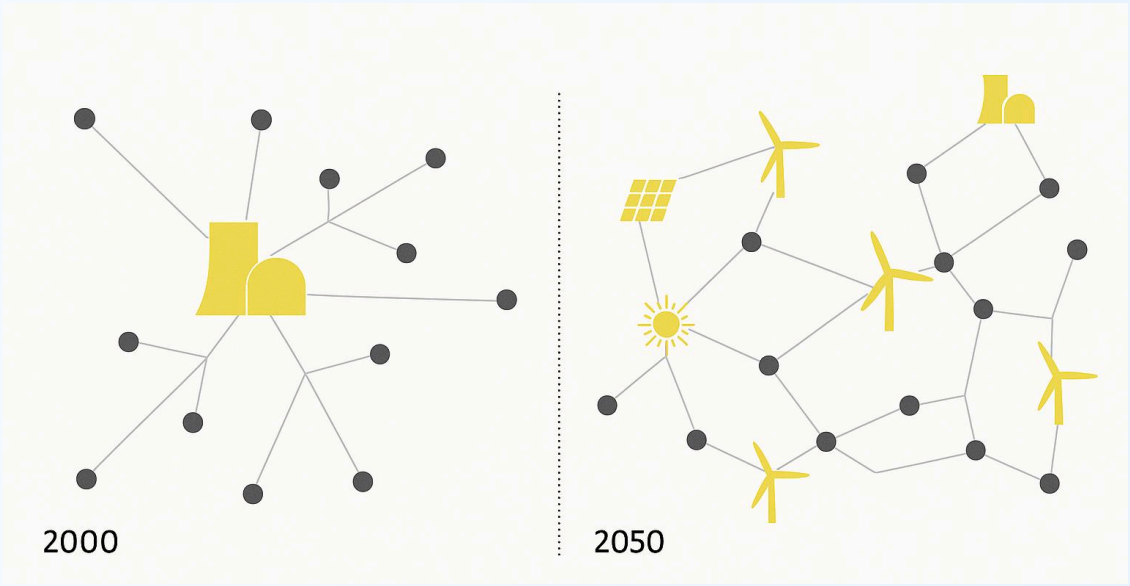


Cybersecurity for Solar Professionals

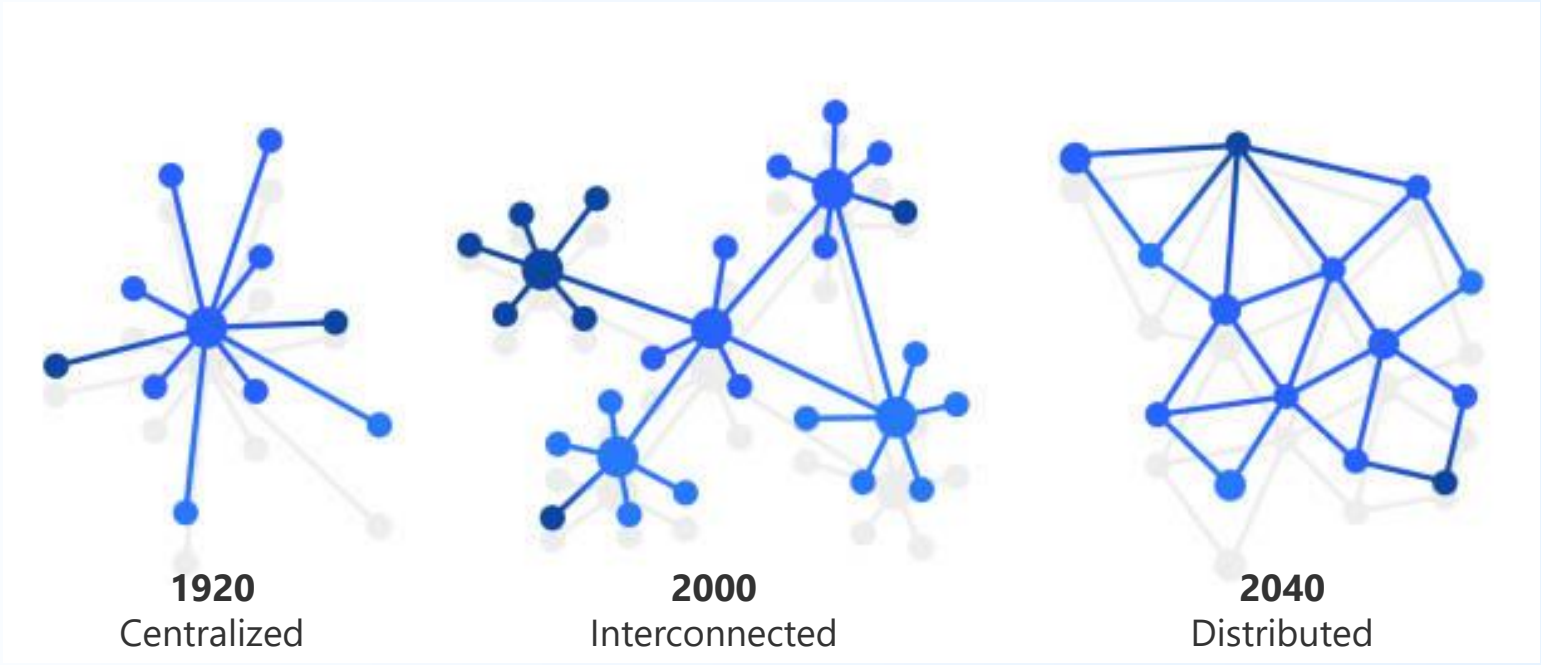
RE+ Deep Dive

Sep 2025, Las Vegas

The Grid is Changing

The **US Bulk Power** System is **in rapid change**

- **Consumers becoming producers** (homes, BESS plants, flexible loads & data centers)
- **5 million** solar installations powering America
- **40GWp** (residential only)
- **250GWp** total power



SOLAR DEFEND

A Paradigm Shift

Public Service Announcement:

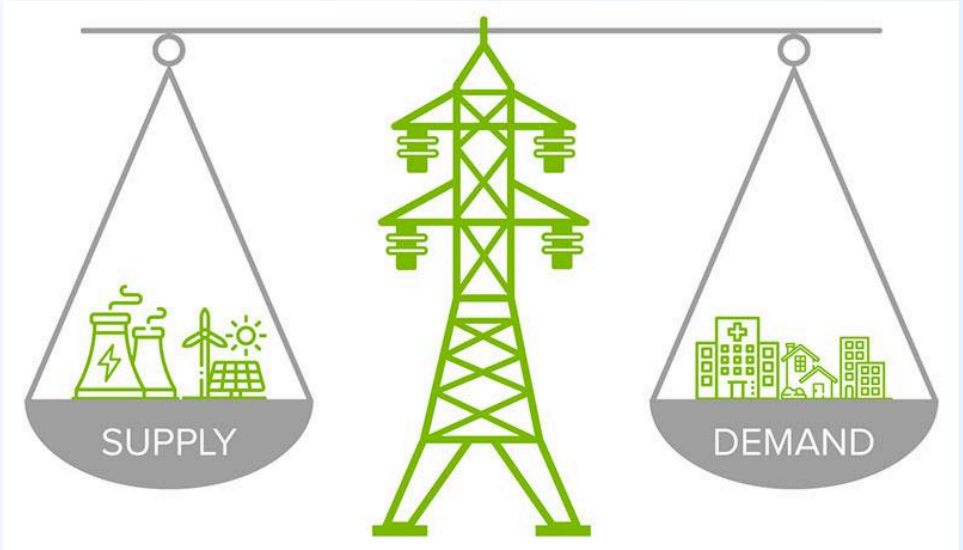
You are in the Critical Infrastructure Business!

A Paradigm Shift

Public Service Announcement:

You are in the Critical Infrastructure Business!

Power grids must stay balanced



SOLAR DEFEND

A Paradigm Shift

Public Service Announcement:

You are in the Critical Infrastructure Business!

A sudden shutdown of **2.2GW** triggered Spain's Blackout

- Less than 12 hours
- No cell phones, trains, lights

Reminder: There are **250GW** of solar in US

SOLAR DEFEND

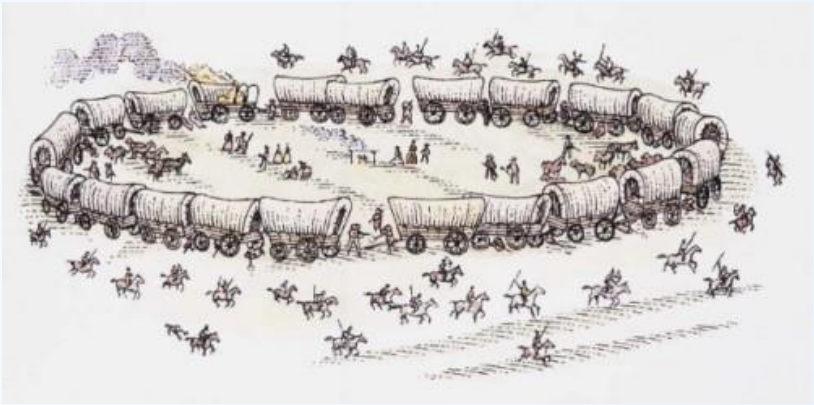
A Paradigm Shift

Public Service Announcement:

You are in the Critical Infrastructure Business!

Securing one big plant ≠ Securing many small plants…

≠



A Paradigm Shift

Public Service Announcement:

You are in the Critical Infrastructure Business!

We have lived through similar Paradigm Shifts:

SOLAR DEFEND

A Paradigm Shift

Public Service Announcement:

You are in the Critical Infrastructure Business!

We have lived through similar Paradigm Shifts:

The fittest survived

SOLAR DEFEND

A Paradigm Shift

Public Service Announcement:

You are in the Critical Infrastructure Business!

And now comes our turn

SOLAR DEFEND

What does this mean for your business?

The solar world is made of **three cyber stories:**

What does this mean for your business?

The solar world is made of **three cyber stories:**

1. Consumer solar

Residential

C&I

What does this mean for your business?

The solar world is made of **three cyber stories:**

1. Consumer solar
2. Utility solar

SOLAR DEFEND

What does this mean for your business?

The solar world is made of **three cyber stories:**

1. Consumer solar
2. Utility solar
3. Community solar *(<75MW)*

SOLAR DEFEND

What does this mean for your business?

The solar world is made of **three cyber stories:**

	Key players	Close parallels
1 Consumer solar	Residential Installers, C&I Installers, Inverter OEMs, VPP platforms & operators	EV Chargers, Smart Thermostats, Smart Meters
2 Utility solar	EPCs, Developers, IPPs, Asset Owners, PV Monitoring Companies, O&Ms, BESS Operators, Trackers	Wind farms, Hydro, Geothermal, Gas turbines
3 Community solar *(<75MW)*	In between Consumer & Utility	-

SOLAR DEFEND

What does this mean for your business?

Why are the **three cyber stories** distinct?

	Key players	Cyber Characteristics
1 Consumer solar	Residential Installers, C&I Installers, Inverter OEMs, VPP platforms & operators	Dozens of specialized companies Unregulated
2 Utility solar	EPCs, Developers, IPPs, Asset Owners, PV Monitoring Companies, O&Ms, BESS Operators, Trackers	Hundreds of companies Under NERC CIP
3 Community solar *(<75MW)*	In between Consumer & Utility	Hundreds of companies State level Cyber solutions gap

SOLAR DEFEND

What can go wrong?

Your business and customers may be targeted for ransom, data or to target the US grid

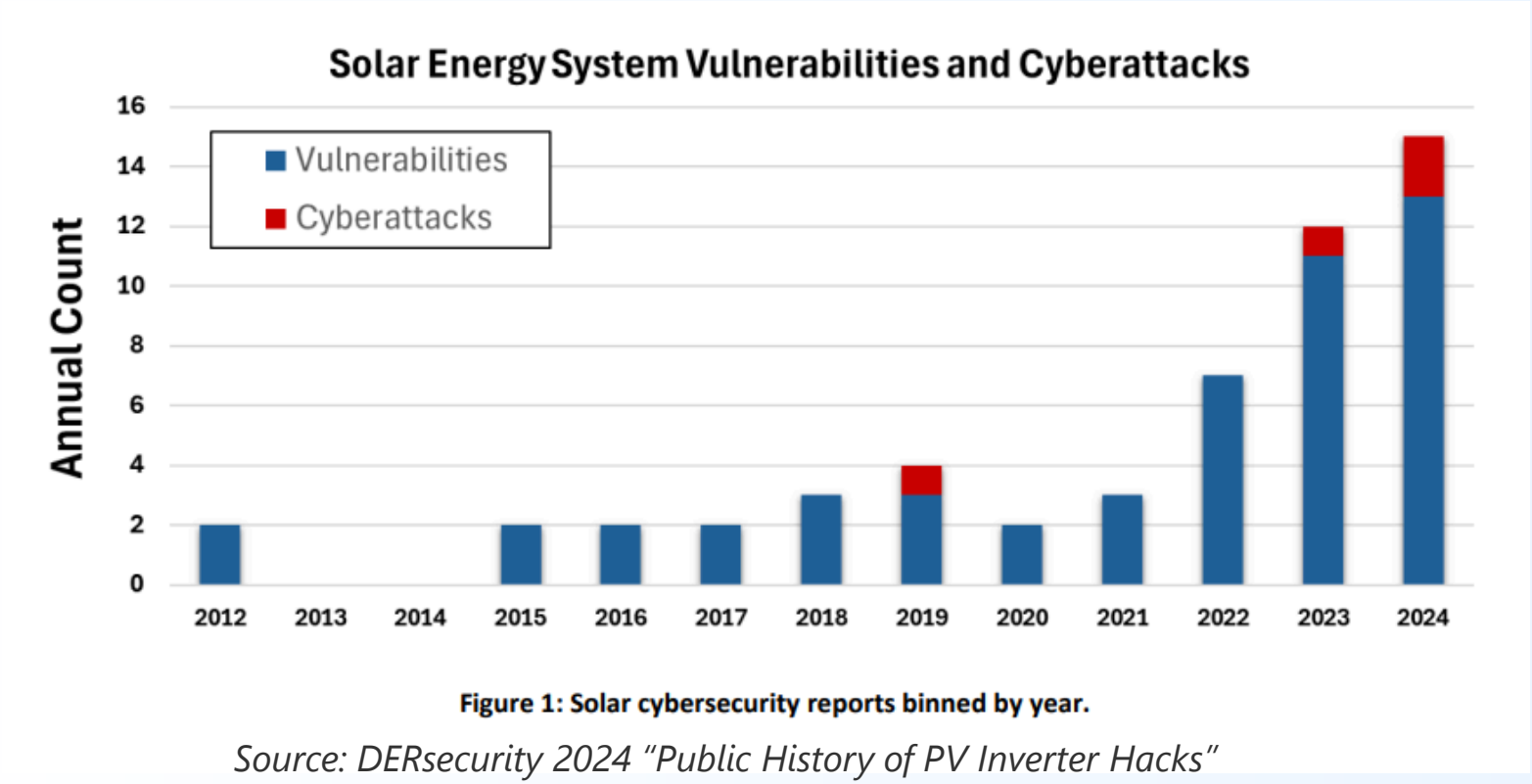


Figure 1: Solar cybersecurity reports binned by year.

Source: DERsecurity 2024 "Public History of PV Inverter Hacks"

SOLAR DEFEND

What can go wrong?

Your business and customers may be targeted for ransom, data or to target the US grid

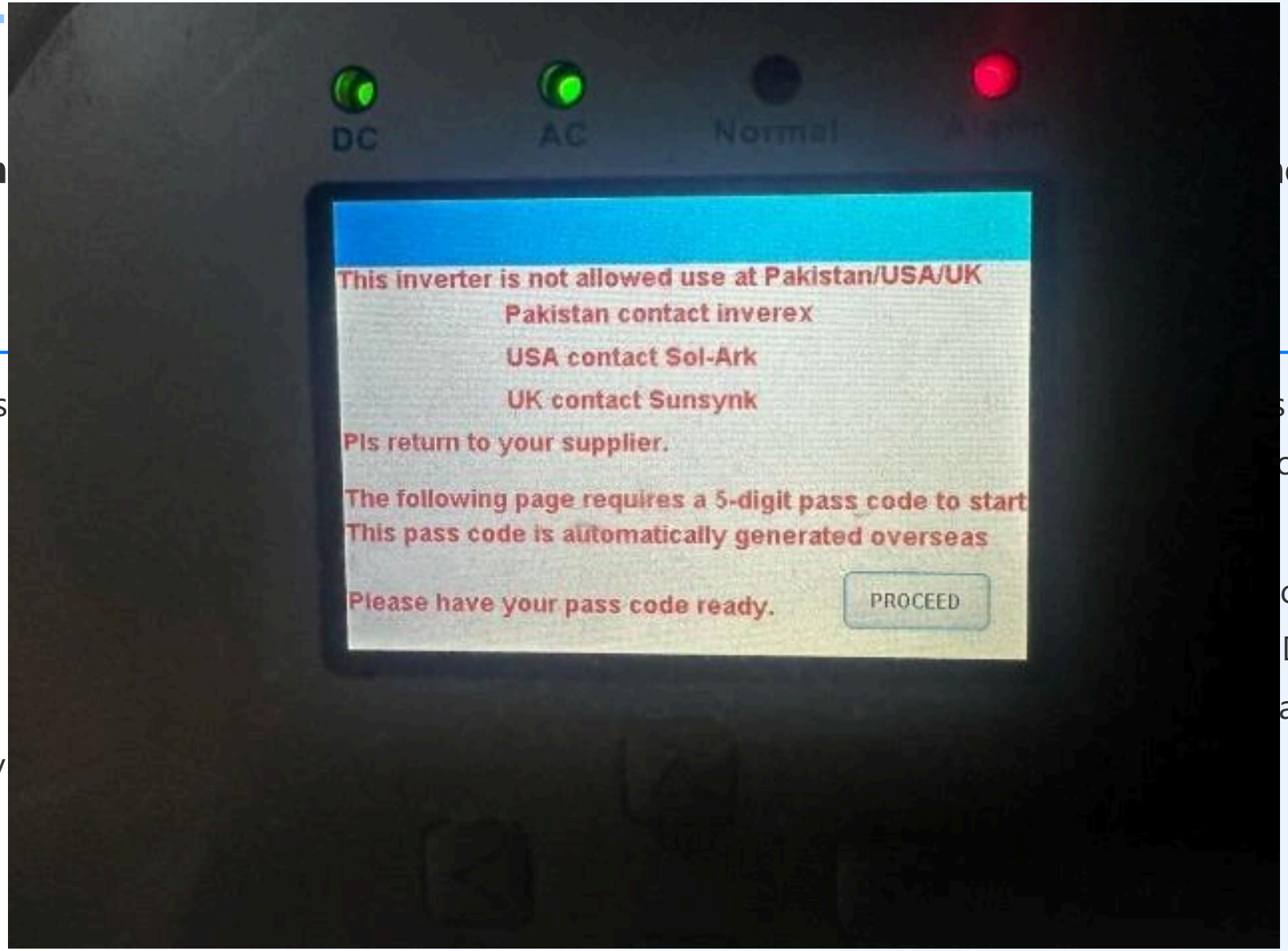
	Attack	Real world example
1 Consumer solar	Grid Damage; C&I Data Theft; Ransom Attack; Metering Fraud; Cyber-Physical (fires)	**2024**: "Bricked Residential Inverters Controversy" **2024**: "Cyble: Russian Ransom attack of European Hospitals" **2021**: "Waylon Grange: Generating Fake Clean Energy Credits"
2 Utility solar	Grid Damage; Site Downtime Ransom Attack;	**2019**: Utah's sPower Solar Plant Hacked **2020**: Japan SolarView Monitoring Device Hijacked **2023**: Denmark: Dozens of Solar Plants Breached by Russia
3 Community solar *(<75MW)*	-	

SOLAR DEFEND

What can go wrong?

