

The background features a vibrant, abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, cyan, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

Securing transportation and utilities at scale

Industrial Internet of Things (IIoT)

Fayce Daira - TSA

BRKIOT-1627

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

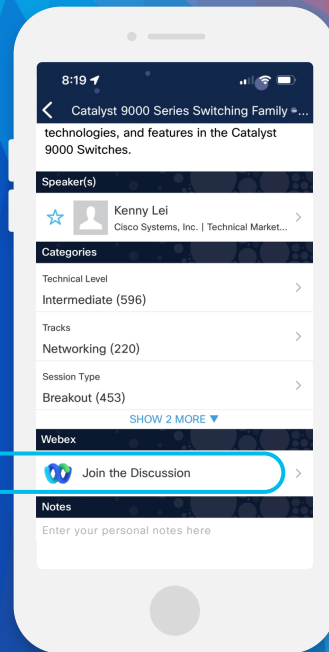
Questions?

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

How

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

Webex spaces will be moderated by the speaker until December 22, 2023.

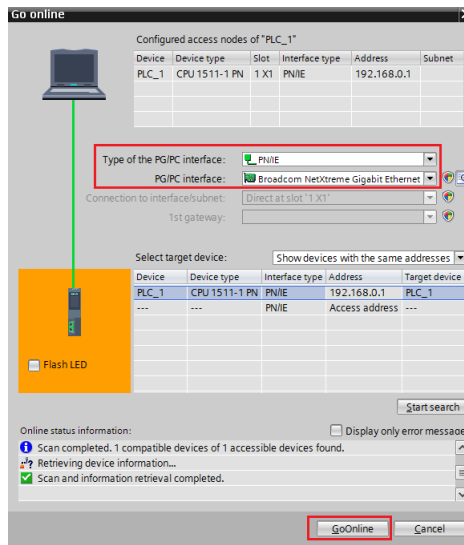


<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKIOT-1627>

Agenda

- Introduction
- Transportation
- Utilities
- How to secure it?
- Assess Security
- Conclusion

A little bit about myself

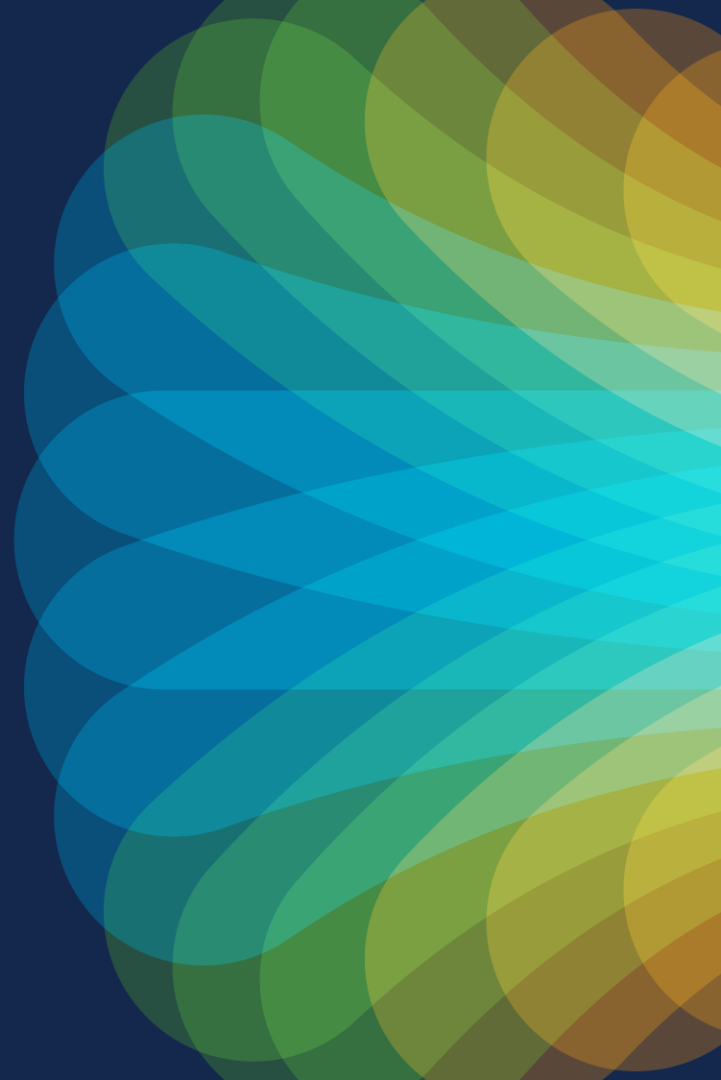


Identical twins getting identical
twins is nearly impossible.
It's like winning the lottery twice

