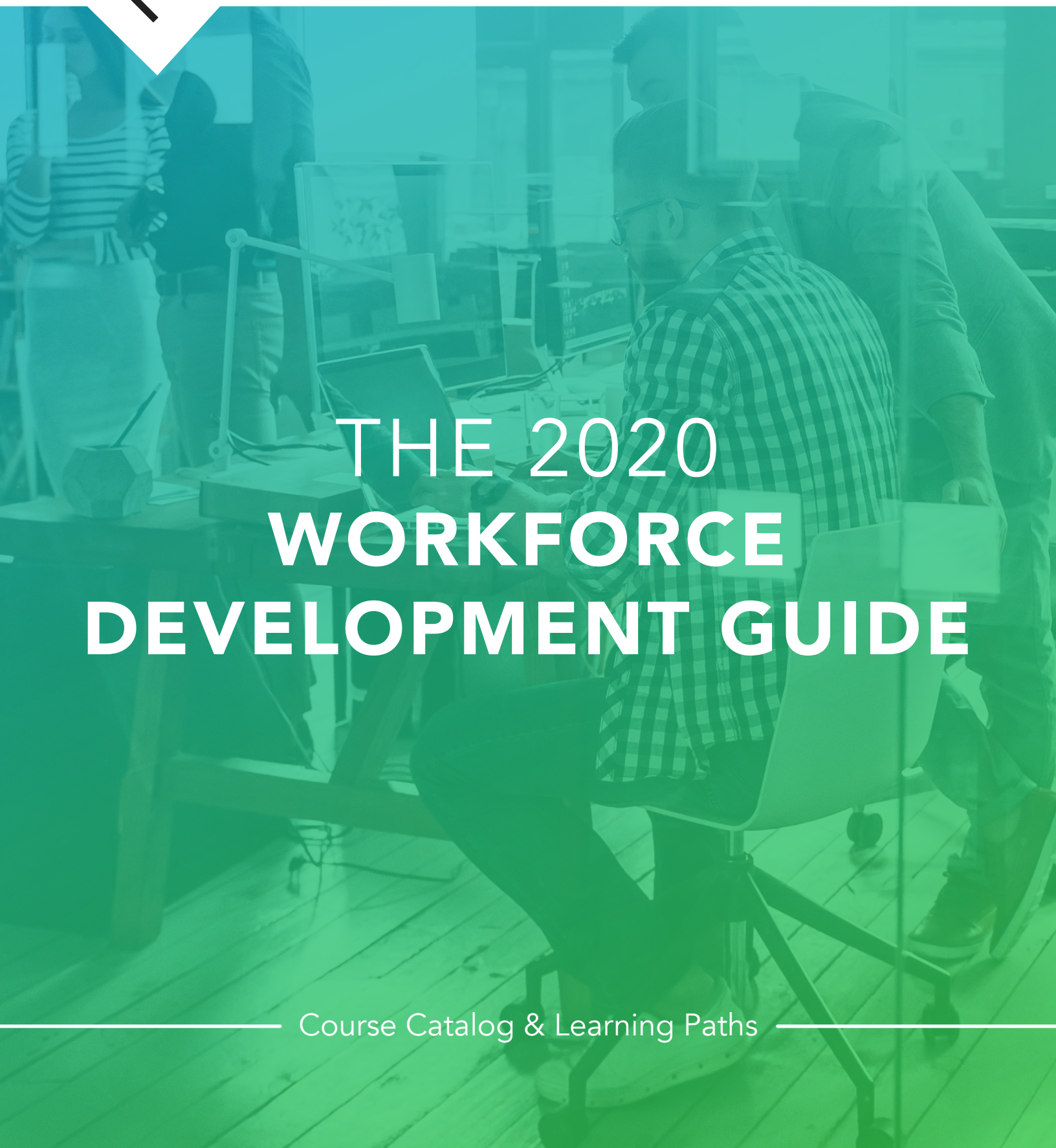
FOCAL POINT
ACADEMY



THE 2020 WORKFORCE DEVELOPMENT GUIDE

Course Catalog & Learning Paths

CONTENTS

CYBER WORKFORCE **DEVELOPMENT**

Focal Point Academy's mission is to build better, faster, more agile cybersecurity teams – teams that have the skills to identify threats in real time, the knowledge to reverse engineer attacks, and the experience to prevent them from happening again. This is what sets Focal Point apart. We build elite cybersecurity teams by focusing not only on training, but on workforce development.

Without a cyber workforce development plan in place, it is difficult to measure a return on your training investments. A workforce development program keeps training relevant, focused, and engaging. It also allows you to:

Secure your organization.

A workforce development program is the most effective way to fill your cyber talent gaps and reduce unnecessary risk exposure, stop breaches, and respond to threats.

Reduce costs.

A workforce development program creates an internal talent pipeline capable of filling entry, senior, and management roles without the high upfront recruiting and onboarding costs.

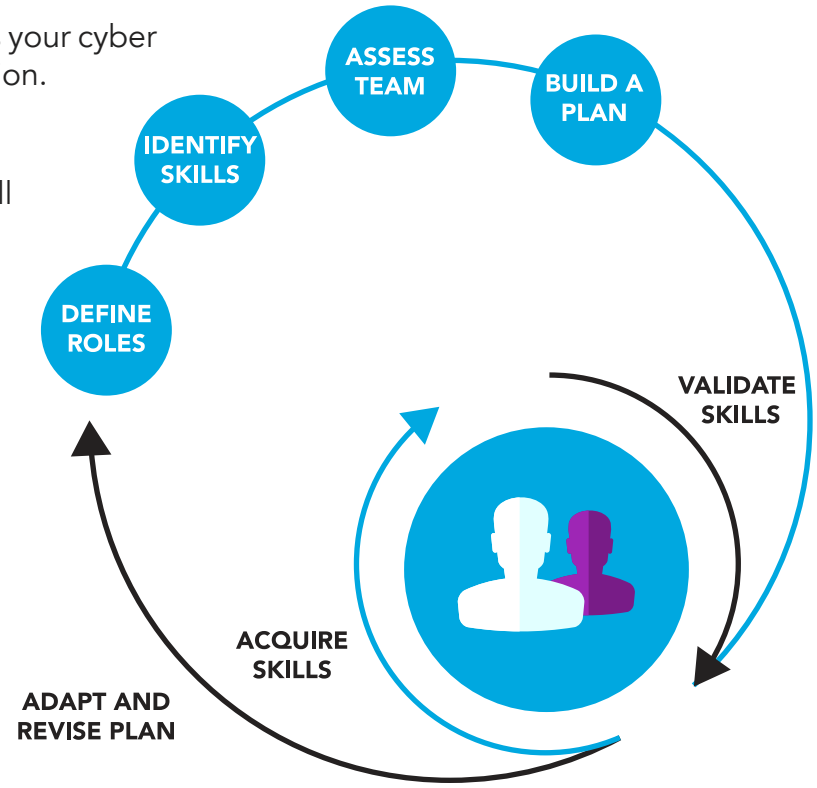
Improve employee retention.

