protiviti®
Global Business Consulting

IDENTIFYING AND MEASURING OT SECURITY RISKS THROUGH INTERNAL AUDIT

IIA Houston

April 17, 2023

INTRODUCTION

Justin Turner

Director
Security & Privacy
Protiviti

AGENDA

01 Differences between IT and OT

02 Why OT networks and system vulnerable

03 Example Internal Audit approaches to evaluating OT environments

04 Sample output and observations from the field

05 Common myths

06 Key recommendations and focus areas

WHAT IS OT, AND WHY DOES SECURING IT MATTER?

WHAT IS IT & OT?

Information Technology (IT)

- Hardware, software, and networks that manage, transact, or analyze data
- Supports the business - examples include our company systems that enable Customer Service (CC&B), Asset Management (Maximo), Enterprise Resource Planning (Workday), Email/Collaboration (O365), and other transactional systems.

Operational Technology (OT)

- Controls, changes, and monitors physical devices, processes, and events
- Is the business – creates revenue
- Highly secure systems critical to public safety
- Examples include our pipeline SCADA system, LNG plants, Compressor Station, Farms, and Interconnects
  - ICS (Industrial Control System) consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).
  - SCADA (supervisory control and data acquisition) is a category of software applications for controlling industrial processes, which is the gathering of data in real time from remote locations in order to control equipment and conditions.

IT/OT Convergence: The growing integration and interconnection between IT and OT systems to improve automation and efficiency and to facilitate the exchange of relevant data within industrial settings

EXAMPLE USES OF OT/SCADA* IN INDUSTRY

Electric power generation, transmission and distribution: Electric utilities use RTUs and HMI SCADA to detect current flow and line voltage of remote sites; to monitor the operation of breakers, and to take power grids on or off.

Water, wastewater and sewage: State and Municipal Water use SCADA applications to monitor and regulate water flow, reservoir levels, pipe pressure, wastewater collection and treatment facilities, water treatment centers and distribution, etc.

Buildings, facilities and environments: Facility managers use SCADA to monitor and control HVAC, temperature sensors, refrigeration units, lighting and entry systems.

Manufacturing: SCADA manages parts lists for just-in-time manufacturing and regulates industrial automation and robots. It also monitors quality and process control in industrial plants.

Automotive: Operators can control scheduling, cargo distribution, fuel consumption, and operate signals and switches. SCADA Software can be used to monitor vehicle routing, equipment maintenance, weather conditions, and more.

Chemicals and fertilizers: SCADA software allows operators to monitor and control chemical process on the plant. The system is based on client/server architecture with the possibility of numerous clients' connections.

Oil & Gas: SCADA software applications are used to remotely monitor, and control equipment related to pipelines, pumps, storage, offshore platforms and onshore wells, refineries and petro-chemical stations, etc.

Other: Other processes include telecommunications, agriculture/irrigation, healthcare, pharmaceutical, and many others.

*SCADA (supervisory control and data acquisition) is a category of software applications for controlling industrial processes, which is the gathering of data in real time from remote locations in order to control equipment and conditions.

Source(s): DPS Telecom, Recursion Software, TechTarget

WHY ARE ICS SYSTEMS VULNERABLE?

1 Inherently Insecure

- Flat Networks
- Weak Authentication
- No encryption
- Insecure ICS Protocols
- Difficult/rare patching

2 Increasingly Connected

- Vendor Remote Access
- Visibility “shop floor to top floor” metrics and KPIs
- Data analytics programs
- Predictive analytics
- Supply chain integration

3 Lacking Collaboration

- “Plant/distribution” vs. IT Security
- No common IT/OT view of complete ICS environment
- No IT/OT collaboration tools
- Governance gaps or conflicts

4 Insufficient Visibility / Security

- No visibility across ICS networks
- Undetected network configuration issues
- No threat monitoring
- Poorly managed remote access control & password

POTENTIAL UNFAVORABLE BUSINESS OUTCOMES FROM CYBER ATTACKS IN OT

Financial Loss

- Lost revenue from production delays
- Significant costs associated with major IT incident
- Ransom payments
- **Example: $11 million ransomware payment from JBS Foods**

