Strengthening Cybersecurity at the Intersection

Addressing Vulnerabilities from Controller Devices to Network Infrastructure

Mike McIntee, Q-Free
Alex Clark, Cisco

Taking things seriously

Transportation is one of the 16 critical infrastructure sectors designated by DHS and CISA

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

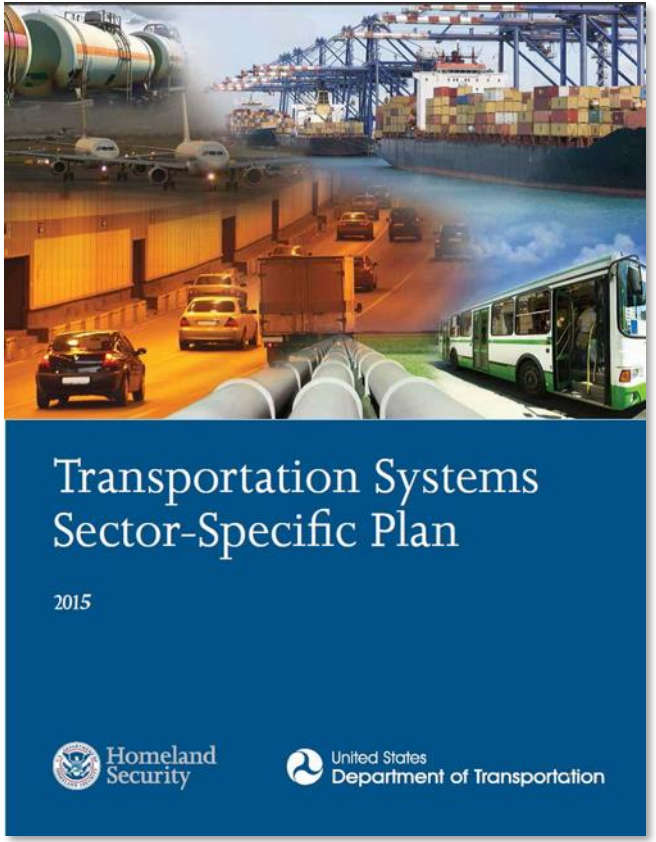
Transportation Systems Sector

- Aviation
- Highway and Motor Carrier
  - *"traffic management systems; and cyber systems used for operational management."*
- Maritime Transportation Systems
- Mass Transit and Passenger Rail
- Pipeline Systems
- Freight Rail
- Postal and Shipping

How well are we executing against the plan?

3.3.2 Cybersecurity

Cyber-based technologies in transportation operations enable greater economies and efficiencies, improve customer service, enhance operational controls, and provide better security capabilities. Consequently, transportation companies are increasingly dependent on cyber systems for business, security, and operational functions. Cyber technologies upon which transportation services rely include positioning, navigation, tracking, shipment routing, industrial system controls, access controls, signaling, communications, and data and business management. These technologies are often interconnected through networks and remote access terminals, which may allow malicious actors easier access to key nodes. Continuity of operations and system resilience following a disaster are increasingly dependent on the recovery of cyber systems.



How bad is it?

Transportation was 37% of tracked OT cyber attacks with physical consequences in 2024.

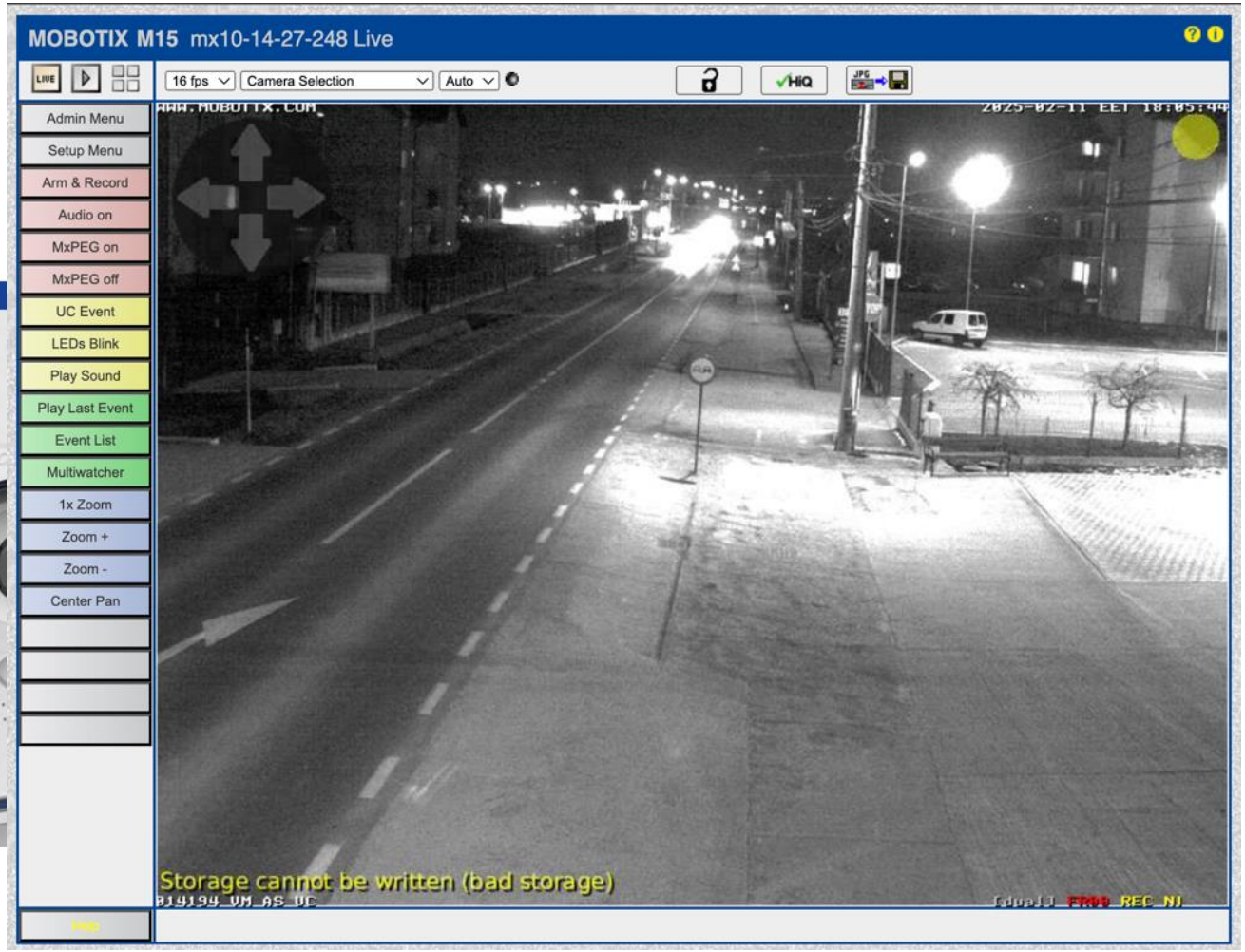
146% increase in sites suffering physical impairment of operations because of cyber attacks vs. 2023