A well-structured development program gives your cyber talent a path to success within your organization.

Validate your team.

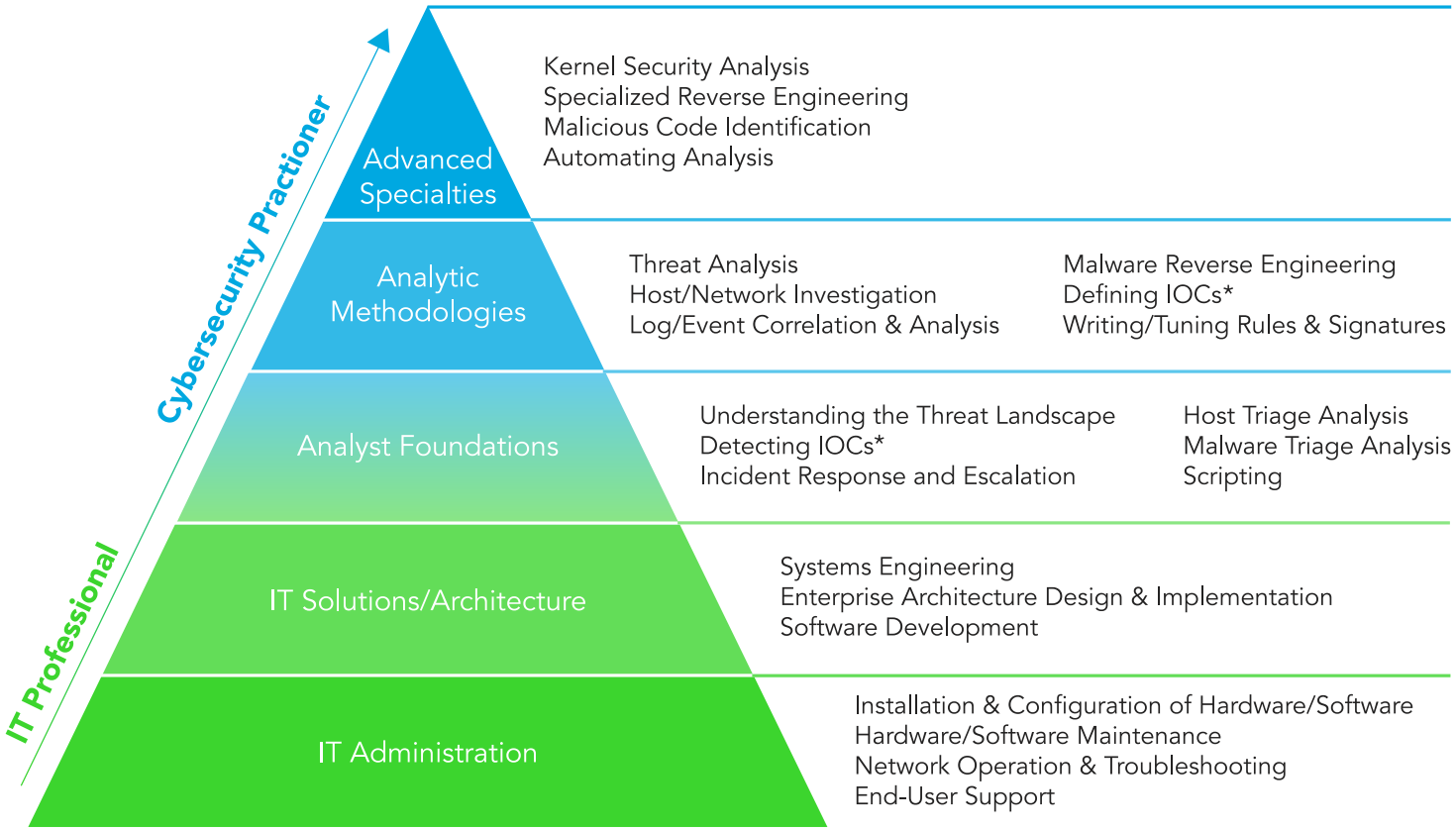
A good workforce development program will test your team's ability to function as a unit, not just as individuals.

To us, workforce development is the process of defining, measuring, and training your cybersecurity team, and building a long-term strategy to guarantee that their skills remain aligned with the threats facing your organization.



SKILLS PYRAMID

Every career in cybersecurity has a starting point. By evaluating your team's existing knowledge and skills, we can start to build a roadmap that will grow each team member into a capable cybersecurity practitioner. Our programs are perfect for those with an IT background and those wanting to operationalize their existing cyber knowledge. The skill areas below are viewed as critical for analytic cyber teams and are defined as essential within recognized industry frameworks.



*Indicators of Compromise

DIGITAL BADGING **PROGRAM**

Focal Point Academy's badging program recognizes the accomplishments of cybersecurity professionals and helps cybersecurity leaders identify and qualify cyber talent. After completing a course or series of courses, students can receive digital badges that qualify their mastery of a skill or skillset for a specific role. These badges signify that their skills have been developed and vetted by industry experts.

How It Works

Focal Point uses Credly's Acclaim platform for its badging program. Each unique badge provides a one-click, real-time virtual representation of a student's successful achievement of a new skill or completion of a learning path, with the metadata to match. The metadata built into the badge validates the credential and provides details on the achievement, including the criteria the individual met to earn it, the skills they now have, and when, or if, the credential expires. Once badges are awarded through Focal Point Academy, individuals can showcase their accomplishments online through professional and social networks, such as LinkedIn, Facebook, Twitter, email signatures, and digital resumes.

Badge Categories

Focal Point's badging program is divided into two key credential categories: Skills and Role Proficiencies. These categories are intended to recognize security professionals' expertise and qualifications for critical roles on cybersecurity teams.

ROLE PROFICIENCIES

Role proficiency badges are awarded to students who have the cumulative skills required to fill a specific role on a cybersecurity team. Examples include:

Reverse Engineer I

Cyber Threat Analyst II

SKILLS BADGES

Skills badges are awarded when a student masters a specific capability through a series of hands-on labs and exercises during one of our courses. Examples include:

Network IOC Identification & Investigation

Scripting IDA with Python

System Log & Event Analysis

SAMPLE LEARNING **TRACKS**

Learning tracks help you see where your team can go with Focal Point Academy. These aren't prescriptive paths to success, but simply suggestions on how your team can reach the next level.

