HACKINETIX ACADEMY

MASTERING THE CYBER FLOW

PROFESSIONAL COURSE

Ethical Hacking Expert

(H|EHE)

Detailed Course Curriculum

Advanced skills to identify, exploit and mitigate vulnerabilities in systems, networks and applications.



DURATION
200 Hours

CURRICULUM
11 Levels

MODULES
59 Modules

OUTCOMES
257 Learning Outcomes

MASTERING THE CYBER FLOW

www.hackinetix.com | info@hackinetix.com

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

COURSE OVERVIEW

Course Overview

The Ethical Hacking Expert course is a comprehensive program designed to equip learners with advanced skills to identify, exploit, and mitigate vulnerabilities in systems, networks, and applications. This course delves into the methodologies and tools used by ethical hackers to simulate cyberattacks and strengthen an organization's security posture.

200 Hours
Duration

11
Levels

59
Modules

257
Learning Outcomes

Who Should Enroll in this Program?

The Ethical Hacking Expert program is designed for individuals interested in advanced cybersecurity skills and ethical hacking and penetration testing careers. Here's a detailed breakdown of who should consider enrolling:

IT and Security Professionals

Cybersecurity Specialists

Students and Recent Graduates

PROGRAM ELIGIBILITY CRITERIA

Eligibility & Prerequisites

01 Educational Background (Preferred but not mandatory)

02 No specific work experience is mandatory, but familiarity with IT systems, networking, or cybersecurity is advantageous.

Course Roadmap

11 levels · 59 modules · 257 learning outcomes

01 **Cybersecurity Fundamentals** — 5 Modules · 6 Days · 10 Hours — p. 05

02 **Advanced Penetration Testing** — 6 Modules · 12 Days · 24 Hours — p. 07

03 **Web Application Security & Bug Bounty Hunting** — 9 Modules · 12 Days · 24 Hours — p. 09

04 **Cyber Forensics Investigation** — 6 Modules · 8 Days · 16 Hours — p. 12

05 **Mobile Application Pentesting & Bug Bounty Hunting** — 5 Modules · 10 Days · 10 Hours — p. 14

06 **Exploit Development** — 6 Modules · 13 Days · 26 Hours — p. 16

07 **Malware Analysis** — 5 Modules · 10 Days · 20 Hours — p. 18

08 **SoC Analysis** — 4 Modules · 8 Days · 10 Hours — p. 20

09 **Threat Intelligence** — 4 Modules · 8 Days · 10 Hours — p. 22

10 **Python for Security** — 5 Modules · 10 Days · 20 Hours — p. 24

11 **AI in Cybersecurity** — 4 Modules · 4 Days · 8 Hours — p. 26

PROGRAM OUTCOMES

Program Outcomes

01 Understand the fundamentals of ethical hacking and cybersecurity principles.

02 Master tools and techniques used in penetration testing and vulnerability assessment.

03 Learn to exploit security flaws in various environments, including networks, web applications, and wireless systems.

04 Develop skills in bypassing security controls and implementing countermeasures.

05 Gain knowledge of legal and ethical considerations in hacking practices.

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 01 — 6 Days · 10 Hours

Cybersecurity Fundamentals

01

The core ideas, guidelines, and procedures necessary for safeguarding digital systems and data are presented in Cybersecurity Fundamentals. The CIA triad, typical cyber threats, security tools, network protection, risk management, and legal and ethical issues are among the fundamental subjects covered in the course. While investigating the role of human behavior and emerging technology in cybersecurity, learners will acquire knowledge on how to detect vulnerabilities, reduce risks, and handle incidents. This course gives students the information and abilities they need to improve their personal and corporate digital security or provide a solid foundation for a career in cybersecurity.

Key Learning Outcomes

- Define cybersecurity and explain its importance in the modern digital world.
- Understand the importance of adopting security best practices in personal and professional environments.
- Explore emerging threats and technologies such as AI in cybersecurity and quantum computing risks.
- Recognize key cybersecurity regulations and compliance standards (e.g., GDPR, CCPA, HIPAA).
- Gain familiarity with widely recognized frameworks (e.g., NIST Cybersecurity Framework, ISO/IEC 27001).
- Learn about basic tools used for threat detection and prevention (e.g., firewalls, antivirus software, and intrusion detection systems).
- Learn the steps involved in responding to cybersecurity incidents.
- Learn the basics of threat modelling to identify potential attack vectors.

