smart
SOLUTIONS SUMMIT

VAN METER

5 Steps Towards a Better Cybersecurity Plan

Jason Vandenberg, Cybersecurity Consultant, Rockwell
Jordan Lutz, Industrial Networks and Cybersecurity Specialist, Rockwell
Scott Larson, Business Consultant, Van Meter Inc

Agenda

Introductions

Overview

5 Steps

Group Question #1

Group Question #2

Recap

Questions

smart
SOLUTIONS SUMMIT

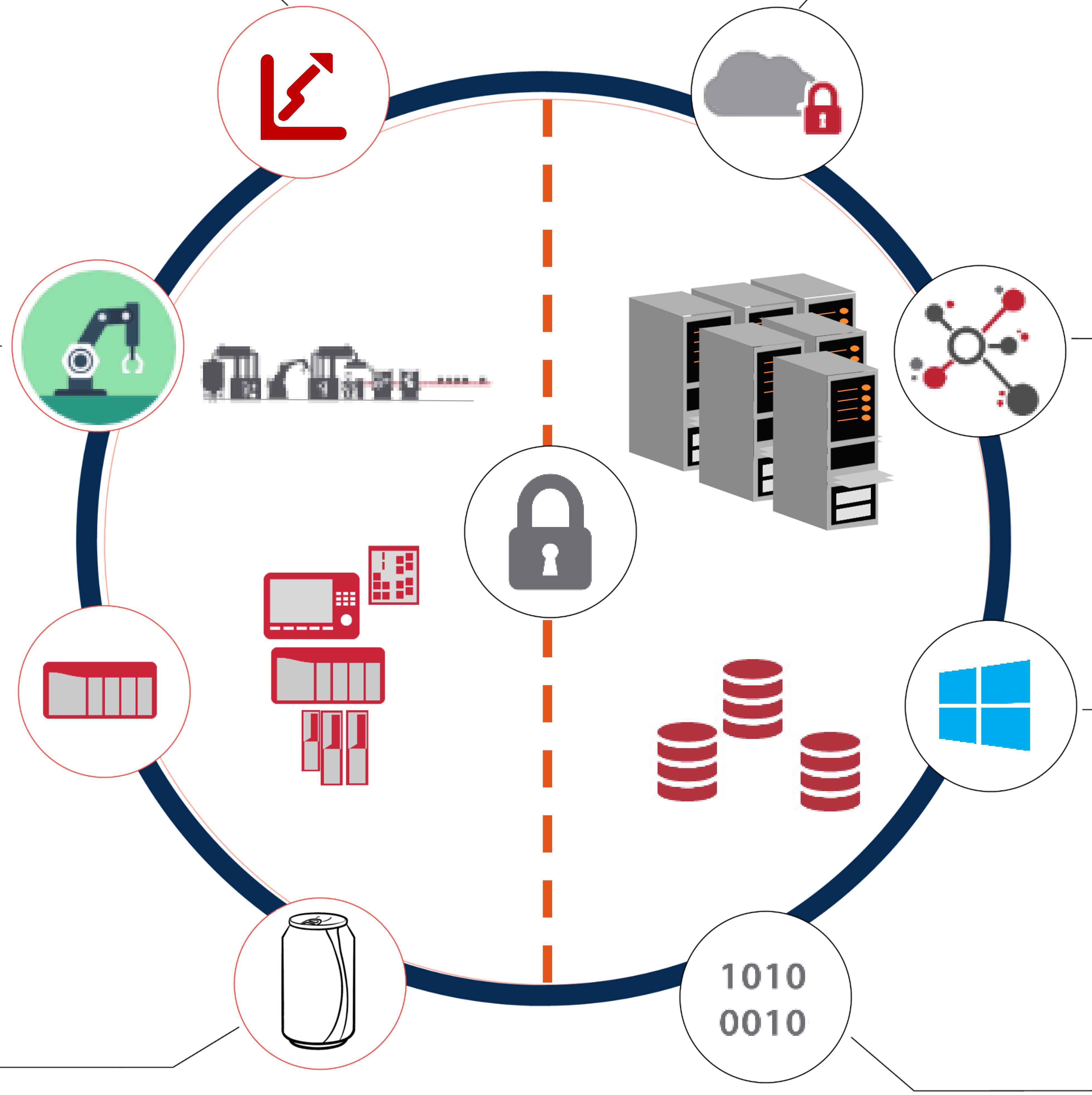
Jason Vandenberg
Rockwell
Cybersecurity Consultant

Jordan Lutz
Rockwell
Industrial Networks &
Cybersecurity Specialist

Scott Larson
Van Meter
Business Consultant

INFORMATION TECHNOLOGY VS. OPERATIONAL TECHNOLOGY

OT VS IT



OT

<u>Focus</u>
Operation of Physical Processes

Architecture:
- **Proprietary**
- **Task Specific**

Diverse Endpoints
w/ Long Lifespans

Outcomes are **<u>Physical</u>**

IT

<u>Focus</u>
Manage Data & Information

Architectures:
- **Ubiquitous**
- **Universal**

Similar Endpoints
w/ Short Lifespans

Outcomes are **<u>Digital</u>**

CYBERSECURITY
FAST FACTS

605

2022 RANSOMEWARE INCIDENTS

Targeting specifically manufacturing companies.

Source: DRAGOS

$12B

COST OF CYBERCRIME

In the last 3 years.

Source: LNS Research Study

61%

INDUSTRIAL MANUFACTURERS

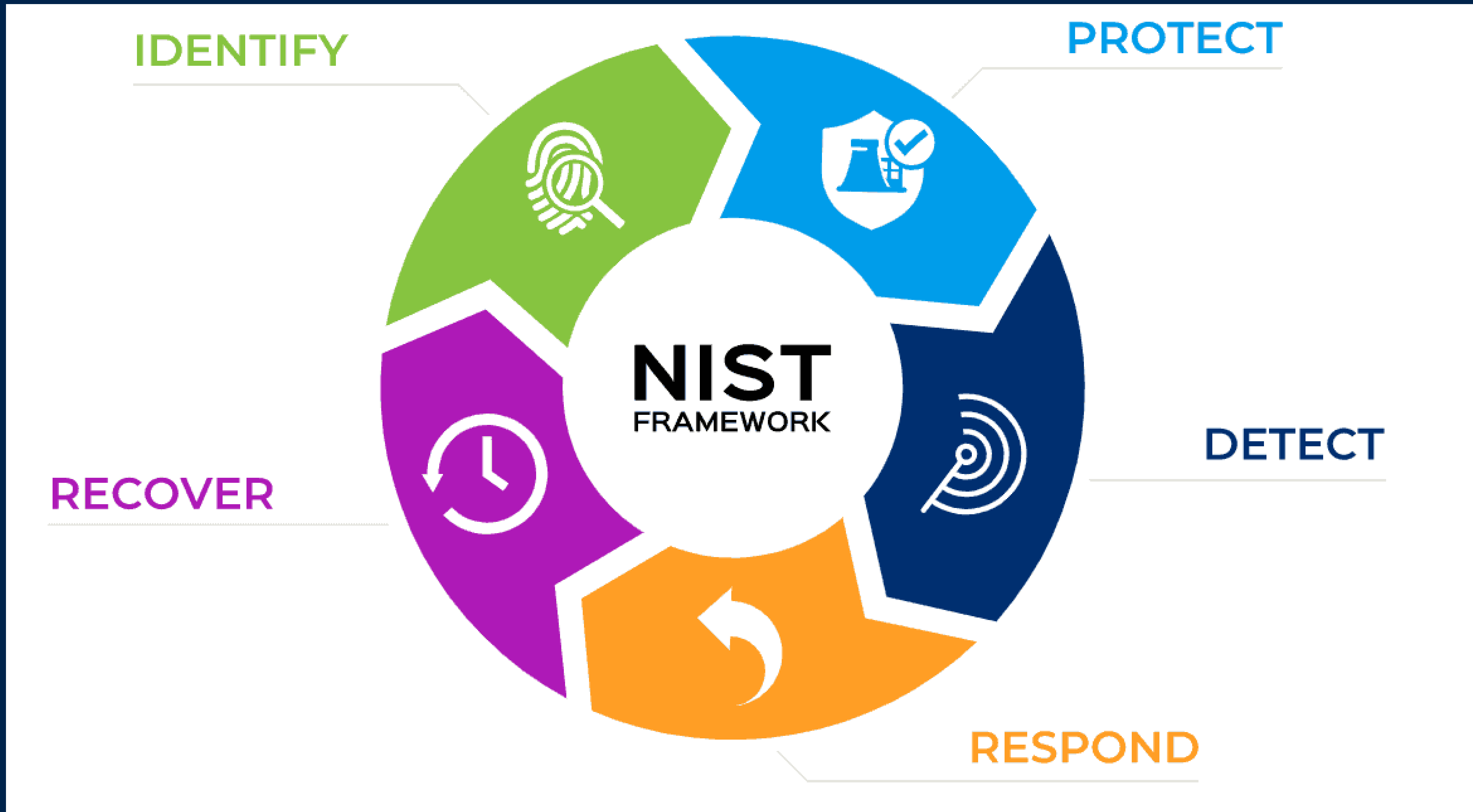
Experienced a cybersecurity breach in the last three years.