My OBGY March 2015



Introduction



Critical Infrastructure Priorities

1

Reduce Accident and Incident

2

Improve Operational Efficiency

3

Optimize Costs

Cyber Security Priorities

1

Reduce attack surface : Patch and upgrade regularly

2

Only need to give access when needed

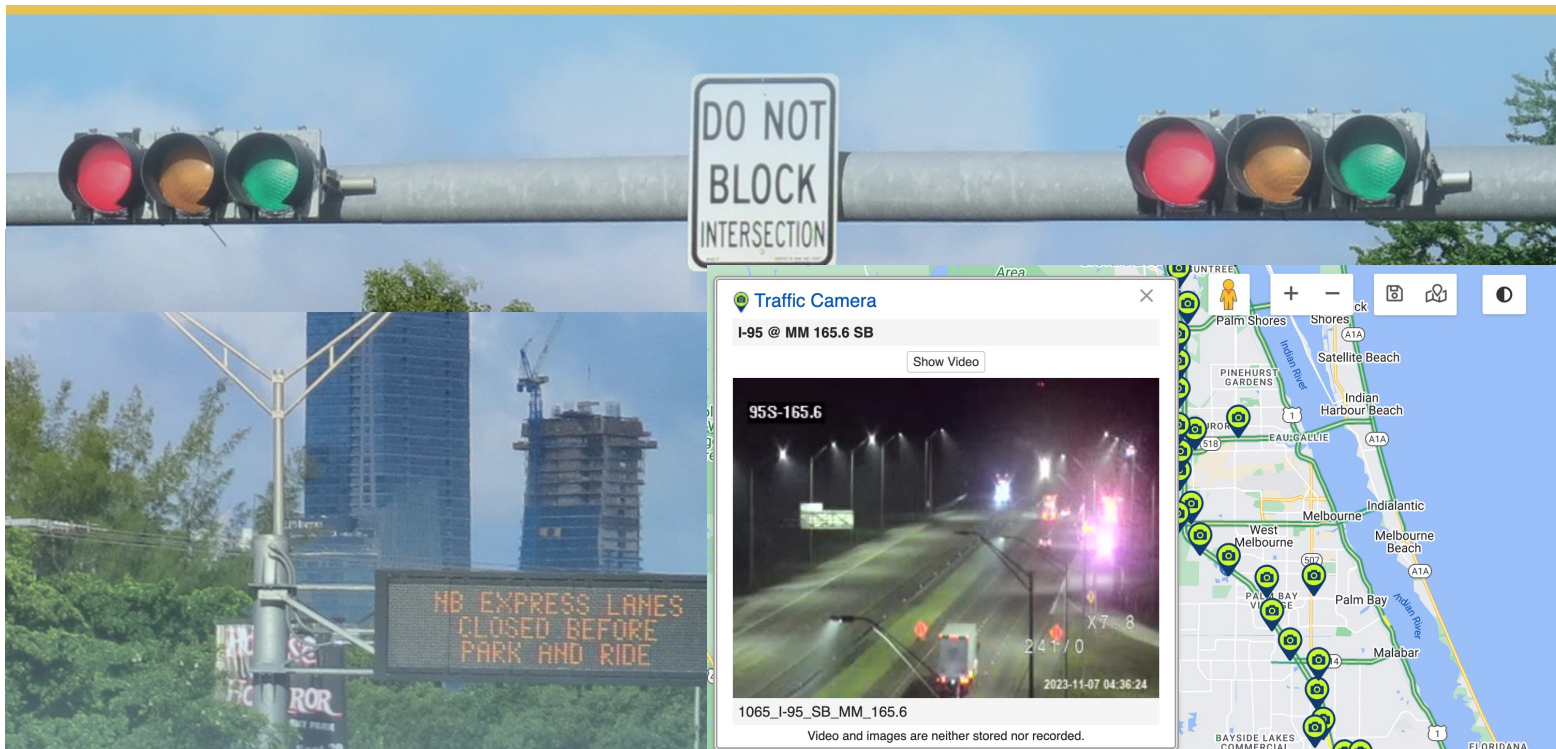
3

Resilience against attack

Transportation

What is Transportation ?





Tools to gain access to the network

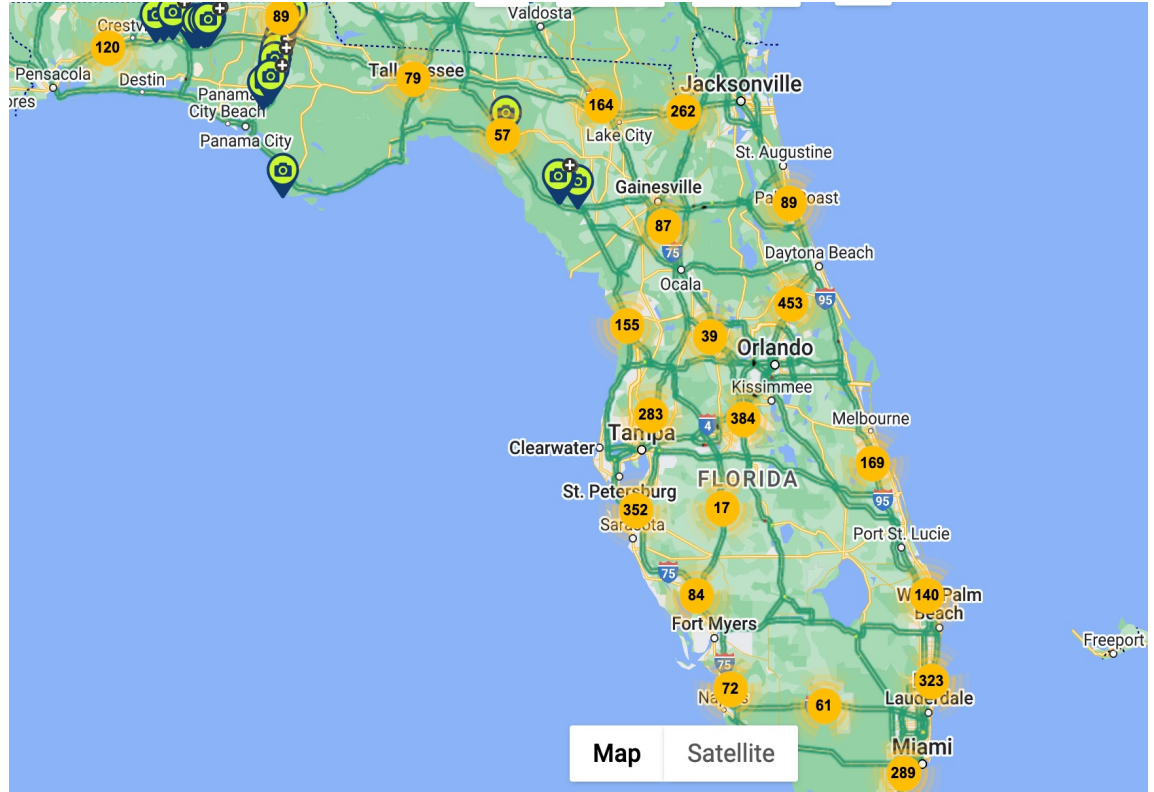


Challenges

- Large Scale networks
- One Centralize Traffic Management reaching ten thousands of sites
- Each site is a cabinet on the roadway with low bandwidth network connection (Broadband, LTE)
- Life Cycle are very long for the hardware 15-35 years
- A lots of devices behind a routers and ring-based architecture
- Multiple Vendors of hardware

