



**Rockwell
Automation**

Security: Why, Where and What Should I do

Steve Wynne

Business Development Lead.
Network and Security Services.

INDUSTRIAL SECURITY CHALLENGES

NOT BEING PREPARED CAN BE CATASTROPHIC WITH NEW THREATS EMERGING CONSTANTLY

Complexity exposes threats



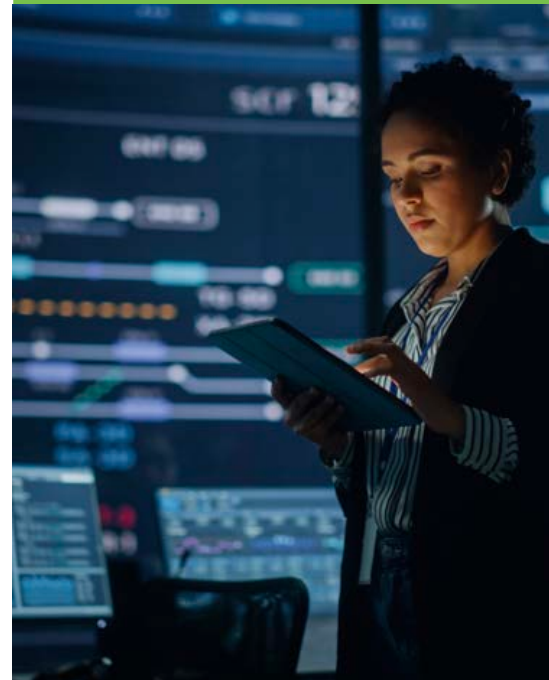
75% of executives believe infrastructure is too complex

Sophisticated attacks



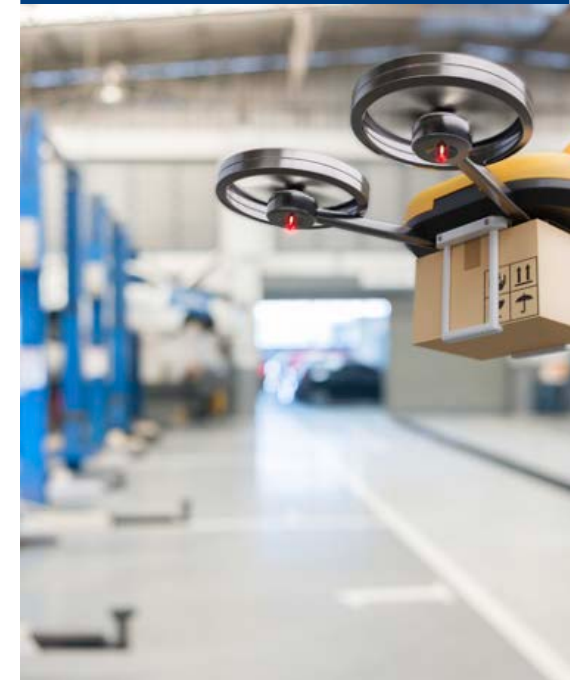
2/3 attacks are facilitated by ransomware-as-a-service

Widening skills gap



Cybersecurity job openings in U.S. up 29% in the past 12 months

Emerging threats



IoT devices suffer an average 5,200 cyberattacks per month

#CYBER RISK JULY 28, 2017 / 5:56 AM / 10 DAYS AGO

Merck says cyber attack halted production, will hurt profits

Michael Erman and Jim Finkle

4 MIN READ

“Merck, whose ability to manufacture some drugs was temporarily shut down by NotPetya, told shareholders it lost a staggering **\$870 million due to the malware.**” – Wired - 8-22-2018

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



U.S. Attorneys » Middle District of Louisiana » News

Department of Justice

U.S. Attorney's Office

Middle District of Louisiana

SHARE

IMMEDIATE RELEASE

Thursday, February 16, 2017

Former Systems Administrator Sentenced to Prison for Hacking into Industrial Facility Computer System

Renault, Nissan European operations deal with global cyber attack

May 13, 2017 @ 7:49 am

Mathieu Rosemain, Yann Le Guernigou and James Davey
Reuters

0 Shares

THIS WEEK'S ISSUE

ICS Threat Actors

Nation States

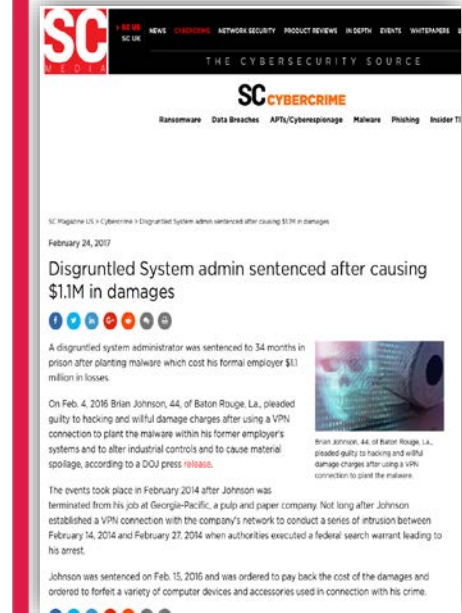
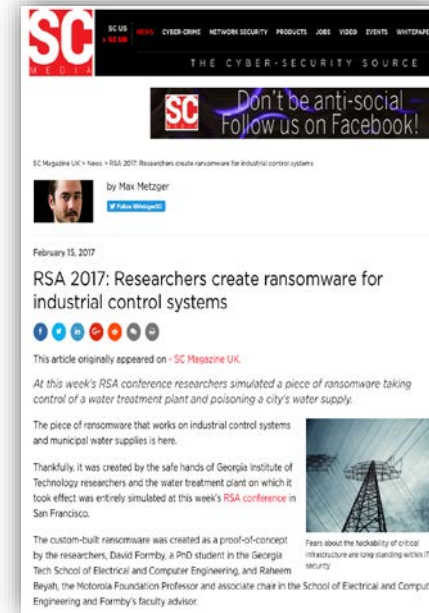
Terrorists

Hacktivists

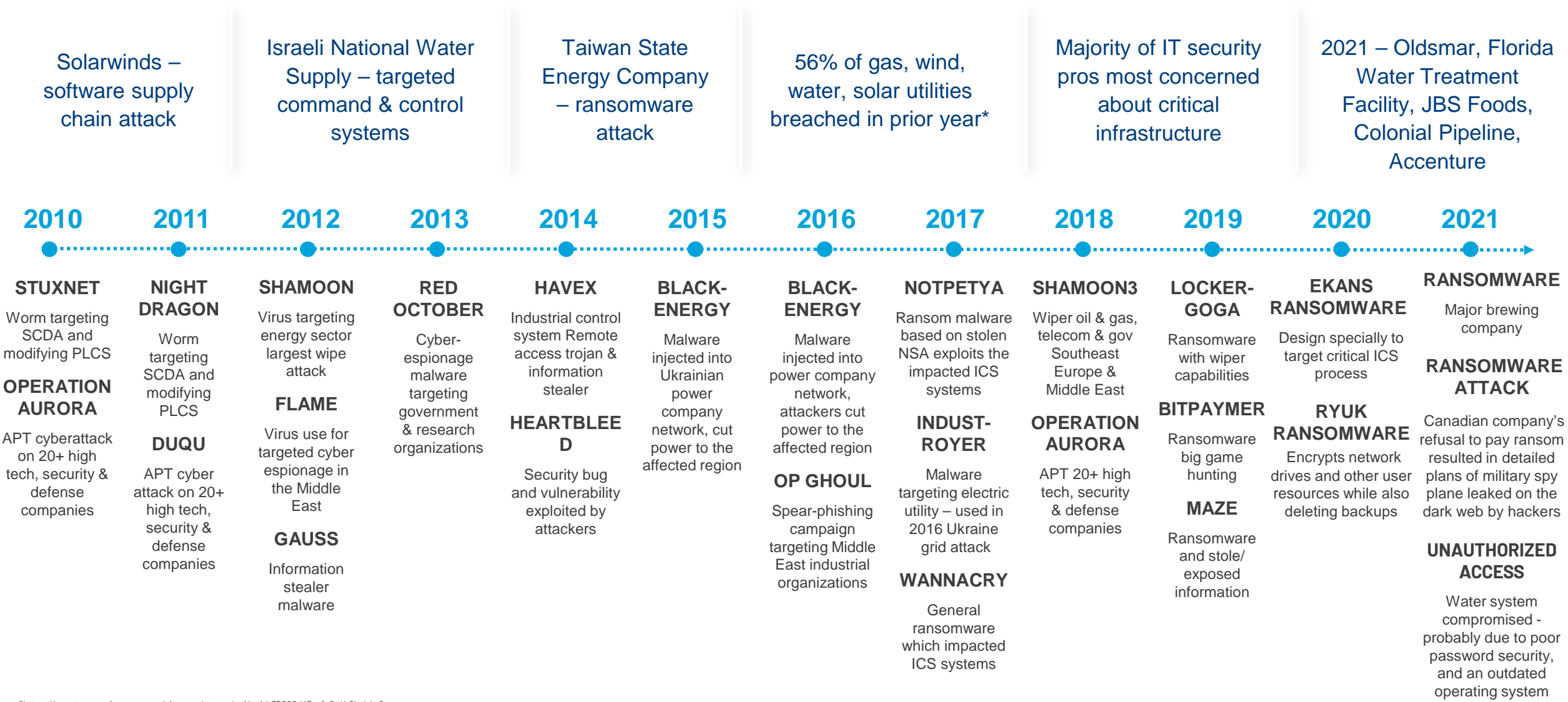
Cyber Criminals

> 40%
Cyber Events

Insiders



ICS-Focused campaigns, attacks



Solarwinds – software supply chain attack

Israeli National Water Supply – targeted command & control systems

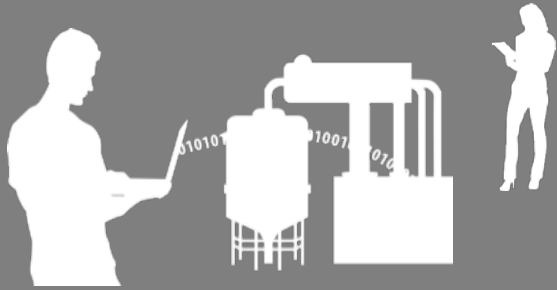
Taiwan State Energy Company – ransomware attack

