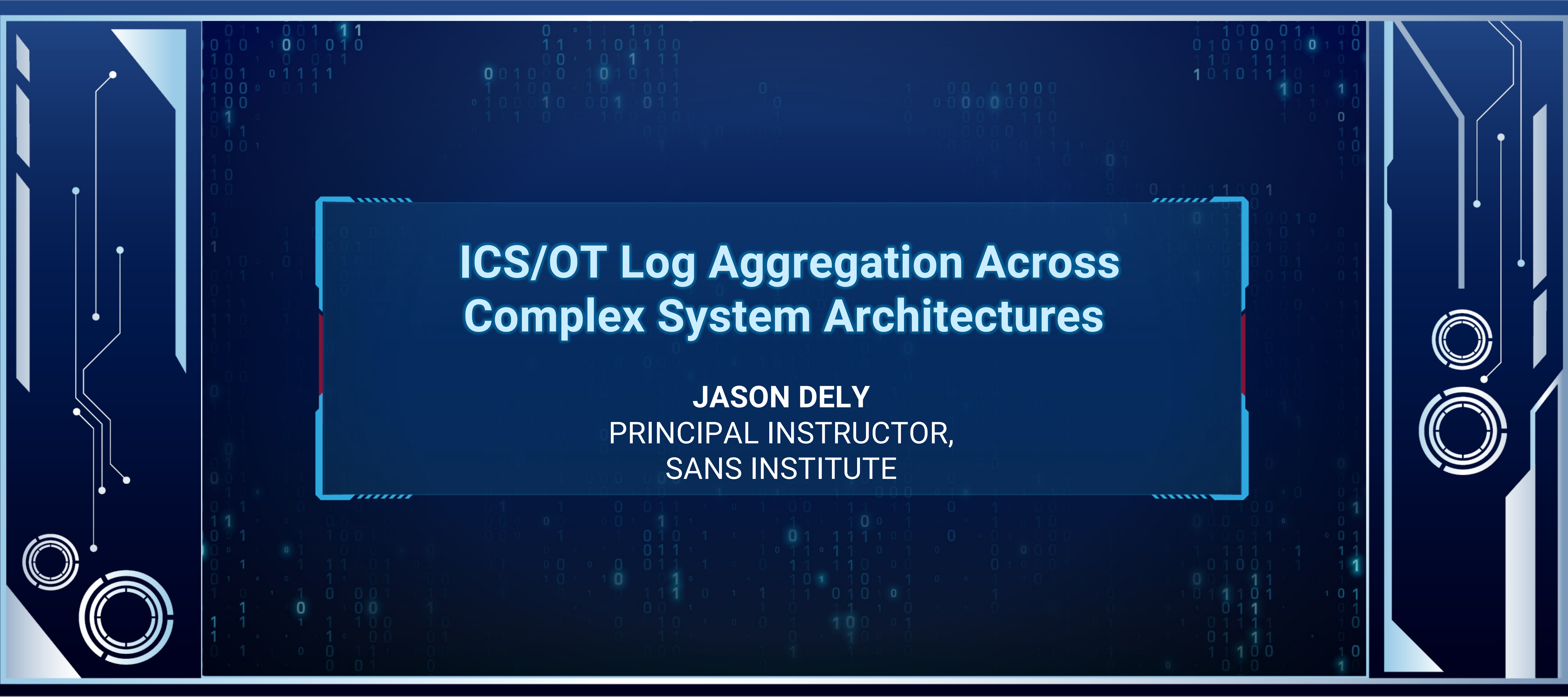




ICS/OT Log Aggregation Across Complex System Architectures

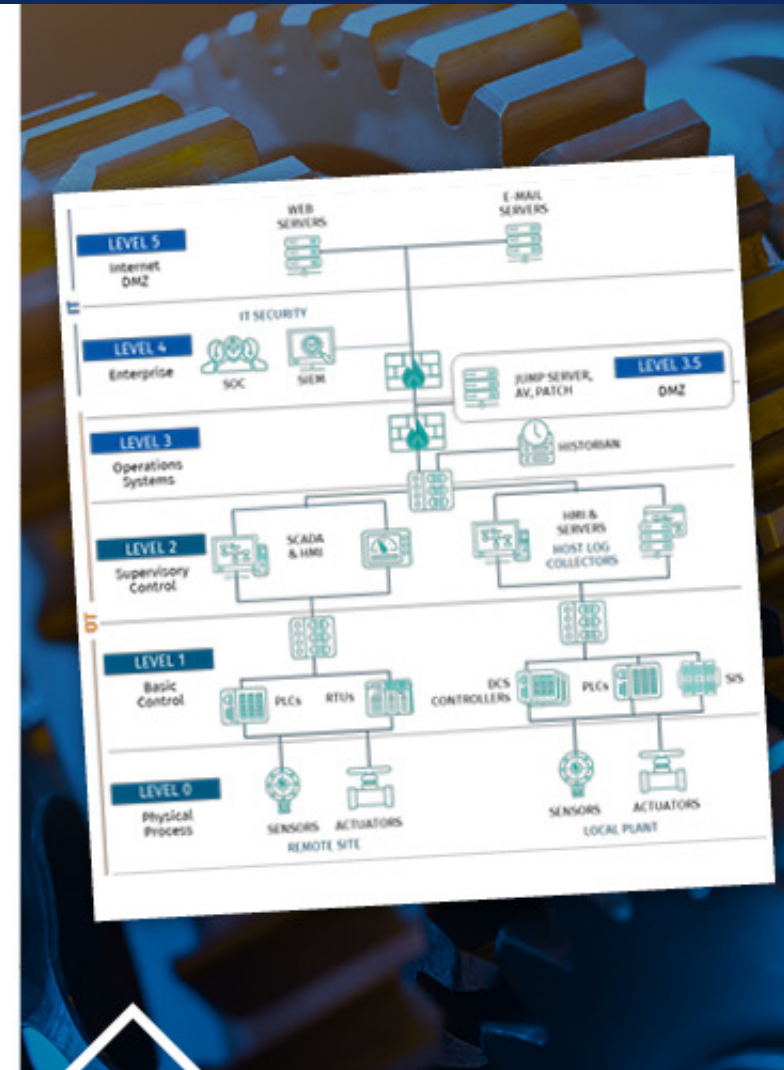
JASON DELY
PRINCIPAL INSTRUCTOR,
SANS INSTITUTE

Five Critical Controls for ICS/OT Cybersecurity



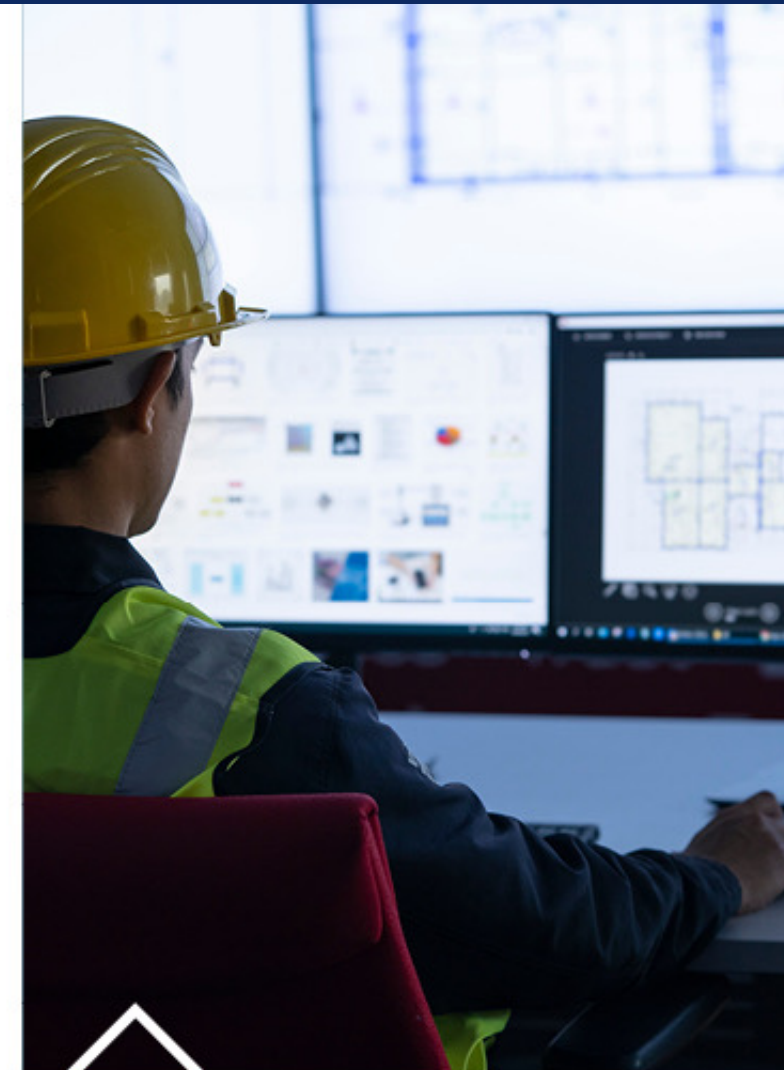
ICS INCIDENT RESPONSE

Operations informed IR plan with focused system integrity and recovery capabilities during an attack. Exercises designed to reinforce risk scenarios and use cases tailored to the ICS environment.



DEFENSIBLE ARCHITECTURE

Architectures that support visibility, log collection, asset identification, segmentation, Industrial DMZ's, process communication enforcement.



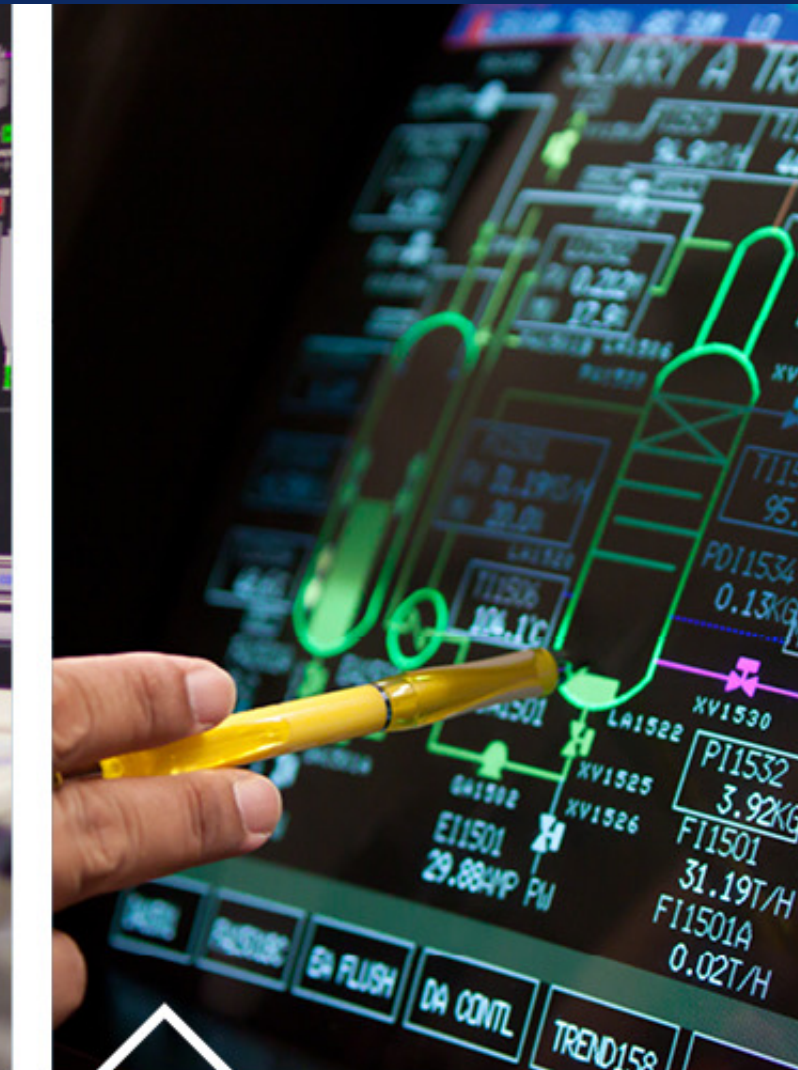
ICS NETWORK VISIBILITY AND MONITORING

Continuous network security monitoring of the ICS environment with protocol aware toolsets and system of systems interaction analysis capabilities used to inform operations of potential risks to control.



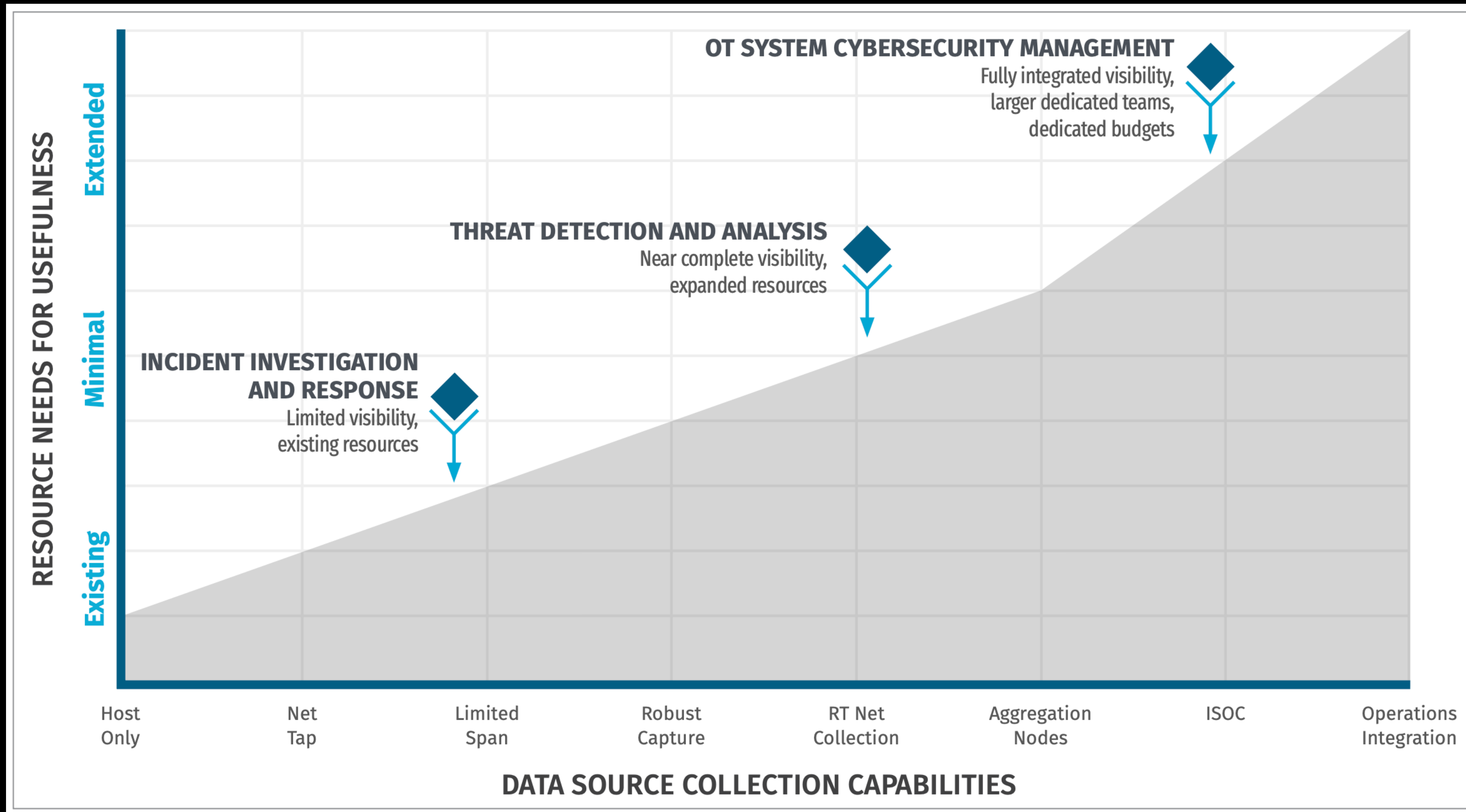
SECURE REMOTE ACCESS

Identification and inventory of all remote access points and allowed destination environments, on demand access and MFA where possible, jump host environments to provide control and monitor points within secure segment.



RISK BASED VULNERABILITY MANAGEMENT

Understanding of cyber digital controls in place and device operating conditions that aid in risk-based vulnerability management decisions to patch for the vulnerability, mitigate the impact, or monitor for possible exploitation.

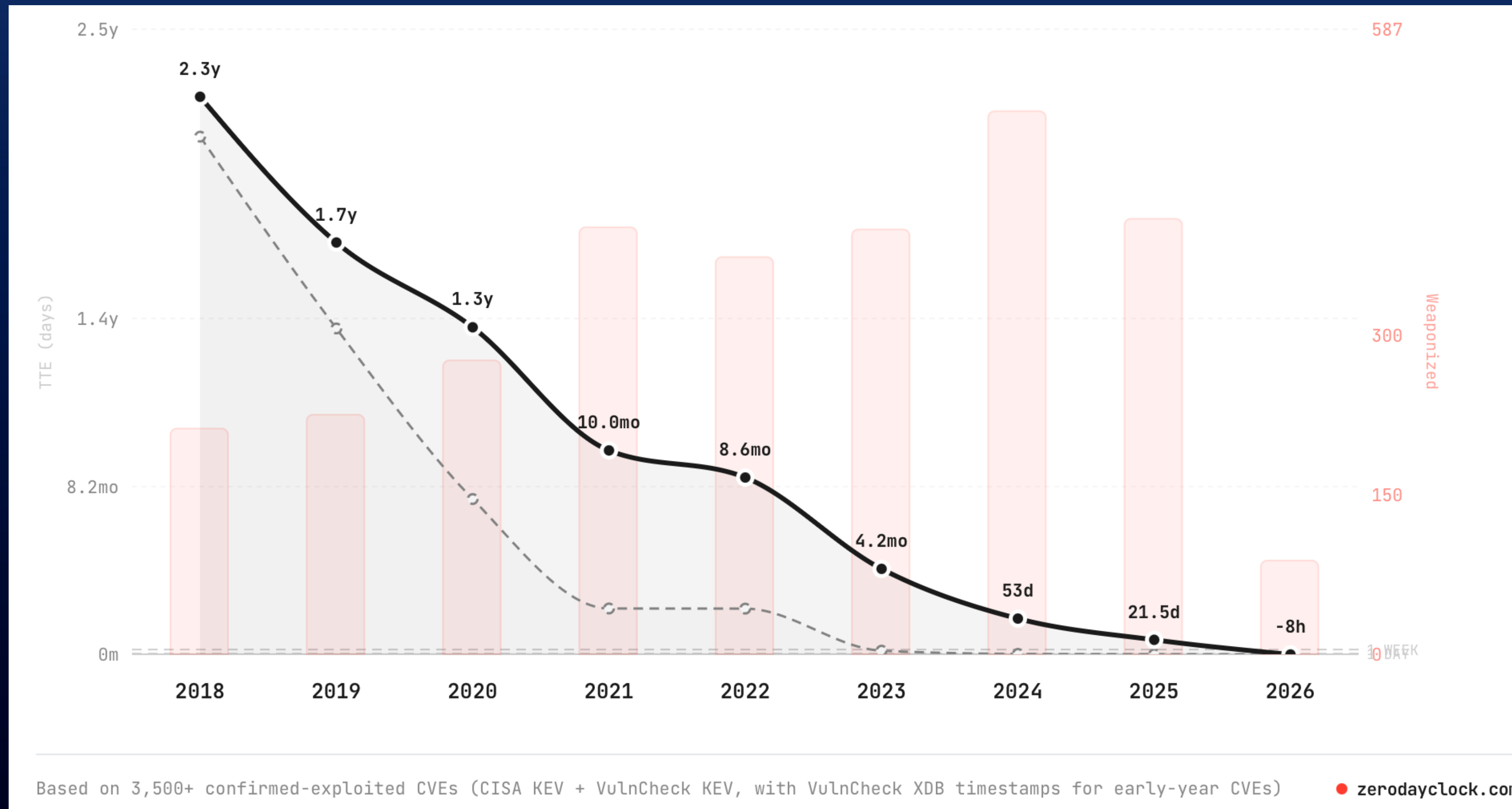


Why Visibility and Monitoring?

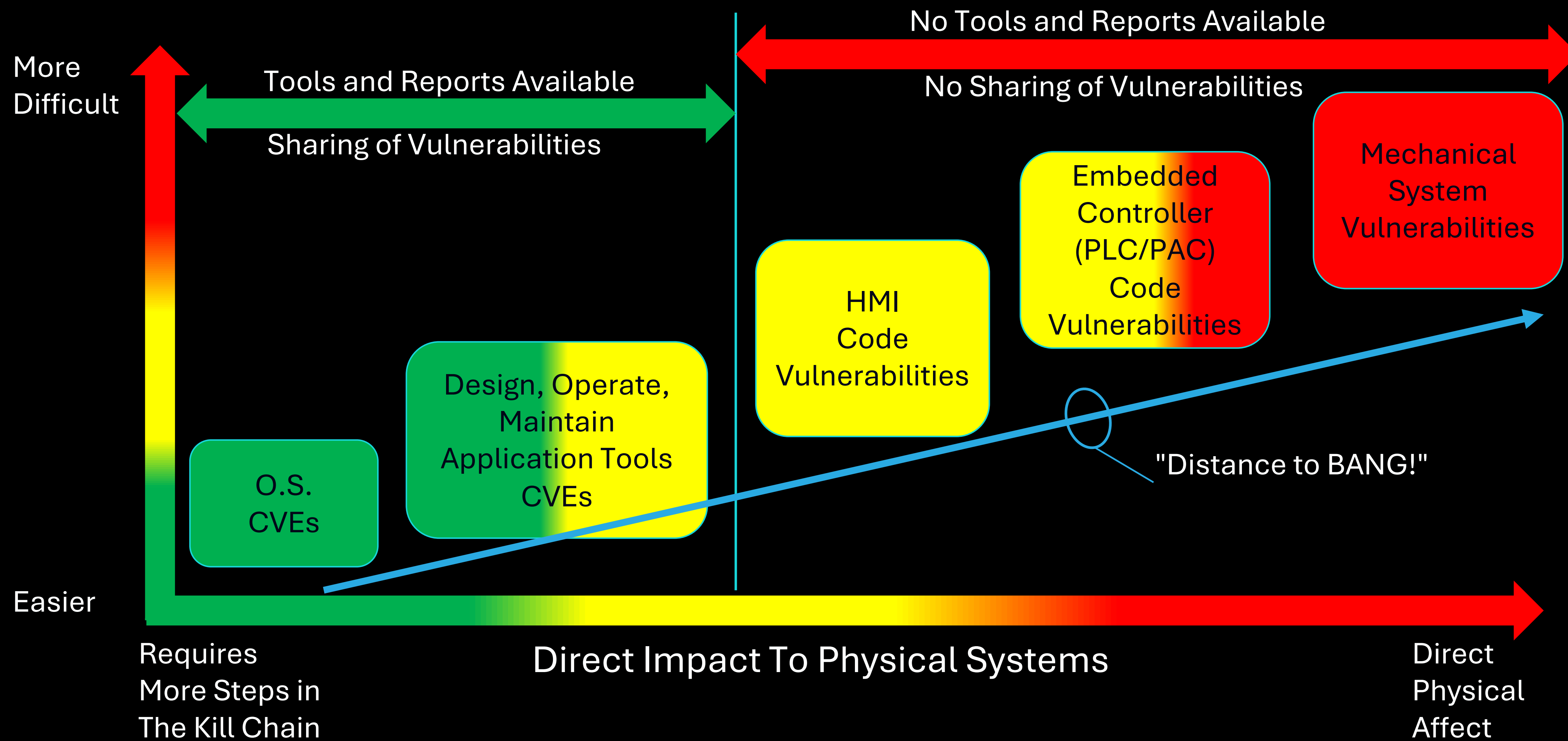
- **Compliance and Regulatory Requirements**
 - Industry Standards Alignment
 - Regulatory Compliance
- **Security Monitoring and Threat Detection**
 - Intrusion Detection
 - Incident Response
 - Threat Hunting
- **Operational Monitoring and Troubleshooting**
 - System Performance
 - Process Upsets
 - Predictive Maintenance
 - Operational Traceability
 - Management of Change



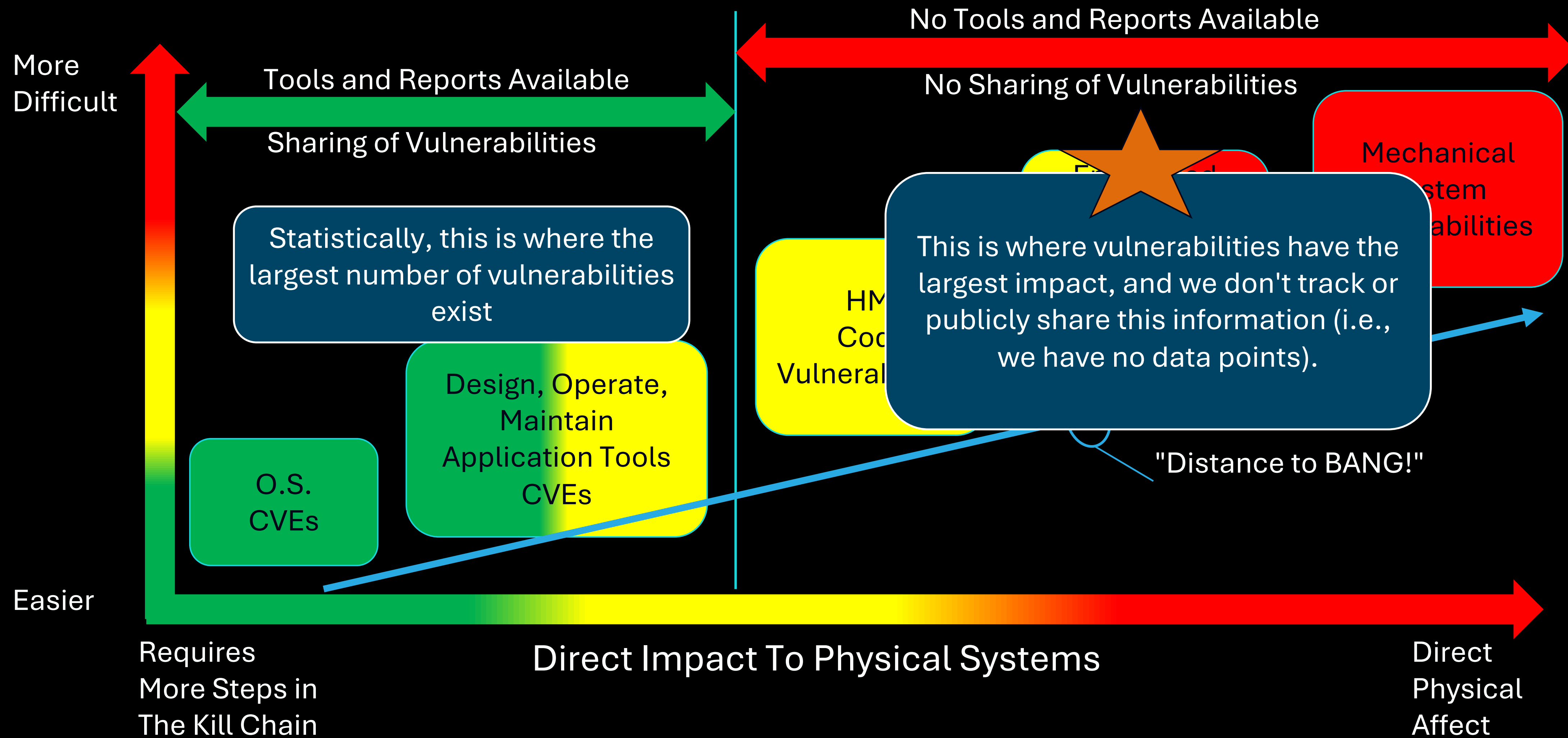
Zero Day Clock: From Vulnerability to Exploitation



CVEs and ICS Vulnerabilities



CVEs and ICS Vulnerabilities



Challenges in Log Aggregation

- **Servers**
 - Vendors, OEM's may not allow agents
 - Proprietary logging and collection methods
- **Network**
 - Lacking or inaccessible log support
 - Lacking port mirror functionality
- **ICS Hardware**
 - No log generation
 - Log accessibility
- **ICS Environment**
 - Scale of the environment
 - Control Panel Space
 - Accessibility - Routing, Path, Bandwidth
- **Budget and Resource Limitation**



Network Monitoring Misconceptions

MISCONCEPTIONS



Image Ref: ChatGPT Image Creator 5.1



You need to have a complete asset inventory list.