Curriculum

5 modules · 20 learning outcomes

01 Introduction to Cybersecurity

- LO 1 What is Cybersecurity?
- LO 2 Describe Key Cybersecurity Domains
- LO 3 Key Concepts: Confidentiality, Integrity, and Availability (CIA Triad)
- LO 4 The Cybersecurity Landscape: Threat Actors and Motivations

02 Common Cyber Threats and Attacks

- LO 1 Malware: Viruses, Worms, Trojans, Ransomware
- LO 2 Phishing and Social Engineering Attacks
- LO 3 Denial-of-Service (DoS) and Distributed DoS (DDoS) Attacks
- LO 4 Insider Threats

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 01

Cybersecurity Fundamentals

Curriculum (continued)

03 Cybersecurity Frameworks and Standards

- LO 1 Overview of NIST Cybersecurity Framework
- LO 2 ISO/IEC 27001 Basics
- LO 3 Compliance Standards: GDPR, HIPAA, PCI DSS
- LO 4 Best Practices for Cybersecurity Management

04 Risk Management and Threat Modelling

- LO 1 Identifying and Assessing Cyber Risks
- LO 2 Fundamentals of Threat Modelling (e.g., STRIDE, DREAD)
- LO 3 Implementing Risk Mitigation Strategies
- LO 4 Importance of Cybersecurity Policies

05 Emerging Trends and Future of Cybersecurity

- LO 1 Artificial Intelligence and Machine Learning in Cybersecurity
- LO 2 IoT Security Challenges
- LO 3 Quantum Computing Risks
- LO 4 Global Cybersecurity Trends

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 02 — 12 Days · 24 Hours

Advanced Penetration Testing

A specific course called Advanced Penetration Testing is intended to give experts in-depth information and cutting-edge methods for mimicking complex cyberattacks. The course covers complex subjects such as advanced reconnaissance, enterprise system exploitation, post-exploitation strategies, wireless and Internet of Things security, and red team operations. In addition to conducting thorough vulnerability assessments, participants will learn how to circumvent contemporary security measures and replicate advanced persistent attacks (APTs). This course equips students to handle complex security issues and enhance organizational resilience against sophisticated cyber threats by placing heavy emphasis on ethical hacking, real-world scenarios, and emerging threats.

Key Learning Outcomes

- Perform detailed information gathering using OSINT and advanced enumeration tools.
- Escalate privileges and establish persistence across diverse platforms.
- Simulate Advanced Persistent Threats (APTs) to assess organizational resilience.
- Create and deploy advanced payloads using frameworks like Metasploit and custom scripts.
- Perform advanced attacks on wireless networks, IoT devices, and embedded systems.
- Understand the legal implications of penetration testing in different jurisdictions.

Curriculum

6 modules · 20 learning outcomes

01 Advanced Information Gathering Using OSINT

- LO 1 Passive and Active Reconnaissance Techniques
- LO 2 Advanced OSINT (Open-Source Intelligence) Methods
- LO 3 Enumeration of Services, Ports, and Applications

02 Advanced Exploitation Techniques

- LO 1 Exploiting Operating System Vulnerabilities
- LO 2 Bypassing Antivirus (Evasion Techniques)
- LO 3 Exploiting Zero-Day Vulnerabilities
- LO 4 Public or Private Exploits and CVE Exposures Tools

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 02

Advanced Penetration Testing

Curriculum (continued)

03 Privilege Escalation and Post Exploitation Techniques

- LO 1 Post Exploitation Techniques
- LO 2 Maintaining Access with Persistence Mechanisms
- LO 3 Privilege Escalation (Windows and Linux)

04 Exploiting Enterprise Systems

- LO 1 Active Directory Attacks: Kerberos Abuse, Golden/Silver Tickets
- LO 2 Cloud Penetration Testing: AWS, Azure, Google Cloud
- LO 3 Common Enterprise Cybersecurity Threats

05 Red Team Operations

- LO 1 Red Team Fundamentals
- LO 2 Client-Side Exploitations
- LO 3 Network Security Evasion
- LO 4 Command and Control (C2) Frameworks and Infrastructure

06 Advanced Social Engineering

- LO 1 What is Social Engineering
- LO 2 Advanced Vishing and Smishing Techniques
- LO 3 Creating Realistic Phishing Campaigns

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 03 — 12 Days · 24 Hours

Web Application Security & Bug Bounty Hunting

Web Application Security focuses on the principles, techniques, and tools necessary to secure web applications against modern threats. The course addresses common vulnerabilities such as those outlined in the OWASP Top 10, including SQL Injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF). Learners will explore topics such as secure authentication, API security, input validation, encryption, and secure development practices. With hands-on exercises and practical tools like Burp Suite and OWASP ZAP, this course equips participants to identify, mitigate, and prevent web-based attacks, ensuring the resilience and integrity of web applications in dynamic environments.