Source: Rockwell Automation

5 STEPS

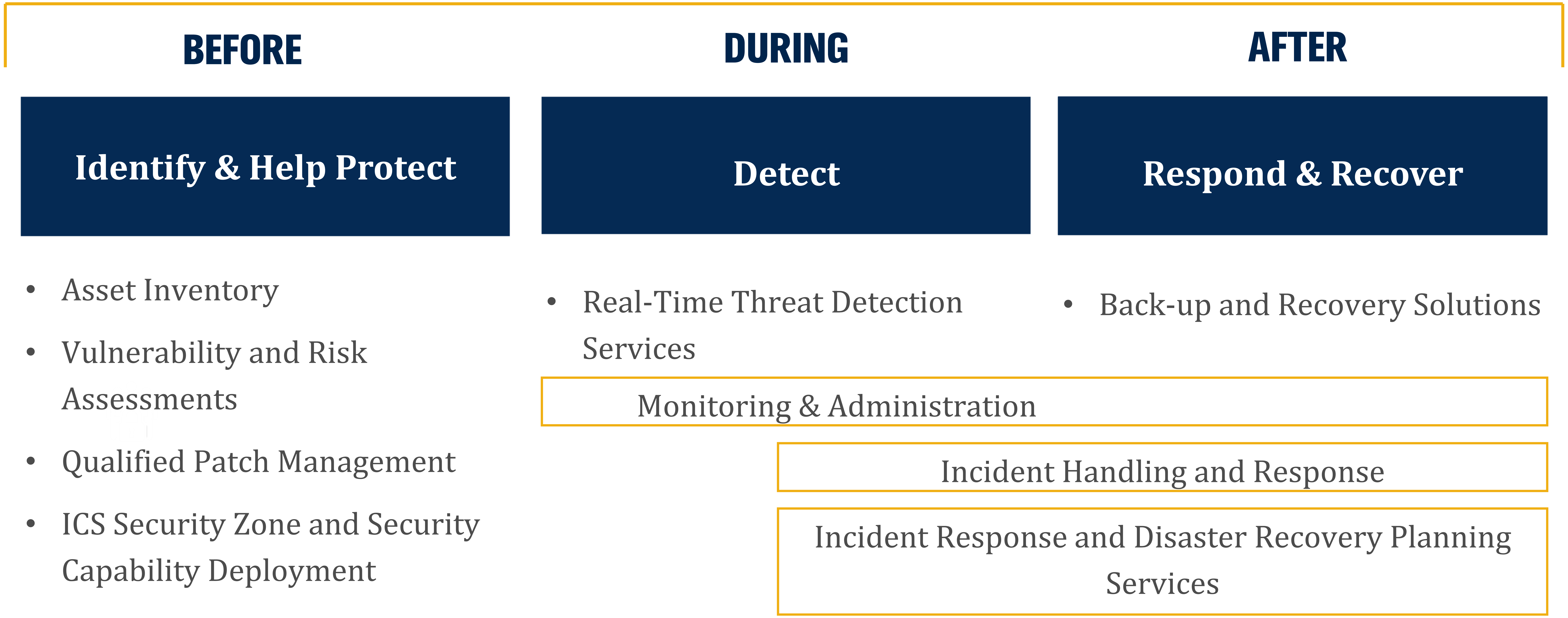
TOWARDS A BETTER CYBERSECURITY PLAN

1. Identify / Document
2. Strategy Development/Review
3. Protect
4. Detect
5. Respond and Recover



ATTACK CONTINUUM

BUILD A SECURE, ROBUST, FUTURE-READY NETWORK



BEFORE

Identify & Help Protect

- Asset Inventory
- Vulnerability and Risk Assessments
- Qualified Patch Management
- ICS Security Zone and Security Capability Deployment

DURING

Detect

- Real-Time Threat Detection Services

AFTER

Respond & Recover

- Back-up and Recovery Solutions

Monitoring & Administration

Incident Handling and Response

Incident Response and Disaster Recovery Planning Services

QUESTION #1

2023 Budget for Cybersecurity

1. 0-$100,000

2. $100,000 - $300,000

3. $300,000 - $500,000

4. > $500,000

STEP 1

IDENTIFY YOUR RISKS

HARDWARE AUDIT

Identify and develop a list of all installed hardware on your Network.

- Servers
- Computers
- Switches
- PLCS
- HMIs
- Cameras

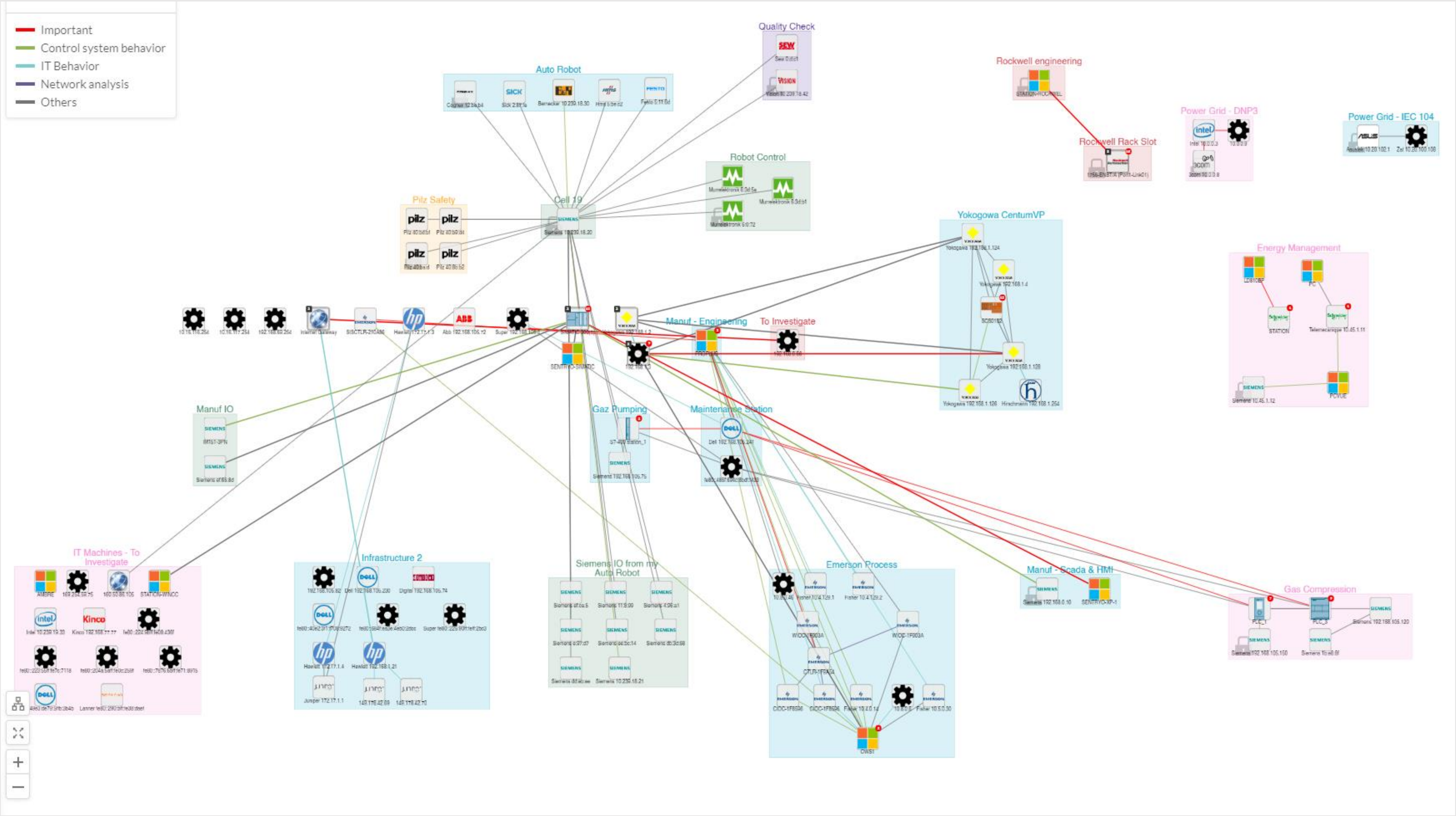
SOFTWARE AUDIT

Develop a list of:

- Installed software
- Activations
- Lifecycle status
- Firmware Level
- Patch Status
- License usage

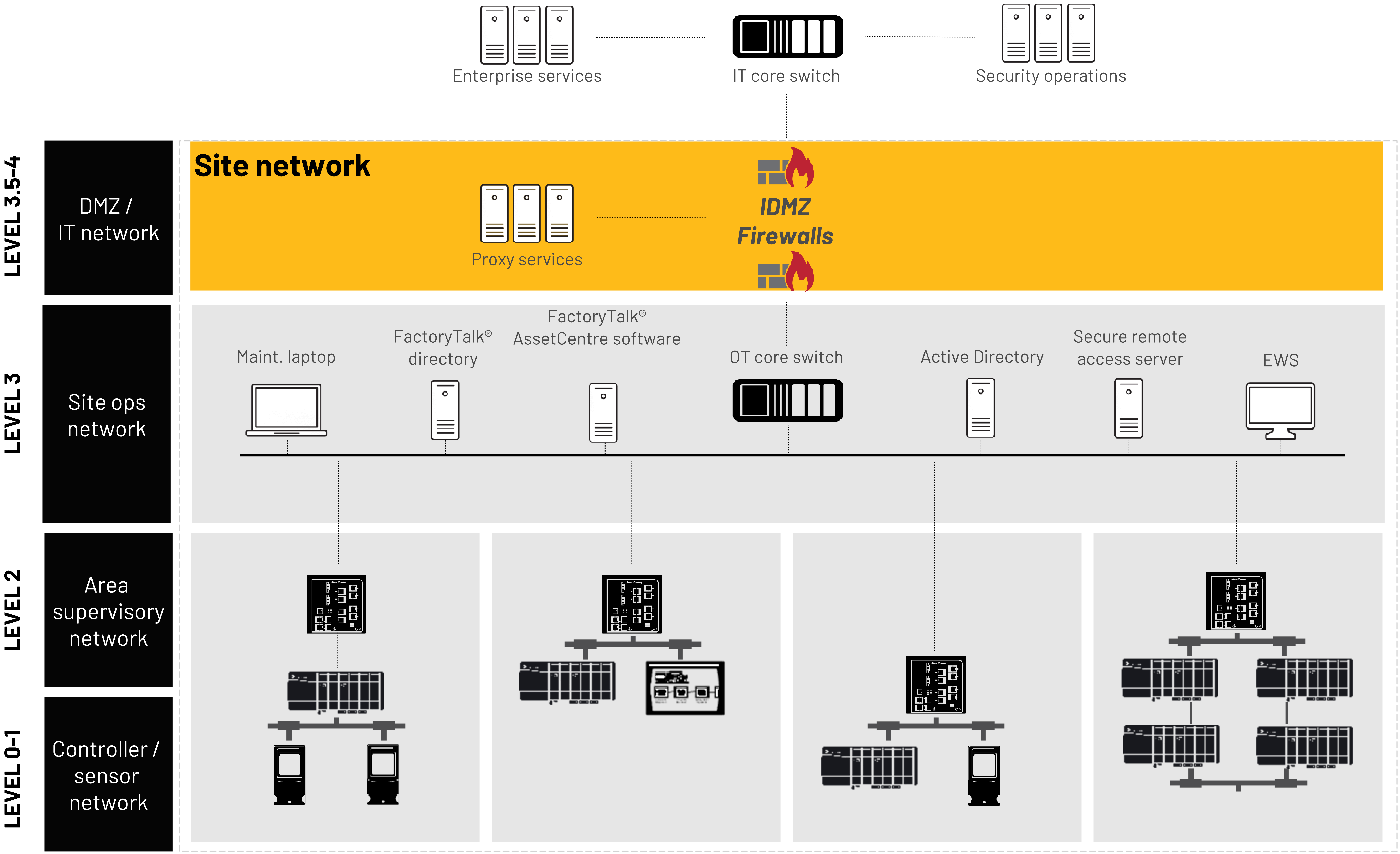
NETWORK DOCUMENTATION STRATEGY

STAY AHEAD OF THE EVER-CHANGING ASSETS AND PLATFORMS



UNDERSTAND YOUR NETWORK

DOCUMENT THE OT NETWORK & INTEGRATION TO THE IT NETWORK



STEP 2

STRATEGY Development/Review

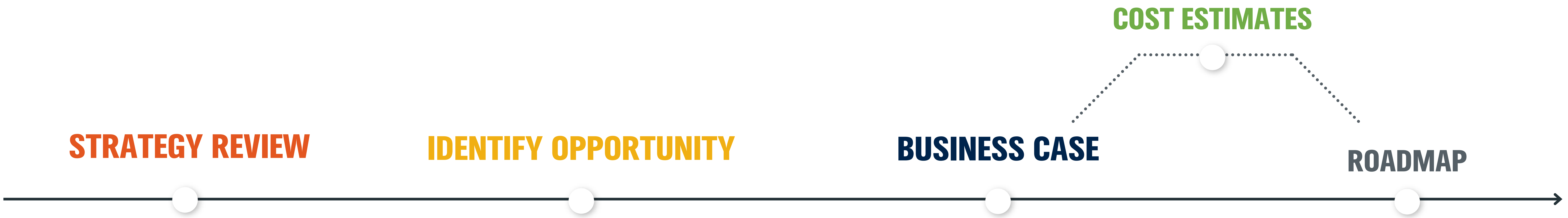
STEP-BY-STEP APPROACH

Develop a Cybersecurity Strategy

&

Build a Roadmap to the Optimal Architecture

STRATEGY ROADMAP



COST ESTIMATES

STRATEGY REVIEW

- Develop a risk-based approach
- Future operating vision
- Cybersecurity Strategy
- Understand Stakeholders
- Align around a defined vision

