



7 Cybersecurity Within OT

Topics

- Insight into OT Cybersecurity
- Core Principles of OT Cybersecurity
- The Layers of Defense-in-Depth
- Risk Assessment and Management Within OT Systems
- Regular Security Assessments
- The Journey of a Security Assessment Process
- Advantages of Regular Security Assessments
- Reporting and Information Sharing
- Best Practices for Incident Response and Information Sharing
- The Big Three: NERC CIP, IEC 62443, and NIST SP 800-82

Insight into OT Cybersecurity

Challenges Unique to OT Cybersecurity

- OT systems oversee physical processes
- The demands of real-time processes
- Integration of legacy systems
- Interaction of IT and OT

Layered Defenses

- **Defense in Depth**
 - Physical security
 - Network segmentation
 - Access control
 - Intrusion detection and prevention
 - Endpoint protection
 - Security monitoring

Risk Assessment & Monitoring

- Identifying and evaluating potential risks
- Prioritizing based on impact and probability
- Risk mitigation
- Maintaining asset inventory
- Threat modeling
- Vulnerability assessments
- Establishing risk tolerance levels

Security Technologies & Solutions

- Firewalls
- IDS/IPS
- Secure remote access solutions
- SIEM (Security Information and Event Management) systems
- Encryption
- Authentication
- Secure coding

Incident Response & Recovery

- Incident response plans
- Regular testing
- Scenario-based exercises

Awareness & Training

- Educate employees about
 - Cyber threats,
 - Social engineering techniques
 - Secure behavior best practices
 - Security policies
 - Procedures
 - Individual responsibilities

Core Principles of OT Cybersecurity

Core Principles

- **Risk Management**
 - Risk assessments, vulnerability management, monitoring
- **Asset Inventory and Classification**
 - Inventory OT assets, including devices, software, and networks
 - Classify based on criticality, functionality, and impact
- **Secure by Design**
 - Implement security measures from the inception of OT systems
- **Continuous Monitoring and Incident Response**
 - Swift detection and response to security incidents
 - Detection, containment, eradication, and recovery

The Layers of Defense-in-Depth

Defense in Depth

- **Physical Security**
 - Surveillance systems, access controls, intrusion detection systems
- **Network Segmentation**
 - Isolate critical assets
 - Confine a security breach to reduce its impact
- **Access Control**
 - Least privilege

Defense in Depth

- **Intrusion Detection and Prevention Systems (IDS/IPS)**
 - Monitor network traffic
- **Endpoint Protection**
 - Anti-malware, application allow-lists, patch management
- **Security Monitoring and Event Management**
 - Centralized log collection, analysis, and correlation
 - Real-time monitoring of security events
- **Security Awareness and Training**
 - Train employees about common threats, best practices, and their roles in maintaining a secure OT environment

Risk Assessment and Management within OT Systems

The Risk Assessment Process

- **Asset Identification**

- Catalog every asset: hardware, software, networks, data repositories

- **Threat Identification**

- Internal and external threats
- Unauthorized access, malware, physical tampering, natural disasters

- **Vulnerability Assessment**

- Weak points in the OT system
- System configurations, patch levels, access controls, other security controls

The Risk Assessment Process

- **Likelihood Determination**
 - Historical data, threat intelligence, environmental conditions, organizational context
- **Impact Analysis**
 - Operational disruption, safety risks, financial losses, reputational damage
- **Risk Calculation and Prioritization**
 - Combine likelihood and impact
 - Give high priority to risks with high likelihood or impact

The Risk Assessment Process

- **Risk Mitigation**
 - Security controls, patches and updates, enhanced access controls, incident response plans
- **Continuous Monitoring and Review**
 - Review and update risk assessments

Regular Security Assessments

Security Assessments

- Like health check-ups
- Measure OT systems's overall health
- Weaknesses and vulnerabilities
- Possible attack vectors

The Journey of a Security Assessment Process

Security Assessment Process

- **Scoping and Planning**
 - Boundaries of the security assessment
 - Identify systems, assets and processes that need evaluation
 - Set objectives, methodologies, and timelines
 - Ensure communication channels
 - Secure permissions and approvals
- **Information Gathering**
 - Network diagrams, system configurations, asset inventories, security policies

Security Assessment Process

- **Vulnerability Scanning and Penetration Testing**
 - Locate weaknesses
 - Vulnerability scanning uses an automated tool
 - Penetration testing simulates real-world attacks
- **Configuration and Compliance Review**
 - Compare system to industry best standards, security standards, and regulatory requirements
 - Assess compliance with security policies and guidelines, find gaps, and recommend necessary modifications

