THE REYNOLDS COMPANY
ELECTRICAL SUPPLY

Industrial Cybersecurity Seminar

July 14, 2021

2021 Online Events

Register to receive a calendar invite

THE REYNOLDS COMPANY
ELECTRICAL SUPPLY

Tech Talks

Using The Plant Pax System Estimator

Wed, July 28, 2021 @ 10am

Modern Lockout/Tagout for Deployment, Management, and Compliance

Wed, August 11, 2021 @ 10am

User Groups

System Redundancy Best Practices

Wed, July 21, 2021 @ 10am

reynoldsonline.com

Our Guest Panelists

Luis Ramos
Process and Security Solution Consultant
ISA/IEC 62443 Cybersecurity Expert
Rockwell Automation

Cybersecurity Attacks in the news

"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

Colonial Pipeline paid $5 million ransom to hackers

PUBLISHED THU, MAY 13 2021•2:05 PM EDT | UPDATED THU, MAY 13 2021•6:38 PM EDT

Renault, Nissan European operations deal with global cyber attack

May 13, 2017 @ 7:49 am

Hacked meat company paid $11 million ransom to cybercriminals

By Jesse O'Neill June 9, 2021 | 8:08pm | Updated

Automotive News THIS WEEK'S ISSUE

Hacker Breaches Florida Water Treatment Plant, Adds Lye to City's Water Supply

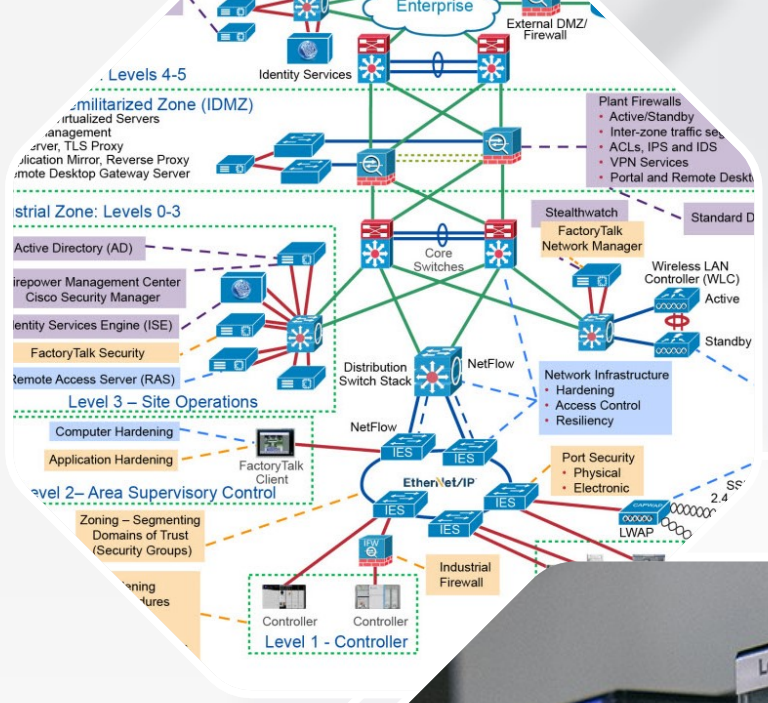
An unknown hacker virtually infiltrated the city of Oldsmar's water ... a significant security breach during a news conference on Monday.

10 hours ago

Rockwell Automation

Industrial Cybersecurity Risk

Understanding Risk



Security Risk "is a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization." - NIST SP800-30

Risk = (Threat x Vulnerability) x Impact

Risk = Likelihood x Impact

Remember: Threats do not have to be malicious – they can be accidental

Rockwell Automation

Threats

Understanding Risk

- Malware
- Infected USBs
- Contractors
- Infected Laptops
- Unprotected Wireless
- Ransomware
- Human Error
- Disgruntled Employees
- Hackers
- Denial of Service

