FireEye Cyber Defense Summit 2017

Enterprise Incident Response (2 days)

Attacks against computer systems continue to increase in frequency and sophistication. In order to effectively defend data and intellectual property, organizations must have the ability to rapidly detect and respond to threats. This intensive three-day course is designed to teach the fundamental investigative techniques needed to respond to today's landscape of threat actors and intrusion scenarios. The class is built upon a series of hands-on labs that highlight the phases of a targeted attack, key sources of evidence, and the forensic analysis know-how required to analyze them. Students will learn how to conduct rapid triage on a system to determine if it is compromised, uncover evidence of initial attack vectors, recognize persistence mechanisms, develop indicators of compromise to further scope an incident, and much more.

Modules Included (with labs throughout the instruction)

- **The Incident Response Process** – An introduction to the targeted attack life-cycle, initial attack vectors used by different threat actors, the stages of an effective incident response process, and remediation. This module includes an in-depth study of the following topics:
    - Preparation – Reviewing the key security controls that have the most significant impact on an organization's susceptibility to compromise, as well as the availability of sources of evidence and tools required to make a network "investigation friendly".
    - Detection and Analysis – Common mechanisms to detect threats, how to prioritize and categorize leads, the need to fully-scope targeted attacks, and methods to proactively hunt for signs of compromise.
    - Remediation – Understanding the goal of remediation and when remediation is necessary, how to plan for a remediation, and how to execute a remediation event.

- **Acquiring Forensic Evidence** – A basic overview of the most common forms of endpoint forensic evidence collection and the benefits and limitations of each. Includes the following sub-sections:
    - Forensic Imaging – Understanding the different types of forensic imaging and file system access.
    - Live Response Acquisition – Objectives of live response data collection, the key sources of evidence typically acquired during this process, guidelines for forensically sound acquisition, and an introduction to Mandiant's Redline toolkit.

- **Introduction to Windows Evidence** – An overview of the key sources of evidence that can be used to investigate a compromised Windows system, including the NTFS file system, Prefetch, web browser history, event logs, the registry, memory, and more. This module focuses on the following artifacts:
    - Network Connections and Browser History – A review of forensic evidence that may capture active or historical network activity on a system.
    - Prefetch – How Prefetch files can capture evidence of previously-executed applications and additional metadata.

  - File System Analysis – Understanding the behavior of the NTFS file system and its key artifacts, including the Master File Table, timestamp behavior, alternate data streams, recovery of deleted data, and directory index attributes.
  - The Registry – An introduction to the registry, how to acquire and parse its artifacts, and the system and user-specific evidence it contains.
  - Event Logs – An introduction to the core system, security, and application event logs as well as the Application and Services logs maintained in modern versions of Windows.
  - Memory Analysis – An overview of the Windows memory architecture, including physical memory, the pagefile, and virtual memory. This module demonstrates how to analyze basic sources of evidence in memory including processes, handles, and memory sections. Finally, it walks through attack scenarios that typically require memory analysis, such as recovery of command history, process injection, and rootkit behavior.

- **Persistence** – This module includes an in-depth study of the following topics:

  - Common Persistence Mechanisms – A review of common persistence mechanisms introduced in the previous module, followed by an in-depth look at how attackers leverage Windows Services for persistence.
  - Advanced Persistence Mechanisms – More sophisticated forms of persistence including DLL search order hijacking and binary modification.
  - Alternative Remote Access Techniques – Understand alternative remote access techniques such as VPN compromise and web shells.

- **Investigating Lateral Movement** – An in-depth analysis of how attackers move from system-to-system in a compromised Windows environment, the distinctions between network logons and interactive access, and the resulting sources of evidence on disk, in logs, and in the registry. This module includes an in-depth study of the following topics:

  - Reconnaissance – How attackers enumerate domains, users, systems, shares, and other information in a Windows environment.
  - Windows Credentials – Understanding sources of credentials in a Windows environment and the various forms of password attacks, including pass-the-hash and in-memory clear-text password recovery.
  - Logon Events – Provides scenario-based examples of the types of logons attackers perform when moving from system-to-system and the resulting sources of evidence in event logs.
  - Remote Command Execution – How attackers execute commands from one system to another during lateral movement using built-in Windows mechanisms.
  - Interactive Session Artifacts – Insight into the file system and registry-based sources of evidence resulting from interactive / GUI access to a Windows system, including topics such as Shell Bags, LNK files, and MRU keys.

- **Hunting** – How to apply the lessons-learned from the previous modules to proactively investigate an entire environment, at-scale, for signs of compromise. This includes:

    - Objectives of Hunting – An introduction to the objectives of "hunting."
    - Examples – Walks through several examples of sources of evidence that are well-suited to large-scale analysis, such as Task Scheduler event log entries, ShimCache, and Windows Services. Techniques for efficiently searching, stacking, and data reduction are provided for each.

Who Should Attend

This is a fast-paced technical course that is designed to provide hands-on experience with investigating targeted attacks and the analysis steps required to triage compromised systems. The content and pace is intended for students with some background in conducting forensic analysis, network traffic analysis, log analysis, security assessments & penetration testing, or even security architecture and system administration duties. It is also well suited for those managing CIRT / incident response teams, or in roles that require oversight of forensic analysis and other investigative tasks.

Course Prerequisites

- Students must have a working understanding of the Windows operating system, file system, registry, and use of the command-line. Familiarity with Active Directory and basic Windows security controls and common network protocols will also be beneficial.