EBOOK

The CISO's 5 Step Guide to Securing Operational Technology (OT)

COPIA

Introduction

Operational Technology (OT) environments, the backbone of manufacturing and distribution, are facing an ever-growing spectrum of cyber threats. As digital transformation accelerates, OT environments are subject to new attack vectors. CISOs are now tasked with securing complex, interconnected systems that were traditionally isolated and often designed without security in mind. This guide outlines a **practical 5 step approach** to building a robust OT security posture, enabling safe, scalable, and compliant operations.

STEP 1:
Understand your Business Operational Workflows and Data Needs

Explainer:

There is no one size fits all approach for securing OT environments and downtime for implementing change is often expensive and scarce. Securing OT environments requires a deep understanding of your business operational workflows and data needs to properly design a secure OT network that is adaptable to your current and future business requirements. Learning your business is critical for designing an OT network that is built to grow with your business without having to implement anti-patterns (Ex. RDP exposed to the public internet) as a tactical response to business changes.

Action Plan: 2 Key Decisions

1. **Document Business Workflow:**
   - Document manufacturing workflows and understand how they change over time.
   - Understand who is part of your business works (System Integrators, Full-Time Staff, Remote Support, etc.).
2. **Document & Anticipate Data Needs:**
   - Document data required for reports and analytics for architectural consideration.

STEP 2:

Network Your Factories and Devices

Building a Secure Foundation

Explainer:

The next step involves establishing a secure and reliable network infrastructure that connects the necessary OT devices and systems. This often requires modernizing legacy networks to support contemporary technologies and address evolving cyber threats, particularly ransomware. A robust network segmentation strategy, coupled with secure remote access patterns and Mulit-Factor Authentication (MFA), is crucial.

Action Plan: 5 Key Decisions

1. Network Segmentation Strategy:

- Define clear zones and conduits based on business workflows, egress data, remote access, critical operational assets (domain controllers, etc.), and other identified risk factors.
- Implement firewalls, micro segmentation, and Zero-Trust validation measures to enforce segmentation.

2. Secure Remote Access:

- Use encrypted remote connections with Multi-factor authentication (MFA) for all remote access.
- Move beyond jump servers and utilize an OT native remote access solution that enables robust session visibility and zone access management capabilities.

3. Data Accessibility:

- Implement data diodes to enforce traffic flows for egress data.
- Replicate data from its source to a secure location outside of your OT network intended for wide-spread user access.

4. Industrial Protocol Security:

- Utilize firewalls that understand OT protocols like Modbus and Profinet.
- Implement deep packet inspection (DPI) to monitor and control industrial protocols.

5. Modernization Roadmap:

- Develop a phased modernization plan to upgrade legacy network infrastructure.

STEP 3:
Device Management and Security
Achieving Visibility and Control

Explainer:

You cannot defend what you cannot see. This requires collaboration between IT, OT, and the CISO to identify and manage all assets, including legacy systems and IoT devices. Continuous monitoring and threat detection are essential for identifying and mitigating potential risks.

Action Plan: 5 Key Decisions

1. **Asset Discovery and Inventory:**
   - Deploy network monitoring tools to identify all connected devices.
   - Maintain an accurate and up-to-date asset inventory.
2. **Vulnerability Management:**
   - Conduct regular vulnerability assessments and penetration testing.
   - Prioritize patching and mitigation efforts based on risk.
3. **Anomaly Detection and Threat Monitoring:**
   - Implement Intrusion Detection and Intrusion Prevention Systems (IPS / IDS) for OT networks.
   - Utilize Security Information and Event Management (SIEM) systems for centralized logging and analysis.
   - Consider partnering with an OT Managed Detection and Response (MDR) vendor for specialized OT monitoring.
4. **Endpoint Security:**
   - Deploy anti-malware monitoring on all OT endpoints.
   - Implement application whitelisting and device control.
5. **Collaboration and Communication:**
   - Establish clear communication channels and align on organization goals across IT, OT, and the CISO.
   - Conduct regular security awareness training for OT, IT, and other personnel that interact with operations.
   - Create a cross functional team to review, assess, and address security issues.