Your busin **e US grid**

1. Consumer s … s Controversy”
2. Utility solar … ck of European Hospitals”
3. Community … Fake Clean Energy Credits”
   (<75MW) … cked … Device Hijacked … ants Breached by Russia



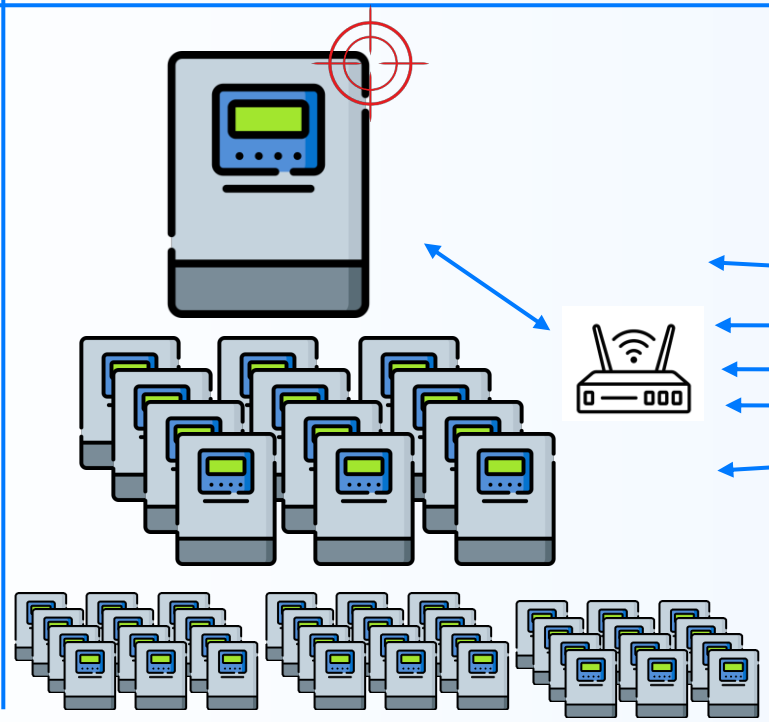
SOLAR DEFEND

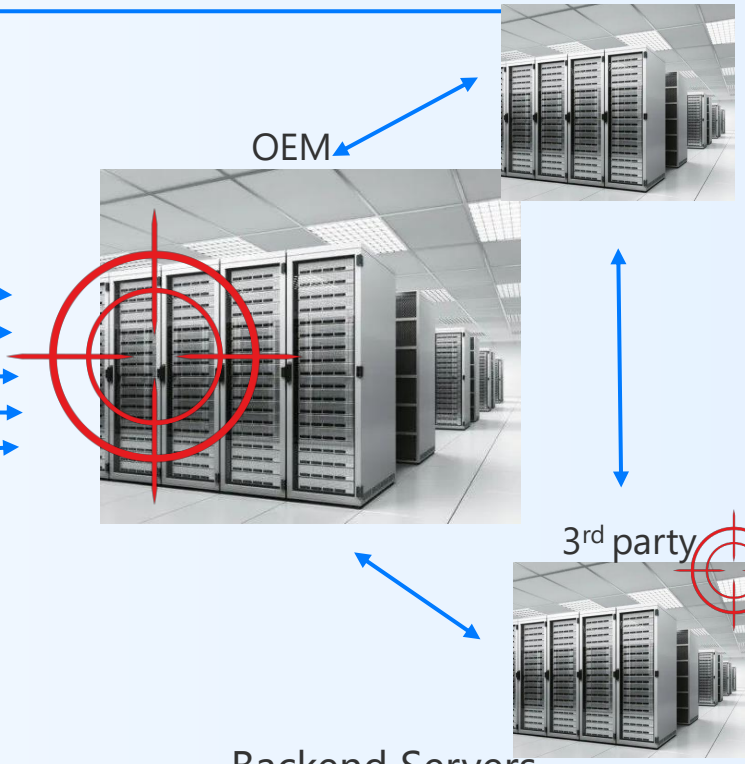
What hackers look for

Financial and political goals, and **easy hacks**

Typical product layout

1. **Consumer solar**
2. Utility solar
3. Community solar *(<75MW)*





Inverters

Communication lines

Backend Servers

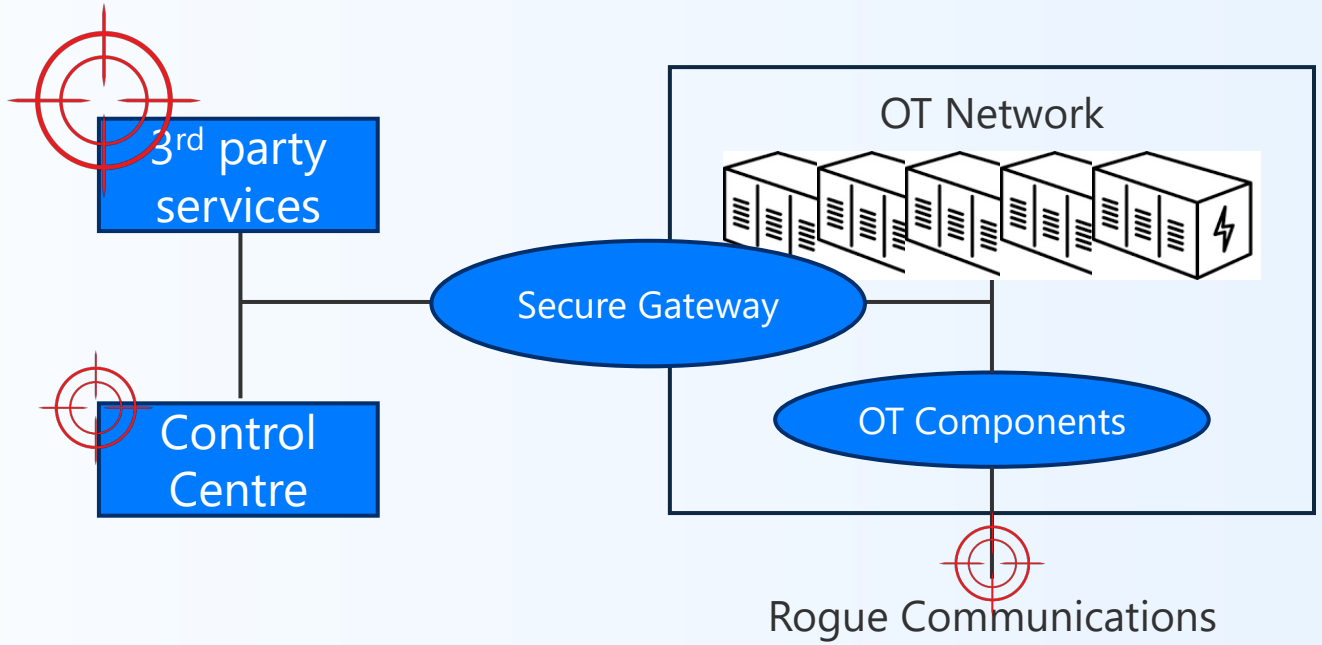
SOLAR DEFEND

What hackers look for

Financial and political goals, and **easy hacks**

Typical product layout

1. Consumer solar
2. **Utility solar**
3. Community solar *(<75MW)*



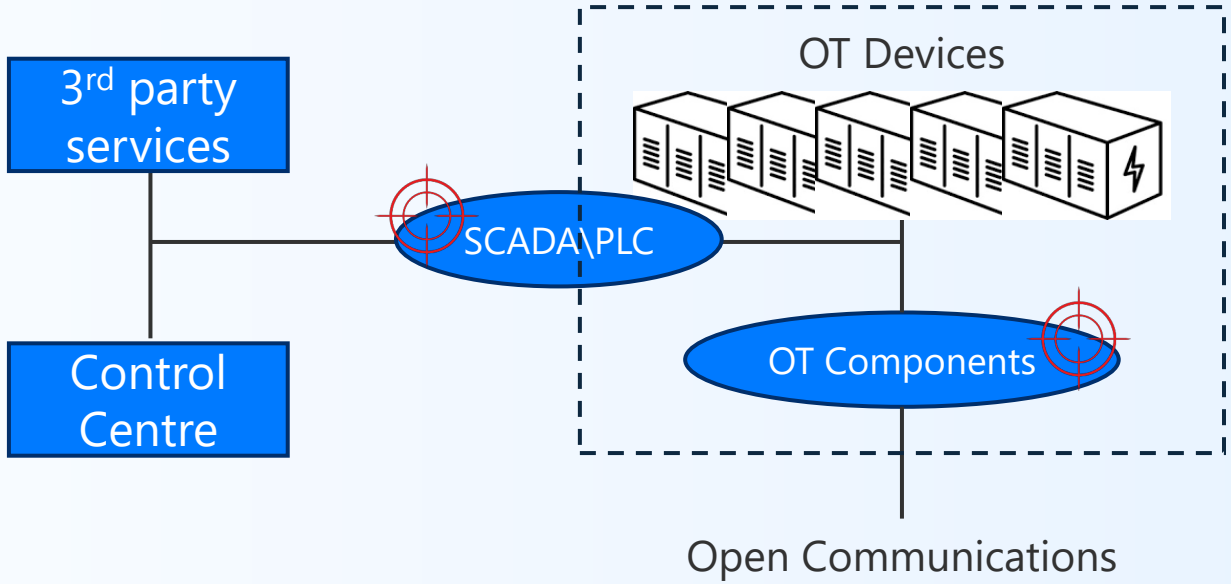
SOLAR DEFEND

What hackers look for

Financial and political goals, and **easy hacks**

Typical product layout

1. Consumer solar
2. Utility solar
3. **Community solar** ***(<75MW)***



SOLAR DEFEND

What regulations are coming

A global trend of increased regulation

	In America	Europe and Australia
1 Consumer solar	**NIST 8498** **UL 2941**	**Remote connection limitations** **CER Cybersecurity Roadmap** **Cyber Resilience Act**
2 Utility solar	**NERC CIP 15** **IEEE 1547.3**	**NIS 2** **Network Code on Cybersecurity**
3 Community solar *(<75MW)*	**IBR registration requirements**	**India MNRE and Hungary FEAK reporting requirements**

SOLAR DEFEND

So, what can you do TODAY to stay ahead

The Lion

&

The Dentist

What can you do TODAY to stay ahead

Start with the basics:

- Choose equipment **manufacturers you can trust**
- Check who has **remote control** of your asset
- Change all **default passwords**

Always stay ahead of the pack

SOLAR DEFEND

What can you do TODAY to stay ahead

Start with the basics:

- Choose equipment **manufacturers you can trust**
- Check who has **remote control** of your asset
- Change all **default passwords**

Always stay ahead of the pack

For Bespoke Consultation – reach out today

Uri Sadot
Managing Director
SolarDefend
uri.sadot@solardefend.eu
www.solardefend.eu
LinkedIn

Summary

- You are in the critical infrastructure business!
- Bad guys may try and compromise your systems, or your customers
- Regulation is on its way
- Simple steps can solve 90% of the problem
- Follow SolarDefend on Linkedin

SOLAR DEFEND

Questions?

OT Cybersecurity Strategies for Critical Infrastructure

Ahmik Hindman – Sr. Network & Security Solutions Consultant
B.S. EE, MBA-IT, CISSP, CCSP, CCNA, Security+, Fortinet Certified Associate
ISA/IEC 62443 Cybersecurity Expert
abhindman@rockwellautomation.com
https://www.linkedin.com/in/ahmik-hindman/

CYBERCRIME PAYS – **AND IT'S ONLY GETTING WORSE**

Industrial companies are prime targets

Legacy unpatched infrastructure, IoT, insider threats and a lack of skilled resources create vulnerabilities.

In 2024...

80% Of manufacturing Organizations reported a loss of revenue due to security incidents.*

Cybercrime costs accelerate...

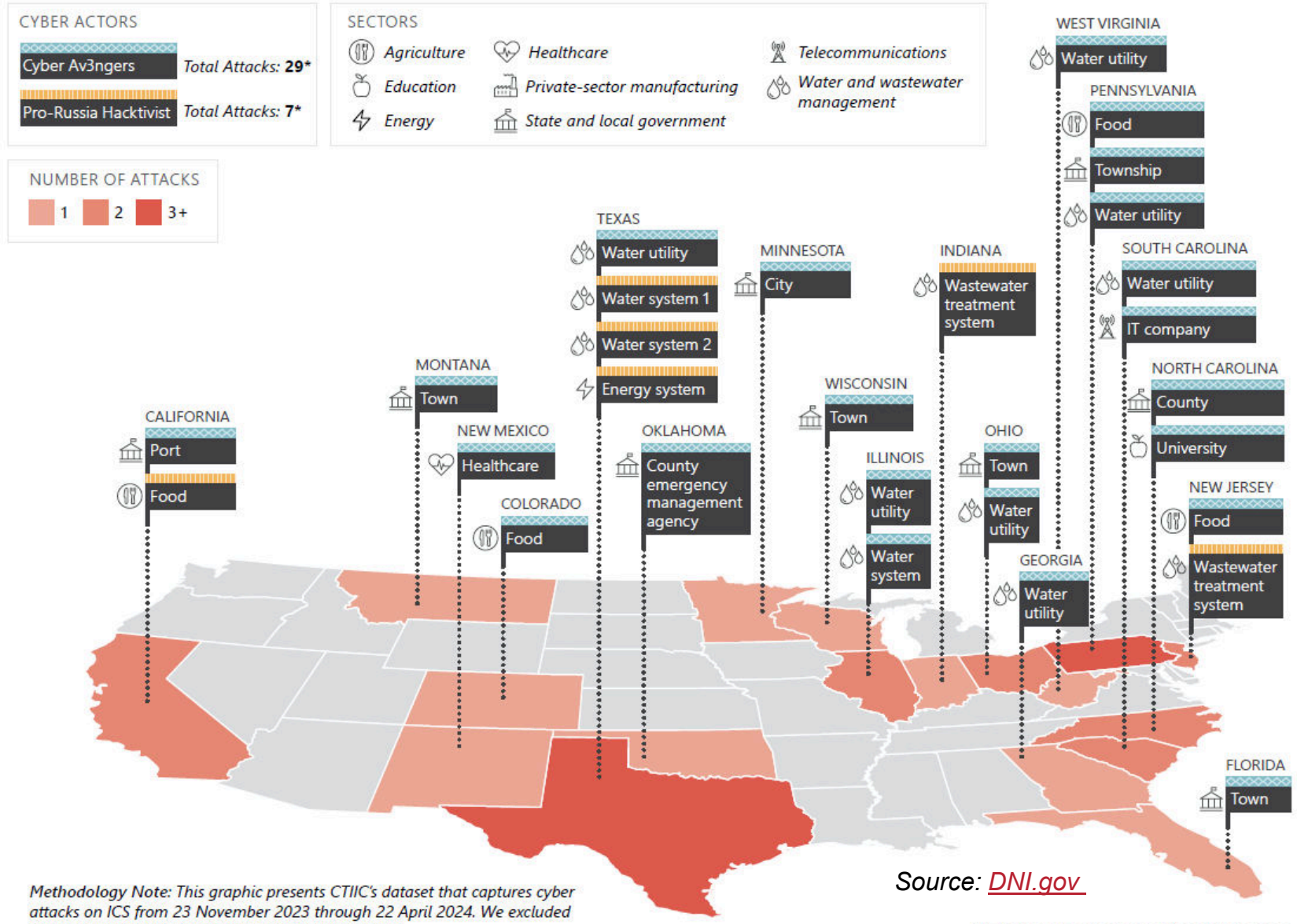
$13.8T cybercrime is expected to surge in the next four years, rising from $9.22 trillion in 2024 to $13.82 trillion by 2028*

* Dragos 2025 OT/ICS Cybersecurity Report—Year in Review * *Statista.com*

Industrial Automation Control Systems are Under Attack

Reported Cyber Attacks on US ICS systems (11-23-23 – 4-22-24) – Ransomware attacks excluded

- Iran-affiliated and pro-Russia cyber actors access to and manipulated critical US industrial control systems (ICS)
- Food and Agriculture, Healthcare, and Water and Wastewater sectors in late 2023 and 2024
- "These attacks highlight a potential public safety threat and an avenue for malicious cyber actors to cause physical damage and deny critical services. Outdated software, poor password security, the use of default credentials, and limited resources for system updates render ICS devices vulnerable to compromise"



Methodology Note: This graphic presents CTIIC's dataset that captures cyber attacks on ICS from 23 November 2023 through 22 April 2024. We excluded ransomware attacks on critical infrastructure entities.

Source: DNI.gov

*Including seven attacks at additional US locations.