56% of gas, wind, water, solar utilities breached in prior year*

Majority of IT security pros most concerned about critical infrastructure

2021 – Oldsmar, Florida Water Treatment Facility, JBS Foods, Colonial Pipeline, Accenture

*<https://assets.new.siemens.com/siemens/assets/api/uuid:35089d45-etc2-4b8b-b4e9-7ed0aee81e0a/version:16001019/siemens-cybersecurity.pdf>
https://www.siemens.com/press/press-releases/state_of_industrial_cybersecurity_form



The Approach

Strategic

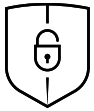
- Develop an OT cybersecurity program
- Adopt an industry framework
- Understand business drivers and risk tolerances to drive target profiles
- Conduct assessments to develop an understanding of gaps
- Create an improvement plan to drive the tactical approach

Tactical

- Execute on filling gaps as defined and prioritized in the strategic approach
- Utilize validated designs and architectures
- Implement pre-engineered infrastructure and software solutions to achieve targets



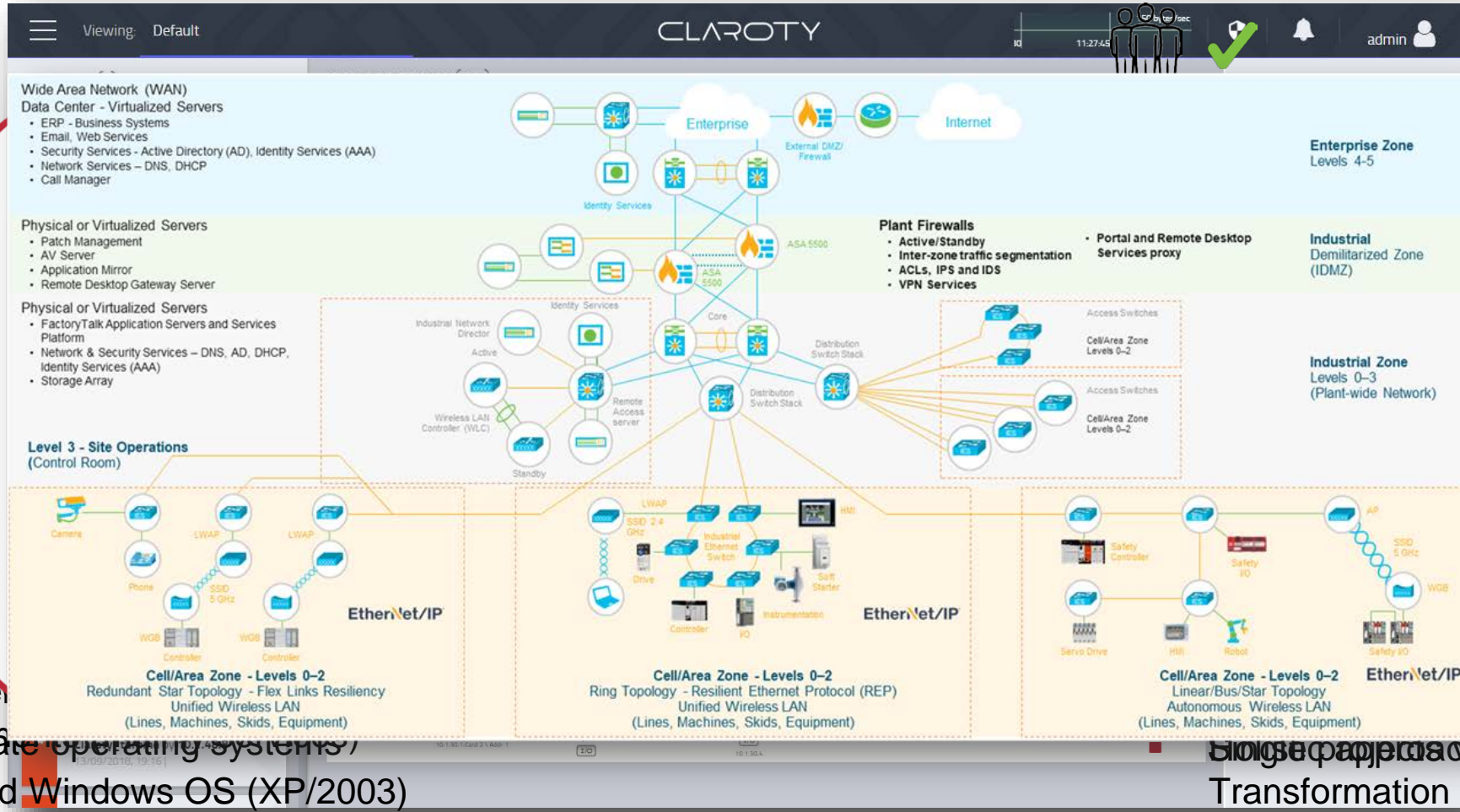
Industrial Infrastructure – secure and reliable



- Existing standards
- Missile (Patch)
- Secure network



- Mainframe
- Data center
- requirement
- Outdated operating systems /
- Outdated Windows OS (XP/2003)

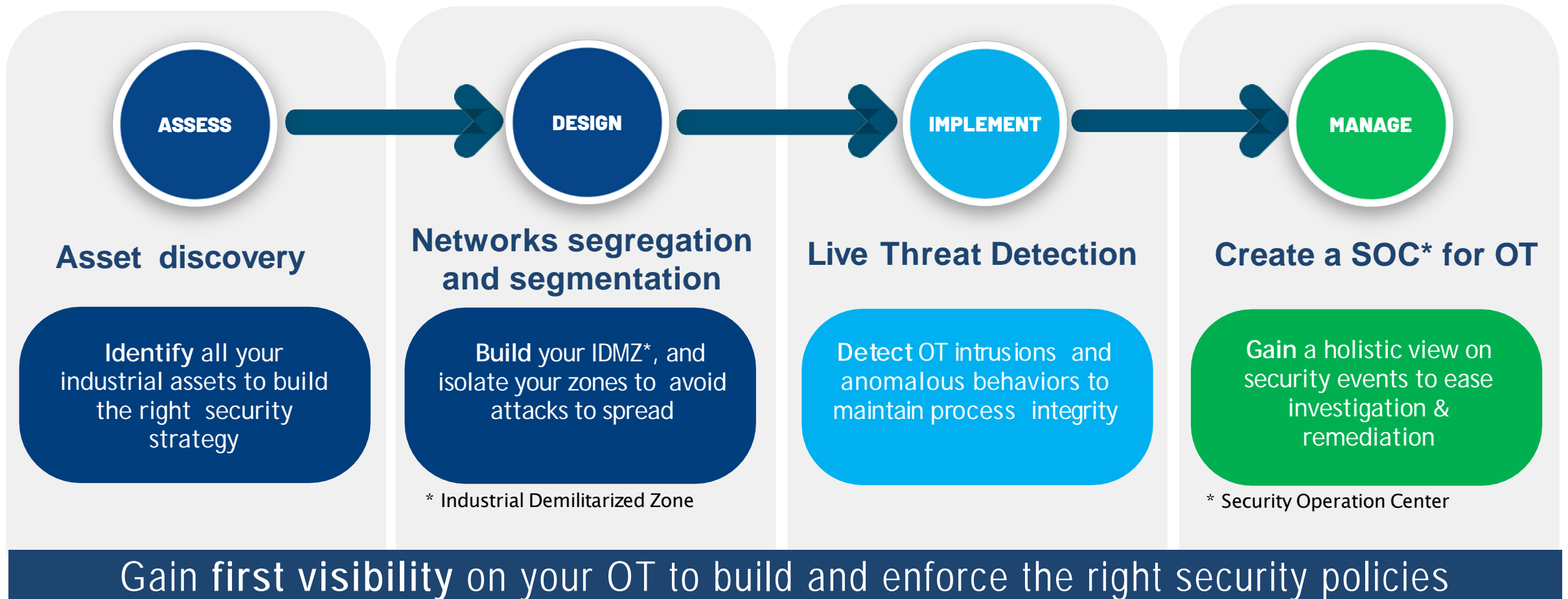


procedures
user

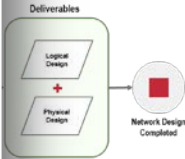
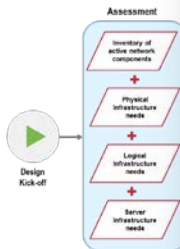
OT and OT
ability
responsibility