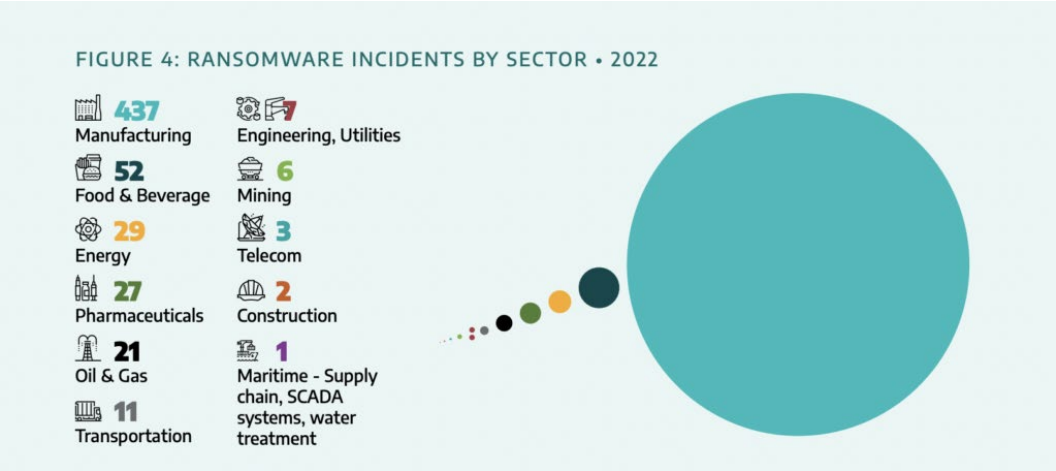
Production Line(s) Down

- Inability to manufacture and deliver products
- Inefficiency in production due to lack of connection to analytics
- Potential downstream impacts to supply chain
- **Example: OT environment shut down during Colonial Pipeline ransomware attack**

Negative Impacts to the Health / Safety of Employees

- Unsafe parameters set on manufacturing systems that could impact employees
- Inability of alarms to properly identify unsafe working conditions
- Improper set points could lead to plants operating at unsafe environmental levels
- **Example: Attacker poisoned water supply in Oldsmar, FL attack**

CURRENT TRENDS IN THREAT LANDSCAPE



Key Ransomware Findings

87%

Ransomware attacks against industrial organizations **increased 87 percent** over last year.

+35%

Dragos tracked **35% more ransomware groups** impacting ICS/OT in 2022.

72%

of all ransomware attacks targeted **437 manufacturing entities** in **104 unique manufacturing subsectors**.

POTENTIAL APPROACHES FOR AUDITING OT SECURITY, AND SAMPLE OUTPUT

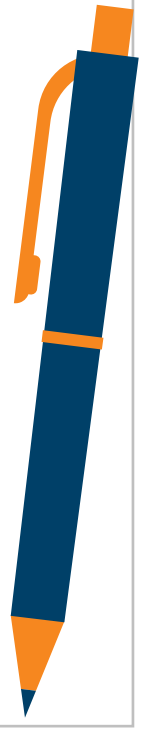
POTENTIAL AUDIT SCOPES

There are different ways that Operational Technology can be included in the audit plan

Risk & Governance – Assess and provide recommendations on how to role out a governance program

Sample Field Sites – Security assessments with site walkthroughs, control testing, and how aligned with the overall security plan

Advisory Track – Influencing what control framework the field sites use and help drive training opportunities



OT SECURITY FRAMEWORKS / REGULATIONS

TSA Security Directives

- TSA released security directives that are applicable to owners and operators of a hazardous liquid and natural gas pipeline, or a liquefied natural gas facility notified by the TSA that their pipeline system or facility is critical

NERC-CIP Regulations

- Mandatory security standards that apply to entities that own or manage facilities that are apart of the US and Canadian electric power grid

Frameworks

- IEC-62443
- NIST 800-82
- NIST CSF

AUDIT APPROACH EXAMPLE

Industrial Control System Security Review

Protiviti recommends following a holistic approach to assessing the security of Process Control Systems.

Security Assessment

The goal of these engagements is to assess the security posture of industrial controls and identify risk based on network architecture, device configuration and management, as well as network and physical access control.

Asset Management

- Perform a review of site maps, network diagrams and equipment lists for each site.
- Obtain system/device lists from site operators.
- Perform interviews to confirm assets.
- Catalog all assets identified.

Network Architecture

- Utilize asset catalog to determine networks and supporting equipment.
- Obtain device configurations and rule sets.
- Review rules and validate security parameters of the devices.
- Evaluate ports, protocols, and services needed for each device.

Security Management

- Review system/device configuration standards.
- Review patch management policies and processes.
- Assess a sample of device configurations to industry best practices.
- Perform risk assessments to determine business impact and support requirements.

