Training: OffSec

OffSec SOC-200 Foundational Security Operations and Defensive Analysis

OffSec Learning Partner

TRAINING GOALS:

Learn the foundations of cybersecurity defense with Foundational Security Operations and Defensive Analysis (SOC-200), a course designed for job roles such as Security Operations Center (SOC) Analysts and Threat Hunters. Learners gain hands-on experience with a SIEM, identifying and assessing a variety of live, end-to-end attacks against a number of different network architectures. Learners who complete the course and pass the exam earn the OffSec Defense Analyst (OSDA) certification, demonstrating their ability to detect and assess security incidents.

Benefits

Learners will learn how to:

- Recognize common methodologies for end-to-end attack chains (MITRE ATT&CK® framework)
- Conduct guided audits of compromised systems across multiple operating systems
- Use a SIEM to identify and assess an attack as it unfolds live

Who is this course for?

- Job roles like: Security Operations Center (SOC) Tier 1, Tier 2 and Tier 3 Analysts, Jr. roles in Threat Hunting and Threat Intelligence Analysts, Jr. roles in Digital Forensics and Incident Response (DFIR)
- Anyone interested in detection and security operations, and/or committed to the defense or security of enterprise networks

Each participant in an authorized OffSec SOC-200 training held in Compendium CE will receive a free OSDA exam voucher.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

CONSPECT:

- Attacker Methodology
  - The Network as a Whole
    - Gain a basic understanding of an enterprise network's DMZ
    - Learn about deployment environments
    - Understand the difference between core and edge network devices
    - Study virtual private networks and remote sites
  - The Lockheed-Martin Cyber Kill-Chain
    - Learn the parts of the Lockheed-Martin Cyber Kill-Chain
    - Apply the Kill-Chain to malware that performed cryptomining
    - Apply the Kill-Chain to three iterations of ransomware
  - MITRE ATT&CK Framework
    - Learn the classifications of the MITRE ATT&CK Framework
    - Review a case study of OilRig campaigns with MITRE ATT&CK principles
    - Review a case study of APT3 campaigns with MITRE ATT&CK principles
    - Review a case study of APT28 campaigns with MITRE ATT&CK principles
- Windows Endpoint Introduction
  - Windows Processes
    - Gain a basic understanding of programs running within Windows
    - Learn about Windows Services and their relationship with processes
    - Review the common states of Windows Services
  - Windows Registry
    - Review the configuration structure of the Windows Registry
    - Learn about the key-value pair relationship within the Windows Registry
    - Understand the value types and formats for Windows Registry keys
  - Command Prompt, VBScript, and PowerShell
    - Review the non-graphical means of interacting with Windows
    - Build batch scripts used for the command prompt to run local commands
    - Write a Visual Basic Script for collecting operating system
    - Build custom PowerShell functions
  - Programming on Windows
    - Review the Component Object Model in Windows
    - Learn about the development of the .NET Framework and .NET Core
  - Windows Event Log
    - Gain a basic understanding of Windows Event logs and sources

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Review several Windows Event logs using the Windows Event Viewer
- Use PowerShell to query Windows Event logs

- Empowering the Logs
  - Gain a basic understanding of System Monitor Sysmon)
  - Review Sysmon events using the Windows Event Viewer
  - Review Sysmon events using PowerShell
  - Use PowerShell Core in Kali Linux to query event logs remotely

- Windows Server Side Attacks
  - Credential Abuse
    - Learn about the Windows Security Account Manager
    - Learn about Windows Authentication
    - Understand the concept of suspicious login activity
    - Evaluate the behavior of brute-force login activity
  - Web Application Attacks
    - Learn about the configuration of Internet Information Services IIS in Windows
    - Evaluate logging artifacts of local file inclusion for attacking web servers
    - Evaluate logging artifacts of command injection and file upload for attacking web servers
  - Binary Exploitation
    - Learn about binary attacks through buffer overflows, and the artifacts they create
    - Study the use of Windows Defender Exploit Guard and how it protects against binary exploitation
    - Evaluate logging artifacts generated by the Windows Defender Exploit Guard

- Windows Client Side Attacks
  - Attacking Microsoft Office
    - Review social engineering and spearphishing techniques
    - Evaluate the use of Microsoft Office products to deploy phishing attacks
    - Review logging artifacts generated from a phishing attack
  - Monitoring Windows PowerShell
    - Gain a basic understanding of extended PowerShell logging capabilities
    - Understand the use of PowerShell module logging
    - Understand the use of PowerShell script block logging
    - Understand the use of PowerShell transcription
    - Review PowerShell logging artifacts generated from a phishing attack
    - Learn about PowerShell obfuscation and deobfuscation

- Windows Privilege Escalation
  - Privilege Escalation Introduction

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Gain a basic understanding of Windows integrity levels and enumeration
- Learn about Windows' User Account Control UAC
- Evaluate a UAC bypass technique and the logging artifacts it creates

- Escalations to SYSTEM
  - Perform an elevation using UAC Bypass and review the logging artifacts created
  - Learn about service permissions for privilege escalation along with relevant logging artifacts
  - Learn about unquoted service paths for privilege escalation along with logging artifacts