Nation states 6:1 Hacktivists

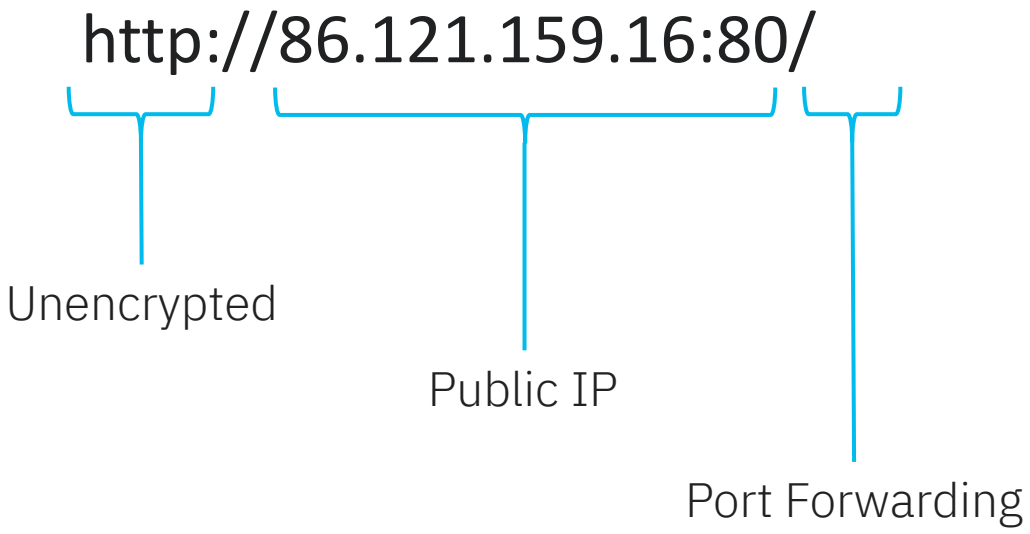
Source: Waterfall ICS Strive 2025 OT Cyber Security Report

Troublesome Cameras

Somewhere in Romania…



A screw up, in three acts:



MOBOTIX mx10-14-27-248 Camera Status

▽ System

Model	M15D-Sec
Serial Number	10.14.27.248
Hardware	T2r4.3b, 806 MHz
Image Sensor	b/w 5MP, L51,F2.0 color 5MP, L51,F2.0
Software	MX-V4.4.2.69 (2017-07-20)
Date and Time	2025-02-11 18:07:04 EET
Current Uptime	1 day 15:01:52

▽ Networking

Camera Name	mx10-14-27-248	
BOOTP/DHCP	off	
Zeroconf	on	
IP Address	192.168.1.2	
Network Mask	255.255.255.0	
Broadcast	192.168.1.255	
Additional IP Address	10.14.27.248	
DNS Server	8.8.8.8, 193.231.247.13	
Link Speed and Duplex	10Mbps / Full Duplex	
Statistics	Dropped: 0.0%	Collisions: 0%
Time Server IP(s)	0.pool.ntp.org (NTP)	

▽ Routing

Default Route	Gateway: 192.168.1.1 Connection: Ethernet interface

▷ Audio

▷ File Server / Flash Device

▷ Event and Action Setup

▷ Recording Setup

▷ Sensors

▷ Image Setup

▽ Web and Network Access

Active Clients	5 live and 0 playback channels	
Listening Ports	80/tcp (IPv6)	thttpd
	123/udp	ntpd
	443/tcp (IPv6)	thttpd
	5353/udp	mdnsd
	60150/udp	mdnsd
	60555/udp (IPv6)	mdnsd
Your IP Address	83.97.13.216	
Your Browser	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36	