Security Assessment Process

- **Incident Response and Management Assessment**
 - Evaluate the potency of incident response and incident management capabilities
 - Review incident response plans
 - Test incident response processes
 - Gauge organization's readiness to tackle security incidents
- **Documentation and Reporting**
 - Comprehensive report with results and actionable recommendations
-

Security Assessment Process

- **Remediation and Follow-Up**
 - Follow recommendation to address vulnerabilities and weaknesses
 - Formulate a plan to remediate security gaps
 - Implement necessary security controls
 - Track progress towards a more secure posture

Advantages of Regular Security Assessments

Advantages of Regular Security Assessments

- **Vulnerability Identification**
- **Improved Security Posture**
- **Regulatory Adherence**
- **Incident Response Preparedness**
- **Risk Mitigation and Resource Allocation**
 - Effective resource allocation based on assessment findings

Reporting and Information Sharing

Reporting

- **Incident Response Activation**
 - Sparks a swift response, to
 - Evaluate the incident, neutralize the threat, and minimize its impact
- **Lessons and Upgrades**
 - Record of attacker's **Tactics, Techniques, and Procedures (TTP)**
- **Regulatory Compliance**

Reporting

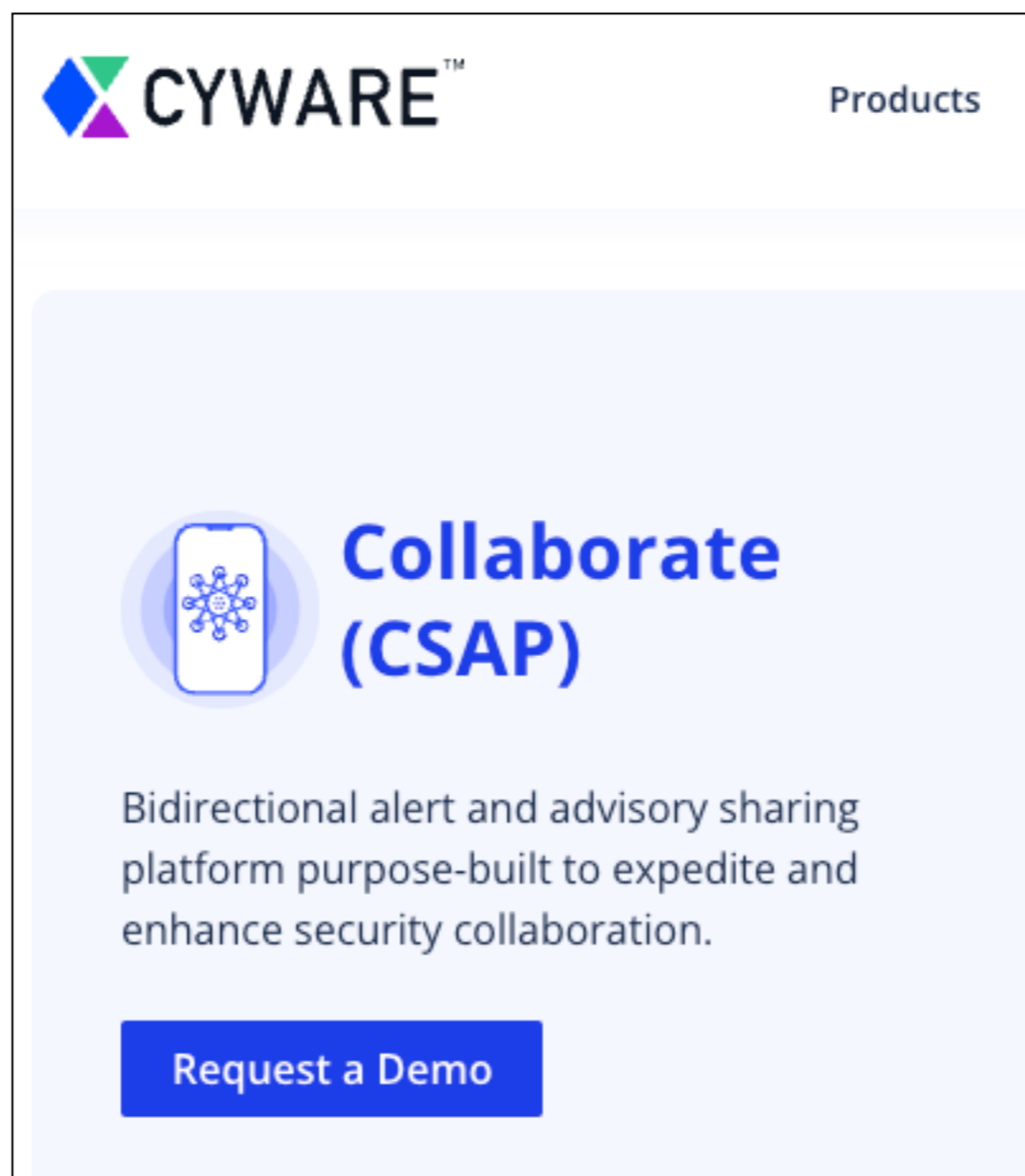
- **Information Sharing**
 - Information sharing with industry organizations, government agencies, and cybersecurity communities fosters collective defense, providing information about
 - Attack vectors
 - Indicators of Compromise
 - Mitigation strategies
- **Early Warning System and Threat Intelligence**
 - New attack vectors and emerging threats
- **Boosting Incident Response**
- **Widening Situational Awareness**