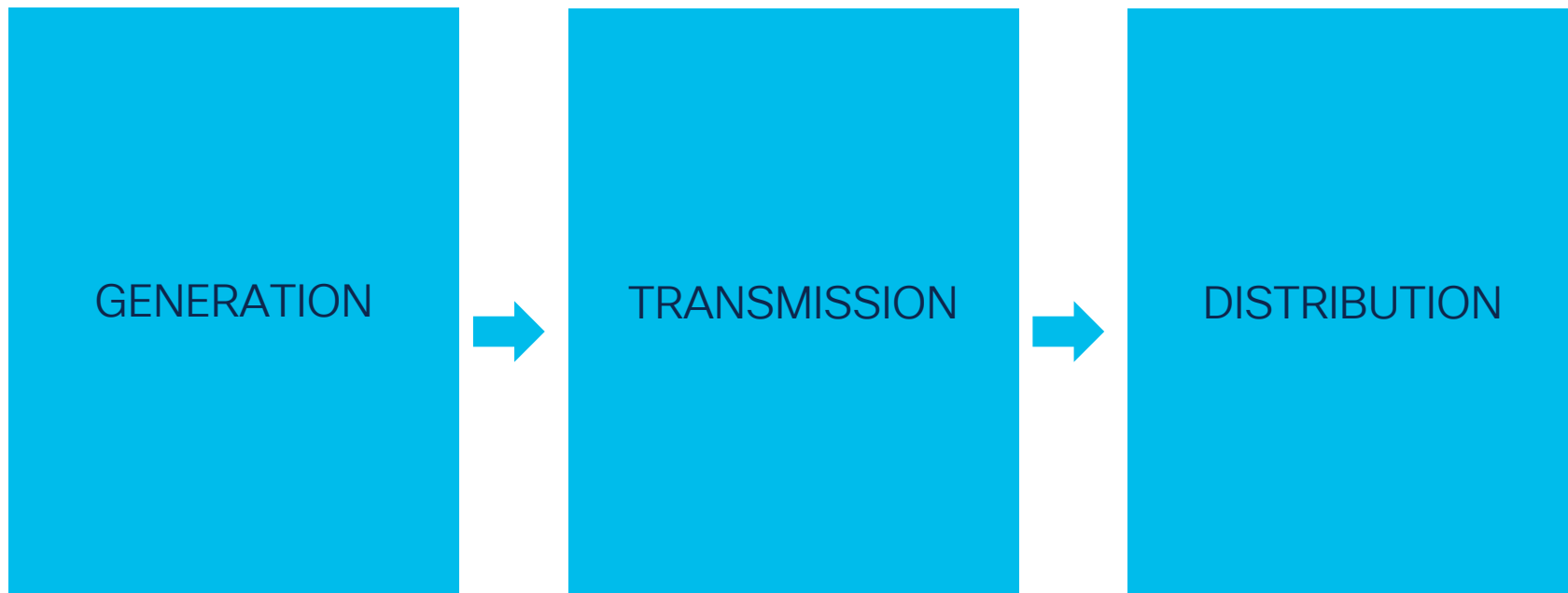
Large Scale Network

- Public Information Available
- Traffic Camera provides you information about cabinet location



Utilities

What is Utilities ?



Generation challenges

- Older systems (Nuclear, Thermal, water not connected or data diode system)
- Solar and Wind Farms management with limited connectivity

Distribution challenges

- Substation not necessarily connected
- Highly segmented network but no visibility

Challenge to address Physical attacks



Moore County Substation Attack

Power substations at the Duke Energy West End location in Moore County, N.C., were damaged in an attack that left tens of thousands of people without electricity.

How to secure it ?



You can't secure what you don't
know

Attack Techniques used to exploit the Industrial Network



Initial
Access
(TA0108)



Discovery
(TA0102)



Lateral
Movement
(TA0109)



Command and
Control
(TA0101)

Colonial Pipeline ransomware attack: Everything you need to know

Updated: DarkSide has claimed responsibility for the catastrophic ransomware

What is SMB vulnerability and how it was exploited to launch the WannaCry ransomware attack?

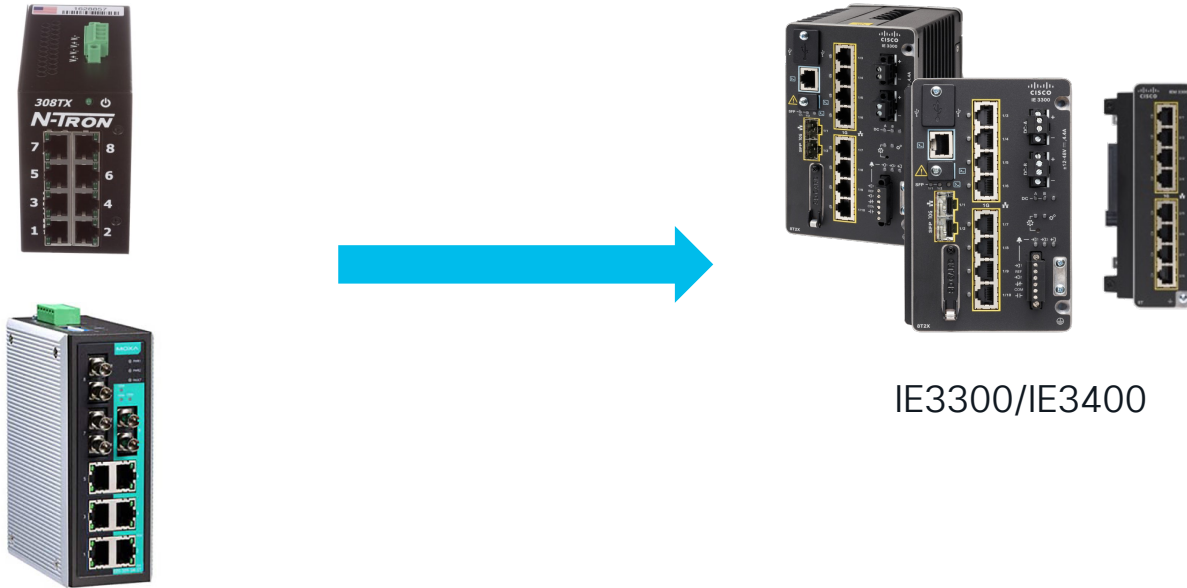
• Cyware Hacker News

S0604	Industroyer	The Industroyer IEC 61850 payload component has the ability to discover relevant devices in the infected host's network subnet by attempting to connect on port 102. ^[6] Industroyer contains an OPC DA module that enumerates all OPC servers using the <code>ICatInformation::EnumClassesOfCategories</code> method with <code>CATID_OPDAServer20</code> category identifier and <code>IOPCServer::GetStatus</code> to identify the ones running.
S1006	PLC-Blaster	PLC-Blaster scans the network to find other Siemens S7 PLC devices to infect. It locates these devices by checking for a service listening on TCP port 102. ^[7]
S1009	Triton	Triton uses a Python script that is capable of detecting Triconex controllers on the network by sending a specific UDP broadcast packet over port 1502. ^[8]

Stuxnet explained: The first known cyberweapon

Thanks to Stuxnet, we now live in a world where code can destroy machinery and stop (or start) a war.

Move away from unmanaged switches



Switches Must have

- Support 802.1x authentication
- Support MAB (Mac Authentication Bypass)
- 802.1x/MAB provides network visibility because the authentication process provides a way to link the IP address, MAC address, switch, and port of a device.