Single paper works for digital approach
Transformation

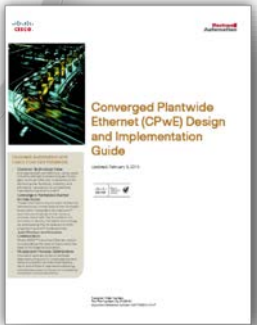
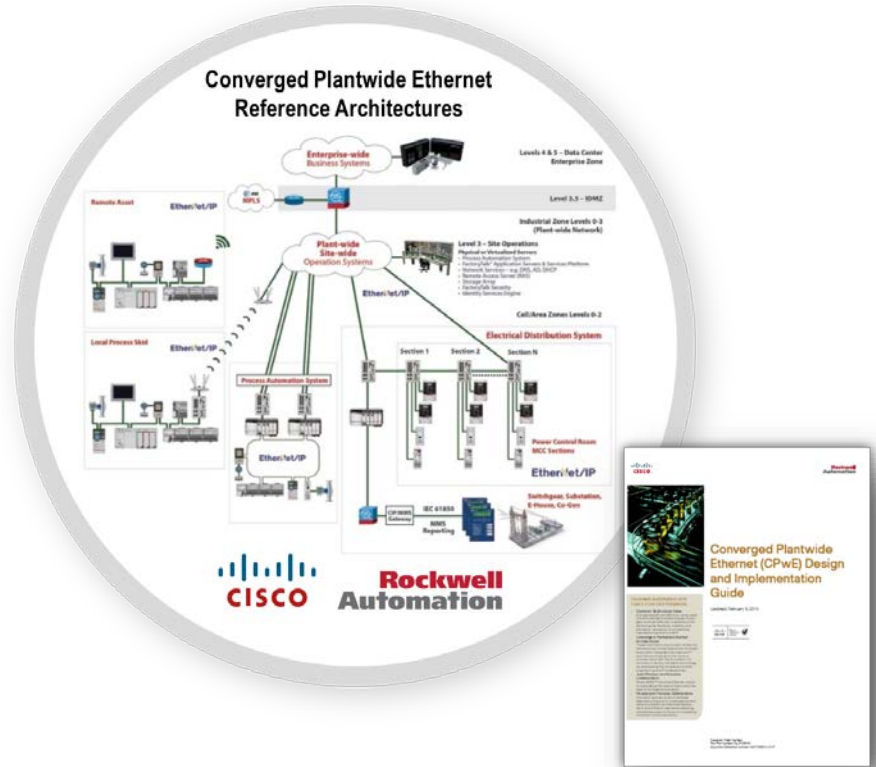
The 4-step journey to secure your ICS



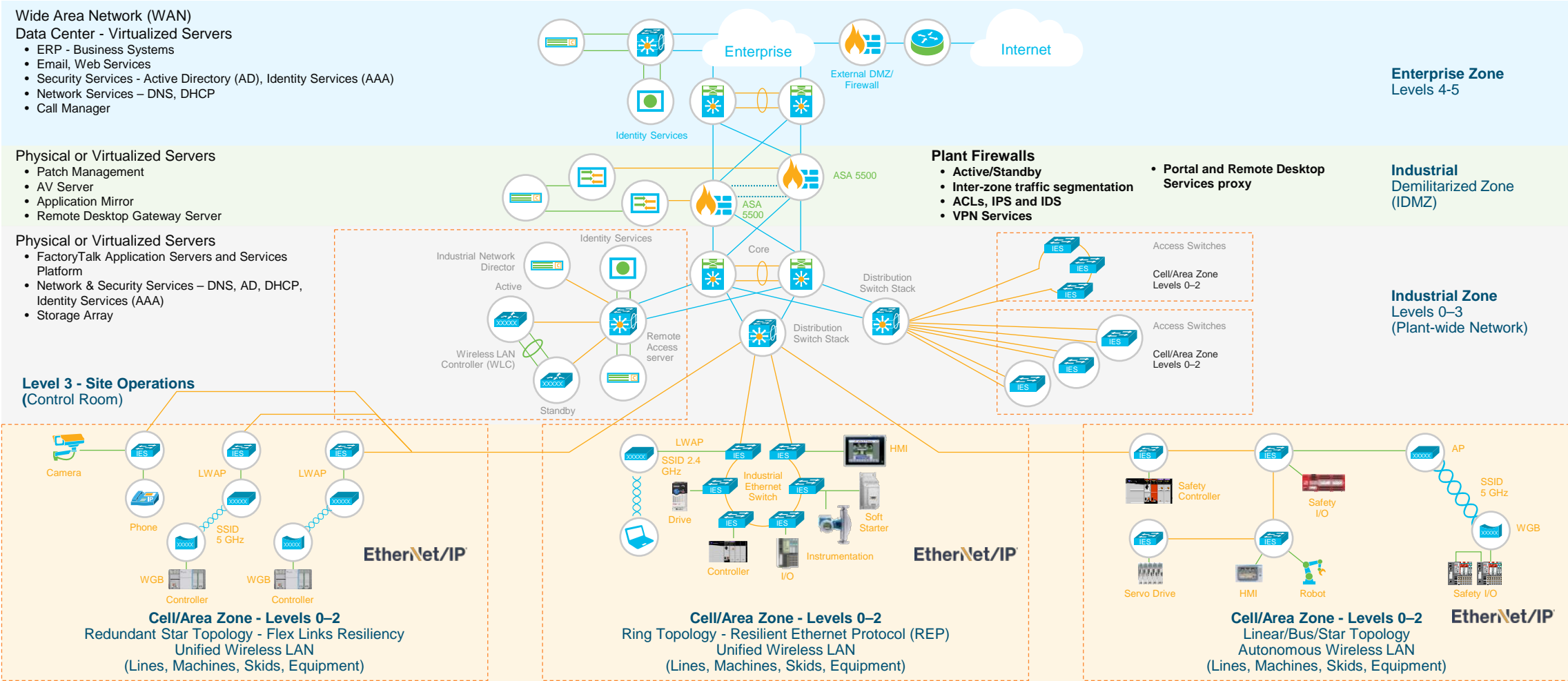
Secure and Reliable Network Infrastructure



- Create standard set up (CPwE)
- Proven Performance and Reliability
- Cyber Security ready (IEC 62443)
- Remote Monitoring and Remote Support



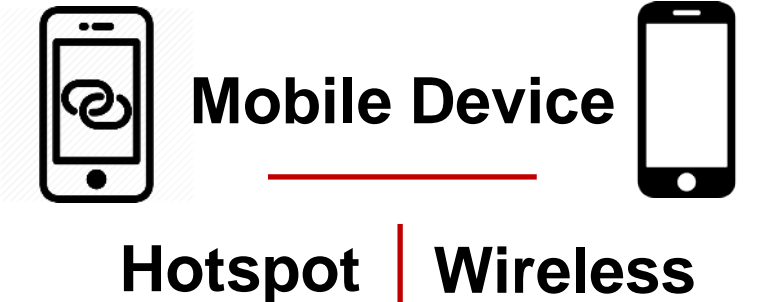
A holistic blueprint for digital transformation



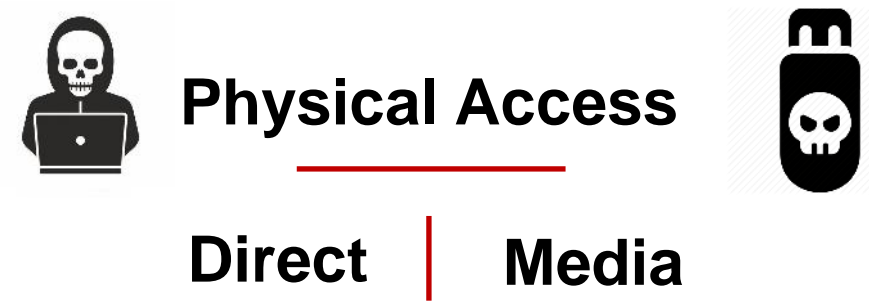
ICS Threat Vectors



Network based threat vector is most typically associated with remote access.

