Understanding Cisco Cybersecurity Fundamentals (SECFND)

COURSE OVERVIEW:

The Understanding Cisco Cybersecurity Fundamentals (SECFND) v1.0 course will provide you with an understanding of network infrastructure devices, operations and vulnerabilities of the TCP/IP protocol suite, basic information security concepts, common network application operations and attacks, the Windows and Linux operating systems, and the types of data that are used to investigate security incidents.

After completing this course, you will have basic knowledge that is required to perform the job role of an entry-level cybersecurity analyst in a threat-centric security operations center.

WHO WILL BENEFIT FROM THIS COURSE?

This course is intended for students who have general knowledge about:

- Security Operations Center – Security Analyst
- Computer/Network Defense Analysts
- Computer Network Defense Infrastructure Support Personnel
- Future Incident Responders and Security Operations Center (SOC) personnel.
- Students beginning a career, entering the cybersecurity field.
- Cisco Channel Partners

PREREQUISITES:

- Attendance in CCNAX, OR ICND1 and ICND2, OR have approximate level of knowledge from work experience
- Interest in learning more about Cyber Security

COURSE OBJECTIVES:

After completion of this course, students will be able to...

- Describe, compare and identify various network concepts
- Fundamentals of TCP/IP
- Describe and compare fundamental security concepts
- Describe network applications and the security challenges
- Understand basic cryptography principles.
- Understand endpoint attacks, including interpreting log data to identify events in Windows and Linux
- Develop knowledge in security monitoring, including identifying sources and types of data and events
- Know various attack methods, security weaknesses, evasion methods, and remote versus local exploits

COURSE OUTLINE:

Module 1: TCP/IP and Cryptography Concepts

Lesson 1: Understanding the TCP/IP Protocol Suite

- OSI Model
- TCP/IP Model
- Introduction to the Internet Protocol
- IP Addressing
- IP Address Classes
- Reserved IP Addresses
- Public and Private IP Addresses
- IPv6 Addresses
- Introduction to the Transmission Control Protocol
- TCP Three-Way Handshake
- Introduction to the User Datagram Protocol
- TCP and UDP Ports
- Address Resolution Protocol
- Host-to-Host Packet Delivery Using TCP
- Dynamic Host Configuration Protocol
- Domain Name System
- Internet Control Message Protocol
- Packet Capture Using tcpdump
- Wireshark

Lesson 2: Understanding the Network Infrastructure

- Analyzing DHCP Operations
- IP Subnetting
- Hubs, Bridges, and Layer 2 Switches
- VLANs and Trunks
- Spanning Tree Protocols
- Standalone (Autonomous) and Lightweight Access Points
- Routers
- Routing Protocols
- Multilayer Switches
- NAT Fundamentals
- Packet Filtering with ACLs
- ACLs with the Established Option

Lesson 3: Understanding Common TCP/IP Attacks

- Legacy TCP/IP Vulnerabilities
- IP Vulnerabilities
- ICMP Vulnerabilities
- TCP Vulnerabilities
- UDP Vulnerabilities
- Attack Surface and Attack Vectors
- Reconnaissance Attacks
- Access Attacks
- Man-in-the-Middle (MITM) Attacks
- Denial of Service and Distributed Denial of Service
- Reflection and Amplification Attacks
- Spoofing Attacks
- DHCP Attacks

Lesson 4: Understanding Basic Cryptography Concepts

- Impact of Cryptography on Security Investigations
- Cryptography Overview
- Hash Algorithms
- Encryption Overview
- Cryptanalysis
- Symmetric Encryption Algorithms
- Asymmetric Encryption Algorithms
- Diffie-Hellman Key Agreement
- Use Case: SSH
- Digital Signatures
- PKI Overview
- PKI Operations
- Use Case: SSL/TLS
- Cipher Suite
- Key Management
- NSA Suite B

Module 2: Network Applications and Endpoint Security

Lesson 1: Describing Information Security Concepts

- Information Security Confidentiality, Integrity, and Availability
- Personally Identifiable Information
- Risk
- Vulnerability Assessment
- CVSS v3.0

- Access Control Models
- Regulatory Compliance
- Information Security Management
- Security Operations Center

Lesson 2: Understanding Network Applications

- DNS Operations
- Recursive DNS Query
- Dynamic DNS
- HTTP Operations
- HTTPS Operations
- Web Scripting
- SQL Operations
- SMTP Operations

Lesson 3: Understanding Common Network Application Attacks

- Password Attacks
- Pass-the-Hash Attacks
- DNS-Based Attacks
- DNS Tunneling
- Web-Based Attacks
- Malicious iFrames
- HTTP 302 Cushioning
- Domain Shadowing
- Command Injections
- SQL Injections
- Cross-Site Scripting and Request Forgery
- Email-Based Attacks

Lesson 4: Understanding Windows Operating System Basics

- Windows Operating System History
- Windows Operating System Architecture
- Windows Processes, Threads, and Handles
- Windows Virtual Memory Address Space
- Windows Services
- Windows File System Overview
- Windows File System Structure
- Windows Domains and Local User Accounts
- Windows Graphical User Interface
- Run as Administrator
- Windows Command Line Interface

- Windows PowerShell
- Windows net Command
- Controlling Startup Services and Executing System Shutdown
- Controlling Services and Processes
- Monitoring System Resources
- Windows Boot Process
- Windows Networking
- Windows netstat Command
- Accessing Network Resources with Windows
- Windows Registry
- Windows Event Logs
- Windows Management Instrumentation
- Common Windows Server Functions
- Common Third-Party Tools