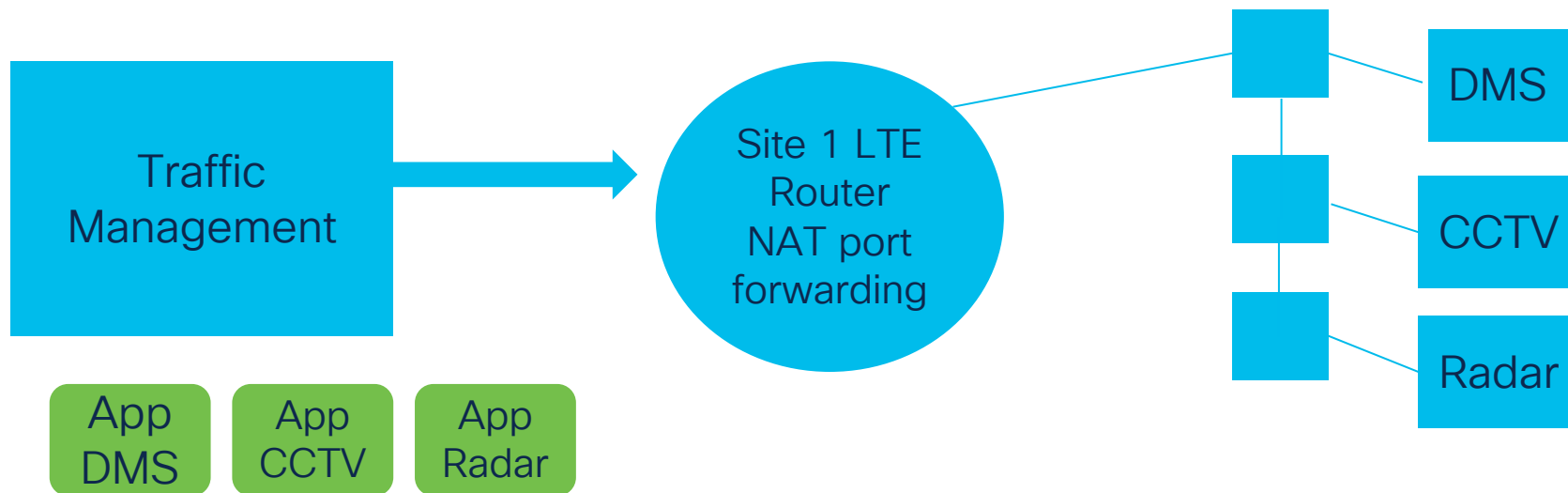
Assess Security

What is the current Level of security on each main sites?

Security	Site 1 : Atlanta	Site 2 : Austin
IT and OT distinct Network	Yes	No
Industrial DMZ	Yes	No
Antivirus on Windows systems	No	No
Multi-factor authentication	Yes	No

Extending Visibility

Transportation Network Challenges



Cisco Cyber Vision

Visibility & Security Platform for the Industrial IoT

Context & insights foundational to building reliable and secure OT networks



Visibility

Asset inventory
Communication patterns



Security Posture

Device vulnerabilities
Risk scoring



Operational Insights

Track process/device modifications
Record control system events

CISCO *Live!*



Enlist your network for security



Cisco Industrial switches and routers **see everything** that attaches to them so you can gain **visibility at scale**

CISCO *Live!*

#CiscoLiveAPJC

BRKIOT-1627

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

34



Deep Packet Inspection & Active Discovery
built into your network infrastructure

Benefits

- No bandwidth consuming of copy of traffic
- Router and switches provides visibility no additional hardware with long live-cycle 15years
- Support visibility behind VPN with NAT
- Support of multiple identical subnets (192.168.0.x)

Security Posture

Use Risk Scoring to assess your security posture

Identify Riskiest Operations

Preset	Risk score	Last precomputation	Devices	Vulnerabilities
All Controllers	24.5	Jun 17, 2021 9:46:41 AM	14	94
Broadcast traffic only	12	Jun 17, 2021 9:46:47 AM	30	158
IT Activities	16	Jun 17, 2021 9:46:47 AM	36	169
IT Devices	25	Jun 17, 2021 9:46:49 AM	23	94
Internet Activities	12	Jun 17, 2021 9:46:45 AM	0	0
OT Devices	28	Jun 17, 2021 9:46:46 AM	21	128

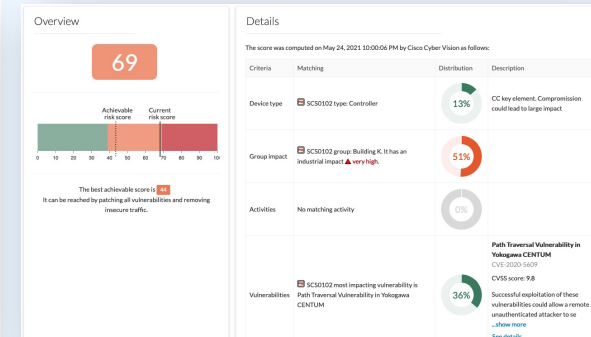
Preset widgets help identify operations at highest risk

Identify Riskiest Endpoints within operations

Device	Group	First activity	Last activity	IP	MAC	Risk score	Tags
SC50102	Building K	Oct 11, 2019 11:06:52 AM	May 24, 2021 12:30:15 PM	192.168.1.5 (+ 1 other)	00:06:64:8c:8a:5c (+ 1 other)	41	# Controller - # Time Server
Fisher 10.5.0.22	Emerson Process	Oct 11, 2019 11:03:46 AM	May 24, 2021 12:30:15 PM	10.5.0.22	00:22:45:1f:90:18	41	# Controller - # Default
Fisher 10.4.0.14	Emerson Process	Oct 11, 2019 11:03:46 AM	May 24, 2021 12:30:15 PM	10.4.0.14	00:22:45:1f:9a:54	41	# Controller - # Default
10.4.0.30	Emerson Process	Oct 11, 2019 11:03:46 AM	May 24, 2021 12:30:15 PM	10.4.0.30 (+ 1 other)	00:22:45:21:0a:6f	41	# Controller - # Time Server - # Default
Yokogawa 192.168.1.124	Fujitsu	Oct 11, 2019 11:06:52 AM	May 24, 2021 12:30:15 PM	192.168.1.124	00:06:64:8c:8a:00 (+ 1 other)	41	# Controller
Fisher 10.5.0.18	Emerson Process	Oct 11, 2019 11:03:46 AM	May 24, 2021 12:30:15 PM	10.5.0.18	00:22:45:1f:90:25	41	# Controller - # Default
Fisher 10.4.129.2	Emerson Process	Oct 11, 2019 11:03:46 AM	May 24, 2021 12:30:15 PM	10.4.129.2	00:22:45:04:43:4a	41	# Net Management Server
Fisher 10.4.129.1	Emerson Process	Oct 11, 2019 11:03:46 AM	May 24, 2021 12:30:15 PM	10.4.129.1	00:22:45:12:4c:9c	41	# Net Management Server
192.168.1.123	Fujitsu	Mar 11, 2020 8:21:58 PM	May 24, 2021 12:30:15 PM	192.168.1.123 (+ 1 other)	4c:52:62:33:95:09	35	# Email Server
Hirschmann 192.168.1.254	Building K	Oct 11, 2019 11:06:52 AM	May 24, 2021 12:30:15 PM	192.168.1.254	ec:74:b0:03:96:46	35	# Time Server
Yokogawa 192.168.1.128	Fujitsu	Oct 11, 2019 11:06:52 AM	May 24, 2021 12:30:15 PM	192.168.1.128	00:06:64:8c:8a:15 (+ 1 other)	35	# Time Server