Physical Security

- Confirm physical security procedures to field sites.
- Identify physical security risks to Process Control systems and networks.

Deliverables: Catalog of plant assets, including device, type and version, network device configuration and access control assessment report, review of network architecture, patch and vulnerability process review, report on device/software vulnerabilities, report on physical security risk points

EXAMPLE REPORT FINDINGS

III. Summary of Observations

The following table summarizes the total number of findings in each priority ranking identified during this OT Security Review.

Ref.	Observation	Priority
OT.1	Anti-Virus Not Installed or Enabled Across all OT systems	High
OT.2	Patch Management Procedures Not Established for OT Systems	High
OT.3	Asset Inventories Are Ad Hoc and Inconsistently Updated	High
OT.4	OT Governance and Project Management Practices Not Established	High
OT.5	Visibility Gaps in OT Network	High
OT.6	Legacy Operating Systems in use at Sampled OT Sites	High
OT.7	Gaps in DMZ Security Controls	Medium
OT.8	Weak Controls for Physical Security	Medium
OT.9	OT Sites Do Not Have Continuity Procedures	Medium
OT.10	IDS/IPS Solution Not in Place for OT Network	Medium
OT.11	Ineffectual or non-existent access reviews	Medium
OT.12	Insecure OT Account Password Settings	Medium
OT.13	OT Admins used Shared Accounts with Elevated Privileges	Medium
OT.14	Firewall Management	Medium
OT.15	Network Access Control (NAC) Not in Place for OT Network	Low

