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 two-day course is designed to teach the fundamental investigative techniques needed to respond to today's threat. 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. This class will primarily focus on analyzing Windows-based systems and servers; however, the techniques and investigative processes are applicable to all systems and applications. 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, investigate an incident throughout the enterprise, and much more.

Modules Included (with labs throughout the instruction)

- **The Incident Response Process –** An introduction to the threat landscape, targeted attack life-cycle, initial attack vectors used by different threat actors, and the phases of an effective incident response process.

- **Single System Analysis –** This module includes in-depth information about the most common forms of endpoint forensic evidence collection and the benefits and limitations of each. A deep dive will be taken into file system metadata, registry, event logs, services, common persistence mechanisms, and artifacts of execution. Students will be taught to answer the key questions about what transpired.

    - *File System Metadata*
    - *Event Logs*
    - *Registry*
    - *Memory Analysis*

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

- **Investigation Management –** Managing and effectively recording information related to ongoing investigations and incidents is crucial for success. This module will cover the best practices and some approaches to information management which enrich the investigative process and bolster the enterprise security program.

- **Remediation –** The remediation phase of an enterprise investigation is an important part of the incident response process. Discussion on the containment and remediation of a security incident will bridge short-term immediate actions taken during a live incident, to longer term strategic posturing to improve the resiliency of the organization as a whole.

- **Threat Hunting –** Threat hunting is a critical component of an effective enterprise security program. Hunting using threat intelligence, anomaly detection and known threat actor techniques, tactics and procedures (TTPs). Applying the lessons-learned from the previous modules to proactively investigate an entire environment, at-scale, for signs of compromise.

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 security operations, incident response, 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, basic Windows security controls, and common network protocols.

What Students Should Bring

Students must bring a laptop that meets the following minimum requirements:

- Students must possess Administrator rights to the system they will use during class and must be able to install software provided on a USB drive.
- Students must bring a laptop that meets the following minimum requirements:
  - Operating System: Windows 7 or newer
  - Processor: Core i5 or equivalent
  - RAM: At least 6GB, preferably 8GB
  - HDD: At least 25GB free space
- Virtual machines are acceptable provided at least 4GB of RAM can be allocated. Students are responsible for providing their own copies of and licenses for Windows.

Course Materials

Students will receive:

- a participant guide
- a USB drive containing all required lab materials and tools
- Mandiant-branded gear