You only need to capture logs from the endpoints.



OT is too big, only AI can solve the log analysis problem.



The network needs to be overhauled to support monitoring.



You need to monitor 100% of the network

Develop a Plan

Goals and Objectives

- **What problem are we trying to solve?**
- **Support ICS Operations**
 - ☐ Improve system resilience & planning
 - ☐ Improve root cause analysis
 - ☐ Minimize unplanned downtime events
- **Support ICS Security Operations**
 - ☐ Comprehensive and contextual view of events
 - ☐ Network security visibility and threat hunt activities
 - ☐ ICS incident response activities



Visibility and Monitoring Program



Requirements

Threat Model
Crown Jewel Analysis
Attack Path Identification
Asset Identification
Collection Management
Framework



Design

Visibility and Monitoring
Architecture
Network Sensor Placement
Host and Device Collection
Vendor and Operations
Approval
Collection Methods
Analysis Methods
Tool Selection



Implementation

Systems Install
Sensor Installs
End Point Adoption
Network and Application
Log Baselines
Network Flow Analysis
Context and Alert Creation
Log Protection



Maintain

Maintain Log, Collector
and Tool Configurations
Verify Log Presence
End Point Alert Testing
Network Alert Testing
Asset and Attack Path
Deviations
Notification and Response
Workflows

Requirements

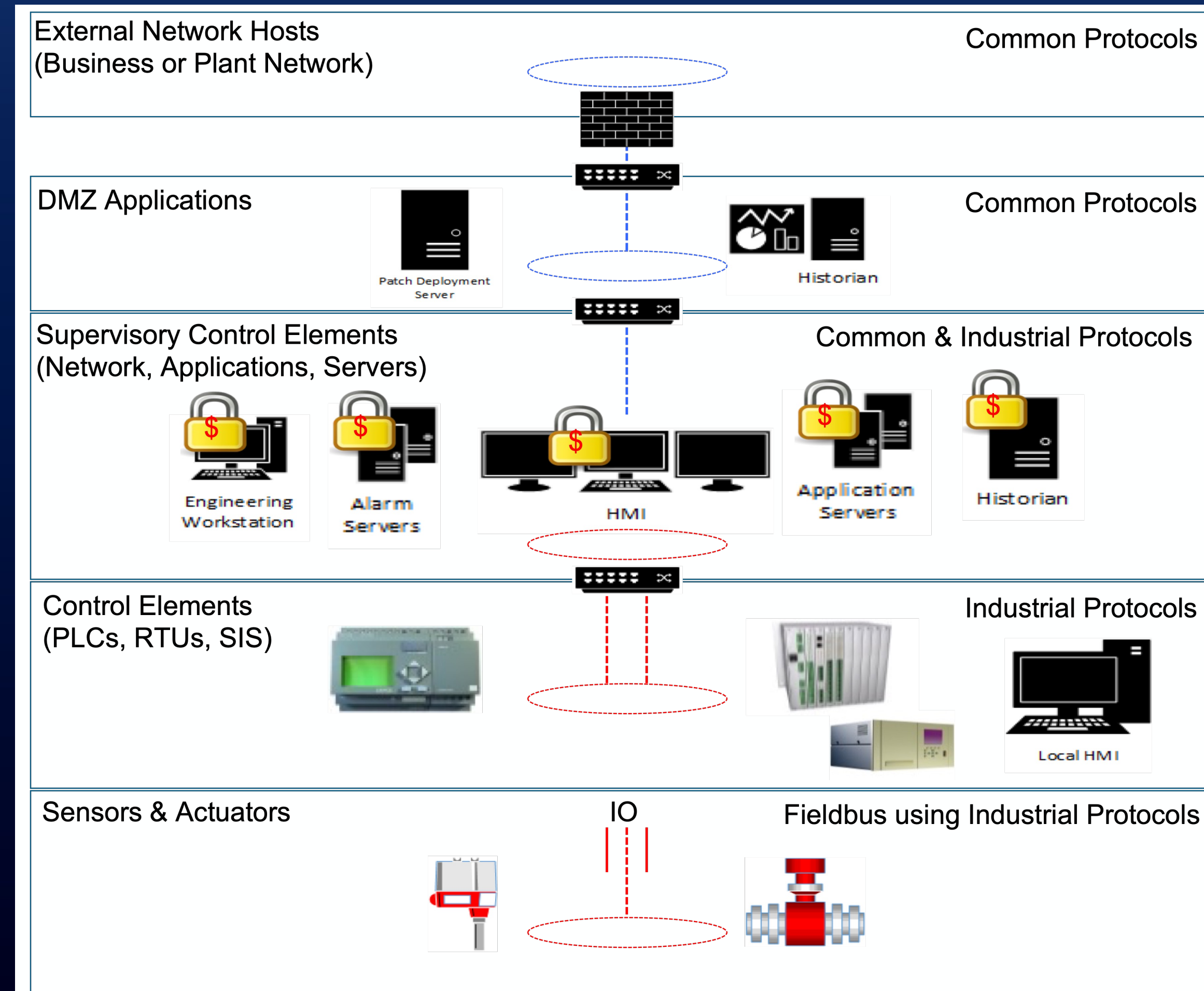
ICS Opportunistic Malware:

- Impactful malware
 - Ransomware
- Non-impactful malware
 - Incidental malware

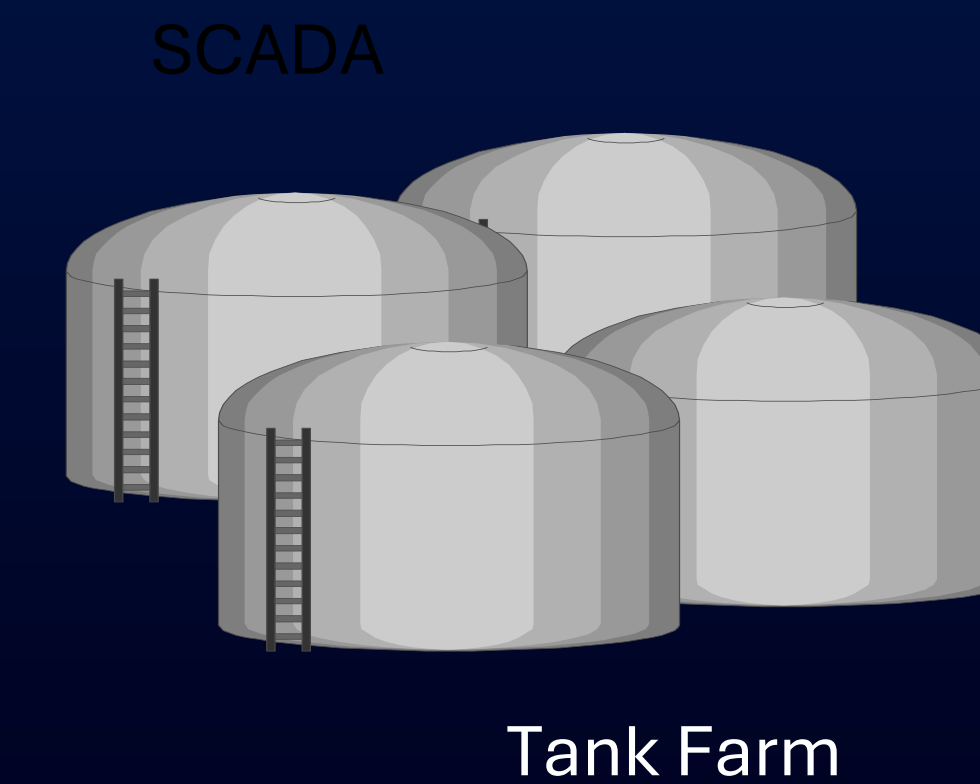
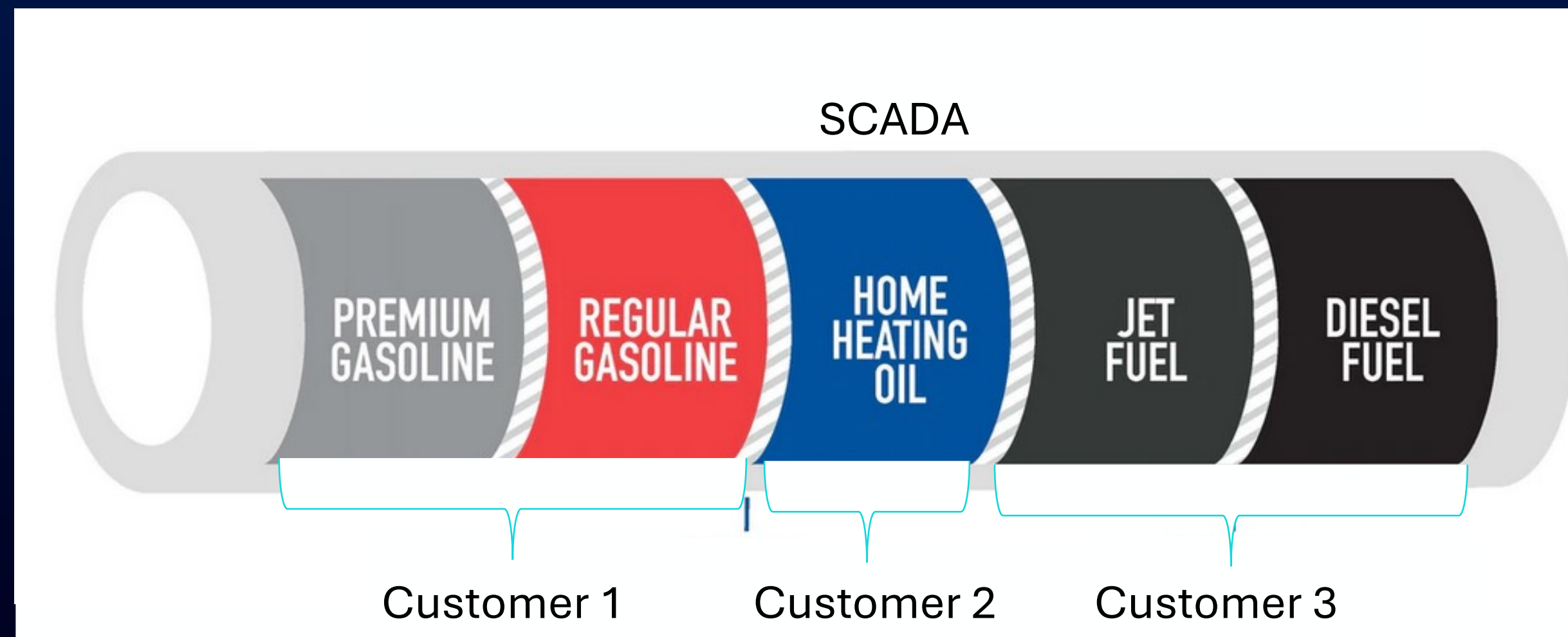


OT Assets – Ransomware Low-Hanging Fruit

- Currently, ransomware targets computer systems, not embedded systems like PLCs
- Effects include but are not limited to:
 - No access to design tools on engineering workstations
 - Loss of process visibility (HMI) and alarm servers
 - Loss of historical data
 - Loss of quality assurance systems
 - Loss of analytics tools
 - Loss of SCADA functions
 - Inability to authenticate users

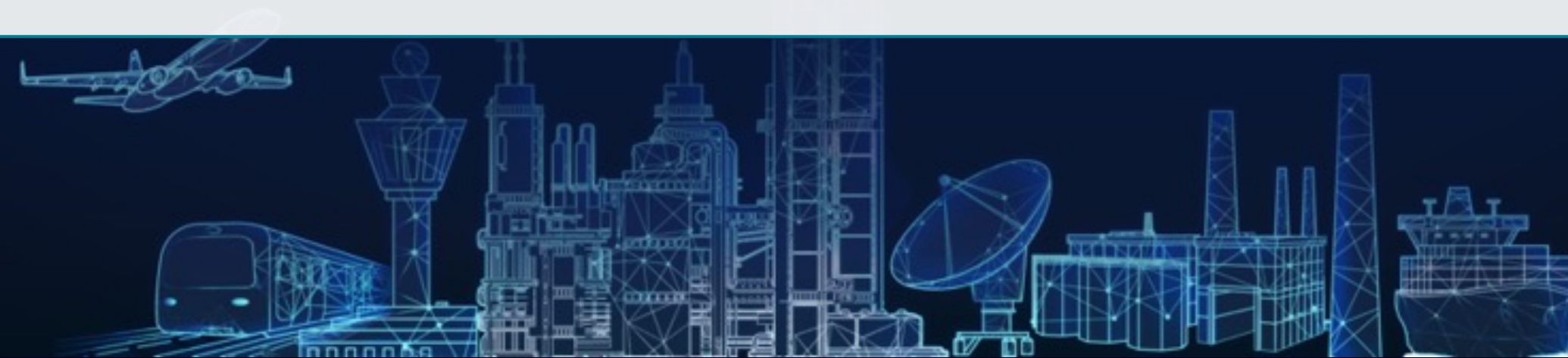


IT and OT Asset Critical Interdependencies



Targeted ICS Malware:

- ICS Espionage
 - HAVEX
- ICS Disruptive
 - CrashOverride, Trisis
- ICS Destructive
 - Stuxnet



Malware Discovery Associated with Electric Outages

Russia has developed a cyberweapon that can disrupt power grids, according to new research



The malware, dubbed CrashOverride, is just the second instance of malware specifically tailored to disrupt or destroy industrial control systems, according to new research. The Washington Post's Ellen Nakashima explains. (The Washington Post)

By Ellen Nakashima June 12 at 4:20 PM

Hackers allied with the Russian government have devised a cyberweapon that has the potential to be the most disruptive yet against electric systems that Americans depend on for daily life, according to U.S. researchers.

ANDY GREENBERG SECURITY 06.13.17 12:41 PM

'CRASH OVERRIDE': THE MALWARE THAT TOOK DOWN A POWER GRID

Cyber firms warn of malware that could cause power outages



CRASH OVERRIDE

Analysis of the Threat
to Electric Grid Operations

Case Study: XENOTIME

- **Industry targets**
 - Electric, oil, and gas
- **Goals**
 - Penetrate control system environments
 - Deliver tailored malware targeting specific SIS platforms
 - Cause significant damage or loss of human life
- **Tactics, targets, and techniques**
 - Initial access reconnaissance: External logon portals, VPN concentrators, hosts with SMB (TCP/445) exposed externally
 - Lateral movement using LOTL and common pentest tools like NetExec: Valid accounts
 - Execute ICS attack with TRISIS custom malware



XENOTIME
SINCE 2014

ADVERSARY:
+ Unique tool development

CAPABILITIES:
+ TRISIS
+ Custom credential harvesting
+ Off-the-shelf tools

VICTIM:
+ Oil & Gas, Electric Utilities
+ Middle East, North America

INFRASTRUCTURE:
+ Virtual Private Server and compromised, legitimate infrastructure
+ European web hosting providers
+ Asian shipping company

ICS IMPACT:
+ Demonstrated capability to execute disruptive ICS attack, such as the 2017 TRISIS incident

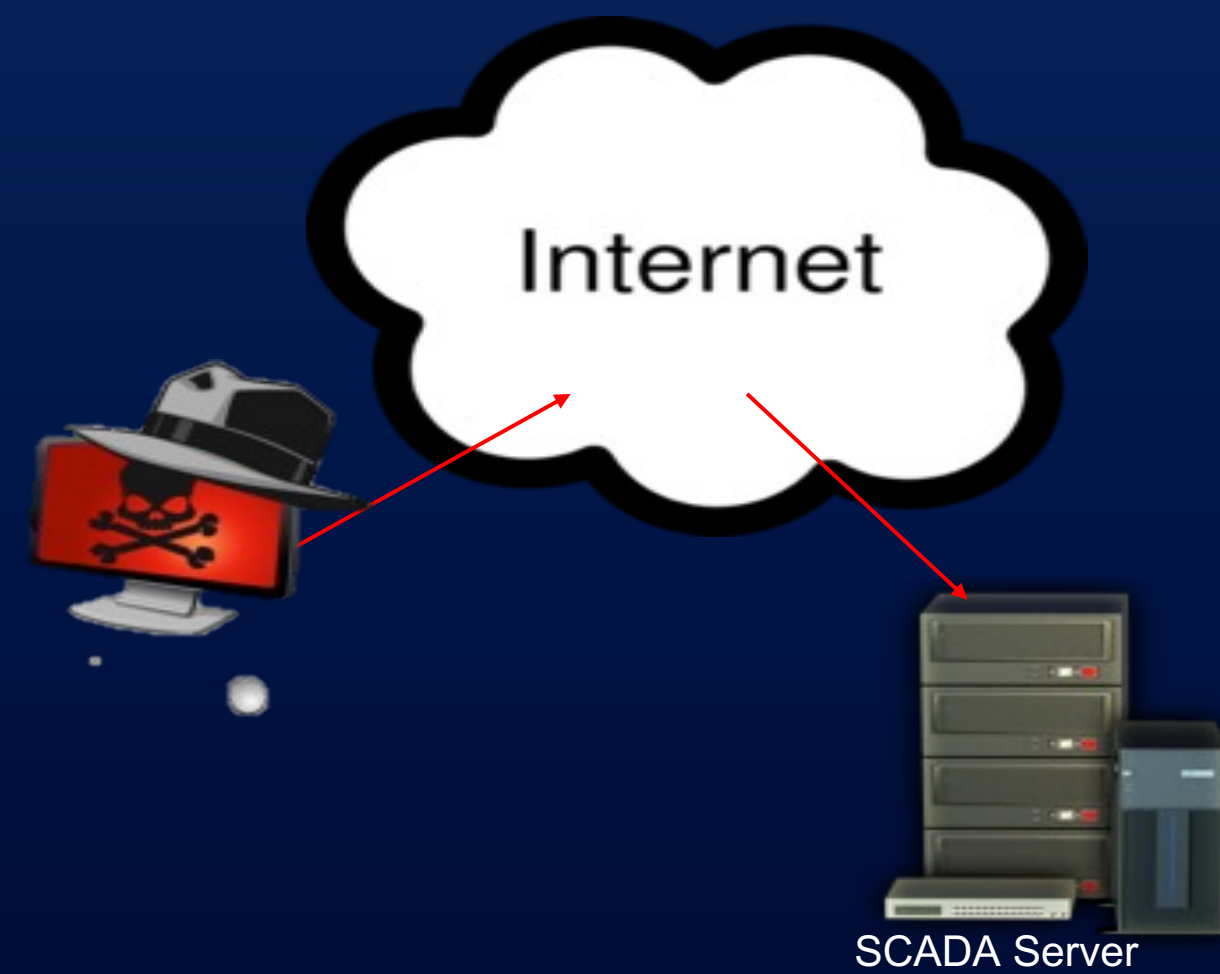


Non-malware ICS Tactics:

- VPN Credential Theft
- ICS Supply Chain Abuse
- ICS Espionage
- ICS Living-off-the-Land
- Attack Amplification



ICS Hijack, Damage and Disruption



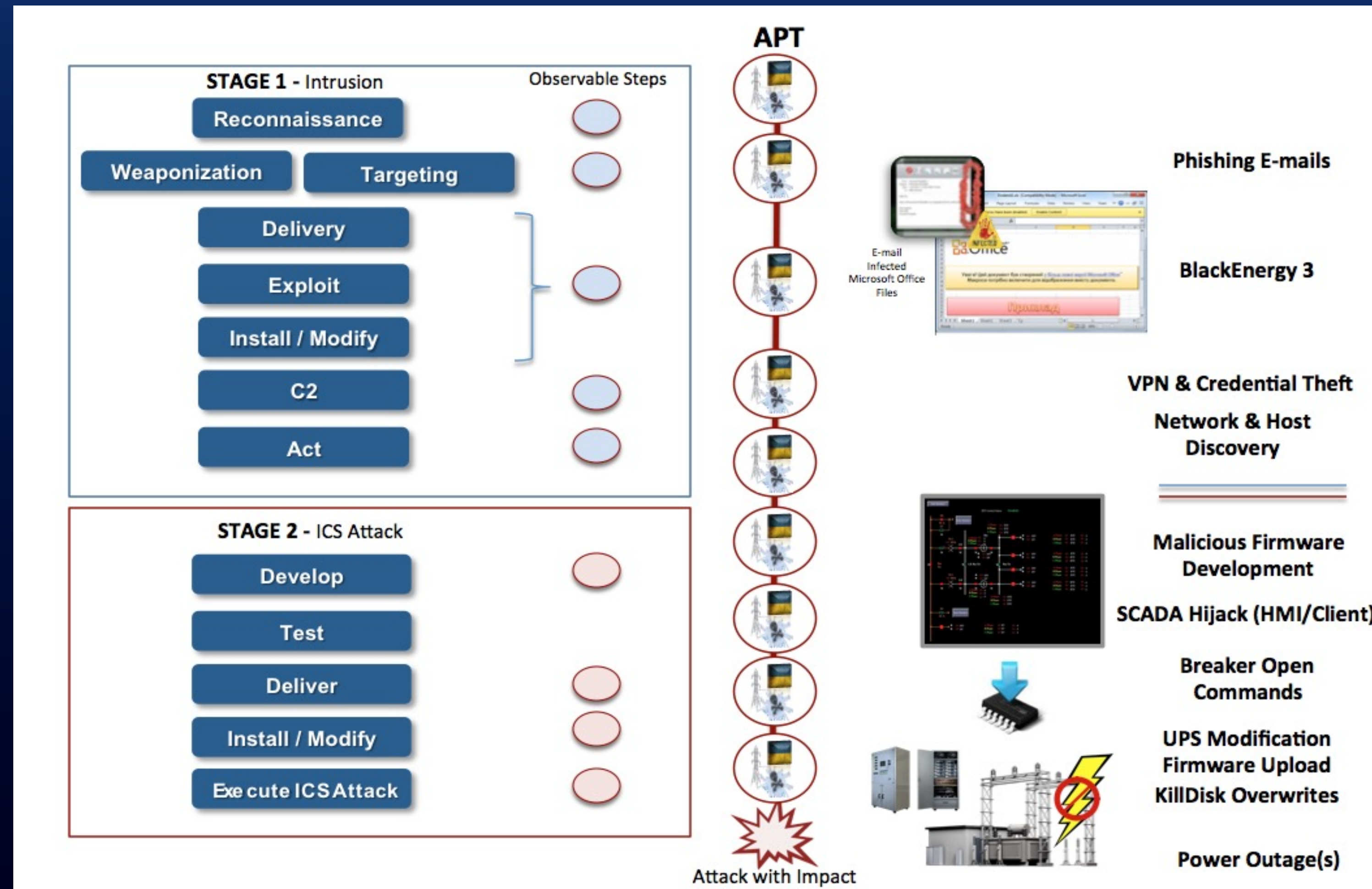
Rogue Client
Remote SCADA Client Software



