Industrial Cybersecurity: The Never-Ending Journey

Abid Ali

RAOTM, 22nd January 2019
IT/OT Convergence - the Opportunity

“Smart Manufacturing & the Internet of Things, can foster tremendous business outcomes”.

Source: survey of 418 manufacturing line of business executives & Plant managers by SCM World & CISCO,

A Robust & Secure OT Network Infrastructure key to “Smart Manufacturing”
It's not IF ..... But WHEN

IT/OT Convergence the Risk

92% of manufacturers rank cyber risk as a top risk factor for their business.

23% of manufacturers don't consider cybersecurity until the quality control or marketing stage of the manufacturing process.

Biggest ransomware outbreak in history hits nearly 100 countries with data held for ransom

Petya and WannaCry tip of the iceberg as Australian businesses fight ransomware

WannaCry malware hits traffic cameras in Australia

The ransomware that shut down Britain's healthcare system still seems to be going strong.
IT and OT – The Same, but Different

**IT NETWORK**

**LEVEL 5**
Corporate Network

- **Security Controls**
- **Cloud-Based Apps**
- **Network Devices**
- **Assets**
- **ERP Systems**

**LEVEL 4**
Business Apps

- **Cloud-Based Apps**
- **Email Services**

**OT NETWORK**

**LEVEL 3**
Control System LAN

- **MES/MIS**
- **Workstations**
- **Security Controls**
- **Smart Motor Control**
- **Smart Sensors & Instrumentation**

**LEVELS 0-2**
Control, Supervising & Process Devices

- **SCADA/HMIs**
- **PLCs**

**OT FOCUS**

**Availability # 1**

Traffic
Data, Control Information, Safety, & Motion.

Security
Strict physical access & Simple network device access.

Access
Isolate threat & keep working..

**IT FOCUS**

Confidentiality # 1
Traffic,
Data, Voice & Video.

Security

Access
Shut down access to detected threats.

Different Focus & Priorities - Different Performance & Security Requirements - Different Architectures & Support Models
Industrial Security Trends

Established Industrial Security Standards

- International Society of Automation
  - ISA/IEC-62443 (Formerly ISA-99)
  - Industrial Automation and Control Systems (IACS) Security
  - Defense-in-Depth
  - IDMZ Deployment

- National Institute of Standards and Technology
  - NIST 800-82
  - Industrial Control System (ICS) Security
  - Defense-in-Depth
  - IDMZ Deployment

- Department of Homeland Security / Idaho National Lab
  - DHS INL/EXT-06-11478
  - Defense-in-Depth
  - IDMZ Deployment
Converged Plantwide Ethernet (CPwE)

Industrial IT - OT/IT Convergence

- Tested, validated and documented reference architectures
  - Based on use cases - customer and application
  - Tested for performance, availability, repeatability, scalability and security
  - Comprised of nine (9) Cisco Validated Designs
- Built on technology and industry standards
  - “Future-ready” network design
- Content relevant to both IT Network Engineers and Control System Engineers
- Deliverables
  - Recommendations, best practices, design and implementation guidance, documented test results and configuration settings
  - Simplified design, quicker deployment, reduced risk in deploying new technology
- Enabler for OT/IT Convergence, Industrial IoT and The Connected Enterprise

“With this implementation guide, for the first time IT and manufacturing professionals can share a common document for planning a converged IP network including the factory floor and automation equipment.”

– Harry Forbes, ARC Advisory Group
Lack of Skilled Resources

Out of Date Infrastructure

Wiper/Ransomware
Spillover from Nation State Campaigns

Impact to:
- Human Health & Safety
- Product Quality
- Environmental
- Unplanned Production Loss

Countermeasures
Must add capabilities to defend Manufacturing Digital Environment across the Attack Continuum
INDUSTRIAL CYBER SECURITY SERVICES

Security Roadmap Step 1: What do I have?

Identify
- Asset Inventory Services
- Vulnerability and Risk Assessments
- Policy & Procedure Development

Protect
- Application Whitelisting Deployment
- Qualified Patch Management
- ICS Security Zone and IDMZ Segmentation
- FactoryTalk Security Implementation Services
- Network Access Control Deployment
- Cyber Security Awareness Training

Detect
- Real-Time Threat Detection Services
- Remote Monitoring and Administration Services

Respond
- Incident Handling and Response*

Recover
- Incident Response and Disaster Recovery Planning Services
Security Roadmap Step 2: Implement Basic Hygiene

**Identify**
- Asset Inventory Services
- Vulnerability and Risk Assessments
- Policy & Procedure Development

**Protect**
- Application Whitelisting Deployment
- Qualified Patch Management
- ICS Security Zone and IDMZ Segmentation

**Detect**
- Real-Time Threat Detection Services
- Remote Monitoring and Administration Services
- Incident Handling and Response*

**Respond**
- Network Access Control Deployment
- Incident Response and Disaster Recovery Planning Services
- Cyber Security Awareness Training

**Recover**
- Backup Management
Security Roadmap Step 3: Persistent Countermeasures

**Identify**
- Asset Inventory Services
- Vulnerability and Risk Assessments
- Policy & Procedure Development

**Protect**
- Qualified Patch Management
- ICS Security Zone and IDMZ Segmentation
- FactoryTalk Security Implementation Services