Sort and Filter Risk scores of endpoints to identify riskiest devices

Understand Scoring to Reduce Risk



See what impacts endpoint risk score
See where you are, and where you could be

Build an action plan to reduce risk

Identify and stop existing leak to public ip

28 External Communications

Direction	Source IP	Destination IP	Destination Port	Hostname	Protocol
Outbound	10.122.101.241	20.189.173.16	443		HTTPS
Outbound	10.122.101.241	20.189.173.16	443	v10.events.data.microsoft.com	HTTPS
Outbound	10.122.101.241	52.142.223.178	80	dmd.metaservices.microsoft.com	HTTP
Outbound	10.122.101.241	52.142.223.178	80		HTTP
Outbound	10.122.101.241	23.65.13.232	80	tile-service.weather.microsoft.com	HTTP
Outbound	10.122.101.241	23.65.13.232	80		HTTP
Outbound	10.122.101.241	23.215.126.183	80		HTTP
Outbound	10.122.101.241	23.215.126.183	80	go.microsoft.com	HTTP
Outbound	10.122.101.241	40.126.29.15	443		HTTPS
Outbound	10.122.101.241	20.189.173.20	443	umwatson.events.data.microsoft.com	HTTPS



Remote Admin Server ^①



Desktop ^{As}



Desktop [▲] None

IP: 10.122.101.241

MAC: 4c:3b:df:c1:b6:97



First activity

Nov 6, 2023 2:06:51 PM



Last activity

Nov 6, 2023 2:09:40 PM



Device with external communications

Sensors:

-

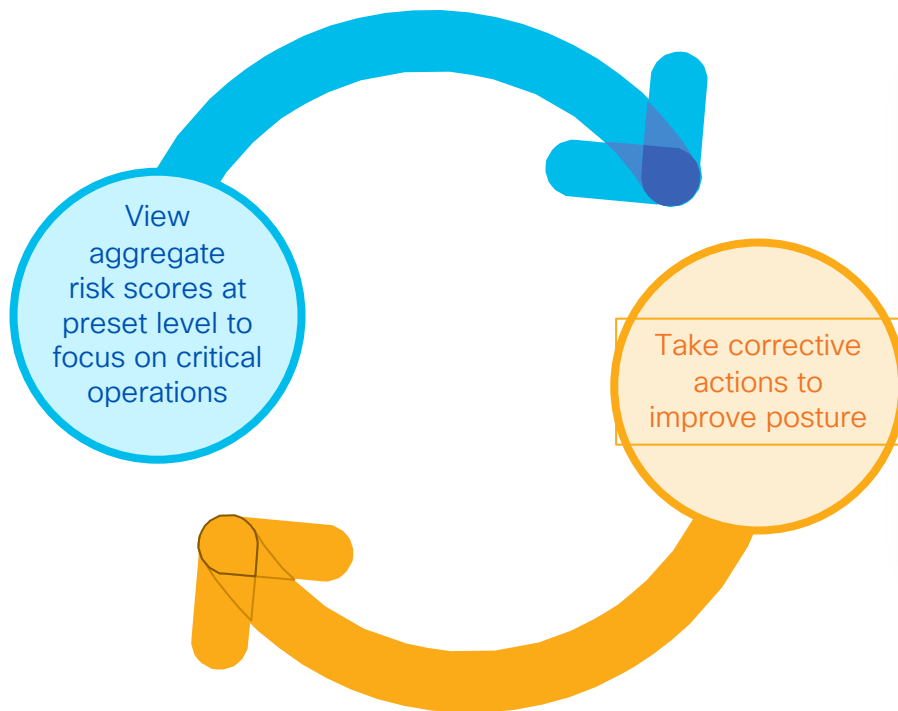
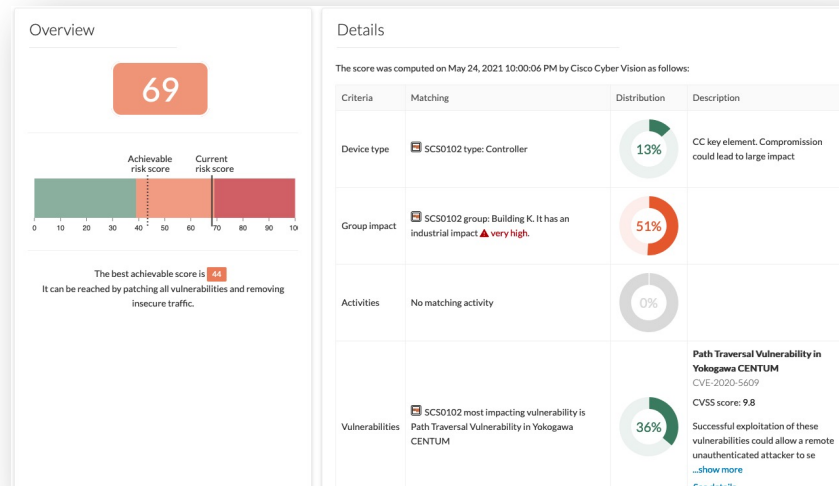
Tags:

HTTP Client, HTTPS Client,
Remote Admin Server, Windows

Activity tags:

Insecure, RDP, Remote access, Web,
Broadcast, Low Volume, Multicast, ARP,
HTTP, Multicast DNS, ...4+

Iterate until your posture is where it needs to be



Endpoint risk score indicates what is impacting the current scoring, and shows the best achievable score