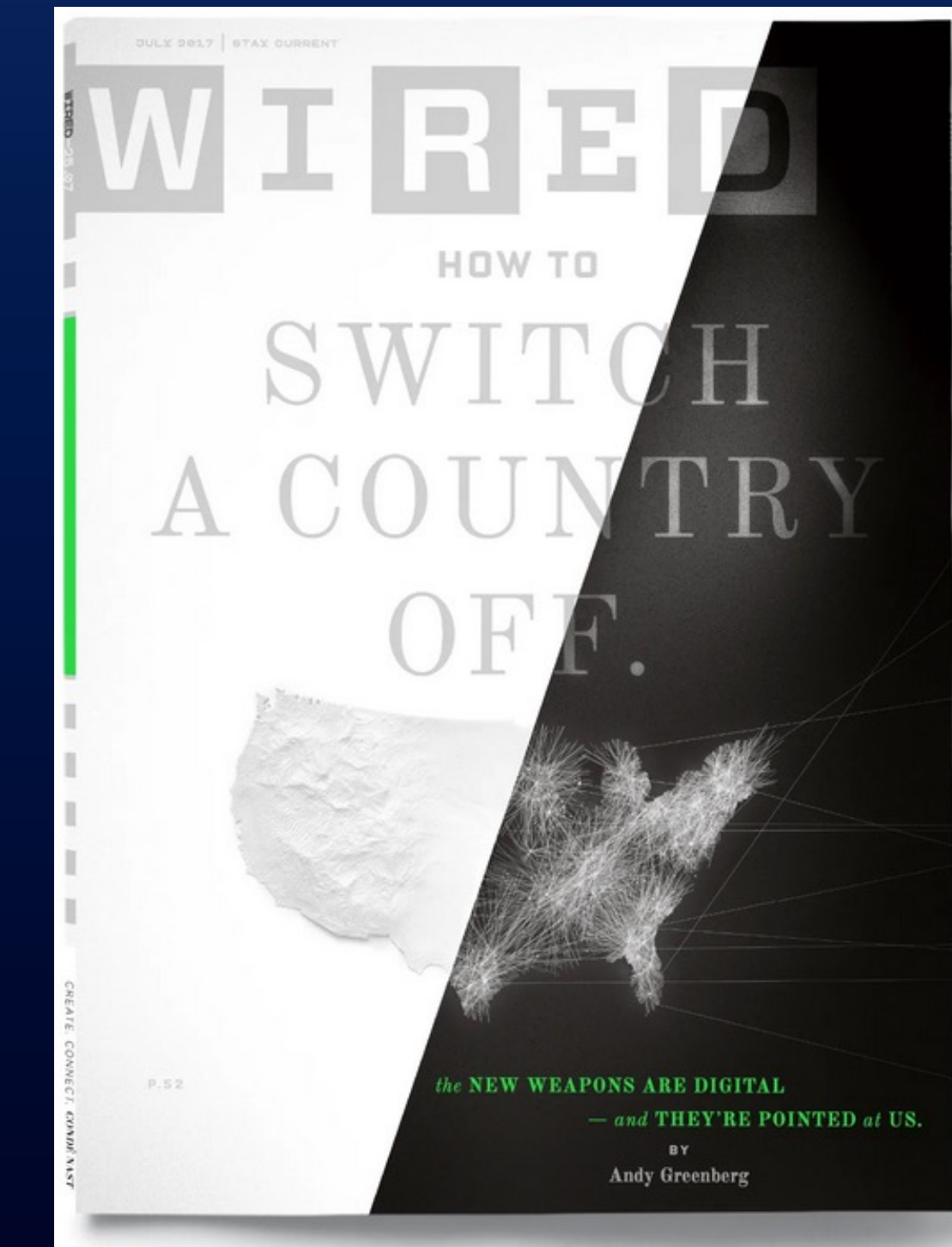
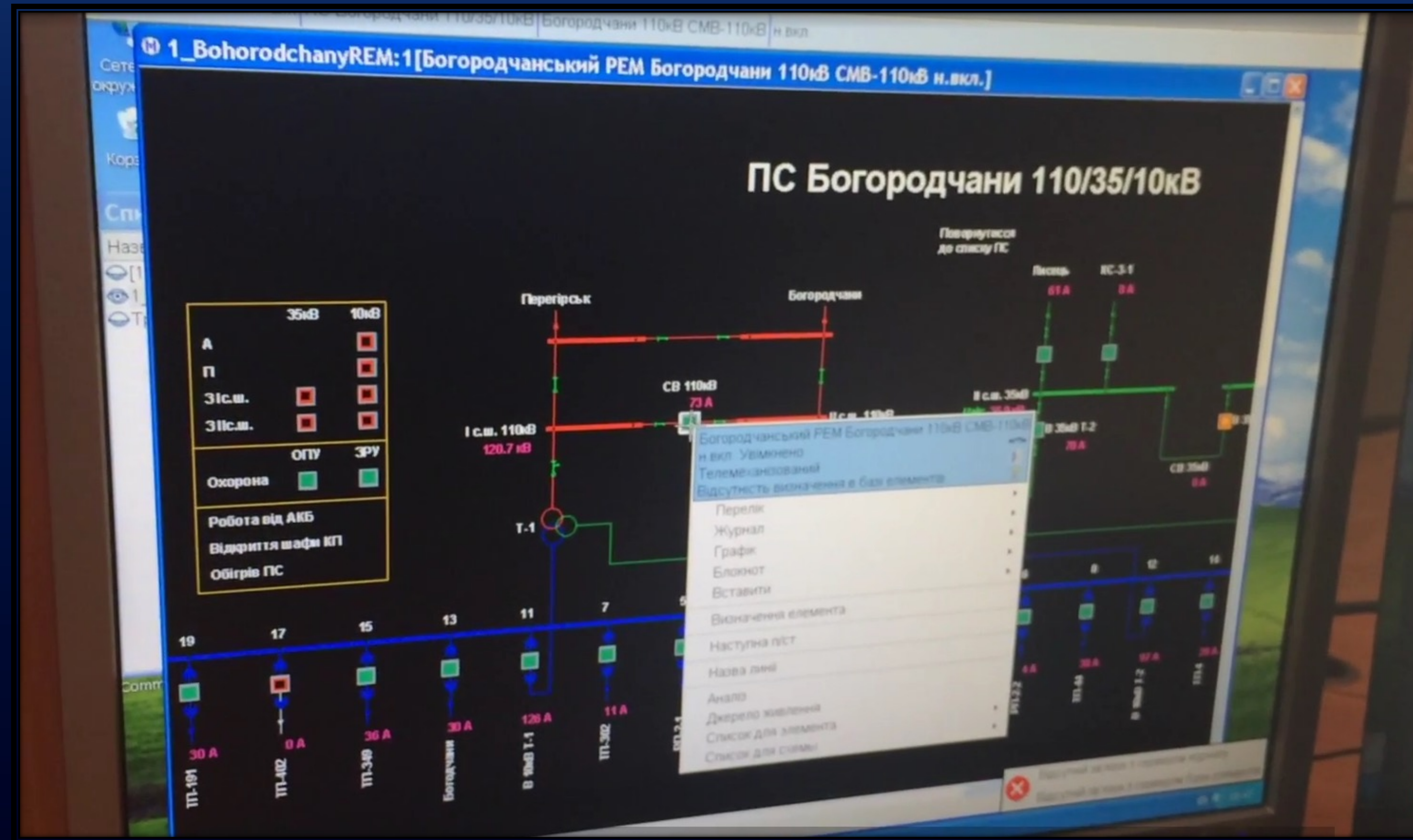
Phantom Mouse
Remote Admin Tools at OS Level

The attackers developed two SCADA hijack approaches (one custom and one agnostic) and successfully used them across different types of SCADA/DMS implementations at three companies

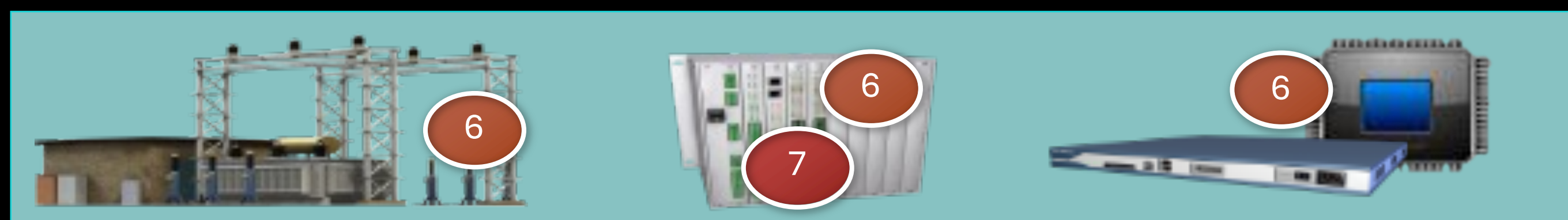
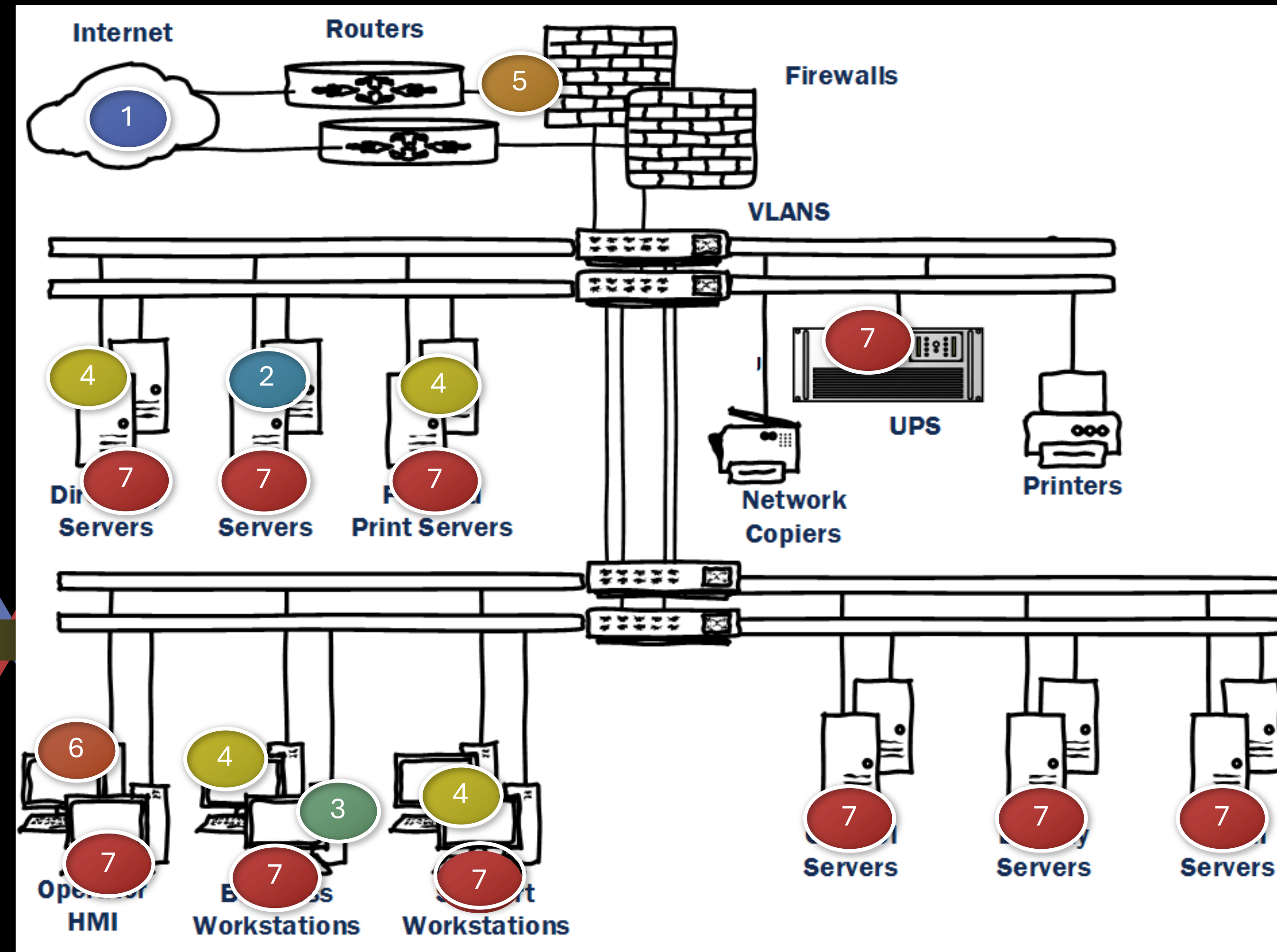
Ukraine Power Outage ICS Cyber Kill Chain



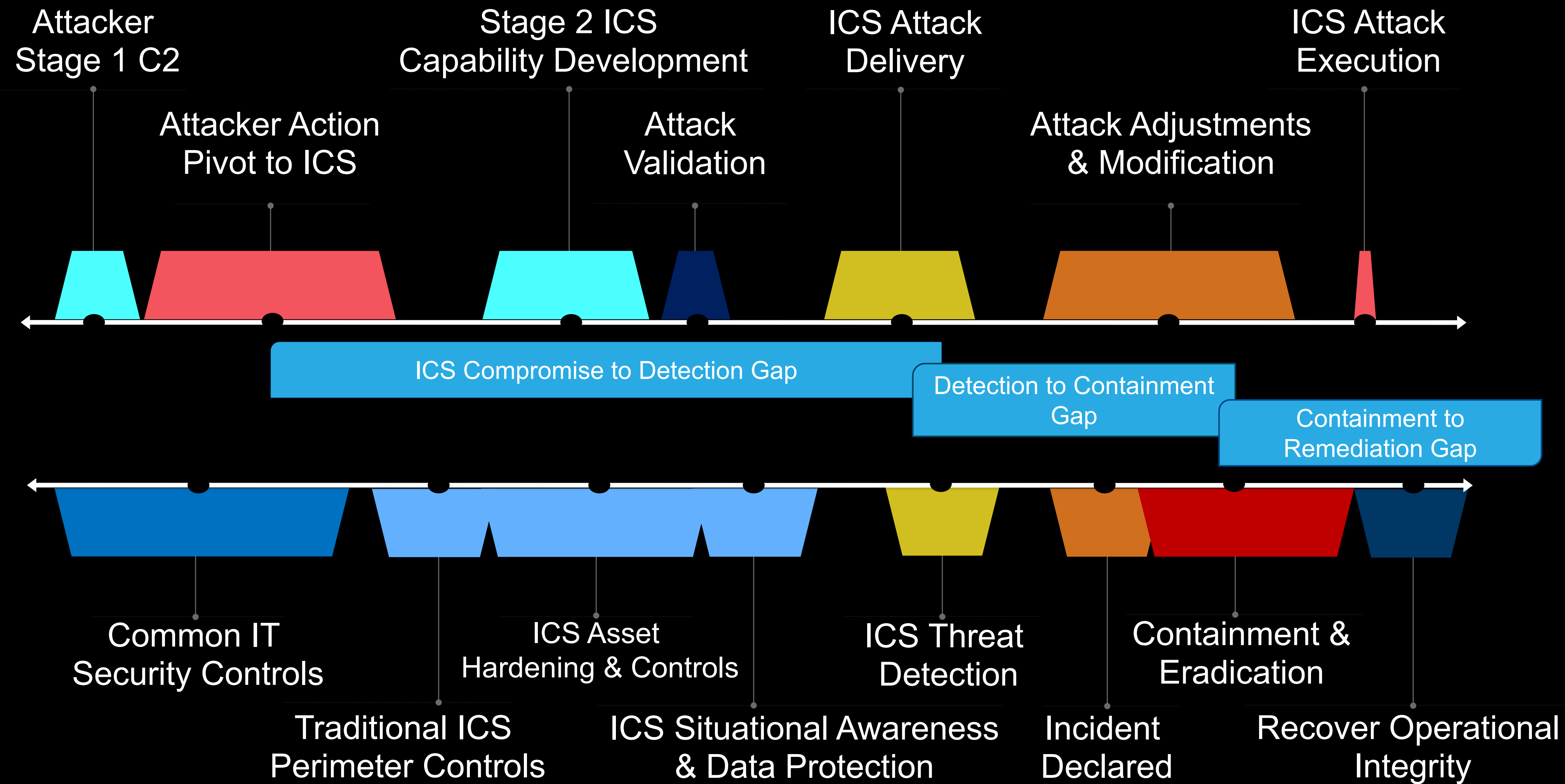
What Did They Do?



- 1 Reconnaissance
- 2 Spear phish
- 3 Foothold
- 4 Credentials/
Pivot
- 5 VPN Access/
Discovery
- 6 Operations/
firmware
- 7 KillDisk, UPS, TDOS



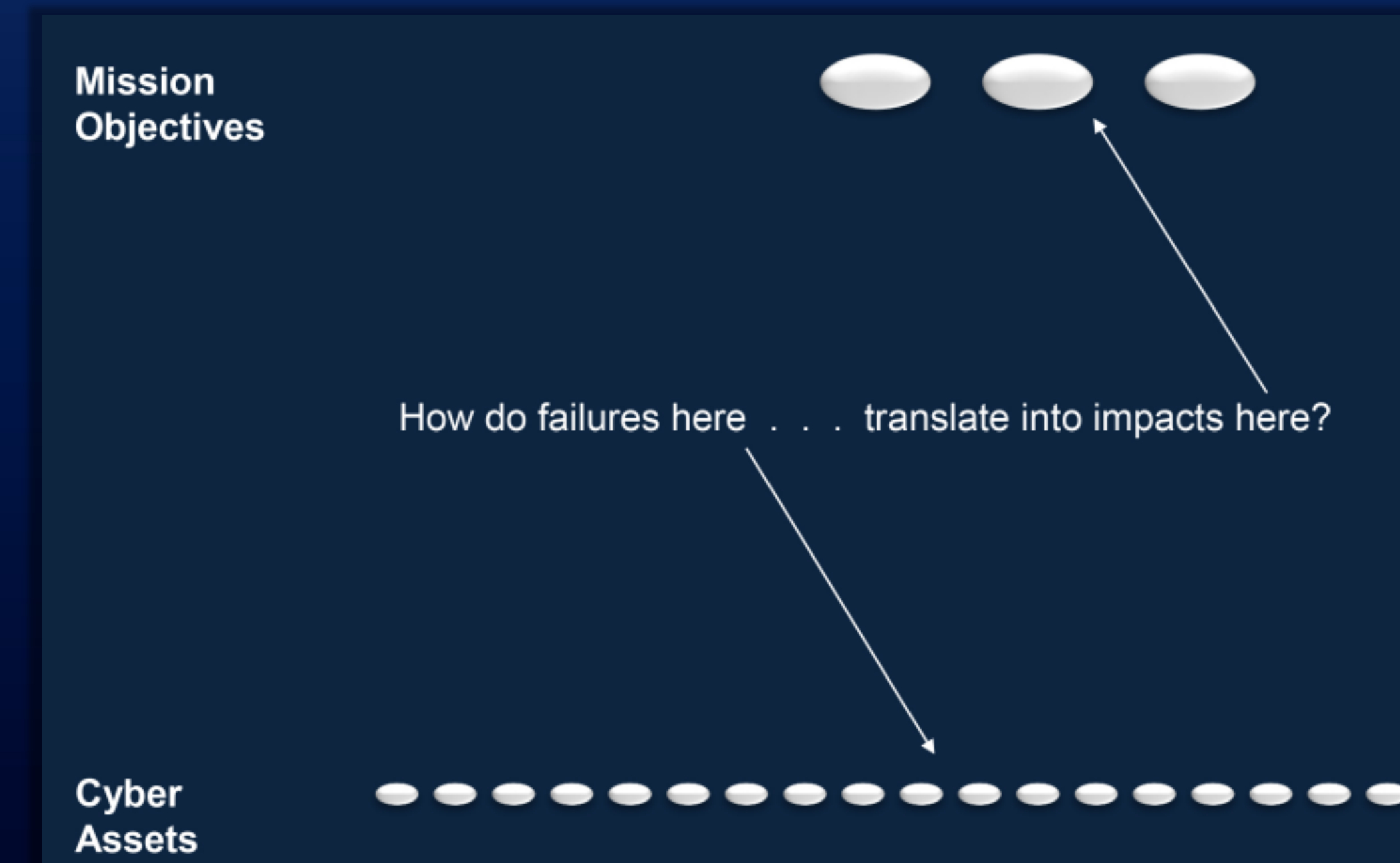
ICS Defender Gap Reduction



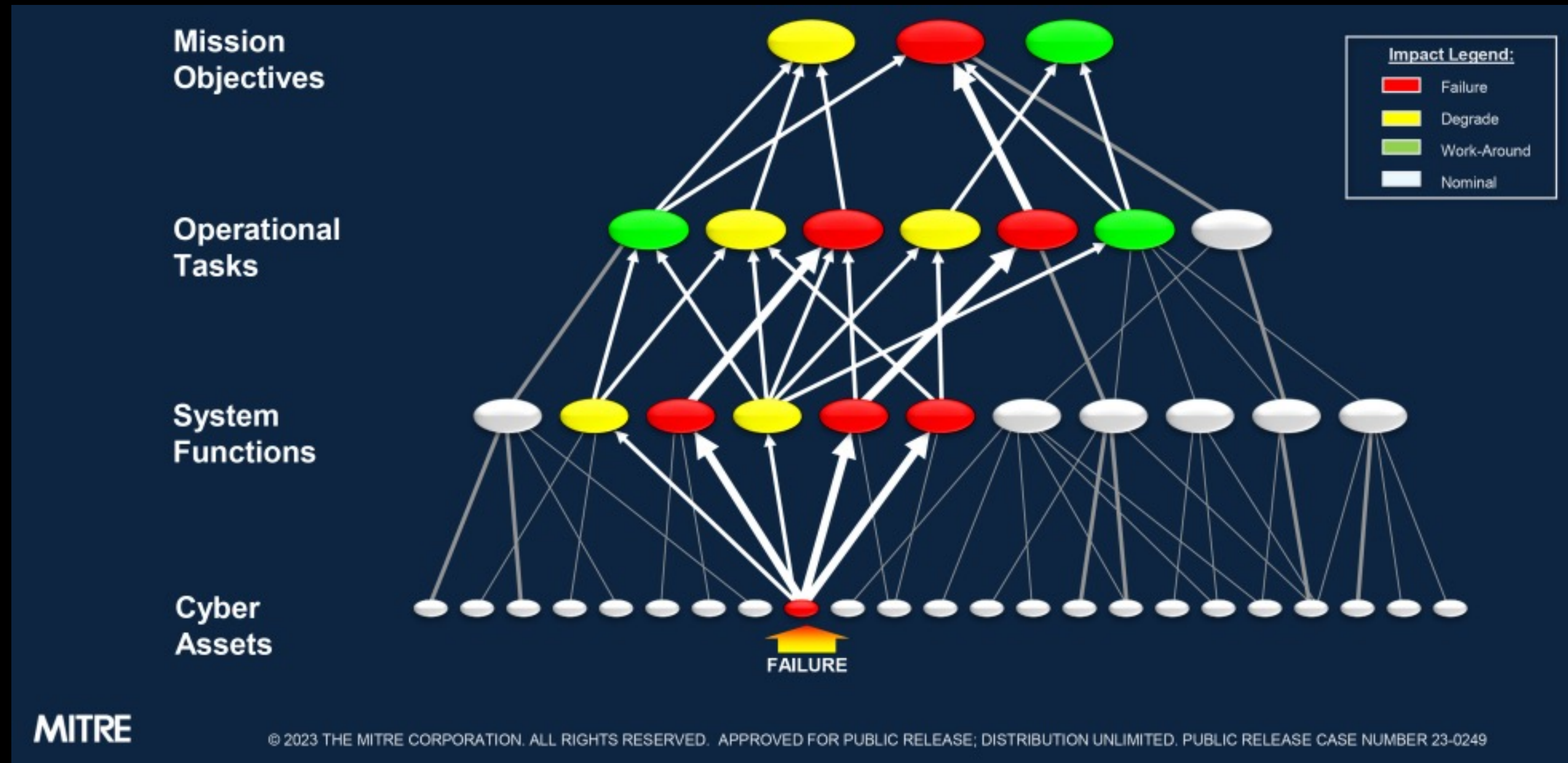
Asset-Based Crown Jewel Analysis

"A crown jewel is a logic-bearing or non-logic-bearing device, whose failure – **or failure to perform as intended** – can cause one or more mission objectives to fail."

- How do we know what is important to a process, solution, service, or production?
- How do we reduce the cost of cybersecurity and assessments while ensuring reliability and availability?
- CJA helps to identify the most critical functions, systems, and assets whose compromise would cause unacceptable impact to safety, reliability, or business operations.



"A crown jewel is a logic-bearing or non-logic-bearing device, whose failure – or failure to perform as intended – can cause one or more mission objectives to fail."