Software Version

192.168.1.2

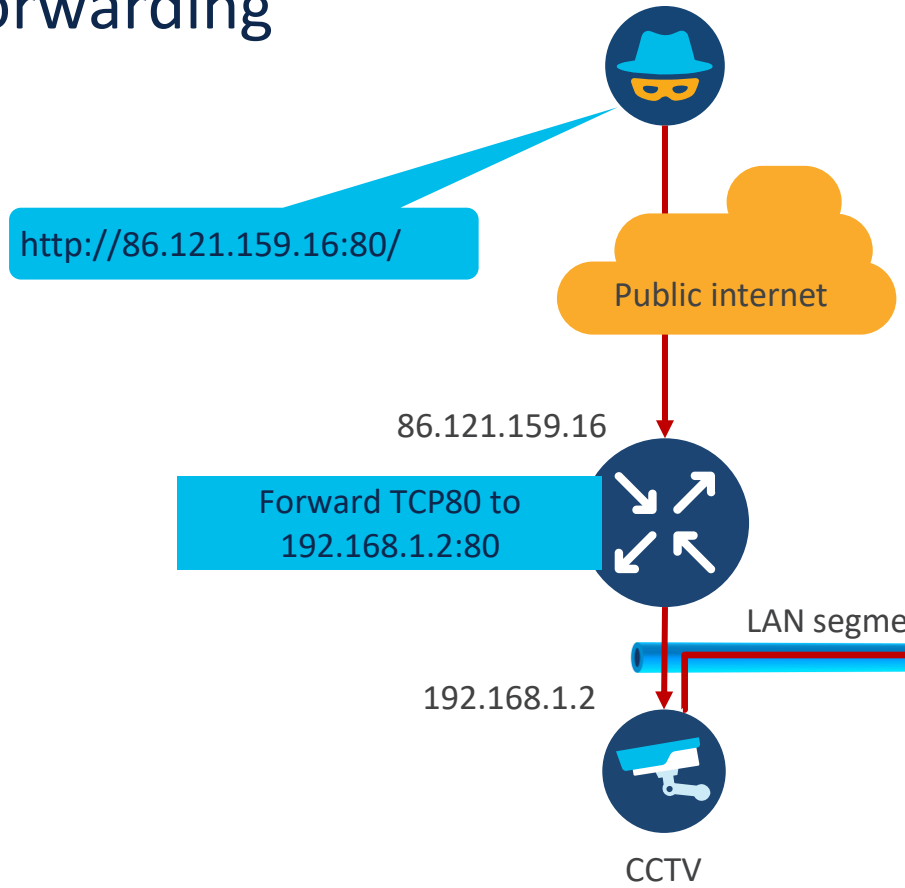
10Mbps / Full

NTP Server

192.168.1.1

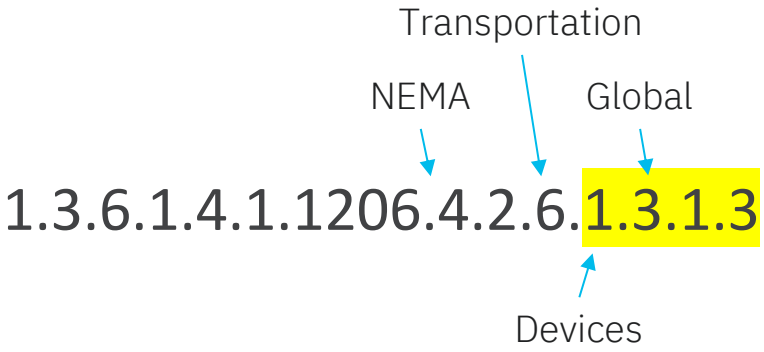
⚠ All the open ports!

Port forwarding



Also...

- Port 81 -> Hikvision Cam
- Port 82 -> Hikvision Cam
- Port 83 -> Hikvision Cam
- Port 84 -> Hikvision Cam
- Port 443 -> Ubiquiti
- Port 554 -> RTSP



NTCIP 8004

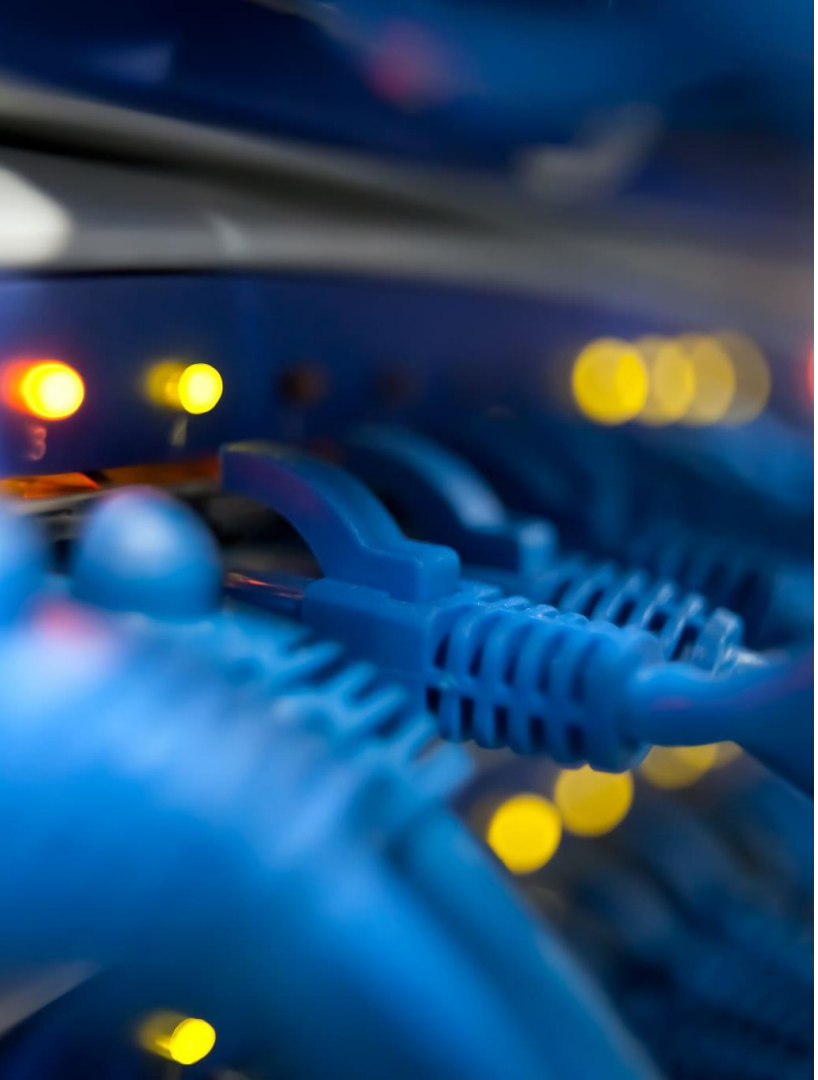
Structure and Identification of Management Information

NTCIP 1201

Global Object Definitions

2.2.3.3 Module Make Parameter

```
moduleMake OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS mandatory
DESCRIPTION
"<Definition>This object specifies the manufacturer of the
associated module. A null-string shall be transmitted if this
object has no entry.
<Object Identifier> 1.3.6.1.4.1.1206.4.2.6.1.3.1.3"
::= { moduleTableEntry 3 }
```



