The Cybersecurity Certificate Program

The Cyber Certificate Program is a progression of three courses designed to impart a strong foundation of defensive cybersecurity skills in 18 weeks of study at 25 hours per week. Development of the 100% project-based, learn-by-doing program was funded, in part, by the Department of Defense (under agreement C5-16-0023), and the curriculum was designed in conjunction with DoD-selected and industry experts.

Students work through 10 tasks (spending 1-2 weeks per task) online in a private cloud environment with help, advice, and feedback from a knowledgeable mentor and extensive online learning resources. The tasks are embedded in the realistic, but fictional, context of work as an entry-level employee of a government cyber operations agency.

In addition to the task-based curriculum, an implicit curriculum runs throughout the program via which students learn and practice the cognitive skills essential for success in all areas of information security. These include:

• Understanding complex, novel problems
• Effectively researching solutions
• Designing and testing solutions
• Making evidence-based decisions
• Communicating effectively with stakeholders
• Self-directed learning

Given the constantly changing nature of threats and challenges, these skills are arguably of equal or greater importance than the task-specific skills students learn. Students must successfully complete each successive course to be eligible to continue.
Cyber Attack and Defense: Immediate Immersion

Duration: Six weeks working 25 hours per week

Prerequisites: No formal IT experience is required. The ideal student is intensely curious, unwilling to give up on a problem no matter how difficult it is, attentive to detail, and predisposed towards self-directed learning. Strong computer skills are required, and basic knowledge of computer networks, protocols, and the fundamentals of operating systems is recommended.

Key Skills: Thinking Like an Attacker and Network Traffic Analysis

Course Overview

The field of Information Security deals with the ever-growing volume of threats to businesses and government entities. While hardening computer and network infrastructure with patching, firewalls, and intrusion protection systems is important, those tools will probably never stop the threats completely. Adept individuals are needed to monitor the security tools, watching for threats that bypass the automated protections. The analysts in the Security Operations Center (SOC) are the last line of defense. The SOC tries to detect and remediate threats that make it past the protections. The SOC analyst role has traditionally been an entry-level position, but a great deal of knowledge and skills are necessary for success.

The success of a SOC is difficult to measure since attackers and attacks never stand still: Everything is a moving target. Success is typically measured by reducing organizational risk by detecting, remediating, and automatically preventing future instances of known attacks. In reality, this is far beyond the capability of most SOCs today. And to make matters even worse, SOC analysts rarely have the tools, tactics, procedures, or training to deal with all the threats that can affect organizations today. Nobody wants to admit how difficult the struggle is, which means it’s difficult to even get the conversation going.

Qualifications for entry-level SOC analysts are problematic because most applicants have little if any training in information security. Realistically, an entry-level SOC analyst can only be expected to be passionate about security and have some networking background – which happen to be the prerequisites for this course.

In this six-week "on-ramp" course, you will be working as an analyst at a fictional government agency. First, you will gain experience thinking like an attacker. You will then investigate alerts by analyzing network traffic. We have designed this course to provide you with initial experience
analyzing and understanding what alerts mean through realistic hands-on tasks. (Future courses will deal with log analysis, malware analysis, digital forensics, and incident response.)

Immediate Immersion includes the following tasks:

• Exploit a website and fix its vulnerabilities

Students learn to think like attackers. They investigate a defense contractor’s website surreptitiously, fix a vulnerability, and remove malware. To accomplish this, they must use a vulnerability uncovered by human intelligence to access to the webserver themselves and then crack the webmaster’s encrypted password, so they can remove the malware and patch the vulnerability that left the system open to attack.

OBJECTIVE: Think like an attacker
OBJECTIVE: Exploit a website using a local file inclusion vulnerability
OBJECTIVE: Crack a password
OBJECTIVE: Determine if a website has embedded malware
OBJECTIVE: Conduct online technical research
OBJECTIVE: Patch the code of a website to eliminate a local file inclusion vulnerability

• Investigate suspicious behavior

You receive a report that an employee had unusual text on his screen which didn’t seem to be work related. The security team captured a recording of that employee’s network traffic from the time of the report. Your task is to use two traffic analysis tools to determine what the employee was doing. Was his activity benign—or is this evidence of an insider attack?