Raj
Senior IT Administrator

Raj had been in an IT admin role at his old company for 4 years, growing into a senior admin. He wanted to transition into cybersecurity and studied on his own time to attain several relevant industry certifications. A hiring manager with a knack for spotting talent brought Raj in for an interview. They were impressed by Raj's self-starter attitude and pursuit of new knowledge and skills. They have committed to developing Raj into a Cyber Threat Analyst Level I over a 9 month period.

Cyber Threat Analyst I

- Intro to Cybersecurity
- Network Forensics and Investigation
- Windows System Analysis

Sr. IT Admin — 9 months → **Cyber Threat Analyst I** — 12 months → **Cyber Threat Analyst II** — 18-24 months → **Threat Hunter I**

Sam
Incident Responder

The CISO at Sam's company recently formalized a cyber workforce development program, which highlighted a gap in their threat-hunting capability. Sam is an incident responder with two years of experience at the company and scored highly in an assessment designed to identify suitable resources for a new threat-hunting team. Sam, along with five teammates, will be participating in a development program over the next 18 months to enable this critical new function.

Threat Hunter I

- Network Forensics and Investigation
- Windows/Live System Analysis
- Behavioral Malware Anaylsis
- Malicious Network Traffic Analysis
- Python for Network Defenders
- Hacker Methodologies
- Cyber Threat Detection & Mitigation

Incident Responder — 18 months → **Threat Hunter I** — 18 months → **Threat Hunter II** — 24-36 months → **SOC Manager**

SAMPLE LEARNING **TRACKS** (cont.)

Alex
Incident Responder

Alex is an incident responder on her company's cybersecurity team. After a year in this role, she wants an opportunity to further specialize her skillset. She has demonstrated a passion for analysis and research, always digging deeper to uncover the source of a problem. Her manager has noticed that Alex displays exceptional attention to detail, catching anomalies many of her teammates miss. After Alex expressed her desire to advance in her career during her annual review, her manager gave her the opportunity to grow into a malware triage role.

Malware Triage Analyst Track

- Windows/Live System Analysis
- Behavioral Malware Analysis

12 months → **Incident Responder** → 18-24 months → **Malware Triage Analyst** → 18 months → **Reverse Engineer I** → **Reverse Engineer II**

Chris
Junior Web Developer

Chris is a junior-level web developer who wants learn new coding languages, so he can expand his skillset to include application development. His company is actively looking for app developers to help them build and optimize custom tools to support key operations. Chris's existing knowledge of company tools and operations makes him the perfect fit. His company has committed to helping him learn these skills and move into an app developer role over the next six months.

Application Developer Track

- Intro to C Programming
- Intro to C++
- Assembly for Reverse Engineers

6 months → **Jr. Web Developer** → 18 months → **App Developer** → 18-24 months → **Reverse Engineer I** → **Reverse Engineer II**

Olivia
Software Developer

Olivia is a software developer who has been with her company for six years. She was identified in a company-wide challenge organized by the SOC manager to find those with both a technical background and a puzzle-solving mentality that could be applied in security investigations. She is experienced in both procedural and object-oriented programming with languages such as C, C++, Java, and Python. She has been set an initial 12-month goal to become a malware reverse engineer.

Reverse Engineer I Track

- Behavioral Malware Analysis
- Windows System Analysis
- Assembly for Reverse Engineers
- Malware Reverse Engineering

12 months → **Software Developer** → 18-24 months → **Reverse Engineer I** → 24 months → **Reverse Engineer II** → **Technical Director**

HOW TO USE THIS CATALOG

This catalog presents most of the courses currently offered by Focal Point. It is designed to equip professionals at every level with the cybersecurity skills they need to advance their careers and strengthen their teams. Courses align with three key stages in a cyber career: those who are just entering the realm of cybersecurity (or transitioning from an IT role), individuals who want to progress to a cyber analyst role, and finally, cyber professionals ready to advance to key positions like cybersecurity engineer and cyber threat hunter.

While the skills obtained in these courses are all essential for a well-rounded cybersecurity team, they may not be right for each individual cybersecurity practitioner. Before you begin a workforce development program at Focal Point, we will work with you to build a course lineup that is right for your team. Our goal is to give each specialist the skills needed to do their job most effectively, without wasting resources on courses that don't help fulfill their job responsibilities.

Therefore, we recommend using this catalog simply as a starting point for understanding the range of possibilities offered by Focal Point. But before beginning your workforce development journey, you should discuss your strategic goals with a Focal Point expert. We leverage our experience, best practices, and standards like the NICE Cybersecurity Workforce Framework to ensure you are building skills that meet your actual needs.

If you think workforce development is right for your organization, contact us:

Visit us: focal-point.com/academy

Drop us a line: academy@focal-point.com

Give us a ring: 800-969-7770

OUR GOAL

To give each specialist **the skills needed to do their job most effectively, without wasting resources** on courses that don't help fulfill their job responsibilities.

CATALOG KEY:


primary audience


virtual delivery available


lab exercises


college credit

course length


CPE/CEU credits*

* up to 30 credits for a 5-day course

CYBER THREAT **ANALYSIS**

Less than 30% of security professionals start their careers in cyber, instead beginning their journeys in IT, accounting, software development, or even the arts. Many times, success in the field of cybersecurity is not reliant on years of experience or having the coding skills of a seasoned hacker. What your security team needs are problem solvers, creative thinkers, strategists, and those with passion and drive. The technical skills can be trained. Our cyber threat analysis courses provide non-cyber professionals with the foundational skills to start their security careers and take those with experience to the next level.

CORE SKILLS

- Understanding the Threat Landscape
- Detecting IOCs
- Incident Response and Escalation
- Host Triage Analysis
- Malware Triage Analysis
- Scripting

> ***You don't have to be born with the coding skills of a seasoned hacker to have a successful career in cybersecurity.***

KEY COURSES

Intro to Cyber Risk Management	Intro to Cybersecurity	Windows System Analysis
Understanding Operating Systems	Live System Analysis	Network Forensics and Investigation
Malicious Network Traffic Analysis	Behavioral Malware Analysis	Python for Network Defenders

CYBER THREAT ANALYST I

Level I Cyber Threat Analysts are capable of identifying and investigating incidents from an operating system and network forensics perspective. They have the skills to identify anomalous activity, determine the scope of that activity, and report or mitigate as appropriate.

Cyber Threat Analyst I Track

Intro to Cybersecurity (or equivalent)

↓

Network Forensics and Investigation

↓

Windows or Live System Analysis

↓

Demonstrated Skills
Network Traffic Analysis | Endpoint Threat Analysis

Related Skills Badges

CYBER THREAT ANALYST II

Level II Cyber Threat Analysts have developed the ability to analyze and investigate complex, multi-stage intrusions, and to mitigate such intrusions by deploying active defensive measures.

