OT Asset Security - A CISO's Guide for Best Practices

In today's digitally interconnected landscape, securing operational technology (OT) environments has become paramount. These environments, which control critical infrastructure and industrial processes, face a myriad of cybersecurity challenges. From legacy infrastructure to supply chain vulnerabilities, the complexities of OT security are vast and multifaceted. As OT systems continue to converge with IT networks and regulatory demands evolve, organizations must navigate a dynamic landscape to ensure the resilience and integrity of their OT environments. Chief Information Security Officers (CISOs) and OT security professionals must implement robust measures to safeguard critical infrastructure and industrial processes. This document presents key best practices for securing OT systems, along with relevant industry standards and regulations, particularly focusing on regulatory landscapes in different regions.

Common Industry Standards and Regulations

Japan Regulations

Act on the Protection of Critical Infrastructure (ACI):

- The ACI mandates that organizations operating critical infrastructure sectors, including OT environments, implement cybersecurity measures to protect against cyber threats.
- Key controls outlined in the ACI include requirements for vulnerability management, secure configuration, access control, and incident response tailored to the unique needs of critical infrastructure sectors.

Industrial Cybersecurity Guidelines:

- Issued by METI and IPA, the Industrial Cybersecurity Guidelines provide comprehensive recommendations and best practices for enhancing cybersecurity in industrial settings, including OT environments.

Japan's Cybersecurity Basic Act:

- The Cybersecurity Basic Act sets forth Japan's national cybersecurity strategy and establishes the framework for cybersecurity measures across various sectors, including critical infrastructure and industrial systems.
-

- The Act emphasizes the importance of implementing robust cybersecurity measures in OT environments to protect against cyber threats and ensure the resilience of critical infrastructure.

US Regulations

In the United States, OT security is subject to various regulations and guidelines, including:

- NIST Special Publication 800-82: Provides guidance on securing industrial control systems (ICS) within critical infrastructure sectors.

Department of Homeland Security (DHS) Critical Infrastructure Cyber Community (C3) Voluntary Program: Offers resources and tools for enhancing cybersecurity in critical infrastructure sectors.

UK/EU Regulations

- In the United Kingdom and the European Union, OT security regulations and standards include:
    - EU Directive 2008/114/EC: Requires EU member states to identify and designate critical infrastructure sectors and develop measures to ensure their protection against threats, including cyber attacks.

- UK National Cyber Security Centre (NCSC) Industrial Control Systems Security Guidance: Provides guidance on securing industrial control systems against cyber threats.

Summary of Controls and Instructions for OT Security

Vulnerability Management:

- OT Security Best Practices: Establish processes for identifying, assessing, and mitigating vulnerabilities in OT systems, including timely deployment of security patches and updates.
- US Regulations (e.g., NIST Special Publication 800-82): Implement vulnerability management practices to ensure timely identification and remediation of vulnerabilities in OT systems.
- UK/EU Regulations (e.g., EU Directive 2008/114/EC): Align vulnerability management processes with regulatory requirements to protect critical infrastructure sectors against cyber threats.
- Japan Regulations: Comply with the Act on the Protection of Critical Infrastructure (ACI), which mandates organizations to implement cybersecurity measures, including vulnerability management, tailored to the unique needs of critical infrastructure sectors.

Secure Configuration:

- OT Security Best Practices: Configure OT systems securely, following industry best practices to minimize security risks and vulnerabilities.
- US Regulations (e.g., DHS C3 Voluntary Program): Implement secure configurations in OT systems to enhance resilience against cyber attacks and unauthorized access.
- UK/EU Regulations (e.g., UK NCSC Industrial Control Systems Security Guidance): Adhere to secure configuration requirements outlined in regulatory frameworks to mitigate cybersecurity risks associated with OT deployments.
- Japan Regulations: Adhere to secure configuration guidelines provided by the Ministry of Economy, Trade, and Industry (METI) and the Information-technology Promotion Agency, Japan (IPA), ensuring OT systems are hardened against cyber threats.

Supply Chain Security:

- OT Security Best Practices: Vet and monitor OT system suppliers, ensuring the integrity and security of components throughout the supply chain.
- US Regulations (e.g., NIST Special Publication 800-82): Establish supply chain security measures to verify the

- integrity and authenticity of components sourced from vendors and mitigate supply chain-related risks.
- UK/EU Regulations (e.g., EU Directive 2008/114/EC): Ensure that supply chain security practices comply with regulatory requirements to protect critical infrastructure sectors against cyber threats.
- Japan Regulations: Implement supply chain security measures in line with guidelines provided by METI and IPA, verifying the integrity of components and mitigating supply chain risks in OT environments.

How DeviceTotal can help enforce OT security strategy and meet compliance

Comprehensive Security Assessment: DeviceTotal offers comprehensive security assessments to identify vulnerabilities, compliance gaps, and security risks in OT systems, helping organizations ensure compliance with regulatory requirements and industry standards.

