Cyber Defense Analyst Bootcamp

Overview

LEVEL EFFECT

Introduction

Why did we make the Cyber Defense Analyst Bootcamp?

Our team has years of experience working in the Cyber industry and have taught Cyber security training at other companies and we realized a gap - most training is focused on Cyber skills not actually needed in private organizations.

The CDA bootcamp is mapped to the NIST NICE framework and equips students with all the skills they need to defend and protect an enterprise network. In the bootcamp we learn, practice and train to **actually work in the field.**

While the CDA bootcamp focuses on defensive tradecraft, students also learn about adversary tactics, threat hunting and using Linux OS, setting the foundation to show you how offensive tactics are used against organizations.

Our program (and our team) is dedicated to making these **skills accessible to everyone.** You do not need a background in IT or Tech to succeed in this bootcamp. We have tons of free primer content for you to sharpen your computer skills and knowledge before starting the bootcamp.

Bootcamp Overview

- 14 Weeks long, including 13 weeks in class and a 1 week capstone exam
- Live classes are taught remotely Mon-Thurs from 7pm - 9pm CST
- The bootcamp is run 3 times a year and only accepts up to 35 students/class
- Bootcamps start in September, January and May

- There are 4 instructors per cohort, each with their own specialized skills, they circulate based on the module being taught
- Private office hours are available with every instructor throughout the bootcamp, ensuring there is lots of time for personalized learning

Tuition

The Cyber Defense Analyst bootcamp is **$9,500.**

To register, a deposit of $1,000 is required.

The following discounts are available:

- Veterans, Active Duty Military and First Responders from Canada and the USA **receive $500 off.**

- Students who register more than four weeks before the cohort start date receive a **$1,000 Earlybird discount applied to their final tuition.**

Visit **www.leveleffect.com** to apply for financing, a sponsorship and to reserve your spot in the bootcamp.

Curriculum

Module 1: Networking

Malware can only get so far until it needs to get over the wire to spread and become an advanced threat. In this module you will:

- Perform in-depth network traffic capture analysis and triage.
- Learn how to use industry tools like Wireshark, Snort, and Zeek, to dissect network traffic and identify malicious activity on the wire disguising itself.
- Additionally, learn how to leverage vulnerability scanning tools to detect network service misconfigurations and alert on known vulnerabilities well before they become security incidents or lead to permitting malicious network traffic.

Module 2: Windows Enterprise Network

Learn the fundamentals of enterprise Windows networks in today's workplaces from the server to the regular user workstation. In this module you will:

- Configure key active directory infrastructure and understand how domain services work.
- Administer group policies and understand how different components of active directory work together to identify common pitfalls of enterprise networks.

Module 3: Advanced Windows OS (2 weeks)

You're not done with Windows yet! It's critical to learn this operating system as you'll work in and out from it the vast majority of your cyber career. You need to be able to defend and triage this operating system inside out. In this module you will:

- Use the infrastructure you built and dive deep into the Windows operating system in this module.
- Learn key components like processes, threads, memory, I/O, DLLs, drivers, and registry.
- You'll learn how to perform complete triage of the Windows operating system, binaries, and services.
- Finally, you'll perform complete triage of live compromised Windows systems and identify indicators of compromise along with reporting on how to remediate the incidents.

Module 4: Security Operations (2 weeks)

You've been taught the tools and tradecraft. You'll now start working in a SOC (Security Operations Center) as an analyst using what you've learned with the infrastructure you've learned how to build. In this module you will:

- You'll use Event Monitoring and Log Aggregation Tools alongside Windows to work with network and endpoint data to identify threats contained in logs and network activity.
- You'll also learn how to create advanced IDS rules to detect threats using concepts like byte/hex code and eradicate persistence and learn how to work with EDR (endpoint detection and response) solutions.
- Additionally, you'll develop your scripting abilities making your own security automation tool in PowerShell!

Module 5: Cyber Threat Intelligence

Learn how to compile threat intelligence so that your organizations are dedicating their resources effectively. In this module you will:

- Learn how to use tools such as MITRE ATT&CK, MISP, and FireEye intelligence reports to gather threat actor data.
- Share your research as indicators of compromise in a threat intelligence sharing platform.
- Develop the ability to succinctly research and deliver a Threat Intelligence Report on real-world adversaries.
- Ultimately, be able to describe and summarize what a threat actor is and suggest solutions to prevent attacks based on their tactics, techniques, and procedures.

