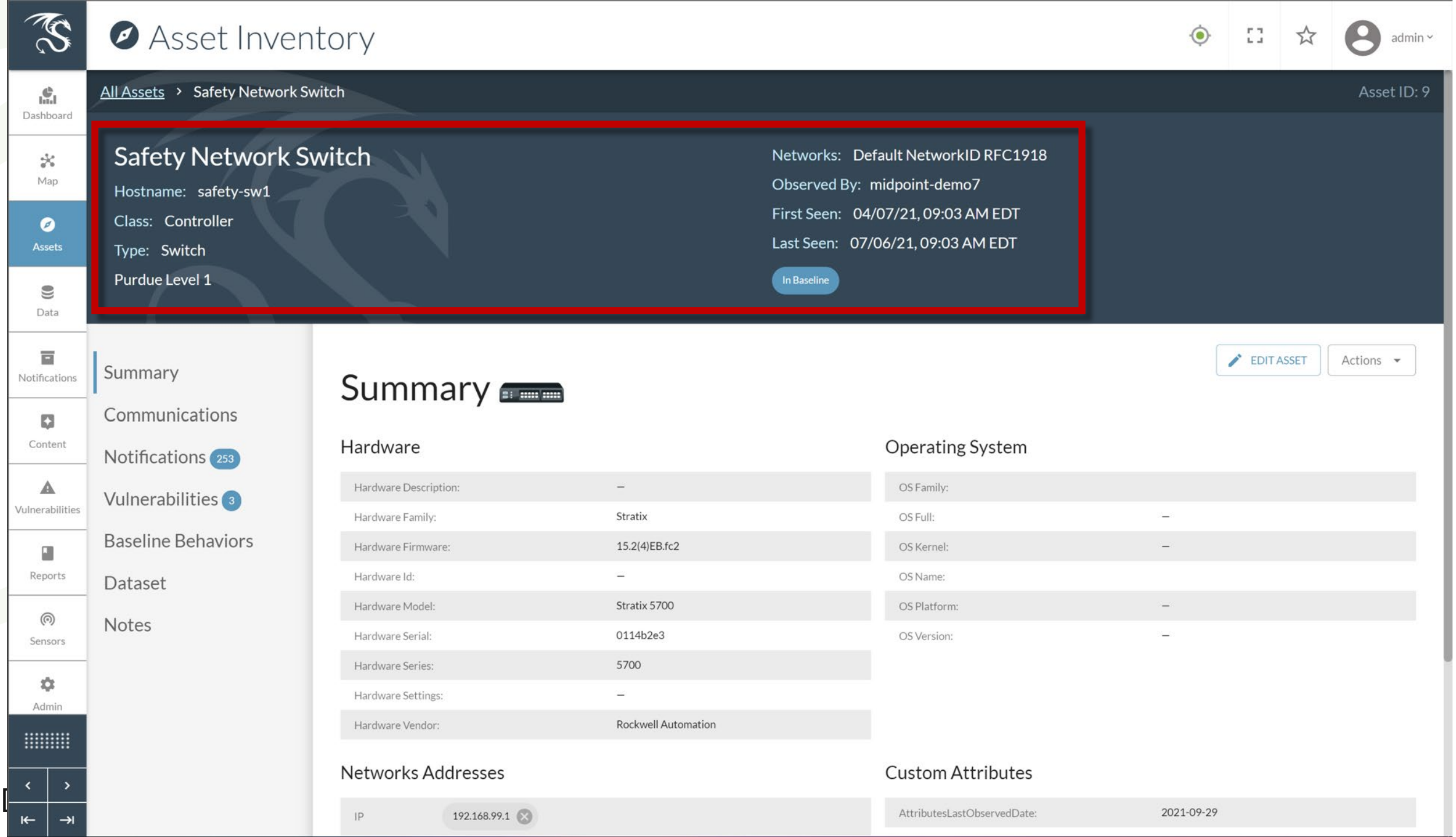
THREATQUOTIENT

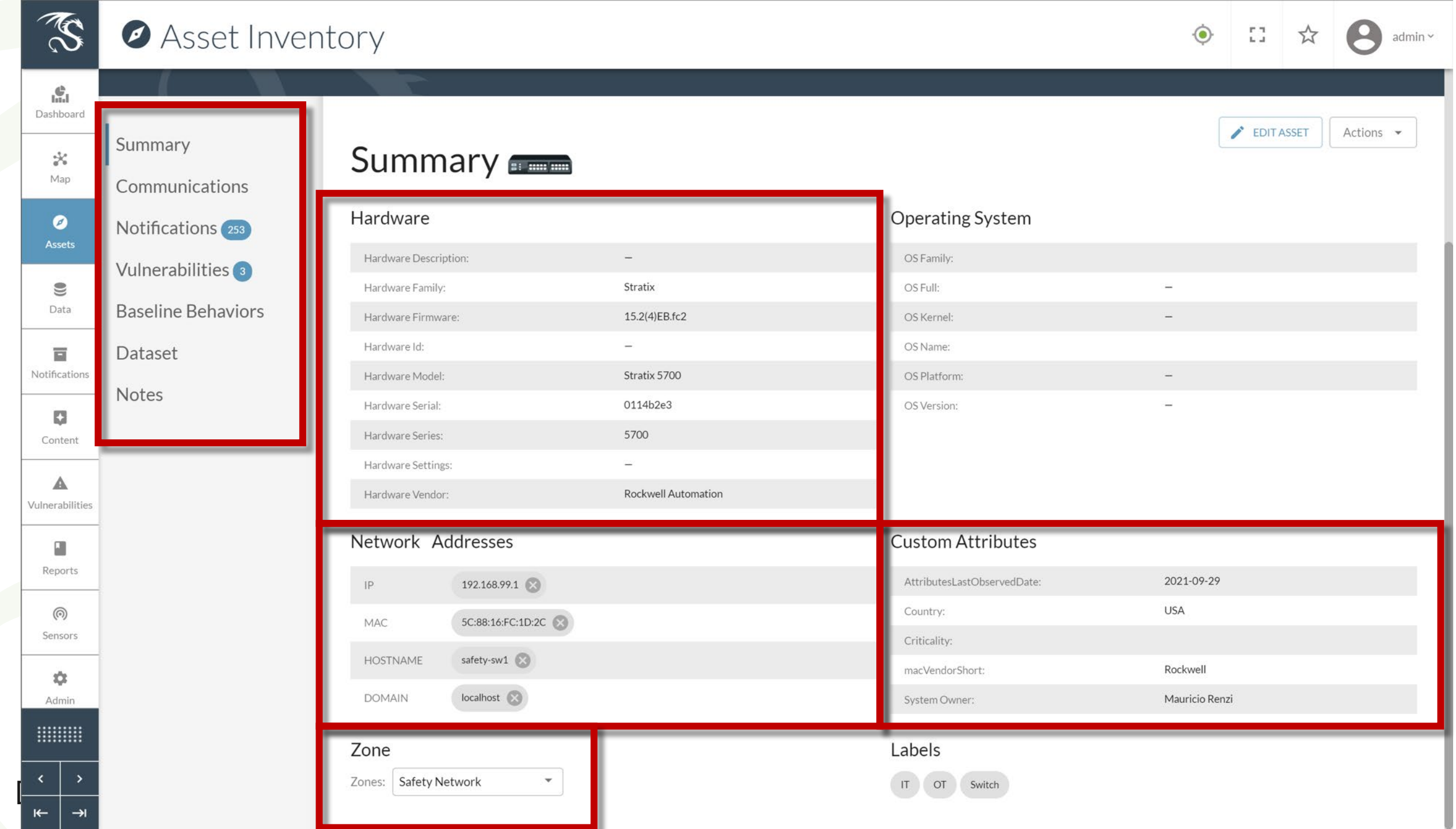
TRUSTAR

EclecticIQ

Recorded Future

* 2021 Planned Integrations


Asset Inventory
admin
Dashboard
Map
Assets
Data
Notifications
Content
Vulnerabilities
Reports
Sensors
Admin
All Assets › Safety Network Switch
Asset ID: 9
Safety Network Switch
Hostname: safety-sw1
Class: Controller
Type: Switch
Purdue Level 1
Networks: Default NetworkID RFC1918
Observed By: midpoint-demo7
First Seen: 04/07/21, 09:03 AM EDT
Last Seen: 07/06/21, 09:03 AM EDT
In Baseline
Summary
Communications
Notifications 253
Vulnerabilities 3
Baseline Behaviors
Dataset
Notes