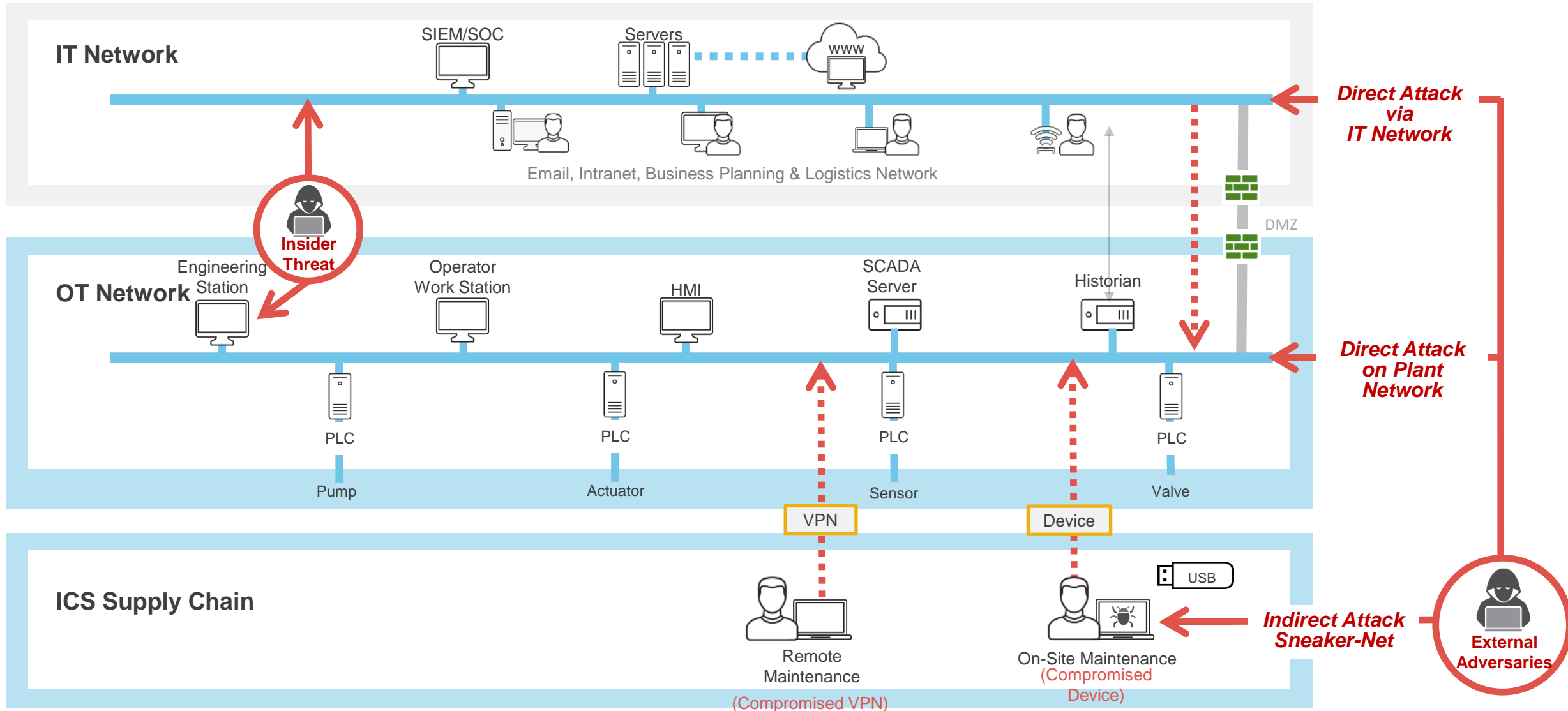


1. Mobile hotspot can present direct internet access to device
2. Inadvertent physical connection to target



1. Direct access to target by adversary
2. SneakerNET: Inserting malicious removable media to target

ICS THREAT VECTORS



Cyber Security Strategy – a Holistic Approach



security countermeasures

ty of vendors in our

ds, including policies &

ectives and Standards

of protection

implemented

CPNI
Centre for the Protection
of National Infrastructure



IEC 62443 is a collection of standards for IACS

General		Policies & Procedures		System		Components & Products	
1-1	Models and concepts	2-1	Requirements for an IACS security management system	3-1	Security technologies for IACS	4-1	Product development requirements (ML2) ✓
1-2	Master glossary of terms and abbreviations	2-2	Implementation guidance for an IACS security management system	3-2	Security Risk Assessment and System Design	4-2	Technical security requirements for IACS components (SL1) ✓
1-3	System security compliance metrics	2-3	Patch management in the IACS environment	3-3	System security requirements and security levels (SL1) ✓		
1-4	IACS security lifecycle and use-case	2-4	Security program requirements for IACS service providers (ML3) ✓				
		2-5	Implementation guidance for IACS asset owners				

System Design and Delivery:

2-4 Integrator Certification – Demonstrates ability to deliver and support a secure solution.

3-3 System Certification - Suppliers will provide a system designed with security in mind and provide guidance on operation and lifecycle management.

Product and Product Process:

1 Product Development Certification (PDP)

Demonstrates secure development lifecycle.

2 Product Certification - Demonstrates product development and support conforms to PDP process.

NIST Cybersecurity Framework

Functions	Categories
IDENTIFY (ID)	Asset Management (AM)
	Business Environment (BE)
	Governance (GV)
	Risk Assessment (RA)
	Risk Management Strategy (RM)
PROTECT (PR)	Access Control (AC)
	Awareness and Training (AT)
	Data Security (DS)
	Information Protection Processes and Procedures (IP)
	Maintenance (MA)
	Protective Technology (PT)
DETECT (DE)	Anomalies and Events (AE)
	Security Continuous Monitoring (CM)
	Detection Processes (DP)
RESPOND (RS)	Incident Response Planning (RP)
	Communications (CO)
	Analysis (AN)
	Mitigation (MI)
	Improvements (IM)
RECOVER (RC)	Recovery Planning (RP)
	Improvements/Gap Remediation (IM)
	Communications (CO)



Know what you have



Secure what you have



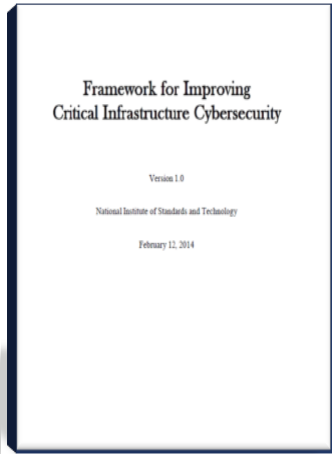
Spot threats quickly



Take action immediately



Restore operations



Compliance & Standards

Certified Products, Architectures and Solution Delivery

ISA/IEC 62443: Series of standards that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS).

Applies to those responsible for ***designing, manufacturing, implementing or managing*** industrial control systems:

- End-users (i.e. asset owner)
- System integrators
- Security practitioners
- ICS product/systems vendors