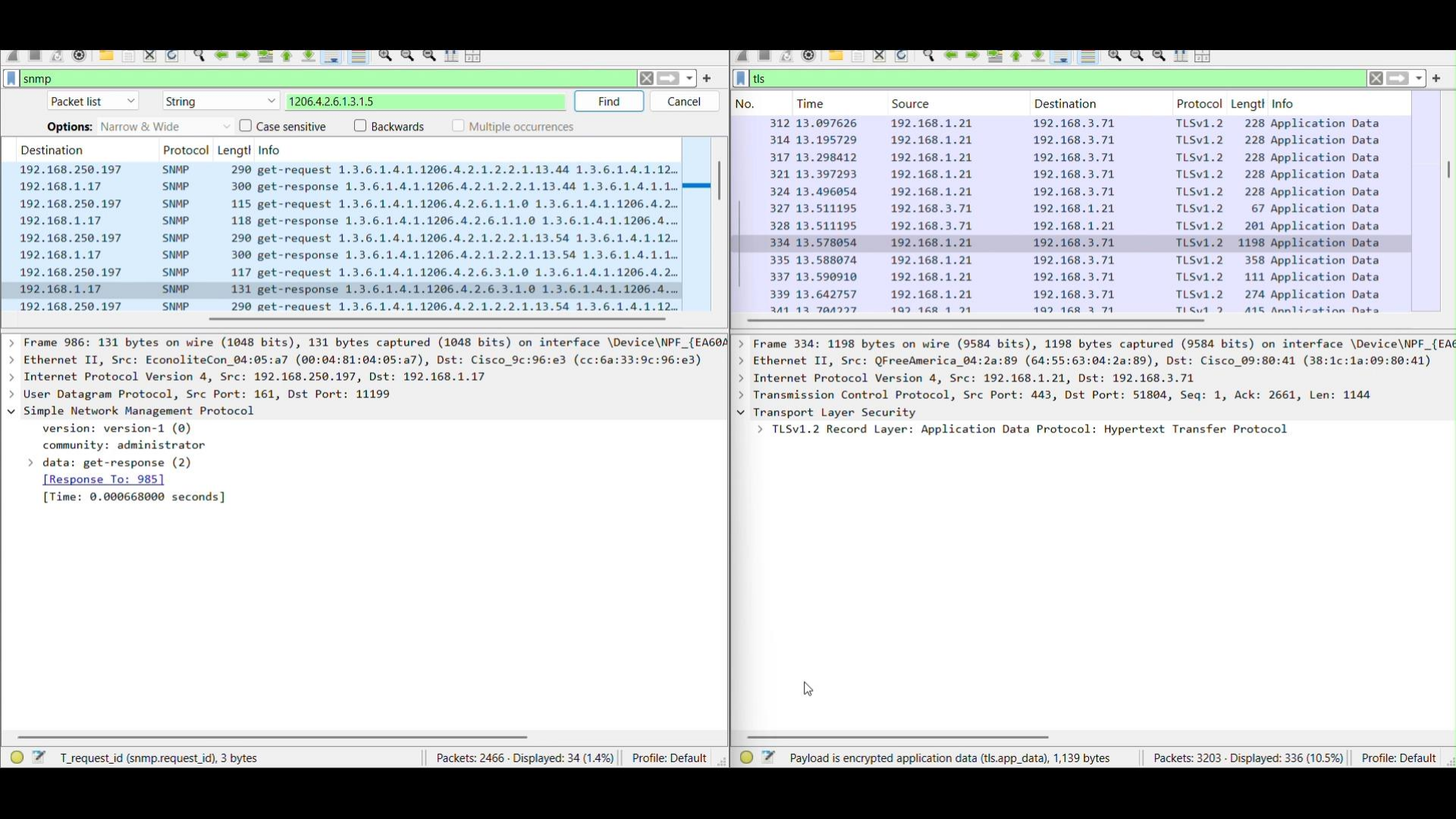
SNMP: Simple Network Management Protocol

SNMPv1 (circa 1980)

Plain text, non-encrypted, communications

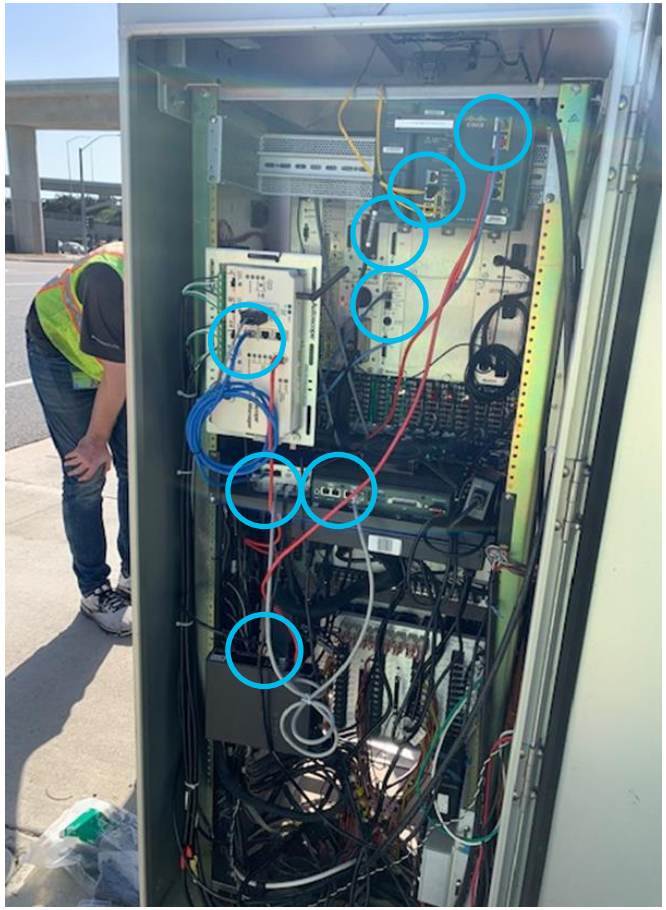
Well-known security vulnerabilities including (spoofing, message stream modification, and denial of service)