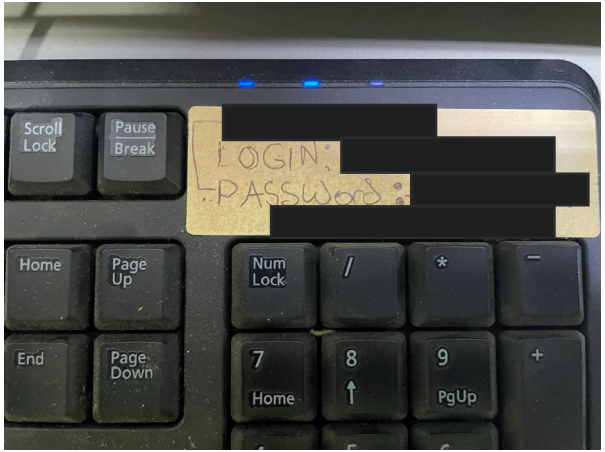
EXAMPLE SITE SURVEYS TO ASSESS RISK

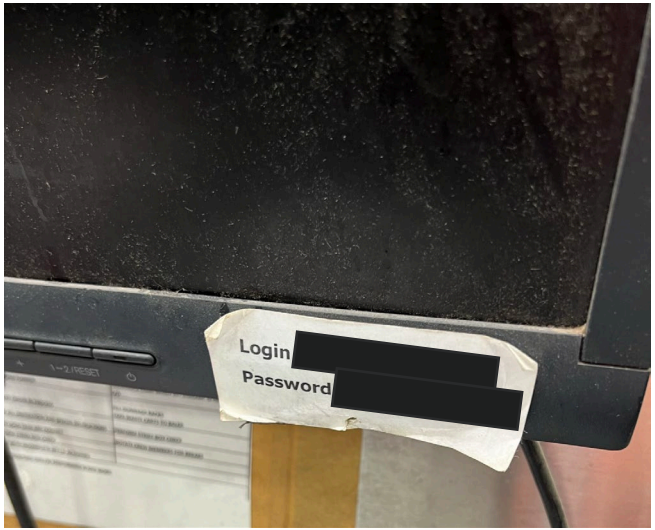
NIST Categor	OT Security Policy	Corp / Plant	Questions list	Considerations	Scope	Category	Answers
IDENTIFY	5.1.2	Corp	**Does this plant have a measurable risk management program in place?**	Is threat intelligence information related to plant OT assets received by means of advisories, vendor notifications, security alerts, etc.?	Tier 1, Tier 2	Risk Management	▪ YES for all listed items (Risk Score: 0) ▪ NO for all listed items (Risk Score: 2) ▪ Partial - Yes for some or most listed items (1) ▪ NA
				Are internal and external threats to plant OT assets documented?	Tier 1 only	Risk Management	
IDENTIFY	5.1.3 5.1.5	Corp	**Is business impact analysis (BIA) conducted to include this plant and OT assets?**	Does this plant have a risk classification in relation to [redacted] overall manufacturing processes and facilities e.g. high risk, medium risk, low risk plant?	Tier 1, Tier 2	Business Impact Analaysis	▪ YES for all listed items (Risk Score: 0) ▪ NO for all listed items (Risk Score: 5) ▪ Partial - Yes for some or most listed items ▪ NA
				Do accurate network architectures and data flow diagrams exist for OT assets at this plant?	All Plants	Business Impact Analaysis	
				Are assets and applications prioritized by criticality?	Tier 1 only	Business Impact Analaysis	
				If yes, are critical asset and application dependencies identified?	Tier 1 only	Business Impact Analaysis	
				Is redundancy built in to plant processes / network to ensure resiliency and high availibility of critical assets and applications?	Tier 1, Tier 2	Business Impact Analaysis	
IDENTIFY	5.1.3	Corp	**Are third party risks identified and managed?**	Are critical vendors to this plant identified?	Tier 1, Tier 2	Supply Chain Risk	▪ YES for all listed items (Risk Score: 0) ▪ NO for all listed items (Risk Score: 4) ▪ Partial - Yes for some or most listed items ▪ NA
				Are critical vendors monitored for compliance with [redacted] policies?	Tier 1 only	Supply Chain Risk	
				Do vendor agreements and / or contracts address OT security risks?	Tier 1, Tier 2	Supply Chain Risk	
				Are vendors periodically re-evaluated for compliance with [redacted] policies related to security and risk management?	Tier 1 only	Supply Chain Risk	
IDENTIFY	5.1.4	Plant	**Does the plant implement and maintain an adequate asset management standard?**	Is there an inventory of physical assets i.e. OT hosts and network devices at this plant?	All Plants	Asset Management	▪ YES for all listed items (Risk Score: 0) ▪ NO for all listed items (Risk Score: 5) ▪ Partial - Yes for some or most listed items ▪ NA
				Is there a list/inventory of software and applications installed and in use maintained? If yes, does it include version and build info?	Tier 1, Tier 2	Asset Management	
				Do all hardware and software assets have an owner or responsible team assigned?	All Plants	Asset Management	
				Are inventories maintained i.e. updated periodically and checked for accuracy?	All Plants	Asset Management	
				Is there a decommissioning procedure followed e.g. updating status in inventory after retiring or uninstalling?	Tier 1, Tier 2	Asset Management	

EXAMPLE INPUTS TO RISK REGISTER

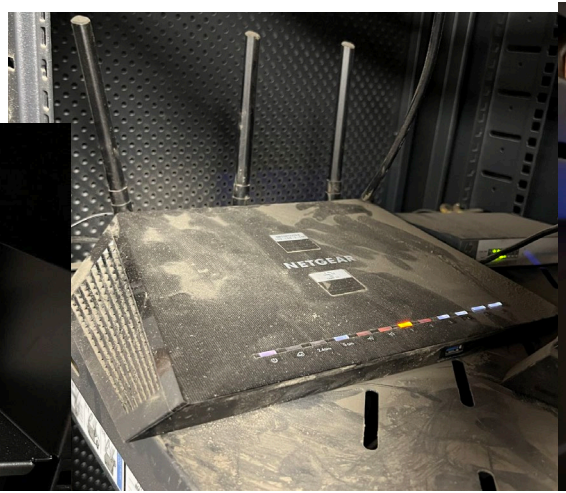
Name	Effort Owner	Likelihood of Occurrence (1-5)	Operations Impact (1-5)	Calculated Risk Score (2 - 10)	Weighted Risk Score
Secure Remote Access		5	5	10	10
OT Site Segmentation		5	5	10	10
Privileged Access Management		4	5	9	9.5
OT Patch Management		4	5	9	9.5
OT Vulnerability Management Program		4	4	8	8
Semi-Annual Firewall Ruleset Reviews		4	4	8	8
Establish OT Network Visibility		4	4	8	8
Asset Management		3	4	7	7.5
Network Access Control		3	4	7	7.5
Resources and Governance		2	4	6	7
Risk Indicators for Site Priority		2	4	6	7
Security Awareness & Training		4	3	7	6.5
Endpoint Protection		4	3	7	6.5
Physical Security Controls		4	3	7	6.5
OT Log Aggregation		4	3	7	6.5
Incident Response Tabletops		3	3	6	6
Socialize OT Security Policy		2	3	5	5.5
OT Risk Register		2	3	5	5.5
Business Impact Analysis		2	3	5	5.5
OT System Change Auditing		2	3	5	5.5
Third-Party Risk Management		3	2	5	4.5
Semi-Annual User Reviews		3	2	5	4.5

EXAMPLE OBSERVATIONS – VISIBLE PASSWORDS



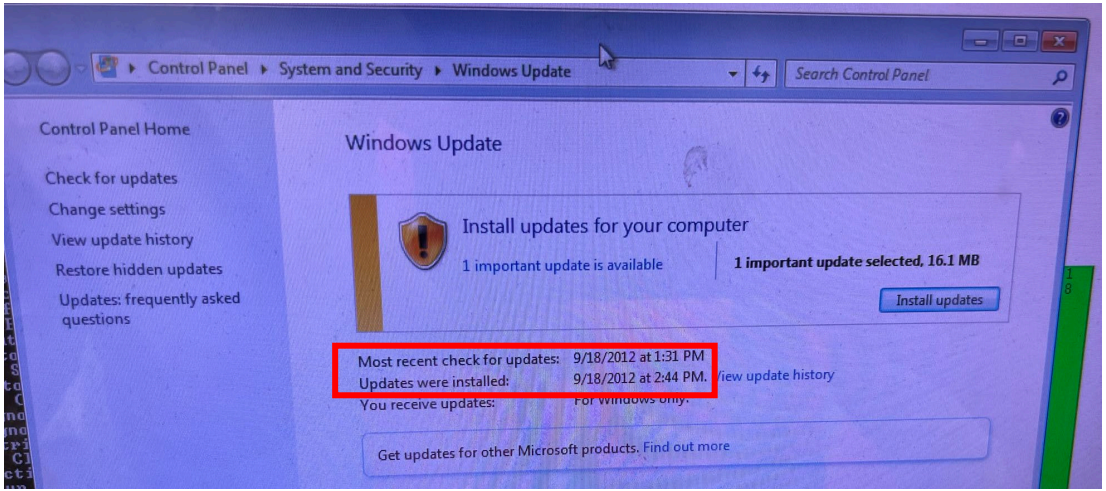


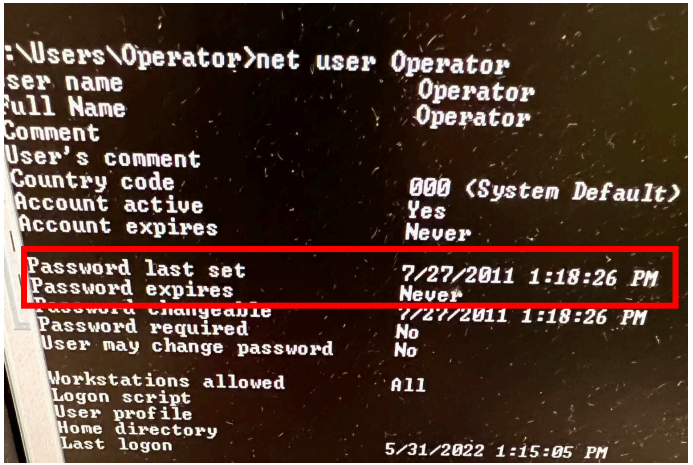
EXAMPLE OBSERVATIONS – NON-STANDARD DEVICES