EDIT ASSET
Actions
Summary
Hardware
Hardware Description: –
Hardware Family: Stratix
Hardware Firmware: 15.2(4)EB.fc2
Hardware Id: –
Hardware Model: Stratix 5700
Hardware Serial: 0114b2e3
Hardware Series: 5700
Hardware Settings: –
Hardware Vendor: Rockwell Automation
Operating System
OS Family:
OS Full: –
OS Kernel: –
OS Name:
OS Platform: –
OS Version: –
Networks Addresses
IP 192.168.99.1
Custom Attributes
AttributesLastObservedDate: 2021-09-29


Asset Inventory
admin
Dashboard
Map
Assets
Data
Notifications
Content
Vulnerabilities
Reports
Sensors
Admin
Summary
Communications
Notifications 253
Vulnerabilities 3
Baseline Behaviors
Dataset
Notes
EDIT ASSET
Actions
Summary
Hardware
Hardware Description: –
Hardware Family: Stratix
Hardware Firmware: 15.2(4)EB.fc2
Hardware Id: –
Hardware Model: Stratix 5700
Hardware Serial: 0114b2e3
Hardware Series: 5700
Hardware Settings: –
Hardware Vendor: Rockwell Automation
Operating System
OS Family:
OS Full: –
OS Kernel: –
OS Name:
OS Platform: –
OS Version: –
Network Addresses
IP 192.168.99.1
MAC 5C:88:16:FC:1D:2C
HOSTNAME safety-sw1
DOMAIN localhost
Custom Attributes
AttributesLastObservedDate: 2021-09-29
Country: USA
Criticality:
macVendorShort: Rockwell
System Owner: Mauricio Renzi
Zone
Zones: Safety Network
Labels
IT
OT
Switch