Key Learning Outcomes

- Understand Web Application Security Fundamentals
- Master Authentication and Authorization Security
- Mitigate Input Validation and Injection Attacks
- Apply Tools and Techniques for Web Application Security
- Respond to Incidents Effectively
- Stay Updated with Emerging Security Trends

Curriculum

9 modules · 49 learning outcomes

01 Techniques for Testing Web Applications

- LO 1 Introduction to Web Application Testing
- LO 2 OWASP Top 10
- LO 3 SANS Top 25 Vulnerabilities
- LO 4 Common Weakness Enumeration (CWE) Vulnerabilities
- LO 5 Bug Bounty Platforms Like Bug Crowd and HackerOne
- LO 6 Bug Hunting Penetration Testing Lab Setup

02 Essential Reconnaissance Methods for Bug Hunters

- LO 1 Manual Subdomain Identification and Analysis
- LO 2 Recon Automation Using Bash Shell Scripting
- LO 3 Reconnaissance Techniques: Active and Passive
- LO 4 Recognizing Web Application Frameworks and Technologies
- LO 5 Offensive Approach to Hunt Bugs
- LO 6 Techniques for Identifying Sensitive Endpoints
- LO 7 Information Gathering Framework (OSINT)
- LO 8 Analysis of Sensitive and Hidden Directories in Web Applications

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 03

Web Application Security & Bug Bounty Hunting

Curriculum (continued)

03 Web Application Firewalls and Security Tools

- LO 1 Overview of Web Application Firewalls (WAFs)
- LO 2 Tools for Vulnerability Scanning (e.g., Burp Suite, OWASP ZAP)
- LO 3 Penetration Testing Techniques for Web Applications
- LO 4 Automated vs. Manual Testing Approaches

04 Input Validation and Injection Attacks

- LO 1 Introduction to Injection Attacks
- LO 2 Finding All Possible Insertion Points
- LO 3 Injection Flaws: OS Command Injection
- LO 4 Injection Flaws: XSS (Cross-Site Scripting)
- LO 5 Injection Flaws: SQL Injection
- LO 6 Injection Flaws: Host Header Injection
- LO 7 Injection Flaws: CSV Injection
- LO 8 Injection Flaws: Cookie Injection

05 Client-Side Attacks

- LO 1 How CSRF Works and Its Impact
- LO 2 Protecting Against CSRF Attacks
- LO 3 Clickjacking and Frame Injection
- LO 4 Improper Authentication Issues
- LO 5 IDOR (Insecure Direct Object Reference)
- LO 6 Authorization Bypass Through User-Controlled Key

06 Server-Side Attacks

- LO 1 Broken Access Control
- LO 2 Business Logic Flaws
- LO 3 Insecure File Uploads
- LO 4 Directory Traversal
- LO 5 Remote Code Execution (RCE)

07 Secure Data Transmission and Storage

- LO 1 Understanding HTTPS and SSL/TLS Protocols
- LO 2 Implementing Secure Cookies and Secure Headers
- LO 3 Data Encryption for Storage and Transit
- LO 4 Preventing Insecure Deserialization

08 API Security

- LO 1 Understanding RESTful and GraphQL APIs
- LO 2 Common API Vulnerabilities
- LO 3 Securing API Keys and Tokens
- LO 4 Implementing Rate Limiting and Throttling

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 03

Web Application Security & Bug Bounty Hunting

Curriculum (continued)

09 Secure Development Practices

- LO 1 Secure Coding Standards and Practices
- LO 2 Static and Dynamic Application Security Testing (SAST and DAST)
- LO 3 Integrating Security in CI/CD Pipelines (DevSecOps)
- LO 4 Secure Use of Third-Party Libraries and Frameworks

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 04 — 8 Days · 16 Hours

Cyber Forensics Investigation

04

Cyber Forensics Investigation is a comprehensive course that delves into the processes and tools required to investigate and analyze digital crimes. The course covers the principles of digital forensics, as well as evidence collection, preservation, and analysis techniques. Participants will explore topics such as incident response, file system analysis, network forensics, and malware investigation. Emphasis is placed on using forensic tools, maintaining the chain of custody, and adhering to legal and ethical standards. Through hands-on activities and real-world case studies, learners will gain the skills needed to uncover digital evidence, reconstruct cyber incidents, and support legal investigations effectively.

