Cyber Defender 2: Digital Forensics and Incident Response

An Information Security Course for Corporate and Government IT Personnel

Cyber Defender 2 is a mentored, learn-by-doing course that is delivered online. Students will learn the basic skills of conducting memory and file system forensics guided by a set of indicators of compromise. They will then go on to learn the basic procedures and skills of responding appropriately to a security incident.

Tasks

- Examine a compromised host's memory

  Students perform forensics examination of a memory image taken from a computer to identify sophisticated malware that infected the device.

  OBJECTIVE: Acquire a working knowledge of process structures in memory using Volatility
  OBJECTIVE: "Know normal to find evil"
  OBJECTIVE: Formulate plan for a memory forensics investigation
  OBJECTIVE: Recognize malware "footprints" in a forensic memory image
  OBJECTIVE: Locate a malicious binary in a forensic memory image
  OBJECTIVE: Corroborate findings with other sources such as [Splunk] SIEM logs
  OBJECTIVE: Identify malware actions such as privilege escalation and browser hooking
  OBJECTIVE: Extract, safely package, and share a malware sample from a forensic disk image

- Conduct a forensic disk examination

  Students perform disk forensics on an infected computer. By analyzing an image the computer's file system, the students are able to identify malware infections and to create a timeline for the attack.

  OBJECTIVE: Analyze a forensic disk image and identify indicators of compromise using Autopsy.
  OBJECTIVE: Generate a timeline of suspicious events in a forensic disk image.
  OBJECTIVE: Determine how a device was infected and what malware variant was used.

- Close the investigation

  Students are asked to conclude their investigation, carried out over Cyber Defender 1 and 2, by compiling a timeline for the attack and writing a comprehensive report for technical and non-technical stakeholders.

  OBJECTIVE: Cross-correlating information from a range of sources
  OBJECTIVE: Combining information from a range of sources into a comprehensive report
  OBJECTIVE: Communicating a complex story effectively to technical and non-technical audiences.

- Observe and critique the response to a complex cyber attack

  Students observe and critique a sub-optimal response to a cyber attack, and then they revise the company's incident response plan based on lessons learned from responding to an attack.

  OBJECTIVE: Recognize common errors in incident response
  OBJECTIVE: Incorporate best practices into an incident response plan.

Duration: 6 weeks at 25 hours/week
Prerequisite: Cyber Defender 1