ACTIVITY
Leadership interviews, workshops, governance models

IDENTIFY OPPORTUNITY

- Conduct Asset Inventory Audits
- Determine Applicable Standards
- Facility Review
- Analyze attack continuum, Define Priority
- Evaluate Risk impact for Projects

ACTIVITY
Plant visits, performance data review

BUSINESS CASE

- Align IT and OT
- Develop Project Scope & Costs
- Determine Financial Stakeholders
- Understand Budget Cycles
- Evaluate workforce skills & support strategy

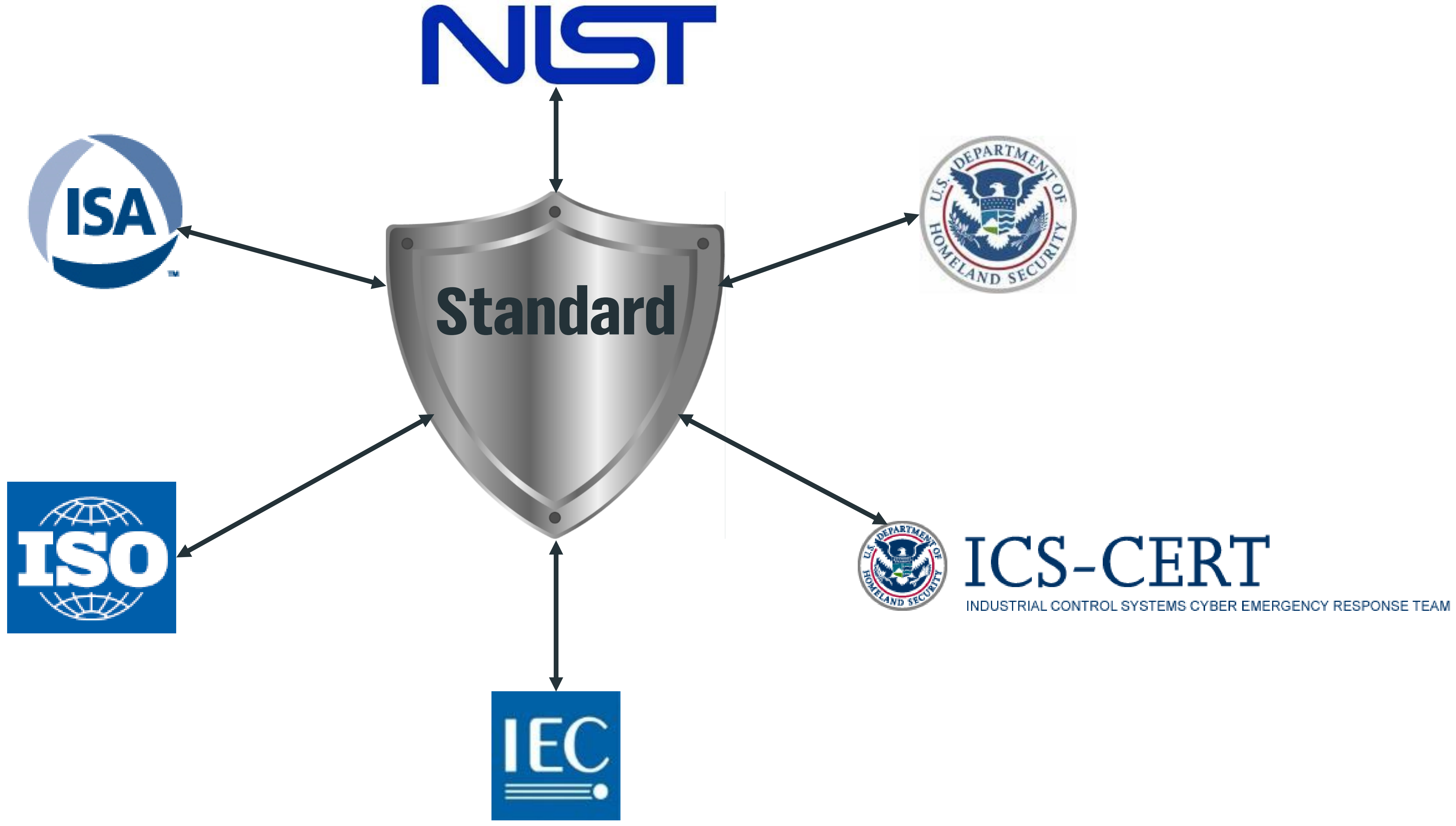
ACTIVITY
Analysis, stakeholder inputs

ROADMAP

- Sequence Projects
- Align on outcomes
- Program Management
- Estimate timelines & resources
- Define multi-year Capex/Opex funding

ACTIVITY
Working sessions, leadership review

DEVELOP A FRAMEWORK LEVERAGING STANDARDS


NIST
ISA
Standard
U.S. DEPARTMENT OF HOMELAND SECURITY
ISO
ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
IEC