Key Learning Outcomes

- Explain the core concepts of digital forensics, including evidence handling, chain of custody, and legal considerations.
- Perform file system analysis to recover deleted files, examine file metadata, and identify hidden data.
- Use industry-standard forensic tools (e.g., EnCase, FTK, Autopsy) for evidence acquisition, analysis, and reporting.
- Adapt forensic practices to tackle new and evolving cyber threats, including ransomware, insider threats, and advanced persistent threats (APTs).
- Employ techniques for securely collecting digital evidence from various devices, including computers, mobile phones, and cloud systems.
- Identify and track the movement of data and attackers within networks using tools like Wireshark and NetFlow.
- Analyze real-world case studies to apply investigative methods and draw actionable conclusions.

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 04

Cyber Forensics Investigation

Curriculum · 6 modules · 25 learning outcomes

01 Introduction to Cyber Forensics

- LO 1 Definition and Importance of Cyber Forensics
- LO 2 Legal and Ethical Issues in Digital Forensics
- LO 3 Types of Digital Evidence (e.g., File systems, Network logs, Mobile devices)
- LO 4 Overview of Cybercrime and Digital Forensics Investigations

02 Evidence Collection and Preservation

- LO 1 Guidelines for Evidence Collection and Chain of Custody
- LO 2 Forensic Imaging and Duplication Techniques
- LO 3 Collecting Evidence from Various Sources
- LO 4 Preserving Integrity of Digital Evidence

04 Network Forensics

- LO 1 Introduction to Network Forensics and Traffic Analysis
- LO 2 Capturing Network Traffic with Tools Like Wireshark
- LO 3 Analyzing Network Protocols and Logs
- LO 4 Tracing Malicious Activity Through Network Communication

03 File System Forensics

- LO 1 File Systems Overview (e.g., FAT, NTFS, ext4)
- LO 2 Recovering Deleted Files and Hidden Data
- LO 3 Analyzing File Metadata (e.g., timestamps, File signatures)
- LO 4 Techniques for Data Carving and Forensic Analysis of Storage Devices
- LO 5 Investigating Operating System Artifacts

06 Advanced Topics in Cyber Forensics

- LO 1 Emerging Trends in Cyber Forensics
- LO 2 Investigating Encrypted and Hidden Data
- LO 3 Analyzing Insider Threats and Corporate Espionage
- LO 4 Future of Digital Forensics: Challenges and Innovations

05 Windows Forensics

- LO 1 Investigating Windows Memory
- LO 2 Investigating Windows Registry Part 1
- LO 3 Investigating Windows Registry Part 2
- LO 4 Web Browser Artifacts

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 05 — 10 Days · 10 Hours

Mobile Application Pentesting & Bug Bounty Hunting

The main emphasis of mobile application security is the methods, resources, and best practices needed to protect mobile apps from online attacks. Common vulnerabilities unique to mobile platforms are covered in the course, including inadequate encryption, poor session handling, and unsafe data storage. In both native and hybrid mobile apps for iOS and Android environments, participants will gain knowledge about how to recognize and reduce risks. Strong authentication procedures, API security, and secure code techniques are emphasized. Students will learn how to test, secure, and protect mobile applications against contemporary security breaches and attacks through practical exercises.

Key Learning Outcomes

- Understand Mobile Application Security Fundamentals
- Manage Authentication and Session Security
- Secure Mobile APIs and Backend Services
- Stay Updated with Emerging Mobile Security Trends
- Secure Mobile App Data Storage and Transmission
- Conduct Mobile Application Security Testing
- Perform Mobile Application Incident Response

Curriculum

5 modules · 19 learning outcomes

01 Android Bug Bounty Hunting and Pentesting Approach

- LO 1 In-Depth Exploration of Android Bug Bounty Hunting Methodologies
- LO 2 Differences Between Android Pentesting and Bug Bounty Methodologies
- LO 3 Penetration Testing Test Cases for Traditional Android Applications
- LO 4 Traditional Android Penetration Testing Approach and Guidelines