Threat

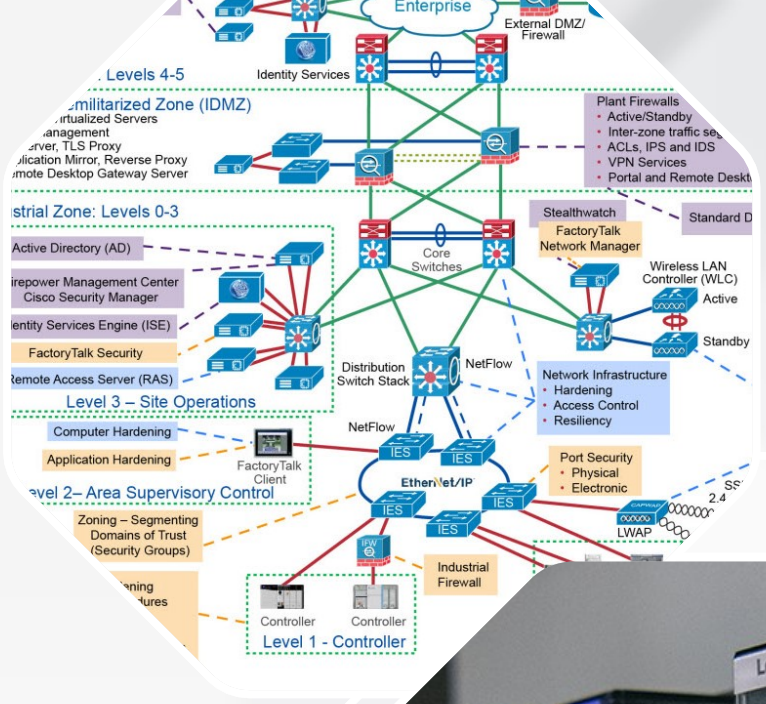
Malicious Act that seeks to Damage / Steal / Disrupt Data - not always Financial

Malware – External / Infected Laptop / Infected USB

- Antivirus Software
- EndPoint Protection
- Dedicated Engineering Stations
- No External USBs

Human Error – Insider / Employee / Contractor

- Network Segmentation
- Role Based Segmentation
- Management of Change
- Audit Logs
- Backup System



Rockwell Automation

Vulnerability

Understanding Risk

- Policy and Procedure
- Operating Systems
- Weak Password
- Unsegmented networks
- Outdated antivirus
- Unpatched systems
- Poor backups
- Physical access
- Remote access
- Misconfigured wireless
- File shares (SMB v1)

Vulnerability

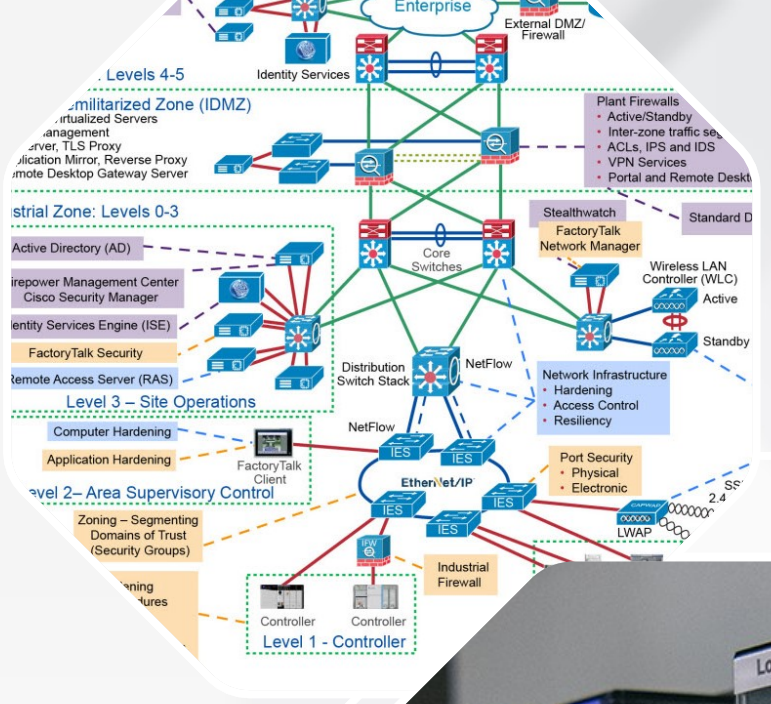
Weakness in Network, Operating Systems, and existing Policies and Procedures

Weak Passwords

- Domain Controller – User Groups / Role Based
- Group Policy – Industry standard password strength
- FactoryTalk Security
- Two-Factor Authentication

Physical Access

- Key switch Position – Controller set to “Run”
- Locks – Cabinet / Switch Ports / USBs
- Trusted Slot – ControlLogix Restricted Communication