IEC-62443

International Electrotechnical Commission

NIST 800-82

National Institute of Standards and Technology

ICS-CERT

Industrial Control Systems Cyber Emergency Response Team

EXT-06-11478

Department of Homeland Security / Idaho National Lab

STEP 3

PROTECT

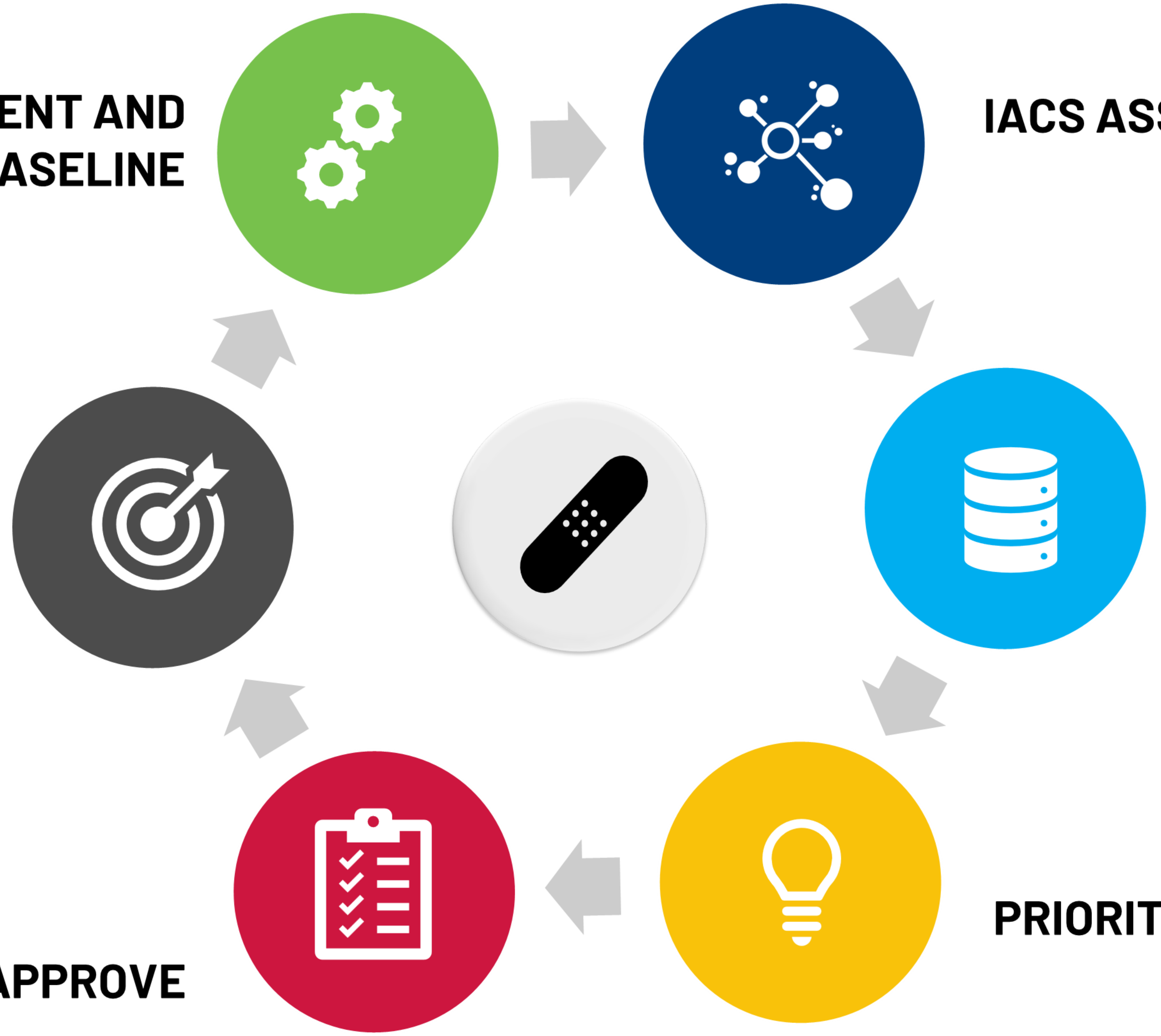
PATCH MANAGEMENT

Scheduled updates of Firmware, Software, and Drivers to Protect against Vulnerabilities

ANTIVIRUS & ENDPOINT PROTECTION

Incorporate and Manage Antivirus Protection wherever possible

IACS PATCH MANAGEMENT



DOCUMENT AND ESTABLISH BASELINE

IACS ASSET INVENTORY

ASSEMBLE VULNERABILITY / PATCH INFORMATION

PRIORITIZE VULNERABILITY

REVIEW AND APPROVE

TEST AND DEPLOY

Next Gen Antivirus

Machine Learning
Block Known Bad
IOA Behavioral Blocking
Exploit Blocking

Machine Learning

The ability to identify malicious files and activity based on the attributes of previous attacks.

IOA Behavioral Blocking

Block attacks based on intent of the behavioral of the attacker regardless of the malware or exploit used in an attack

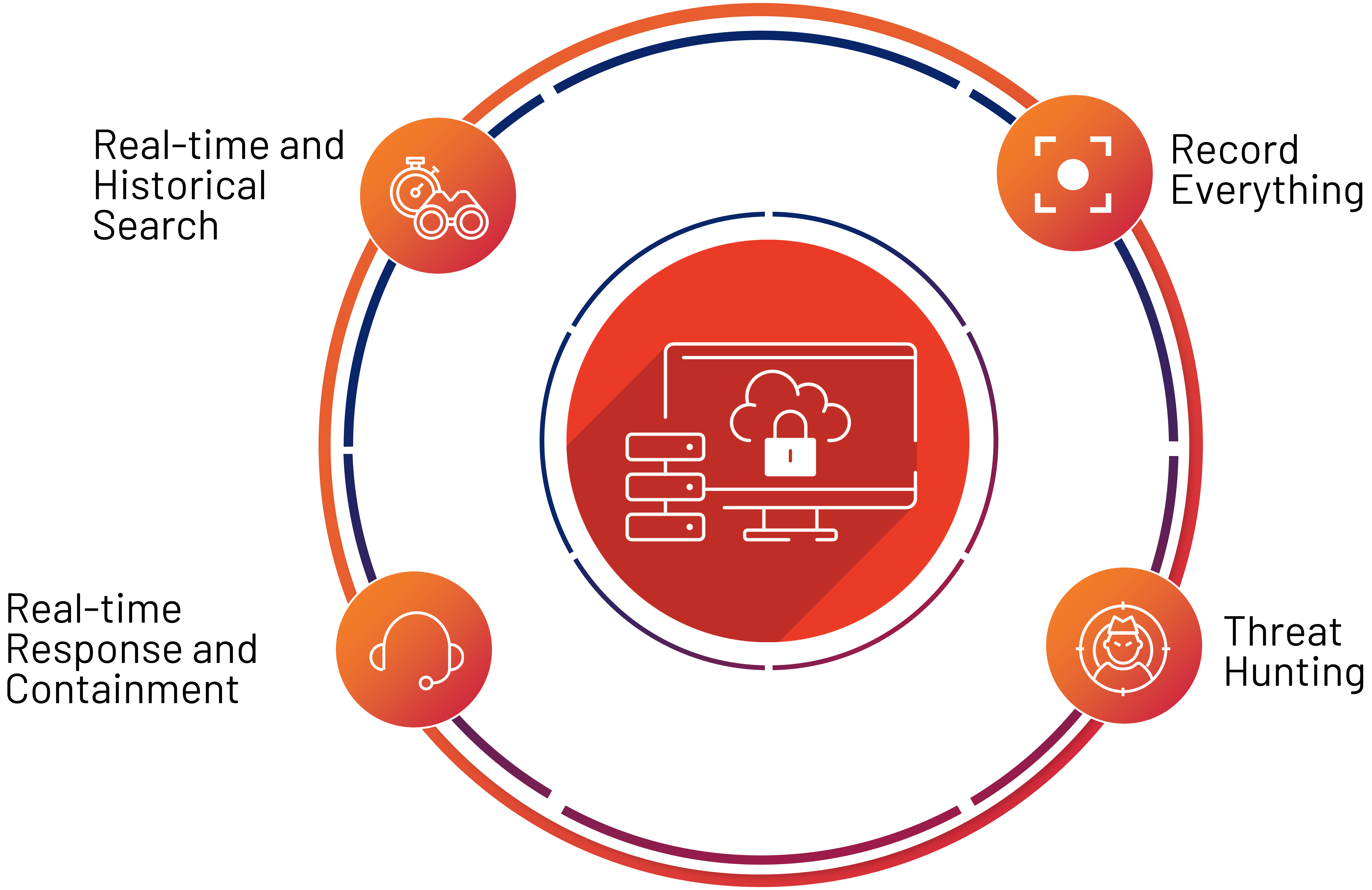
Block Known Bad

Block known bad malicious threats

Exploit Blocking

Block exploits and techniques used in malware and fileless attacks

Endpoint Detection


Real-time and Historical Search
Record Everything
Real-time Response and Containment
Threat Hunting

Record Everything
All activities are tracked and stored

Real-time Historical Search
Historical database of all activities with ability to search those records

Real-time Response and Containment
Accelerate response and containment efforts conducting real-time forensic analysis and remediating system remotely

Threat Hunting
Block exploits and techniques used in malware and fileless attacks