Impact Discussions with Operations



Failure



Degradation



Misuse

Considerations

Loss of System Function

Replacements and Spares

Loss of Inter-dependent
Systems

Intermittent Functionality

Minimal Viable System

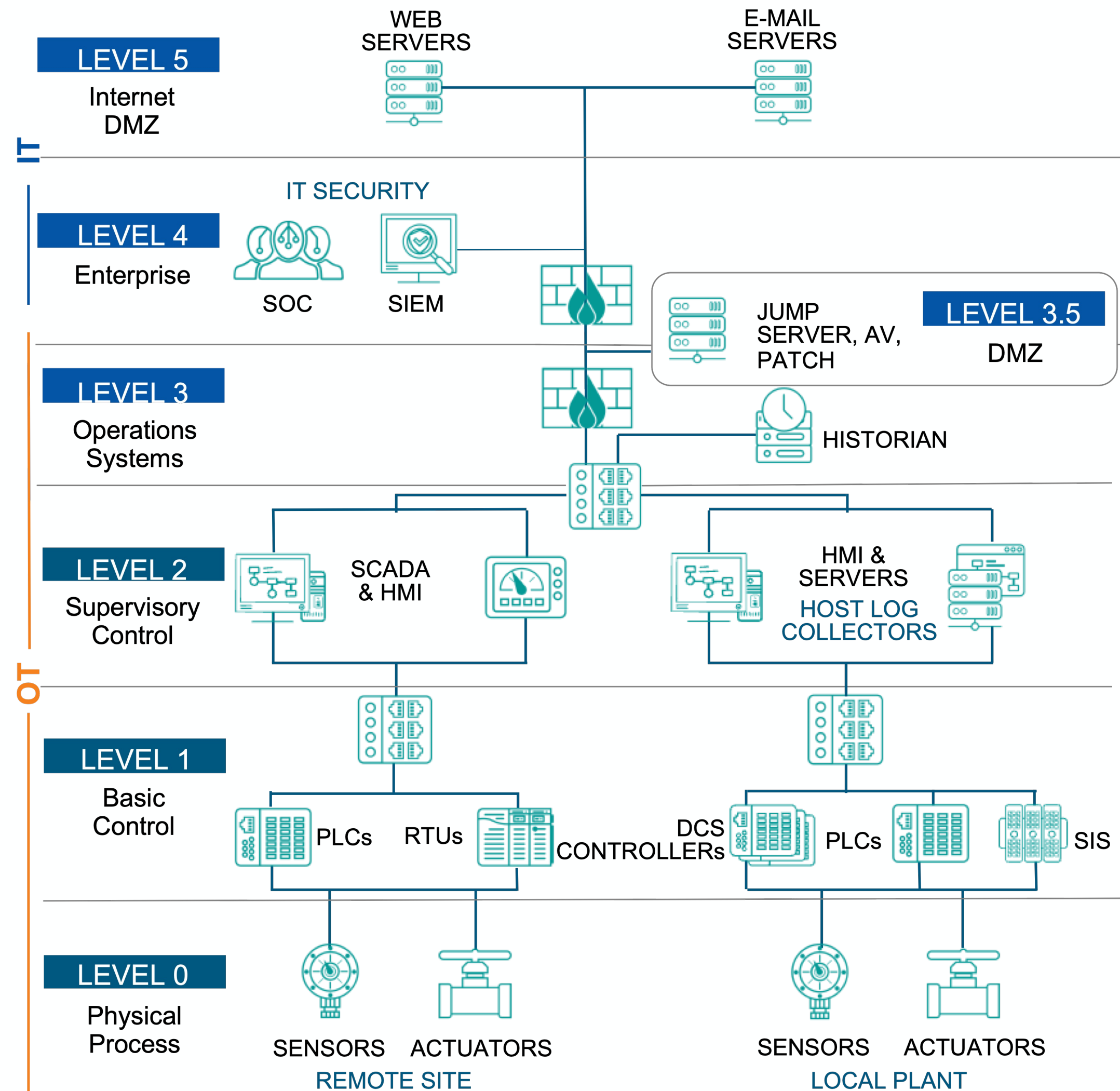
Data Manipulation

Process Manipulation



Attack Path Analysis

- Identify attack path through ICS/OT Pen Test & Assessment
- Choose target from crown jewel analysis
- Select industry threat scenario to align efforts
- Identify network paths, assets involved, pivots, protocol usages, etc.
- Discover architectural changes and network visibility opportunities



Collection Management Framework

- Framework to catalogue asset log details
- Adaptable to meet individual needs
- Core Elements
 - Asset Type - Description of asset/role
 - Data Type - Format of data source
 - Question Type – ICS Kill Chain Phases or MITRE ATT&CK for ICS
 - Follow-on Collection - Additional data source of interest on event
 - Data Storage Location - Remote Accessible or Remote Only
 - Data Storage Time - Data buffer size

Collection Management Framework

	CONTROL CENTER	CONTROL CENTER	CONTROL CENTER	TRANSMISSION SUBSTATION	TRANSMISSION SUBSTATION
ASSET TYPE	Windows Human Machine Interface	Data Historian	Network Monitoring Appliance	Windows Human Machine Interface	Remote Terminal Units
DATA TYPE	Windows Event Logs	Alarms	Alerts	Windows Event Logs	Syslog
QUESTION TYPE (KILL CHAIN PHASES)	Exploration, Installation, Actions on Objectives	Actions on Objectives	Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives	Exploitation, Installation, Actions on Objectives	Installation, Actions on Objectives
FOLLOW-ON COLLECTION	Registry Keys	Set Points and Tags	Packet Capture	Registry Keys	Controller Logic
DATA STORAGE LOCATION	Enterprise SIEM	Local	Enterprise SIEM	Local	Local
DATA STORAGE TIME	60 Days	120 Days	30 Days	30 Days	7 Days

Host and Device Collection

Industrial
DMZ

Manufacturing Zone

Servers

Firewalls

Core
Switches

Distribution
Switch Stack

Traditional
IT log
sources

Traditional
IT log
sources

Legacy OS, log
availability,
access

Vendor and
model
dependent

Syslog is
possibly
available

Lowest level
devices (I/O)
least likely

Layer 2 Access
Switches

Instrumentation

Controller

Drive

I/O



Design

- **Network Traffic**
 - Baselines, ICS events
- **Access Controls**
 - AD Servers, Identity Providers
- **Network Devices**
 - Switches, Firewalls
- **ICS Servers**
 - Engineering Stations, Remote Access, MES
- **ICS Operator Interfaces**
 - SCADA, HMI
- **ICS Control Devices**
 - PLC, DCS, RTU, Event Monitors
- **ICS Data and Code**
 - Code, Parameters, Configs

WHAT TO MONITOR

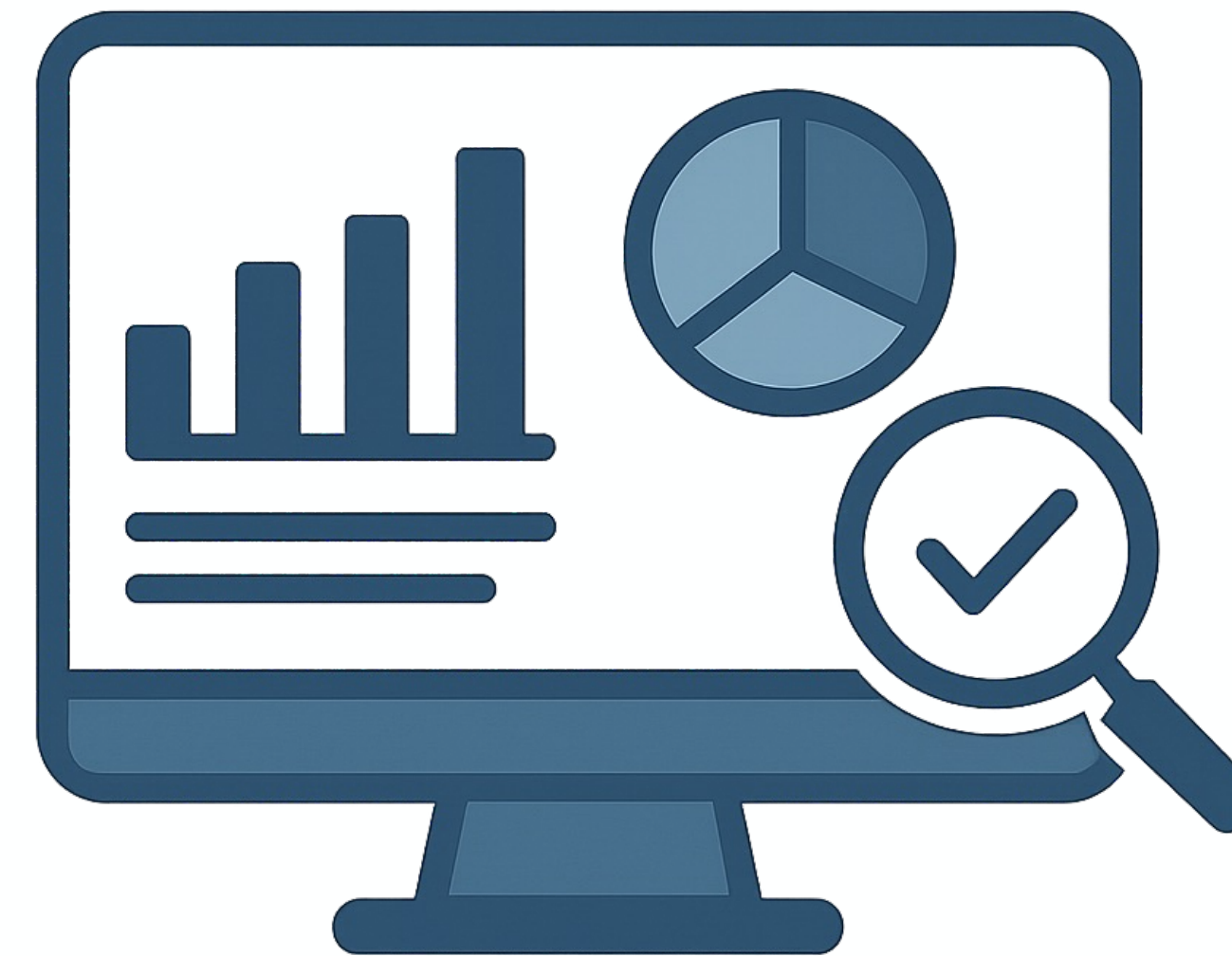
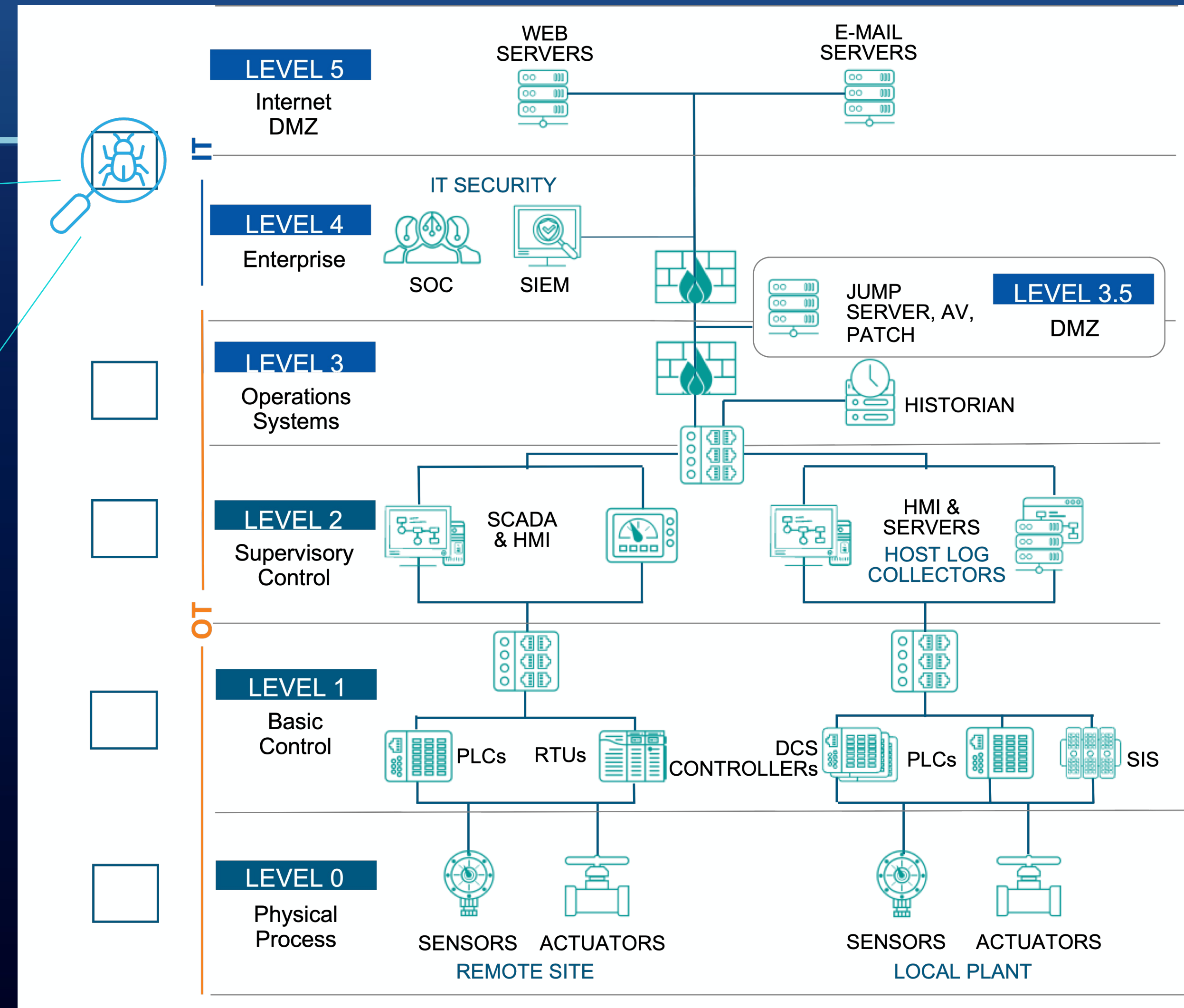


Image Ref: ChatGPT Image Creator 5.1

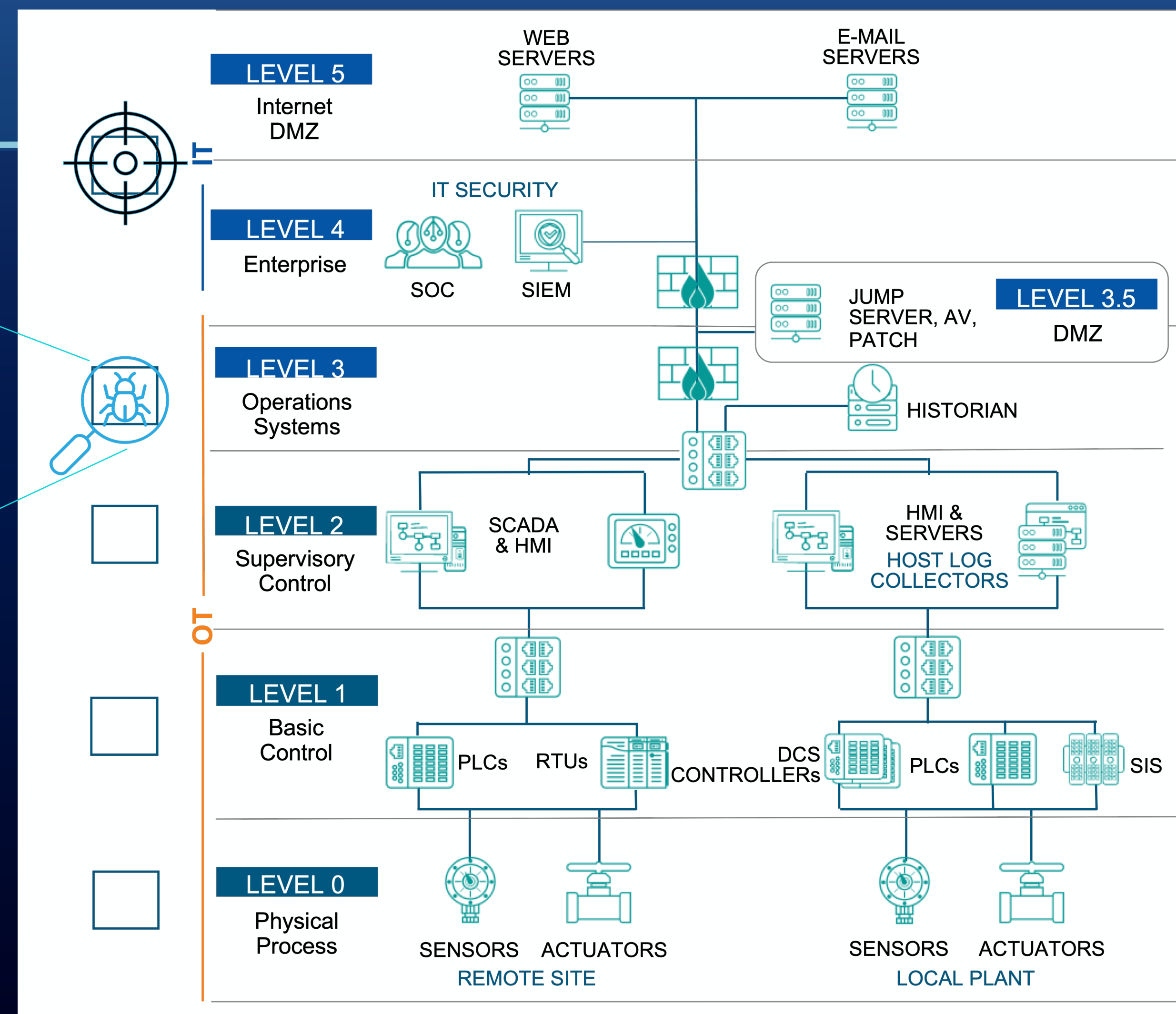
Visibility Across IT and OT

- Attacks from corporate IT networks that pivot to OT
- Attacks from vendor support IT networks that pivot to remote OT environments



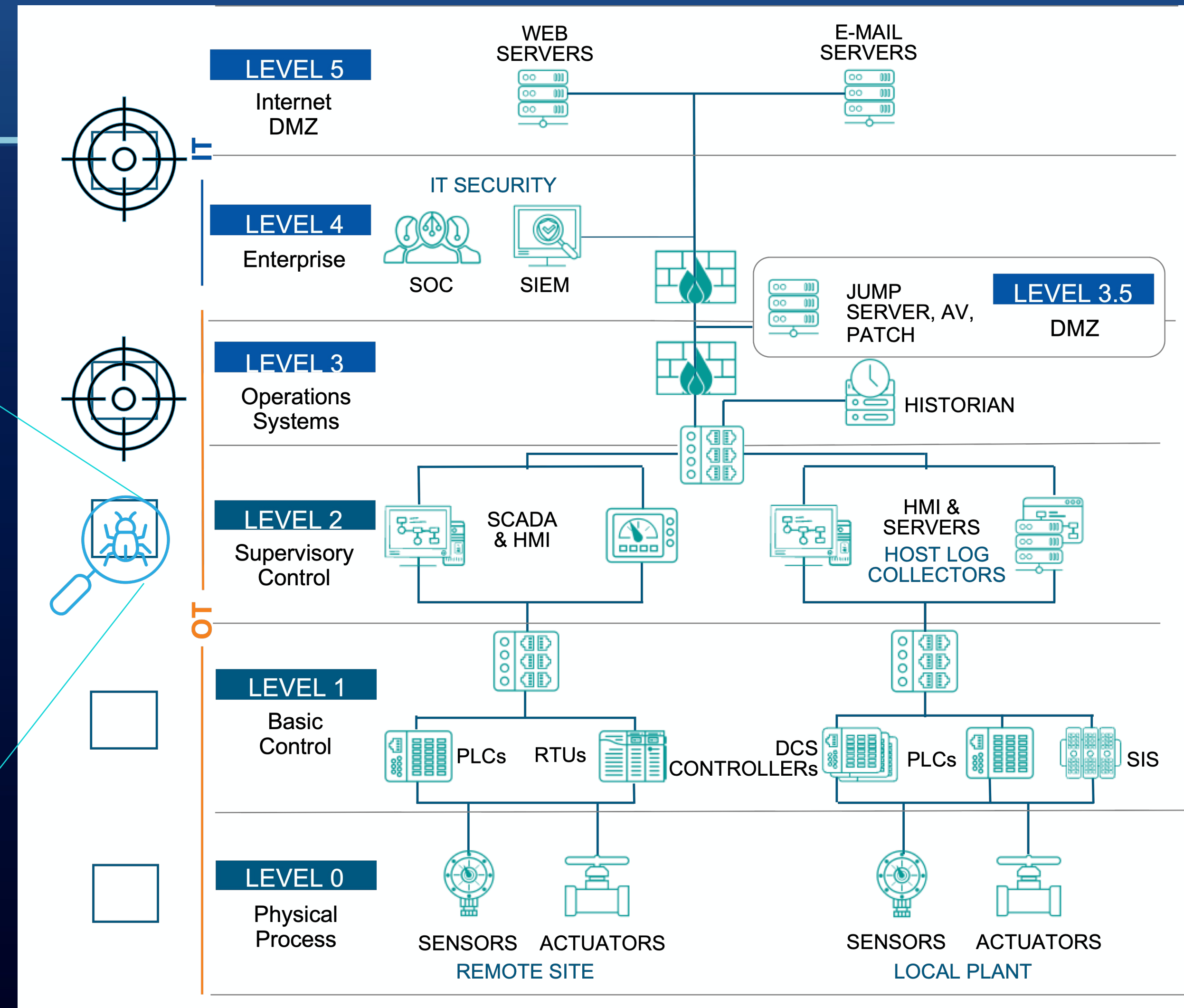
Visibility Across IT and OT

- Attacks targeting trusted communications and applications communicating in and out of ICS environments



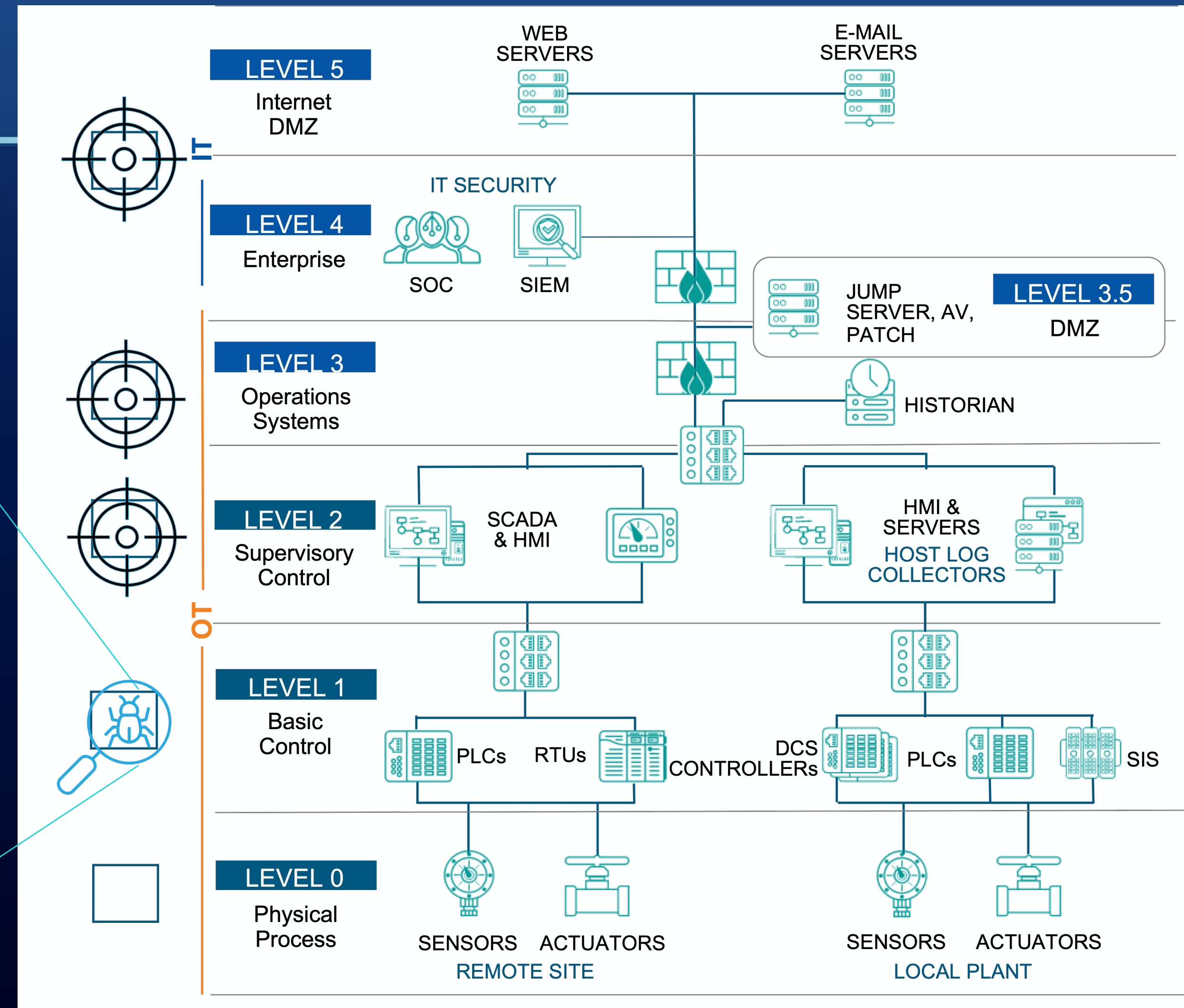
Visibility Across IT and OT

- Attacks utilizing engineering workstations to obtain connectivity, and configurations to develop or inform an ICS attack
- Attacks that mis-operate the control system through an operator workstation
- Attacks sending manipulated commands directly to field devices

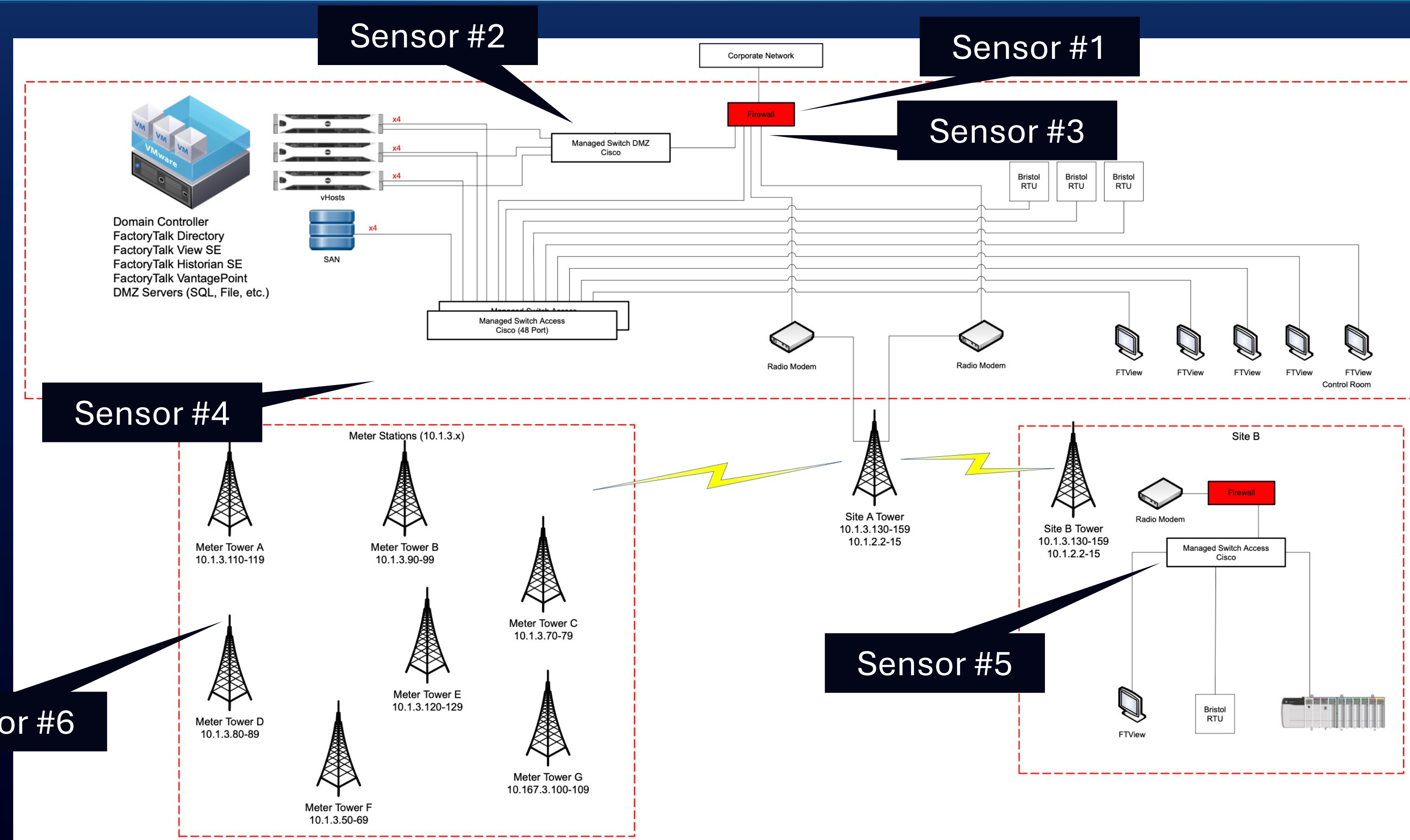


Visibility Across IT and OT

- Attacks on supply chain lifecycles
- Attacks over direct OEM access paths
- Attacks directly targeting process controls: Access, Denial, Manipulation
- Combination attack targeting equipment