Industrial Automation Control Systems are Under Attack

FBI Director Warns of CCP escalation and targeting our Critical Infrastructure

"When I described the CCP as a threat to Americans' safety a moment ago, I meant that in some ways quite literally. There has been far too little public focus on the fact that PRC [People's Republic of China] hackers are targeting our critical infrastructure—our water treatment plants, our electrical grid, our oil and natural gas pipelines, our transportation systems—and the risk that poses to every American requires our attention now." - Christopher Wray, FBI Director

".. China's hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities. If or when China decides the time has come to strike, they're not focused solely on political or military targets. We can see from where they position themselves, across civilian infrastructure, that low blows aren't just a possibility in the event of a conflict. Low blows against civilians are part of China's plan." – Christopher Wray, FBI Director

Source: FBI News – Jan 31, 2024 – Openings Statement to House Select Committee

Nation State ICS Malware – FrostyGoop

Rockwell Automation

expanding **human possibility**®

Nation State ICS Malware – FrostyGoop

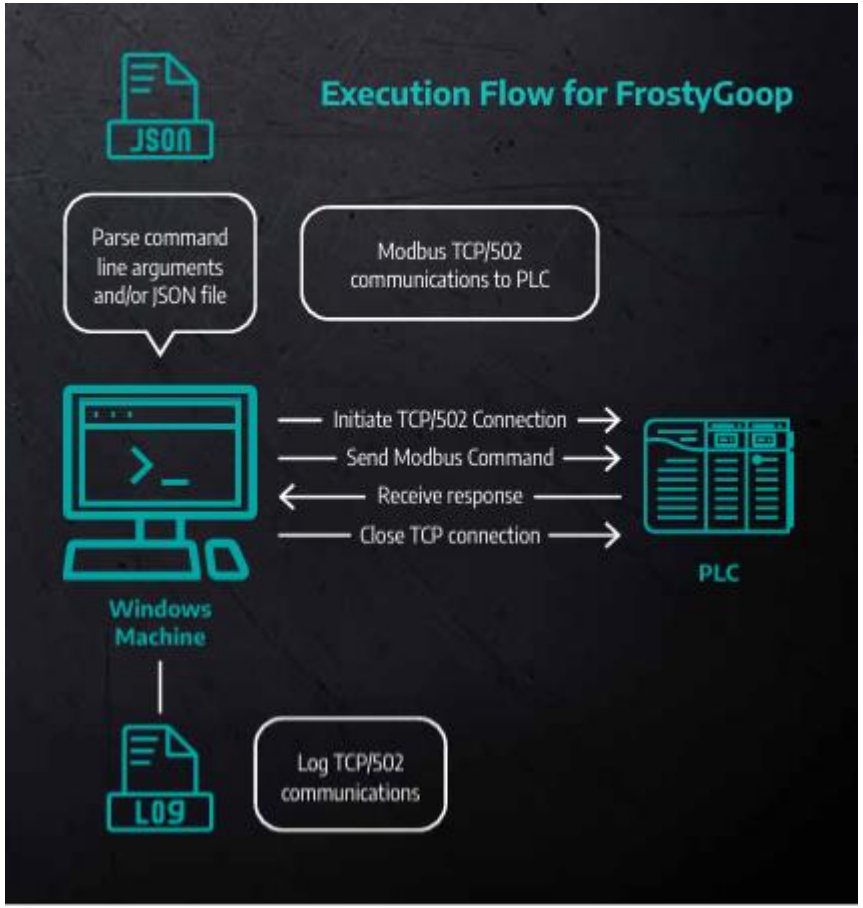
Example of a recent ICS attack identified by Dragos – Overview

- In January, 2024 with sub-zero temperatures in Lviv, Ukraine, a cyber attack targeting Modbus controllers disrupted the central heating for more than 600 apartment buildings

Nation State ICS Malware – FrostyGoop

Example of a recent ICS attack identified by Dragos – ICS Malware Capabilities

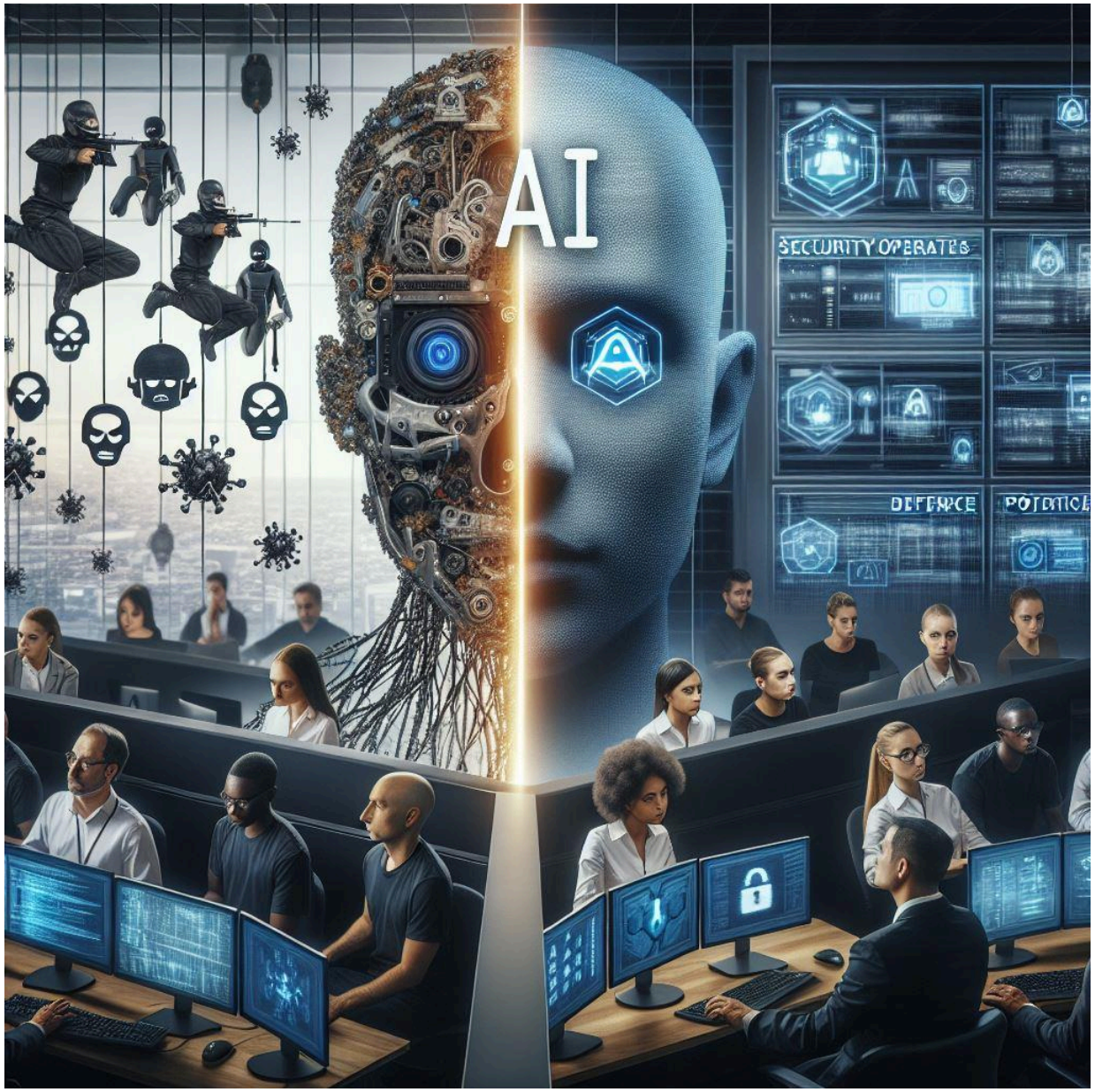
- FrostyGoop ICS Malware Capabilities
- Accepts optional command line execution arguments.
- Uses separate configuration files to specify target IP addresses and Modbus commands.
- Communicates with ICS devices via Modbus TCP protocol.
- Sends Modbus commands to read or modify data on ICS devices.
- Logs output to a console or JSON file.



Graphic from: Dragos 2025 OT/ICS Cybersecurity Report—Year in Review

Dragos FrostyGoop Intel Brief

Weaponized AI

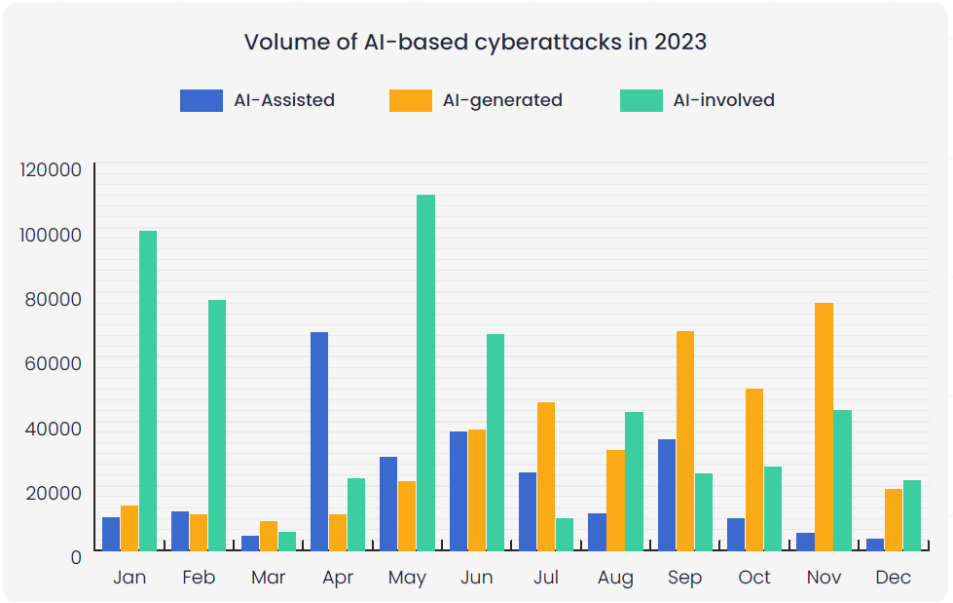


Defensive AI

AI: Double-edged Sword in Cybersecurity

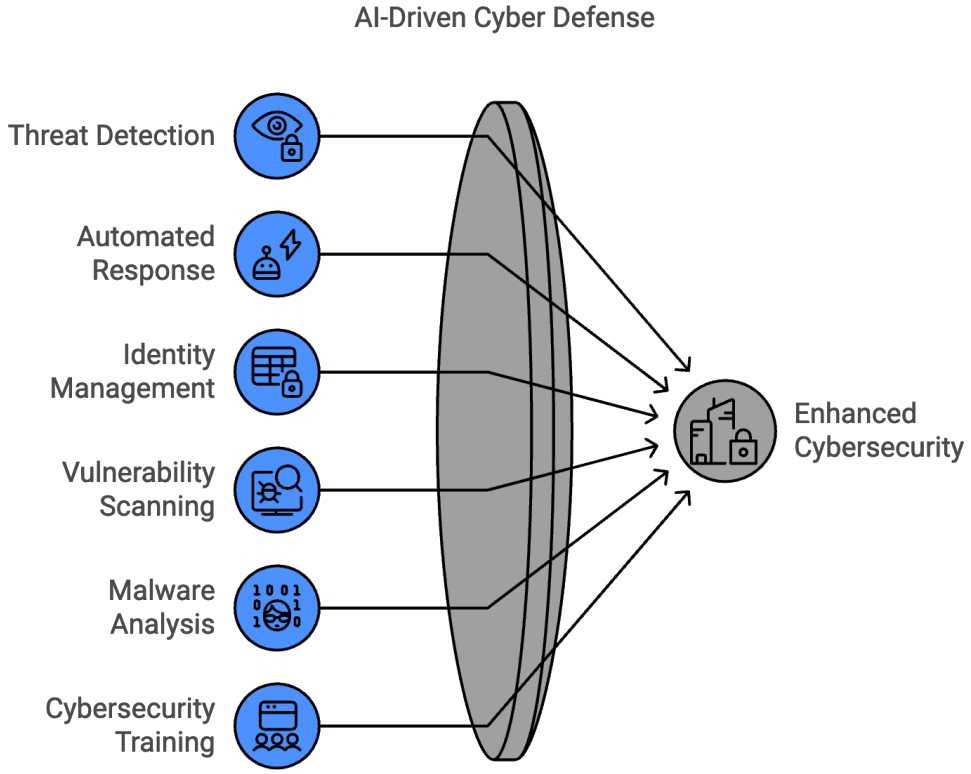
Weaponized AI:

- 2023 saw numerous AI-modified malware in the wild with experimental, aiming for stealthier, more potent vectors.
- AI-based tampering of existing malware is an ongoing trend.
- Complete profiles of target employees are created in days, including phishing and deep fake messages.



Sectrio 2024 OT & IoT Threat Landscape Assessment and Analysis Report

Defensive AI:



DataProt, 1-16-2025

NATIONAL ARCHIVES

FEDERAL REGISTER

The Daily Journal of the United States Government

Rule

Critical Infrastructure Protection Reliability Standard CIP-015-1-Cyber Security-Internal Network Security Monitoring

A Rule by the Federal Energy Regulatory Commission on 07/02/2025

DATES:

This action is effective September 2, 2025.

NERC – CIP Updates

New Addition to the NERC – CIP

CIP-002: Identification and Categorization of BES Cyber Systems
Defines which assets are critical and must be protected.

CIP-003: Security Management Controls
Requires policies, governance, and management oversight for CIP compliance.

CIP-004: Personnel & Training
Mandates background checks, training, and access management for personnel with access to BES Cyber Systems.

CIP-005: Electronic Security Perimeter(s)
Requires the creation and protection of electronic security perimeters (ESPs) around critical cyber assets including Remote Access

CIP-006: Physical Security of BES Cyber Systems
Requires physical security controls (e.g., card access, cameras) for critical cyber assets.

CIP-007: System Security Management
Covers patch management, malware protection, security event monitoring, and system hardening.

CIP-008: Incident Reporting and Response Planning
Requires incident response plans and timely reporting of cybersecurity incidents.

CIP-009: Recovery Plans for BES Cyber Systems
Mandates disaster recovery and business continuity plans for critical cyber assets

.

CIP-010: Configuration Change Management and Vulnerability Assessments
Requires change management, configuration monitoring, and regular vulnerability assessments.

CIP-011: Information Protection
Mandates protection of sensitive BES cyber system information during storage, transit, and disposal.

CIP-012: Communications between Control Centers
Requires protection (e.g., encryption) of data exchanged between control centers.

CIP-013: Supply Chain Risk Management
Mandates risk management practices for the supply chain of BES Cyber Systems.

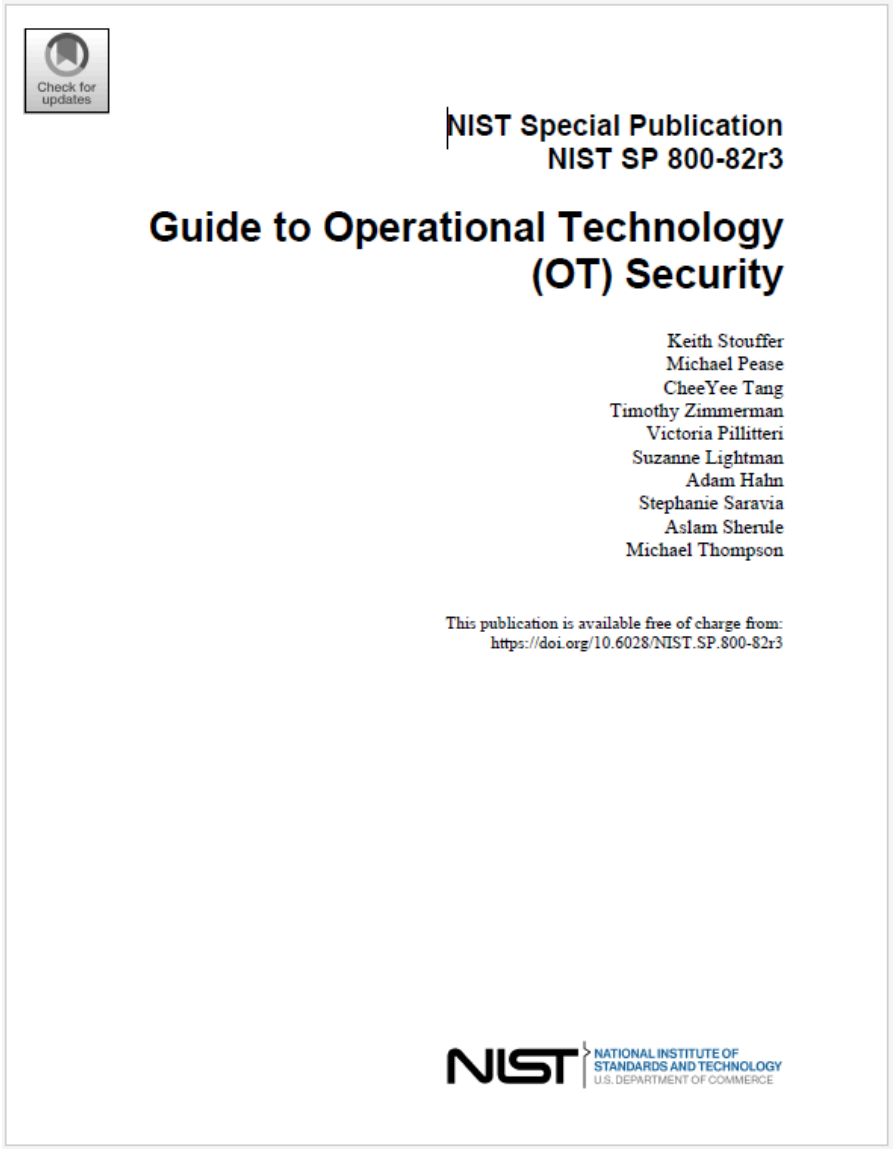
CIP-014: Physical Security
Requires risk assessments and physical security plans for critical substations and control centers.

CIP-015: Internal Network Security Monitoring (INSM)
Newly approved and effective September 2025, with implementation deadlines extending to 2028.

Requires utilities to implement internal network security monitoring for high and medium impact BES Cyber Systems, focusing on detecting anomalous activity within the Electronic Security Perimeter (east-west traffic monitoring).

ICS Cybersecurity Guidelines, Standards and Frameworks

NIST 800-82-r3 – Guide to Operational Techology (OT) Security



Purpose: Provides comprehensive guidance for securing OT systems (ICS, SCADA, DCS, IIoT, building automation) with unique safety, reliability, and performance needs.

- **Expanded Scope:** Now covers all OT, not just ICS; aligns with NIST CSF and SP 800-53.
- **OT Security Challenges:** Increased IT/OT connectivity raises cyber and physical risks.
- **Risk Priorities:** Safety and availability take precedence; incidents can cause real-world harm.
- **Defense-in-Depth:** Emphasizes layered security—segmentation, firewalls, DMZs, strict access.
- **Cybersecurity Program:** Requires cross-functional teams, OT-specific policies, and training.
- **Risk Management:** Applies NIST RMF with tailored, risk-based controls for OT.
- **Incident Response & Recovery:** Stresses robust detection, response, and recovery planning.
- **OT Security Controls Overlay:** Tailors NIST controls for OT and regulatory needs.

Secure by Demand

CISA: Selecting OT Products with Key Security Features – Jan 15, 2025

TLP:CLEAR

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

European Commission

Bundesamt für Sicherheit in der Informationstechnik

National Cyber Security Centre
Ministry of Security and Justice

Te Tira Tiaki
Government Communications Security Bureau

National Cyber Security Centre
PART OF THE GCSB

National Cyber Security Centre
a part of GCHQ

JOINT CYBER DEFENSE COLLABORATIVE

Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products

January 13, 2025

U.S. Cybersecurity and Infrastructure Security Agency
U.S. National Security Agency
U.S. Federal Bureau of Investigation
U.S. Environmental Protection Agency
U.S. Transportation Security Administration
Australian Signals Directorate's Australian Cyber

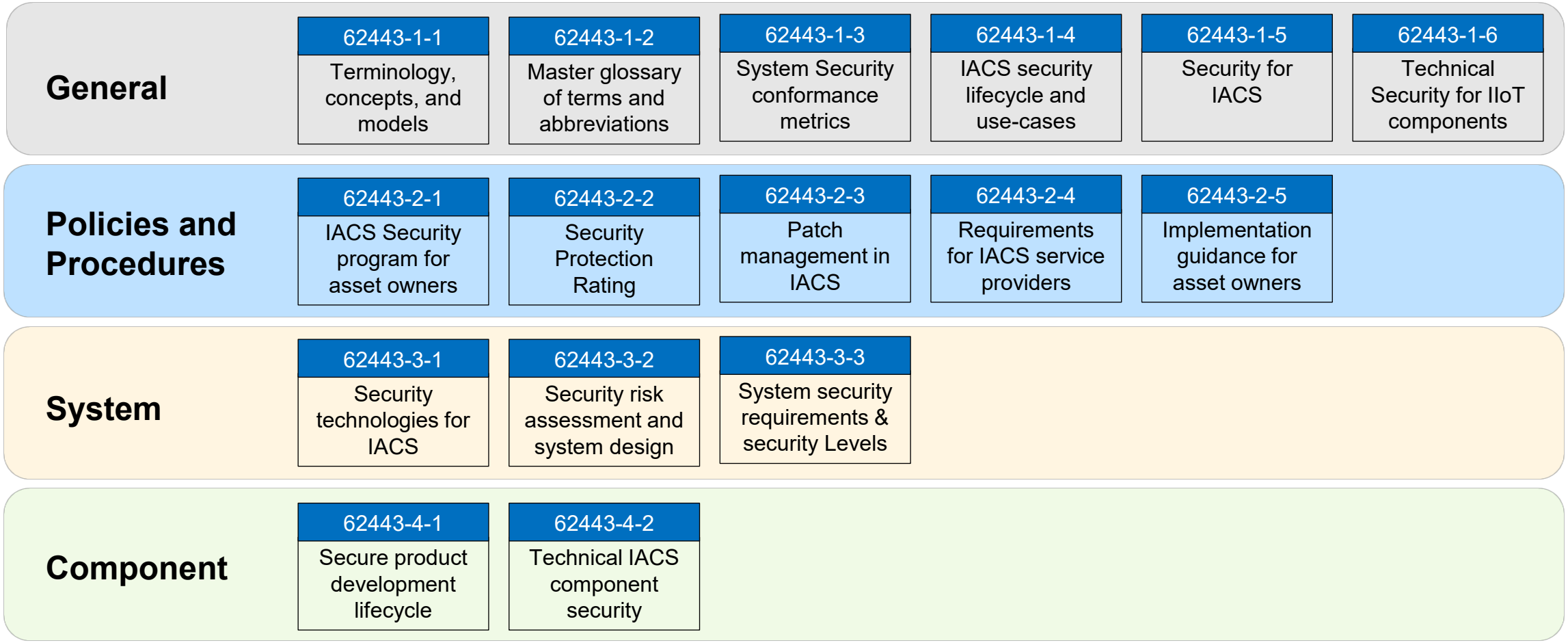
Canadian Centre for Cyber Security
Directorate General for Communications Networks, Content and Technology, European Commission
Germany's Federal Office for Information Security
Netherlands' National Cyber Security Centre
New Zealand's National Cyber Security Centre
United Kingdom's National Cyber Security Centre

Demand Products with:

1. Configuration Management
2. Native Logging
3. Open Standards
4. Give Owners Control
5. Data Protection
6. Security by Default
7. Secure Communications
8. Secure Controls
9. Strong Authentication
10. Threat Modeling
11. Vulnerability Management
12. Upgrade and Patch Tooling

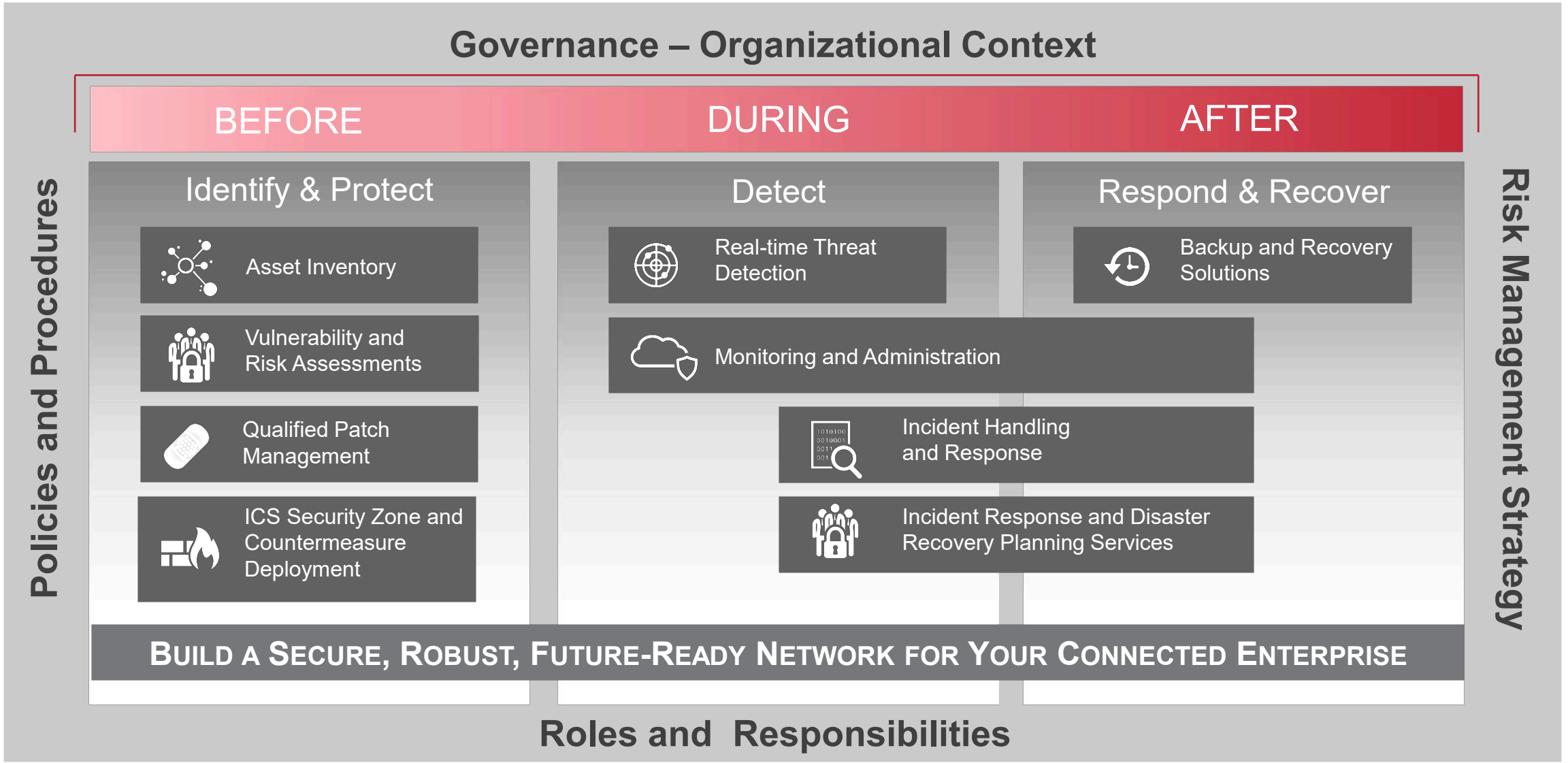
ICS Cybersecurity Guidelines, Standards and Frameworks

IEC / ISA 62443 Series of Standards for IACS Cybersecurity



A PROACTIVE APPROACH TO **INDUSTRIAL CYBERSECURITY – NIST CSF 2.0**

NIST Cybersecurity Framework (CSF) 2.0 – Overview



ICS Cybersecurity Guidelines, Standards and Frameworks

NIST Cybersecurity Framework (CSF) 2.0 – Key Controls and Measurement Criteria

GOVERN (GV)
- Organizational Context
- Risk Management Strategy
- Cybersecurity Supply Chain Risk Management
- Roles, Responsibilities, and Authorities
- Policy
- Oversight
- Cybersecurity Program

IDENTIFY (ID)
- Asset Management
- Risk Assessment
- Improvement

PROTECT (PR)
- Identity Management, Authentication, and Access Control
- Awareness and Training
- Data Security
- Platform Security
- Technology Infrastructure Resilience
- Configuration Management
- Vulnerability Management

DETECT (DE)
- Anomalies and Events
- Continuous Monitoring
- Detection Processes
- RESPOND (RS)
- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER (RC)
- Recovery Planning
- Improvements
- Communications

ICS Cybersecurity Guidelines, Standards and Frameworks

NIST Cybersecurity Framework (CSF) 2.0 – Key Controls & Measurement Criteria – Detailed Example

GOVERN (GV)
- Organizational Context
- Risk Management Strategy
- Cybersecurity Supply Chain Risk
- Roles, Responsibilities, and Auth
- Policy
- Oversight
- Cybersecurity Program

IDENTIFY (ID)
- Asset Management
- Risk Assessment
- Improvement

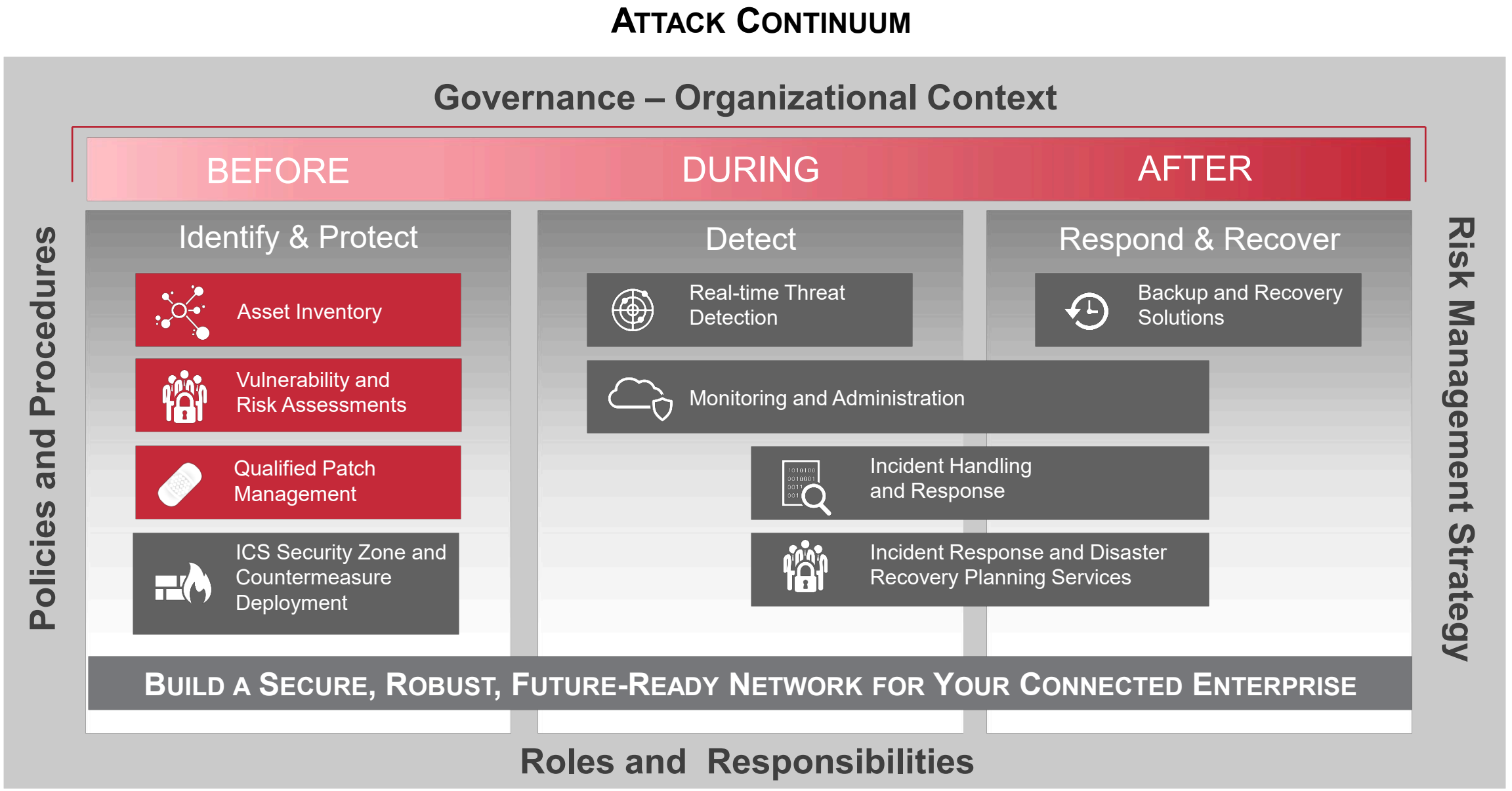
PROTECT (PR)
- Identity Management, Authentication, and Access Control
- Awareness and Training
- Data Security
- Platform Security
- Technology Infrastructure Resilience
- Configuration Management
- Vulnerability Management

DETECT (DE)
- Anomalies and Events

- Improvements
- Communications

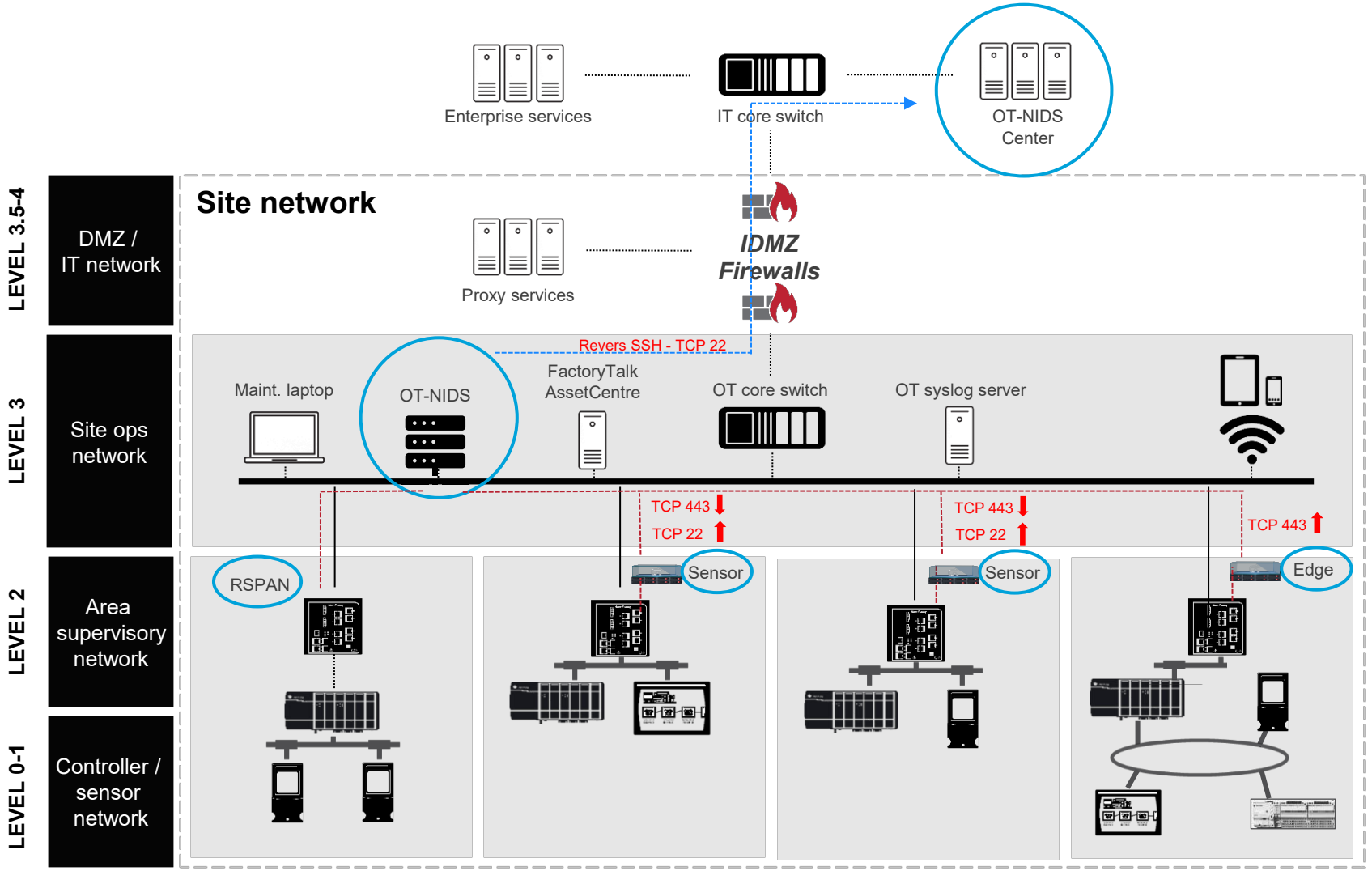
- ID.AM-01: Physical devices and systems are inventoried.
- ID.AM-02: Software platforms and applications are inventoried.
- ID.AM-03: Organizational communication and data flows are mapped.
- ID.AM-04: External information systems are cataloged.
- ID.AM-05: Resources are prioritized based on classification, criticality, and business value.

A PROACTIVE APPROACH TO **INDUSTRIAL CYBERSECURITY – NIST CSF 2.0**



Asset Inventory - Visibility

OT-NIDS



Asset inventory

- Vendor agnostic ICS/IT Passive Asset discovery
- Vendor agnostic ICS/IT Active asset discovery

Asset Topology

- Bi-directional Dataflow with Purdue Model Overlay
- Vendor / Product Filters

Risk / Vulnerability Identification

- Always updated agnostic vulnerability detection, classified by Asset and ranked by CVSS
- Agnostic asset End of Life status notification

IACS Change Detect

- Vendor agnostic IACS change detect and notification
- Historical change and optional trend by asset.

Anomaly & Threat Detection

- Heuristic, Signature and Baseline Deviation
- Event correlation to MITRE ICS ATT&CK® Framework

Monitoring & Administration

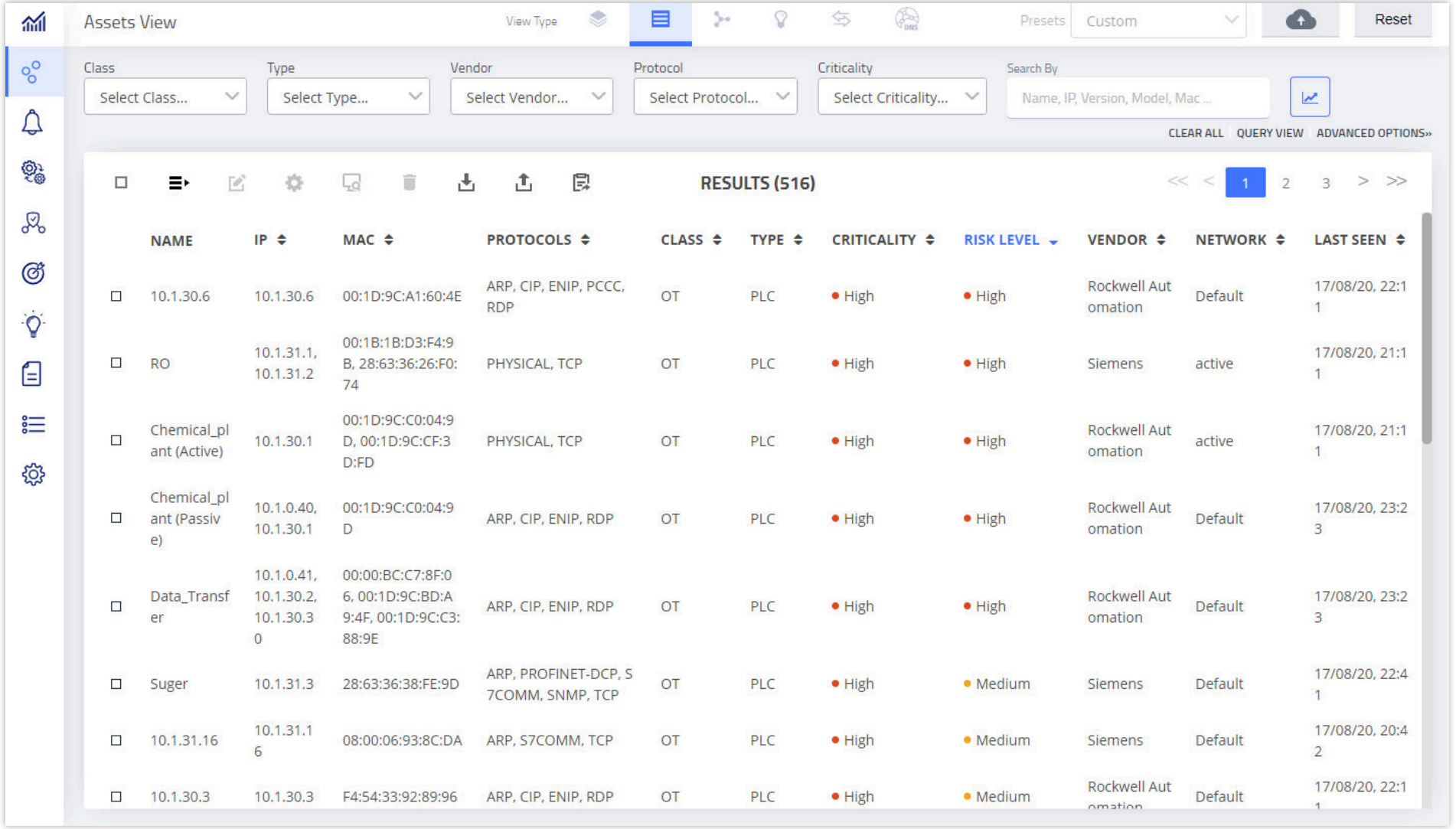
- Central monitoring of health/hygiene of the system.
- Integration with CMDB's, Firewalls, NAC's, CMS's, VMS's, Secure Access, SIEM's and SOAR''s

Compliance

- IEC 62443-3-3 Reports

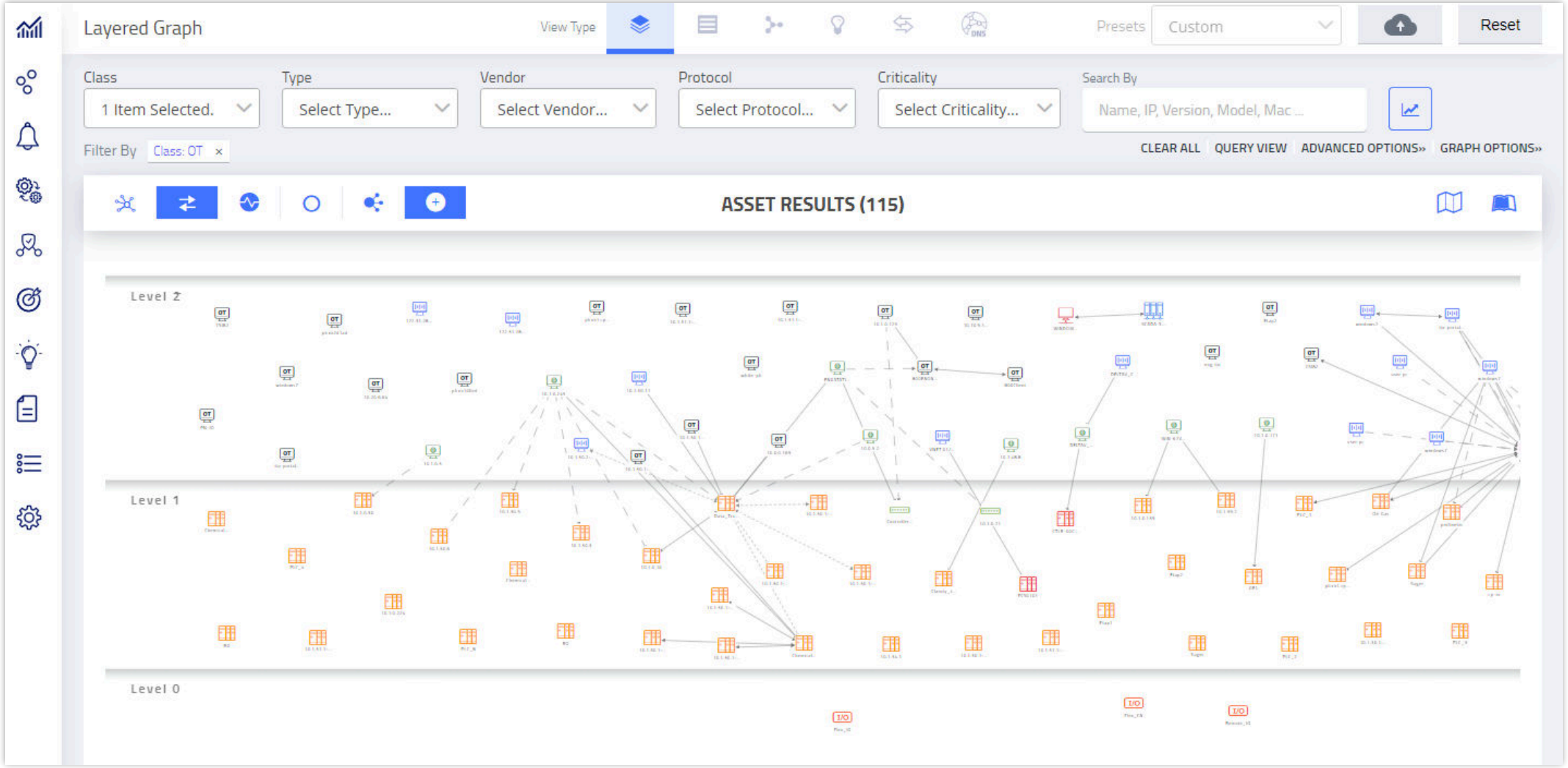
Asset Inventory - Visibility

OT-NIDS – Industrial ICS protocols + IT Protocols



Asset Inventory - Visibility

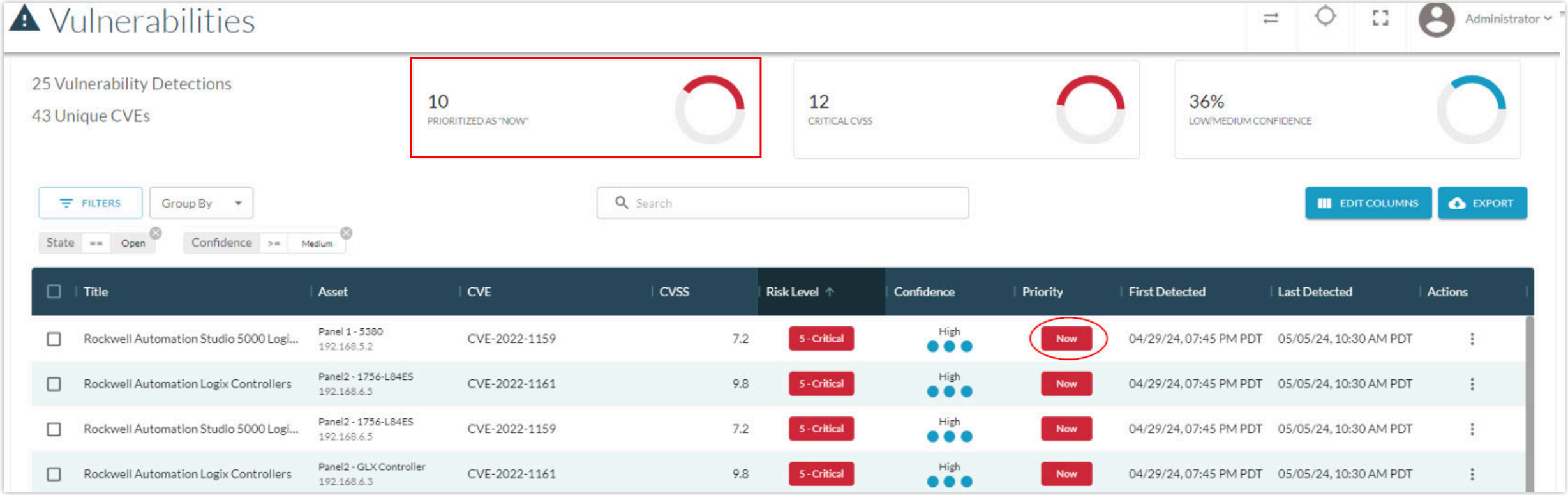
OT-NIDS – Comms Direction – Highly Filterable – Communication Direction shown



Vulnerability and Risk Assessments

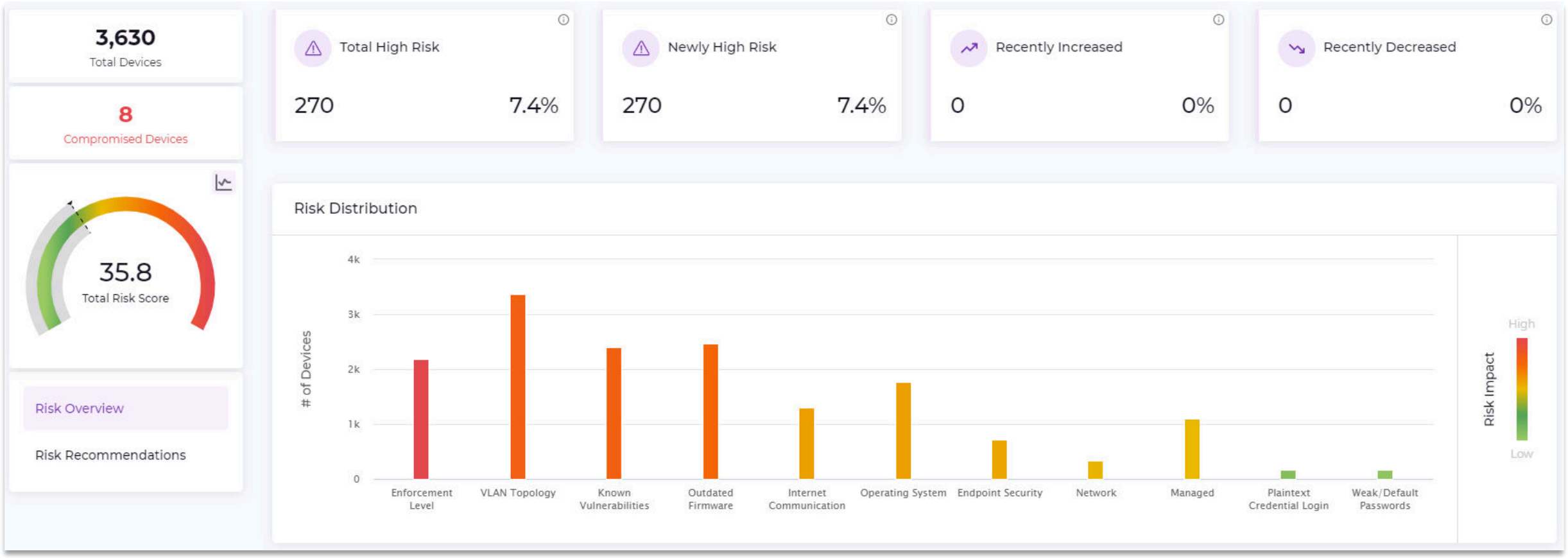
NIDS Prioritization – CVSS and Now / Next / Never

- This OT-NIDS reclassifies the CVE CVSS score to Now, Next, Never to streamline prioritization



Vulnerability and Risk Assessments

NIDS – Overall Risk Dashboard



IACS Patch Management

Iterative Patch / Change Management Program

1. IACS ASSET INVENTORY

Continuous Industrial Automation Control System (IACS) asset inventory is the first step to a compile patch management system

2. ASSEMBLE VULNERABILITY / PATCH INFORMATION

Automated IACS Software and Firmware patch identification & correlation to installed assets against installed patches.

3. PRIORITIZE VULNERABILITY

IACS patch prioritization supporting business objectives, criticality of the IACS assets and vulnerability impact.

4. REVIEW & APPROVE

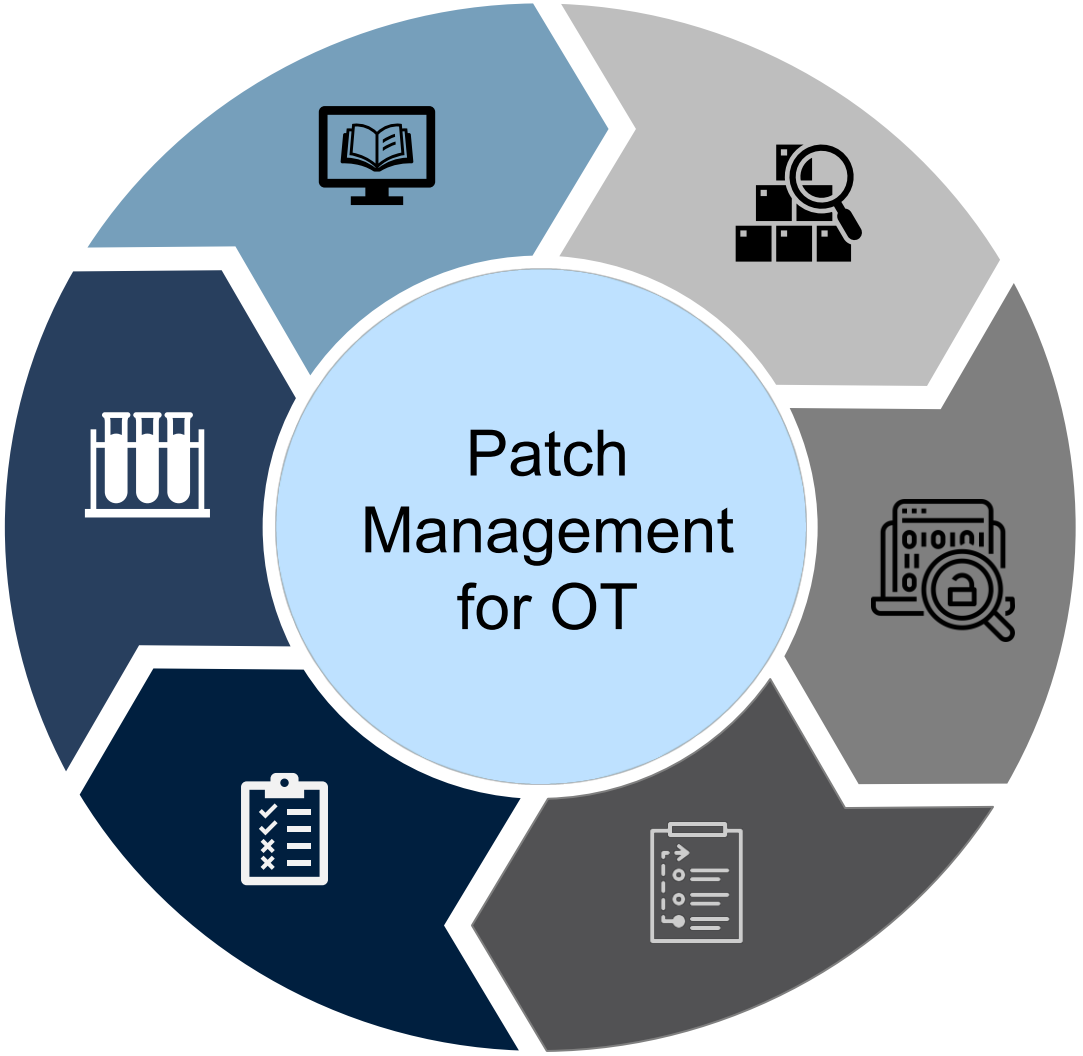
A Change review board should review proposed patch/update prioritization includes the validation of manufacture approved Operating system patches, application patches and firmware updates against the planned prioritized list.

5. TEST AND DEPLOY

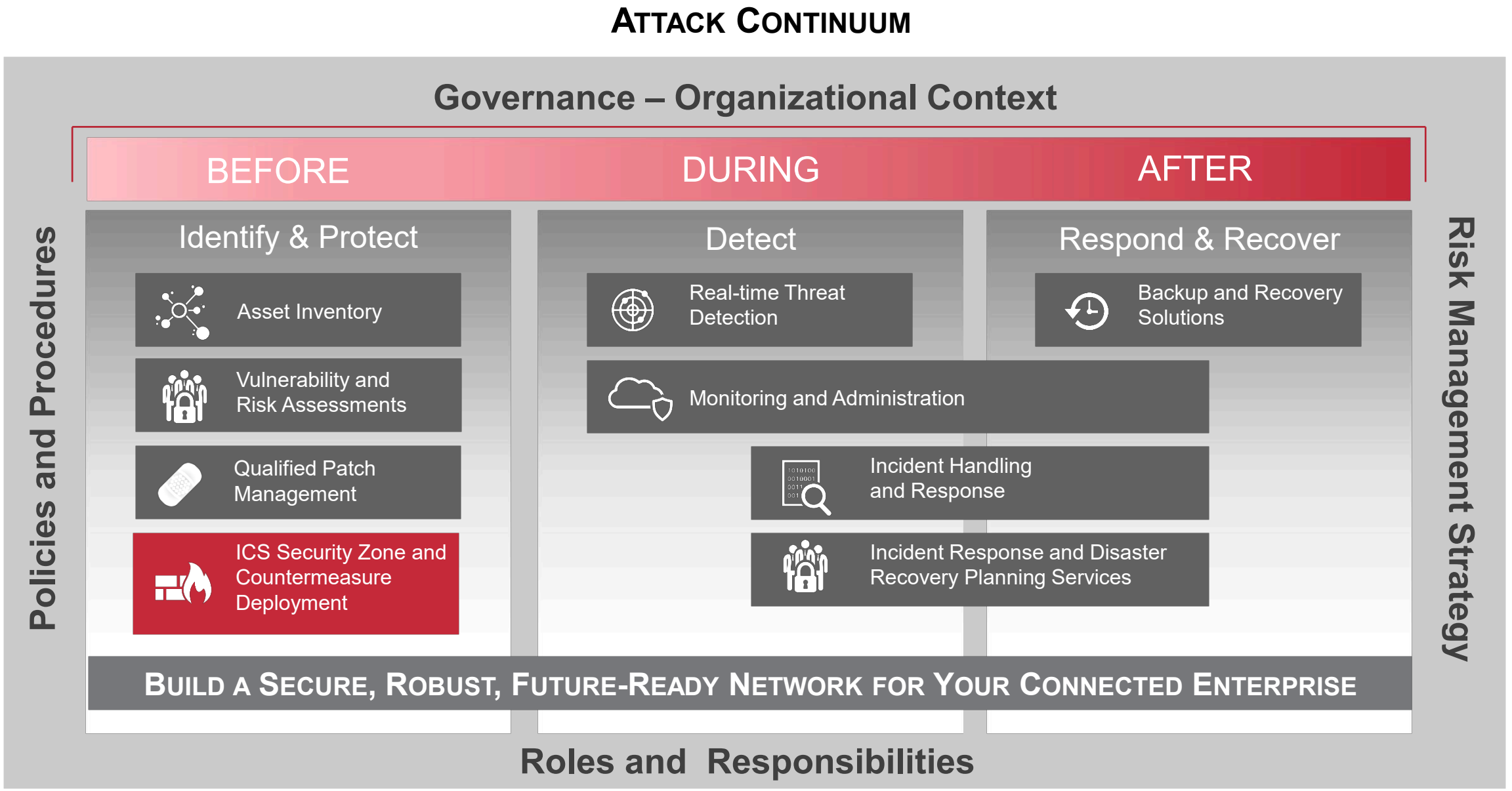
Validate and test against local applications and configurations in sandbox and schedule deployment based upon criticality assessment.

6. DOCUMENTATION & CONFIGURATION MANAGEMENT

Documentation via change/configuration management solution and establish new baseline for IACS assets.

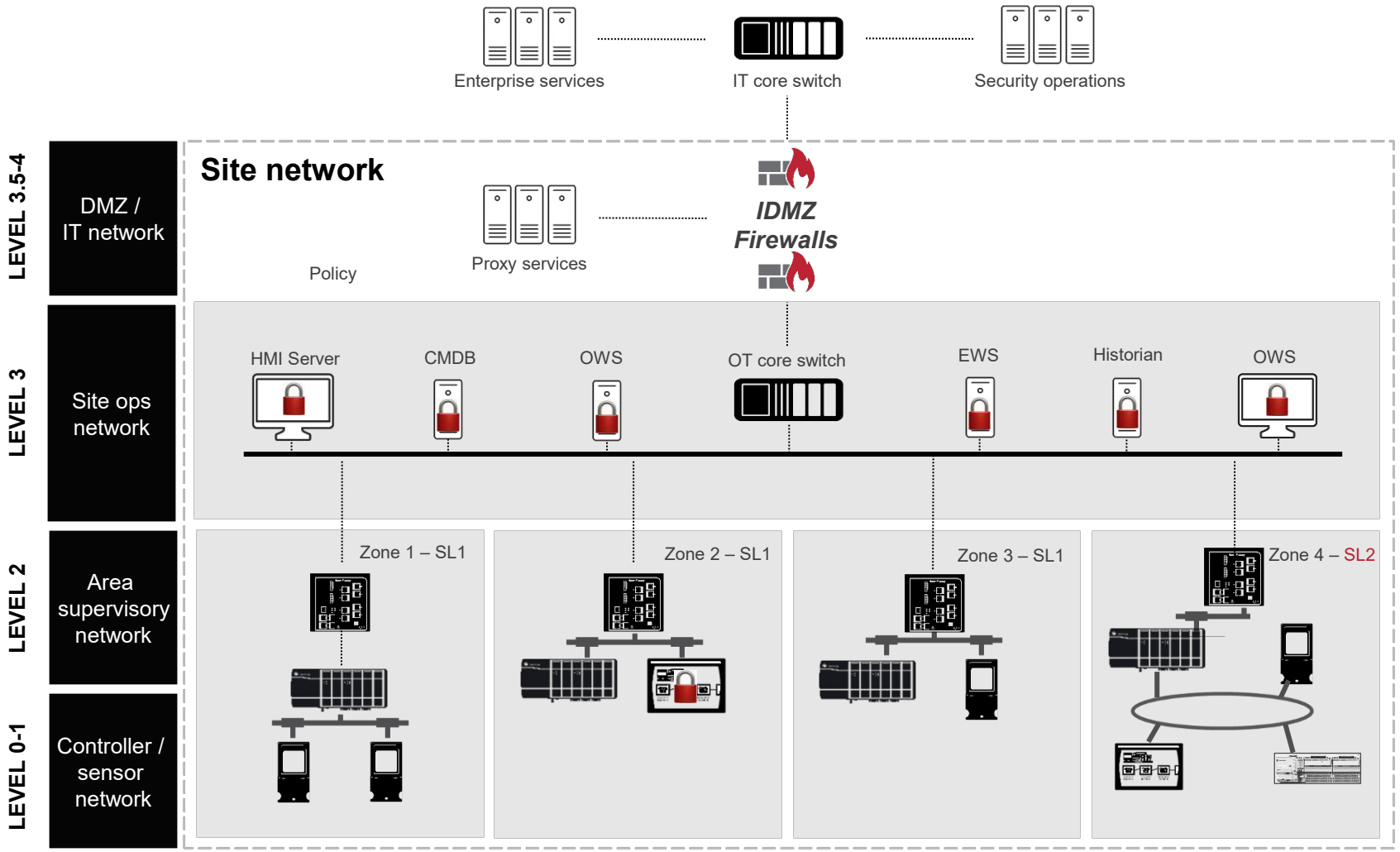


A PROACTIVE APPROACH TO **INDUSTRIAL CYBERSECURITY – NIST CSF 2.0**



ICS Security Zone and Countermeasure Deployment

Managed Endpoint Solution for OT/ICS



Application Allowed listing

- Blocks unauthorized apps
- Limits attack surface
- Fits static OT environments

Threat Detection & Response

- Flags anomalies fast
- Enables quick containment
- Stops lateral movement

Visibility

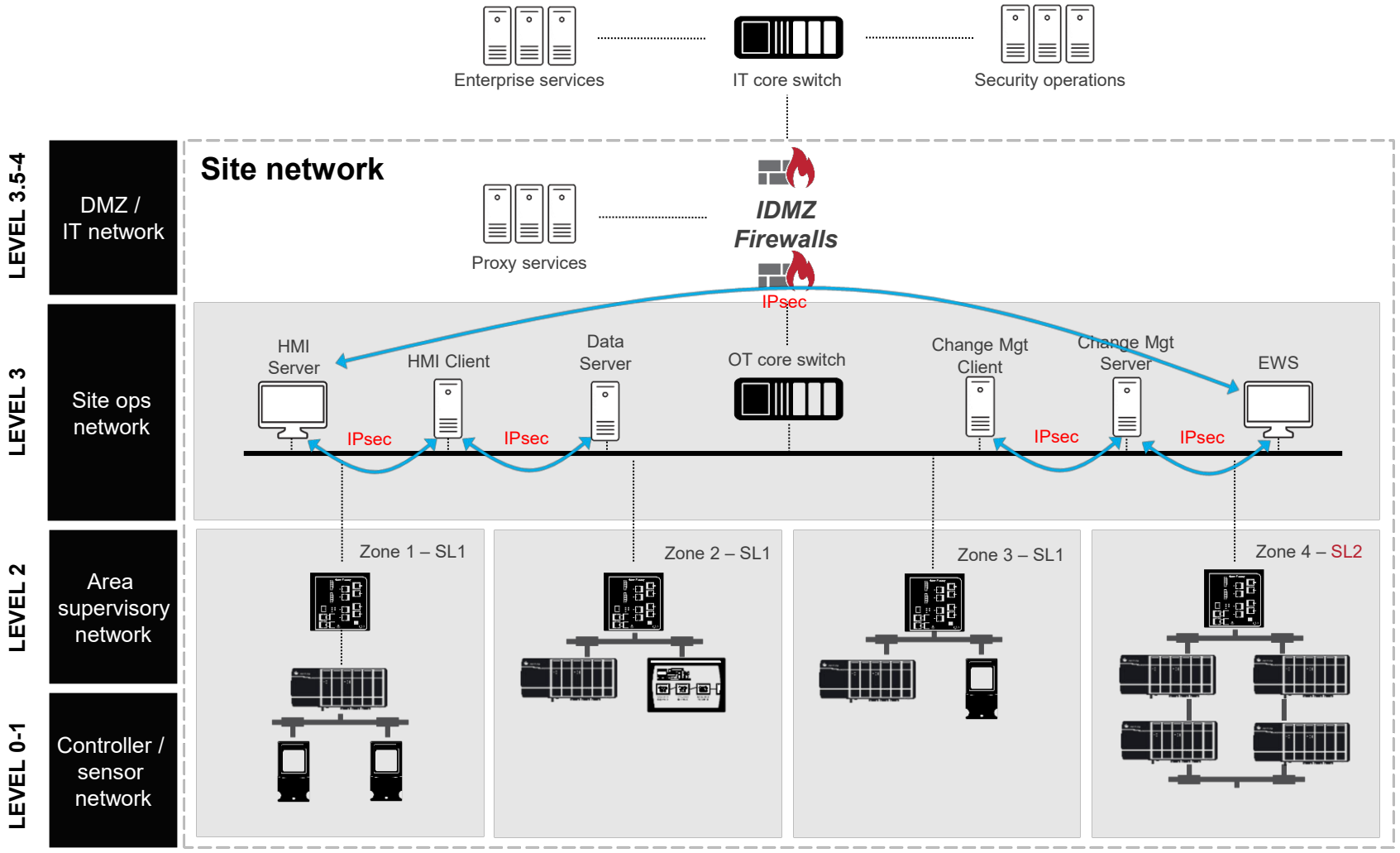
- Integration with OT-NIDS
- Connects with SIEM/SOAR
- Optional Managed

Operational Resilience

- Reduces downtime risks
- Maintains system integrity
- Enhances incident response

ICS Security Zone and Countermeasure Deployment

Internet Protocol Security (IPsec) – Secure Data in Transit for Compute Assets



Authentication

- Secure connection to ensure that each of the computers receives proof that a network packet is originating from an authentic source.

Integrity

- Helps prevent tampering or modification of communications

Confidentiality

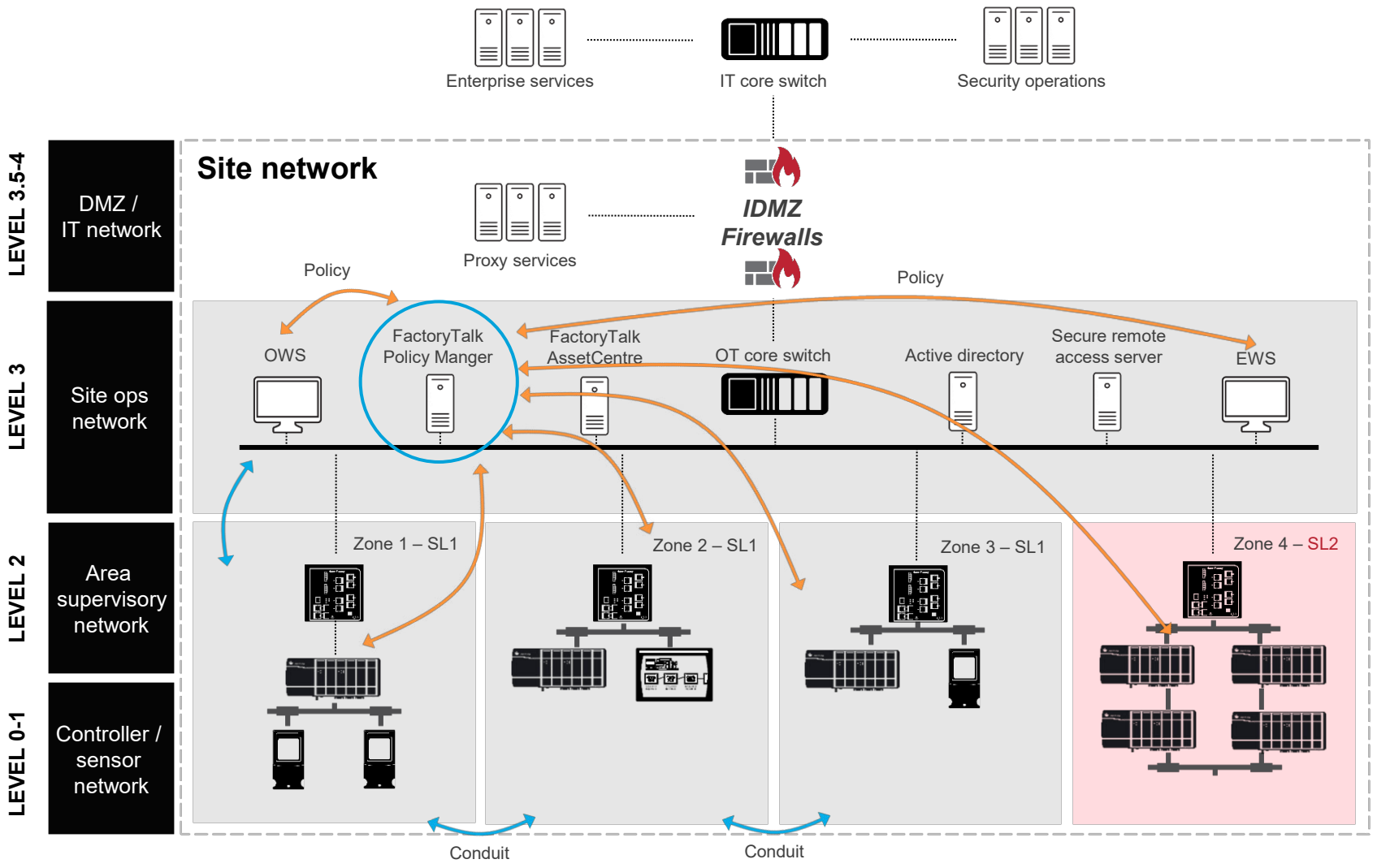
- Helps prevent snooping or disclosure of data

Anti-relay Protection

- Ensures that a network packet cannot be intercepted, and a new and modified packet injected during transmission stream from source to destination.