**Detect**
- Application Whitelisting Deployment
- Real-Time Threat Detection Services
- Remote Monitoring and Administration Services

**Respond and Recover**
- Network Access Control Deployment
- Incident Handling and Response*
- Incident Response and Disaster Recovery Planning Services

**Before**
- Security Roadmap

**During**
- Persistent Countermeasures

**After**
- Security Measures Implemented
Addressed Throughout the Journey: People and Policy

**Identify**
- Asset Inventory Services
- Vulnerability and Risk Assessments
- Policy & Procedure Development

**Protect**
- Application Whitelisting Deployment
- Qualified Patch Management
- ICS Security Zone and IDMZ Segmentation

**Detect**
- Real-Time Threat Detection Services
- FactoryTalk Security Implementation Services

**Respond**
- Remote Monitoring and Administration Services
- Incident Handling and Response*
- Network Access Control Deployment

**Recover**
- Backup Management
- Cyber Security Awareness Training
- Incident Response and Disaster Recovery Planning Services
Asset Inventory through Passive Network Analysis

Auto Baseline Development and Behavioral Anomaly Detection

Security and Operational Event Monitoring and Response

Powered by Clarity
THREAT DETECTION SERVICES

Capabilities

• Comprehensive Asset Inventorying
• Passive Network Monitoring
• Vendor and Protocol Agnostic
• Fine grained DPI Model

Benefits

• Continuous Monitoring without Interrupting Production
• Single Solution for Many ICS Vendors
• Collect Information on How Assets are configured, communicate and change
• Discover issues with full visibility of ICS Networks

Asset Monitoring

• Behavioral Anomaly Detection
• Real-Time Change Detection
• Alert on Operational and Security Events
• Incident Response Services

Security and Operational Monitoring

• Validate Operational Tasks to reduce risk, and maintain process integrity
• Near Real Time Detection of Cyber Threats (conficker, wannacry, etc)
• Recover from Security Incidents with Highly-Trained Professionals
• Reduce Risk of Downtime with 24x7 Response
Plan, Design, and Implement

- Review infrastructure and documentation
- Definition of Asset Criticality
- Appliance implementation
- Review and sterilization of baseline results for immediate remediation

Manage, Monitor and Detect

OT Assets
- Deep Packet Inspection (DPI) on IT and OT Data Streams

IT Assets
- Individually Managed Site Appliance

Managed Service Provider with OT Knowledge
- Centralized Self Management (IT SOC)
- And / Or

Respond, Recover

- Response and Recovery Plan Development and Review
- Containment, eradication, and recovery workflows
- Characterize and scope potential impact
- Set Course of Action and Incident Reporting
Architecture Options

- Central Office Architecture
- The Industrial DMZ separates IT and OT Networks.
- The data across separate sites is collected at the central Appliance.
Architecture Options

- Small Site with compute available on-site.
- Site appliances forwards alerts to Central Appliance.
Architecture Options

- Small Site without on-site compute
  - Site Switch Sends SPAN traffic to Central Appliance
- Depending on architecture and size of these sites “brick” style compute can be deployed.
Industrial Cyber Security Services Portfolio

Rockwell Automation offers the following services to help our customers improve their security posture and reduce cyber risk within their Industrial Control System (ICS) environment:

• **Qualified Patch Management Services** – Provide Rockwell Automation tested and approved Anti-Virus Definitions and Microsoft Windows patch lists to your on-site WSUS responsible for managing patches of your ICS software systems (FactoryTalk Software). This will insure a timely and disciplined approach to addressing OS related vulnerabilities. (Additional management options available)

• **Security Assessment** – Understand risk posture of your ICS environment to identify areas of improvement against established ICS Cyber Security Standards such as ISA/IEC 62443, NIST 800-82 and NIST CSF.

• **Security Control Implementations** - provide turnkey implementation of security controls that help address gaps/risks that have been identified in specific areas such as zone based segmentation, device hardening and application whitelisting (Symantec CSP), threat/anomaly detection (Claroty), network access control (Cisco ISE)

• **Network Assessments** including onsite visit to collect data, identify issues, and analyze the gap with Industry best practices to insure your infrastructure is meeting the availability requirements of your control systems.

• **Network Design and Implementation** – provide a turnkey Network Infrastructure which is scalable, resilient and future ready, based on Industry best practices such as CPwE Converged Plantwide Ethernet.

• **iDMZ Design and Implementation** – Secure the data flow between Enterprise systems and plant systems, plus optionally setup secure remote access for OEMs and vendors.

• **FactoryTalk Security**: Consulting on how to best utilize the security features available through Rockwell Automation products.

• **Anomaly and Threat Detection Services**. Provide visibility into control systems, protocols and networks, real-time monitoring and analytics to detect anomalies and threats that may impact the security and operational integrity of your ICS systems.

• **TechConnect**. Knowledgebase email alerts on Rockwell Automation product security with access to the latest SW and Firmware updates.

• **Remote Monitoring / Administration**. Converged IT/OT monitoring and administration support of infrastructure, end nodes and industrial applications throughout their lifecycle.

• **Incident Response**. We partner with top security firms to help customers respond to incidents in the event of a breach.

• **Training**: we offer IMINS and IMINS 2, trainings to prepare for Industrial Networking and Security certification
Thank You
Please help us know your Queries