CSX Practitioner (CSXP) Prep Boot Camp

Course Details

Course Outline

1. **Identify**
    - Hardware Software Identification and Documentation
    - Lab: Preliminary Scanning
    - Network Discovery Tools
    - Lab: Additional Scanning Options
    - Sensitive Information Discovery
    - Lab: Sensitive Information Identification
    - Vulnerability Assessment Process
    - Lab: Vulnerability Scanner Set-up and Configuration
    - Patch Upgrade Configure Vulnerability Scanners
    - Lab: Vulnerability Scanner Set-up and Configuration, Part 2
2. **Protect**
    - Specific Cyber Controls
    - Lab: System Hardening
    - Collecting Event Data
    - Lab: Firewall Setup and Configuration
    - Verifying the Effectiveness of Controls
    - Lab: Microsoft Baseline Security Analyzer
    - Monitoring Controls
    - Lab: IDS Setup
    - Updating Cyber Security Controls
    - Lab: Personal Security Products
    - Patch Management
    - Lab: Linux Users and Groups
    - Verifying Identities and Credentials
    - Cyber Security Procedures Standards
3. **Detect**
    - Analyze Network Traffic Using Monitors
    - Lab: Using Snort and Wireshark to Analyze Traffic
    - Detect Malicious Activity AntiVirus
    - Lab: Detect the Introduction and Execution of Malicious Activity

- Assess Available Event Information
- Lab: Analyze and Classify Malware
- Baselines for Anomaly Detection
- Lab: Windows Event Log Manipulation via Windows Event Viewer
- Initial Attack Analysis
- Lab: Host Data Integrity Baselining
- Incident Escalation Reporting
- Lab: Performing Network Packet Analysis
- Change Implementation Escalation

4. **Respond**
    - Defined Response Plan Execution
    - Lab: Incident Detection and Identification
    - Network Isolation
    - Lab: Remove Trojan
    - Disable User Accounts
    - Lab: Block Incoming Traffic on Known Port
    - Blocking Traffic
    - Lab: Implement Single System Changes in Firewall
    - Documentation
    - Lab: Conduct Supplemental Monitoring
    - Incident Report
    - Lab: Create Custom Snort Rules
5. **Recover**
    - Industry Best Practices
    - Lab: Comprehensive Lab Response
    - Disaster Recovery and BC Plans
    - Lab: Patches and Updates
    - Cyber System Restoration
    - Lab: Data Backup and Recovery
    - Data Backup and Restoration Key Concepts
    - Lab: Recovering Data and Data Integrity Checks
    - Actualizing Data Backups and Recovery
    - Post Incident Service Restoration
    - Implementing Patches and Updates
    - Ensuring Data Integrity
    - Post-Incident Review