Community strings provide a primitive form of authentication management


snmp
Packet list
String
1206.4.2.6.1.3.1.5
Find
Cancel
Options: Narrow & Wide
Case sensitive
Backwards
Multiple occurrences
Destination Protocol Lengtl Info
192.168.250.197 SNMP 290 get-request 1.3.6.1.4.1.1206.4.2.1.2.2.1.13.44 1.3.6.1.4.1.12…
192.168.1.17 SNMP 300 get-response 1.3.6.1.4.1.1206.4.2.1.2.2.1.13.44 1.3.6.1.4.1.1…
192.168.250.197 SNMP 115 get-request 1.3.6.1.4.1.1206.4.2.6.1.1.0 1.3.6.1.4.1.1206.4.2…
192.168.1.17 SNMP 118 get-response 1.3.6.1.4.1.1206.4.2.6.1.1.0 1.3.6.1.4.1.1206.4.…
192.168.250.197 SNMP 290 get-request 1.3.6.1.4.1.1206.4.2.1.2.2.1.13.54 1.3.6.1.4.1.12…
192.168.1.17 SNMP 300 get-response 1.3.6.1.4.1.1206.4.2.1.2.2.1.13.54 1.3.6.1.4.1.1…
192.168.250.197 SNMP 117 get-request 1.3.6.1.4.1.1206.4.2.6.3.1.0 1.3.6.1.4.1.1206.4.2…
192.168.1.17 SNMP 131 get-response 1.3.6.1.4.1.1206.4.2.6.3.1.0 1.3.6.1.4.1.1206.4.…
192.168.250.197 SNMP 290 get-request 1.3.6.1.4.1.1206.4.2.1.2.2.1.13.54 1.3.6.1.4.1.12…
Frame 986: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits) on interface \Device\NPF_{EA60A
Ethernet II, Src: EconoliteCon_04:05:a7 (00:04:81:04:05:a7), Dst: Cisco_9c:96:e3 (cc:6a:33:9c:96:e3)
Internet Protocol Version 4, Src: 192.168.250.197, Dst: 192.168.1.17
User Datagram Protocol, Src Port: 161, Dst Port: 11199
Simple Network Management Protocol
version: version-1 (0)
community: administrator
data: get-response (2)
[Response To: 985]
[Time: 0.000668000 seconds]
T_request_id (snmp.request_id), 3 bytes
Packets: 2466 · Displayed: 34 (1.4%)
Profile: Default
tls
No. Time Source Destination Protocol Lengtl Info
312 13.097626 192.168.1.21 192.168.3.71 TLSv1.2 228 Application Data
314 13.195729 192.168.1.21 192.168.3.71 TLSv1.2 228 Application Data
317 13.298412 192.168.1.21 192.168.3.71 TLSv1.2 228 Application Data
321 13.397293 192.168.1.21 192.168.3.71 TLSv1.2 228 Application Data
324 13.496054 192.168.1.21 192.168.3.71 TLSv1.2 228 Application Data
327 13.511195 192.168.3.71 192.168.1.21 TLSv1.2 67 Application Data
328 13.511195 192.168.3.71 192.168.1.21 TLSv1.2 201 Application Data
334 13.578054 192.168.1.21 192.168.3.71 TLSv1.2 1198 Application Data
335 13.588074 192.168.1.21 192.168.3.71 TLSv1.2 358 Application Data
337 13.590910 192.168.1.21 192.168.3.71 TLSv1.2 111 Application Data
339 13.642757 192.168.1.21 192.168.3.71 TLSv1.2 274 Application Data
Frame 334: 1198 bytes on wire (9584 bits), 1198 bytes captured (9584 bits) on interface \Device\NPF_{EA6
Ethernet II, Src: QFreeAmerica_04:2a:89 (64:55:63:04:2a:89), Dst: Cisco_09:80:41 (38:1c:1a:09:80:41)
Internet Protocol Version 4, Src: 192.168.1.21, Dst: 192.168.3.71
Transmission Control Protocol, Src Port: 443, Dst Port: 51804, Seq: 1, Ack: 2661, Len: 1144
Transport Layer Security
TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
Payload is encrypted application data (tls.app_data), 1,139 bytes
Packets: 3203 · Displayed: 336 (10.5%)
Profile: Default

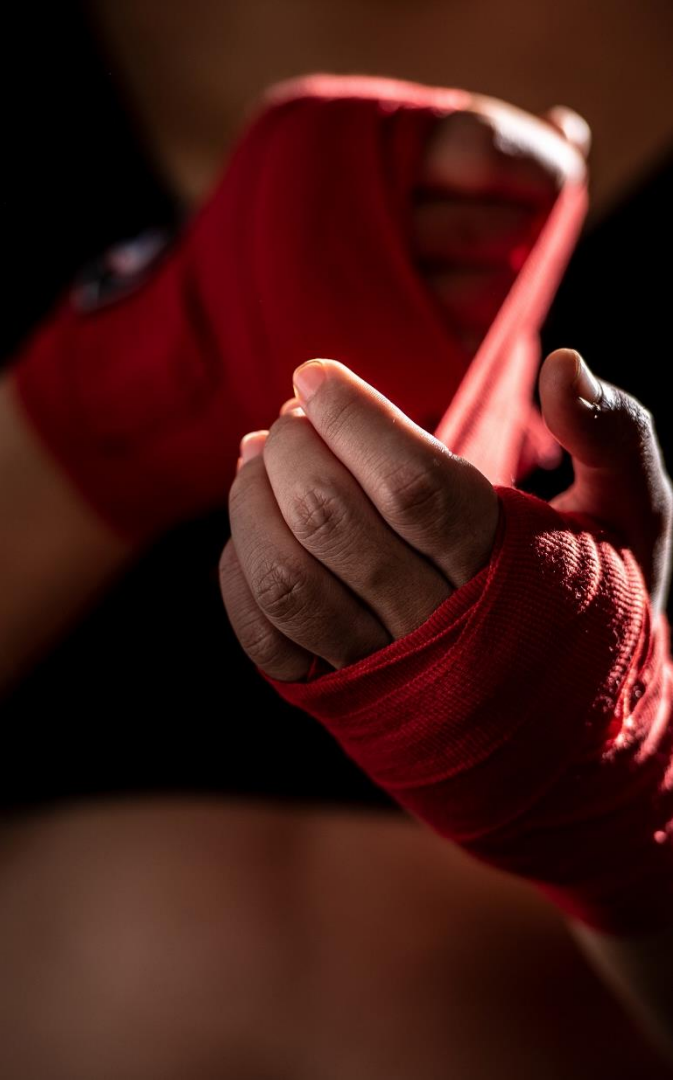
Once you are in... oof!