STEP 4

DETECT

REAL TIME THREAT DETECTION

Monitor & Configure Alerts to Identify New Devices

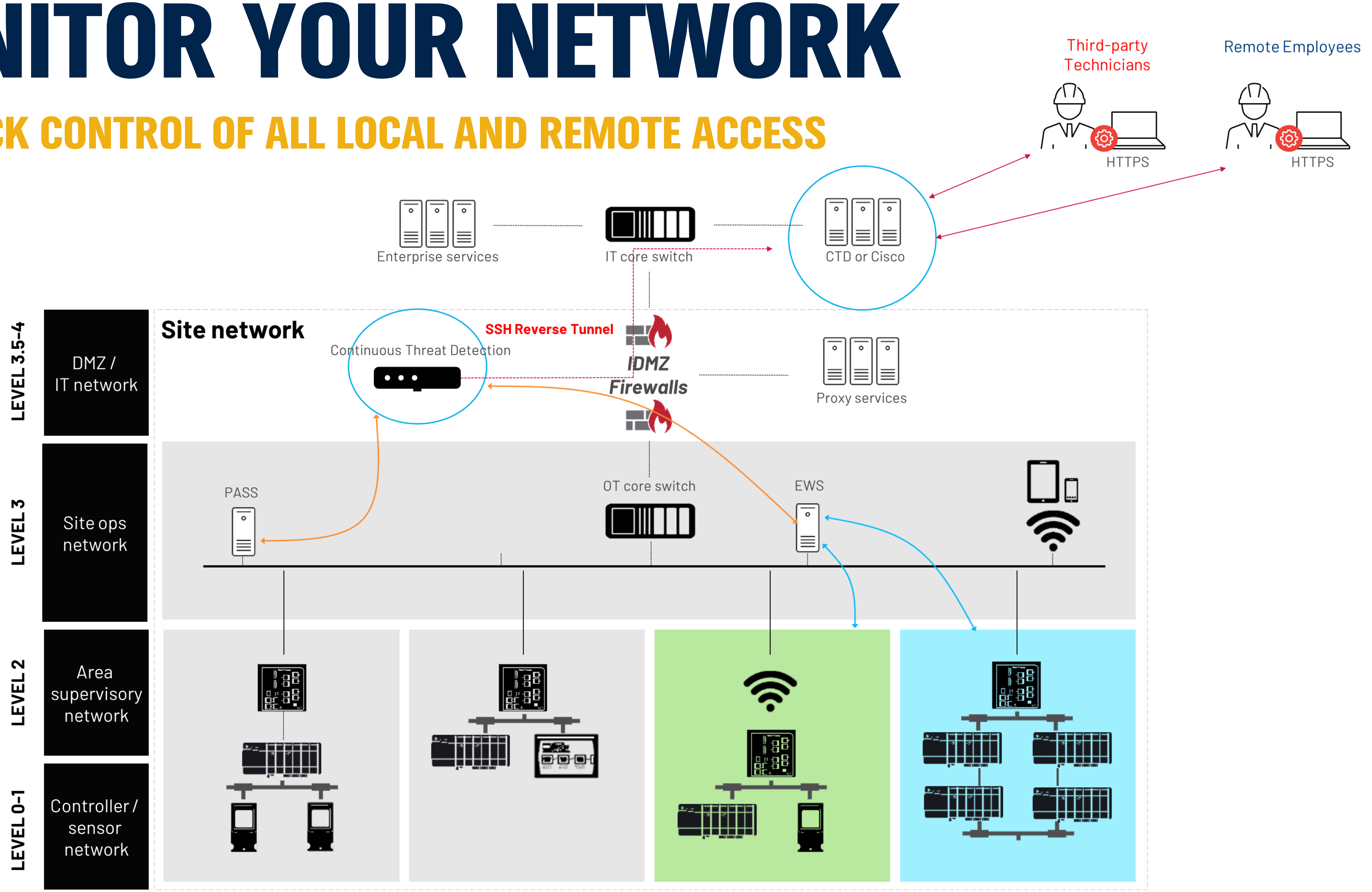
Identify both Internal/External Threats

ACCESS CONTROL

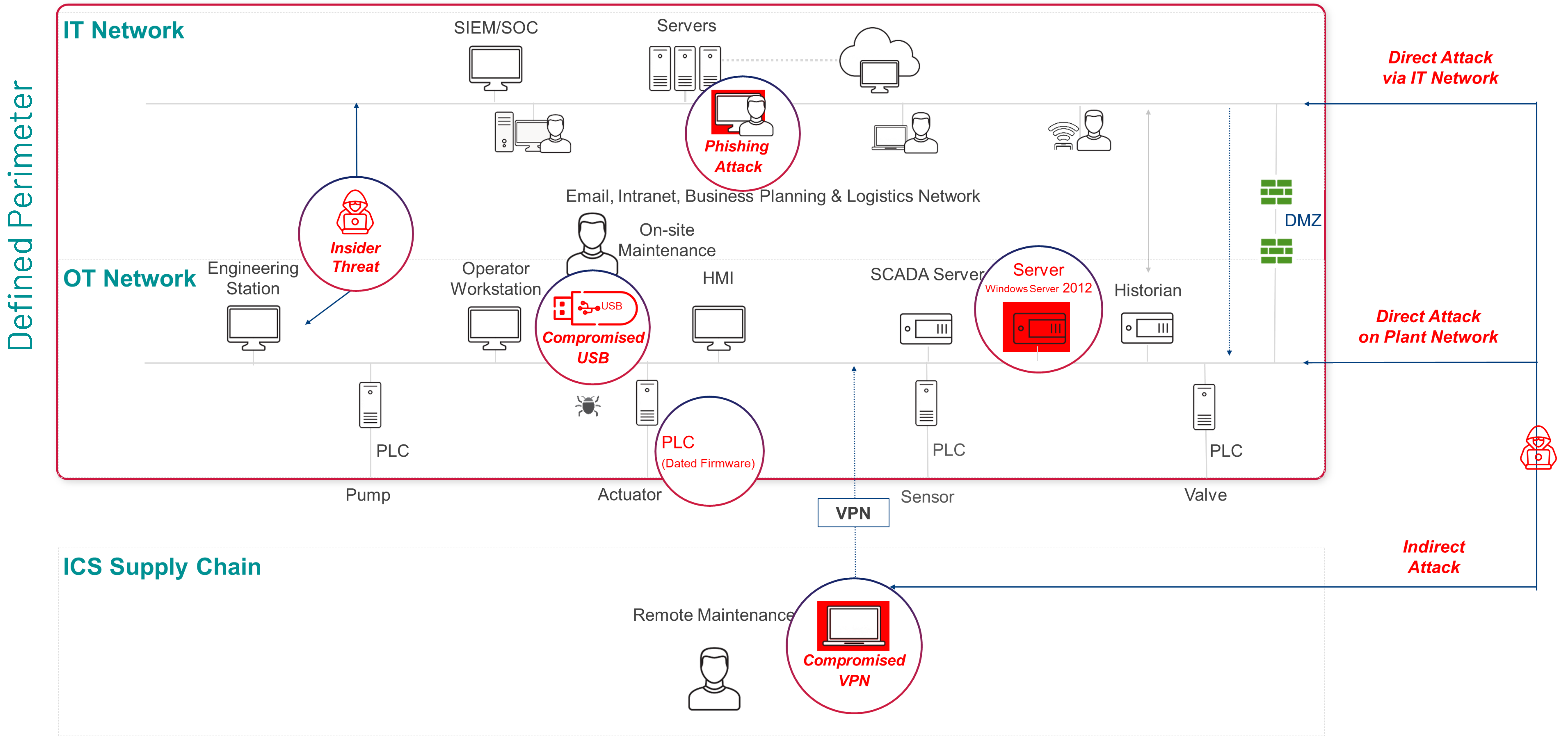
Actively Control both Internal/External Access to Your Network

