# CSX Practitioner: Course 2
## Detection

### DAY 1
**LESSON** | **LAB**
---|---
Analyzing Network Traffic Using Monitors | 
Monitoring Network Traffic | 
Monitoring Schedule Using Snort and Wireshark to Analyze Traffic | 
Searching for Indicators of Compromise | 
Monitoring for False Positives Monitoring Network Traffic

### DAY 2
**LESSON** | **LAB**
---|---
Escalate Potential Compromises | 
Network Packet Analysis Searching for Indicators of Compromise | 
Malicious Activity and Anti-Virus | 
Malicious Code and Activity Types Monitoring for False Positives | 
Remediation Steps

### DAY 3
**LESSON** | **LAB**
---|---
Assessing Available Event Information | 
Performing Initial Analysis | 
Identifying Potential Collection Sources | 
Deploy the Data Collection Utility | 
Using Event Correlation Analyze and Classify Malware

### DAY 4
**LESSON** | **LAB**
---|---
Using Established Baselines to Detect Anomalies | 
Documenting Yours Steps Event Log Collection | 
Initial Attack Analysis | 
Determine the Initial Scope Windows Event Log Manipulation | 
Identify if High-Risk Systems Were Affected Host Integrity Baselining

### DAY 5
**LESSON** | **LAB**
---|---
Ongoing Monitoring Performing Network Packet Analysis | 
Build an Event Timeline Automated In-Depth Packet Decoding | 
Documenting Steps Taken High Risk Effects | 
Incident Escalation Reporting Comprehensive Assessment | 
Change Implementation/ Escalation

### ASSOCIATED TOPICS
- Traffic Flow Analysis
- IR Resources
- Attack Types
- Attack Methods
- Network Access Control
- Virus Types
- Worm Variants
- Incident Identification Methodologies
- IP Reputation Databases
- Port Scanning
- Host Analysis
- Network Traffic Behavior
- Malware Functionality
- Spyware
- Trojans
- Rootkits
- Viruses
- Backdoors
- NIST Roles
- ISO Designations
- CEERT Designation
- CSIRT Roles
CSX Training Courses are the perfect way to build and hone critical skills in cyber security, and prepare you for the next level in your career.

The **CSX Practitioner Series** offers three unique, week-long courses conducted in an adaptive, performance-based cyber laboratory environment. Students will have hands-on instruction and practice in applying basic concepts and industry-leading methods and in utilizing a large array of open source tools within real-world scenarios.

Each course utilizes PerformaScore®, a learning and development tool that measures a professional’s ability to perform specific cyber security job tasks and enables the instructor to provide the student with immediate feedback.

The courses help students build skills necessary to be successful in a variety of cyber security-related positions, and to earn the related CSX Practitioner certification.

---

**CSX Practitioner: Course 2**

**Detection**

**Course Overview**
The second course in the CSX Practitioner series goes deeper into skills focused in the Detect domain. Students will learn the basic concepts, methods and tools used to leverage cyber security controls in order to identify system events and non-event level incidents. By completing multiple lab-reinforced modules, students will gain the skills necessary to detect potential network events and incidents.

Students will gain the following skills in the Detect domain:
- Analyzing and monitoring network output
- Detecting malware
- Detecting incidents
- Notifying proper channels
- Analyzing attacks
- Escalating incidents
- Performing change monitoring

**Course Learning Objectives**
Provide students with an environment to discuss and practice methods implemented by cyber security professionals in the Detect domain. Ensure students develop into complimentary team members for enterprises who are workforce ready.

**Training Notes**
Provided during the training session and shall be retained by the students.

**Recommended Participants**
Individuals in the field of cyber security who are interested in learning hands-on technical skills.

**Course Structure**
- Classes consist of at least 50% hands-on lab exercises.
- Lessons and lectures are comprised of up-to-date coursework and demonstrations.

---

**Classroom-Based Instruction Topics**
- IDS Traffic Analysis vs Packet Analysis
- Behavioral Designation
- Compromise Identifiers/False Positive Differentiation
- Compromise Escalation
- Malicious Code Differentiation
- Antivirus Deployments
- Antivirus Monitoring/Malicious Code Identification
- Malicious Code Remediation
- Incident Identification
- Initial Incident Identifiers
- Incident Event Collection
- Identifying Established Baselines
- Event Characteristic Capture
- Attack Intent Assessment
- System Exposure Analysis/Change Identification
- Attack Timeline Construction
- Attack Documentation
- Event Escalation
- Support Role Designation/Action
- Incident Response Report Generation

**Lab Topics**
- Networking Traffic and Log Comparison
- Log Qualification
- Event Comparison
- Threat Detection and Identification
- Containment/Eradication
- Traffic Analysis Threat Detection and Identification
- Threat/Incident Component Evaluation
- Traffic and Log Assessment and Analysis
- Baselines
- Packet Character Observation
- Compromise Indicators
- Traffic Analysis