= attack surfaces



Best practices

- Cybersecurity begins with physical security
- Know what is on your network!
- Avoid the three epic fails in your network schema
- Upgrade your systems with security in mind
  - Authentication
  - Encryption
- Deploy network tools that monitor and control authorized communication



SOC it 2 me

System and Organization Controls (SOC)

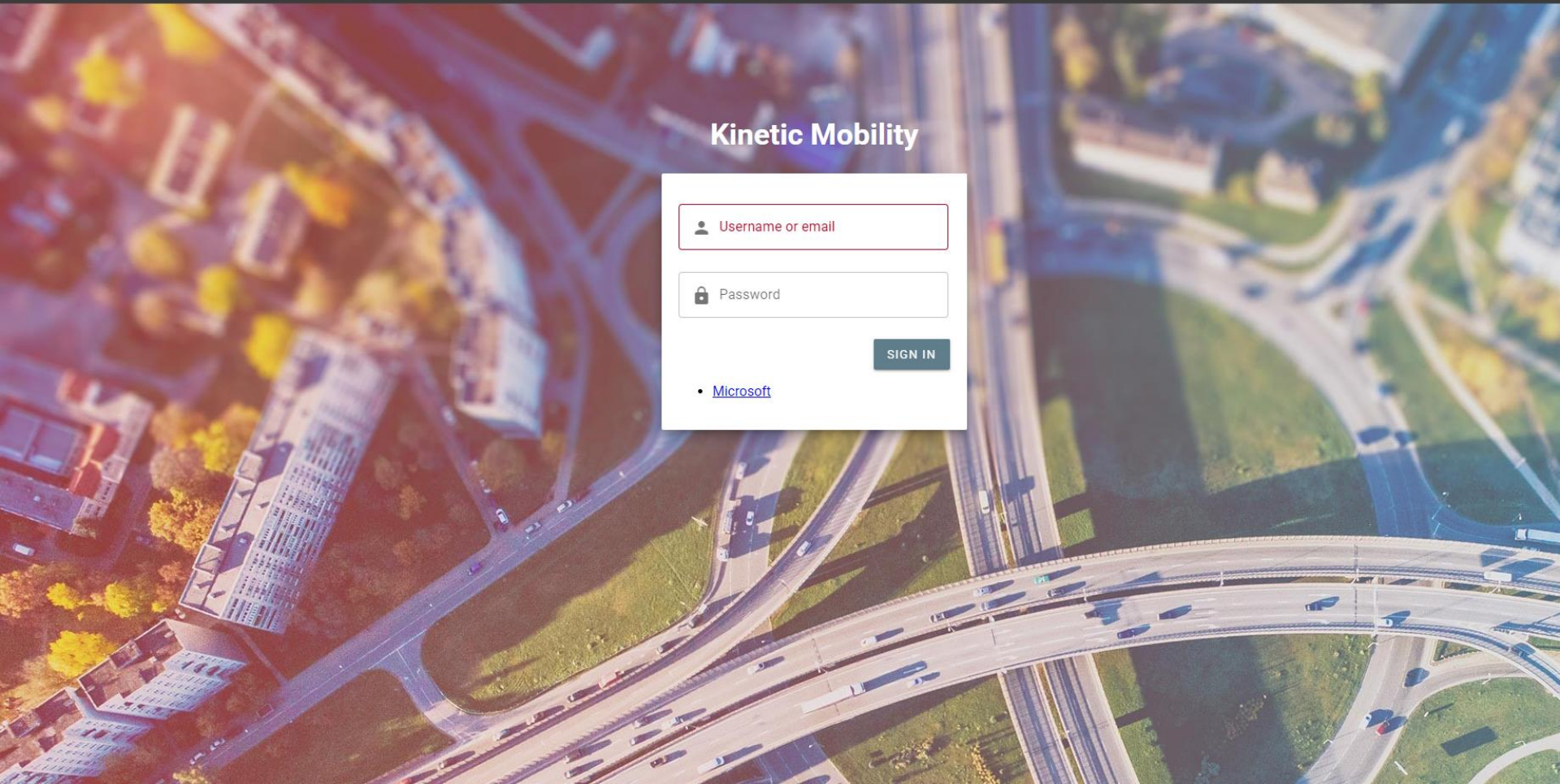
Defined by the American Institute of Certified Public Accountants (AICPA).