02 Android Application Attack Surface

- LO 1 Understanding the Attack Surface of Android Applications
- LO 2 Android Application Attack Surface - Client Side Vulnerabilities
- LO 3 Android Application Attack Surface - Server Side Vulnerabilities
- LO 4 Android Application Attack Surface - Logical Security Threats

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 05

Mobile Application Pentesting & Bug Bounty Hunting

Curriculum (continued)

03 Android Application Security Testing Lab Environment

- LO 1 Getting Started with Android Pentesting: Emulator
- LO 2 An Overview of the Android Architecture
- LO 3 An Overview of the Android Permissions Model

04 Security Analysis of Android Application Source Code

- LO 1 Dynamic Source Code Analysis to Find Security Vulnerabilities
- LO 2 Static Source Code Analysis to Find Security Vulnerabilities
- LO 3 Searching for Vulnerable Functions in Source Code

05 Module 06: Exploiting Common Vulnerabilities in Android

- LO 1 Testing for Insecure Logging Issues
- LO 2 Testing for Hardcoding Issues
- LO 3 Testing for Insecure Data Storage
- LO 4 Testing for Input Validation
- LO 5 Testing for Access Control Issues

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 06 — 13 Days · 26 Hours

Exploit Development

06

A focused, hands-on module that teaches students how vulnerabilities are discovered, analyzed, and reliably exploited in controlled environments. The module covers the full exploit lifecycle: vulnerability discovery (fuzzing & code review), root-cause analysis (debugging & reverse engineering), exploit design (control-flow hijacking, memory corruption, ROP), payload creation, and hardening/mitigation bypass techniques (ASLR, DEP, stack canaries). Emphasis is placed on safe, ethical practice and defensive uses of exploit knowledge for secure software engineering and red/blue team readiness.

Key Learning Outcomes

- Identify and reproduce common vulnerability classes (buffer overflow, use-after-free, format string) in a lab environment.
- Evaluate and bypass basic exploit mitigations (ASLR, DEP, stack canaries) ethically.
- Classic exploit techniques: stack/heap overflows, format strings
- Perform root-cause analysis using debuggers and disassemblers to locate exploitable program state.
- Vulnerability discovery: fuzzing basics and code review

Curriculum

6 modules · 26 learning outcomes

01 Introduction to Exploit Development

- LO 1 What is an Exploit? Types and Lifecycle
- LO 2 Role of Exploit Development in Cybersecurity and Ethical Hacking
- LO 3 Real-world Examples of Famous Exploits (Morris Worm, EternalBlue, Heartbleed)
- LO 4 Setting Up a Safe Lab Environment for Exploit Testing (VMs, isolation, tools)

02 Understanding System Architecture & Memory

- LO 1 Computer Memory structure: Stack, Heap, Data, and Code Segments
- LO 2 How Programs are Loaded and Executed in Memory
- LO 3 Registers, pointers, and Instruction Flow
- LO 4 CPU Architecture (x86/x64 basics)
- LO 5 Understanding System Calls and Privilege Levels

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 06

Exploit Development

Curriculum (continued)

03 Binary & Assembly Fundamentals

- LO 1 Introduction to Binary Files (ELF and PE Format overview)
- LO 2 Understanding opcodes, instructions, and Disassembly
- LO 3 Common Assembly Instructions (MOV, PUSH, CALL, JMP, RET)
- LO 4 Stack Frames and Function Calls

04 Tools for Analysis and Debugging

- LO 1 Overview of Debuggers and Disassemblers
- LO 2 Exploring Tools: x64dbg, OllyDbg, IDA Free, and Ghidra
- LO 3 Using GDB to Trace Program Execution and Inspect Memory
- LO 4 Understanding Breakpoints and Watchpoints
- LO 5 Dynamic vs. Static Analysis of Binaries

05 Stack-Based Buffer Overflow

- LO 1 How Stack Overflow Works (Return Address overwrite)
- LO 2 Finding and Exploiting a Buffer Overflow Manually
- LO 3 Crafting Shellcode and Payloads
- LO 4 Stack-Based Overflow on EXE Application

06 Exploit Development Tools & Automation

- LO 1 Using Pwntools and Python for Exploit Automation
- LO 2 Writing Simple Exploit Scripts
- LO 3 Using Metasploit Framework for Controlled Exploit Testing
- LO 4 Exploit Development Workflow and Debugging