Best Practices for Incident Response and Information Sharing

Best Practices for Incident Response and Information Sharing


- **Clear Reporting Procedures**
 - Furnish employees with necessary channels to report security incidents
- **Promoting Anonymity and Confidentiality**
 - Allows reports, free from fear of repercussions
- **Adopting Standardized Reporting Formats**
- **Using Collaborative Information Sharing Platforms**
 - See next slides

Collaborative Information Sharing Platforms



The image is a screenshot of the Cyware website's product page. At the top left is the Cyware logo, which consists of a stylized 'X' made of four colored triangles (blue, green, purple, and red) followed by the word 'CYWARE' in a bold, sans-serif font with a trademark symbol. To the right of the logo is the word 'Products' in a smaller, grey font. Below the header is a light blue banner. On the left side of the banner is an icon of a smartphone with a network diagram of nodes and lines on its screen. To the right of the icon, the word 'Collaborate' is written in a large, bold, blue font, with '(CSAP)' in a slightly smaller, bold, blue font below it. Underneath the title, there is a paragraph of text: 'Bidirectional alert and advisory sharing platform purpose-built to expedite and enhance security collaboration.' At the bottom of the banner is a blue rectangular button with the white text 'Request a Demo'.

CYWARE™ Products

 **Collaborate
(CSAP)**

Bidirectional alert and advisory sharing platform purpose-built to expedite and enhance security collaboration.

[Request a Demo](#)

Collaborative Information Sharing Platforms

The screenshot displays the MISP Open Source Threat Sharing website. The browser address bar shows www.misp-project.org. The navigation menu includes [HOME](#), [FEATURES](#), [DATA MODELS](#), [DOCUMENTATION](#), and [COMMUNITIES](#). A secondary menu contains [DOWNLOAD](#), [EVENTS](#), [NEWS](#), and [CONTACT](#).

The main content area features the text: **OPEN SOURCE THREAT INTELLIGENCE AND SHARING PLATFORM**. Below this, it lists capabilities: **SHARE. STORE. CORRELATE. ANALYSE. TARGETED ATTACKS. FINANCIAL FRAUD. COUNTER-TERRORISM.**

A central diagram illustrates the MISP architecture. It shows **UI USERS** and **API USERS** interacting with the **MISP Threat Sharing** core. The core is connected to a **Database** and an **API**. A list of supported formats and integrations is provided:

- MISP XML and JSON
- OpenIOC
- STIX XML and JSON (export)
- Suricata export
- Snort export
- CSV export
- GFI import

Best Practices for Incident Response and Information Sharing

- **Engaging in Information Sharing Programs**
 - Information Sharing and Analysis Centers (ISACs)
- **Embracing Regular Reporting and Analytics**

**The Big Three: NERC CIP,
IEC 62443, and NIST SP 800-82**

NERC CIP

- **North American Electric Reliability Corporation Critical Infrastructure Protection**
 - Mandatory cybersecurity standards for electric power in North America
 - The United States, several provinces in Canada and one state in Mexico
- **Cyber Critical Assets (CCAs)**
- **Security Controls**
- **Incident Reporting and Response**
- **Compliance and Auditing**

IEC 62443

- **International Electrotechnical Commission 62443**
- International standards for **Industrial Automation and Control Systems (IACS)**
- **Security Levels**
- **Risk Assessment and Management**
- **Security Policies and Procedures**
- **Secure Development Lifecycle**

NIST SP 800-82

- **National Institute of Standards and Technology Special Publication 800-82**
- US Gov't Standard to secure **Industrial Control Systems (ICS)**
- **ICS Security Program Development**
- **Security Controls**
- **Network Segmentation**
- **Secure Configuration and Patch Management**
- **Incident Response**

Kahoot!

Ch 7