Module 6: Linux OS

Linux is an incredibly important supplemental tool in your toolkit and sometimes your main tool depending on the scenario. In this module you will:

- Learn how to navigate Linux and understand the fundamentals of the operating system. Be able to manage applications, users, group permissions, and to triage and hunt for indicators of compromise on a Linux system.
- Learn how to hunt for common misconfigurations and scenarios that could lead to incidents.
- You'll also learn data stream redirection in depth, a fundamental component of nearly all remote threat actor activity and how to utilize variables, iteration, user input, error logging, and bash scripting to create your very own security tools! Finally, you'll go through the gauntlet of a very compromised live Linux system that will put your triage knowledge to the test.

Module 7: Adversary Tactics

You'll put your red team hat on and learn how to perform the same tactics that adversaries use to exploit modern networks while configuring event and log shipping to monitor the attacks you'll carry out yourself observing the events generated by your actions! In this module you will:

- Build on your data stream redirection knowledge gained and understand how bind and reverse shells are created which are the backbone of many attacks.
- Learn how to thoroughly enumerate Windows and Linux systems and bypass controls like Windows Defender.
- Utilize Command & Control (C2) frameworks and toolkits to exploit vulnerable systems and services like threat actors do and maintain a form of advanced persistence.
- Perform threat actor attacks like pass-the-hash, impersonation, lateral movement, data exfiltration, SQL injection, SMB exfiltration, domain controller takeovers, and more.

Module 8: Network and Computer Forensics

At this point you're more than ready to be a Security Analyst but you'll come out more than just entry-level in this bootcamp. You're going to learn more advanced concepts from here on out and continue building your repertoire of skills. In this module you will:

- Learn the concepts of forensic collection for both network and endpoint usecases and use cases for registry hive forensics.
- Analyze and extract indicators and evidence from network traffic and identify how artifacts from malware can be recovered from areas such as Shimcache and Amcache, and other overlooked areas of the registry.
- Collect and parse volatile memory from a compromised system identifying how malicious activity spread and hid through processes and remained in memory.
- Compare and contrast the benefit and visibility provided by Windows forensic triage to uncover and identify malicious activity.

Module 9: Memory & Malware Analysis

Learn the difference between static and dynamic malware analysis. In this module you'll:

- Learn how malware is created live in class by working as a group to create a new variant.
- Practice dumping strings from a binary to look for clues.
- Learn what obfuscation really means and how it pertains to malware. Practice de-obfuscating messages to uncover hidden messages.
- Familiarize yourself with reverse engineering and how code becomes a program using tools like Ghidra and PEStudio.
- Participate in a guided walk through as the instructor reverse engineers several binaries to unlock their secrets.

Module 10: Practical Cyber Triage

Put it all together for a week of intense live triage with everything you've learned with more complex incident scenarios on compromised systems including live attacks on your infrastructure that you need to respond to! Triage and report on diverse incidents within the network.

Module 11: Threat Hunting

Just when you thought you were done with triage – we're pulling you back in for more!

- You'll go through more complex triage scenarios and learn how to perform Threat Hunting and what it means for an organization.
- You'll identify, hypothesize, and plan a Threat Hunting engagement. You'll heavily utilize and apply the methods of the MITRE ATT&CK framework to operationalize and support your engagement.

CDCP Capstone Exam!

The CDCP is a 1-week practical application of the knowledge, tools, techniques, and procedures acquired through the Cyber Defense Analyst Bootcamp. This is accomplished through a battery of real-world security operations scenarios that students must overcome and articulate in a detailed report that includes the appropriate executive summary, findings, recommendations and remediation steps along with applicable evidence. A holder of the CDCP has demonstrated the knowledge, skill, and practical application to work within a security operations team.

& then what?

Bonus Learning Content

This content is not required for entry-level Cybersecurity work but does help improve your overall versatility and technical skill set. These additional modules are included at no cost to CDA Bootcamp students. They may also help you explore further areas of Cybersecurity of interest! Currently offering additional learning content on Cloud & Application Security.

Cloud & Application Security: Infrastructure and Web Apps

The cloud hosts many critical pieces of infrastructure and is a large component of application security. Learn core concepts of cloud virtualization, and how cloud infrastructure works by spinning up your own infrastructure and administering virtualized cloud resources. Learn the foundations of web application security and conduct a practical assessment of a web application. Additionally, learn how to audit cloud security for misconfigurations and known vulnerabilities.

+ plus

Career support

Throughout the bootcamp, our instructors offer support and 1:1 coaching for mock interviews, career coaching and career guidance. After the bootcamp, our team is continuously there to support you until you find a role.

Community

Join our discord community for support from alumni and instructors, enjoy continued access to VMs and labs as an alumni and get first access to exclusive perks as we launch more free and paid courses on our learning platform.

Discord invite link: https://discord.gg/8xNTpQGbpK