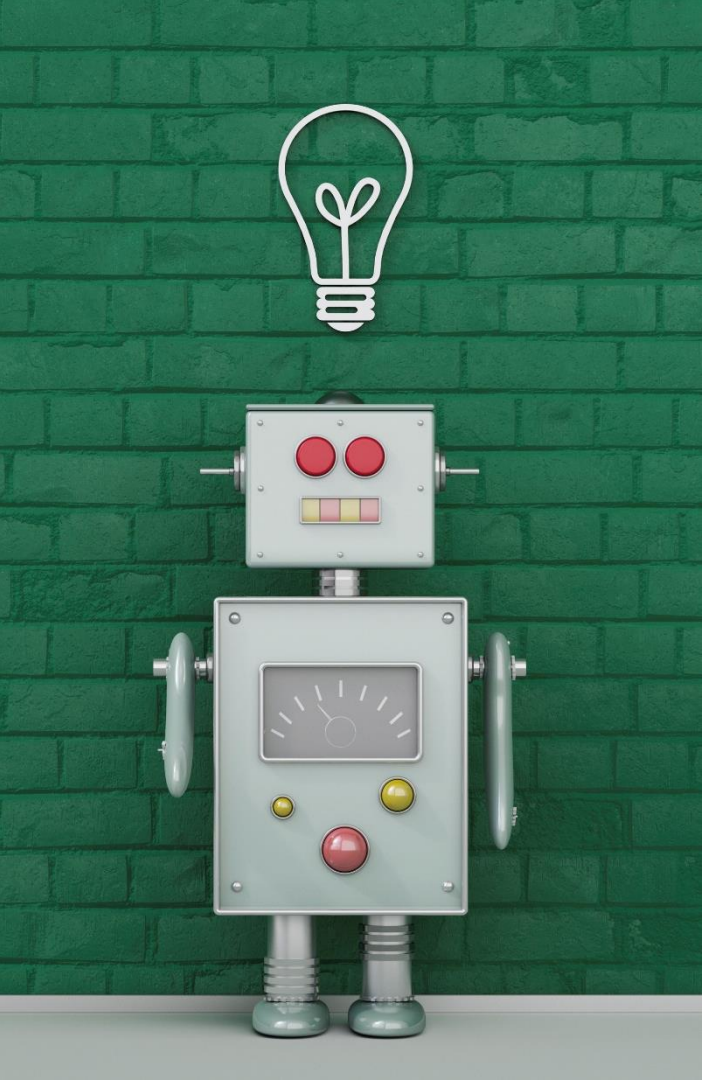
- SOC 1 is about financials
- SOC 2 is about security

SOC 2

1. Security
2. Availability
3. Confidentiality
4. Processing integrity
5. Privacy

www.aicpa.org/soc4so


Kinetic Mobility
Username or email
Password
SIGN IN
Microsoft



Tools and automated scans

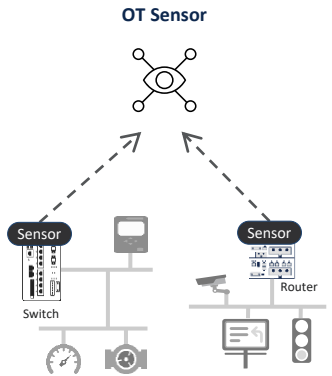
Vulnerability Scanning
Scan Linux host for missing patches. Repositories for security vulnerabilities in component software.

Penetration Testing
Simulated attack performed to evaluate system security.

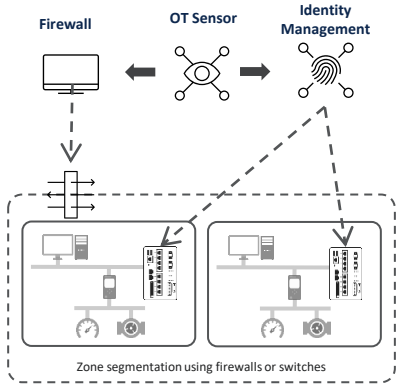
End Point Security
Intrusion detection systems (IDS) and intrusion prevention systems (IPS).

Journey to secure critical infrastructure

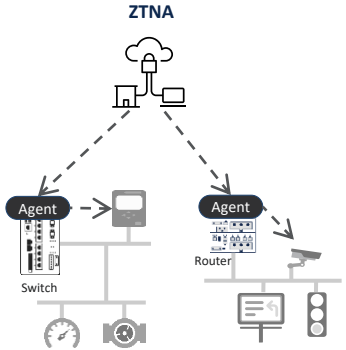
1 Asset Visibility and Security Posture



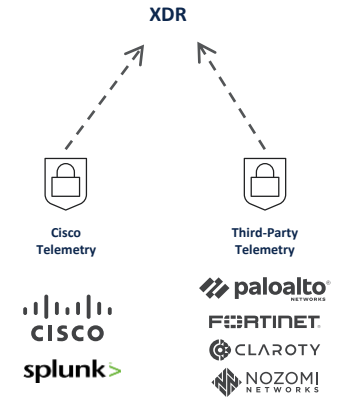
2 Zero Trust Segmentation



3 Zero Trust Network Access (ZTNA)



4 Cross-Domain Detection, Investigation & Response

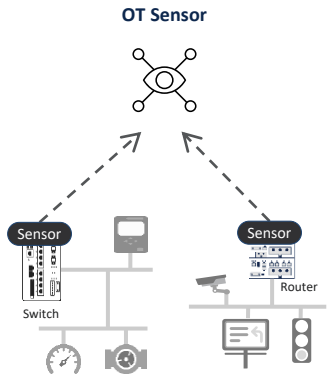


Threat Intelligence + Incident Response

Journey to secure critical infrastructure

1

Asset Visibility
and Security Posture

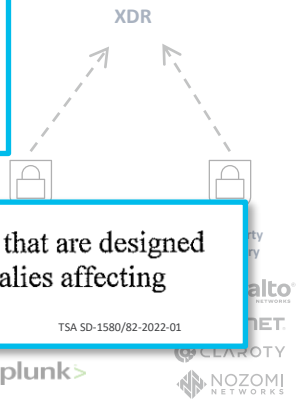


2

3

4

oss-Domain Detection,
vestigation & Response



Most teams do not have accurate asset Inventory

They are blind to what their assets are communicating with

D. Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and correct anomalies affecting Critical Cyber Systems. These measures must include:

TSA SD-1580/82-2022-01

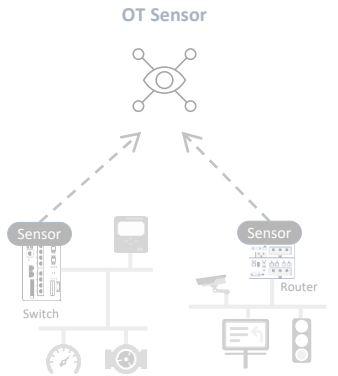
Threat Intelligence + Incident Response

TSA Security Directive TSA SD-1580/82-2022-01 Rail Cybersecurity Mitigation Actions and Testing