Leverage Visibility Segmentation



Lessons learnt from customers

Crawl → Walk → Run



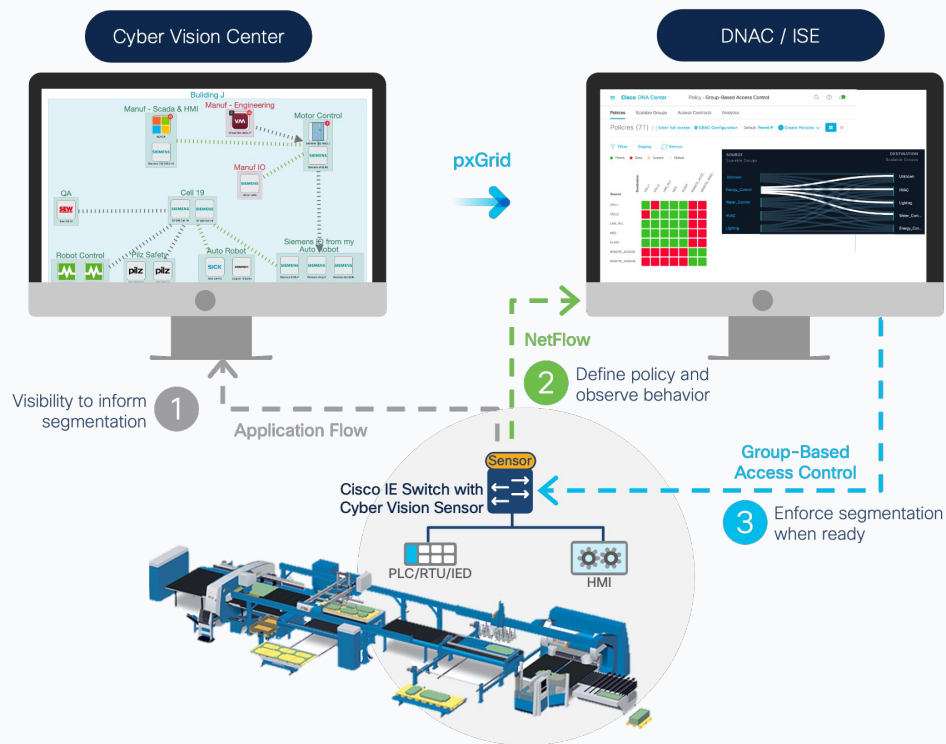
Most customers are not staffed to operationalize segmentation in industrial networks right from the get-go

1. Start with Visibility & Security Posture
2. Advance to macro-segmentation
3. Evolve towards shrinking the zones of trust with micro-segmentation as teams get comfortable with the technology

As you shrink zones of trust, OT's ability to see/understand why certain flows are blocked becomes important for seamless operations

Cisco Segmentation Solution

Visualize -> Dynamically Assign Tags -> Monitor Policy -> Enforce



Visualize Zones & Conduits

Group endpoints into zones to visualize aggregated flows as conduits to inform segmentation policy

Dynamic SGT Mapping

Cyber Vision grouping results in dynamic Group-based policy assignment to endpoints through ISE

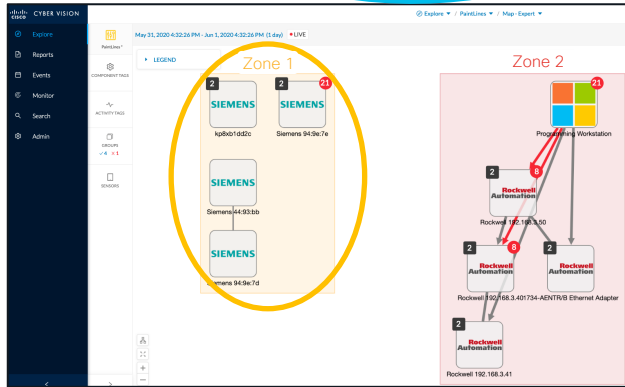
Monitor Before Enforcement

Visualize Group-based network behavior in DNAC and enable enforcement when confident after monitoring

Uses the right team with their expertise



This user interface maps ITS assets. I can group assets into zones



Cyber Vision Map View



I now have OT context to build the right security policies

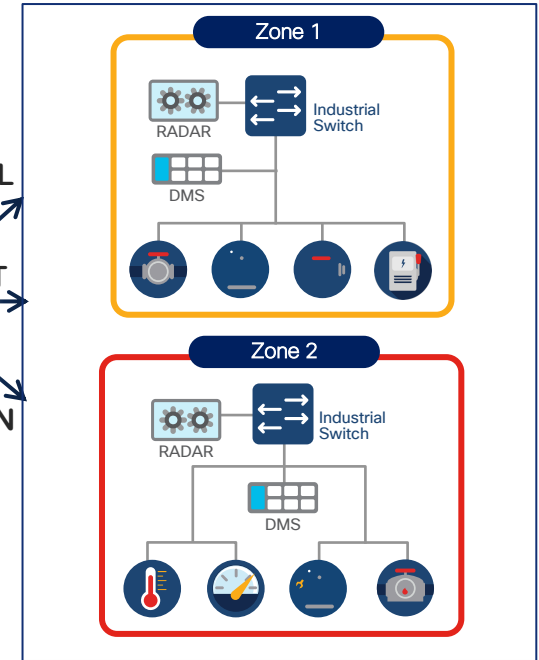
	Zone 1	Zone 2	Zone 3	Zone 4
Zone 1	✓	✗	✓	✗
Zone 2	✗	✓	✓	✗
PLC	✓	✓	✓	✓
MES	✗	✗	✓	✓

pxGrid update with asset endpoint identities and group Cell1 as custom attribute

Cisco ISE Policy Matrix

dACL
SGT
VLAN

Segmentation of industrial network





Cisco industrial network helps you secure OT



Leverage your network to **gain** visibility



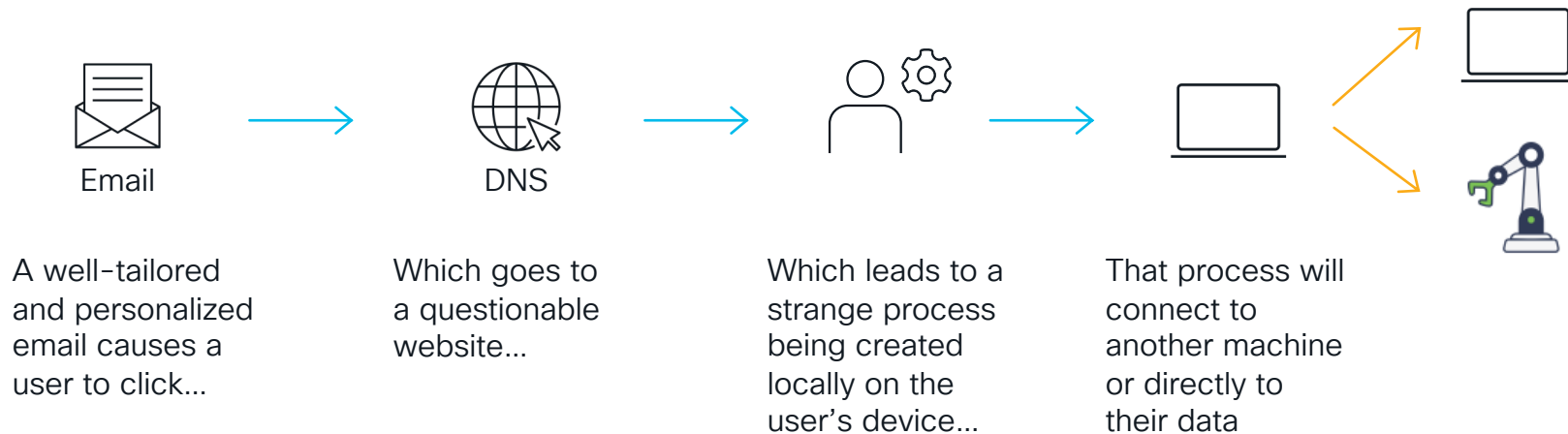
Leverage your network to **gain** insights