Safety Network Switch

Hostname: safety-sw1

Class: Controller

Type: Switch

Purdue Level 1

Networks: Default NetworkID RFC1918

Observed By: midpoint-demo7

First Seen: 04/07/21, 09:03 AM EDT

Last Seen: 07/06/21, 09:03 AM EDT

In Baseline

Notifications

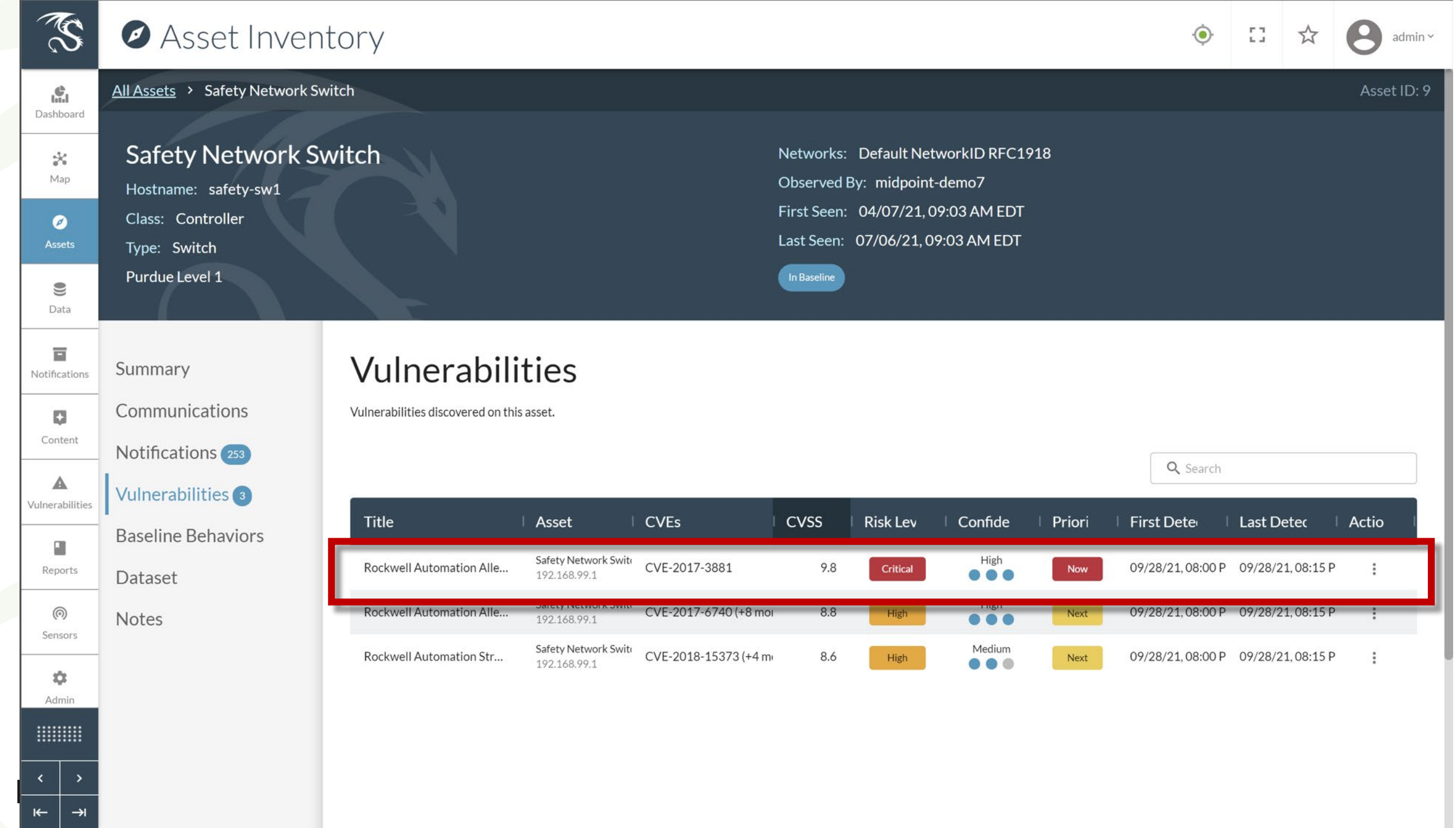
Records of all notifications and alerts for this asset.

Notification Type: All Notifications

VIEW ALL

View	ID	Source	Type	Summary	Occurred At	Severity	Reviewed
VIEW	29121	edef0c7...	Indicator	suspicious .hta file download request	09/27/21, 03:49 PM EDT	2	
Content: suspicious .hta file download request							
VIEW	28969	96012d4...	Indicator	suspicious .hta file download request	09/27/21, 02:07 AM EDT	2	
VIEW	28952	7103aa0...	Indicator	suspicious .hta file download request	09/26/21, 10:45 PM EDT	2	
VIEW	28784	796afa3...	Indicator	ETPRO TROJAN PowerShell Empire Request HTTP Pattern	09/26/21, 09:40 AM EDT	1	
VIEW	28659	a857322...	Indicator	ETPRO TROJAN PowerShell Empire Request HTTP Pattern	09/25/21, 11:33 PM EDT	1	
VIEW	28625	8281813...	Indicator	suspicious .hta file download request	09/25/21, 08:16 PM EDT	2	
VIEW	28481	50071e1...	Indicator	ETPRO TROJAN PowerShell Empire Request HTTP Pattern	09/25/21, 09:46 AM EDT	1	

Showing 10 of 253 Notification(s)