Casse Study: Network Sensor Placement



Network Sensor Challenges

- **Bandwidth and Latency**
 - Remote Telemetry
 - Legacy Communications
- **CPU and Memory Limitations**
 - Embedded Devices
- **Poor Logging Implementations**
 - Variations of Log Information/Format
- **Cabinet Space**
 - Limited Space
 - Power



Access Controls

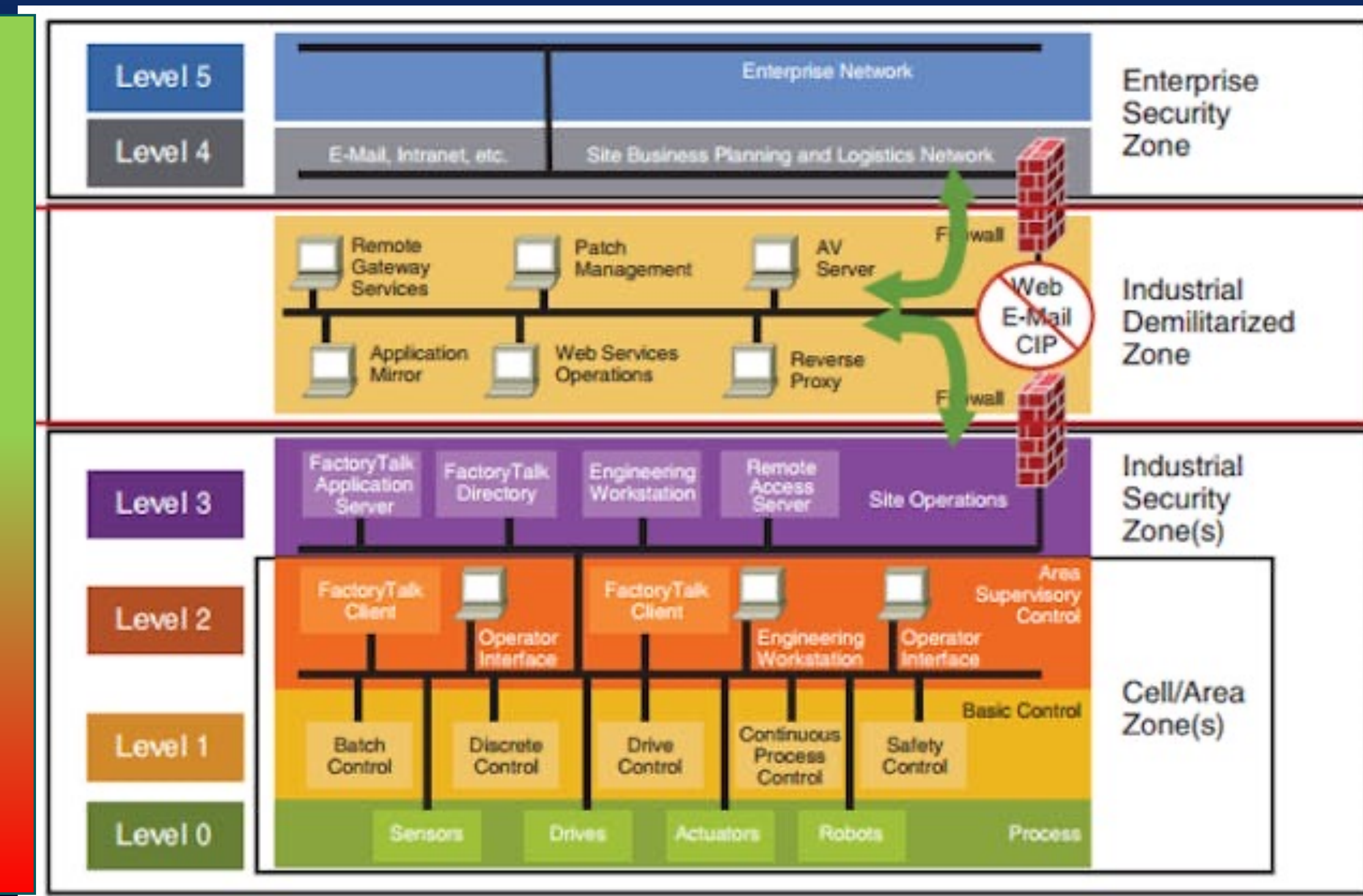
- **Active Directory Servers**

- Failed Login Attempts
- Password Changes
- Known adversarial activity
- Account Creation
- Service Startup/Shutdown

- **Identity Providers**

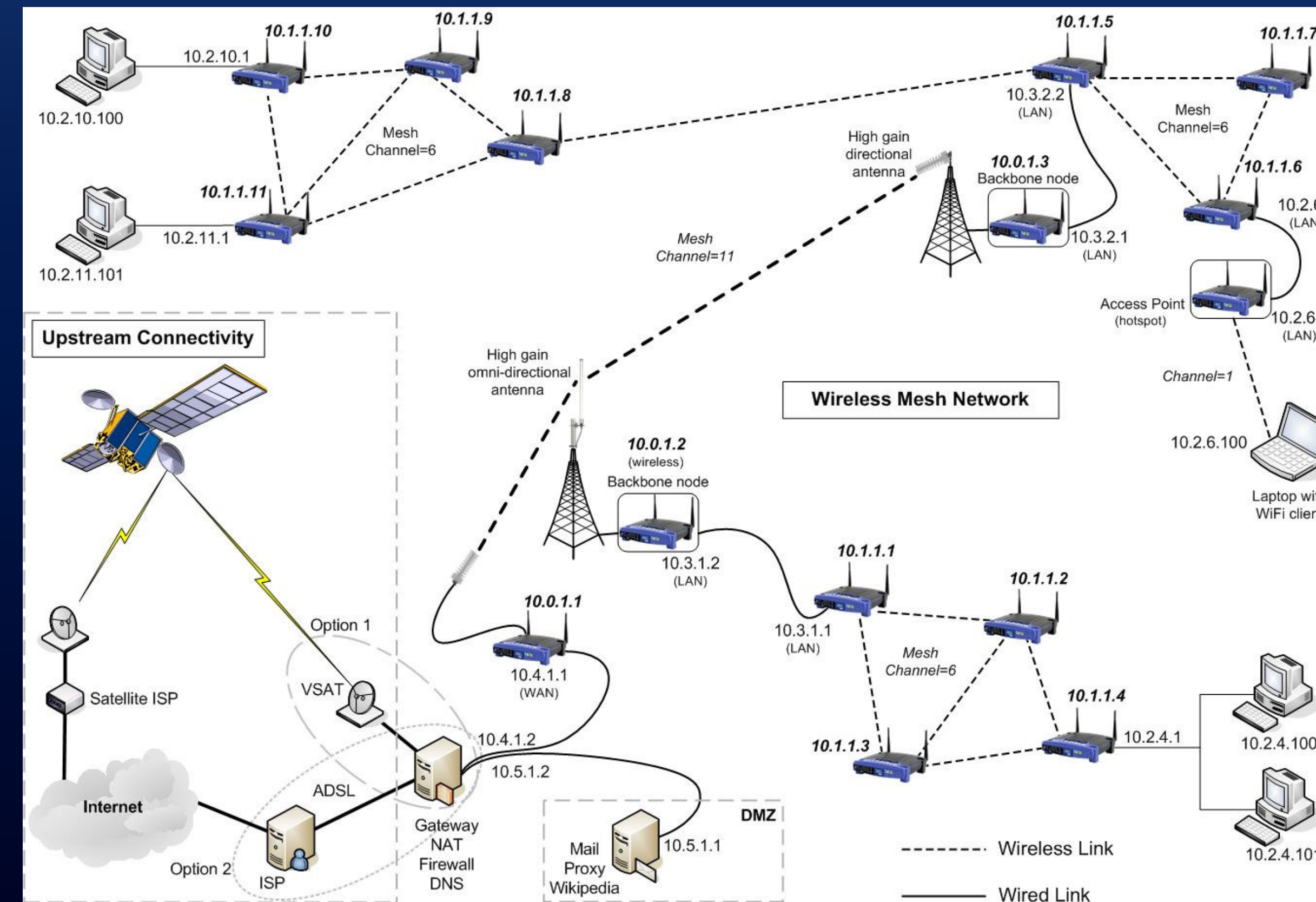
- Authentication Events/Failures
- User Lifecycle
- Authorization (Escalation) Events
- Security/Risk (Geofence, Log alteration)
- Data Protection Events

Access Control Coverage



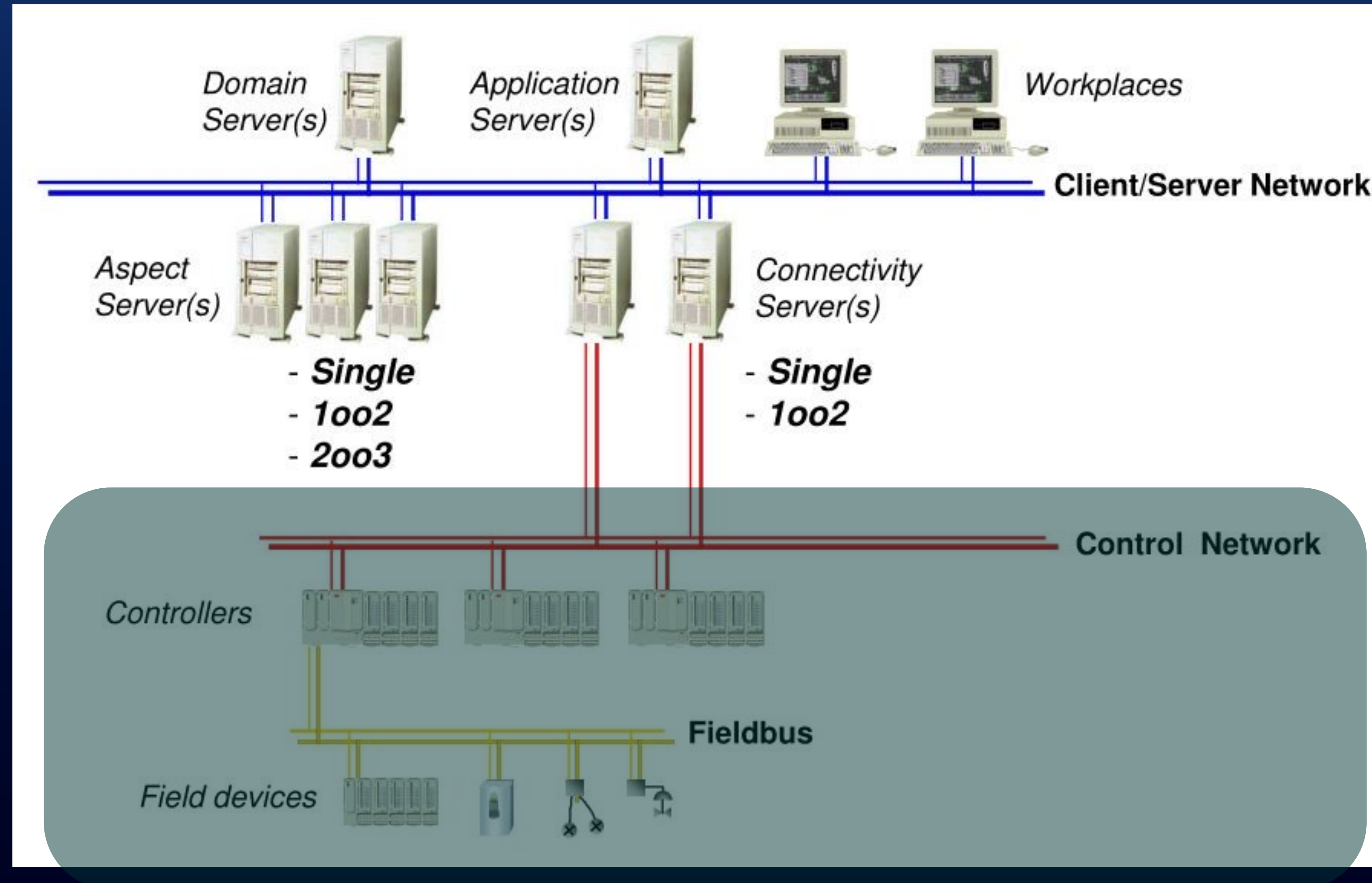
Network Devices

- Switches
 - Port Up/Down
 - Spanning Tree
- Firewalls
 - Denied Traffic
 - Ports Up/Down
 - Traffic out of Context
- Access Point
 - Connections
 - Failed Logins
- ISP (Sat, Cell, etc.)
 - Connections



ICS Servers

- **Engineering Stations**
 - Configuration Changes
 - Service Starts/Stops
 - Software Install
- **Remote Access**
 - Session Logging
- **Operating System**
 - Service Starts/Stops
 - Log Edits
- **Historians**
 - Stale Tags
 - Data Manipulation



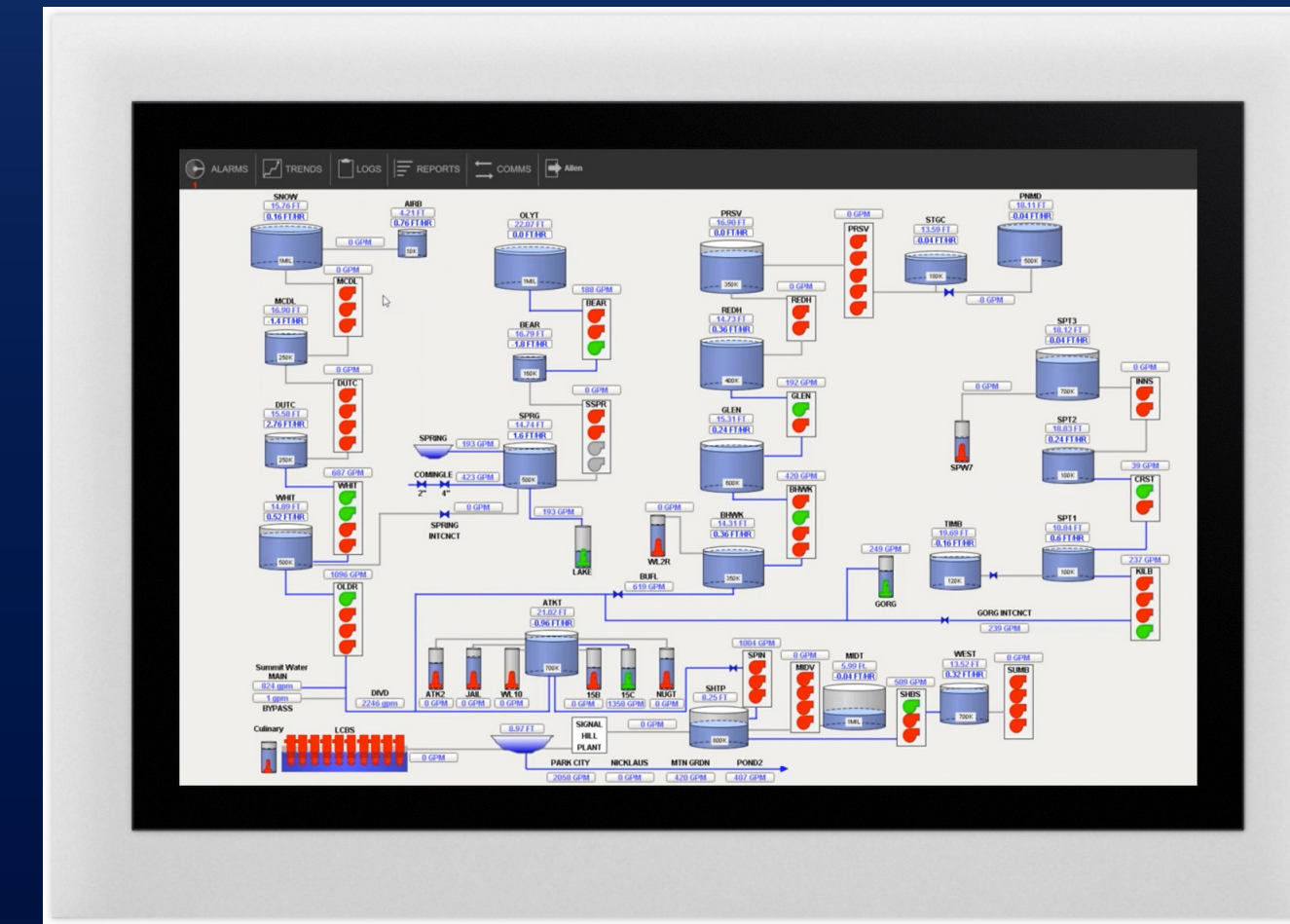
ICS Operator Interfaces

- **SCADA / Supervisory HMI**

- Operator Actions
- Alarm Events
- Security Events (Login/Logout, User Role Change)
- Anomaly or EDR detection
- Service Start/Shutdown
- Software Installs
- Log Tampering

- **Electronic Operator Interfaces**

- Basic OS Events
- Basic Operator Actions



ICS Control Devices

- **Program**
 - Modification
 - Backup or Restore
- **Security**
 - New Policy, Identity Expiration, Modify Policy
- **Network Modification**
- **IO Device**
 - Stops Communicating
 - Communication Resets
- **Device Specific**
 - Firmware Updates
 - Power Failure
 - Time Change
- **Log Configuration Change**