**Equivalence to ISO 27001 and NIST Cybersecurity Framework*

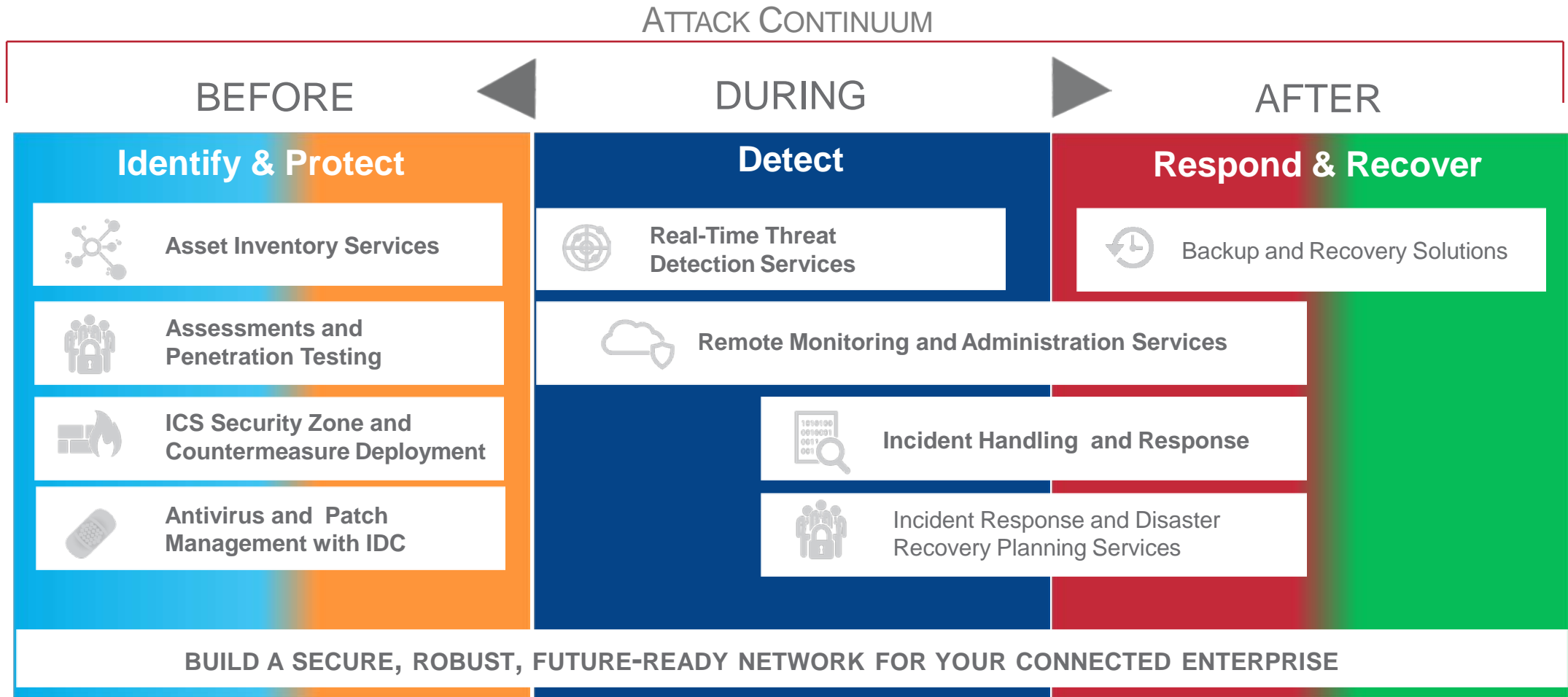


NIST



NIST - Cybersecurity Framework

The Risk-Based Approach to Secure ICS Networks

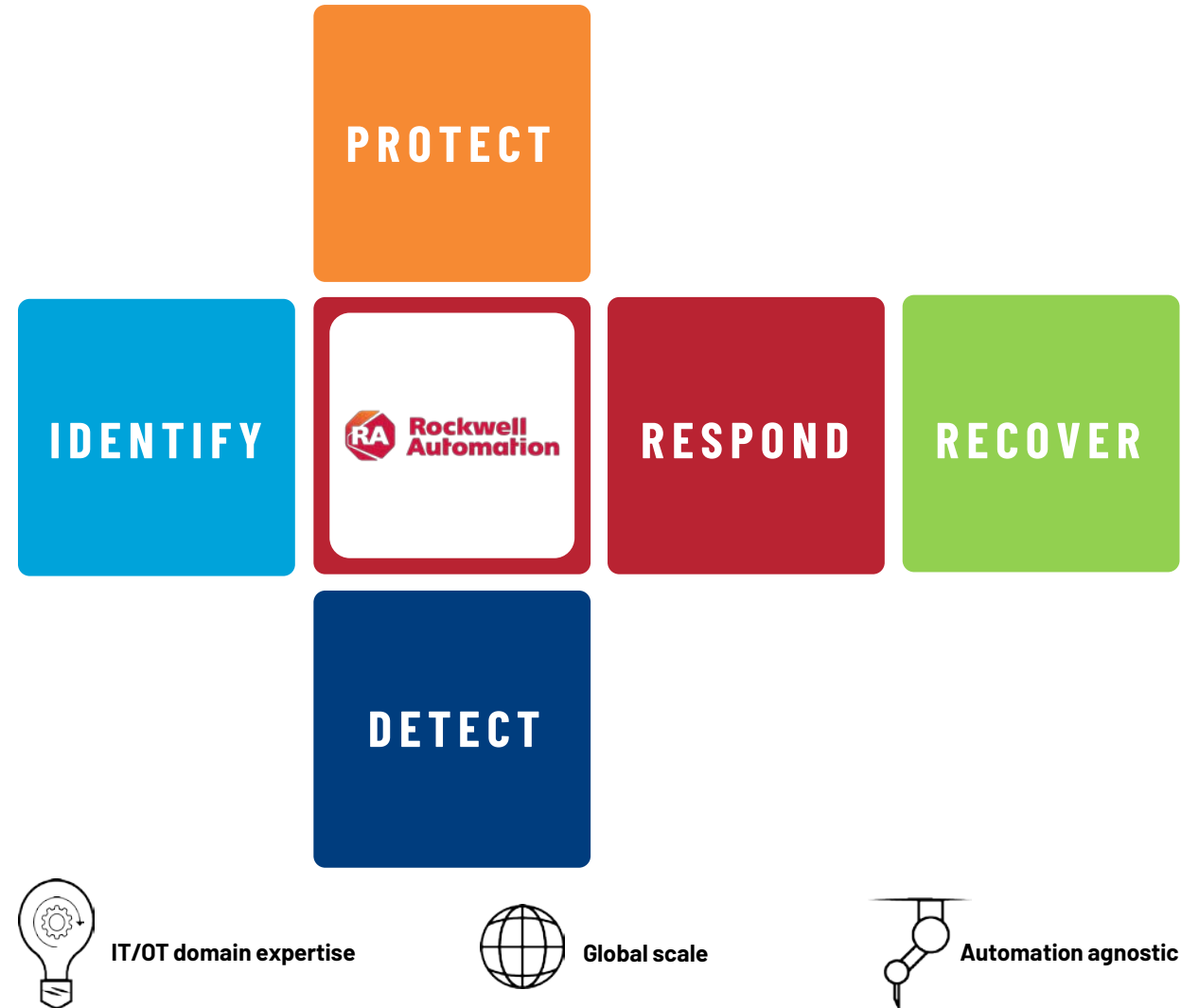


INDUSTRIAL CYBERSECURITY SERVICES FRAMEWORK

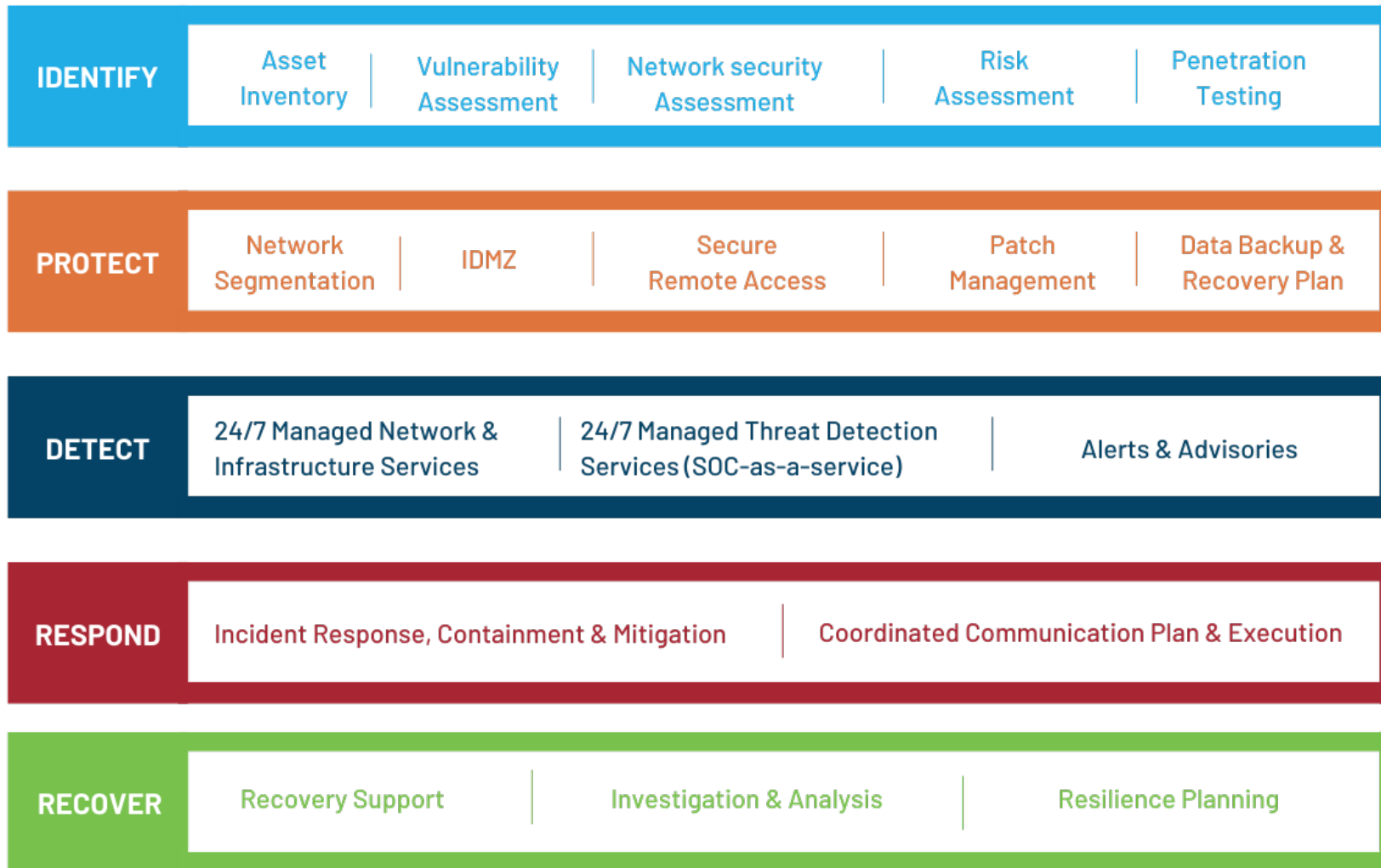
A Reliable, NIST-Based Approach for 360° Protection

Solutions and managed services should be mapped to the widely recognized NIST Cybersecurity Framework.

Using this framework makes it simple for clients to understand how solve key categories of industrial cybersecurity.



MANAGED SERVICES OR SCALABLE DEPLOYMENT FOR A CUSTOM FIT



IDENTIFY

IDENTIFY RISKS TO OT NETWORKS, SYSTEMS, APPS, DATA & SERVICES

Using passive and active assessment tools, will help learn where security vulnerabilities exist, establish priorities, and create comprehensive plans for cybersecurity implementation and ongoing monitoring.

Capabilities & Offerings	Benefits
Asset Inventory	Understand potential risks and exposures
Network Security Assessment	Comprehensive future state logical and physical design blueprint
Risk Assessment	Get a full view of organizational cyber risk to strengthen security posture
Penetration Testing	Discover vulnerabilities through ethical hacking and then flagging them for ease of attack and difficulty
Vulnerability Assessment	Test industrial security effectiveness & identify external and internal security risks

Your Industrial Cybersecurity Journey

Recommended Path based on Your Priorities

1 Priority: Understand Your Network

- What assets are in your network?
- How is your network structured?
- What vulnerabilities and risks are present?
- How can you manage those risks?

▪ Continuous Threat Detection (CTD)

2 Priority: Detect Threats

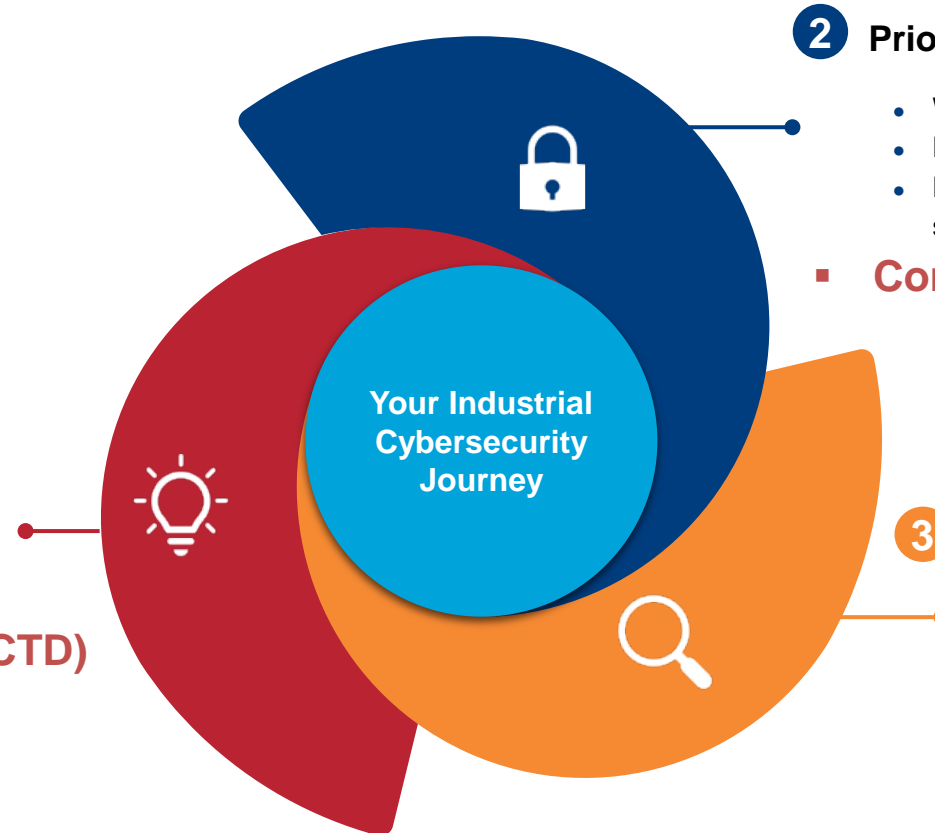
- What threats are you most concerned about?
- How should your staff manage alerts?
- How can your existing IT security tech stack support your industrial network?

