International Centre for
Chemical Safety and Security

INDUSTRIAL CYBERSECURITY TRAINING SYLLABUS

ICCSS cybersecurity trainings discuss both the attack and defence methodologies. We believe that teaching appropriate procedures through counterexamples, of how **not** following them leads to increased risk for the organization, is very effective. Through describing real world attack scenarios but also trough explanation of potential defence solutions (both open source and commercial) our trainees have a full picture of how to **successfully secure the organization**.

Thus our trainings are an enabler for an **organization to perform a self-audit**. As this could be long and tedious process, we assist our clients in building a successful team that will deliver appropriate results. These people usually include but are not limited to: Risk management experts, OT managers, IT network managers, IT maintenance, Finance Directors, Chief Security Directors, Physical Security managers. After finishing of the self-audit, companies are aware of the gaps in their system, have much better understanding of the vulnerabilities and can clearly define their needs in relation to cybersecurity.

Our approach follows from the training material made available from **Department of Homeland Security** but is extended by norms and best practices from other organizations. These include**: NIST-SP 800-82, NERC 5, IEC 62443.** We enrich those methodologies by relating them to real world examples and showcasing various tools via online demonstrations. In our approach we extend the cybersecurity topics with issues relating to physical security, business continuity, risk management and emergency response. This allows us to clearly relate to the OT working environment and the **needs of the Operations Technology Department** to which our cybersecurity program is dedicated.

Training program

Introduction to ICS security

- Discussion of ICS operations requirements and difference with IT cybersecurity
- Description of threats: APT, Cyber Terrorism, Cyberwar, information stealing, modification of process, loss of quality. Examples of where and how it happened)
- Myth of the airgap. Questions of physical security

Discussion of various cybersecurity methodologies available. Differences and similarities between the above approaches

- NIST Cybersecurity framework (emphasis on manufacturing)
- DHS CSET tool and categories available.
- Defense in Depth methodology - introduction
- NIST-800-82
- NERC 5 CIP
- CFATS
- IEC 62443 standard
- IT related methodologies brief description: COBIT, CCS, ISO 27000

Discussion of ICS equipment:

- General discussion of process control
- Distributed Control Systems - architecture
- PLC (programmable logic controller)
- HMI (Human Machine Interface)
- EWS (Engineering Work Station)
- SIS (Safety Instrumented Systems)
- Historian Server

- Configuration Servers
- Application servers
- Distributed control system (controllers, IO, basic physics of PID, altering the set points)

Discussions of ICS networks

- Industrial Network overview
- Discussion of OSI Layers 1-7
- Discussion of TCP/IP protocol and Ethernet and their use in industrial networks
- Types of network components: firewalls, IDS, IPS, switches, routers, Remote Access Servers, Unidirectional devices
- Various network structures: SCADA/PLC/RTU vs. Distributed control systems
- Discussion of common protocols between SCADA/RTU/PLC and Distributed Control Systems
- Network topologies (Bus, mesh, star, branch, ring, dual-homing) Discussion of field equipment: I/O systems, protocols
- Considerations - security and latency depending on network design

Discussion of ICS protocols:

- Production level: OPC, Modbus PLC and Field level field protocols (
    - Profibus-DP
    - Foundation Fieldbus
    - Wireless HART
- Analysis of vulnerabilities (authentication, man in the middle attack) Encryption possibilities
- Wide Area Network security issues. Discussion of protocols
    - DNP
    - ICCP
- Wireless solutions
    - Mesh Protocols, Wifi
    - APN and 3G technologies – modems
    - Bluetooth

Assessment of risk

- Vulnerability detection
- Theoretical vs. physical tests
- Penetration testing in ICS environment
- Risk calculation
- Risk Governance

Hacking industrial control systems

- Attack methodologies (planning, social engineering attacks)
- Finding Vulnerabilities within the components in the network (PLC, HMI).
- Tools for scanning industrial networks (Kali/Moki Linux, NMAP)
- Various attack techniques (SQL injection, fuzzing, cross-scripting)
- Attacking of field equipment through firmware update
- Man in the middle attacks. Exploiting protocols vulnerabilities

Attack case study - step by step going through potential weaknesses in approach.

- General Methodology of penetration testers.
- Discussion of publically available (usually open source) tools
- Lessons learned from: Stuxnet, Havex, Petya

Zone segmentation.

Identifying zones and conduits

- Difference between the Purdue model and zone segmentation.
- Definition of security levels
- Segmentation vs. segregation - depending on OSI Layers (routers vs. switches)
- Discussion of how segmenting the network helps the attacks from pivoting

Firewalls and boundary protection

- various firewall rules
- IDS equipment
- uni-directional diodes as separation of zones

Network monitoring tools

- Usefulness and easiness to monitor (predictability, no encryption, no NAT considerations,)
- Packet inspection (pcap files).
- Inclusion of Modbus protocols
- Description of deep packet inspection

Patching

- Vulnerability management
- Scheduling appropriate patching procedure - avoiding the pitfalls
- Discussing the Havex case study in relation to patching
- Knowledge of vulnerabilities: Using the resources: ICS-CERT - and others

Various IT tools applicable to ICS environment:

- Discussion of applicability of various IT controls to OT. Defining in which zones they could be present
- Application whitelisting
- Anomaly detection
- Tools for logging
- SIEM solutions (correlating OT to IT incidents)
- Antivirus / Host protection systems
- Intrusion detection systems Encryption of networks – discussion