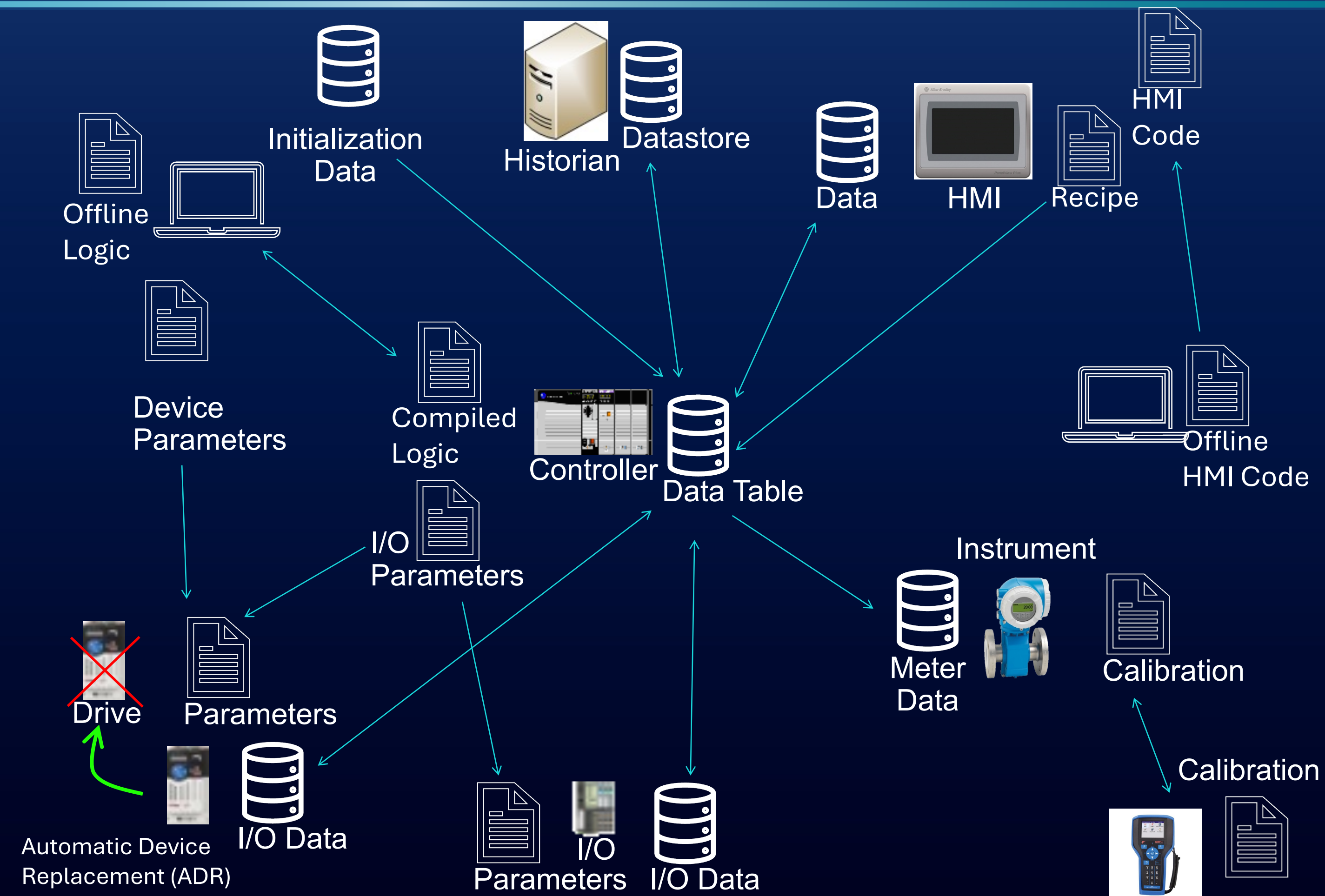
ICS Data and Code Changes

- **Considerations**

- Integrity
- Influence one or many systems
- Impact to system and operations

- **Difficulty**

- Influence on some devices
- Detect change on most



Implementation



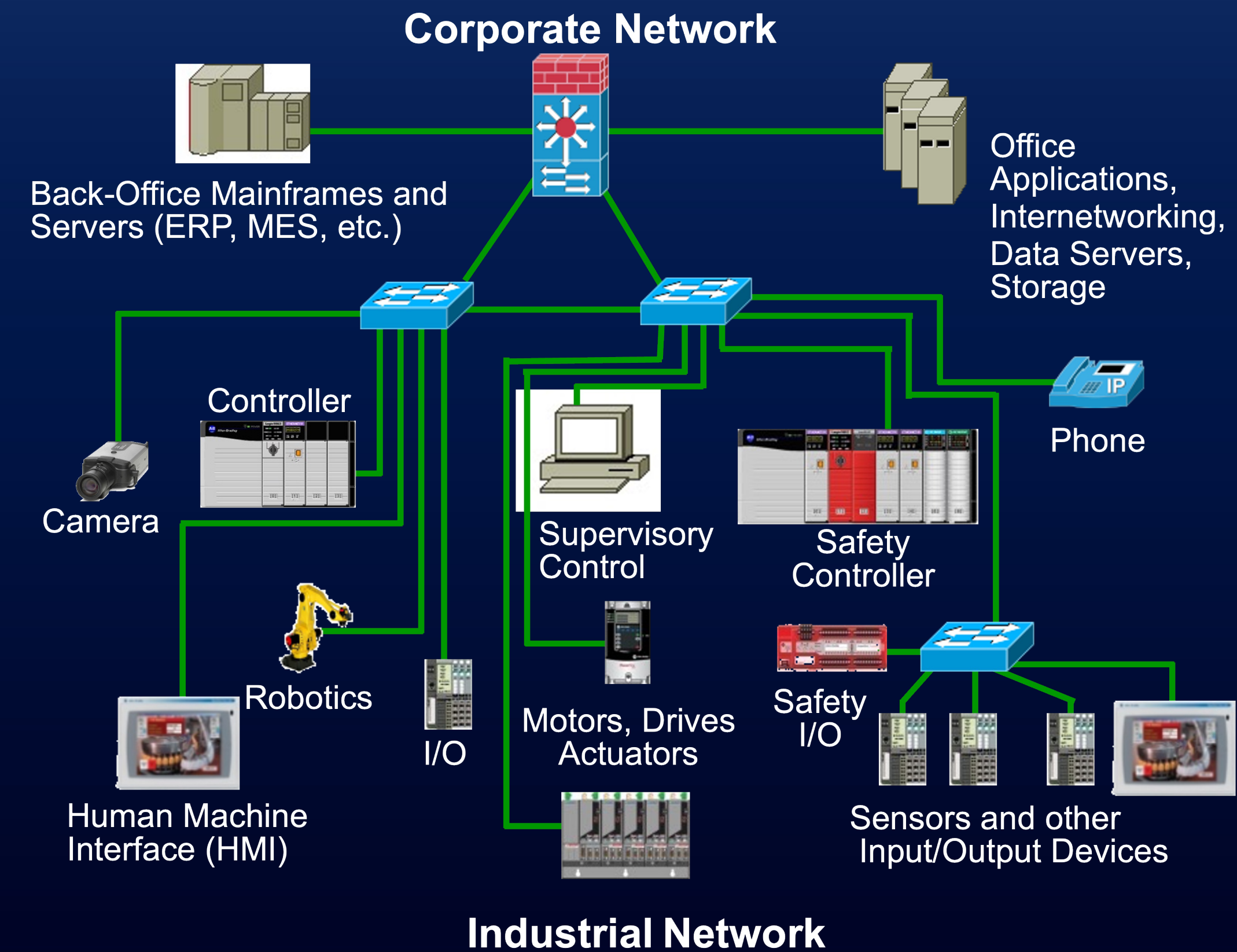
Network Traffic

- **Network Communications**

- Baselines and Deviations
- Bandwidth
- Sessions – Continuous / Periodic

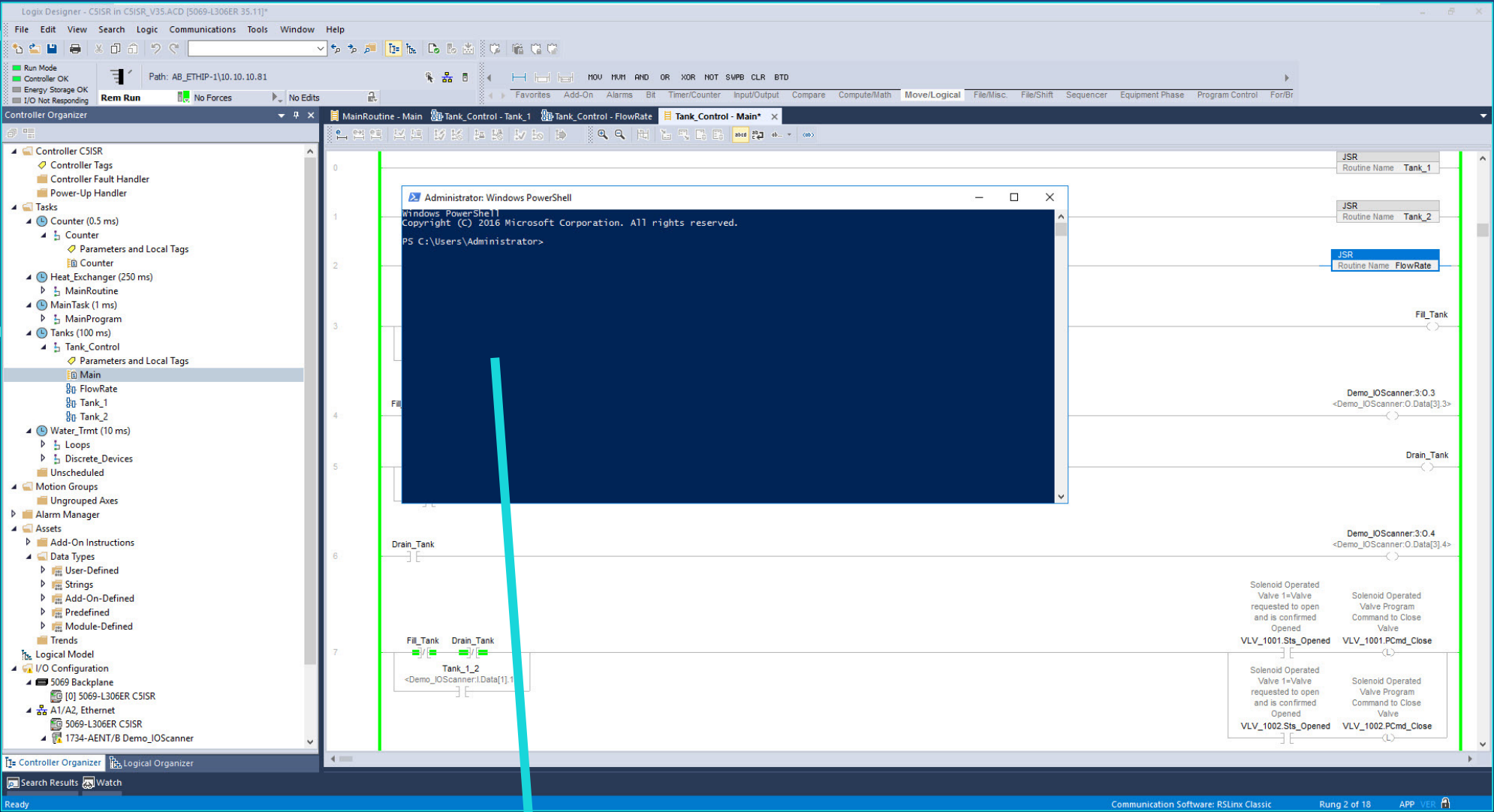
- **Network Intrusion Detection**

- Alerts
- ICS protocols
 - Firmware Change
 - Project Change
 - Data Change



Unusual Process Detected

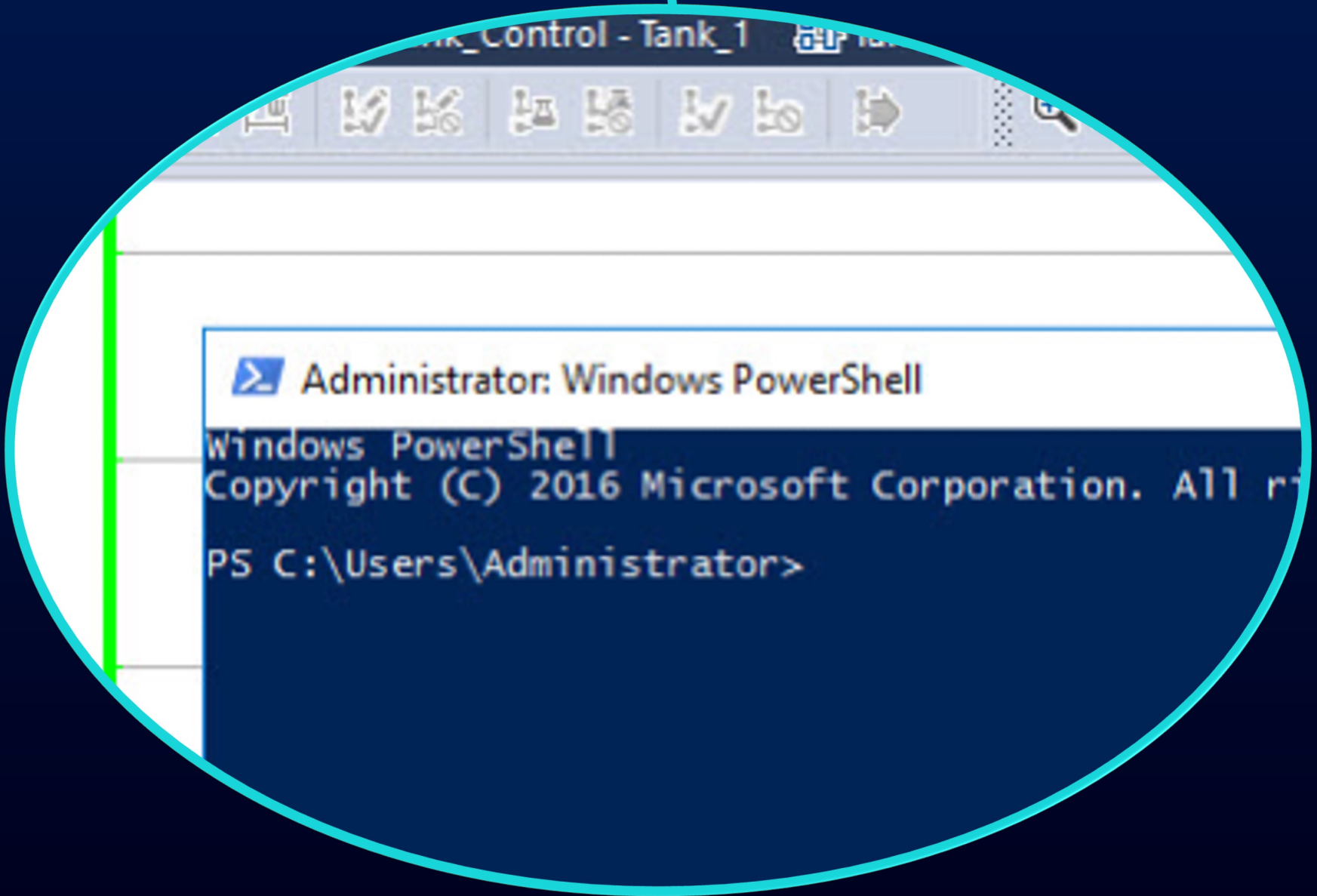
- Data Source
 - Host Events
- Collection
 - Windows Event Logs
 - Host Agent



Alerts by name

Rule name

BAS.3-Unusual Process Detected



New Remote Connection

- Data Source
 - Host Events
 - Network Events
- Collection
 - Host Agent
 - Port Mirror

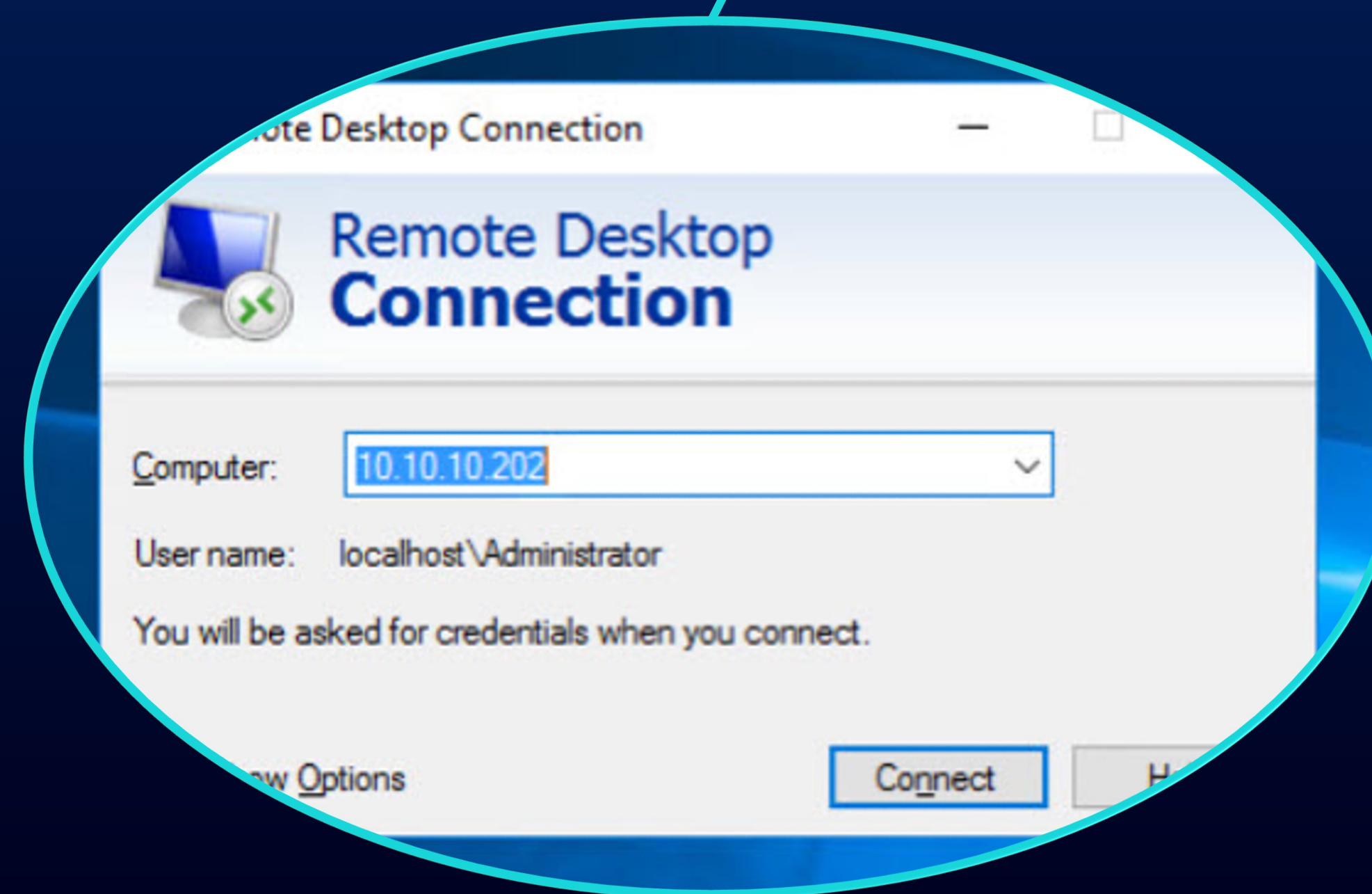
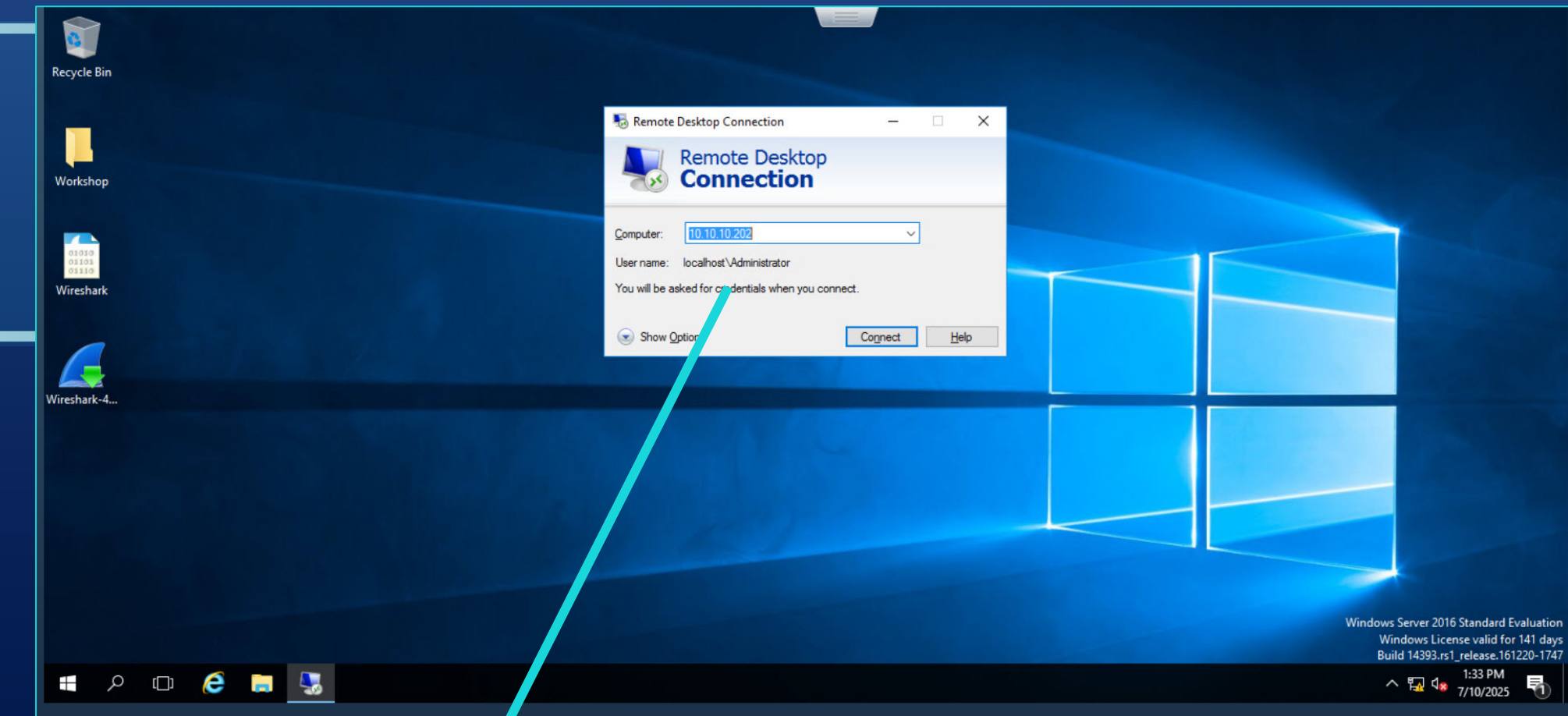
Alerts by name

Rule name

BAS.1-Remote Access to Environment

BAS.2-Remote Desktop Connection Attempted

BAS.6-Remote Desktop Connection w/Administrative Access



Connection Loss

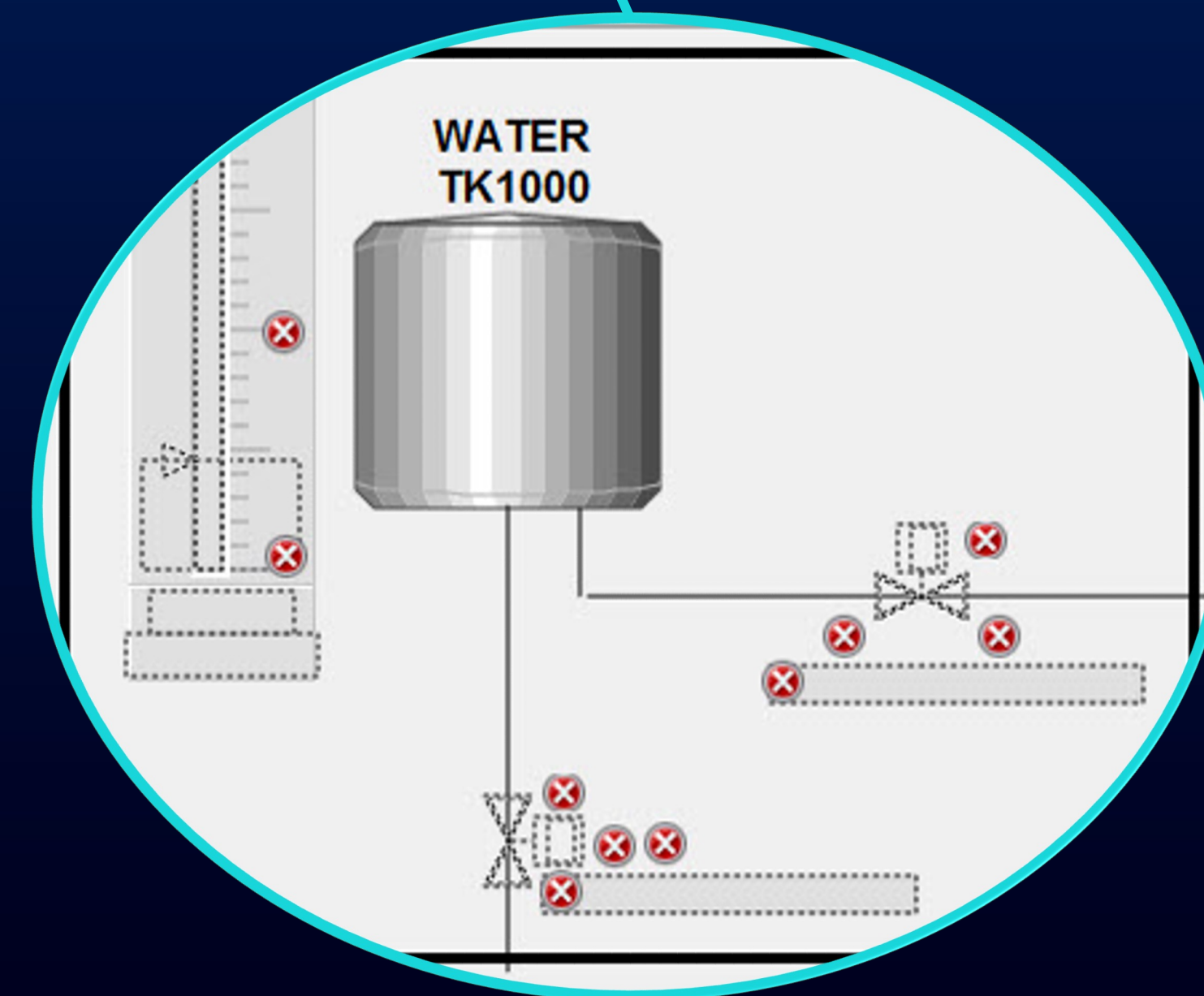
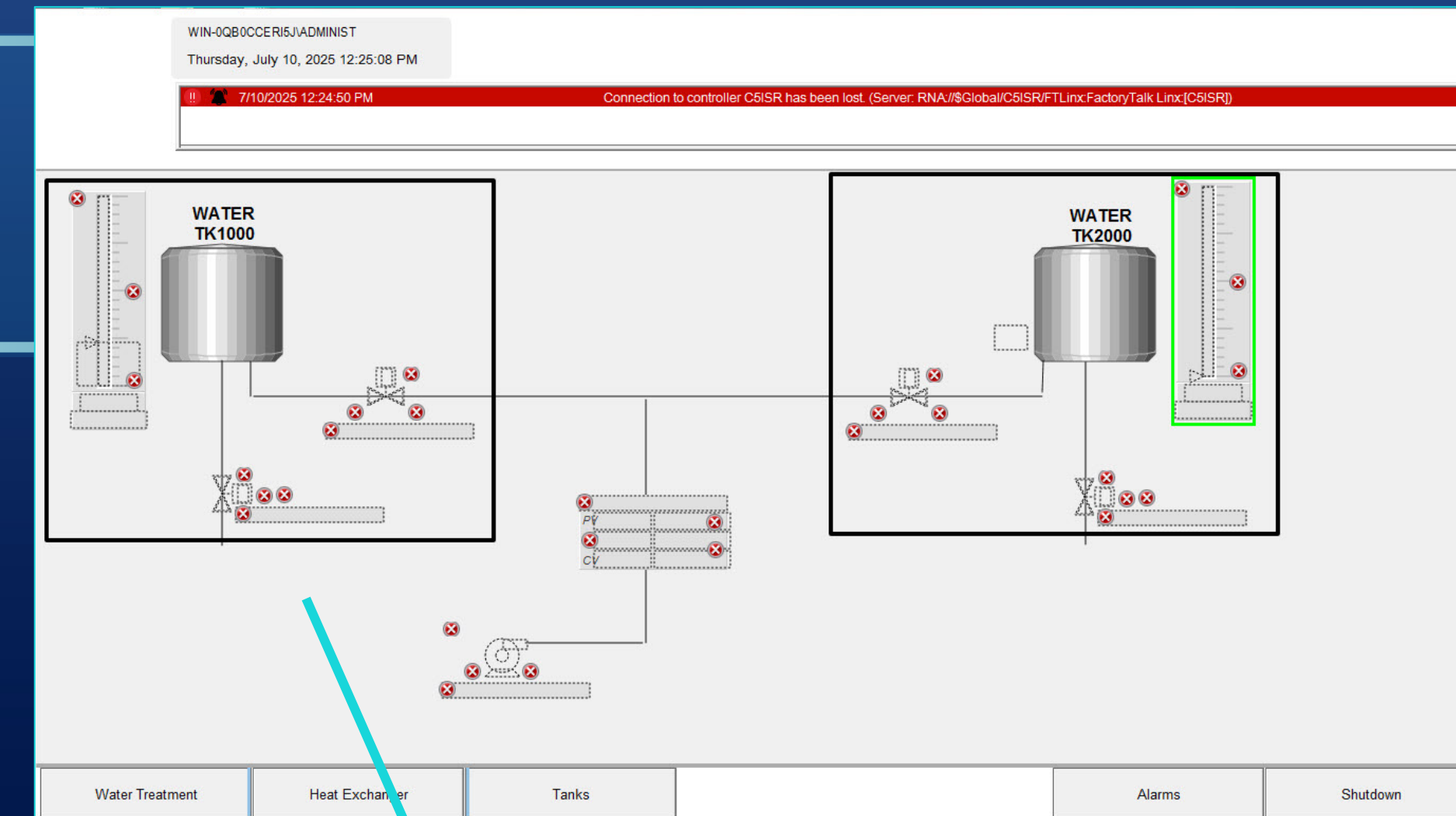
- Data Source
 - Network Events
- Data Collection
 - Syslog

```
28 04:33:10.844: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/2, changed state to down
```

+ Filter for

- Filter out

Copy value



Operations Alarm

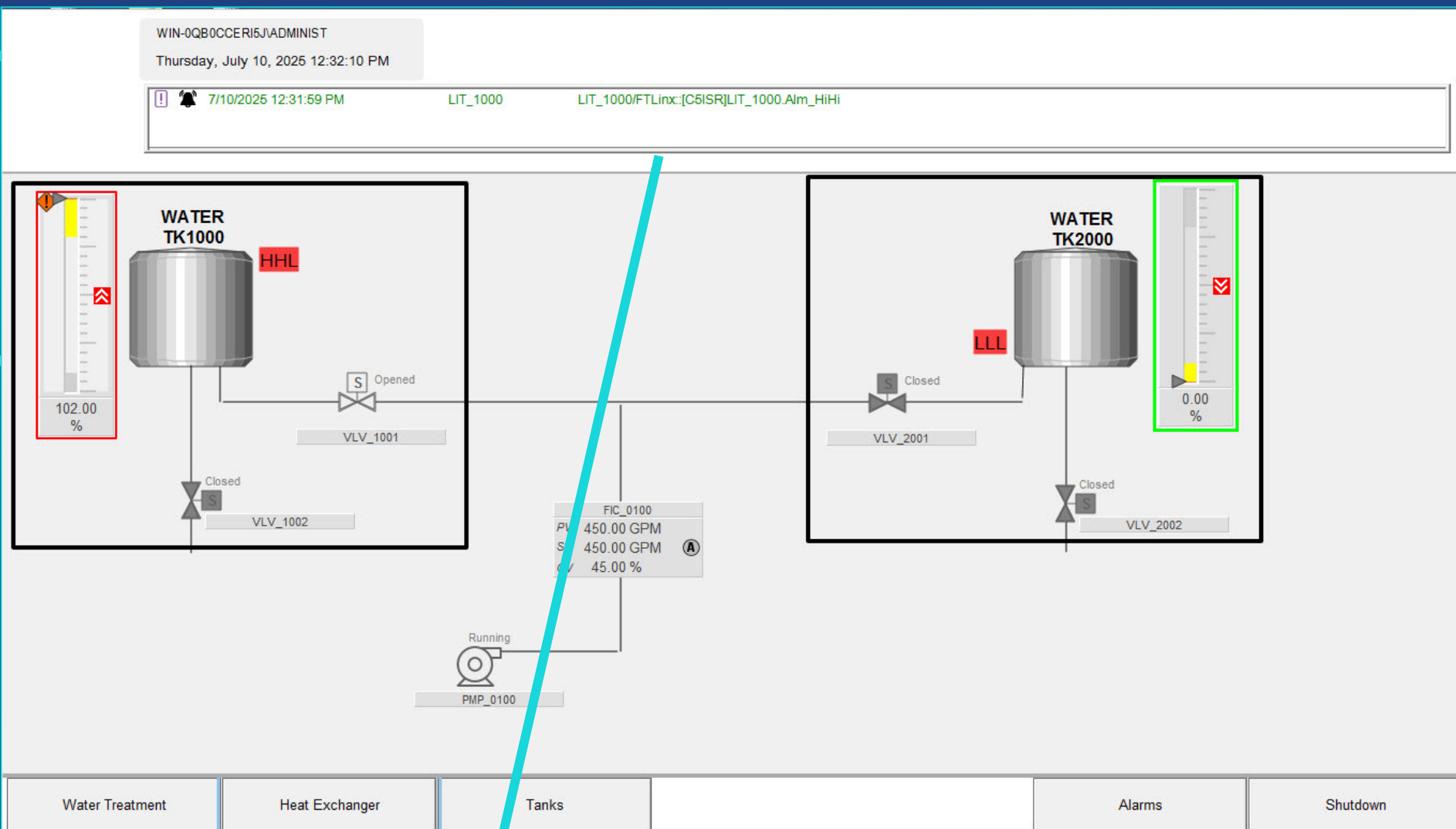
- Source
 - Host Events
- Collection
 - ICS Application
 - Custom Host Script

Recieved an alarm event from condition
'RNA://\$Global/C5ISR/FTAlarms/FTAlarms::LIT_1000:TRIP'. Its state is 'ACTIVE ENABLE UNACK UNSUPPRESS UNSHELVE ', quality is '192', and message is 'LIT_1000/FTLinx::[C5ISR]LIT_1000.Alm_HiHi'.

