Six Best Practices for OT Cybersecurity

A whitepaper

Sekurinova

A W-INDUSTRIES Company

Introduction

How to protect your operational technology from cyber threats

Operational technology (OT) refers to the hardware and software that control physical processes and devices in the manufacturing, energy, transportation, and healthcare industries. OT systems are often connected to the internet or other networks, which exposes them to cyberattacks that can disrupt operations, damage equipment, or endanger safety. According to a report by Gartner, 75% of OT organizations experienced at least one security breach in the past year, and 85% reported a high or critical level of risk to their OT environment (Gartner, 2023). Some of the common challenges for OT cybersecurity are:

- Lack of visibility and monitoring of OT assets and network activity, which makes it difficult to detect and respond to cyber incidents
- Legacy systems that are outdated, unsupported, or unpatched, which create vulnerabilities and compatibility issues
- Insufficient segmentation and isolation of OT networks from IT networks, which increases the attack surface and the potential impact of cyberattacks
- Low awareness and training of OT staff on cybersecurity best practices, which leads to human errors and weak security hygiene

This article will discuss six best practices for OT cybersecurity that can help you protect your OT systems from cyber threats and enhance your OT resilience.

1. Conduct a risk assessment

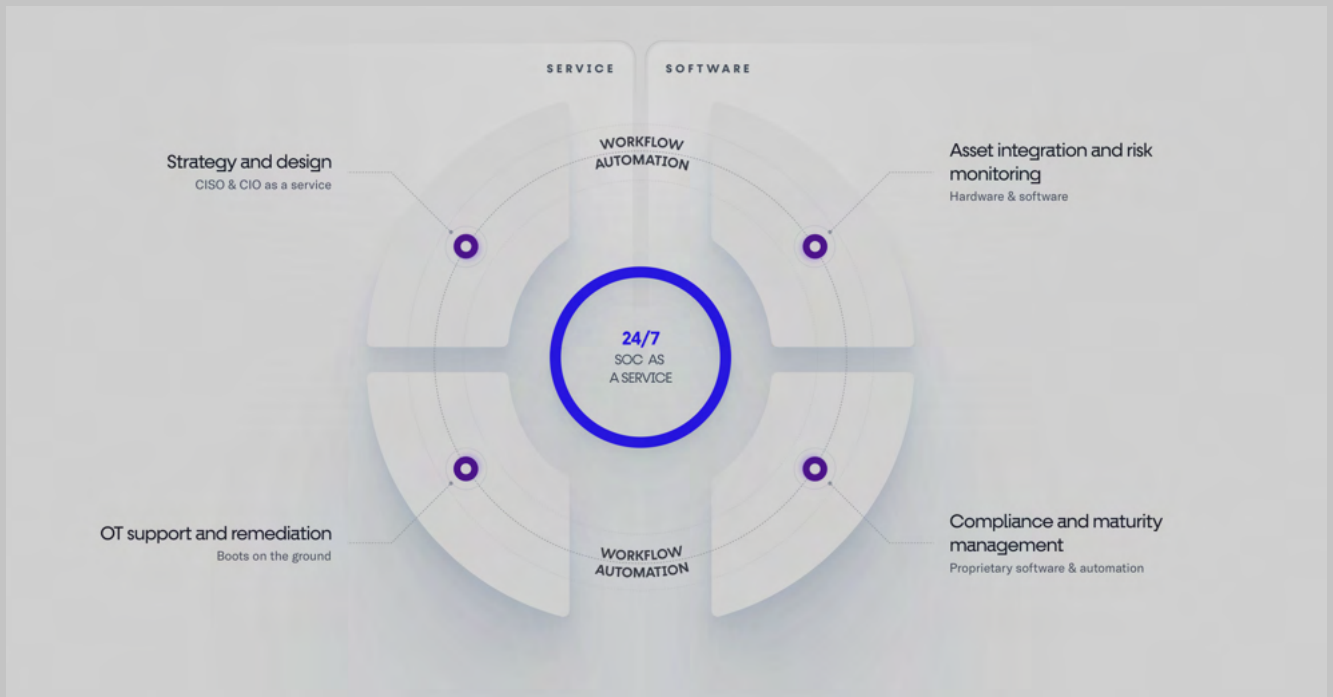
The first step to improve your OT cybersecurity is to conduct a risk assessment that identifies your OT assets, threats, vulnerabilities, and impacts. A risk assessment can help you prioritize your OT security needs and allocate your resources accordingly. You can use frameworks and standards such as NIST CSF, IEC 62443, or ISO 27001 to guide your assessment and establish a baseline for your OT cybersecurity maturity. You should also perform regular audits and tests to validate your controls and detect gaps or weaknesses. For example, you can use vulnerability scanners, penetration testing, or red teaming to assess your OT security posture and identify areas for improvement.

