Training: OffSec

OffSec SOC-200 Security Operations and Defensive Analysis

OffSec | Learning Partner

TRAINING GOALS:

SOC-200 (Security Operations and Defensive Analysis) is a defensive-minded course covering the foundations of defending networks and systems against cyber threats. The course will focus on developing techniques for easily parsing and analyzing logs, which can be performed at scale. This more manual approach ensures a better understanding of how logs and artifacts are generated and how they can be queried in both Windows and Linux environments. Along the way, learners will develop an understanding of network security incidents and detection techniques.

SOC-200 equips learners with a wide range of practical skills and defensive techniques, including:

- Understanding Windows endpoint security, including desktops, laptops, and other user devices, along with the threats and vulnerabilities that affect them
- Identifying social engineering and spear phishing tactics, two of the most common attack methods used by adversaries
- Using the Invoke-Obfuscation framework to automate PowerShell obfuscation and create realistic traps for simulated attackersExploring Linux endpoint concepts, including security mechanisms and common vulnerabilities, to understand how attackers target Unix-based systemsLeveraging administrative groups such as Domain Admins, Enterprise Admins, and Full Administrators to understand access control in secure domain environmentsDeploying and working with SIEM tools like ELK and Splunk to monitor logs, detect anomalies, and investigate security incidents

SOC-200 is organized into 19 modules, many with companion videos for learners who prefer a more visual presentation of the information. Each of the modules also includes hands-on activities and labs, which allow the learners to "show their work" and prove they have completed and understand what was covered. Once learners have completed the course materials, there are more than a dozen Challenge Labs to test their ability to bring all of the concepts together and actually defend their infrastructure against attackers. Once they are ready, learners can sit for the OSDA exam, where they will demonstrate their ability to identify, analyze, and respond to potential threats within a live lab environment.

Each participant in an authorized OffSec SOC-200 training held at Compendium CE

receives a Learn One" license, which includes, among other benefits, a free OSDA exam voucher.

SOC-200 is for anyone looking to take a serious step into the world of information security and learn the skills of detecting cyber attacks. The course material will describe how to detect a variety of attacks and techniques used by malicious entities against enterprises. To be successful in this course, learners should have a solid foundation in TCP/IP networking, a familiarity with Linux and Windows operating systems, and a basic understanding of cybersecurity concepts.

Objectives

After completing this course, learners will be able to:

- Understand the fundamentals of security operations
- Analyze and interpret log data for threat detection
- Implement and configure intrusion detection systems
- Develop strategies for effective incident response
- Utilize security tools for monitoring and analysis
- Understand the role of threat intelligence in security operations
- Implement defensive measures to protect enterprise environments

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

CONSPECT:

- Attack Methodology Introduction
  - Build a foundation for understanding attacker behaviors and how to anticipate their moves in penetration testing engagements
- Windows Endpoint Introduction
  - Discover common vulnerabilities in Windows endpoints and the attack vectors adversaries use to target them
- Windows Server-Side Attacks
  - Learn methods commonly used to exploit critical services and vulnerabilities on

compromised Windows servers

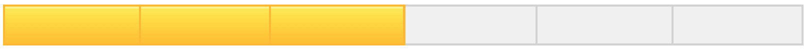
- Windows Client-Side Attacks
    - Analyze browser-based attacks, vulnerabilities in software, and social engineering techniques attackers use to compromise user-facing sides of Windows systems
- Windows Privilege Escalation
    - Exploit misconfigurations, software flaws, and zero-day vulnerabilities to increase your level of network control
- Windows Persistence
    - Explore file system persistence, registry modifications, scheduled tasks, and other methods to retain the upper hand on attackers trying to stay hidden on compromised Windows systems
- Linux Endpoint Introduction
    - Get familiar with common attack vectors used to target Linux endpoints, their security mechanisms, and potential vulnerabilities
- Linux Server-Side Attacks
    - Understand how adversaries compromise Linux servers through privilege escalation methods, service exploits, and configuration weaknesses
- Network Detections
    - Refine your evasion strategies by using firewalls, intrusion detection systems, and other tools to identify malicious activities
- Antivirus Alerts and Evasion
    - Use advanced methods for evading antivirus solutions and minimize your digital footprint with techniques like payload obfuscation and exploit customization
- Network Evasion and Tunneling
    - Avoid being detected by defensive technologies while making lateral network moves using covert communication methods and tunneling techniques
- Active Directory Enumeration
    - Uncover potential attack paths with methods and tools that gather information about Active Directory’s structure, users, groups, and permissions
- Windows Lateral Movement
    - Leverage compromised credentials, remote execution, and network pivoting to expand control in Windows environments post-exploit
- Active Directory Persistence
    - Explore hidden accounts, service manipulation, and other methods of blending into network fabrics using the same techniques as attackers
- SIEM Part One
    - Building an ELK SIEM: Get hands-on with setting up a SIEM solution using the ELK stack (Elasticsearch, Logstash, and Kibana). Learn how to install, configure, and integrate these components to start collecting and analyzing security logs
- SIEM Part Two

- Operationalizing Your SIEM: Discover how to effectively manage and use your ELK SIEM deployment. Learn to collect logs from various sources, normalize data, create insightful dashboards, and set up alerts to proactively detect a security incident

REQUIREMENTS:

All learners are required to have completed or have the equivalent knowledge corresponding to OffSec SEC-100 CyberCore - Security Essentials course.

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 OSCP+ penetration testing certification.
Learn more about the OSDA exam
https://help.offsec.com/hc/en-us/articles/4410105675412-OSDA-Exam-Guide

Each participant in an authorized OffSec SOC-200 training held at Compendium CE receives a Learn One" license, which includes, among other benefits, a free OSDA exam voucher.

TRAINER:

Authorized OffSec Trainer

ADDITIONAL INFORMATION:

The course includes a license "Learn One"

The license includes:

- One 200 or 300-level course
- 365 days of access
- 2 exam attempts
- Bonus KLCP and OSWP courses + exams
- 200+ Proving Grounds Practice labs