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 07 — 10 Days · 20 Hours

Malware Analysis

07

Malware analysis is the process of closely examining and studying malware to determine its sources, function, and any effects on the system. To complete their work, malware analysts use a variety of technologies and in-depth expertise to determine what a piece

Key Learning Outcomes

- Understand Core Malware Concepts
- Perform Static Malware Analysis
- Conduct Memory and Behavioral Forensics
- Establish a Safe Malware Analysis Environment
- Perform Dynamic Malware Analysis
- Extract and Document Indicators of Compromise (IOCs)

Curriculum

5 modules · 25 learning outcomes

01 Intro to Malware Analysis

- LO 1 Overview of Malware Analysis and Methodology
- LO 2 Types of Malware
- LO 3 Setting Up a Safe Malware Analysis Lab
- LO 4 Basic Static Analysis
- LO 5 Basic Dynamic Analysis
- LO 6 Role of Malware Analysts in SOC, DFIR, and Threat Intelligence Teams

02 Static Malware Analysis

- LO 1 Fingerprinting the Malware
- LO 2 Extracting Strings and Resources
- LO 3 Dissecting PE Structure and Imports
- LO 4 Entropy and Packing Detection
- LO 5 Identifying Obfuscation and Encryption Techniques
- LO 6 Basic Disassembly with Ghidra

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 07

Malware Analysis

Curriculum (continued)

03 Dynamic Malware Analysis

- LO 1 Preparing the Analysis Environment for Execution
- LO 2 Process Monitoring
- LO 3 API Logger and Registry Monitoring
- LO 4 Network Traffic Monitoring
- LO 5 Behavioral Analysis with Sandbox Tools

04 IOC Extraction, Detection & Reporting

- LO 1 Identifying Indicators of Compromise (IOCs): Hashes, Domains, IPs, Registry Keys, Mutexes
- LO 2 Writing YARA Rules for Malware Family Detection
- LO 3 Using MISP for IOC Management and Threat Sharing
- LO 4 Creating Executive and Technical Reports

05 Host-Based Evasions

- LO 1 Introduction to Antivirus
- LO 2 AV Detection Techniques
- LO 3 AV Evasion Using Shellcode Encoding
- LO 4 AV Evasion Using Packers and Crypters

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 08 — 8 Days · 10 Hours

SoC Analysis

08

Participants in the Security Operations Center (SoC) Analysis learn about the fundamental ideas, procedures, and tools used in the monitoring, identification, and handling of cybersecurity threats in an organization's IT environment. The function and organization of a Security Operations Center, as well as its essential elements (including SIEM, threat intelligence, and incident response), are covered in the course, along with the duties of SoC analysts. Along with best practices for efficient cooperation and communication during security crises, it also examines the tools and techniques utilized in threat detection, monitoring, and incident handling. Participants will learn how SoCs support organizational security posture and proactive threat management.

Key Learning Outcomes

- Understand the Role and Function of a SoC
- Master Threat Detection and Monitoring Techniques
- Understand the SoC Workflow and Communication
- Gain Awareness of Compliance and Regulatory Requirements
- Learn Key SoC Components and Technologies
- Incident Response and Management
- Analyze Security Logs and Alerts

Curriculum

4 modules · 18 learning outcomes

01 Introduction to Security Operations Center (SoC)

- LO 1 Overview of SoC: Purpose, Structure, and Importance
- LO 2 The Role of SoC in an Organization's Security Posture
- LO 3 Key Components and Functions of a SoC
- LO 4 Different Types of SoCs (In-house, Outsourced, Managed Security Service Providers)

02 SoC Technologies and Tools

- LO 1 Introduction to Security Information and Event Management (SIEM) Systems
- LO 2 Overview of Threat Intelligence Platforms
- LO 3 Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
- LO 4 Security Orchestration, Automation, and Response (SOAR) Tools
- LO 5 Endpoint Detection and Response (EDR) Solutions
- LO 6 Commonly Used SoC Tools (Splunk, IBM QRadar, AlienVault, etc.)