Asset Inventory
admin
Dashboard
Map
Assets
Data
Notifications
Content
Vulnerabilities
Reports
Sensors
Admin
All Assets › Safety Network Switch
Asset ID: 9
Safety Network Switch
Hostname: safety-sw1
Class: Controller
Type: Switch
Purdue Level 1
Networks: Default NetworkID RFC1918
Observed By: midpoint-demo7
First Seen: 04/07/21, 09:03 AM EDT
Last Seen: 07/06/21, 09:03 AM EDT
In Baseline
Summary
Communications
Notifications 253
Vulnerabilities 3
Baseline Behaviors
Dataset
Notes
Vulnerabilities
Vulnerabilities discovered on this asset.
Search
Title
Asset
CVEs
CVSS
Risk Lev
Confide
Priori
First Dete
Last Detec
Actio
Rockwell Automation Alle...
Safety Network Swit
192.168.99.1
CVE-2017-3881
9.8
Critical
High
Now
09/28/21, 08:00 P
09/28/21, 08:15 P
Rockwell Automation Alle...
192.168.99.1
CVE-2017-6740 (+8 mo
8.8
High
Next
09/28/21, 08:00 P
09/28/21, 08:15 P
Rockwell Automation Str...
Safety Network Swit
192.168.99.1
CVE-2018-15373 (+4 m
8.6
High
Medium
Next
09/28/21, 08:00 P
09/28/21, 08:15 P

Rockwell Automation Allen-Bradley Stratix and Allen-Bradley ArmorStratix

Successful exploitation of this vulnerability may allow a remote attacker to im...

Source Intelligence
First Seen 09/28/21, 08:00 PM EDT
Last Seen 09/28/21, 08:15 PM EDT
Published 04/03/17, 08:00 PM EDT
CVE-2017-3881

Priority - Now
Risk Level - Critical
Confidence
Highest CVSS Base: 9.8
Dragos Corrected CVSS: 9.8 (Critical)
State: Open

Asset Details

Name	Safety Network Switch
Hostname	safety-sw1
FQDN	localhost
MAC	5C:88:16:FC:1D:2C
IP	192.168.99.1

Summary

Description

Successful exploitation of this vulnerability may allow a remote attacker to impact the availability of the target device or to execute arbitrary code with elevated privileges.

Dragos Guidance

No patch has been released to address these vulnerabilities.

Disable the Telnet protocol if possible or restrict access to port TCP/23.