2. Implement a layered and defense-in-depth approach

Based on your risk assessment, you should implement a layered and defense-in-depth approach to OT cybersecurity that covers the following aspects:

- Physical security: Secure access to OT facilities and devices with locks, alarms, cameras, and biometrics. Physical security can prevent unauthorized or malicious access to your OT systems and reduce the risk of theft, sabotage, or tampering.
- Network security: Segment and isolate OT networks from IT networks and the internet, and use firewalls, VPNs, and encryption to protect data in transit. Network security can limit the exposure and the impact of cyberattacks on your OT systems and prevent the propagation of malware or intrusions.
- Device security: Regularly update and patch OT devices and use antivirus, whitelisting, and hardening to prevent unauthorized changes or malware infections. Device security can reduce the vulnerabilities and the attack surface of your OT systems and ensure their availability and integrity.
- Data security: Backup and restore OT data frequently and use encryption, hashing, and digital signatures to ensure data integrity and authenticity. Data security can prevent data loss or corruption due to cyberattacks or system failures and enable data recovery and verification.
- User security: Enforce strong authentication and authorization policies for OT users and use role-based access control and logging to limit and track user actions. User security can prevent unauthorized or malicious access to your OT systems and ensure accountability and traceability of user activities.
- Incident response: Prepare and test an OT incident response plan that defines roles, responsibilities, procedures, and communication channels for handling cyber incidents. Incident response can help you respond to and recover from cyberattacks on your OT systems and minimize their impact and damage.

Sekuranova approach to Cybersecurity



3. Monitor and analyze your OT network data

OT cybersecurity is not a one-time project but a continuous process that requires constant monitoring, review, and improvement. Using tools and technologies such as SIEM, IDS, and OT-specific solutions would be best to collect and analyze OT network data and detect any anomalies or threats. Using metrics and indicators such as KPIs, KRIs, and KCIIs to measure and evaluate your OT security performance and effectiveness would be best. By monitoring and analyzing your OT network data, you can gain visibility and insight into your OT security posture and identify any issues or risks that need to be addressed.

4. Update and refine your OT cybersecurity policies and controls

As the threat landscape and the business needs change, you should update and refine your OT cybersecurity policies and controls to adapt to the new challenges and requirements. You should review your OT security policies and controls regularly and ensure they align with the industry's best practices and standards. You should also periodically test and validate your OT security policies and controls and ensure they are effective and efficient. By updating and refining your OT cybersecurity policies and controls, you can ensure that your OT security strategy is relevant and robust.

5. Train and educate your OT staff on cybersecurity awareness and best practices

One of the most critical factors for OT cybersecurity is the human factor. You should train and educate your OT staff on cybersecurity awareness and best practices and ensure they have the skills and knowledge to operate and protect your OT systems. You should also conduct regular awareness campaigns and simulations to reinforce your OT staff's security culture and behavior. By training and educating your OT staff on cybersecurity awareness and best practices, you can reduce the human errors and insider threats that can compromise your OT security.

6. Foster a culture of collaboration and trust between OT and IT teams

Another key factor for OT cybersecurity is the collaboration and trust between OT and IT teams. You should foster a culture of cooperation and trust between OT and IT teams and ensure they have a common understanding and a shared vision of OT security. You should also establish clear roles and responsibilities and effective communication and coordination mechanisms for OT and IT teams. By fostering a culture of collaboration and trust between OT and IT teams, you can leverage the strengths and expertise of both domains and enhance your OT security.

Conclusion

OT cybersecurity is a critical and complex issue that requires a holistic and proactive approach. Following the six best practices discussed in this article can improve your OT cybersecurity and protect your OT systems from cyber threats. You can also enhance your OT resilience and performance and support your business objectives and outcomes.