MONITOR YOUR NETWORK

TAKE BACK CONTROL OF ALL LOCAL AND REMOTE ACCESS



UNDERSTAND YOUR COMMON THREAT VECTORS



QUESTION #2

2022 Critical Cybersecurity Attacks

1. No Attacks

2. 1-3

3. 3-5

4. > 5

STEP 5

RESPOND AND RECOVER

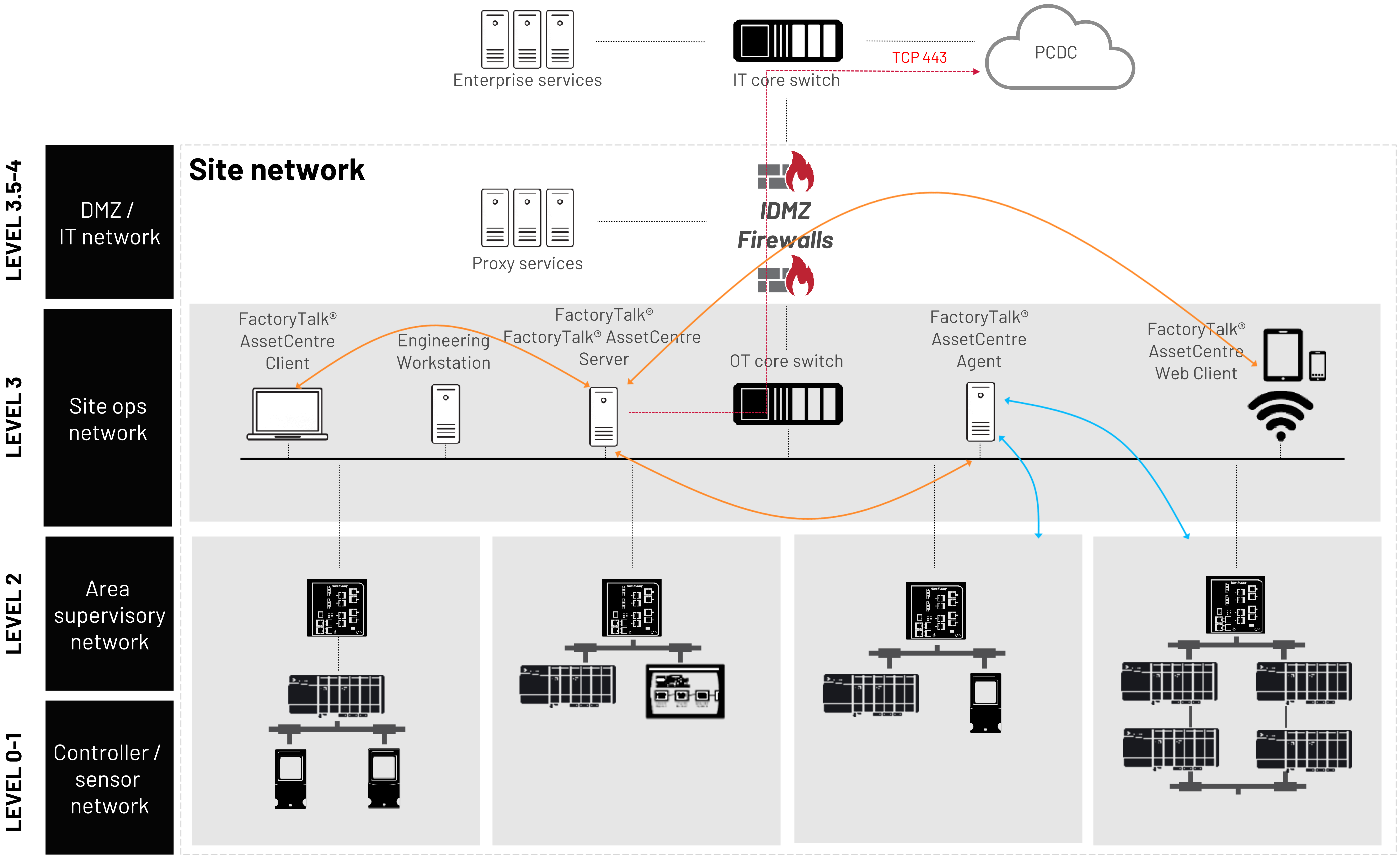
CENTRALIZED BACKUP MANAGEMENT

Utilize Backup Management Software & Incorporate Periodic Backup Stored Onsite & Offsite

CONTINOUS ASSESSMENT & REVIEW

Leverage outside vendors to periodically assess your Vulnerabilities

Centralized Backup Management Software & Disaster Recovery



Asset inventory

- Protocol Specific asset discovery:
  - EtherNet/IP, SNMP, WMI
- Vendor agnostic

Asset Change Management

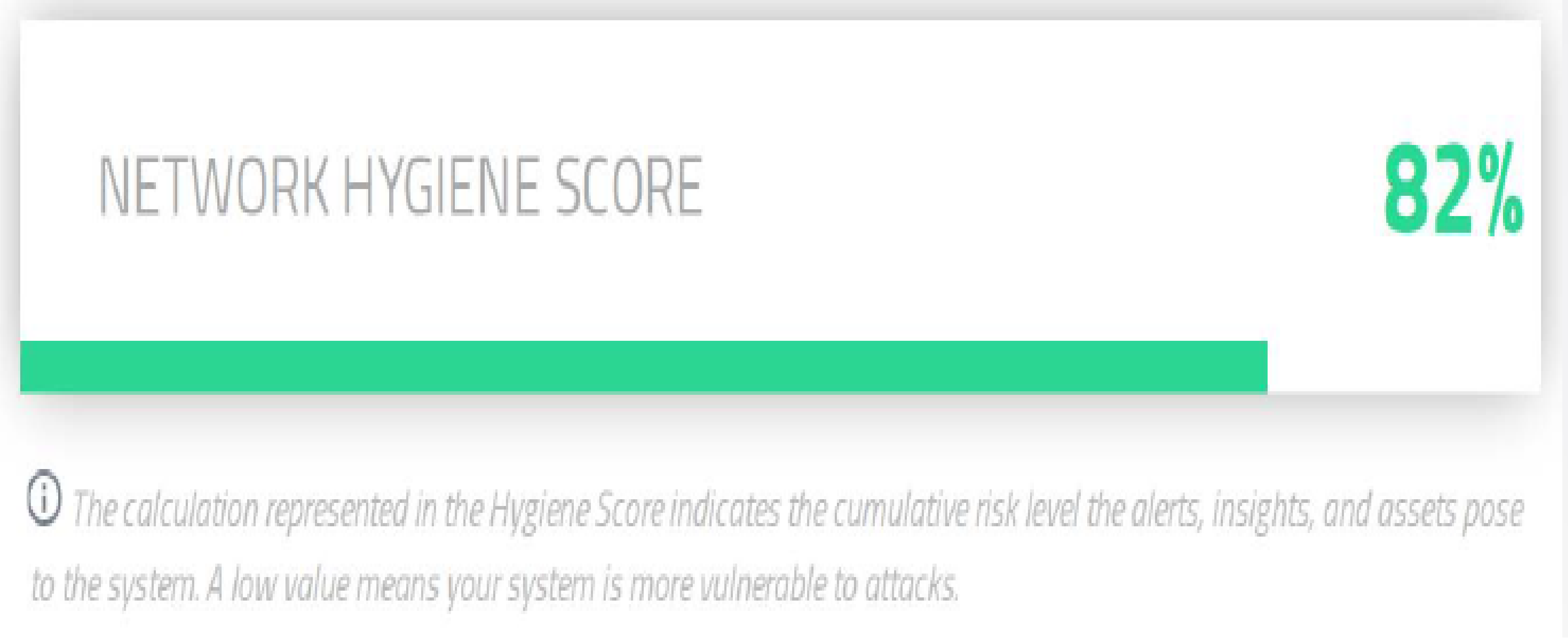
- Agnostic Change management
- Firmware availability
- Lifecycle status via outbound TLS 1.2 on port 443 to api.rockwellautomation.com
- IPSEC or HTTPS support
- Vulnerability reporting
- Immediate Change Detect