Continuous Monitoring: DeviceTotal provides continuous monitoring capabilities to detect and respond to security threats and incidents in real-time, enhancing the overall security posture of OT environments and ensuring compliance with regulatory mandates.

Regulatory Compliance Reporting: DeviceTotal facilitates regulatory compliance reporting by generating compliance reports to demonstrate adherence to relevant regulations and industry standards, streamlining compliance efforts for CISOs and organizations operating in different regions.

DeviceTotal enables CISOs to define thresholds for proactive security issue reporting, allowing them to customize the focus areas based on organizational priorities and risk tolerance. For example:

- **Threshold for Risk Level:** CISOs can set thresholds for risk levels, such as high, medium, and low, based on the organization's risk appetite. This allows them to prioritize remediation efforts for critical vulnerabilities while effectively managing resources.
- **Threshold for Impact Percentage:** CISOs can define thresholds for the impact percentage on the organization and site. For instance, they may set a threshold of 70% for the impact on the organization, indicating that any risk with an impact percentage above this threshold requires immediate attention.
- **Threshold for In the Wild:** CISOs can specify whether they want to receive reports on risks observed "In the Wild," indicating real-world scenarios. This helps prioritize mitigation efforts for risks that are actively exploited or pose imminent threats to the organization.

- **Threshold for EOL/S (End-of-Life/Support):**
    - CISOs can establish thresholds for the EOL/S status of IoT devices and vendors. By setting thresholds for EOL/S status, CISOs can identify devices that may be at increased risk due to lack of vendor support and plan accordingly for their security maintenance or replacement.
- **Threshold for Attack Vector:**
    - CISOs can define thresholds for specific attack vectors, such as remote code execution or denial of service. This allows CISOs to prioritize remediation efforts based on the potential impact and likelihood of exploitation associated with different attack vectors.

By leveraging DeviceTotal's customizable issue reporting capabilities, CISOs can tailor their security strategies to address the most relevant and impactful threats, ensuring effective risk management and compliance with regulatory requirements.

DeviceTotal

DeviceTotal Security Reporting Thresholds Customization Example:

Responsible Vendor	EOL/S	Risk	Attack Vector	Impact on Organization (%)	Impact on Site (%)	In the Wild	Vendor Recommendation	CISO Instruction for DeviceTotal
False	True	Critical	Remote Code Execution	80	70	Yes	Apply latest patches	Present issue
True	False	High	Denial of Service	50	60	Yes	Upgrade to supported version	Preset issue
True	True	Medium	Denial of Service	90	80	No	Upgrade to supported edition	Present issue
True	False	Medium	User Interaction	40	50	No	Upgrade to supported version and apply security updates	Don't present
False	False	Low	Physical Access	20	10	No	Implement additional access controls	Don't present

Severity levels colors:

Critical	High	Medium	Low

By integrating DeviceTotal into their security strategy, CISOs can gain actionable insights and effectively manage IoT device security, ensuring compliance with regulatory requirements and industry best practices :

Customizable Reporting Thresholds

- DeviceTotal allows CISOs to define thresholds for security reports based on their organization's priorities and risk tolerance. CISOs can specify criteria such as risk levels, impact percentages, and the presence of vulnerabilities "In the Wild" to tailor reports to their specific requirements.

Risk-based Approach

- CISOs can utilize DeviceTotal's risk-based approach to determine which security issues should be prioritized for reporting and remediation. By setting thresholds for severity levels, CISOs can focus on addressing critical vulnerabilities that pose the highest risk to their organization's security posture.

Impact Assessment

- DeviceTotal enables CISOs to assess the impact of security risks on their organization and site by defining thresholds for impact percentages. This allows CISOs to prioritize remediation efforts for vulnerabilities that have the most significant potential impact on their operations and infrastructure.

Vendor Recommendations

- DeviceTotal provides vendor recommendations based on the identified security risks and vulnerabilities. CISOs can use these recommendations to guide their decision-making process and develop action plans for addressing security issues, such as applying patches or upgrading to supported versions.

EOL/S Assessment

- DeviceTotal allows CISOs to evaluate the end-of-life (EOL) and end-of-support (EOS) status of IoT devices and vendors. By setting thresholds for EOL/S status, CISOs can identify devices that may be at increased risk due to lack of vendor support and plan accordingly for their security maintenance or replacement.

DeviceTotal recognizes the complex challenges of securing enterprise networks in today's landscape, and enhancing clarity and simplicity in this realm is among our primary objectives.

By specifying the desired thresholds as outlined above, DeviceTotal is committed to optimizing the effectiveness and wisdom of IoT security measures. Our platform streamlines the process, ensuring that organizations can navigate the complexities of IoT security with ease and confidence.