Cyber Threat Analyst II Track

Cyber Threat Analyst I Track

↓

Behavioral Malware Analysis

↓

Malicious Network Traffic Analysis

↓

Python for Network Defenders

↓

Demonstrated Skills
Endpoint Threat Analysis | Behavioral Malware Analysis
Defensive Cyber Operations

Related Skills Badges

INTRO TO CYBER RISK MANAGEMENT

This is a one-day, seminar-style program that covers the cyber fundamentals leaders need to operate their business securely, embrace disruption safely, and effectively communicate cyber risks within their organizations. Designed with busy executives in mind, this program dissects the most important issues in cyber risk management and arms attendees with the tools needed to engage in strategic cyber conversations at the executive level.

Key Outcomes

After successfully completing this course, attendees will be able to:

- Express the importance of a sound cybersecurity strategy in attaining an organization's business goals
- Recognize areas of vulnerability within their organization and the threats that seek to exploit them
- Identify the cyber risks to their organization and the practices that will mitigate and eliminate them
- Practice effective cyber hygiene

> ***"The seminar definitely raised my cyber awareness and knowledge and also showed me how to apply it on a personal level."***

the details

Virtual delivery available

1-day course

6 CPE/CEU credits

Executives & C-suite

lab exercise

Executives participate in hands-on team exercises that put their new knowledge to the test. The final module walks attendees through good cyber hygiene practices.

prerequisites

This course is designed to equip executives from outside the cyber world. No prerequisites are needed.

INTRO TO CYBERSECURITY

Introduction to Cybersecurity is the foundational training for management, IT, end-users, and programmers. This course equips your team with a firm understanding of the threats every organization faces and the skills needed to address them. It leverages information culminated from the most trusted sources: CERT, NIST, DHS, and others. This course presents an overview of the current threat landscape and a vision of the future of cybersecurity.

Key Outcomes

After successfully completing this course, students will be able to:

- Recognize cybersecurity as a business issue, not just an IT issue
- Distinguish between different types of cyber threats and stay up to date with emerging threats
- Determine the levels of cyber risk in an organization
- Identify strategic and high-level tactical steps to improve organizational security posture
- Explain the key components of identity and access management
- Describe the types and uses of cryptography in computer systems and networks
- Define the components of an incident response capability

the details

3-day course

18 CPE/CEU credits

IT professionals

lab exercise

Each module has a series of learning objectives, demonstrative labs and exercises, and an interactive knowledge check to verify learning.

prerequisites

This is a beginner-level course. No prerequisites needed.

UNDERSTANDING OPERATING SYSTEMS

Understanding Operating Systems is a foundational course that exposes students to the underpinnings of modern desktop operating systems and the components that are most vulnerable to attack. It covers the principles of process, memory, and I/O management that drive all modern operating systems. It also includes hands-on labs to discover how they are implemented in Windows and Linux. After attending this course, students will be able to describe how the components of operating systems work and interact, use built-in tools to analyze these components, and have an excellent foundation for courses in malware analysis, intrusion analysis, and penetration testing.

Key Outcomes

After successfully completing this course, students will be able to:

- Describe how modern desktop operating systems function
- Explain the principles of process, memory, and I/O management and distinguish the methods used across common operating systems
- Identify and monitor the standard boot processes of Windows and Linux systems
- Use trusted command-line and GUI-based tools to ascertain the status of a running system
- Retrieve and edit a host's network configuration
- Perform basic user and group management tasks
- Describe the foundational security mechanisms in Windows and Linux systems

the details


Virtual delivery available

5-day course


20+ lab exercises


30 CPE/CEU credits

capstone exercise

A challenge board that requires students to analyze Windows and Linux systems, determine pertinent information from those systems, and identify various types of anomalous behavior.

prerequisites

Familiarity with the use of at least one common desktop operating system

Experience with VMware software is an advantage, but not required

WINDOWS SYSTEM ANALYSIS

Windows System Analysis teaches students how to identify abnormal activity and investigate a running system that may have been compromised. In this course, students will learn the most useful commands, tools, and techniques that can be employed during investigation to reveal the significant indicators of infiltration, as well as how to create a system baseline to be used for future analysis. This course is focused primarily on the Windows 10 operating system, using many tools and techniques that also apply to Windows 7 and recent versions of Windows Server.

Key Outcomes

After successfully completing this course, students will be able to:

- Identify the core components of the Windows operating system and ascertain their current state using built-in or other trusted tools
- Analyze a running system and detect abnormal behavior relating to processes, DLLs, network connections, the registry, and Windows services
- Use event log analysis to verify and correlate the artifacts of anomalous behavior and determine the scope of an intrusion
- Use PowerShell to interact with the operating system and build scripts to automate repetitive analytic tasks
- Create and use a system baseline to identify unexpected items such as rogue accounts or configuration changes

Skills Badges

Live Windows Endpoint Analysis

System & Event Log Analysis

the details

Virtual delivery available

5-day course

20 investigation lab exercises

30 CPE/CEU credits

capstone exercise

Investigation exercise where students will identify and investigate compromised systems in a virtualized network environment.

prerequisites

Familiarity with Windows command-line interface

Basic knowledge of TCP/IP networking

LIVE SYSTEM ANALYSIS

Live System Analysis teaches students how to identify abnormal activity and investigate a running system that may have been compromised. In this course, students will learn sound methodology coupled with the most useful commands and tools that can be employed during investigation to reveal the significant indicators of infiltration, as well as how to create a system baseline to be used for future analysis. Both the Windows and Linux operating systems are covered in this course.

Key Outcomes

After successfully completing this course, students will be able to:

- Identify the core components of the operating system and ascertain their current state using built-in or other trusted tools
- Analyze a running system and detect abnormal behavior relating to operating system objects such as processes, handles, network connections, etc.
- Use event log analysis to verify and correlate the artifacts of anomalous behavior, and determine the scope of an intrusion
- Use PowerShell to interact with the operating system and build scripts to automate repetitive analytic tasks
- Create and use a system baseline to identify unexpected items such as rogue accounts or configuration changes

Skills Badges

Live Linux Endpoint Analysis

System & Event Log Analysis

the details

Virtual delivery available

5-day course

20 investigation lab exercises

30 CPE/CEU credits

capstone exercise

Investigation exercise where students will identify and investigate compromised systems in a virtualized network environment.

prerequisites

Familiarity with Windows command-line interface

Basic knowledge of TCP/IP networking

BEHAVIORAL MALWARE ANALYSIS

Behavioral Malware Analysis teaches students the fundamental skills necessary to analyze malicious software from a behavioral perspective. From simple key loggers to massive botnets, this class covers a wide variety of current threats. Using system monitoring tools and analytic software, students will analyze real-world malware samples in a training environment, giving them hands-on experience building secure lab environments, classifying malware, analyzing behavioral characteristics and their effects to systems, and documenting findings.