ICS Security Zone and Countermeasure Deployment

ODVA's CIP Security – Authentication, Integrity and Confidentiality



Authentication

- Helps prevent unauthorized devices from establishing connections

Integrity

- Helps prevent tampering or modification of communications

Confidentiality

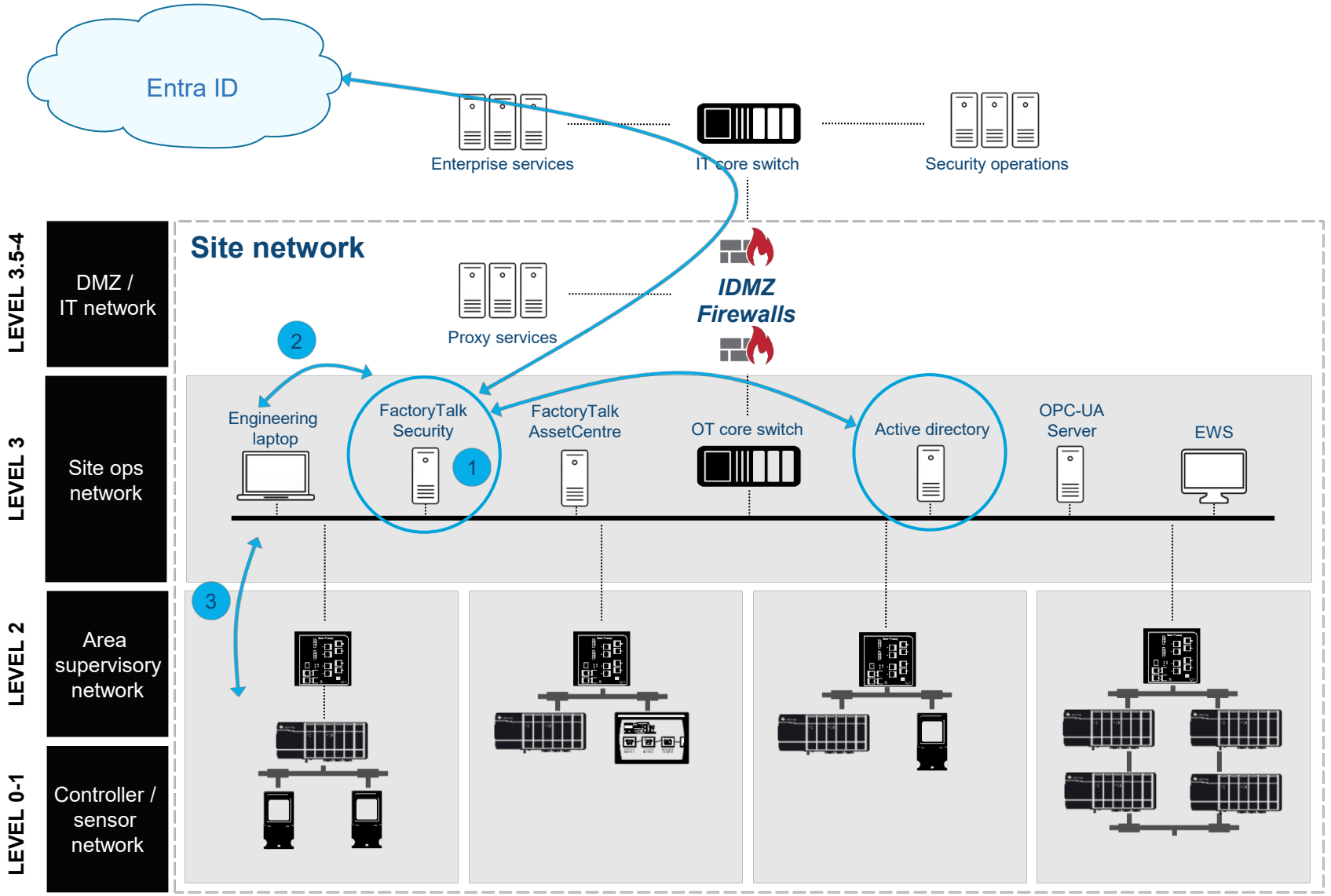
- Helps prevent snooping or disclosure of data

Notable features

- **System management** – Easily create and deploy security policies to many devices
- **Micro-segmentation** – Segment your automation application into smaller cell/zones.
- **Device-based firewall** – Enable/disable (i.e.,/ HTTP/HTTPS)
- **Legacy Systems Support** – Trusted IP – authorize specific communications based on IP address and1783-CSP proxy device in front of legacy products
- Native OPC-UA Client / Server support

ICS Security Zone and Countermeasure Deployment

Role Based Authentication (RBAC) – Rockwell Automation Example



Windows domain architecture

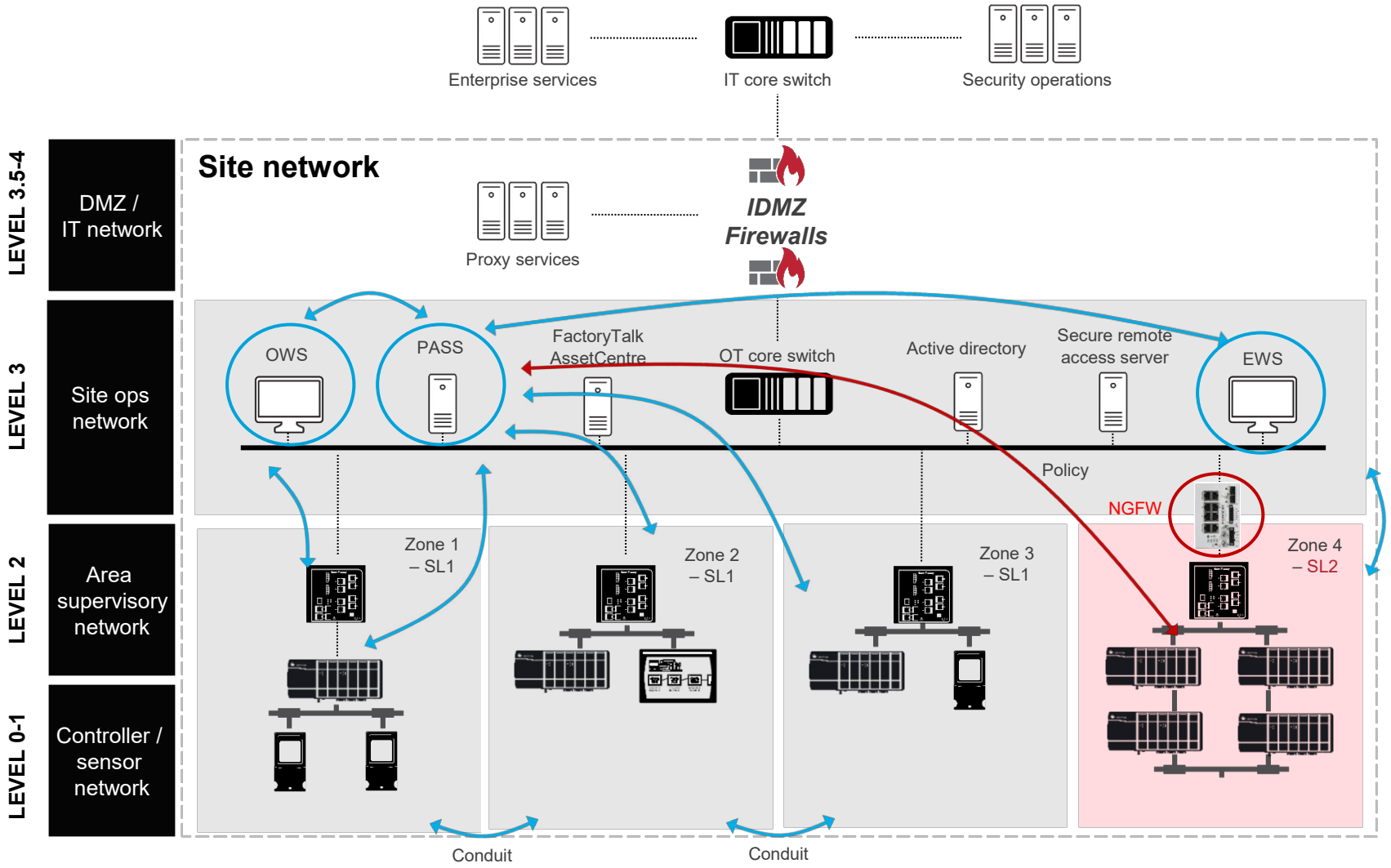
- Active directory
- Authentication best practices with FTSecurity
- SSO Option's to on prem AD
- MFA options with Azure AD and OpenID Connect

FactoryTalk® Security

- Role Based Access Control (RBAC)
- Authentication and authorization services for FactoryTalk® software, Studio 5000®, HMI and Logix5000™ controllers.
- Integration into Windows Active Directory and Entra ID with options for MFA
- Local and centralized audit trail
- Enforce FTSecurity Authentication for 3rd party OPC UA clients with FT Linx OPC Gateway

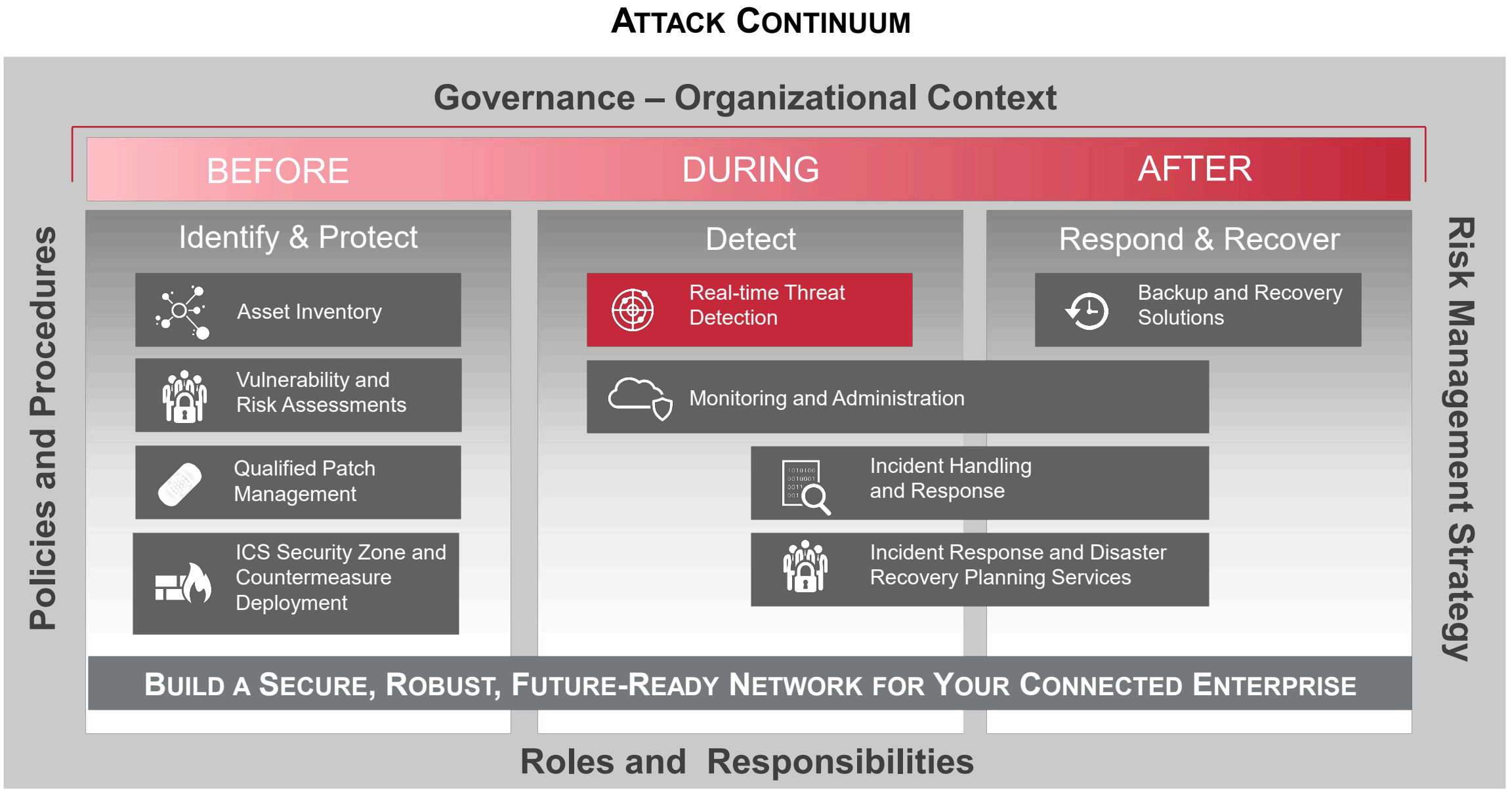
ICS Security Zone and Countermeasure Deployment

Zone Based IPS/IDS – DPI Next Generation Rugged Firewall Series



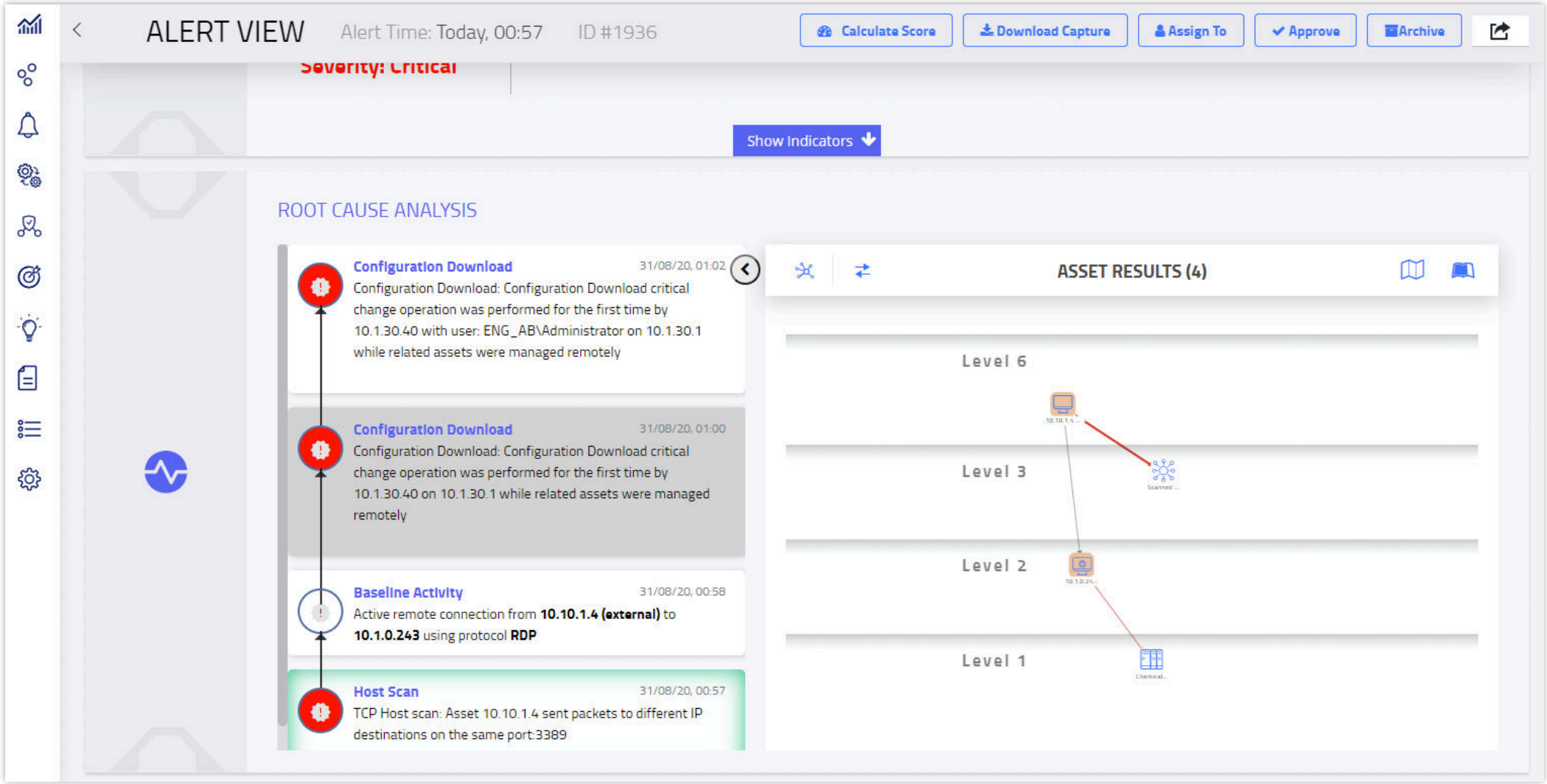
- Deep packet inspection (DPI) provides full visibility and control of OT protocols down to the payload level.
- OT-focused IPS enables virtual patching and shields vulnerabilities from known and unknown threats.
- Network segmentation limits incident impact and supports comprehensive traffic monitoring and protection.
- Real-time SSL/TLS inspection ensures visibility into users, devices, and applications across the network.