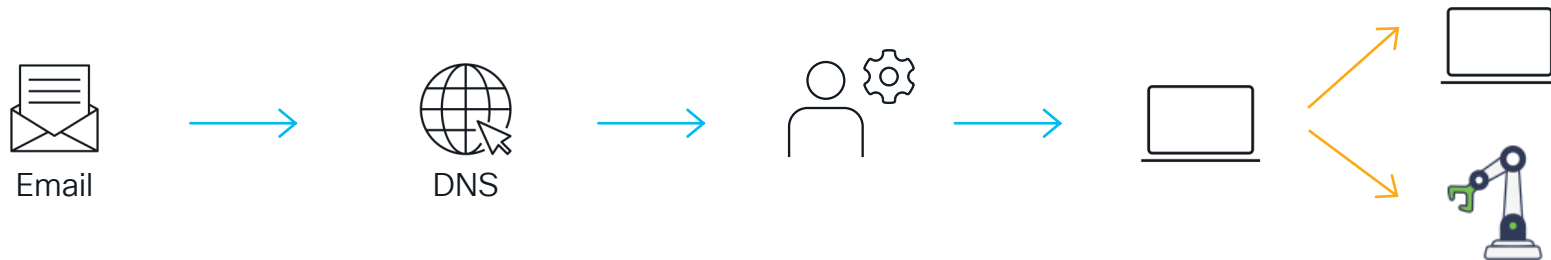
Leverage your network to **enforce** security controls

How to respond?

Most attacks use a sequence like this....



Most attacks use a sequence like this....