Key Outcomes

After successfully completing this course, students will be able to:

- Set up a secure lab environment in which to analyze malicious software
- Build and maintain a toolset of freely available, trusted tools
- Classify different types of malware and describe their capabilities
- Analyze malware samples of varying types to ascertain their specific behavioral characteristics and their impact on a system
- Determine if a given sample is persistent and, if so, identify and remediate the persistence mechanism(s)
- Identify when a sample is aware of its virtual environment and will require more advanced static or dynamic analysis

Skills Badges

Malware Classification

Behavioral Malware Analysis

the details

- Virtual delivery available
- 5-day course
- Eligible for college credit
- 20+ malware analysis exercises
- 30 CPE/CEU credits

capstone exercise

Analyze a current piece of Windows malware and produce a thorough report on its capabilities, system impact, and means of persistence.

prerequisites

Comprehensive understanding of Windows, including its major internal components

Basic understanding of TCP/IP networking

NETWORK FORENSICS AND INVESTIGATION

Network Forensics and Investigation teaches attendees to differentiate between normal and abnormal network traffic, track the flow of packets through a network, and attribute conversations and actions taken over a network segment to specific hosts or users. This course focuses on research, filtering, and comparative analysis to identify and attribute the different types of activity on a network. Students will learn how to follow conversations across a wide range of protocols and through redirection and how to develop custom filters for non-dissected protocols.

Key Outcomes

After successfully completing this course, students will be able to:

- Create a baseline of the protocols, hosts, and interactions in a network environment
- Identify anomalous network traffic using a combination of in-depth packet analysis and higher-level statistical analysis
- Reconstruct event timelines and accurately correlate or distinguish between event threads
- Identify and extract network artifacts for further forensic analysis
- Compare observed network traffic to expected topology
- Research and analyze unknown (nondissected) protocols

Skills Badges

Network Traffic Attribution & Reconstruction

Dissection and Analysis of Network Traffic

the details

Virtual delivery available

5-day course

Eligible for college credit

20 analytic lab exercises

30 CPE/CEU credits

capstone exercise

A category-based CTF challenge that culminates in tracking a simulated SCADA intrusion.

prerequisites

Firm understanding of TCP/IP networking

Knowledge of common network devices and their functions

MALICIOUS NETWORK TRAFFIC ANALYSIS

This course will teach students how to identify and analyze the most common types of reconnaissance, attack, lateral movement, exfiltration, and command-and-control traffic found in today's networks. It covers a range of techniques from deep-packet analysis to statistical-flow analysis to opensource research and more. This course uses tools such as Wireshark, Network Miner, and RSA NetWitness Investigator as well as custom tools and scripts developed by our networking experts.

Key Outcomes

After successfully completing this course, students will be able to:

- Identify and analyze attacks across the various layers of the network stack
- Identify signs of reconnaissance being conducted against a network and recommend mitigation steps to limit the data provided to attackers
- Perform flow analysis to uncover anomalous and malicious activity at a statistical level
- Detect and investigate tunneling, botnet command-and-control traffic, and other forms of covert communications being utilized in a network
- Accurately correlate multiple stages of malicious activity in order to build a complete picture of the scope and impact of a coordinated network intrusion

Skills Badges

Advanced Network Forensic Analysis

Network IOC Identification and Investigation

the details

- Virtual delivery available
- 5-day course
- Eligible for college credit
- 20+ investigation lab exercises
- 30 CPE/CEU credits

capstone exercise

Investigate and report on a complex, multi-stage intrusion. Prepare a report on the attack, document the hacker's activities, and detail the information that was leaked.

prerequisites

Thorough knowledge of TCP/IP networking

Successful completion of Network Forensics and Investigation course

PYTHON FOR NETWORK DEFENDERS

This course was created for novice programmers or those new to Python and designed for a very hands-on instructional experience. Students will learn the foundations of Python, including modules, classes, functions, object types, numeric types, strings, lists and dictionaries, statements, and more. The objective of this course is to equip attendees with skills they can immediately leverage to build powerful Python scripts. This course is a great starting point for security analysts seeking to automate repetitive or complex analytic tasks.

Key Outcomes

After successfully completing this course, students will be able to:

- Understand the foundational concepts of scripting and the Python language
- Use control statements, branching, and looping to establish flow in a script
- Employ modules and libraries to optimize code writing
- Ingest and analyze file inputs using input/output libraries and regular expressions
- Handle errors and exceptions gracefully
- Create simple graphical user interfaces
- Use simple networking functions such as creating sockets and sending email programmatically

the details

5-day course

Eligible for college credit

20 scripting lab exercises

30 CPE/CEU credits

capstone exercise

A programming assignment that includes the use of data structures, file and user I/O, condition/branching statements, functions, and exception handling.

prerequisites

Basic knowledge of TCP/IP networking

No previous programming experience is required

CYBER THREAT **HUNTING**

While good cyber hygiene, strong security policies, and finely tuned tools can detect and address many of the threats facing your organization, you need skilled cyber threat hunters to stalk and eliminate the threats that make it past your defenses. Experienced cyber threat hunters are difficult to find, but many of the incident responders and cyber analysts on your team can be trained to use the top threat hunting tools and techniques to track down your toughest adversaries. Our threat hunting courses teach students how to develop and use offensive security techniques and leverage threat intelligence to effectively target and eliminate malicious activity.

CORE SKILLS

- Threat Analysis
- Host/Network Investigation
- Log/Event Correlation
- Defining IOCs
- Writing/Tuning Rules & Signatures

> ***Experienced cyber threat hunters are difficult to find, but many of the cyber analysts on your team can be trained to use the top threat hunting tools and techniques to track down your toughest adversaries.***

KEY COURSES

Hacker Methodologies for Security Professionals

Cyber Threats Detection and Mitigation

THREAT HUNTER I

Level I Threat Hunters have the ability to proactively identify and track cyber threats in enterprise networks, extract indicators of compromise (IOCs), and incorporate these into new rules and signatures. They can synthesize their knowledge of offensive security tactics and sources of threat intelligence to anticipate and seek out malicious activity at multiple levels of the IT infrastructure stack.

Threat Hunter I Track

- Cyber Threat Analyst I Track
- Cyber Threat Analyst II Track
- Hacker Methodologies for Security Professionals
- Cyber Threat Detection and Mitigation
- **Demonstrated Skills**
  Threat Identification and Mitigation I Threat Analysis
  Host/Network Investigation

Related Skills Badges

THREAT HUNTER

Threat Hunters proactively look for signs of compromise through networks to detect, isolate, and address advanced threats that evade basic cyber defenses and programs. Threat Hunters often advance from Cyber Threat Analyst roles and have extensive knowledge of security monitoring tools, SIEM solutions, security analytics, scripting, compiled languages, TTPs, and operating systems. The top 25% of Threat Hunters earn $90,700 a year, and job opportunities for this role increased by 5% in 2018.