Lesson 5: Understanding Linux Operating System Basics

- History and Benefits of Linux
- Linux Architecture
- Linux File System Overview
- Basic File System Navigation and Management Commands
- File Properties and Permissions
- Editing File Properties
- Root and Sudo
- Disks and File Systems
- System Initialization
- Emergency/Alternate Startup Options
- Shutting Down the System
- System Processes
- Interacting with Linux
- Linux Command Shell Concepts
- Piping Command Output
- Other Useful Command Line Tools
- Overview of Secure Shell Protoco
- Networking
- Managing Services in SysV Environments
- Viewing Running Network Services
- Name Resolution: DNS
- Testing Name Resolution
- Viewing Network Traffic
- System Logs
- Configuring Remote syslog

- Running Software on Linux
- Executables vs. Interpreters
- Using Package Managers to Install Software in Linux
- System Applications
- Lightweight Directory Access Protocol

Lesson 6: Understanding Common Endpoint Attacks

- Classify Attacks, Exploits, and Vulnerabilities
- Buffer Overflow
- Malware
- Reconnaissance
- Gaining Access and Control
- Gaining Access via Social Engineering
- Social Engineering Example: Phishing
- Gaining Access Via Web-Based Attacks
- Exploit Kits
- Rootkits
- Privilege Escalation
- Pivoting
- Post-Exploitation Tools Examples
- Exploit Kit Example: Angler

Lesson 7: Understanding Network Security Technologies

- Defense-in-Depth Strategy
- Defend Across the Attack Continuum
- Authentication, Authorization, and Accounting
- Identity and Access Management
- Stateful Firewall
- Network Taps
- Switched Port Analyzer
- Remote Switched Port Analyzer
- Intrusion Prevention System
- IPS Evasion Techniques
- Snort Rules
- VPNs
- Email Content Security
- Web Content Security
- DNS Security
- Network-Based Malware Protection
- Next Generation Firewall
- Security Intelligence

- Threat Analytic Systems
- Network Security Device Form Factors
- Security Onion Overview
- Security Tools Reference

Lesson 8: Understanding Endpoint Security Technologies

- Host-Based Personal Firewall
- Host-Based Anti-Virus
- Host-Based Intrusion Prevention System
- Application Whitelists and Blacklists
- Host-Based Malware Protection
- Sandboxing
- File Integrity Checking

Module 3: Security Monitoring and Analysis

Lesson 1: Describing Security Data Collection

- Network Security Monitoring Placement
- Network Security Monitoring Data Types
- Intrusion Prevention System Alerts
- True/False, Positive/Negative IPS Alerts
- IPS Alerts Analysis Process
- Firewall Log
- DNS Log
- Web Proxy Log
- Email Proxy Log
- AAA Server Log
- Next Generation Firewall Log
- Applications Log
- Packet Captures
- NetFlow
- Network Behavior Anomaly Detection
- Data Loss Detection Using Netflow Example
- Security Information and Event Management Systems

Lesson 2: Describing Security Event Analysis

- Cyber Kill Chain
- Advanced Persistent Threats
- Diamond Model for Intrusion Analysis
- Cybersecurity Threat Models Summary
- SOC Runbook Automation
- Malware Reverse Engineering
- Chain of Custody

LABS

- Guided Lab 1: Explore the TCP/IP Protocol Suite
- Guided Lab 2: Explore the Network Infrastructure
- Guided Lab 3: Explore TCP/IP Attacks
- Guided Lab 4: Explore Cryptographic Technologies
- Guided Lab 5: Explore Network Applications
- Guided Lab 6: Explore Network Application Attacks
- Guided Lab 7: Explore the Windows Operating System
- Guided Lab 8: Explore the Linux Operating System
- Guided Lab 9: Explore Endpoint Attacks
- Guided Lab 10: Explore Network Security Technologies
- Guided Lab 11: Explore Endpoint Security
- Guided Lab 12: Explore Security Data for Analysis

SUNSET LEARNING INSTITUTE (SLI) DIFFERENTIATORS:

Sunset Learning Institute (SLI) has been an innovative leader in developing and delivering authorized technical training since 1996. Our goal is to help our customers optimize their cloud technology investments by providing convenient, high quality technical training that our customers can rely on. We empower students to master their desired technologies for their unique environments.

What sets SLI apart is not only our immense selection of trainings options, but our convenient and consistent delivery system. No matter how complex your environment is or where you are located, SLI is sure to have a training solution that you can count on!

Premiere World Class Instruction Team

- All SLI instructors have a four-year technical degree, instructor level certifications and field consulting work experience.
- Sunset Learning has won numerous Instructor Excellence and Instructor Quality Distinction awards since 2012

Enhanced Learning Experience

- The goal of our instructors during class is ensure students understand the material, guide them through our labs and encourage questions and interactive discussions.

Convenient and Reliable Training Experience

- You have the option to attend classes at any of our established training facilities or from the convenience of your home or office with the use of our HD-ILT network (High Definition Instructor Led Training)
- All Sunset Learning Institute classes are guaranteed to run – you can count on us to deliver the training you need when you need it!

Outstanding Customer Service

- Dedicated account manager to suggest the optimal learning path for you and your team
- Enthusiastic Student Services team available to answer any questions and ensure a quality training experience