Journey to secure critical infrastructure

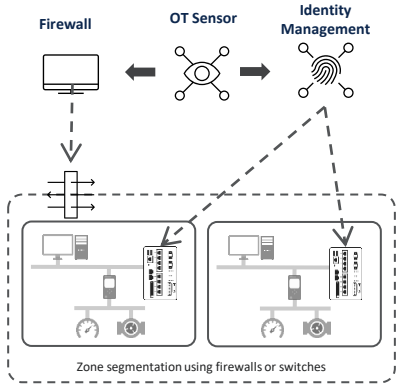
1

Asset Visibility and Security Posture



2

Zero Trust Segmentation



Threat Intelligence

B. Implement network segmentation policies and controls designed to prevent operational disruption to the Operational Technology system if the Information Technology system is compromised or vice-versa. As applied to Critical Cyber Systems, these policies and controls must include:

1. A list and description of —

   a. Information Technology and Operational Technology system interdependencies;

   b. All external connections to the Information Technology and Operational Technology system;

   c. Zone boundaries, including a description of how Information Technology and Operational Technology systems are defined and organized into logical zones based on criticality, consequence, and operational necessity; and

   d. Policies to ensure Information Technology and Operational Technology system services transit the other only when necessary for validated business or operational purposes.

2. An identification and description of measures for securing and defending zone boundaries, that includes security controls—

   a. To prevent unauthorized communications between zones; and

   b. To prohibit Operational Technology system services from traversing the Information Technology system, and vice-versa, unless the content is encrypted or, if not technologically feasible, otherwise secured and protected to ensure integrity and prevent corruption or compromise while the content is in transit.

TSA SD-1580/82-2022-01

Journey to secure critical infrastructure

1

Asset Visibility

2

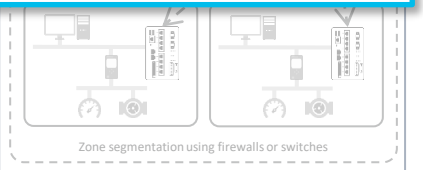
Zero Trust

C. Implement access control measures, including those for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems. These measures must incorporate the following policies, procedures, and controls:

TSA SD-1580/82-2022-01

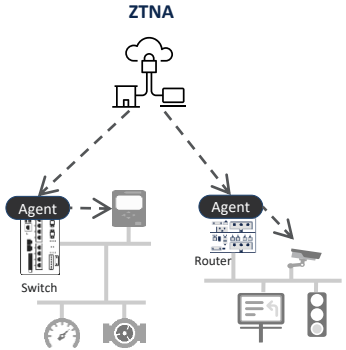
3. Policies and procedures to manage access rights based on the principles of least privilege and separation of duties. Where not technically feasible to apply these principles, the policies and procedures must describe the compensating controls that the Owner/Operator will apply.

TSA SD-1580/82-2022-01



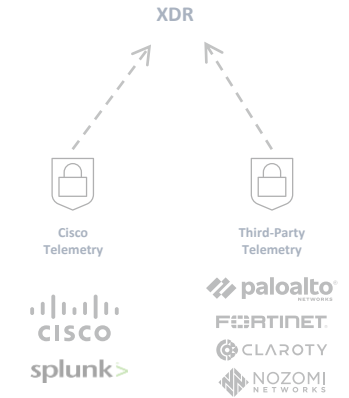
3

Zero Trust Network Access (ZTNA)



4

Cross-Domain Detection, Investigation & Response



Threat Intelligence + Incident Response

Journey to secure critical infrastructure

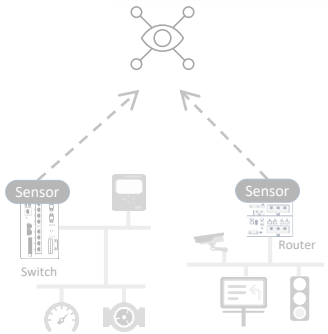
1

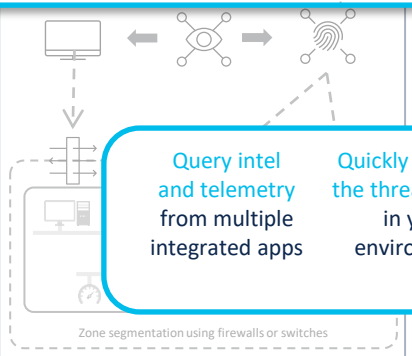
2

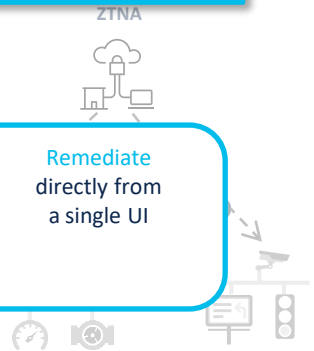
3

4

> 4. Mitigation measures or manual controls to ensure industrial control systems can be isolated when a cybersecurity incident in the Information Technology system creates risk to the safety and reliability of the Operational Technology system.[11]
>
> TSA SD-1580/82-2022-01





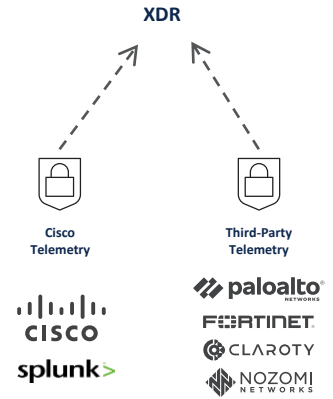


Query intel and telemetry from multiple integrated apps

Quickly visualize the threat impact in your environment

Remediate directly from a single UI

Cross-Domain Detection, Investigation & Response



Threat Intelligence + Incident Response

Thank You!

Contact us

Alex Clark

Industry Acceleration - IIOT
Transportation
Cisco Systems
ayclark@cisco.com
(617) 510-9878

Mike McIntee

Senior Vice President Sales
Q-Free
mike.mcintee@q-free.com
(916) 799-8796