Port	# Source IPs	Actions
23	0	⋮

Affected Products

Hardware: Rockwell Automation, Stratix, 5700, <=15.2(5)EA.fc4

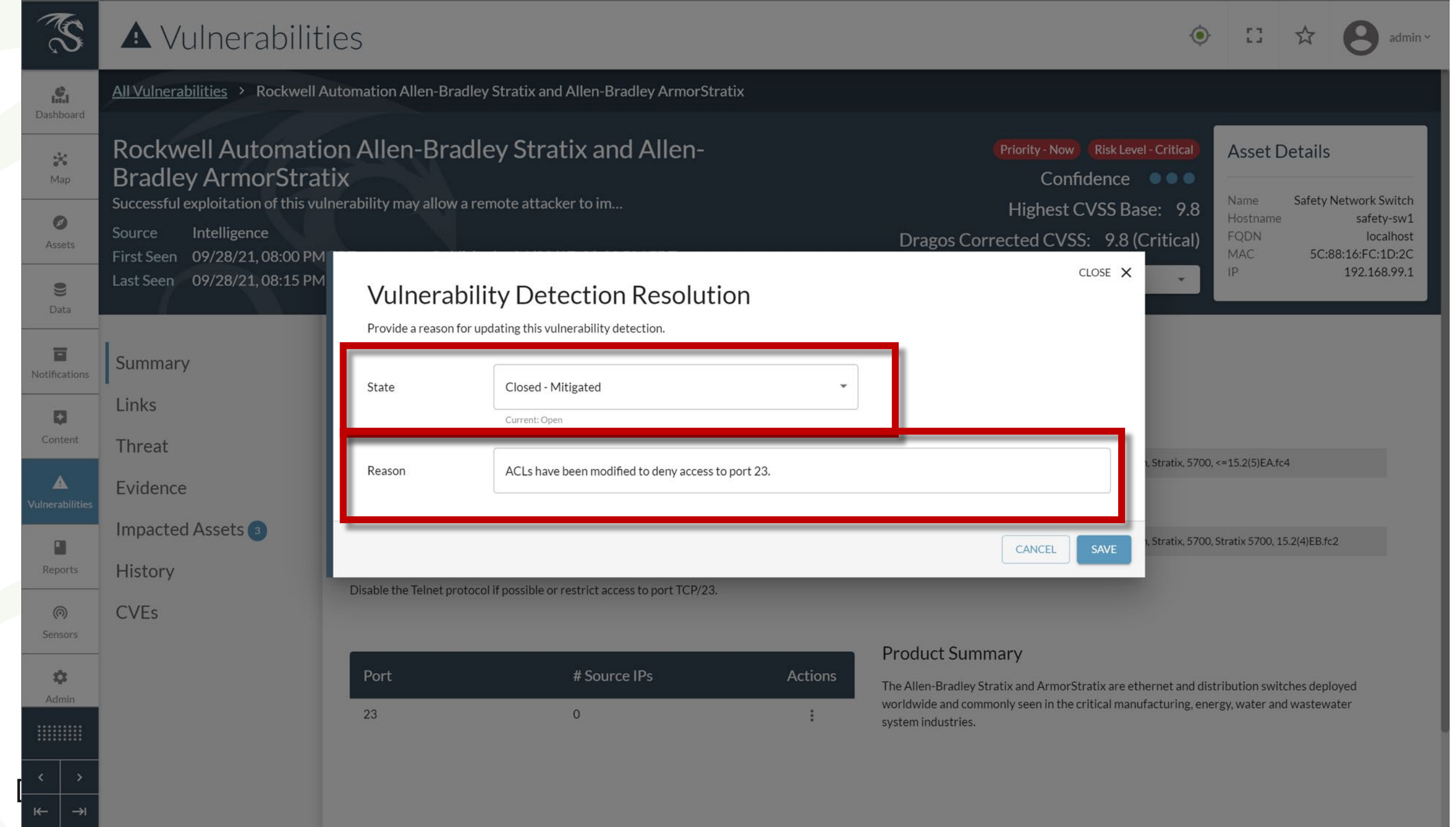
Current:

Hardware: Rockwell Automation, Stratix, 5700, Stratix 5700, 15.2(4)EB.fc2

OS:

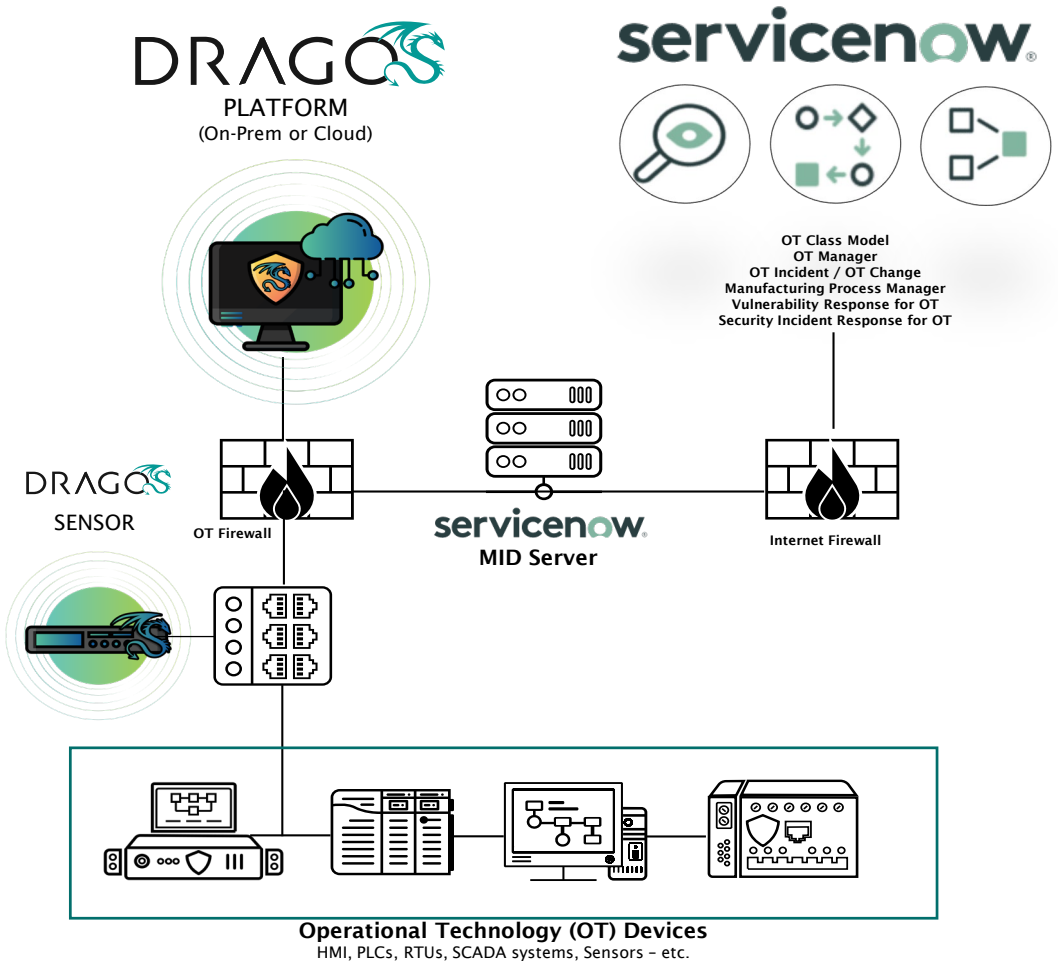
Product Summary

The Allen-Bradley Stratix and ArmorStratix are ethernet and distribution switches deployed worldwide and commonly seen in the critical manufacturing, energy, water and wastewater system industries.


Vulnerabilities
admin
Dashboard
Map
Assets
Data
Notifications
Content
Vulnerabilities
Reports
Sensors
Admin
All Vulnerabilities > Rockwell Automation Allen-Bradley Stratix and Allen-Bradley ArmorStratix
Rockwell Automation Allen-Bradley Stratix and Allen-Bradley ArmorStratix
Successful exploitation of this vulnerability may allow a remote attacker to im...
Source Intelligence
First Seen 09/28/21, 08:00 PM
Last Seen 09/28/21, 08:15 PM
Priority - Now
Risk Level - Critical
Confidence
Highest CVSS Base: 9.8
Dragos Corrected CVSS: 9.8 (Critical)
Asset Details
Name Safety Network Switch
Hostname safety-sw1
FQDN localhost
MAC 5C:88:16:FC:1D:2C
IP 192.168.99.1
Summary
Links
Threat
Evidence
Impacted Assets 3
History
CVEs
CLOSE
Vulnerability Detection Resolution
Provide a reason for updating this vulnerability detection.
State
Closed - Mitigated
Current: Open
Reason
ACLs have been modified to deny access to port 23.
CANCEL
SAVE
Stratix, 5700, <=15.2(5)EA.fc4
Stratix, 5700, Stratix 5700, 15.2(4)EB.fc2
Disable the Telnet protocol if possible or restrict access to port TCP/23.
Port
Source IPs
Actions
23
0
Product Summary
The Allen-Bradley Stratix and ArmorStratix are ethernet and distribution switches deployed worldwide and commonly seen in the critical manufacturing, energy, water and wastewater system industries.

ServiceNow Integrations

- ServiceNow OT Manager
  - Asset Visibility into OT/ICS
  - Service Graph connector
  - MID Server support
- Coming soon:
  - Vulnerability Response for OT
  - Security Incident Response for OT



THANK YOU

Resources

- Dragos in the Deloitte Smart Factory @WSU
  - www.dragos.com/smartfactoryvideo
- An Executive Guide to Industrial Cybersecurity
  - www.dragos.com/resource/executive-guide-to-industrial-cybersecurity/
- Dragos Manufacturing Threat Perspective
  - www.dragos.com/resource/manufacturing-threat-perspective/
- Vulnerability management white paper
  - www.dragos.com/platform/vulnerability-management/
- Asset management white paper
  - www.dragos.com/platform/asset-visibility/

Schedule a demo: dragos.com/request-a-demo/