▪ Continuous Threat Detection (CTD)

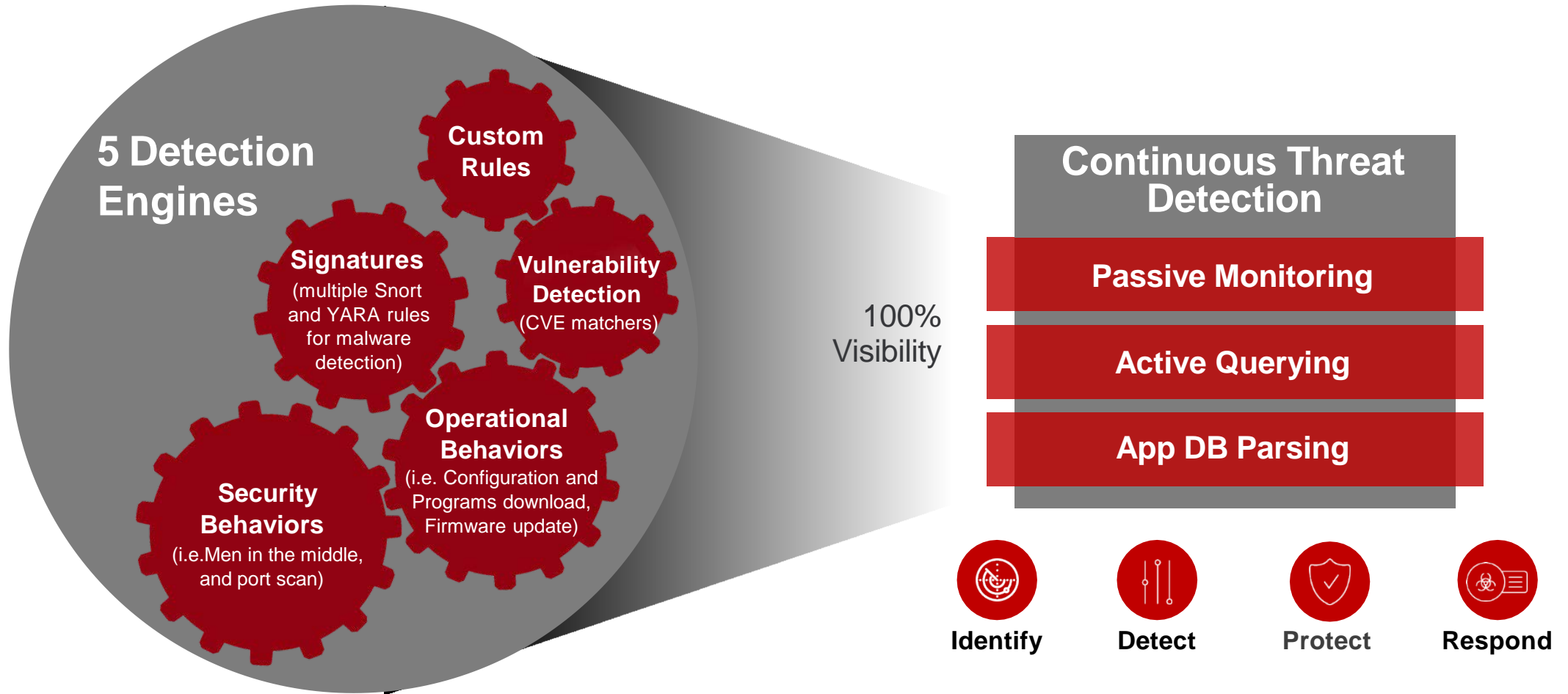
3 Priority: Control Access

- How can you provide internal and third-party personnel with remote access to your network?
- How should you manage the risks posed by their access?
- How should you respond to incidents related to their access?

▪ Secure Remote Access (SRA)



Multi-spectral Data Acquisition for CTD



What is Visibility in OT?

Know what you have and what its attack surface is



Physical Location: Building 5 Freeze Dry Area Line 2 Cabinet 2A
Operation Purpose: Freeze Dry Control

Type: PLC,
Vendor: Rockwell Automation
Model: L71
Serial: 00987DBF
Firmware: v20.015

Program: FreezeDry-L2_Control.acd

Neighbours: Windows Client 'OWS', 1 FT View SE Clients, FT AssetCentre, I/O Chassis 1-5,
Protocols: HTTP, ENIP
Conversations: Program Upload, Data Acquisitions, Read/Write

Location

Where is the asset physically located? What is the operational purpose of the asset?

Device

Type, Vendor, Model, Serial, Firmware, IP, MAC, OS,

Application

Apps Installed, version of apps, context of configuration

Communication

Neighbors, Protocols, Conversations, Frequency

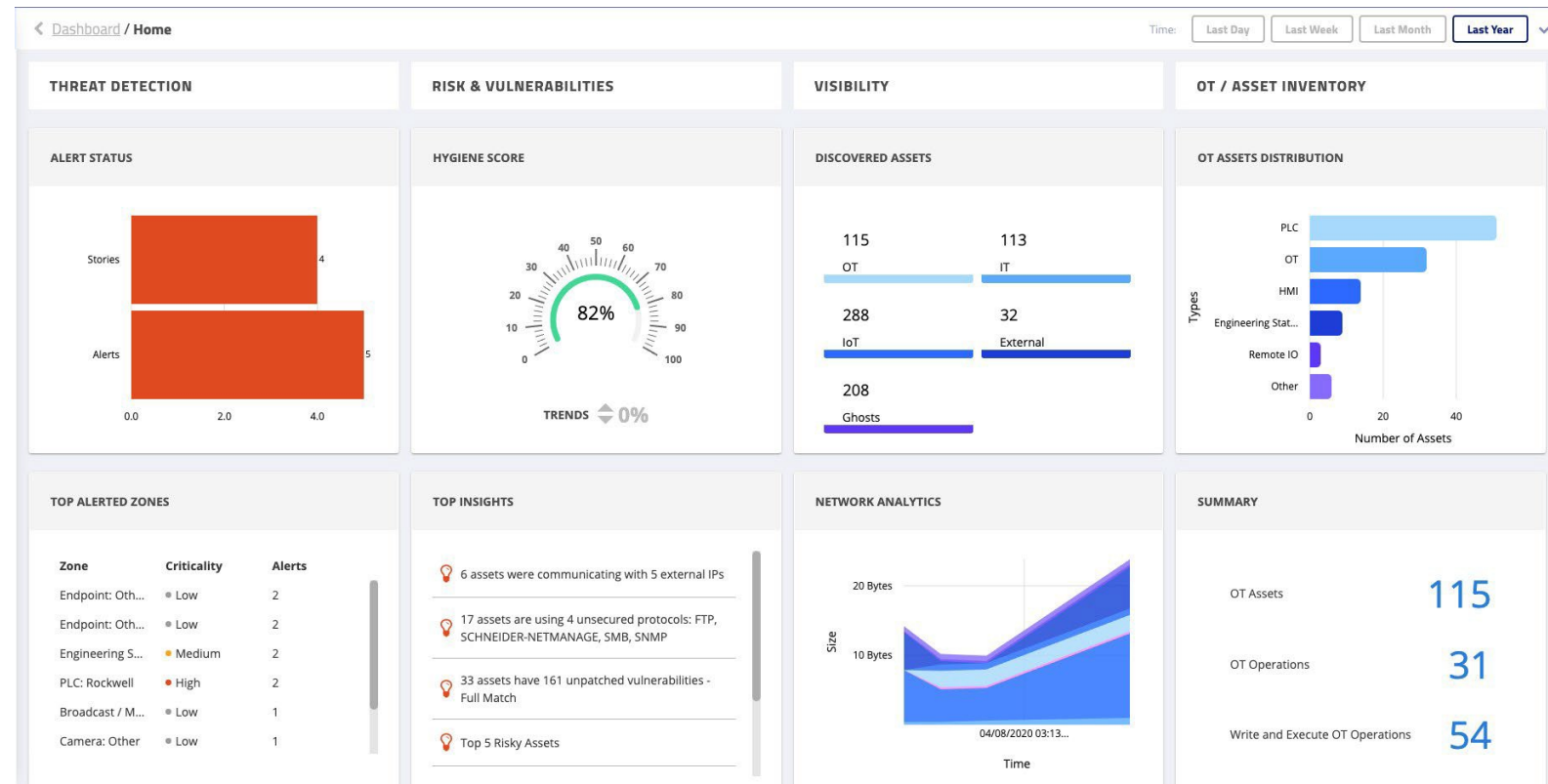
Continuous Threat Detection

Full Customizable Dashboards



Simplify Complexity

- Facilitate reporting and investigation processes with customized dashboards and widgets, clear alerts, and point-and-click investigation tools.
- Rapidly triage alerts, investigate root causes, remediate incidents, and proactively hunt for threats.



