



FOCAL POINT
ACADEMY

THE 2019 COURSE CATALOG

A guide to taking your cyber
security team to the next level

CONTENTS

Cyber Workforce Development 3

Skills Pyramid 4

Learning Tracks 5

How to Use This Catalog 6

Analyst Foundations 7

Intro to Cyber Security **8**

Intro to Cyber Risk Management **9**

Understanding Operating Systems **10**

Windows System Analysis **11**

Live System Analysis **12**

Behavioral Malware Analysis **13**

Network Traffic Analysis **14**

Python for Network Defenders **15**

Analytic Methodologies 16

Malicious Network Traffic Analysis **17**

Cyber Threats Detection and Mitigation **18**

Assembly for Reverse Engineers **19**

Malware Reverse Engineering **20**

Hacker Methodologies for Security Professionals **21**

Advanced Specialties 22

Linux Kernel Internals **23**

Linux/C++ Reverse Engineering **24**

Windows Rootkit Reverse Engineering **25**

Supplemental Courses 26

Intro to C Programming **27**

Intro to C++ **28**

CYBER WORKFORCE DEVELOPMENT

Focal Point Academy's mission is to build better, faster, more agile cyber security 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 cyber security 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.

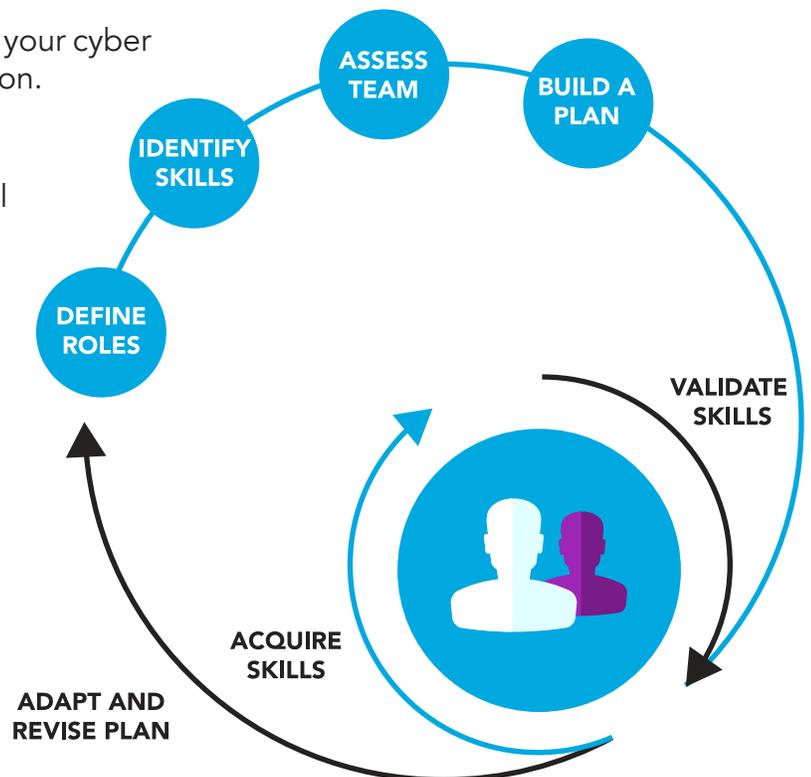
Improve employee retention.

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.

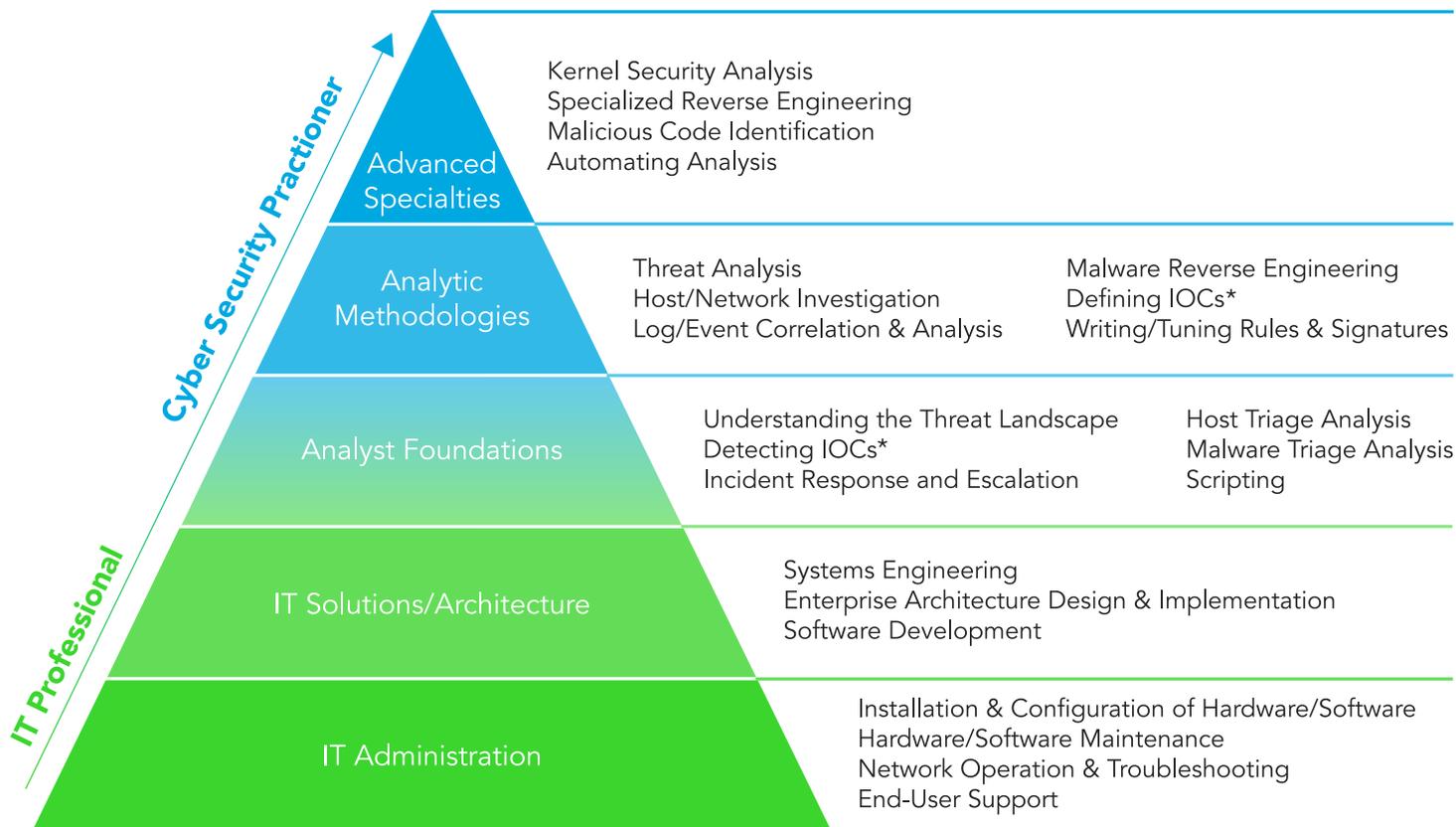
To us, workforce development is the process of defining, measuring, and training your cyber security team, and building a long-term strategy to guarantee that their skills remain aligned with the threats facing your organization.





SKILLS PYRAMID

Every career in cyber security 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 cyber security 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

LEARNING TRACKS

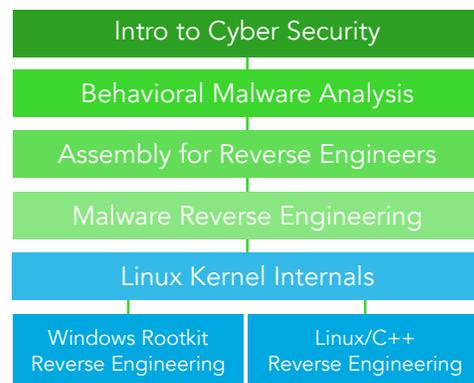
Learning tracks help you see where your team can go with Focal Point Academy. These aren't prescriptive paths to success, but simply suggestions on how your team can reach the next level.



Olivia
Software Developer

Olivia is a software developer who has been with her company for 6 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, and then a further goal to specialize in kernel-level analysis of either Windows or Linux systems.

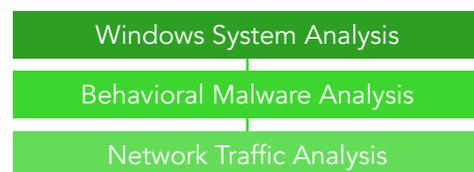
Reverse Engineer Track



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 cyber security 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 SOC Analyst Level I over a period of 9 months.

SOC Analyst I Track



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 2 years of experience at the company, and he scored highly in an assessment designed to identify suitable resources for a new threat-hunting team. Sam, along with 5 teammates, will be participating in a development program over the next 18 months to enable this critical new function.

Threat Hunter Track



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 cyber security skills they need to advance their careers and strengthen your team. Courses align with three key stages in a cyber career: those who are just entering the realm of cyber security (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 cyber security engineer and cyber threat hunter.

While the skills obtained in these courses are all essential for a well-rounded cyber security team, they may not be right for each individual cyber security 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



lab
exercises



college
credit



course
length



CPE/CEU
credits*

* up to 35 credits for a 5-day course

ANALYST FOUNDATIONS

Less than 30% of cyber security professionals start their careers in cyber, instead beginning their journeys in areas like IT, accounting, software development, and even the arts. You don't have to be born with the coding skills of a seasoned hacker to have a successful career in cyber security. What your SOC team needs are problem solvers, creative thinkers, strategists, and those with passion and drive. The technical skills can be trained. These foundational courses are designed to provide non-cyber professionals with the baseline skills they need to transition into a cyber career.

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 cyber security.

KEY COURSES

Intro to Cyber Security

Windows System Analysis

Network Traffic Analysis

Intro to Cyber Risk Management

Live System Analysis

Python for Network Defenders

Understanding Operating Systems

Behavioral Malware Analysis

INTRO TO CYBER SECURITY

Introduction to Cyber Security 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 cyber security.

Key Outcomes

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

- Recognize cyber security 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



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.

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 cyber security 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 details



1-day course



Group exercises and personal cyber hygiene



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.

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



5-day course



20+ lab exercises



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

the details



5-day course



20 investigation lab exercises



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

the details



5-day course



20 investigation lab exercises



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

the details



5-day course



Eligible for college credit



20+ malware analysis exercises exercise



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 TRAFFIC ANALYSIS

Network Traffic Analysis 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

the details



5-day course



Eligible for college credit



20 analytic lab exercises



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

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



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



ANALYTIC METHODOLOGIES

To identify, contain, and remediate cyber attacks, a cyber analyst needs both a honed skill set and a proven method of approach. Through our Analytic Methodologies courses, cyber professionals will gain the skills needed to be highly capable and effective incident responders, event handlers, threat hunters, and investigators. These courses train your team to defend against relentless attackers by gathering and analyzing threat intelligence; employing proactive methodology to identify indicators of compromise (IOCs); and building, customizing, or extending their toolsets to automate their craft.

CORE SKILLS

Threat Analysis

Host/Network Investigation

Log/Event Correlation

Malware Reverse Engineering

Defining IOCs

Writing/Tuning Rules & Signatures

// To identify, contain, and remediate cyber attacks, a cyber analyst needs both a honed skill set and a proven method of approach.

KEY COURSES

Malicious Network Traffic Analysis

Cyber Threats Detection and Mitigation

Assembly for Reverse Engineers

Hacker Methodologies for Security Professionals

Malware Reverse Engineering

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

the details



5-day course



Eligible for college credit



20+ investigation lab exercises



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 Traffic Analysis](#) course

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

the details



5-day course



Eligible for college credit



20+ intrusion detection lab exercises



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

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

the details



5-day course



20+ lab exercises



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

the details



5-day course



Eligible for college credit



20+ lab exercises



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

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

the details



5-day course



10+ lab exercises



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

ADVANCED SPECIALTIES

Sometimes an organization needs to go above and beyond standard incident response procedures and conduct a deep investigation into a compromised system. These specialty courses are designed for experienced analysts, enabling them to investigate complex or targeted threats.

CORE SKILLS

Kernel Security Analysis

Specialized Reverse Engineering

Malicious Code Identification

Automating Analysis

// Sometimes an organization needs to go above and beyond standard incident response procedures and conduct a deep investigation into a compromised system.

KEY COURSES

Linux Kernel Internals

Linux/C++ Reverse Engineering

Windows Rootkit Reverse Engineering

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



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

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

the details



5-day course



15+ lab exercises



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](#) 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

the details



5-day course



20+ lab exercises



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](#)

Strong programming and reverse engineering experience

Comprehensive understanding of Windows OS internals

SUPPLEMENTAL
COURSES

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

the details



5-day course



10+ programming lab exercise



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

the details



5-day course



10+ lab exercises



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

READY TO BUILD THE BEST CYBER SECURITY TEAM IN THE GALAXY?

Focal Point Academy's workforce development specialists are here to help. Let's build a cyber security 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



FOCAL POINT
DATA RISK

Focal Point Data Risk® is a registered trademark of Focal Point Data Risk, LLC.