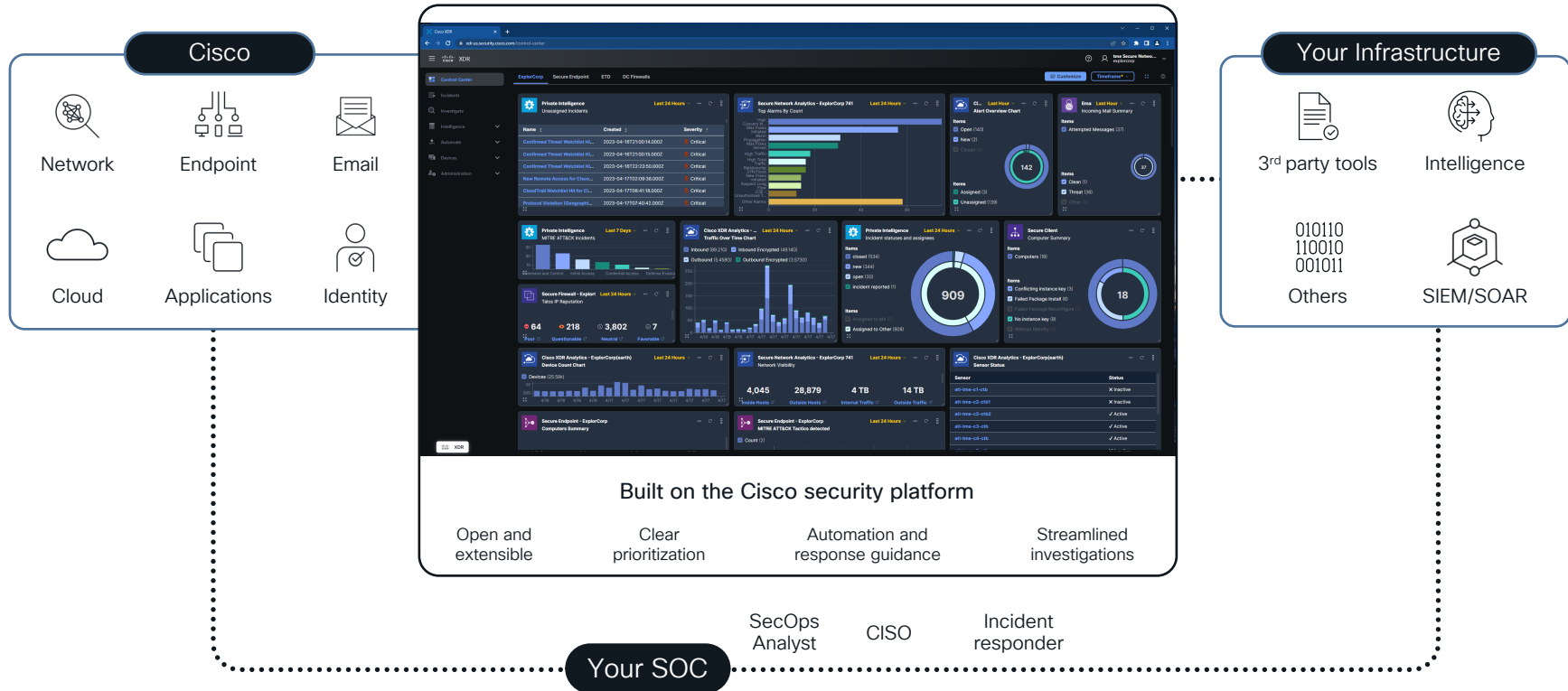


You need a solution that sees deeply across the entire attack chain

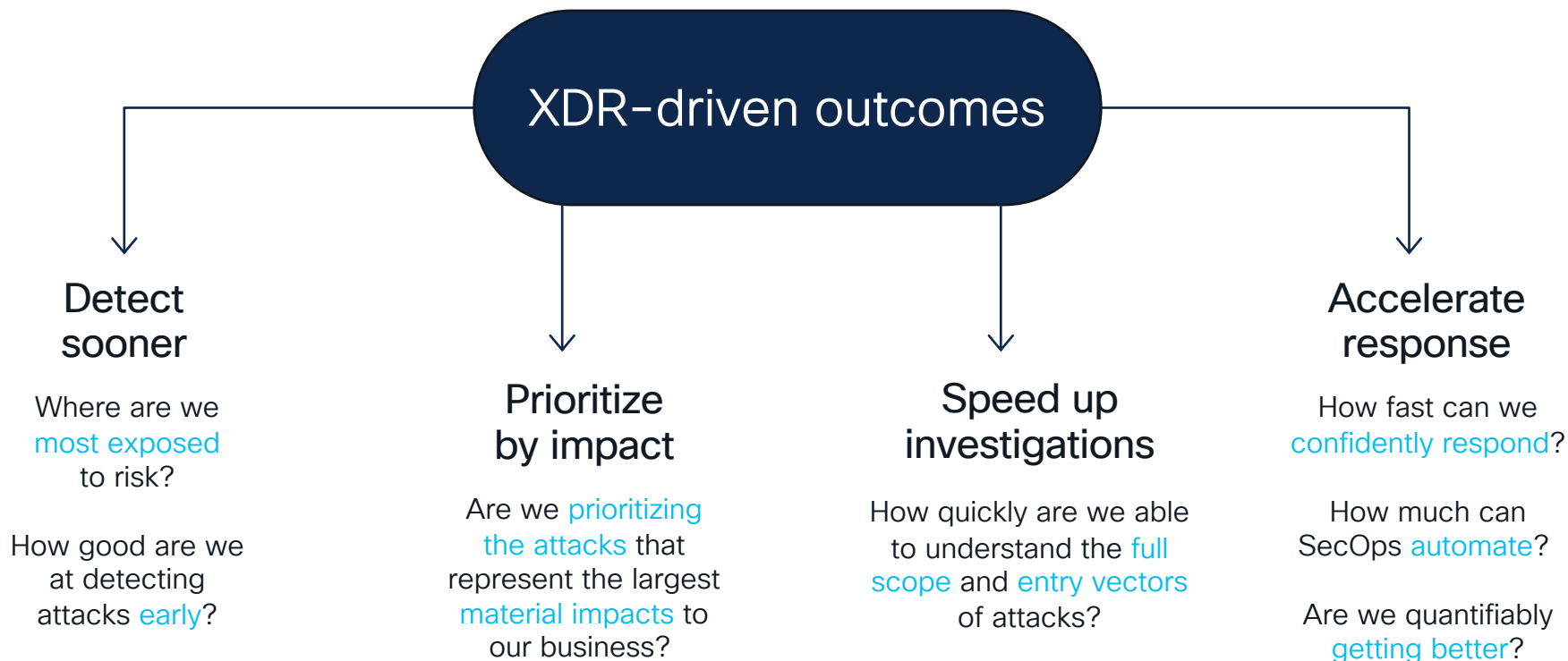


Built on the Cisco Security Cloud platform

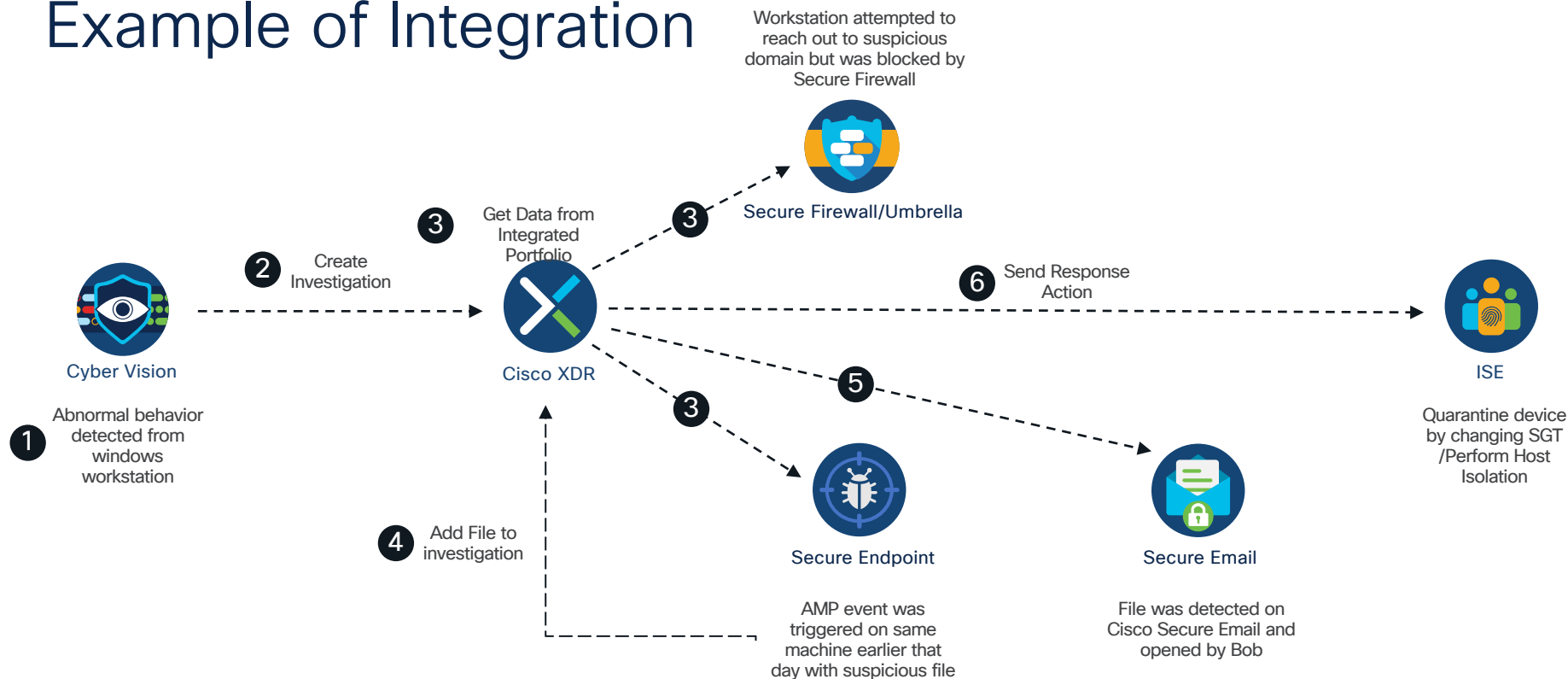
Simplify with Cisco XDR



The Cisco approach to XDR



Example of Integration



Investigation & Orchestration with XDR

Leverage Cyber Vision
Observables to:

Create and **manage**
incidents in XDR

Create and **orchestrate**
playbooks

Launch investigations in
Talos, Umbrella, Secure
Endpoint, Threat Grid, etc.

The screenshot displays the Cisco Cyber Vision interface. The top section shows a table of 23 devices and 32 components. The table columns include Device, Group, First activity, Last activity, IP, MAC, Risk score, Tags, Activities, Yuh, Var, VLAN ID, Vendor, and OS. The bottom section shows an incident detail view for a Snort Network Trojan detected on 2021-07-28 08:16:52 UTC. The incident details include a summary, observables, and a timeline. The observables section lists several IP addresses and MAC addresses. The timeline shows the incident was assigned to the user on 2021-07-28 14:22:28.

XDR Ribbon in Cyber Vision for investigations and remediation orchestration

Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background of the slide is a vibrant, abstract graphic. It features a series of overlapping, wavy bands of color in a rainbow spectrum, transitioning from red and orange on the left to yellow, green, and blue on the right. On the right side, there is a bright, multi-colored sunburst or starburst effect that radiates outwards, creating a sense of energy and excitement.

cisco *Live!*

Let's go

#CiscoLiveAPJC