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 08

SoC Analysis

Curriculum (continued)

03 Threat Detection and Monitoring

- LO 1 Fundamentals of Threat Detection in a SoC
- LO 2 Monitoring Network Traffic, Logs, and Events for Security Indicators
- LO 3 Key Indicators of Compromise (IOCs) and Behavior Analysis
- LO 4 Anomaly Detection and Behavioral Analytics

04 Compliance and Regulatory Considerations in SoC Operations

- LO 1 Key Compliance Standards Affecting SoC Operations (e.g., GDPR, PCI DSS, HIPAA, NIST)
- LO 2 SoC's Role in Ensuring Regulatory Compliance
- LO 3 Best Practices for SoC in Managing Data Privacy and Legal Considerations
- LO 4 Handling Data Breaches and Reporting Requirements

LEVEL 09 — 8 Days · 10 Hours

Threat Intelligence

09

Threat intelligence helps organizations proactively protect against cybersecurity risks by gathering, analyzing, and disseminating information about possible or current attacks. It offers information on potential weaknesses, attack routes, and threat actors and their tactics, methods, and procedures (TTPs). By utilizing threat intelligence, organizations may improve their security posture, prioritize vulnerabilities, foresee attacks, and make well-informed decisions to reduce risks. This field makes proactive defensive tactics, incident response, and general cybersecurity resilience possible.

Key Learning Outcomes

- Understand the Fundamentals of Threat Intelligence
- Understand methods for collecting threat data from open-source intelligence (OSINT), dark web sources, and commercial feeds.
- Stay updated on the latest trends in cybersecurity threats and threat intelligence methodologies.
- Recognize common tactics, techniques, and procedures (TTPs) used by adversaries.
- Learn the importance of sharing threat intelligence through Information Sharing and Analysis Centers (ISACs) and other platforms.
- Develop strategies to address emerging threats such as ransomware, supply chain attacks, and AI-powered threats.

Curriculum

4 modules · 17 learning outcomes

01 Introduction to Threat Intelligence

- LO 1 Overview of Threat Intelligence and Its Importance
- LO 2 Types of Threat Intelligence: Strategic, Operational, Tactical, and Technical
- LO 3 Understanding the Cyber Threat Landscape
- LO 4 Threat Intelligence vs. Threat Hunting

02 Threat Actors, TTPs, and Threat Taxonomies

- LO 1 Identifying Types of Threat Actors (e.g., Nation-States, Cybercriminals)
- LO 2 Understanding Tactics, Techniques, and Procedures (TTPs)
- LO 3 Introduction to MITRE ATT&CK Framework
- LO 4 Analyzing Threat Patterns Using the Diamond Model and Cyber Kill Chain
- LO 5 Case Studies of High-Profile Threat Actors

LEVEL 09

Threat Intelligence

Curriculum (continued)

03 Data Collection and Sources of Threat Intelligence

- LO 1 Data Collection Methods: OSINT, Dark Web, Commercial Feeds, and Closed Sources
- LO 2 Tools for Threat Intelligence Collection
- LO 3 Evaluating Data Quality: Reliability and Relevance
- LO 4 Legal and Ethical Considerations in Threat Intelligence Gathering

04 Threat Intelligence Frameworks and Standards

- LO 1 Understanding MITRE ATT&CK, Cyber Kill Chain, and Diamond Model
- LO 2 Introduction to Standards Like STIX/TAXII for Intelligence Sharing
- LO 3 Implementing Threat Intelligence in Incident Response Frameworks
- LO 4 Case Studies on Framework Applications in Real-World Scenarios

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 10 — 10 Days · 20 Hours

Python for Security

10

Python for Security is a thorough course that emphasizes using Python's ease of use and adaptability to tackle a variety of cybersecurity issues. The capacity to create unique tools for incident response, penetration testing, vulnerability assessment, and threat detection will be taught to participants. The course examines libraries and frameworks created especially for security applications in addition to covering fundamental Python programming ideas. Professionals can improve their capacity to automate processes, analyze data, and fortify their organization's security posture by becoming proficient in Python for Security.

Key Learning Outcomes

- Understand core Python programming concepts, including variables, data types, loops, functions, and file handling.
- Create solutions for malware detection, intrusion detection, and incident response automation.
- Utilize libraries like Scapy for packet manipulation, Paramiko for SSH, and Requests for web scraping.
- Learn to build custom tools for network scanning, vulnerability assessment, and penetration testing.
- Automate testing of web applications for SQL injection, XSS, and other common vulnerabilities.
- Implement cryptographic techniques, including encryption, decryption, hashing, and digital signatures.