STEP 4:

Backup and Disaster Recovery

Ensuring Business Continuity

Explainer:

With asset visibility and security in place, organizations can implement comprehensive backup and disaster recovery (DR) strategies. This includes backing up critical data, configurations, and industrial code. Rapid rollback capabilities are essential for minimizing downtime and ensuring business continuity, especially in the face of ransomware attacks and regulatory requirements like NIS2.

Action Plan: 5 Key Decisions

1. **Industrial Code Backup and Version Control:**
   - Implement version control systems for PLC programs, HMI configurations, and other industrial code.
   - Automate backups and store them in secure, offsite locations, including cloud storage for enhanced accessibility and redundancy.
   - Industrial DevOps platforms provide version control and industrial code backup, ensuring rapid recovery.
2. **Data Backup and Recovery:**
   - Leverage cross functional team (IT-OT-CISO) to identify critical data and implement regular backup schedules.
   - Test recovery procedures to ensure they meet recovery time objectives (RTOs) and recovery point objectives (RPOs).
   - Use backup solutions that are purpose built for the industrial environment.
3. **Disaster Recovery Planning:**
   - Develop a comprehensive disaster recovery plan that addresses various disaster scenarios.
   - Conduct regular disaster recovery drills to test the plan's effectiveness.
   - Develop a plan that includes offline backups.
4. **Vendor Selection:**
   - Choose backup and Disaster Recovery vendors that specialize in OT environments.
   - Ensure the vendor supports rapid rollbacks and meets regulatory requirements.
   - Choose vendors that can provide rapid rollback of PLC and other industrial code.
5. **Regulatory Compliance:**
   - Ensure backup and Disaster Recovery practices comply with relevant regulations, such as NIS2.
   - Maintain detailed records of backup and recovery activities.
   - Document all procedures in a centralized location that is accessible to cross functional teams.

STEP 5:

Scale Production

Leveraging Industrial DevOps and AI

Explainer:

With a secure and resilient OT environment, organizations can scale production through AI-driven Industrial DevOps. This involves moving towards code deployment automation, implementing continuous integration/continuous delivery (CI/CD) pipelines, and using AI for predictive maintenance and process optimization. The foundation of secure networking, device management, and reliable backups ensures that data fed to AI models is clean and trustworthy. Industrial DevOps is crucial for enabling the AI Factory of the Future, providing the necessary tools for managing and optimizing industrial code. It empowers automation engineers, enhances collaboration, and ensures the quality and safety of AI-driven changes in the production environment.

Action Plan: 5 Key Decisions

1. **Industrial DevOps Implementation:**
   - Implement CI/CD pipelines for industrial code deployment.
   - Automate testing and validation of code changes.
   - Integrate AI tools with a structured and version-controlled environment for code management.

2. **AI for Predictive Maintenance:**
   - Deploy AI-powered predictive maintenance solutions to identify potential equipment failures.
   - Utilize sensor data and historical data to train AI models.

3. **Process Optimization with AI:**
   - Use AI to analyze production data and identify opportunities for process improvement.
   - Implement AI-driven control systems to optimize production parameters.
   - Industrial DevOps enables the safe and efficient deployment of AI-driven control systems by providing mechanisms for code review, testing, and validation.

4. **Data Governance and Security:**
   - Establish robust data governance policies to ensure data integrity and security.
   - Implement access controls and encryption to protect sensitive data.
   - Industrial DevOps supports data governance by providing tools for managing and tracking data changes, and ensuring that AI models operate on trusted data.

5. **Continuous Improvement:**
   - Establish a culture of continuous improvement and innovation.
   - Regularly evaluate and refine Industrial DevOps and AI strategies.
   - Industrial DevOps provides the infrastructure for continuous improvement, while maintaining system stability and safety.

Conclusion

By following these 5 steps, CISOs can build a robust OT security posture that enables safe, scalable, and compliant operations. Industrial DevOps and AI are powerful tools for driving efficiency and innovation, but they must be built on a foundation of strong security and resilience. To get started on your journey to a secure and AI-ready future, schedule a demo and explore how Copia Automation's Industrial DevOps platform can help you implement these best practices today.

To speak to a Copia Automation representative about Copia Industrial DevOps Platform and help manage your automation workflow more effectively, visit copia.io.