A PROACTIVE APPROACH TO **INDUSTRIAL CYBERSECURITY – NIST CSF 2.0**



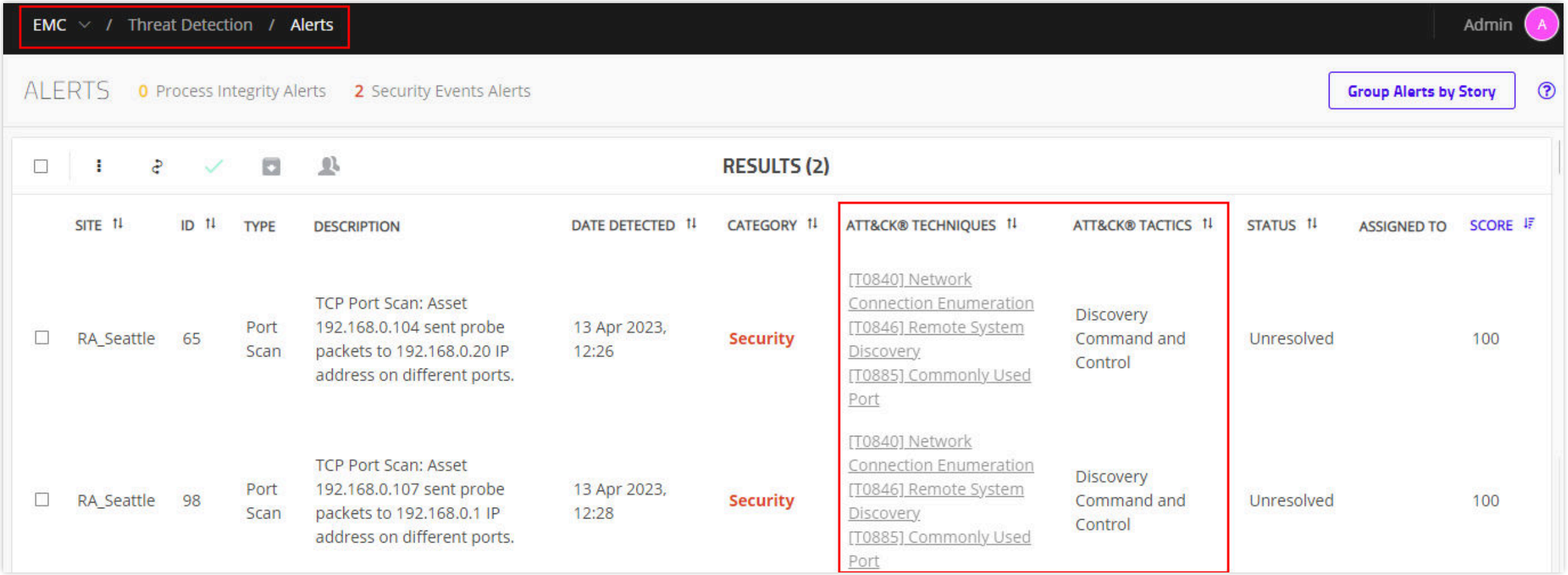
Real-time Threat Detection

OT-NIDS – Event Detection & Correlation



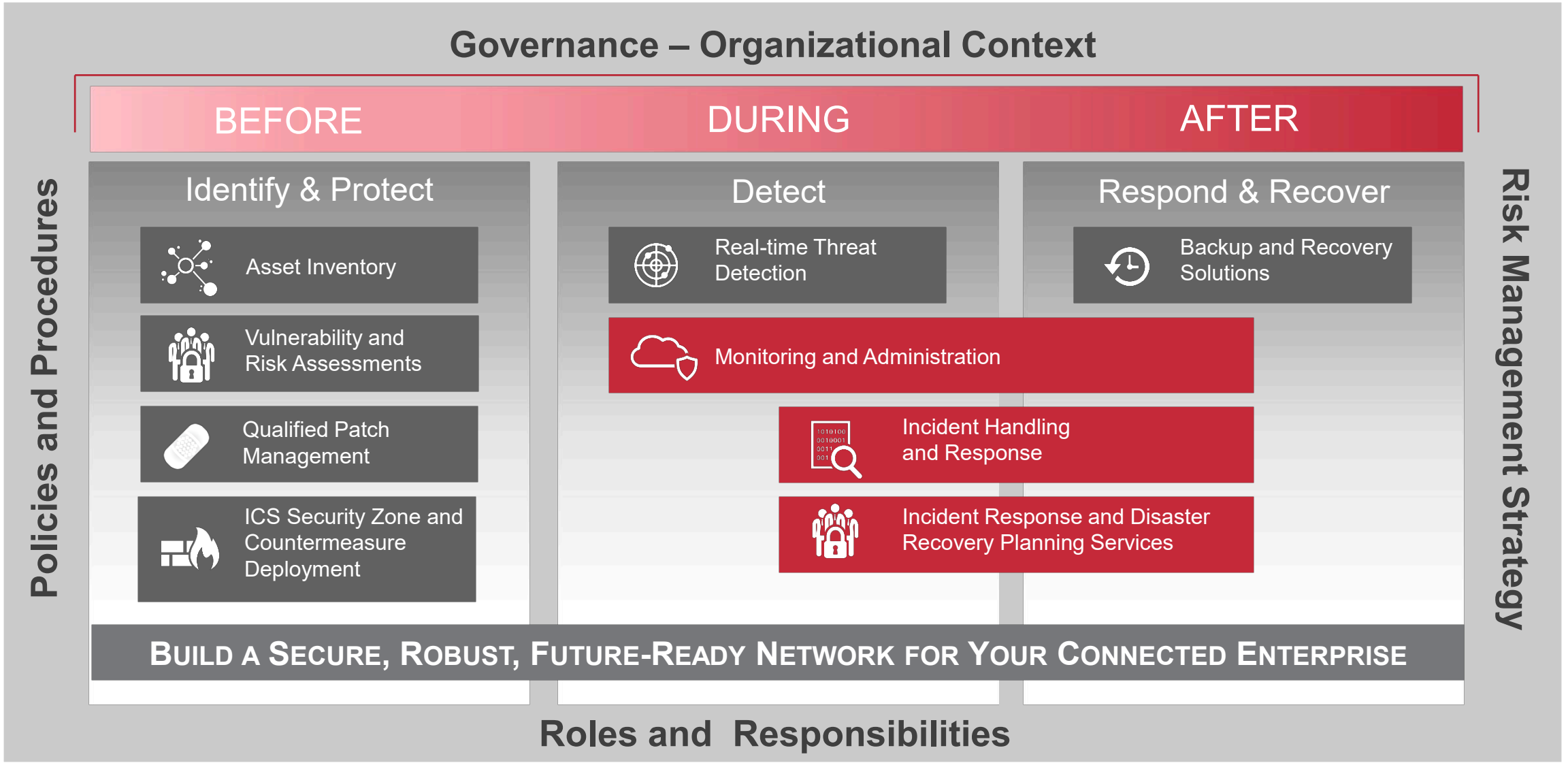
Real-time Threat Detection

OT-NIDS – Alert correlation to MITRE ATT&CK® ICS Techniques and Tactics

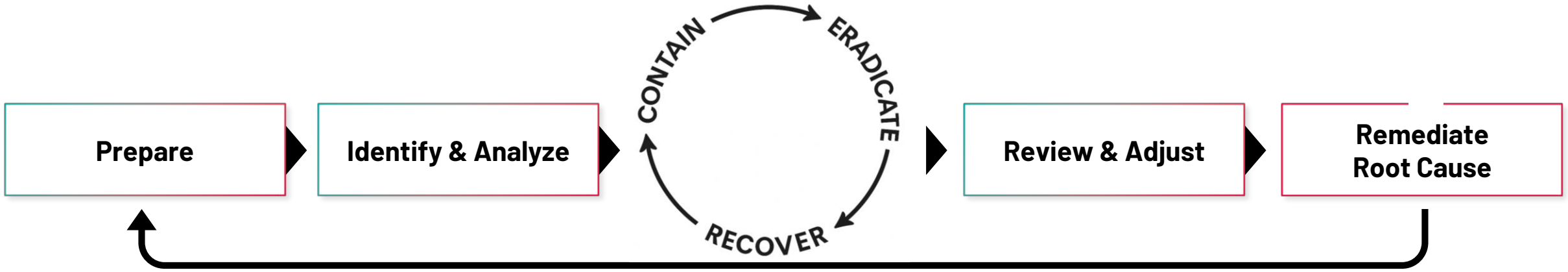


A PROACTIVE APPROACH TO **INDUSTRIAL CYBERSECURITY – NIST CSF 2.0**

ATTACK CONTINUUM



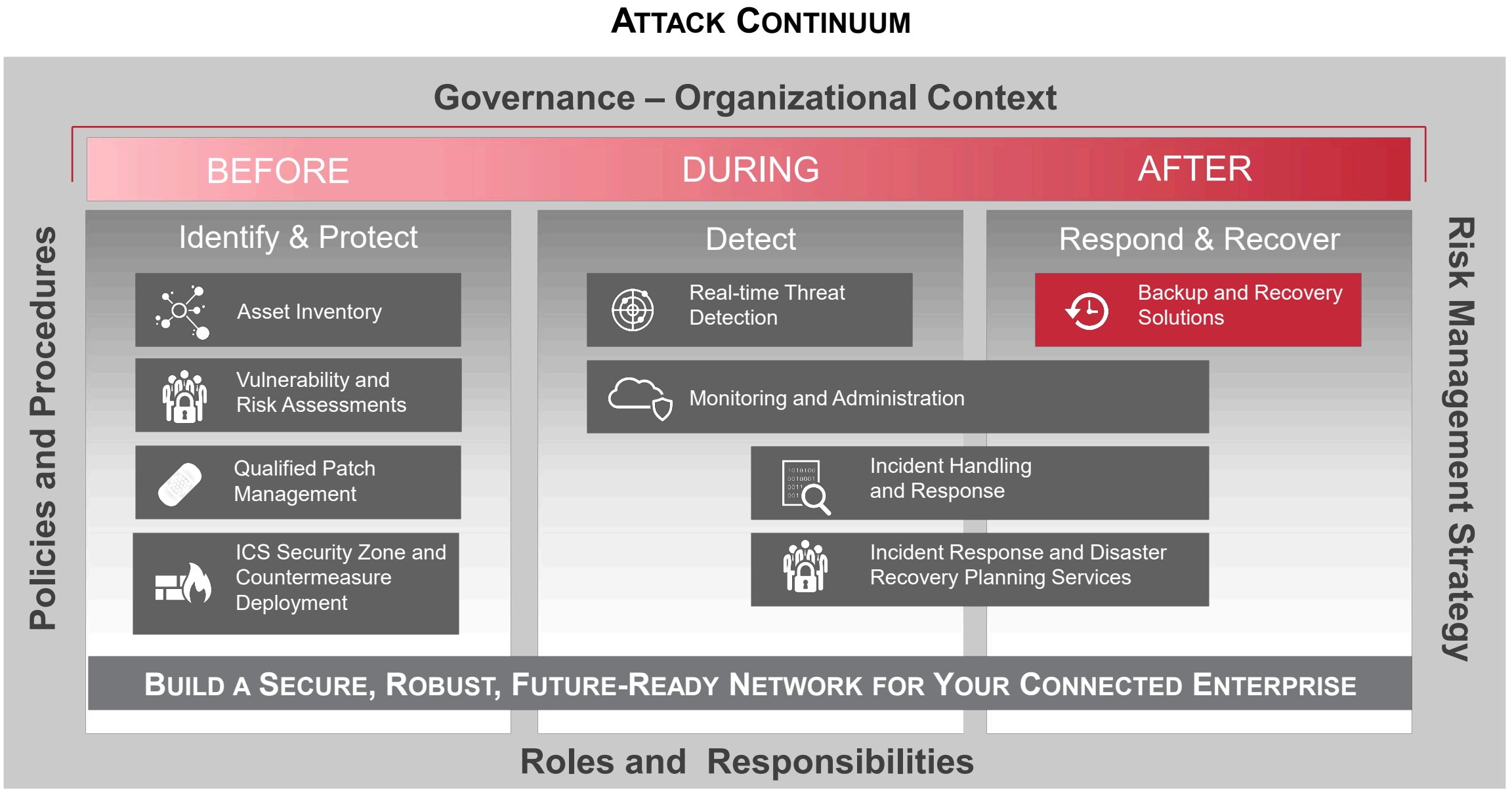
Incident Response Capability Overview



Risk Reduction Methodology

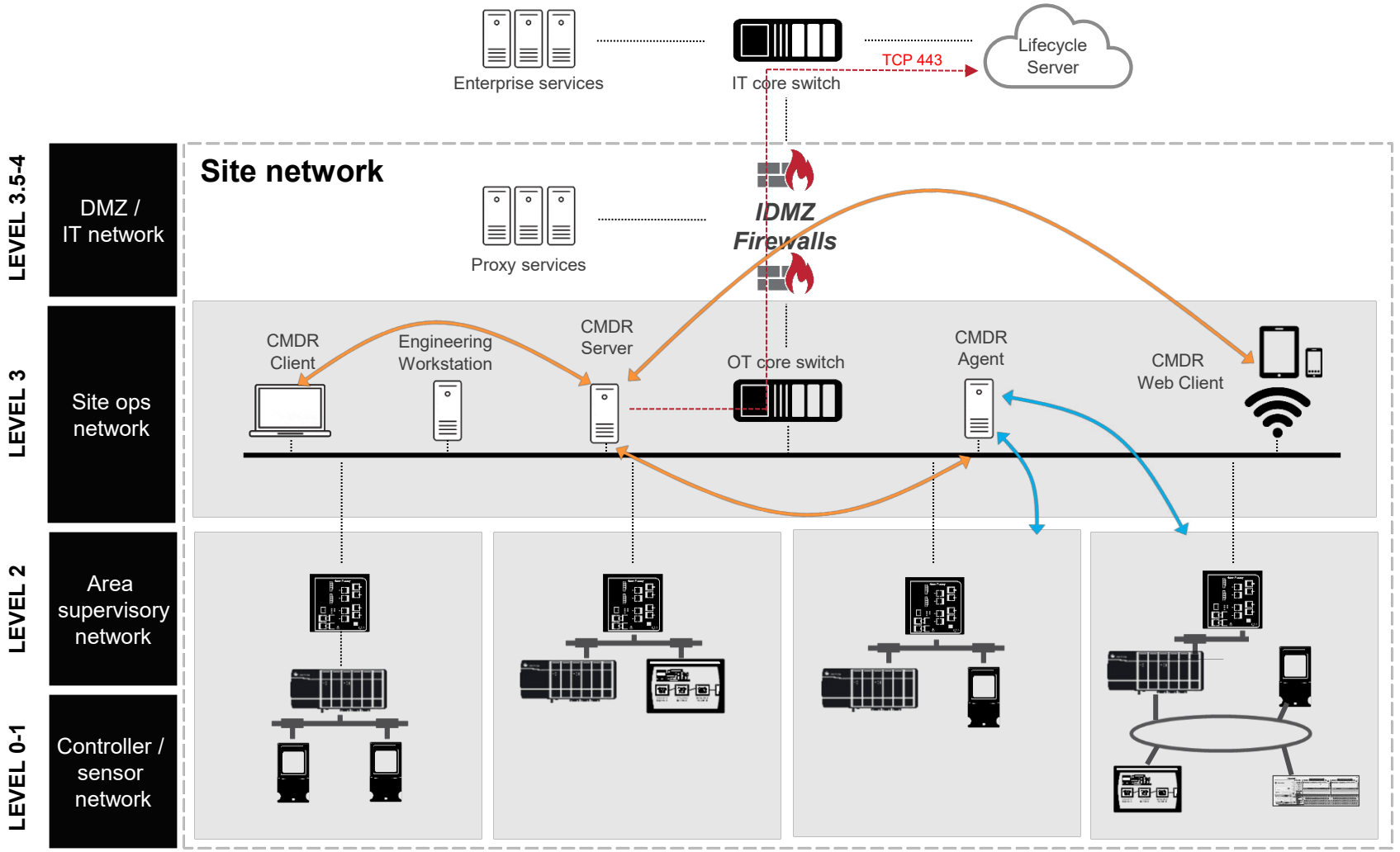
- 24x7 Global Access to ICS/OT cybersecurity incident response professionals
- Rapidly respond to incidents with guaranteed response times in the event the customer suspects a cyber incident
- In the event of a wide scale global attack affecting many customers, customers under a retainer receive priority
- Pre-negotiated terms and conditions that allow for a quick response when the retainer is activated
- Reduce mean time to recover from Industrial Cyber Incidents
- In a multi-year retainer agreement, flexibility to repurpose hours towards proactive services to improve customer cybersecurity posture
- Prevent future industrial incidents with strategic recommendations to strengthen security posture

A PROACTIVE APPROACH TO **INDUSTRIAL CYBERSECURITY – NIST CSF 2.0**



Backup and Recovery Solutions

IACS Asset Change Management and & Disaster Recovery



Asset Change Management

- Agnostic Change management
- Firmware availability
- Lifecycle status for some Assets
- IPSEC or HTTPS support
- Product Notice Notification
- Immediate Change Detect
- Drive any 3rd party compare tool

Asset Disaster Recovery

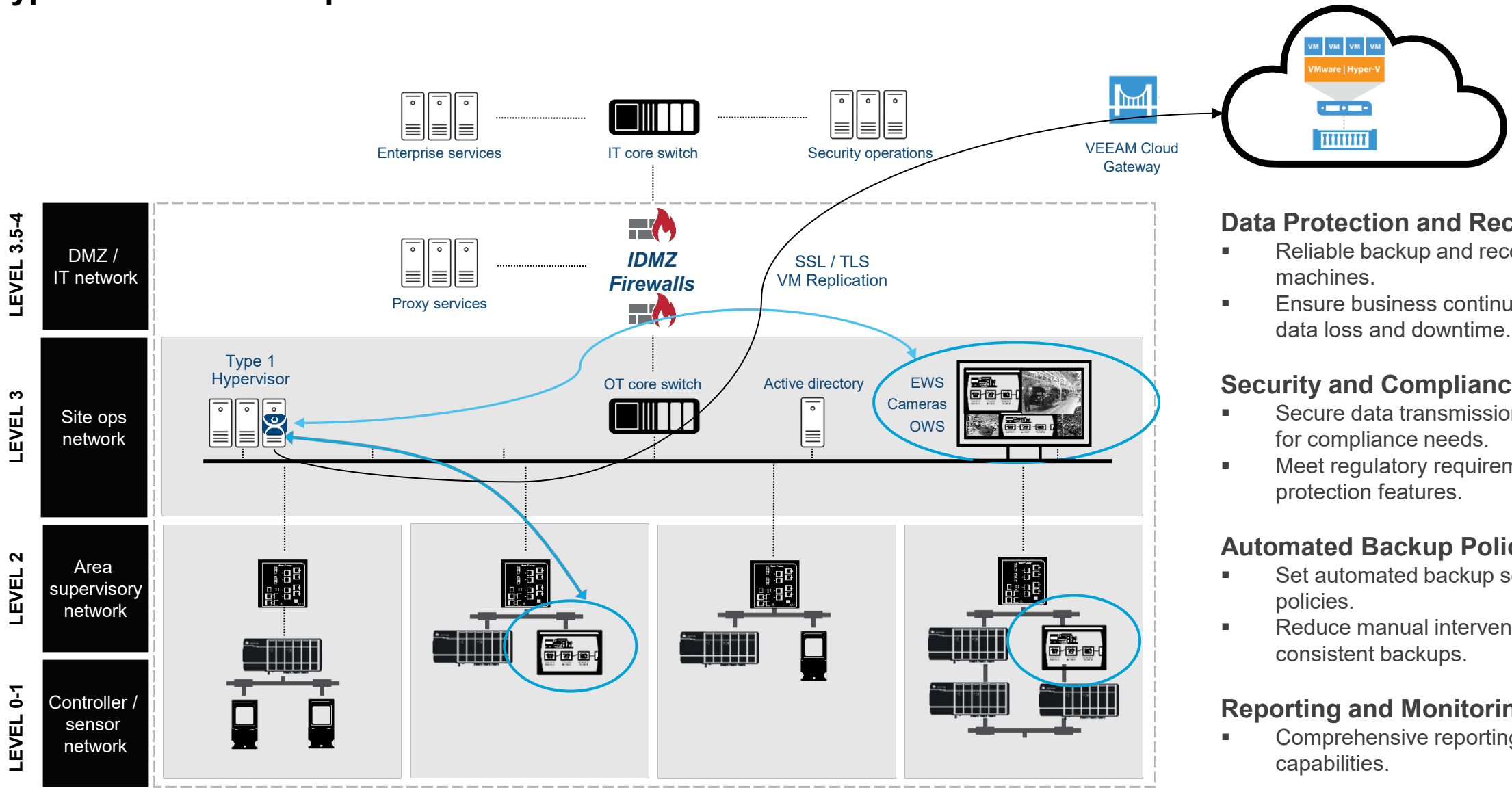
- Agnostic Automated back-up
- Application change detection and notification.

Centralized Audit and Diagnostics Log

- Central place to capture IACS Audits and Diagnostics.

Backup and Recovery Solutions

Hypervisor VM Backup



Data Protection and Recovery:

- Reliable backup and recovery for virtual machines.
- Ensure business continuity by minimizing data loss and downtime.

Security and Compliance:

- Secure data transmission and encryption for compliance needs.
- Meet regulatory requirements with data protection features.

Automated Backup Policies:

- Set automated backup schedules and policies.
- Reduce manual intervention and ensure consistent backups.

Reporting and Monitoring:

- Comprehensive reporting and monitoring capabilities.

CSF 2.0 – Proactive Cybersecurity Strategies / Takeaways

1. **Establish Governance:** Define roles, responsibilities, and policies for cybersecurity risk management.
2. **Know Your Assets:** Inventory hardware, software, data, and third-party dependencies.
3. **Assess and Prioritize Risk:** Regularly evaluate threats, vulnerabilities, and business impacts.
4. **Protect What Matters:** Implement access controls, awareness training, data protection, and system IACS hardening.
5. **Monitor Continuously:** Detect anomalies and monitor systems, networks, and user activity in real time.
6. **Respond Effectively:** Develop and test incident response plans; communicate and mitigate threats quickly.
7. **Ensure Rapid Recovery:** Maintain and test recovery plans to restore operations and learn from incidents.
8. **Drive Continuous Improvement:** Use lessons learned to strengthen your cybersecurity posture.
9. **Engage the Whole Organization:** Foster a culture of cybersecurity awareness and accountability.