OBJECTIVE: Conduct an investigation of a cybersecurity incident
OBJECTIVE: Analyze network traffic using NetworkMiner
OBJECTIVE: Analyze network traffic using Wireshark

• Analyze malicious network traffic

You will analyze suspicious network traffic moving in and out of a US military aide’s personal laptop. Using packet capture (PCAP) files, you will determine if it was infected by malware and if so what malware and how the infection occurred.

OBJECTIVE: Analyze suspicious network traffic in a PCAP using Snort and Wireshark.
OBJECTIVE: Recognize a cushion redirect in network traffic.
OBJECTIVE: Recognize the identifying features of a specific exploit kit.
OBJECTIVE: Recognize a malware payload being transferred to a targeted host.

Who Should Enroll

Students who wish to explore a career in cybersecurity to determine if it is right for them.

Additional Info

Students must successfully complete Cyber Attack and Defense: Immediate Immersion 2020 to be permitted to enroll in the next course in this program, Cyber Defender 1. Success will be assessed by a student’s mentors whose decision is final.
Cyber Defender 1

Duration: Six weeks working 25 hours per week
Prerequisites: Successful completion of Immediate Immersion or substantial professional IT experience and consent of the instructor.

Key Skills: Network Traffic Analysis, Log Analysis, and Triage of Malicious Activity

Students will gain more advanced skills of analyzing network traffic at the packet level, as well as analyzing system and network logs for indicators of malicious activity. They will then learn more complex techniques of log analysis, and static and dynamic analysis of potentially malicious files.

Cyber Defender 1 includes the following tasks:

• Analyze a remote intrusion attempt

  A security operations center analyst has seen evidence of a password cracking attempt within a key network. Students analyze a PCAP and event logs within a security information and event management system (the Splunk SIEM) to determine whether or not any passwords were compromised, and if the network was breached as a result. The student must also identify which tools were used by the attacker, and which steps should be taken to safeguard specific hosts in the network from similar cracking attempts in the future.

  OBJECTIVE: Analyze suspicious network traffic in a PCAP using Wireshark.
  OBJECTIVE: Analyze network and system logs using the Splunk Security Information and Event Management System
  OBJECTIVE: Cross-correlate events seen in a PCAP with events seen in logs
  OBJECTIVE: Recognize a Hydra brute-forcing attack
  OBJECTIVE: Determine if a brute-forcing attack has been successful

• Investigate an incident using a Security Information and Event Management System (SIEM)

  Students analyze a possible “watering hole” attack in which clicking on a malicious link embedded in an otherwise legitimate website launches an exploit kit that infects a user’s machine with a “banking trojan.” To accomplish this, they must analyze multiple logs within the Splunk SIEM.
OBJECTIVE: Analyze network and system logs using Splunk
OBJECTIVE: Pivot among multiple logs using Splunk’s search facilities
OBJECTIVE: Identify possible indicators of compromise
OBJECTIVE: Determine if devices are likely to have been infected using indicators of compromise
OBJECTIVE: Tentatively identify the malware used and the intent of the attack

• Analyze and understand malware using a sandbox coupled with open source intelligence gathering

Students use a “hash” of the possible malware-containing file to conduct research using VirusTotal, online sandboxes, and open source intelligence sources to determine specific indicators of compromise to guide forensic analysis of memory and file system images of infected devices.

OBJECTIVE: Use VirusTotal to identify a malware sample
OBJECTIVE: Use advanced features of VirusTotal to learn detailed information about a malware sample
OBJECTIVE: Use the HybridAnalysis sandbox to perform static and dynamic analysis of a malware sample
OBJECTIVE: Use open source threat intelligence to learn more about specific malware
Cyber Defender 2

Duration: Six weeks working 25 hours per week
Prerequisite: Successful completion of Cyber Defender 1

Key Skills: Digital Forensics and Incident Response

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 to a security incident.

Cyber Defender 1 includes the following 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 tasks four through seven, 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.

• Respond to cybersecurity incidents

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. They then participate in a “tabletop” exercise during which they will respond to an incident themselves.

OBJECTIVE: Recognize common errors in incident response
OBJECTIVE: Incorporate best practices into an incident response plan
OBJECTIVE: Make appropriate incident response decisions under time pressure and in light of business constraints.