CYBER DEFENSE TRAINING

TRAINING PROGRAMS

What Is Cyber Defense Training?

Our cyber defense training courses teach the skills you need to combat the cyber threats you face today—and emerging threats you will face tomorrow. Topics include computer and network exploitation methodologies, packet analysis, network traffic analysis, malware forensics, malware analysis, and reverse engineering malware. We also introduce programming and scripting concepts in languages such as Python, Java, C++, and C# that are fundamental in malware analysis, reverse engineering, and digital forensics.

Why Choose CISO Global?

Our trainers are highly skilled industry veterans with decades of experience working in the cybersecurity and IT fields. They hold the most important cybersecurity-related certifications, including those from (ISC)2 and CompTIA. They have taught in-person and online, delivering cybersecurity training to corporate, military, government, and higher education students. You receive hands-on training with relevant industry tools and techniques that incorporate real-life cyber threat scenarios, so you can detect, diagnose, and mitigate a range of exploits and attacks.

Our cyber defense training program stands out because of our approach:

- Our trainers bring with them decades of cybersecurity expertise combating many cyber threats as well as years of training others to do the same.
- You will train using the same tools and techniques you use to fight the cyber threats your organization is likely to face.
- Course content is engaging, challenging, constantly updated, and relevant to current and emerging cyber threats.

Professional–Grade Cyber Defense **Skills Training**

CISO GLOBAL

480-389-3444 | ciso.inc

CISO Global Teaches These Cyber Defense Skills

Computer and Network Exploitation Methodologies (1 day)

This course provides you with an overview of penetration testing, red teaming, vulnerability analysis, and exploitation methods that you practice using directed hands-on exercises.

Packet Analysis (1 day)

This course teaches you the fundamental concepts, methodologies, and tools necessary to analyze network traffic for the purposes of intrusion and threat detection, network defense, and low-profile offensive operations. The course begins with an introduction of the role of network packet analysis in computer network operations and progresses to a detailed discussion of the TCP/IP protocol suite and ethernet network operations. You will practice using a protocol analyzer to capture and analyze self-generated network traffic. You will learn how to examine packet captures, which illustrate various exploits, network reconnaissance techniques, and more advanced network attacks.

Network Traffic Analysis (5 days)

This course provides you an overview of best practices in analyzing malicious network traffic. You will acquire a fundamental understanding of a variety of network-based malware analysis tools and techniques that can directly support your organization's incident response efforts and increase your performance in your functional role(s). You will be given real-world packet capture samples to dissect in a controlled environment.

Malware Forensics (5 days)

This course teaches you the fundamental requirements necessary to analyze malicious software from a behavioral perspective. You will observe malware in a controlled environment using system monitoring tools to analyze malicious affects to systems. You will analyze a wide variety of current threats, from simple keyloggers to massive botnets, using real-world samples. Survey level – no experience in coding required.

Basic Malware Analysis (5 days)

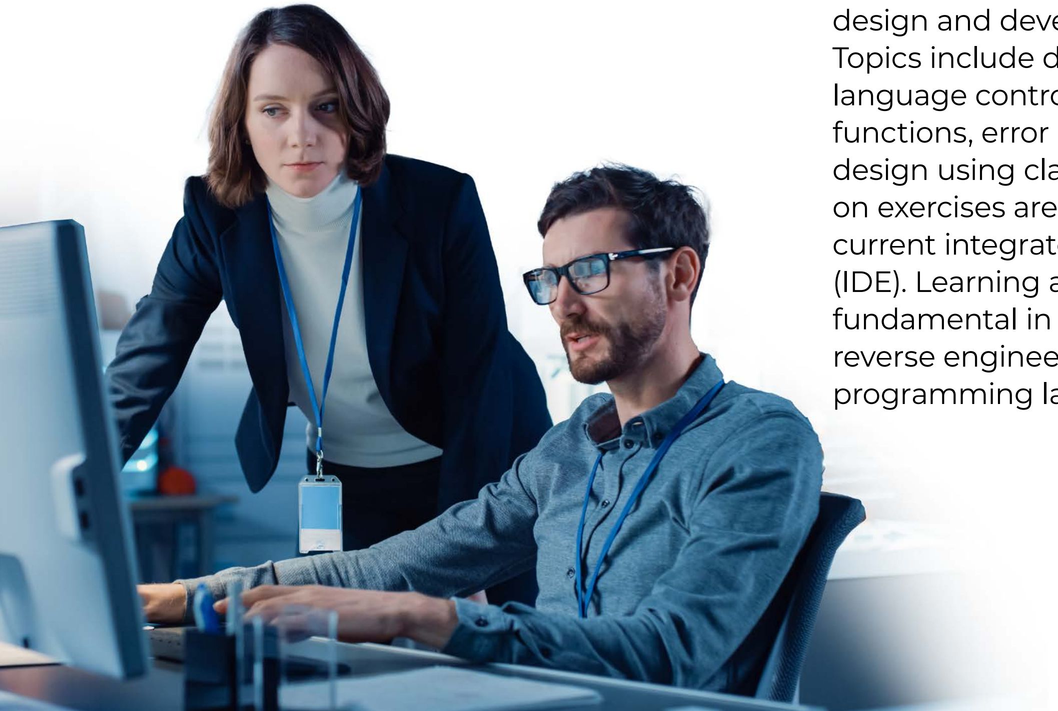
This course teaches you the fundamentals of analyzing malicious code. It focuses on static malware analysis and touches on dynamic malware analysis. Dissect real-world malicious code samples in a controlled environment. Beginner level – some coding experience recommended. View additional courses in coding/programming.

Intermediate Malware Analysis (4 days)

Building on Basic Malware Analysis, this course focuses on dynamic malware analysis using three critical tools for successful malware analysis: disassemblers, decompilers, and Windows SysInternals. You will identify host-based and network-based indicators of compromise and Windows APIs often used by malware authors. You will be given real-world malicious code samples to dissect in a controlled environment. Intermediate level – completing our Basic Malware Analysis course and some coding experience recommended. View the options below for courses in coding/programming.

Reverse Engineering Malware (5 days)

Building on Intermediate Malware Analysis, this course dives deeper into performing dynamic malware analysis using a debugger. You will learn how to identify exactly what a malware sample does and how it does it. You will learn how to patch the sample to make sections inactive or crack the program to allow full access to areas hidden or encrypted by the malware author. You will be given real-world malicious code samples to dissect in a controlled environment. Intermediate level – completing our Intermediate Malware Analysis course and some coding experience recommended. View the options below for courses in coding/programming.



Regular Expressions (1 day)

This course teaches you how to use regular expressions to search through larger collections of data quickly and efficiently.

Burp Suite Pro (2 days)

This course teaches you how to use the popular vulnerability scanning tool Burp Suite Pro that enables you to easily find vulnerabilities in web applications. You will also be exposed to the differences between Burp Suite's Community Edition and Professional (Pro) Edition.

Introduction to Python Scripting (2 days)

This course introduces you to Python scripting, a popular language used in cybersecurity. You will do practical exercises that teach you the aspects of scripting in this language. Topics include data types, operators, collections, external modules, functions, error handling, and analyzing data files. Hackers and penetration testers often use Python scripts in their activities. No previous experience with programming languages is required.

Introduction to Java Programming (5 days)

This course introduces you to Java programming language and software development problem-solving methodologies using current software design and development tools and techniques. Topics include data structures, program design, language control structures, procedures and functions, error handling, and object-oriented design using classes and inheritance. Hands-on exercises are developed in Java using a current integrated development environment (IDE). Learning a programming language is fundamental in performing malware analysis and reverse engineering. No previous experience with programming languages is required.

Introduction to C++ Programming (5 days)

This course introduces you to C++ programming language and software development problem-solving methodologies using current software design and development tools and techniques. Topics include data structures, program design, language control structures, procedures and functions, error handling, and object-oriented design using classes and inheritance. Hands-on exercises are developed in C++ using a current integrated development environment (IDE). Learning a programming language is fundamental in performing malware analysis and reverse engineering. No previous experience with programming languages is required.

Introduction to C# Programming (5 days)

This course introduces you to C# programming language and software development problem-solving methodologies using current software design and development tools and techniques. Topics include data structures, program design, language control structures, procedures and functions, error handling, and object-oriented design using classes and inheritance. Hands-on exercises are developed in C# using a current integrated development environment (IDE). Learning a programming language is fundamental in performing malware analysis and reverse engineering. No previous experience with programming languages is required.

STRATEGY & RISK

- Gap Analysis
- Audit/Assessment
- Third Party Risk Management
- FedRAMP
- StateRAMP
- CMMC
- Advisory
- Virtual CISO
- Managed Compliance
- Managed GRC

CYBER DEFENSE OPERATIONS

- Extended Detection & Response
- Managed Detection & Response
- SIEM as a Service
- Threat Hunting
- Cyber Threat Intelligence
- Digital Forensics
- Vulnerability Management Program
- Attack Surface Reduction
- Cyber Incident Response

CISO

SECURITY ARCHITECTURE & ENGINEERING SOLUTIONS

- Secured Managed Services
- Advanced Firewall Management
- Identity & Access Management
- Cloud Security
- Data Protection
- Remediation

READINESS & RESILIENCY

- Penetration Testing
- Tabletop Exercises with Incident Response Retainer
- Training Programs

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations ™

SOC 2® Type II Audited

CISO GLOBAL

480-389-3444 | ciso.inc