Asset Disaster Recovery

- Automated back-up
- Application change detection

CONTINOUS REVIEW & ASSESSMENT

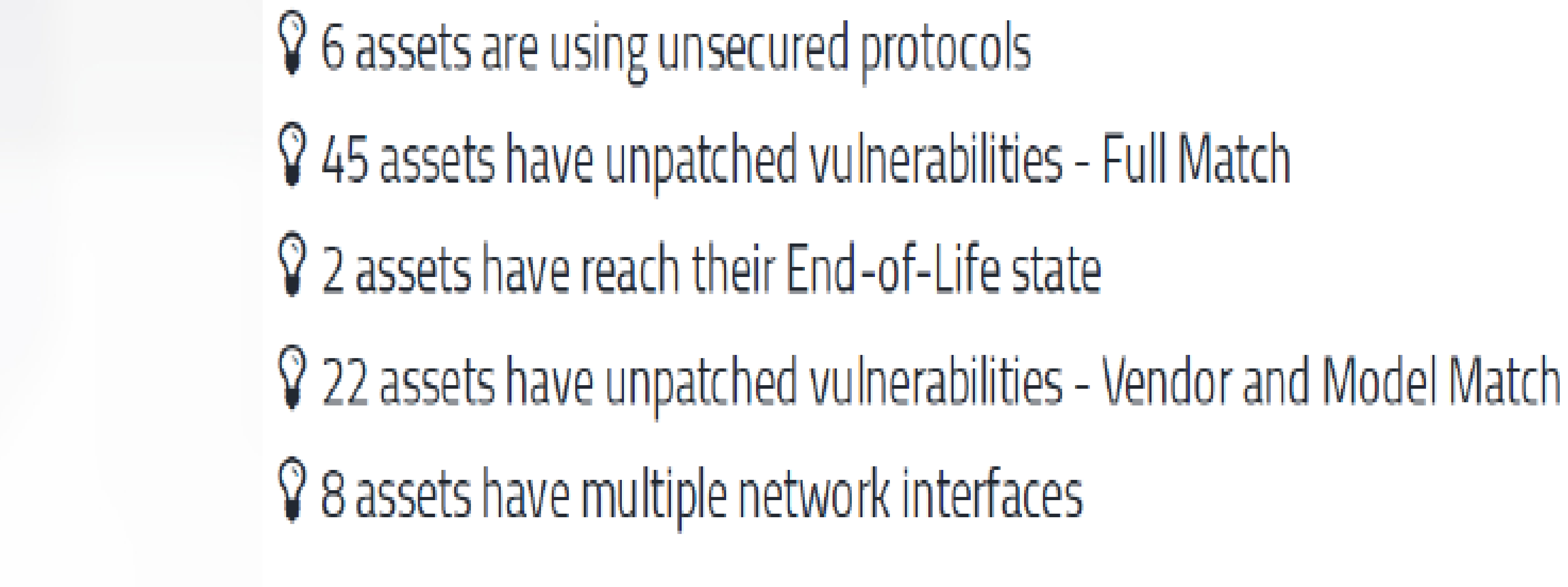
Vulnerability Discovery Survey



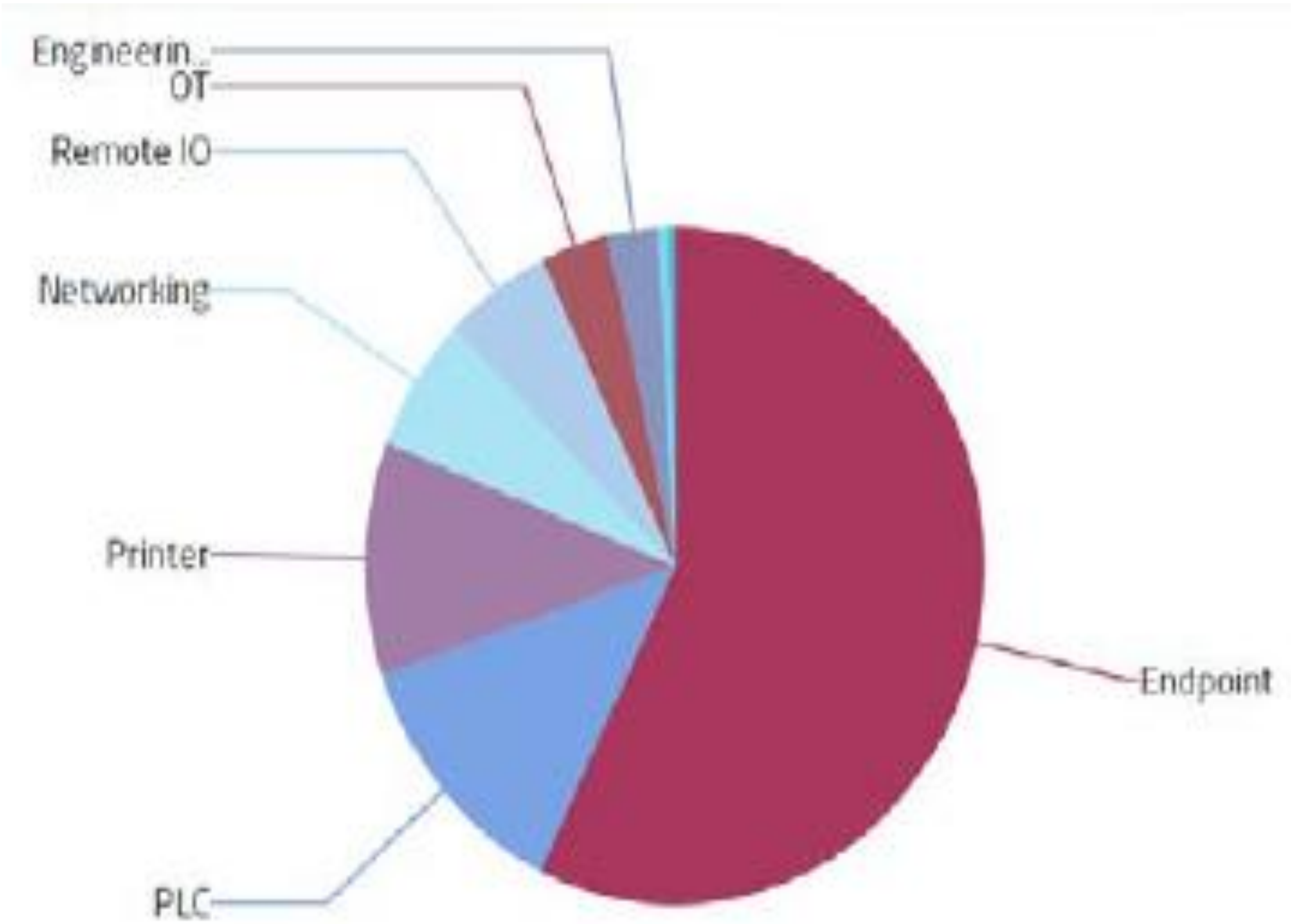
NETWORK HYGIENE SCORE

82%

ⓘ The calculation represented in the Hygiene Score indicates the cumulative risk level the alerts, insights, and assets pose to the system. A low value means your system is more vulnerable to attacks.



- 6 assets are using unsecured protocols
- 45 assets have unpatched vulnerabilities - Full Match
- 2 assets have reach their End-of-Life state
- 22 assets have unpatched vulnerabilities - Vendor and Model Match
- 8 assets have multiple network interfaces



5 STEPS

TOWARDS A BETTER CYBERSECURITY PLAN

1. Identify / Document
2. Strategy Review
3. Protect
4. Detect
5. Respond and Recover

smart
SOLUTIONS SUMMIT

VAN METER

Additional Questions or Discussion?

Jason Vandenberg
Rockwell
Cybersecurity Consultant

Jason Lutz
Rockwell
Industrial Networks &
Cybersecurity Specialist

Scott Larson
Van Meter
Business Consultant

ICS Cyber Resources from Rockwell Automation

Cybersecurity Preparedness Survey- NIST-CSF
Link: Industrial Cybersecurity Solutions | Rockwell Automation

Rockwell Product Compatibility and Download Center (PCDC)
Link: Product Compatibility & Download Center from Rockwell Automation

KnowledgeBase (Included in Tech Connect contracts, ie. Tech Support)
Link: Rockwell Automation Tech Support ... 24 x 7 around the globe! (custhelp.com)

Cisco/ Rockwell Ratified Architecture Design Guides:
Link: Search Rockwell Automation

Microsoft OS Patching Qualifications:
Link: Microsoft Patch Qualifications | Rockwell Automation

WE WANT TO HEAR FROM YOU!

BREAKOUT SESSION FEEDBACK