Rockwell Automation

Impact

Understanding Risk

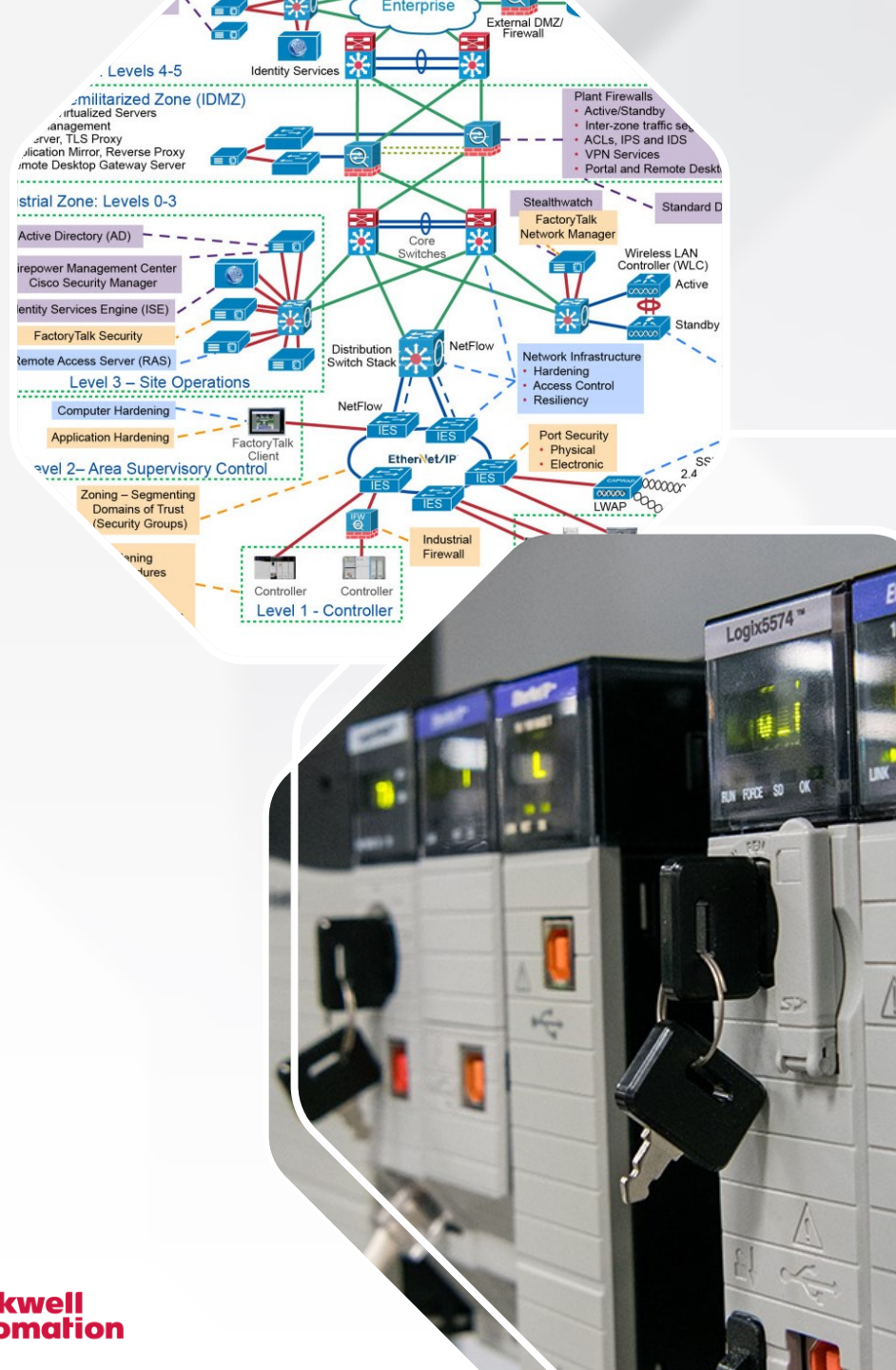
- Health & Safety
- Environment
- Equipment Damage
- Lost Production
- Business Interruption
- Bad Quality Product
- Regulatory Fines

Impact

Consequence of a Security Event / Incident

Loss of Production / Downtime

- Threat Detection
- OT Network Visibility
- Properly Patched ICS



Rockwell Automation

Common Security Challenges

Industrial Automation Control System (IACS) Concerns

Hardware and Software

Legacy Hardware and Software

- Unpatched Systems – Application, Windows, IACS
- Asset Inventory – Lack of Documentation

Network Segmentation

- Enterprise Zone vs. Industrial / Manufacturing Zone
- Security Zones – Intertwined Responsibilities