Incident response

- Preparing a forensics analysis
- Tools for memory analysis
- Establishing chain of command in case of an incident response
- Incident handling
- Tabletop exercise – reacting to an incident

Building cybersecurity teams and management issues within an organization

- Building a cybersecurity culture.
- Selecting appropriate personnel for ICS cybersecurity
- Preparing required documentation for self-audit
- Management issues
- Dealing with insider threats

Appendix 1. Categories of questions for self-audit for network equipment (based on the NIST SP 800-82 and CSET tool)

- Access Control
  - Password
  - User Authentication
- Account Management
  - Management Practices
  - Active Directory
  - Audit and Accountability
  - Logging
- Communication Protection
  - Boundary Protection
  - Securing the Router
  - Configuration Management
  - Encryption
  - Firewall
  - IDS/ IPS
- Info Protection
  - Securing Content
  - Management Practices
- Monitoring and Malware
  - Securing the System
  - System Protection
- Physical Security
  - Physical Access
  - Policies & Procedures General
- Remote Access Control
  - Portable/Mobile/Wireless
- System Integrity
  - Securing the Component
  - Policies & Procedures General

Appendix 2. Categories of questions for self-audit for general cybersecurity procedures (based on the NIST SP 800-82 and CSET tool)

- Access Control
  - Access Agreements
  - Access Enforcement
  - Actions without ID/Auth
  - Authentication Implementation
  - Authentication Management
  - Device Id & Authentication
  - Least Privilege
  - Logon Handling
  - Passwords
  - Session Lock
  - System Use Notification
- Account Management
  - Account Management
  - Authenticator Management
  - Identifier Management
  - Separation of Duties
- Audit and Accountability
  - Audit Failure Response
  - Audit Generation
  - Audit Monitor/ Analysis
  - Auditable Events List
  - Protection of Audit Information
  - Time stamps
- Communication
  - Authorative DNS and name/address resolution
  - Boundary Protection
  - Collaboration
  - Collaborative computing
  - Communication Confidentiality
  - Cryptographic keys
  - Data Flow Controls
  - Encryption
  - Information Flow Enforcement
  - Process Isolation
  - Session Authenticity
  - Shared resources

    - VoIP
- Configuration Management
    - Baseline Configuration
    - Change Control
    - Component Inventory
    - Config Change Control
    - Configuration Assets
    - Configuration Settings
    - Factory Settings
- Continuity
    - Alternate Storage Site
    - Alternate Work Site
    - Alternative Command and Control Methods
    - Alternative Control Center
    - Contingency Plan
    - Continuity of Operations
    - Continuity of Operations Plan Testing
    - Continuity of Operations Plan Update
    - Disaster Recovery
    - Info System Recovery
    - System Backup
- Environmental Security
    - Emergency Power
    - Fire Protection
    - Power Equip/Cabling
    - Sys Asset Location
    - Temperature and Humidity Controls
    - Water Damage Protection
- Incident Response
    - Incident handling
    - Incident Response General
    - Incident Response Support
    - Insider Threat Program
- Information and Document Management
    - Documentation
    - Software Documentation Management
- Information Protection
    - General Information Protection
    - Media Access
    - Media Downgrading
    - Media Marking
    - Media Sanitization

    - Media storage
    - Media transport
    - Media use
    - Publicly Accessible
- Maintenance
    - General Maintenance
    - Maintenance Personnel
    - Maintenance Tools
    - Remote Maintenance
- Monitoring and Malware
    - Denial of Service
    - Malicious Code Protection
    - Monitoring and Evaluation
    - Monitoring Tools
    - Spam protect
    - Vulnerability Scanning
- Organizational
    - Authorization Process
    - Business Process Definition
    - Certification & Accreditation
    - Contacts with Security Groups and Associations
    - Information Security Workforce
    - Resource Allocation
    - Roles & Responsibilities
    - Security Policy
    - System Security Plan
- Personnel
    - Personnel Accountability
    - Personnel Screening
    - Personnel Termination
    - Personnel Transfer
- Physical Security
    - Access Authorizations
    - Device Access Controls
    - Monitor Physical Access
    - Physical Access Control
    - System Monitoring
    - Transmission Medium
    - Visitor Record
- Plans Configuration Management Plan
    - Incident response Plan
    - Plan

    - Plan of Action
    - Risk Management
    - Security Plan
- Policies and Procedures General
    - Baseline Practices
    - Document Classification
    - General Practices
    - Maintenance Policies
    - Management Policies
    - Third Party Security
- Portable/Mobile/Wireless
    - Mobile Code
    - Portable Media
    - Remote Access
    - Wireless
    - Procedures
- Remote Access Control
    - External ICS
    - Remote Access Control
    - Remote Session Termination
- Risk Management and Assessment
    - Continuous monitoring
    - Risk Management Strategy
    - Security Assessments
    - Security Categorization
    - System Connections
- Safety Instrumented System
    - Safety System
- System and Services Acquisition
    - Acquisitions
    - Developer Configuration Management
    - Developer Security Training
    - Engineering Principles
    - External System Services
- System Integrity
    - Error Handling
    - Flaw Remediation
    - General System Integrity
    - Memory Protection
    - Security Alerts
    - Software Information Integrity

- System protection
    - Application Partitioning
    - Confidentiality at Rest
    - Cryptographic considerations
    - Failure State
    - General System Protection
    - Least Functionality
    - System Component Identification
- Training
    - Incident Response Training
    - Security Awareness
    - Security Training
    - Training Records