HACKER METHODOLOGIES FOR SECURITY PROFESSIONALS

Hacker Methodologies for Security Professionals teaches students the processes threat actors use to break into organizations' networks and steal their most sensitive data. Utilizing industry-standard penetration testing and auditing software, attendees will learn to identify, scan, and enumerate target systems; correlate services to vulnerabilities and exploits; employ exploits to gain access to the target systems; elevate privileges; propagate through the network; and cover their tracks within a target network. This course is focused primarily on Windows and Linux operating systems, so students should be comfortable with both.

Key Outcomes

After successfully completing this course, students will be able to:

- Identify the classes of hackers, their motivations, and the methodologies employed by threat actors
- Use publicly available tools and open source intelligence techniques to develop a target footprint
- Scan and enumerate targets to identify underlying operating systems and services
- Research and leverage exploits for vulnerable services to achieve access to target systems
- Identify system configuration weaknesses and viable privilege escalation tactics
- Analyze exploited systems to identify and remove indicators of compromise
- Employ system tools to exploit additional targets within an internal network

Skills Badges

Windows Exploitation

Linux Exploitation

Land & Expand

the details

Virtual delivery available

5-day course

10+ lab exercises

30 CPE/CEU credits

capstone exercise

Red team exercise requiring teams to establish initial access to a DMZ, pivot to other network segments, and retrieve requested information.

prerequisites

Familiarity with Windows or Linux command-line interfaces

Knowledge of TCP/IP networking

CYBER THREATS DETECTION AND MITIGATION

Taught by experts in network defense, this course equips attendees with the skills to build and maintain Intrusion Detection/Prevention Systems (IDS/IPS) and utilize advanced signature-writing techniques to defend large-scale network infrastructures. Students begin with writing basic IDS signatures to identify traffic of interest and advance to creating complex signatures in order to recognize distributed attacks, multi-stage events, and other more complex threats. The course will teach them how to apply decoding and other tools to overcome IDS evasion techniques, how to determine gaps in coverage, and how to manage rule sets to maintain system efficiency.

Key Outcomes

After successfully completing this course, students will be able to:

- Recognize the benefits and limitations of different IDS types (network- and host-based, and distributed systems)
- Identify optimal sensor placement and gaps in coverage
- Write basic IDS signatures to identify traffic of interest and tune them to reduce false positives
- Use reassembly and pre-processing engines to automatically reconstruct streams of network data prior to analysis
- Apply decoding and other tools to overcome IDS evasion techniques

Skills Badges

IDS Signature Creation & Optimization

Automated Network Threat Mitigation

the details

- Virtual delivery available
- 5-day course
- Eligible for college credit
- 20+ intrusion detection lab exercises
- 30 CPE/CEU credits

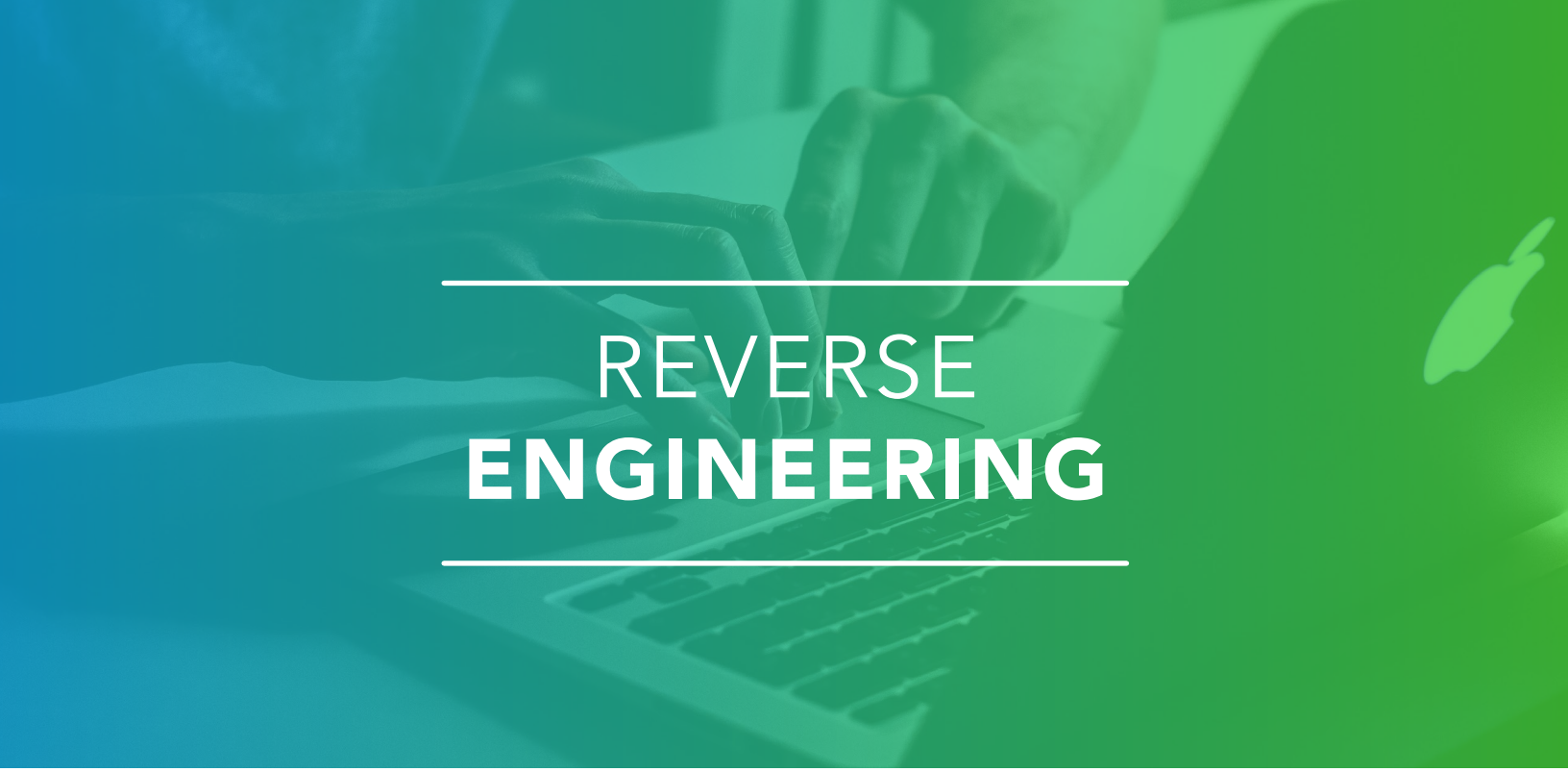
capstone exercise

Identify and analyze the various elements of a complex, multi-stage intrusion. Configure and tune an IDS/IPS to detect and mitigate these attacks, minimizing false positives and consolidating related alerts.

prerequisites

Strong understanding of TCP/IP networking

Successful completion of Malicious Network Traffic Analysis course



REVERSE ENGINEERING

In order to effectively defend against the most sophisticated threats, you need a deeper understanding of their design, behavior, and goals. Reverse engineering is a critical component of strong cybersecurity programs, using static, dynamic, automated, and often manual analysis to deconstruct large, complex binaries that threaten the organization. Our reverse engineering courses establish the skills your team needs to dissect malicious binaries and develop specialized de-obfuscation, categorization, and exploitation techniques that allow for more targeted analysis.

