Incident Response and Forensics (CS106)

40 Hours

Outline

The main propose is to teach the fundamental investigative techniques needed to respond to threat actors and intrusion scenarios. The latest in forensics and intrusion techniques.

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.

Target Audience

Developers, managers, IT /Network administrators

Prerequisites

Basic computers networks and information security knowledge

Contents

The course is composed of the following modules, with labs included throughout the instruction.

SIEM

Security Information and Event management, the architecture and tools to implement SIEM solution.

SOC

Security Operation Center – The structure of SOC, the tools and positions.

Detection and Analysis

Common mechanisms to detect threats, prioritizing and categorizing leads, the need to fully scope targeted attacks, and methods to proactively hunt for signs of compromise Remediation – The goal of remediation, when remediation is necessary, planning for remediation, and executing 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. This module includes the following topics:

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:

Hunting

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

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: