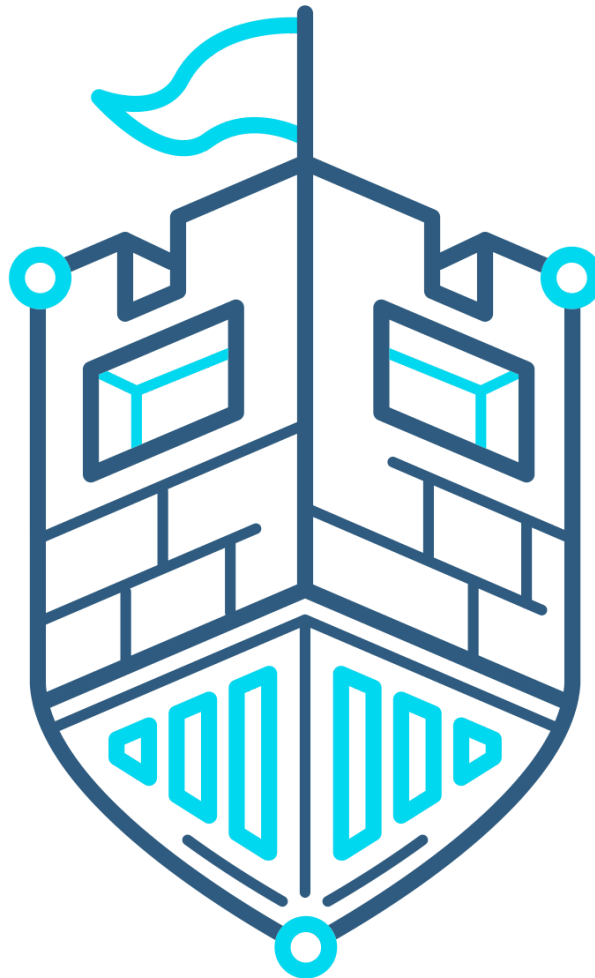


# Security Operations and Defensive Analysis

## Syllabus



1. Copyright
2. Introduction to SOC-200
  - a. Secrets of Success with SOC-200
    - Understand Offense to Improve Defense
    - A Mindset of Learning
    - Collect Data and Do Your Research
  - b. Getting Started With SOC-200
    - The Course Structure
    - Lab Overview
    - Connecting to the VPN
    - Disconnecting from the VPN
    - Conclusion
3. Attacker Methodology Introduction
  - a. The Network as a Whole
    - The DMZ
    - Deployment Environments
    - Core and Edge Network Devices
    - Virtual Private Networks and Remote Sites
  - b. The Lockheed-Martin Cyber Kill-Chain
    - The Importance of the Kill-Chain
    - Case Study 1: Monero Cryptomining
    - Case Study 2: Petya, Mischa, and GoldenEye
  - c. MITRE ATT&CK Framework
    - Tactics, Techniques, and Sub-Techniques
    - Case Study 1: OilRig
    - Case Study 2: APT3
    - Case Study 3: APT28
  - d. Wrapping Up
4. Windows Endpoint Introduction
  - a. Windows Processes
  - b. Windows Registry
  - c. Command Prompt, VBScript, and Powershell
    - Command Prompt



- Visual Basic Script (VBScript)
- PowerShell
- d. Programming on Windows
  - Component Object Model
  - .NET and .NET Core
- e. Windows Event Log
  - Introduction to Windows Events
  - PowerShell and Event Logs
- f. Empowering the Logs
  - System Monitor (Sysmon)
  - Sysmon and Event Viewer
  - Sysmon and PowerShell
  - Remote Access with PowerShell Core
- g. Wrapping Up
- 5. Windows Server Side Attacks
  - a. Credential Abuse
    - The Security Account Manager (SAM) and Windows Authentication
    - Suspicious Logins
    - Brute Force Logins
  - b. Web Application Attacks
    - Internet Information Services (IIS)
    - Local File Inclusion
    - Command Injection
    - File Upload
  - c. Binary Exploitation
    - Binary Attacks
    - Windows Defender Exploit Guard (WDEG)
  - d. Wrapping Up
- 6. Windows Client-Side Attacks
  - a. Attacking Microsoft Office
    - Social Engineering and Spearphishing
    - Installing Microsoft Office
    - Using Macros
  - b. Monitoring Windows PowerShell



- Introduction to PowerShell Logging
- PowerShell Module Logging
- PowerShell Script Block Logging
- PowerShell Transcription
- Case Study: PowerShell Logging for Phishing Attacks
- Obfuscating/Deobfuscating Commands
- c. Wrapping Up
- 7. Windows Privilege Escalation
  - a. Privilege Escalation Introduction
    - Privilege Escalation Enumeration
    - User Account Control
    - Bypassing UAC
  - b. Escalating to SYSTEM
    - Service Creation
    - Attacking Service Permissions
    - Leveraging Unquoted Service Paths
  - c. Wrapping Up
- 8. Linux Endpoint Introduction
  - a. Linux Applications and Daemons
    - Daemons
    - Logging on Linux and the Syslog Framework
    - Rsyslog Meets Journal
    - Web Daemon Logging
  - b. Automating the Defensive Analysis
    - Python for Log Analysis
    - DevOps Tools
    - Hunting for Login Attempts
  - c. Wrapping Up
- 9. Linux Server Side Attacks
  - a. Credential Abuse
    - Suspicious Logins
    - Password Brute Forcing
  - b. Web Application Attacks
    - Command Injection



SQL Injection

- c. Wrapping Up
- 10. Linux Privilege Escalation
  - a. Attacking the Users
    - Becoming a User
    - Backdooring a User
  - b. Attacking the System
    - Abusing System Programs
    - Weak Permissions
  - c. Wrapping Up
- 11. Windows Persistence - *coming soon*
- 12. Network Detections - *coming soon*
- 13. Antivirus Alerts and Evasion - *coming soon*
- 14. Network Evasion and Tunneling - *coming soon*
- 15. Active Directory Enumeration - *coming soon*
- 16. Windows Lateral Movement - *coming soon*
- 17. Active Directory Persistence - *coming soon*
- 18. SIEM pt 1: Intro to ELK - *coming soon*
- 19. SIEM pt 2: Combining the Logs - *coming soon*