protiviti

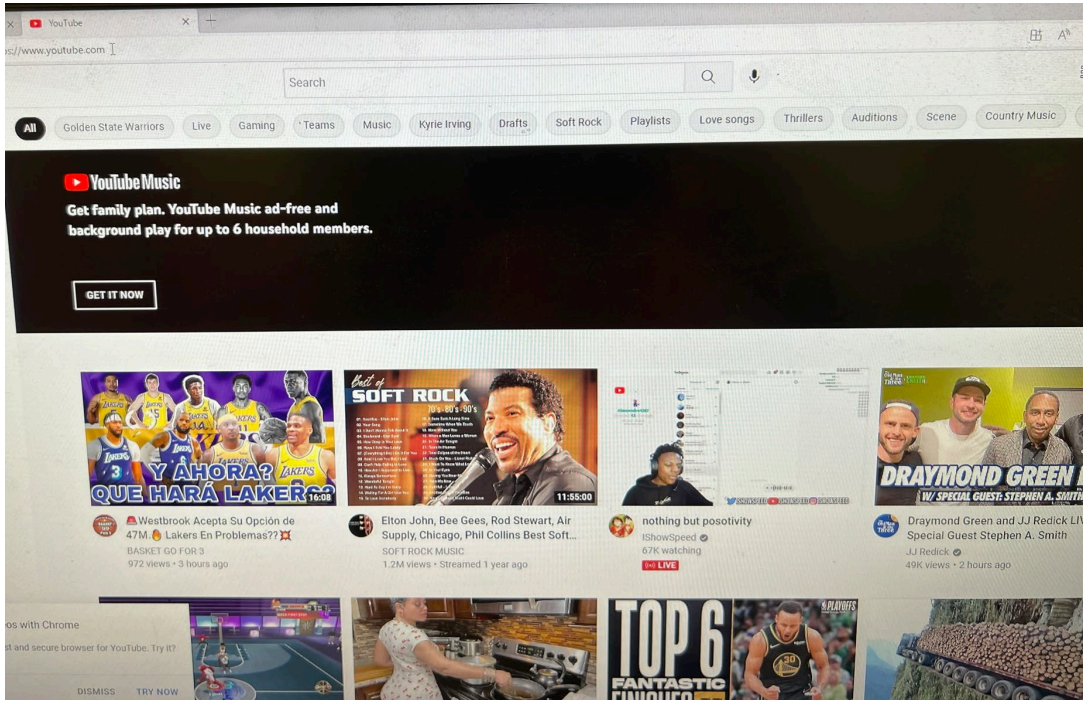
EXAMPLE OBSERVATIONS – OUTDATED PATCHES AND PASSWORDS





protiviti

EXAMPLE OBSERVATIONS – OPERATOR WORKSTATIONS WITH INTERNET ACCESS



protiviti

COMMON MYTHS AND RECOMMENDED FOCUS AREAS

COMMON MYTHS

As OT Security has gained more notoriety, some myths have emerged from the public and IT teams as they gain more accountability for improving the safety, security and reliability of operational environments. While there may be some truth to these myths, some further context is needed to understand whether these myths are true or not.

1. If it’s air gapped, it's secure
2. You can use the same controls in OT as in IT
3. If it’s a legacy system, there's nothing you can do to secure it
4. Our organization isn’t important enough to be a target
5. We need a local cybersecurity team and the latest tools in order to have a safe, secure environment

BUILDING A PATH TO SAFE / RELIABLE OPERATIONS

Now that we understand some of the common pitfalls and myths related to OT security, let's discuss how companies can start to build a roadmap for safe, reliable operations.

1. Prioritize locations/facilities by business risk
2. Identify assets within the OT environment
3. Secure VPN and remote access
4. Enforce Network Segmentation between IT and OT
5. Restrict access control/permissions on a least privilege basis
6. OT network monitoring and visibility
7. Address highest risk vulnerabilities first, focusing on those with publicly available exploits

APPENDIX – PROTIVITI CAPABILITIES

PROTIVITI OT SECURITY CAPABILITIES

The Protiviti's OT Security solution comprises the following components to keep systems supporting critical infrastructure running safely, reliably, and with minimum disruption. Our security solutions are scalable / flexible to meet the needs of your program, to provide assurance for your customers that critical processes are resilient to today's threats.

Where Can Protiviti Help Organization with their OT Security Needs?

1 Governance & Transformation

- OT Security Transformation
- Risk Management Program
- OT Standards
- Compliance (TSA, NERC-CIP)
- Program oversight

2 OT Security Assessment

- Network Segmentation
- Security Architecture
- Physical Security
- Logical Access to OT

3 OT Security Monitoring

- Passive Asset Discovery
- Automated Detection
- Incident Response
- Patch Management
- Tabletop Exercises
- Managed Detect & Respond

4 Security Testing / Compromise Assessment

- Vulnerability Assessment
- Penetration Testing
- Analysis and Remediation
- Targeted Testing

THOUGHT LEADERSHIP

Recent Thought Leadership

- Three Steps to Build an Effective Industrial Control Systems Security Program
- Webcast – Industrial Control System Security Basics
- Ransomware Crisis: 11 Actions to Secure Critical Infrastructure
- Smooth (and Secure) Operator: A Perspective on the Oldsmar Water Plant ICS Breach
- Lessons Learned From The Colonial Pipeline Attack And Recent TSA Directives
- TSA Security Directive Impacts to the Rail Industry

QUESTIONS?

Face the Future with Confidence®

protiviti®