Curriculum

5 modules · 19 learning outcomes

01 Python Fundamentals for Security Applications

- LO 1 Variables, Data Types, and Control Structures (Loops and Conditionals)
- LO 2 Functions and Modules for Reusable Code
- LO 3 File Handling and Directory Operations
- LO 4 Error Handling and Debugging in Python

02 Network Security with Python

- LO 1 Introduction to Network Programming in Python
- LO 2 Packet Analysis and Manipulation Using Scapy
- LO 3 Writing Scripts for Port Scanning and Network Discovery
- LO 4 Automating Network Traffic Analysis with Python

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 10

Python for Security

Curriculum (continued)

03 Web Security Testing with Python

- LO 1 Sending HTTP Requests Using the Requests Library
- LO 2 Web Scraping for Security Testing
- LO 3 Automating Vulnerability Scanning (e.g., SQL Injection, XSS)
- LO 4 Interfacing with Web APIs for Data Retrieval and Testing

04 Python for Cryptography

- LO 1 Introduction to Cryptographic Concepts (Encryption, Hashing, and Signing)
- LO 2 Implementing Symmetric and Asymmetric Cryptography Using PyCryptodome
- LO 3 Creating and Verifying Digital Signatures

05 Real Scripts for Pentesting

- LO 1 Subdomain and Directory Enumeration Using Python
- LO 2 Port Scanner Using Python
- LO 3 Keyloggers Using Python
- LO 4 Perform SSH Brute Force

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 11 — 4 Days · 8 Hours

AI in Cybersecurity

11

The use of artificial intelligence (AI) and machine learning (ML) technologies to improve the security of digital systems and networks is the main focus of AI in cybersecurity. This course examines how artificial intelligence (AI) can anticipate new vulnerabilities, automate tedious security processes, and detect and mitigate cyber threats in real-time. The subjects covered include anomaly detection, threat intelligence, automated incident response, behavioral analysis, and AI-driven defense tactics. In addition to discussing the ethical issues and possible hazards related to AI in cybersecurity, participants will learn how AI and ML models can increase threat detection accuracy, lower false positives, and boost the overall effectiveness of cybersecurity operations.

Key Learning Outcomes

- Understand AI and ML Concepts in Cybersecurity
- Utilize AI for Predictive Security
- Implement AI-Driven Security Automation
- Leverage AI for Malware Detection and Prevention
- Apply Machine Learning for Threat Detection
- Enhance Incident Response with AI
- Address Ethical and Privacy Issues in AI-Driven Security
- Stay Ahead of Emerging Threats with AI

Curriculum

4 modules · 19 learning outcomes

01 Introduction to AI and Machine Learning in Cybersecurity

- LO 1 Overview of AI and Machine Learning Concepts
- LO 2 The Role of AI in Modern Cybersecurity Practices
- LO 3 Types of Machine Learning Algorithms
- LO 4 Benefits and Challenges of Integrating AI in Security Operations
- LO 5 Key AI Terminologies and Tools in Cybersecurity

02 Fundamentals of Machine Learning for Cybersecurity

- LO 1 Introduction to Machine Learning Models & Their Applications in Cybersecurity
- LO 2 Feature Engineering and Data Preprocessing for Cybersecurity Data
- LO 3 Training and Testing Machine Learning Models
- LO 4 Evaluating Model Performance
- LO 5 Common Algorithms Used in Cybersecurity

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 11

AI in Cybersecurity

Curriculum (continued)

03 AI for Threat Detection and Prevention

- LO 1 Using AI for Anomaly Detection in Networks and Systems
- LO 2 Identifying Malicious Behavior with Machine Learning
- LO 3 Real-time Threat Detection with AI Models
- LO 4 AI for Behavioral Analysis in User and Entity Behavior Analytics (UEBA)
- LO 5 Reducing False Positives with AI in Threat Detection

04 Future of AI in Cybersecurity

- LO 1 Emerging AI Techniques and Trends in Cybersecurity
- LO 2 AI for Protecting Emerging Technologies (e.g., IoT, 5G, Cloud)
- LO 3 Exploring AI-Driven Security in Autonomous Systems and Robotics
- LO 4 Research Opportunities and Career Paths in AI for Cybersecurity

HACKINETIX ACADEMY

MASTERING THE CYBER FLOW

START YOUR JOURNEY

Ready to Start Your Cybersecurity Journey?

Join Ethical Hacking Expert (H|EHE) and build practical cybersecurity skills across all levels.

ENROLL NOW →



CONTACT US

www.hackinetix.com

info@hackinetix.com

Join Our WhatsApp Channel