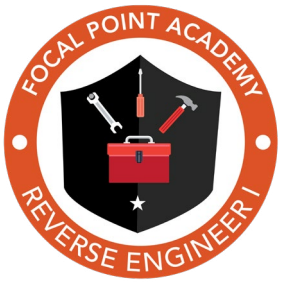
CORE SKILLS

- Malware Reverse Engineering
- Kernel Security Analysis
- Specialized Reverse Engineering
- Malicious Code Identification
- Automating Analysis

> ***In order to effectively defend against the most sophisticated threats, you need a deeper understanding of their design, behavior, and goals.***

KEY COURSES

- Intro to C Programming
- Intro to C++
- Python Reverse Engineering
- Assembly for Reverse Engineers
- Linux/C++ Reverse Engineering
- Linux Kernel Internals
- Malware Reverse Engineering
- Windows Rootkit Reverse Engineering



REVERSE ENGINEER I

Level I Reverse Engineers can analyze unobfuscated assembly code to determine the scope and capabilities of a given binary. They understand program flow, data structures and other programming concepts, and can assert their knowledge in a systematic approach to break up larger programs/systems for analysis.

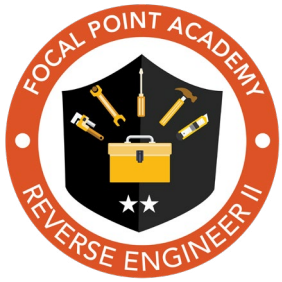
Reverse Engineer I Track

- Behavioral Malware Analysis*
- Windows or Live System Analysis*
- Assembly for Reverse Engineering
- Malware Reverse Engineering

Demonstrated Skills
Reverse Engineering | Endpoint Threat Analysis
Behavioral Malware Analysis

* See Cyber Threat Analysis.

Related Skills Badges



REVERSE ENGINEER II

Level II Reverse Engineers have advanced reverse engineering skills and are able to use a combination of static and dynamic techniques to efficiently reverse engineer large or complex binaries that may include API obfuscation and other anti-analysis techniques. They can also implement objective-oriented analysis to focus on specific portions or behaviors within a program.

Reverse Engineer II Track

- Assembly for Reverse Engineering
- Malware Reverse Engineering
- Python Reverse Engineering
- Linux/C++ Reverse Engineering

Demonstrated Skills
Reverse Engineering | Endpoint Threat Analysis
Behavioral Malware Analysis | IDAPython
X64 Assembly | X86 Assembly

Related Skills Badges

INTRO TO C PROGRAMMING

C is one of the oldest and yet most widely used high-level programming languages in the world today. This course covers the fundamental principles of programming in this essential language. Suitable for beginners, it starts with the basics of programming languages, program structure, and programming concepts before progressing to topics such as variables and scope, arithmetic operators, control flow, basic I/O, and using libraries. By the end of this course, students should be able to write, compile, and execute C programs that perform a variety of functions involving file and user I/O, data structures, algorithmic data manipulation, memory management, and more.

Key Outcomes

After successfully completing this course, students will be able to:

- Describe the difference between compiled and interpreted languages
- Create a development environment for programming in C
- Declare, initialize, and use variables of appropriate types
- Use arrays, pointers, and strings to manage data within a program
- Construct logical program flow using conditional statements, branching, and looping
- Perform logical and mathematical operations on variables
- Build and use data structures
- Use libraries to perform simple I/O and memory management tasks

Skills Badges

Development of
Standard C Programs

the details

5-day course

10+ programming lab exercise

30 CPE/CEU credits

capstone exercise

A programming assignment that includes the use of dynamic memory allocation, pointers, control structures, file I/O, and condition statements, as well as design decisions for data storage.

prerequisites

Familiarity with Windows or Linux command-line interface

Basic knowledge of TCP/IP networking

INTRO TO C++

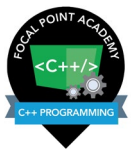
This course introduces the student to the core concepts of object-oriented programming and equips them to implement these concepts in the C++ programming language. Starting with the foundations of classes, objects, inheritance, and polymorphism, the course covers a wide range of techniques and is designed for those who are new to object-oriented programming.

Key Outcomes

After successfully completing this course, students will be able to:

- Describe the differences between object-oriented programming and other paradigms
- Declare, define, and use classes in C++
- Write programs that implement arrays, pointers, functions, and data structures in an object-oriented context
- Implement function overloading
- Create and use abstract data types
- Use virtual functions to implement polymorphism
- Correctly handle runtime exceptions

Skills Badges



Development of Standard C++ Programs

the details

5-day course

10+ lab exercises

30 CPE/CEU credits

capstone exercise

Programming assignment that includes the use of class design, operator overloading, I/O streams, STL containers, and considerations for object serialization, while encouraging a multi-paradigm programming approach.

prerequisites

Intro to C Programming (or comparable experience)

Basic knowledge of TCP/IP networking

ASSEMBLY FOR REVERSE ENGINEERS

Many analysts and programmers have not had the time or opportunity to learn assembly language, yet this is a skill that will save them precious time when effective analysis is needed the most. Designed for malware analysts and code developers alike, Assembly for Reverse Engineers will equip students with the know-how to effectively read assembly, review statements, understand program flow, identify the influence of different compilers, and reverse machine code back to its higher-level equivalent. They will learn and practice development techniques to improve the speed and quality of static analysis.