Availability

- Real-Time Data
- Continuous Process

Policy and Personnel

System Visibility

- OT Network Visibility not on par with IT Monitoring
- Lack of Data Flow Diagram including Industrial Protocols

Access Management

- Management of Change
- 24/7 Access Control – Secure Remote Access

Operational Technology (OT) Security Skills

- Industrial Cyber Security Awareness
- Risk Management and Cybersecurity Governance

Industrial Cybersecurity Framework

Defense-in-depth Approach

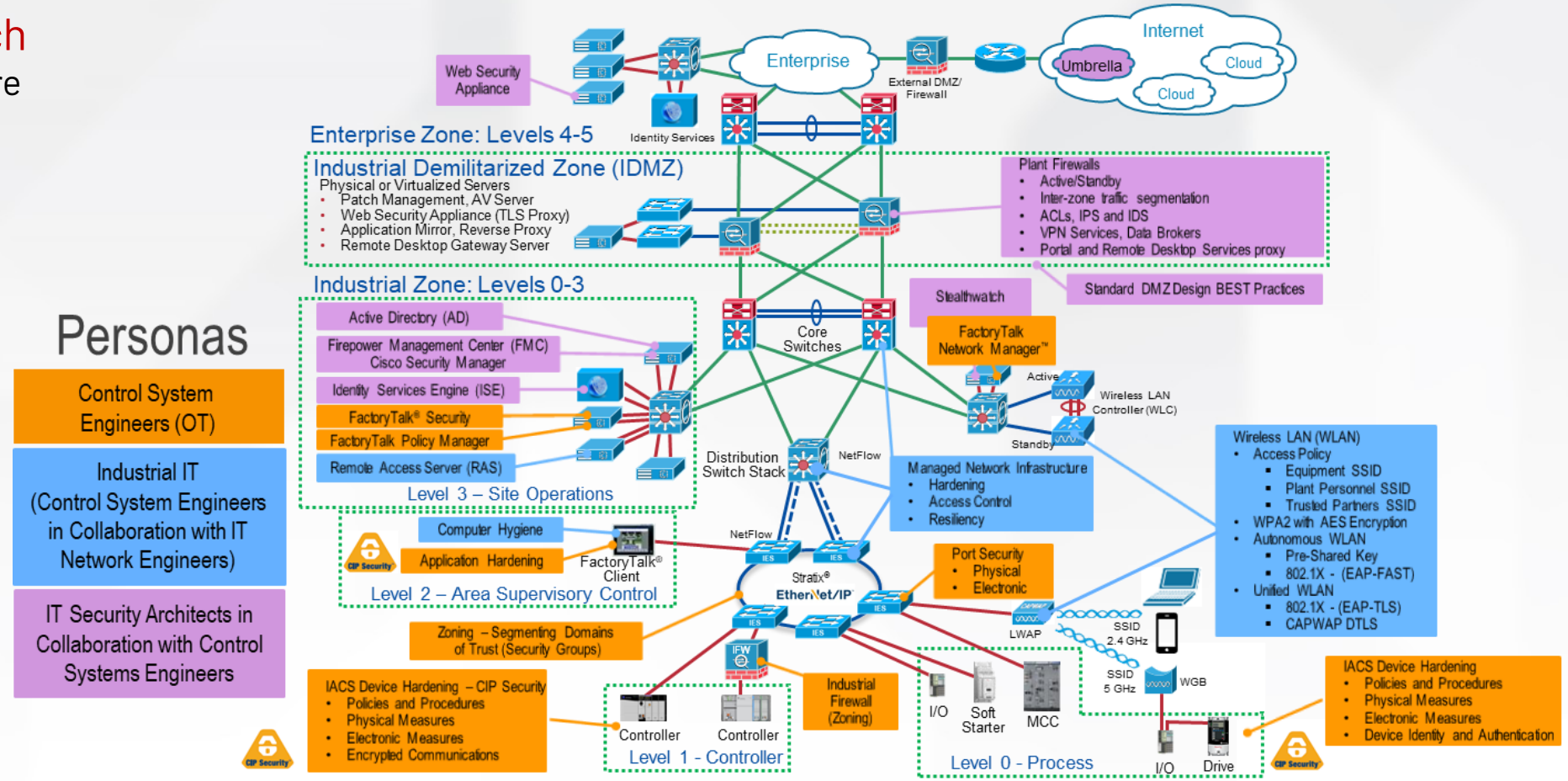
- Network Security Infrastructure
- Threat Detection
- Behavior Analysis
- Content protection
- Cloud Security
- Threat Analysis