⊕ Filter for

⊖ Filter out

📄 Copy value



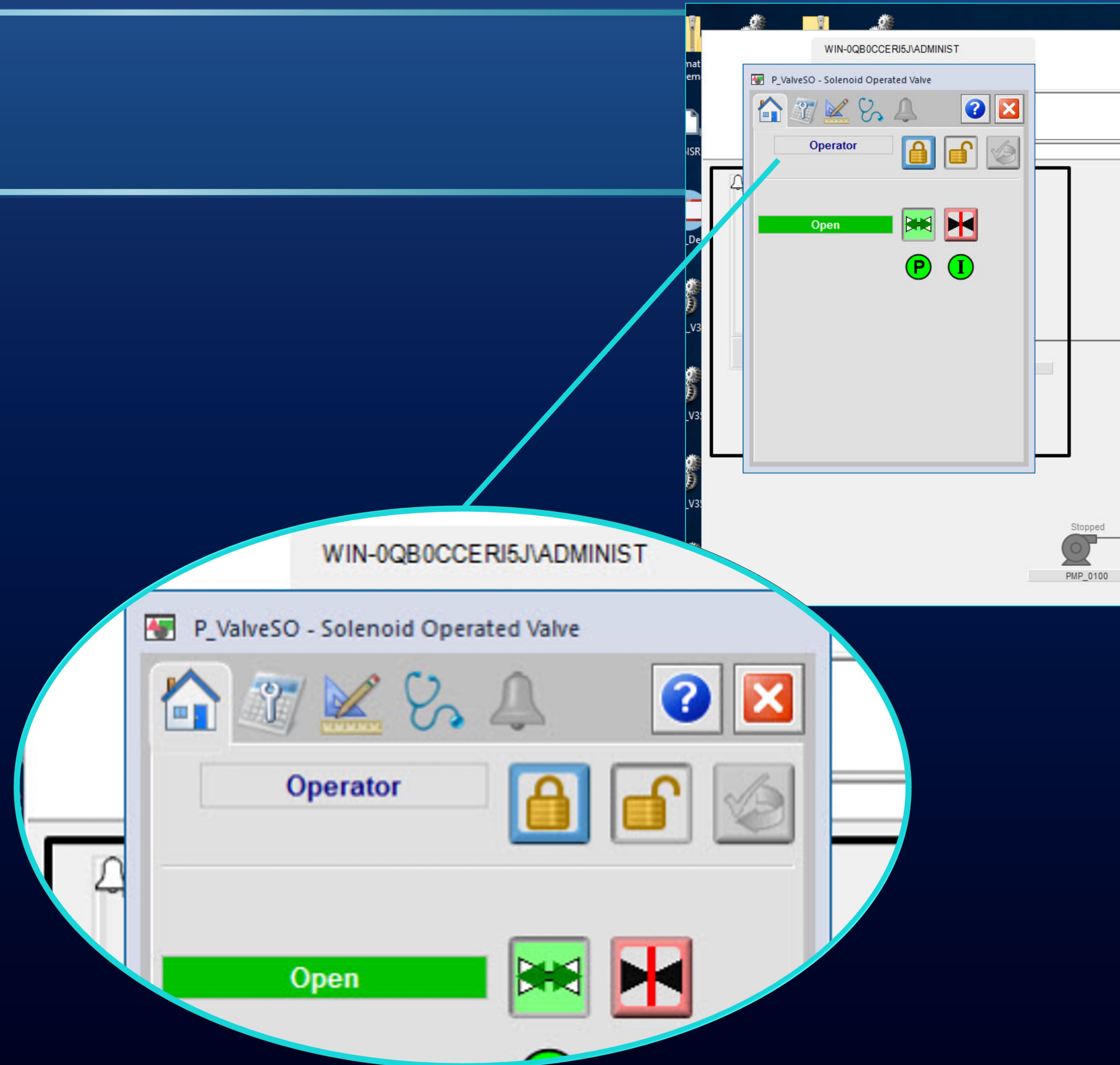
LIT_1000

LIT_1000/FTLinx:[C5ISR]LIT_1000.Alm_HiHi

Operator Action

- Source
 - Host Events
 - Network Events
- Collection
 - Windows Event Log
 - Host Agent
 - Custom Script
 - Packet Capture

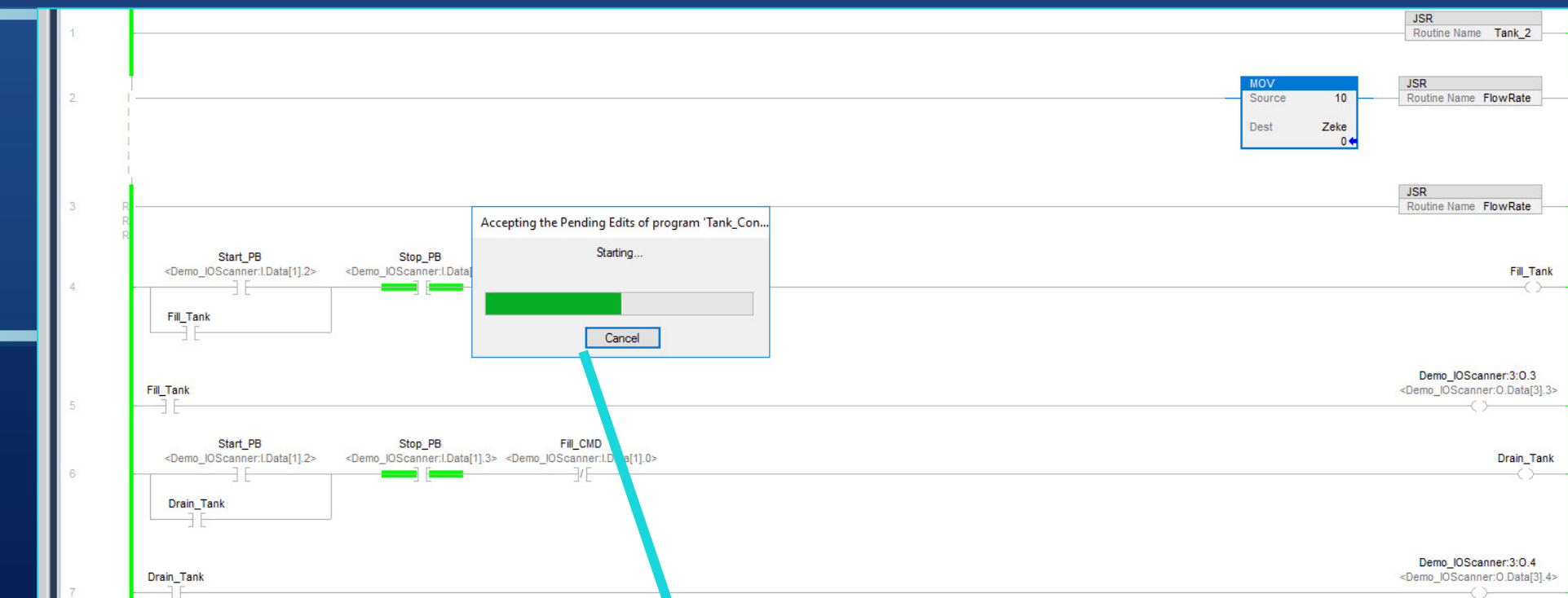
```
<150>1 2025-07-10T17:33:04Z WIN-0QB0CCERI5J FactoryTalk_View_SATag - ftdiag [ftdiag@47349 user="WIN-0QB0CCERI5J\\ADMINISTRATOR"] Write 'True' to '/FTLinux::[C5ISR]VLV_1002.0Cmd_Open'. Previous value was 'False'.
```



Controller Logic Change

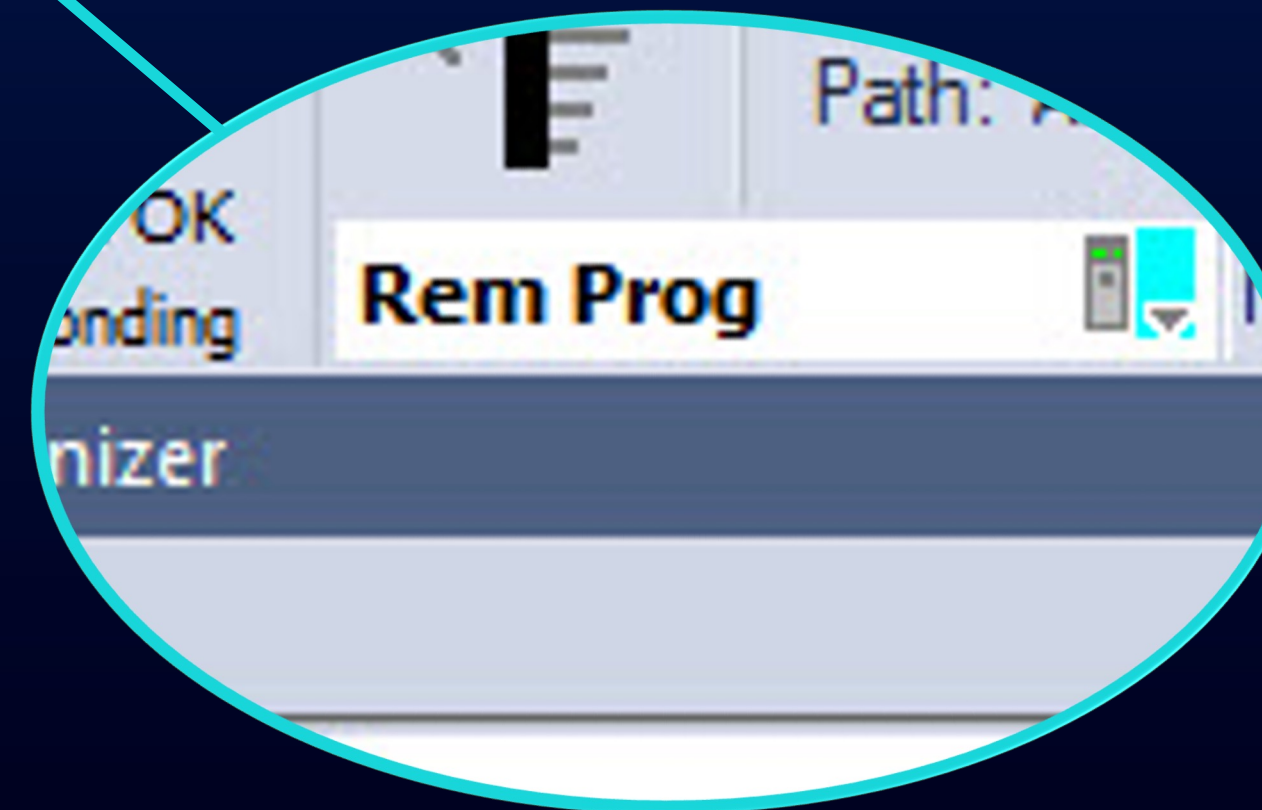
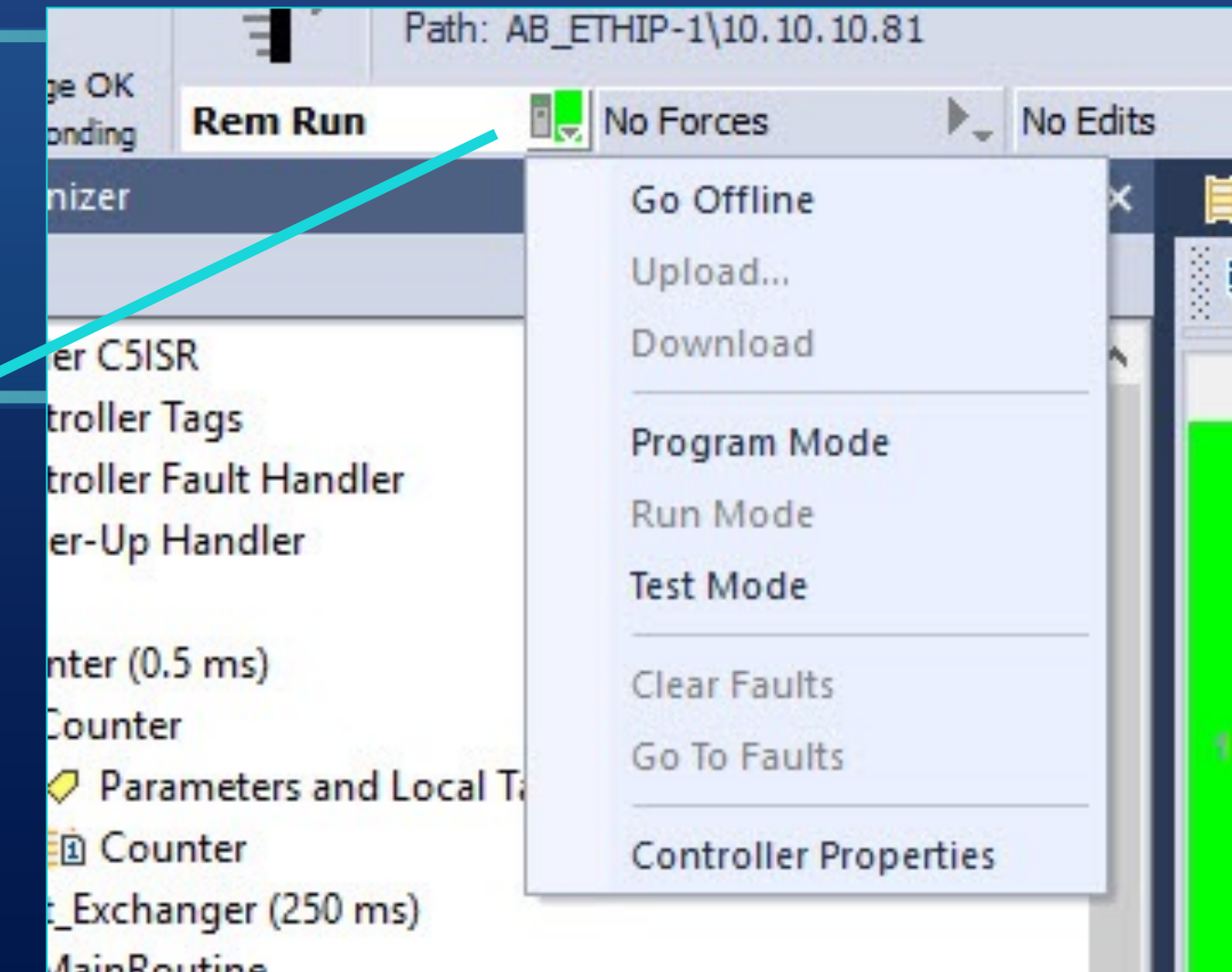
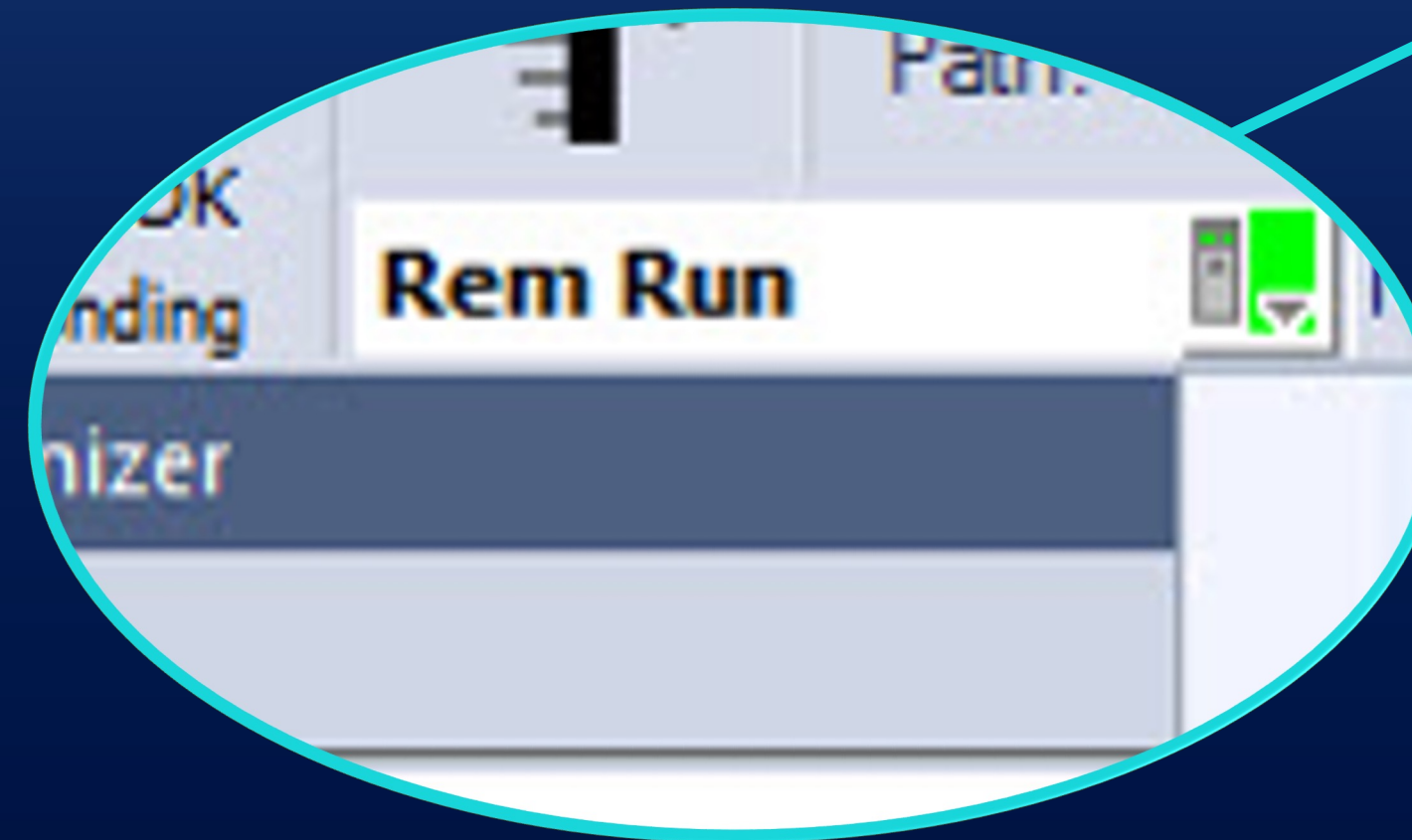
- Source
 - Host Events
 - Network Events
- Collection
 - Windows Event Log
 - Host Agent
 - Custom Script
 - Packet Capture

```
<13>1 2025-07-10T17:54:17Z WIN-0QB0CCERI5J Logix_Designer -
<134>1 2025-07-10T17:54:16Z MyComputer
FactoryTalk_Linux_SharedServices - ftdiag
[ftdiag@47349 user="NT AUTHORITY\\SYSTEM"]
Partial Import Online detected for 5069-
L306ER at 10.10.10.81.
```



Controller Mode Change (Local)

- Source
 - Host (ICS Device) Event
- Collection
 - Syslog



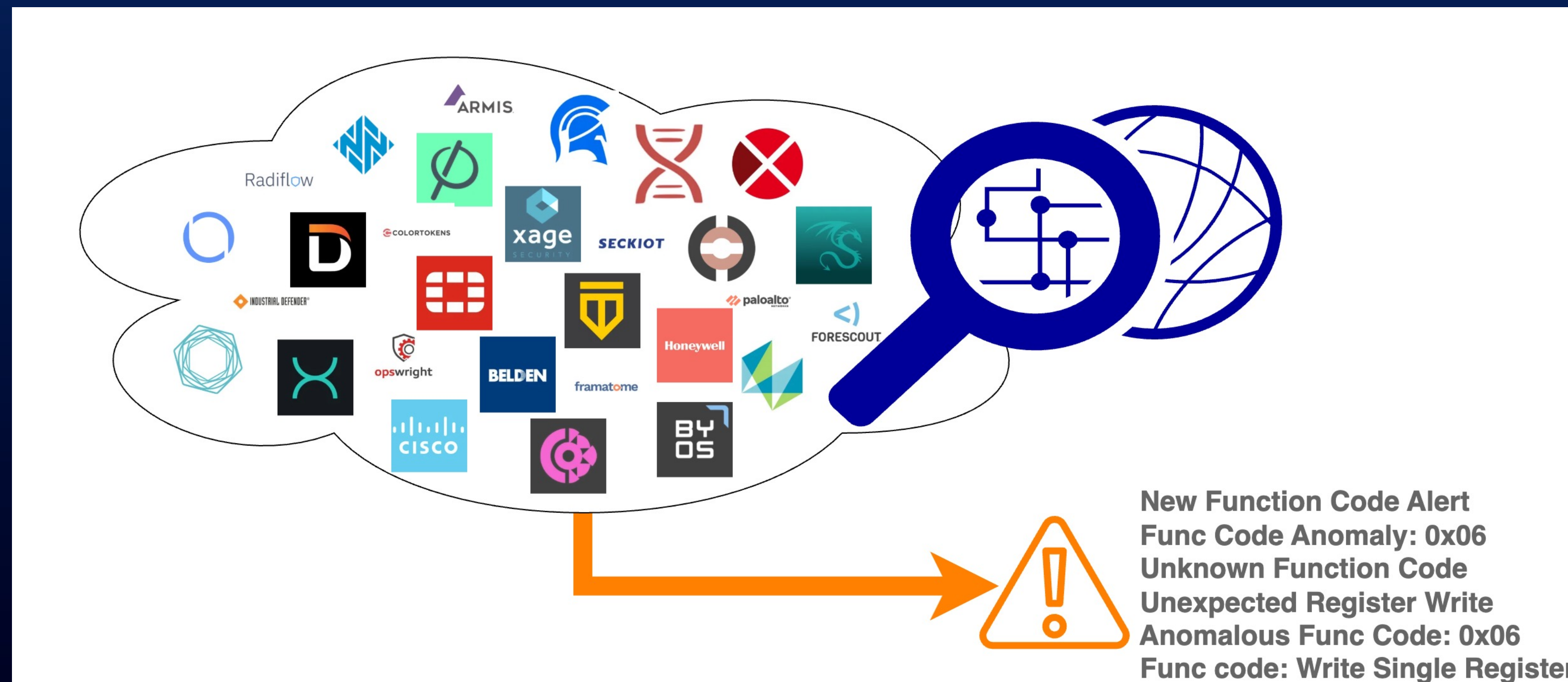
AD: Mode of controller has been changed to Program.