Impact and Outcome

- Tailored user experience for analysts, operators, and managers across diverse use cases

Continuous Threat Detection

Vulnerability Management

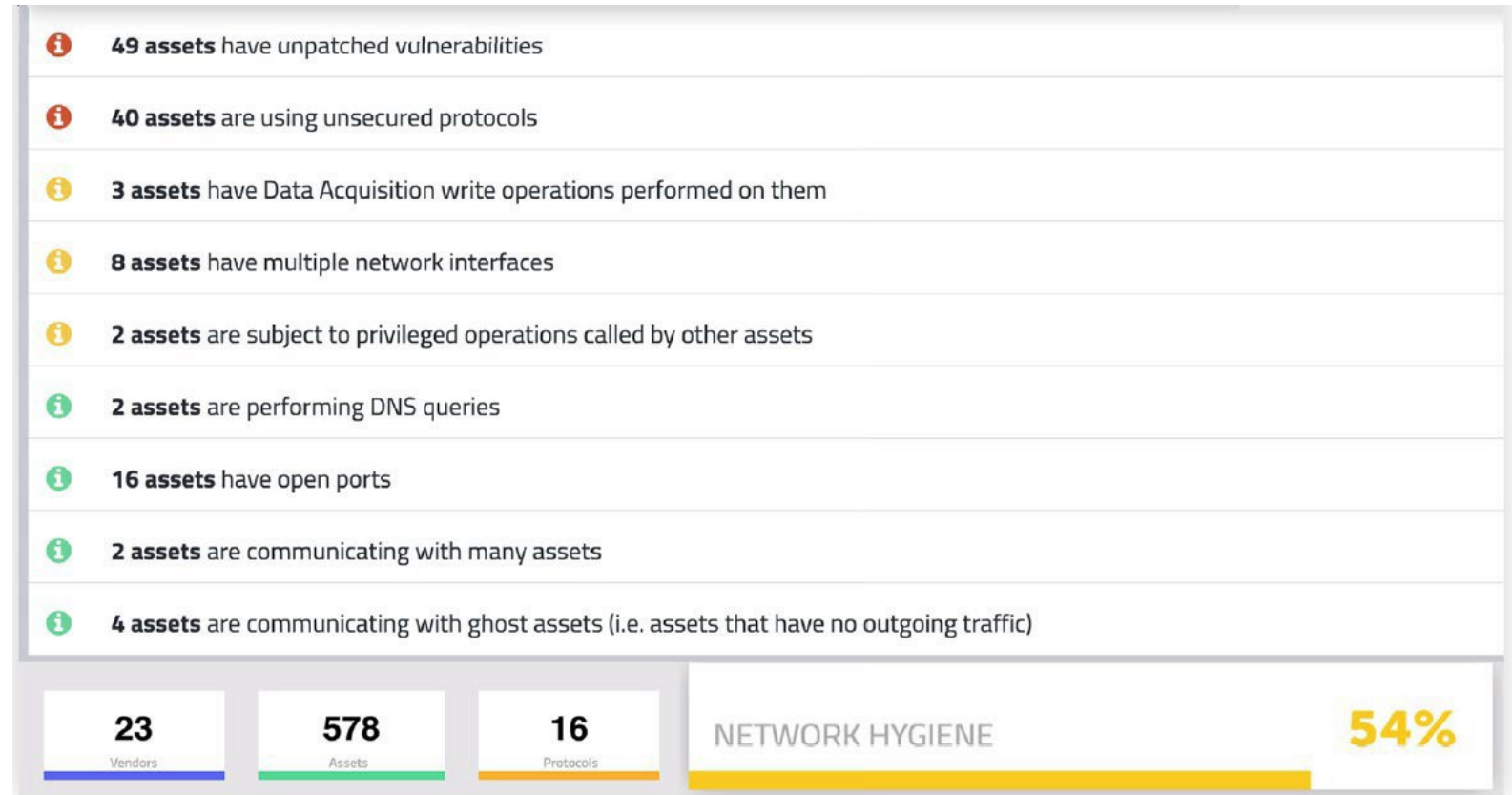


Insights

- Allow to identify and fix issues that can leave ICS networks vulnerable to attacks or lead to operational issues or to plant downtimes.

CVE Matching

- Correlate Common Vulnerabilities and Exposures (CVE) with asset inventory.
- Prioritize patches and compensating controls based on CVE classification and asset function.



Impact and Outcome

- Risk-based vulnerability assessment and mitigation

Continuous Threat Detection

Virtual Zones

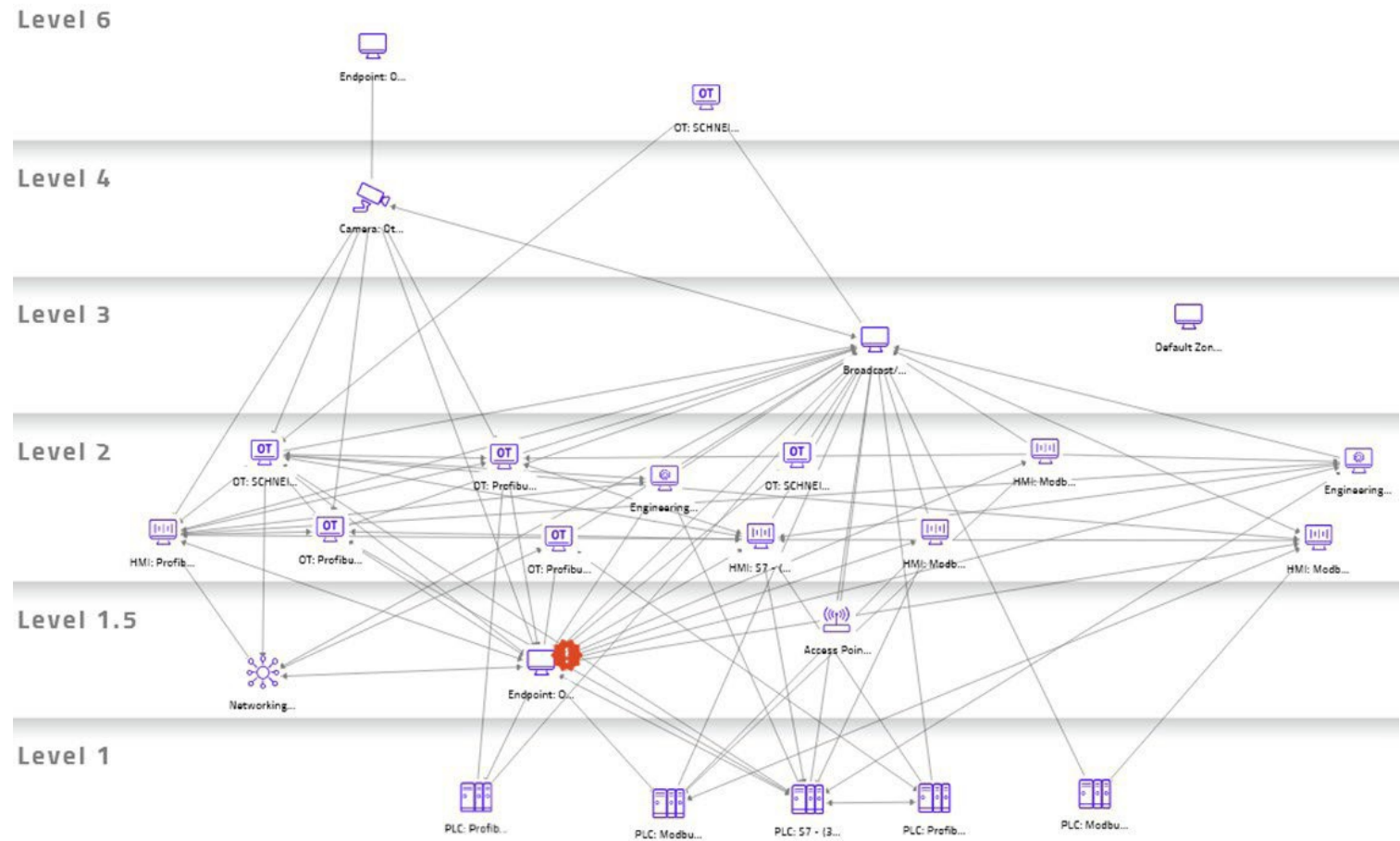


OT-Network Segmentation Mapping:

- Groups similar devices into logical clusters (Virtual Zones)
- Assigns a sensitive level to each Virtual Zone
- Visualizes alert on cross-zone violations (Alerts)
- Enforces OT segmentation
- highlight where boundaries are broken

Key Value Proposition

- Excellent "Segmentation Design Solution"
- Automatically generate current state of OT process communications and presents the ideal segmentation strategy



Impact and Outcome

- Reduce time and cost of segmentation projects
- Lower risk of malware propagation

Continuous Threat Detection







Alerts Scoring & Story



Faster Incident Response & Remediation

- Reduce troubleshooting time by ranking each alert based on its severity level.
- Quickly analyze specific alerts based on detailed metrics.
- Reduce the amount of false positive and false negatives .

ALERT STORYLINE

-  05/02/19 19:56:20 A baseline deviation has been detected from **10.1.44.66** to Zone RTU: DNP3
-  05/02/19 19:55:39 Active remote connection from **DMS-OPER1** to **10.1.44.66** using protocol **VNC**
-  05/02/19 19:55:39 A baseline deviation has been detected from **DMS-OPER1** to **10.1.44.66**.
-  05/02/19 19:54:26 Asset **DMS-OPER1** has performed a network scan.
-  05/02/19 19:54:00 A new asset has been detected: **104.200.22.130 (external) (ghost)**.
-  05/02/19 19:42:41 A baseline deviation has been detected from **DMS-OPER1** to Zone Domain Controller: Other

Impact and Outcome

- Reduced signal-to-noise ratio
- Shorter time to resolution (TTR)

Continuous Threat Detection

Enterprise Management Console - EMC



Scalable OT Monitoring

- Achieve centralized visibility and control from multi-site, distributed architecture.
- Consolidate cross-site asset to spot operational issues and security events.

The screenshot displays the CLAROTY Enterprise Management Console interface. The main section is 'ASSETS VIEW (155)', which contains a table of assets. The table has columns for Name, IP, MAC, Type, Criticality, Risk Level, Vendor, and Site. The assets are listed with various IP addresses and MAC addresses, and are categorized by type (e.g., PLC, NETWORKING, HMI) and vendor (e.g., Rockwell Automation, Siemens, ABB, Yokogawa). The interface also includes an 'ALERTS (2)' section on the left, an 'ACTIVITY LOG' at the bottom left, and a 'STATS' section on the right showing current asset counts and distribution charts.

NAME	IP	MAC	TYPE	CRITICALITY	RISK LEVEL	VENDOR	SITE
10.1.34.12	10.1.34.12	00:A0:45:07:0B:4C	PLC	High	Normal	PHOENIX CONTACT GMBH & CO.	Default
Chemical_plant	10.1.30.1	00:1D:9C:00:04:9D	PLC	High	Critical	Rockwell Automation	Default
10.1.30.6	10.1.30.6	00:1D:9CA1:60:A4	PLC	High	Normal	Rockwell Automation	Default
10.1.30.4	10.1.30.4	E4:90:69:A7:70:0F	PLC	High	Normal	Rockwell Automation	Default
10.1.30.5	10.1.30.5	00:00:BC:03:44:C0	PLC	High	Normal	Rockwell Automation	Default
10.1.30.3	10.1.30.3	F4:54:33:92:89:96	PLC	High	Normal	Rockwell Automation	Default
10.1.31.6	10.1.31.6	28:63:36:88:F7:AE	PLC	High	Normal	Siemens	Default
10.1.34.1	10.1.34.1	00:80:F4:12:8B:10	PLC	High	Normal	TELEMECANIQUE ELECTRIQUE	Default
10.1.30.1:Card 2 \ Addr 1			PLC	High	Normal	Rockwell Automation	Default
10.1.30.1:Card 2 \ Addr 2			PLC	High	Normal	Rockwell Automation	Default
10.1.31.1	10.1.31.1	28:63:36:26:F0:74	PLC	High	Normal	Siemens	Default
10.1.33.1	10.1.33.1	00:00:23:1F:9E:54	PLC	High	Normal	ABB	Default
10.1.30.1:Card 3 \ 192.168.1.13			PLC	High	Normal	Rockwell Automation	Default
10.1.30.1:Card 3 \ 192.168.1.14			PLC	High	Normal	Rockwell Automation	Default
10.1.30.1:Card 2 \ Addr 11			PLC	High	Normal	Rockwell Automation	Default
FC50101	192.168.129.3, 192.168.129.2, 192.168.1.3, 192.168.1.2	00:00:64:9B:26:88, 00:00:64:9B:26:89, 00:00:64:9B:27:85, 00:00:64:9B:27:84	PLC	High	Normal	Yokogawa	Default
10.1.30.1:Card 2 \ Addr 255			PLC	High	Normal	Rockwell Automation	Default
00:A0:84:0D:AF:DD		00:A0:84:0D:AF:DD	NETWORKING	Medium	Normal	HONEYWELL ACS	Default
EAGLEmGuard	1.1.1.1	00:80:63:BF:22:8D	NETWORKING	Medium	Normal	Hirschmann Automation and Control GmbH	Default
800ENGNODE	10.1.33.4, 172.16.0.197	00:50:56:B9:5B:4F	HMI	Medium	Normal	VMware, Inc.	Default
192.168.1.12	192.168.1.12	00:1D:9C:CF:3D:FD	HMI	Medium	Normal	Rockwell Automation	Default

Impact and Outcome

- “Single pane of glass” management for distributed OT footprints

PROTECT

PROTECT INFRASTRUCTURE FROM SOPHISTICATED ATTACKS

By putting the right strategy and controls in place across people, processes and technology, will provide the safeguards to block attacks and to limit or contain the impact of a cybersecurity event.

Capabilities & Offerings	Benefits
Network Segmentation	Protects the network from attacks moving laterally and improves security risk posture
IDMZ Industrial Demilitarized Zone	Build architecture that separates the IT business systems from OT networks/ICS
Secure Remote Access	Mitigate stolen credential & insider attacks
Patch Management	Keep operating systems up to date and secure
Data Back-up & Recovery Plans	Increase the reliability of your network and reduce downtime
Training and Alerts	Reduce human error and insider threats; respond to threats with greater speed

DETECT

DETECT THREATS BEFORE THEY CAUSE DISRUPTION & DOWNTIME

To stay ahead of cybercriminals, you must detect the full spectrum of threats, get instant alerts on common attacks, and continuously monitor the network for unusual activity.

Capabilities & Offerings	Benefits
Threat Detection Implementation	Detect threats across networks, assets, and endpoints
24/7 Managed Threat Detection Services SOC-as-a-service	Quickly detect anomalous behavior to identify potential threats
24/7 Managed Network and Infrastructure services	Providing real-time monitoring of OT network infrastructure, data center and asset lifecycle

RESPOND

RESPOND TO INCIDENTS AND QUICKLY CONTAIN IMPACTS

Organizations should quickly respond to incidents and minimize the impact on the business by building a secure, vigilant, and resilient environment.

Capabilities & Offerings	Benefits
Incident Response Containment & Mitigation	Prevent expansion of an event, mitigate its effects, and eradicate the incident
Communications Plan & Execution	Coordinated and effective response activities

RECOVER

RECOVER QUICKLY AND INCREASE CYBER RESILIENCE

By taking a proactive approach to the recovery phase, will minimize the impact on operational abilities, reputation, and revenue.

Capabilities & Offerings	Benefits
Recovery support	Restore operations to get back up and running quickly, limiting downtime
Investigation & Analysis	More targeted response and recovery activities
Resilience Planning Implement enhanced strategies with lessons learned	Refining cybersecurity strategy

Reducing Risk and Creating Value Throughout Your Production Lifecycle

Feasibility &
Conceptual Studies

Front End
Engineering
& Design

Design &
Engineering

Installation &
Commissioning

Operation &
Maintenance

Upgrades &
Migrations



ASSESS



DESIGN



IMPLEMENT

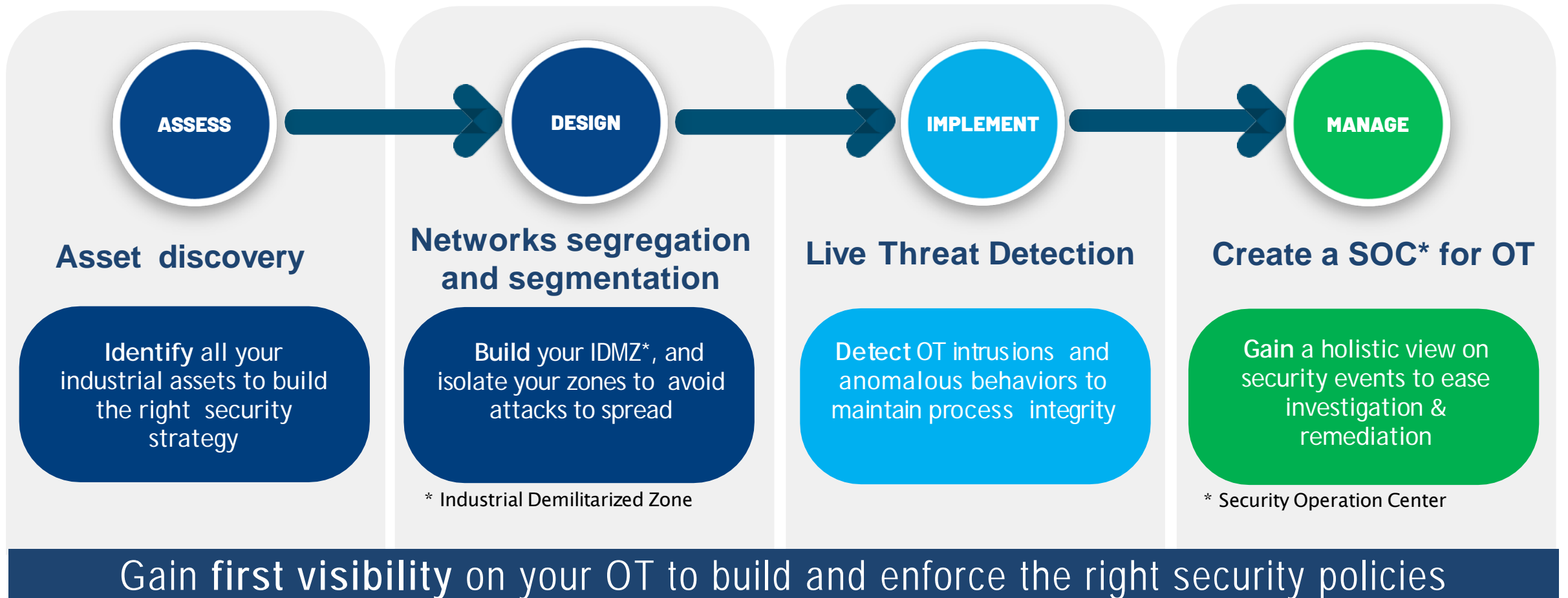


VALIDATE



MANAGE

The **4-step journey** to secure your ICS





**Rockwell
Automation**

Questions

rockwellautomation.com

CONFIDENTIAL • Copyright ©2022 Rockwell Automation,
Inc.