- Linux Endpoint Introduction
  - Linux Applications and Daemons
    - Understand what Linux daemons are
    - Understand the Syslog Framework components
    - Understand how the syslog and the journal daemon work together
    - Understand Linux web logging
  - Automating the Defensive Analysis
    - Understand how scripting can aid log analysis
    - Understand how to scale further scripting with DevOps tools
    - Understand how to put together what we learned in a real-life hunting scenario
- Linux Server-Side Attacks
  - Credential Abuse
    - Understand suspicious logins and how to detect them in logs
    - Understand brute-force password attacks and their log footprints
  - Web Application Attacks
    - Understand command injection attacks and their log footprint and detections
    - Understand SQL injection attacks and their log footprint and detections
- Linux Privilege Escalation
  - User-side privilege escalation attack detections
    - Understand how Linux privileges works
    - Understand how to detect privilege escalation attacks on user's configuration files
  - System-side privilege escalation attack detections
    - Understand how Linux privileges works
    - Understand how to detect privilege escalation attacks on user's configuration files
- Windows Persistence
  - Persistence on Disk
    - Understand and recognize Persisting via Windows Service
    - Understand and recognize Persisting via Scheduled Tasks

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Understand and recognize Persisting by DLLSideloading/Hijacking
- Persistence in Registry
  - Understand Using Run Keys
  - Understand Using Winlogon Helper
- Network Detections
  - Intrusion Detection Systems
    - Understand theory and methodologies behind IPS and IDS
    - Understand Snort rule syntax
    - Learn how to craft basic Snort rules
  - Detecting Attacks
    - Learn how to detect known vulnerabilities with Snort rules
    - Learn how to detect novel vulnerabilities with Snort rules
  - Detecting C2 Infrastructure
    - Understand the components of a C2 framework
    - Learn how to detect a well-known C2 communication through Snort rule sets
- Antivirus Detections
  - Antivirus Basics
    - Understand an Overview of Antivirus
    - Understand Signature-Based Detection
    - Understand Heuristic and Behavioral-Based Detection
  - Antimalware Scan Interface AMSI
    - Understand the basics of AMSI
    - Understand how attackers bypass AMSI
- Active Directory Enumeration
  - Abusing Lightweight Directory Access Protocol
    - Understand LDAP
    - Interact with LDAP
    - Enumerate Active Directory with PowerView
  - Detecting Active Directory Enumeration
    - Audit Object Access
    - Perform Baseline Monitoring
    - Use Honey Tokens
- Network Evasion and Tunneling
  - Network Segmentation
    - Understand the concept of network segmentation
    - Learn the benefits of network segmentation

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

        - Understand possible methods of implementing network segmentation in an enterprise
    - Detecting Egress Busting
        - Understanding the concept of egress filtering
        - Understanding an iptables firewall setup and application of egress filtering
        - Evaluate an "egress busting" technique and the logging artifacts it creates
    - Port Forwarding and Tunneling
        - Understand the concept of tunneling and port forwarding
        - Learn how attackers use it to compromise additional machines in the network
        - Understand the possible methods and tools attackers use to tunnel into the network and how to detect them
- Windows Lateral Movement
    - Windows Authentication
        - Understanding Pass the Hash
        - Understanding Brute Forcing Domain Credentials
        - Understanding Terminal Services
    - Abusing Kerberos Tickets
        - Understanding Pass the Ticket
        - Understanding Kerberoasting
- Active Directory Persistence
    - Keeping Domain Access
        - Understanding Domain Group Memberships
        - Understanding Domain User Modifications
        - Understanding Golden Tickets
- SIEM Part One: Intro to ELK
    - Log Management Introduction
        - Understand SIEM Concepts
        - Learn about the ELK Stack
        - Use ELK Integrations with OSQuery
    - ELK Security
        - Understand Rules and Alerts
        - Understand Timelines and Cases
- SIEM Part Two: Combining the Logs
    - Phase One: Web Server Initial Access
        - Detect enumeration and command Injection
        - Implement Phase One detection rules
    - Phase Two: Lateral Movement to Application Server

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Discover brute forcing and authentication
- Create Phase Two detection rules

- Phase Three: Persistence and Privilege Escalation on Application Server
  - Understand persistence and privilege escalation
  - Build Phase Three detection rules
- Phase Four: Perform Actions on the Domain Controller
  - Identify dumping the AD database
  - Create Phase Four detection rules

REQUIREMENTS:

All learners are required to have completed or have the equivalent knowledge corresponding to SOC-100 Security Operations Essentials.

New to web application assessments? Set yourself up for success by participating in the OffSec Security Fundamentals course (includes SOC-100). Adopt basic cybersecurity-adjacent concepts, cultivate the mindset necessary for a successful cybersecurity career, and provide the prerequisites for OffSec's advanced courses

Difficulty level

CERTIFICATE:

The participants will obtain certificates signed by Compendium CE (course completion).

The SOC-200 course and online lab prepares you for the OSDA OffSec Defense Analyst certification. Learn more about the OSDA exam https://help.offsec.com/hc/en-us/articles/10170036616084-OSDA-Exam-FAQ

Each participant in an authorized OffSec SOC-200 training held in Compendium CE will receive a free OSDA exam voucher.

TRAINER:

Authorized OffSec Trainer

ADDITIONAL INFORMATION:

The course includes a license "Course and Certification Exam Bundle".

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

The bundle includes 90-day access to a single course, a single exam attempt, and a certification badge awarded upon passing your exam.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007