Key Outcomes

After successfully completing this course, students will be able to:

- Describe how code execution works
- Understand the components of the x86 instruction set
- Apply demonstrated analysis techniques to the reverse engineering of Windows executables
- Use IDA Pro's powerful assembly markup features to optimize analysis
- Use static and dynamic analysis to interpret and document program flow

Skills Badges

Reverse Engineering User-Mode x86 Windows Binaries

Static Reverse Engineering I

the details

5-day course

20+ lab exercises

30 CPE/CEU credits

capstone exercise

Two-part capstone including a manual stack trace exercise and a reverse engineering assignment to discover and document the function of a given binary.

prerequisites

Experience with C programming in a Windows environment

Successful completion of Understanding Operating Systems course (or equivalent knowledge)

MALWARE REVERSE ENGINEERING

Malware Reverse Engineering builds on the knowledge and skills from the Assembly for Reverse Engineers course and teaches students how to perform more advanced analysis of real-world malware samples. The primary techniques taught are disassembly and debugging. The course also covers topics such as data decoding and binary obfuscation in order to bypass protections and perform effective analysis on hardened samples; dealing with destructive malware; and defeating anti-debugging and other anti-analysis techniques.

Key Outcomes

After successfully completing this course, students will be able to:

- Use IDA Pro, OllyDbg, x64dbg, and other tools to analyze and debug malware, and report on its capabilities
- Describe in detail the structure and functions of the Portable Executable (PE) header, and analyze PE headers to aid in malware characterization
- Apply techniques for identifying, analyzing, and bypassing data obfuscation
- Understand the structure and use of Dynamic Linked Libraries (DLLs) and apply reverse engineering skills to DLL analysis
- Identify and overcome a range of anti-debugging and anti-analysis techniques used in modern malware
- Identify developer code in a compiled binary

Skills Badges

Reverse Engineering User-Mode Windows Malware

Static Reverse Engineering II

Dynamic Reverse Engineering

the details

Virtual delivery available

5-day course

20+ lab exercises

30 CPE/CEU credits

capstone exercise

Reverse engineering assignment to analyze and report on a real-world malware sample that employs anti-analysis techniques.

prerequisites

Successful completion of Assembly for Reverse Engineers course

Experience in C programming

Strong understanding of operating system internals

LINUX KERNEL INTERNALS

Linux Kernel Internals teaches students all the fundamental requirements necessary to understand and start developing for the Linux kernel. Attendees will go deep into the internals of the Linux operating system and begin to develop kernel modules for the latest popular distributions. From kernel module implementation to memory and process management, including I/O, debugging, file systems, and kernel security mechanisms, this course is all-encompassing.

Key Outcomes

After successfully completing this course, students will be able to:

- Set up a development environment for Linux
- Describe in detail how the Linux kernel functions
- Develop Linux kernel modules that interact with I/O, memory, processes and threads, file systems, and networking
- Detect and analyze obfuscation methods used by attackers to evade detection

the details

5-day course

20+ programming lab exercises

30 CPE/CEU credits

capstone exercise

Build a rootkit to a set of given functional requirements, implemented as a Linux kernel module.

prerequisites

Experience in C programming

Knowledge of systems programming in a UNIX-based environment

Familiarity with standard UNIX tools such as vi, Emacs, and gcc

PYTHON FOR REVERSE ENGINEERS

Python Reverse Engineering is geared towards the reverse engineer and introduces the Python language with a focus on using it to accelerate, automate, and optimize reverse engineering tasks. The course begins with an introduction to Python and a review of object types and flow statements, and then delves into file operations, modules, working with the CTypes library for interaction with Windows operating systems, debugging, and IDA scripting.

Key Outcomes

After successfully completing this course, students will be able to:

- Compose Python scripts to automate repetitive tasks
- Perform tasks with the Windows API from Python using the CTypes library
- Implement a scriptable Windows debugger using Python and CTypes
- Use the IDAPython API to automate common reverse engineering tasks in IDA

Skills Badges

Python Script Development

Windows Debugger Development

Scripting IDA with Python

the details

5-day course

20+ lab exercises

30 CPE/CEU credits

capstone exercise

In a three-part lab, students will build a pure Python Windows debugger implementation from scratch for automating reverse engineering tasks.

prerequisites

Successful completion of Malware Reverse Engineering course

Familiarity with programming/ scripting in some language

LINUX/C++ REVERSE ENGINEERING

This course enables the skilled malware analyst to branch into the less mainstream (but equally important) areas of reversing C++ binaries and Linux binaries. After a review of assembly, including a deeper dive into the differences between x86 and x64 architectures, students will learn about C++ calling conventions, classes, objects, and exception handling and how these affect reverse engineering. The course then turns to the Linux operating system, covering topics such as kernel structure and the Linux Application Binary Interface (ABI) in preparation for statically analyzing and debugging Linux executables and malware.

Key Outcomes

After successfully completing this course, students will be able to:

- Understand the implications of features from high-level languages at the assembly level
- Recognize and analyze the structure of C++ binaries
- Describe the Linux System V ABI, including how processes and threads are executed in Linux
- Understand the structure of the Linux Executable and Linkable Format (ELF)
- Statically analyze Linux binaries using IDA and other tools
- Debug Linux binaries using GDB and the IDA Remote Debugger

Skills Badges

Reverse Engineering C++ Programs

Reverse Engineering User-Mode x64 Binaries

Reverse Engineering User-Mode Linux Binaries

the details

5-day course

15+ lab exercises

30 CPE/CEU credits

capstone exercise

Reverse engineering assignment to analyze an extensive sample that makes substantial use of C++ library objects, object composition, and inheritance relationships in a Linux-based environment.

prerequisites

Successful completion of Malware Reverse Engineering course and reverse engineering experience in a Windows environment

Strong understanding of operating system internals

WINDOWS ROOTKIT REVERSE ENGINEERING

This course takes students into advanced and specialist topics surrounding rootkit analysis. Students will learn about the Windows kernel, automated and manual unpacking, live kernel debugging with IDA and WinDbg, and reverse engineering drivers. This is a heavily lab-intensive course that requires students to have a solid background in programming, reverse engineering, and malware analysis prior to attending.

Key Outcomes

After successfully completing this course, students will be able to:

- Unpack malware using both automated tools and manual processes
- Analyze and defeat mechanisms added by code protectors
- Conduct live remote kernel debugging on Windows using WinDbg and IDA
- Reverse engineer rootkits that are implemented as drivers

Skills Badges

Reverse Engineering Kernel-Mode Windows Malware

Debugging Windows Drivers

the details

5-day course

20+ lab exercises

30 CPE/CEU credits

capstone exercise

Reverse engineering assignment to fully analyze and report on a real-world Windows rootkit.

prerequisites

Successful completion of Malware Reverse Engineering course

Strong programming and reverse engineering experience

Comprehensive understanding of Windows OS internals

READY TO ADVANCE YOUR CYBERSECURITY TEAM?

Focal Point Academy's workforce development specialists are here to help. Let's build a cybersecurity team equipped to handle the threats you're facing today, and those you'll face in the future. From designing your strategy to training and testing each team member, we're right here to guide you and your team every step of the way.

WORK WITH US:


focal-point.com/academy


800-969-7770


academy@focal-point.com

FOCAL POINT

ACADEMY