Hardware and Software

- Upgrading Windows OS
- Upgrading Firmware

Policy and Personnel

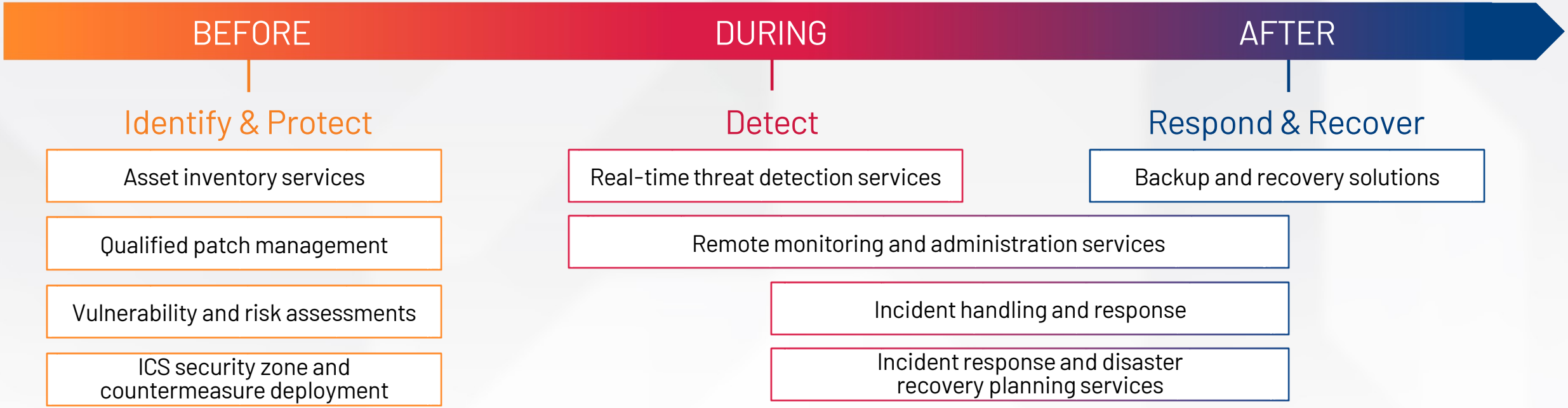
- Enabling FactoryTalk Security
- Proper Access Controls



Converged Plantwide Ethernet (CPwE) Architectures

A proactive approach to industrial cybersecurity

ATTACK CONTINUUM



BUILD A SECURE, ROBUST, FUTURE-READY NETWORK FOR YOUR CONNECTED ENTERPRISE

Rockwell Automation

White House Executive Order

Improving the Nation's Cybersecurity

Best Practices for U.S. Government

- Multifactor Authentication
- Threat Detection
- Threat Response
- Encryption
- Skilled, empowered Security Team

Executive Order Key Points

- Removing Barriers to Threat Information Sharing Between Government and the Private Sector.
- Modernize and Implement Stronger Cybersecurity Standards in the Federal Government
- Create a Standard Playbook for Responding to Cyber Incidents
- Improving Software Supply Chain Security

CISA – Executive Order on Improving the Nation's Cybersecurity

OT Security Key Takeaways

Industrial Automation Control System (IACS) Recommendations

Asset Management

- Comprehensive Network Assessment
- Asset Inventory Identification
- Lifecycle Management
- Vulnerability Management
- IACS Device Hardening
- Patch Management

Visibility

- Network Diagnostics and Monitoring System
- Control System Audits
- Real Time Threat Prevention and Monitoring
- Comprehensive Backup and Recovery Plan

Segmentation

- Proper Network Segmentation
- Designated Security Zones
- Resilient Networks
- Secure Remote Access
- Protocol Management

OT Policy

- Role-based Access Controls
- System Authentication
- Control Data Access
- CIP Security

OT Education

- Industrial Cyber Security Standards
- Baseline Analytics
- Incident Response Plan
- Industrial Cyber Security Team
- Communication and Notifications

Cybersecurity Workshop

Brandon Singh
The Reynolds Company – North TX
Network Specialist
jbsingh@reynco.com

Luis Ramos
Rockwell Automation
Process and Security Solution Consultant
lhramos@ra.rockwell.com

Joe Belaschky
The Reynolds Company - HOU
Automation and Network Specialist
jcbelaschky@reynco.com

Thank you

www.rockwellautomation.com

Rockwell Automation

expanding **human possibility**®