Context Matters

- As a singular event, attacker actions can appear as 'Normal' operations actions
 - i.e. partial download of project file
- Contextualizing across multiple events aligns with how operations typically interacts with the system
 - i.e. system issue, remote connection, program launch, connection to controller
- Not all 'typical' operator behaviors should be filtered out; useful for detection and forensics
 - i.e. verified new, one-off connection to controller
- The ability to create, share and modify ICS alerts empowers security operations alignment with nuances of the environment
 - i.e. ICS protocol usage – non-critical vs critical; read-only vs read-write; periodic

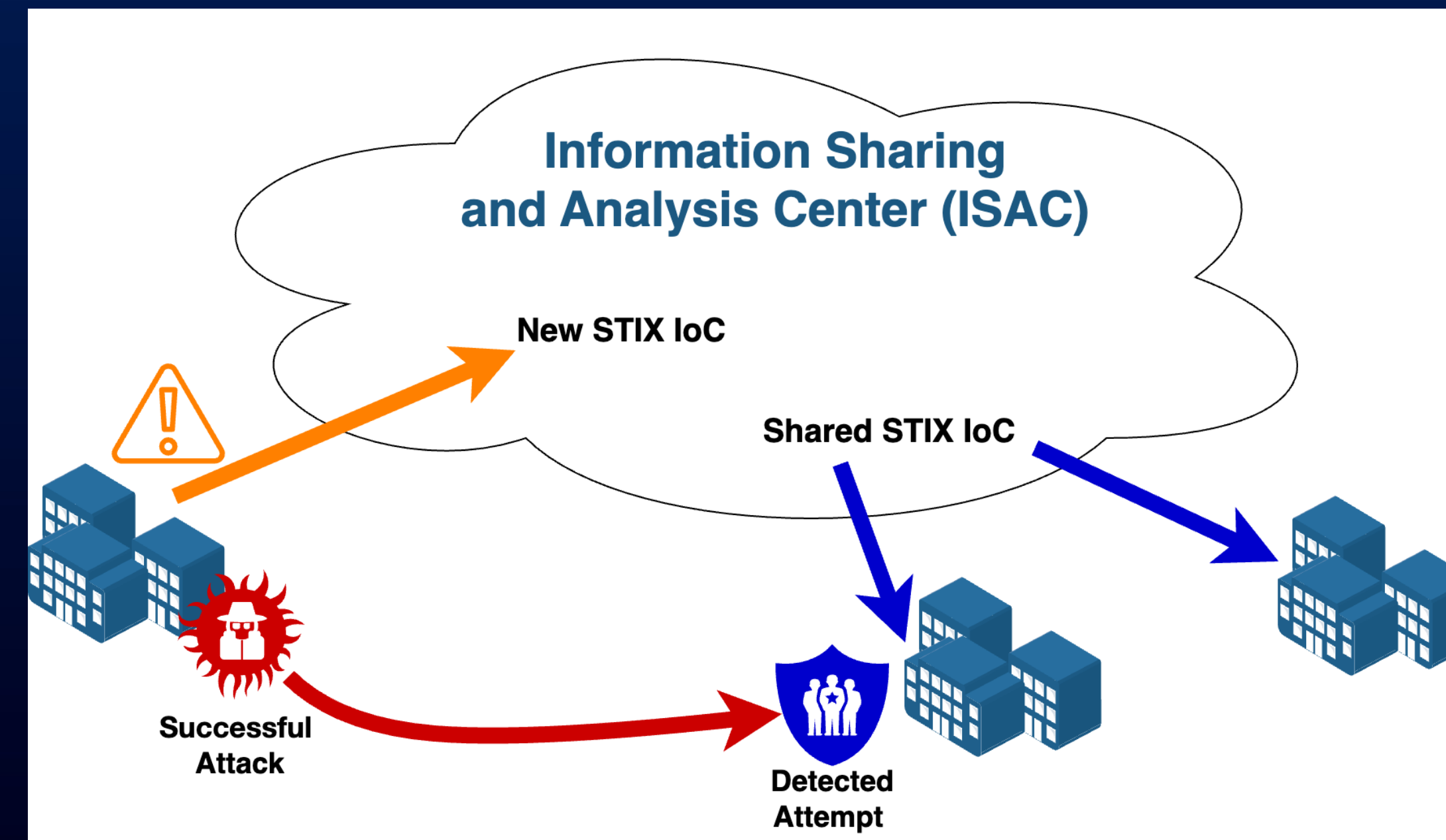
Control System Alerting Problem

- Vendors provide constantly evolving detections for network and host events
- Vendors detect similar activities, but uniquely name and describe

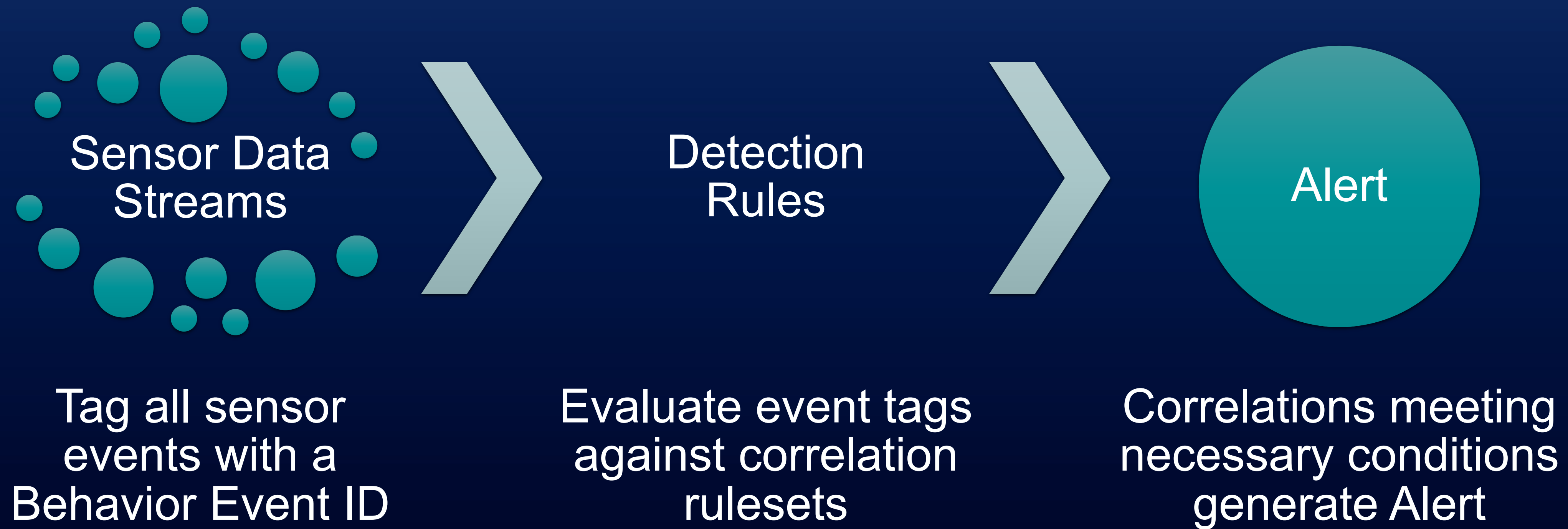


Cyber Threat Information Sharing Gap

- Structured Threat Information Expression (STIX) is a language and serialization format used to exchange cyber threat intelligence (CTI)
- CTI traditionally focused on Indicators of Compromise (IoC)
- Short lifespan, low level of effort to vary IoC signature
- Indicators of Behavior (IoB) being developed for STIX



Behavioral Alerting Sets for Control Systems



Behavior Events (BE)

BAS/CS Host Behaviors						BAS/CS Network Behaviors			
Access		File		Process		Intrusion Detection		Network Flow	
ACC01	Pass the Hash Attempt	FIL01	New File	PRO01	Process Change	IDS01	Network Conversation Anomaly	NET01	Link Traffic Increase
ACC02	Remote Login Attempt	FIL02	File Deletion	PRO02	Application Control Policy Block	IDS02	New Node	NET02	Link Traffic Decrease
ACC03	Successful Remote Login	Log		PRO03	New Command/Scripting Interpreter or Exploitation	IDS03	New Logical Link	NET03	Link Loss
ACC04	Admin Share Access	LOG01	Significant Timestamp Difference	PRO04	Suspicious Use of System Process	IDS04	OT Write Command	NET04	Stale Node
ACC05	New Service	LOG02	Decrease in logging	PRO05	Process Stopped	IDS05	OT Read Command	NET05	Network Scanning
ACC06	Scheduled Task	Peripheral		PRO06	Driver Loaded	IDS06	Function Code Anomaly	NET06	Network Interface Change
ACC07	User Created	USB01	USB Peripheral Connected	PRO07	Potential Process Injection	IDS07	Protocol Anomaly	B Behavir	
ACC08	User Added to Security Global Group	USB02	USB Peripheral Removed	PRO08	WMI Event Detected	IDS08	Configuration Change		
ACC09	User Added to Security Local Group	USB03	USB Storage Connected	PRO09	Security Audit Logs Cleared	IDS09	Hardware Change		
ACC10	Local Group Change	USB04	USB Storage Removed	PRO10	System Logs Cleared	IDS10	Network Interface Change		
ACC11	Explicit Login Attempt			PRO11	Event Logging Stopped	IDS11	External Conversation		
ACC12	Failed Login Attempt			PRO12	Outgoing Connection from Suspicious Process	IDS12	Network Scanning		
ACC13	New Login			PRO13	Remote Management Executed Suspicious Process	IDS13	System Elements Not Synchronized		
ACC14	File Share Write			PRO14	Remote Management Executed Suspicious	IDS14	Device State Change		
				PRO15	Remote Service Management	IDS15	Signature Based Alerts		
		PRO16	Named Pipe	IDS16	Process Variable Anomaly				

APLJOI
APPLIE

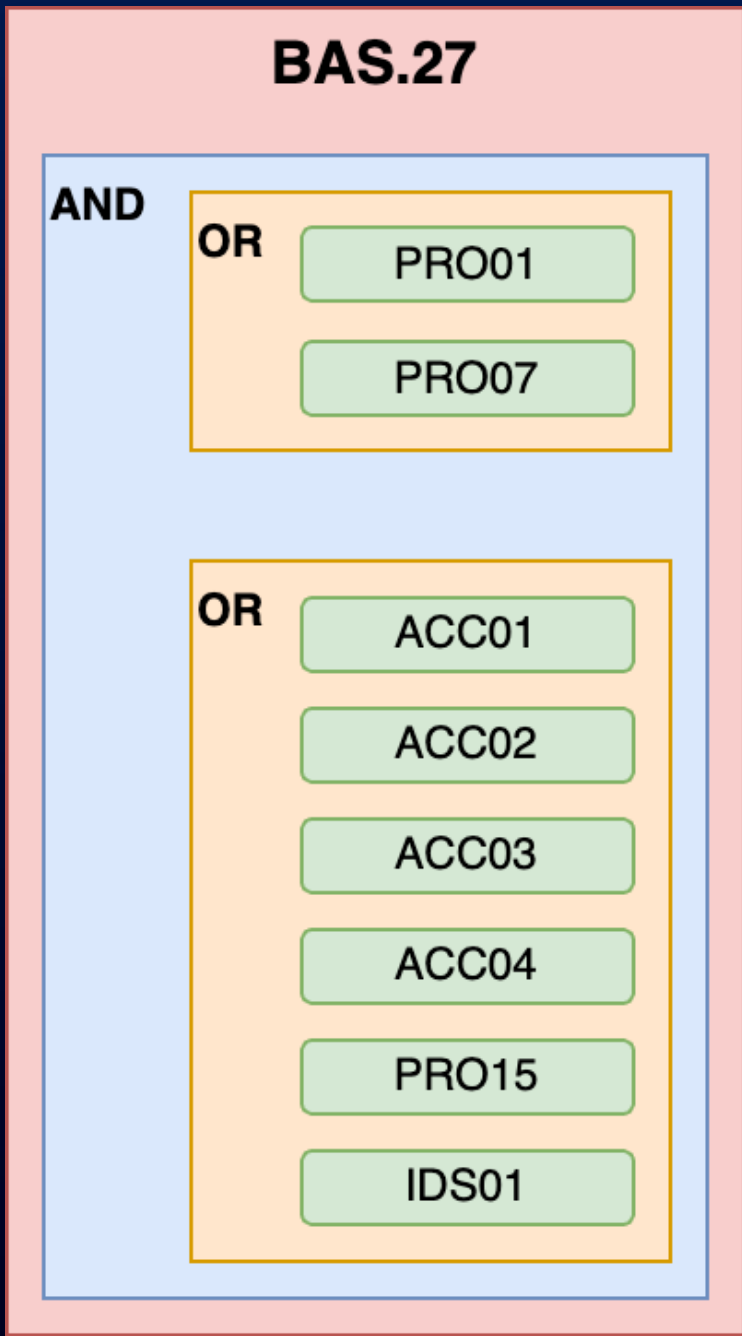
- Method for labeling sensor data with a standard set of behavior-based identifiers
- All source events and/or alerts are tagged with a single BE ID
- BE ID are used for downstream correlative processing

Rules

- Standardized format for describing alerting relationship between tagged behaviors
- Logical relationships between behaviors
- Host against which to correlate behaviors (Source, Target, Both)
- Time window for events to occur
- Severity Level (Low, Medium, High, Critical)

BAS.27	Potential Lateral Movement	An attacker may be conducting lateral movement on the network. Investigate recent network activity, particularly RDP and NTLM protocol traffic, and search for potentially malicious processes.
	(PRO01 PRO07) && (ACC01 ACC02 ACC03 ACC04 PRO15 IDS01)	
	PRO01	Process Change
	PRO07	Potential Process Injection
	PRO15	Remote Service creation from sc.exe
	ACC01	NTLM Login Attempt
	ACC02	RDP Authenticated Login
	ACC03	RDP Login
	ACC04	Admin Shares
	IDS01	Network Conversation Anomaly

Ref: <https://www.jhuapl.edu/work/projects-and-missions/bascs>



```
{
  "ID": "BAS.27",
  "Name": "Potential Lateral Movement",
  "Description": "An attacker may be conducting lateral movement on the network. Investigate recent network activity, particularly RDP and NTLM protocol traffic, and search for potentially malicious processes.",
  "Correlation": "Source",
  "Time": 5,
  "Severity": "Medium",
  "Logic": "(PRO01 || PRO07) && (ACC01 || ACC02 || ACC03 || ACC04 || PRO15 || IDS01)"
}
```

Implementing

- Rules are parsed into formats for SIEM or analytic engine of choice
- A parser combines Rule and system specific information into custom SIEM rules for each unique environment

BAS/CS Rule

```
{
  "ID": "BAS.27",
  "Name": "Potential Lateral Movement",
  "Description": "An attacker may be conducting lateral movement on the network. Investigate recent network activity, particularly RDP and NTLM protocol traffic, and search for potentially malicious processes.",
  "Correlation": "Source",
  "Time": 5,
  "Logic": "(PR001 || PR007) && (ACC01 || ACC02 || ACC03 || ACC04 || PRO15 || IDS01 || BAS/CS)"
}
```

Elasticsearch Rule

BAS.27 - Potential Lateral Movement

Created by: elastic on Feb 7, 2024 @ 13:52:35.785 Updated by: elastic on Feb 29, 2024 @ 07:56:29.485

Last response: ● succeeded at Mar 18, 2024 @ 10:19:42.166 Notify when alerts generated

About

Recent remote login attempts or other suspicious network activity have been detected. An unexpected process has also been identified. An attacker may be conducting lateral movement on the network. Investigate recent network activity, particularly RDP and NTLM protocol traffic, and search for potentially malicious processes.

Severity ● Medium

Risk score 21

Tags PRO01 PRO07 ACC01 ACC02 ACC03 ACC04 PRO15 IDS01 BAS/CS

Definition

Index patterns .alerts-security.alerts-*

EQL query

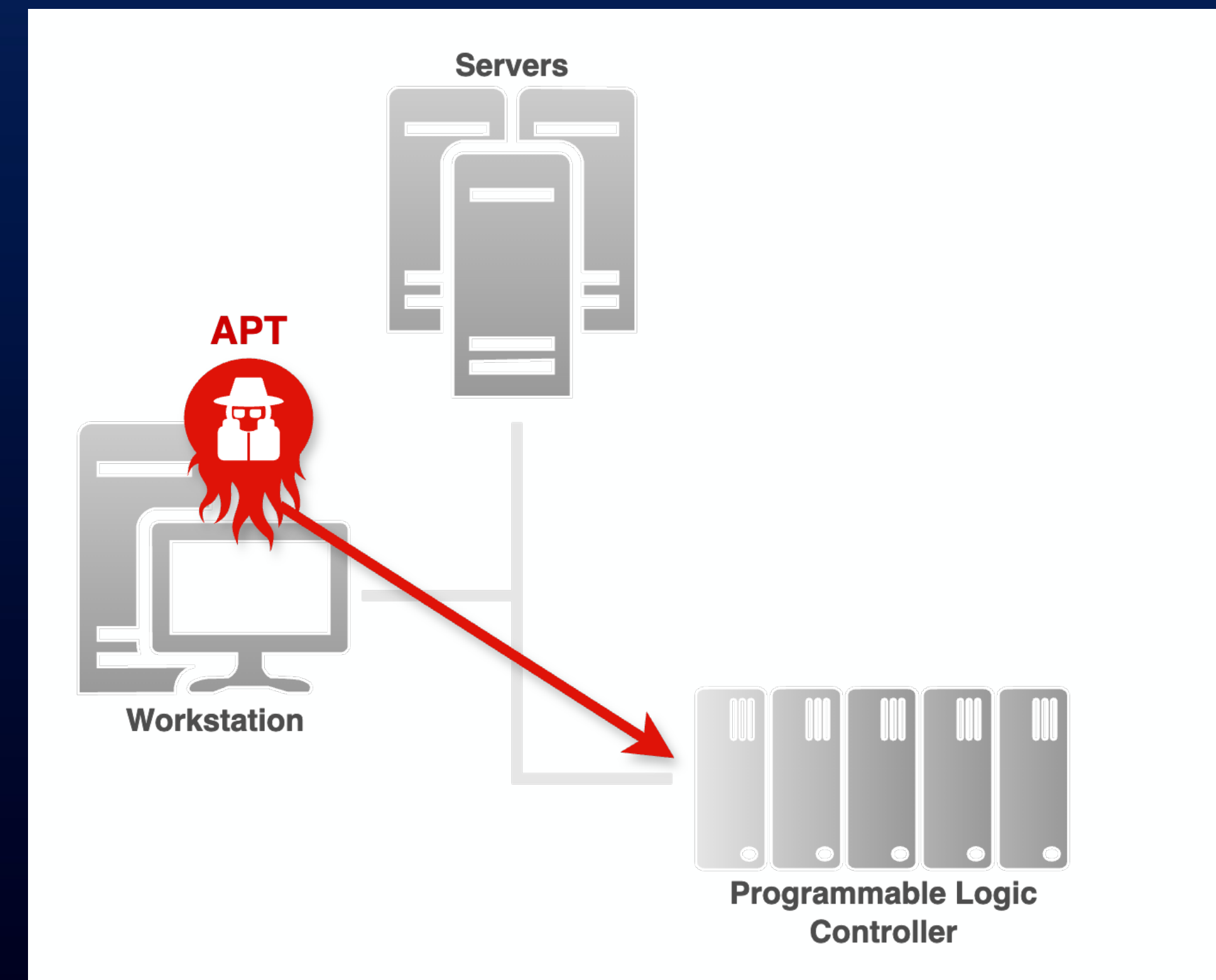
```
sample by host.hostname
[any where kibana.alert.rule.name : ("PRO01*", "PRO07*")]
[any where kibana.alert.rule.name : ("ACC01*", "ACC02*", "ACC03*", "ACC04*", "PRO15*", "IDS01*")]
```

Rule type Event Correlation

Timeline template None

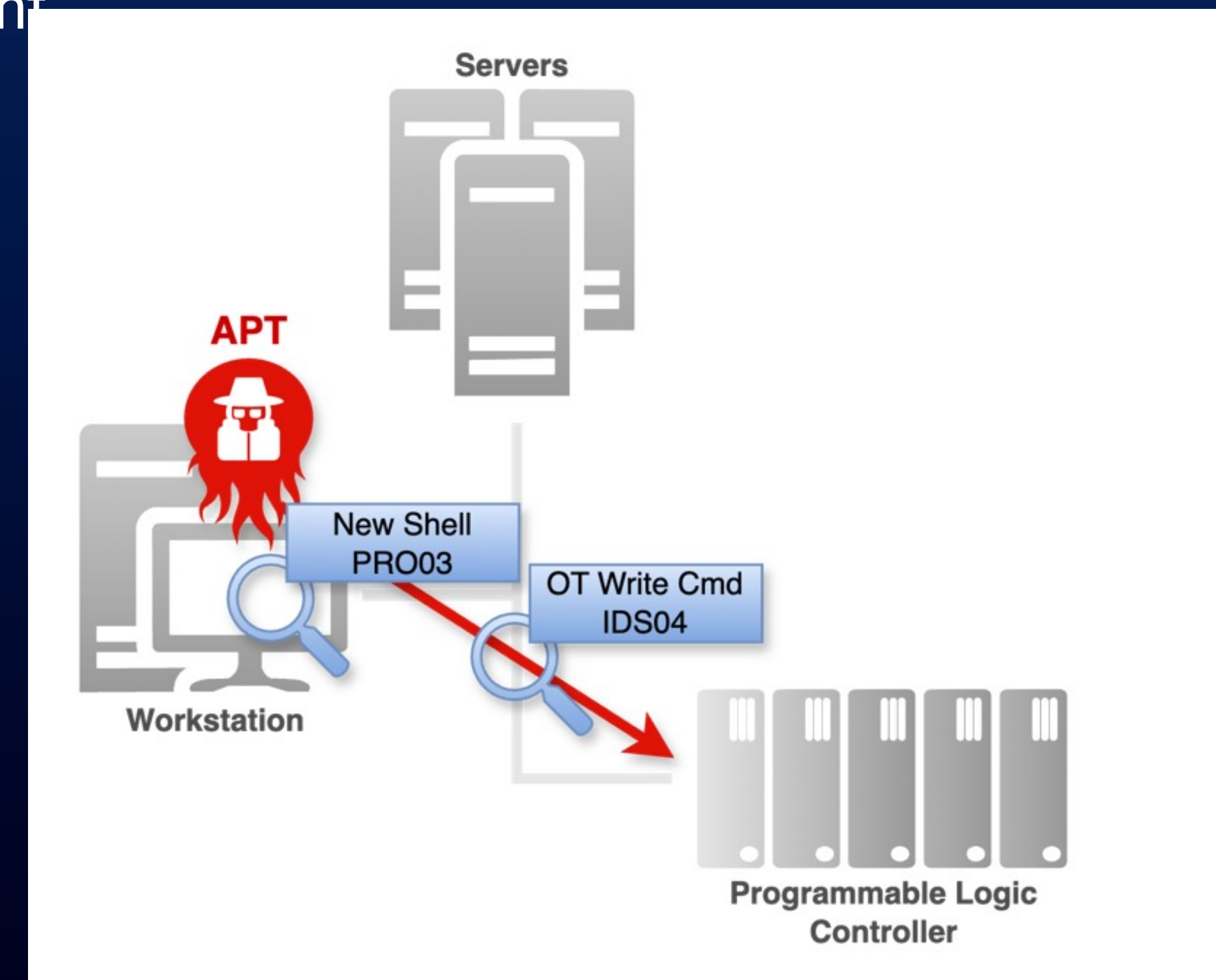
Simplified Detection Process - Ingest

- Ingest all sources of sensor data
- APT launches a cyber attack from a prepositioning foothold on a server
- Generates network traffic analyzed by a network IDS
- Generates windows log events



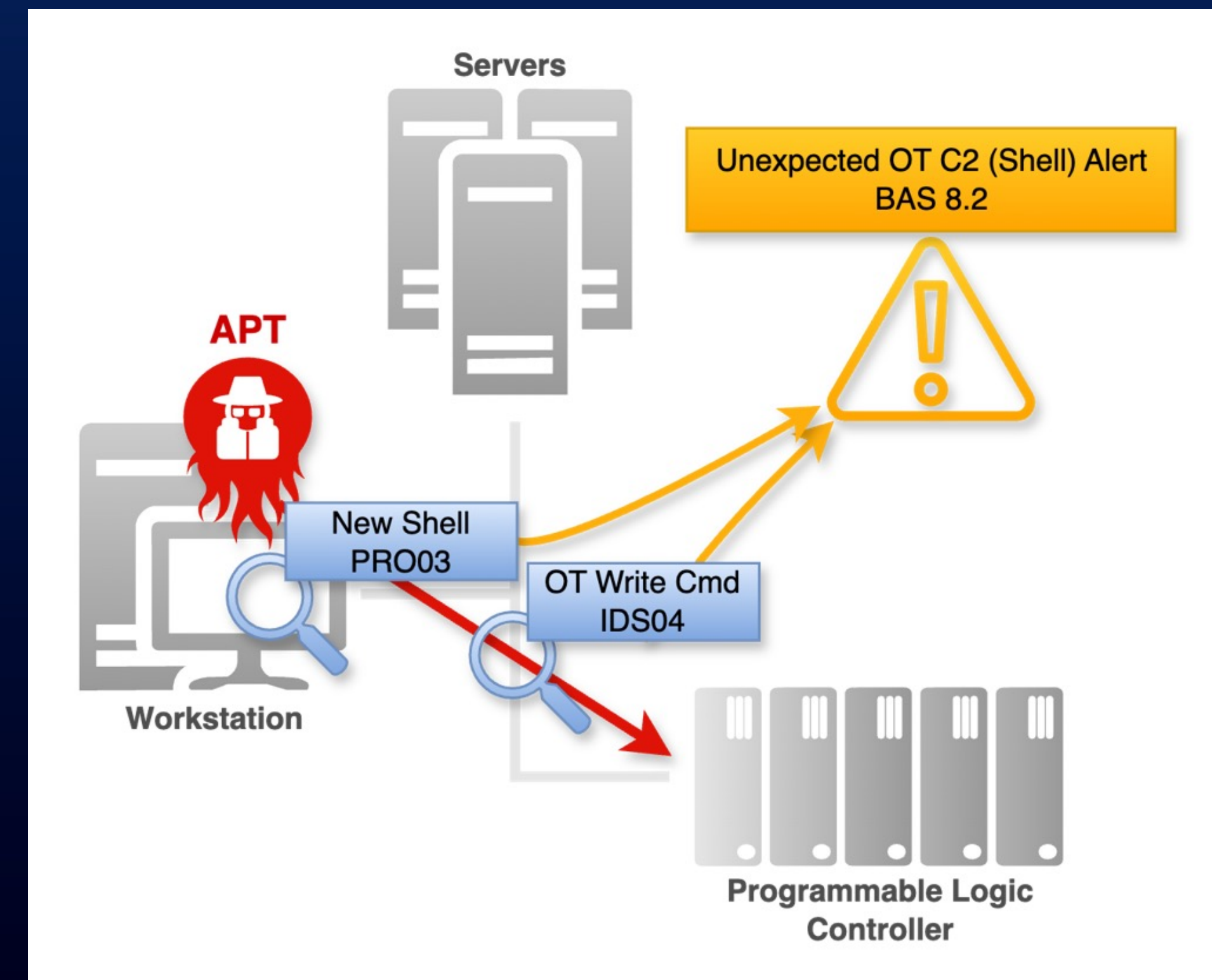
Simplified Detection Process - Ingest

- Tag security relevant sensor data identifying events
- Windows log events are examined and if relevant, tagged with a behavior ID
- Event generated by IDS is tagged with a behavior event
- Events are forwarded to SIEM



Simplified Detection Process - Ingest

- Alert on correlations between tagged events
- Rules in SIEM evaluate tagged events
- Alerts generated on rule hits



Maintain

Primary Methods to Maintain Log Aggregation and Visibility

- Maintain Configurations
 - Host Logs and Collectors
 - Network Collector
 - Collection and Analysis Tools
 - Verify Log Presence
- Testing
 - End Point Alert Testing
 - Network Alert Testing
- Track Deviations
 - Track Asset Changes
 - Proactively Identify New/removed Attack Paths
 - Management of Change
 - Architectural Changes
- Manage Alerts, Notifications and Response Workflows
- REMAIN AGILE – Monitor and incorporate threat reports and feedback from threat hunt activities

THANK YOU