Python for Cybersecurity Automation Training Course

Professional Development Training Course Outline

Category	Defense and Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Python has emerged as the leading programming language for cybersecurity automation, threat detection, and security operations optimization. Python for Cybersecurity Automation Training Course equips participants with practical skills to write scripts, develop automated tools, and implement cybersecurity solutions that enhance efficiency, accuracy, and response time. Participants learn to integrate Python with security platforms, analyze threat intelligence, automate repetitive tasks, and streamline vulnerability assessment and penetration testing. By leveraging Python libraries, APIs, and frameworks, security teams can focus on high-priority tasks while ensuring robust protection of IT assets and networks.

This course provides hands-on exercises in coding, threat simulation, log analysis, malware detection, and automation of security workflows. It emphasizes real-world applications, such as SIEM integration, automated incident response, and network monitoring, ensuring participants can deploy Python-based solutions in professional cybersecurity environments. By completing this training, learners will be capable of designing scripts, automating threat detection, and enhancing security operations, improving organizational cybersecurity resilience and operational efficiency.

Programme Curriculum

Python for Cybersecurity Automation Training Course

Introduction

Python has emerged as the leading programming language for cybersecurity automation, threat detection, and security operations optimization. Python for Cybersecurity Automation Training Course equips participants with practical skills to write scripts, develop automated tools, and implement cybersecurity solutions that enhance efficiency, accuracy, and response time. Participants learn to integrate Python with security platforms, analyze threat intelligence, automate repetitive tasks, and streamline vulnerability assessment and penetration testing.

By leveraging Python libraries, APIs, and frameworks, security teams can focus on high-priority tasks while ensuring robust protection of IT assets and networks.

This course provides hands-on exercises in coding, threat simulation, log analysis, malware detection, and automation of security workflows. It emphasizes real-world applications, such as SIEM integration, automated incident response, and network monitoring, ensuring participants can deploy Python-based solutions in professional cybersecurity environments. By completing this training, learners will be capable of designing scripts, automating threat detection, and enhancing security operations, improving organizational cybersecurity resilience and operational efficiency.

Course Objectives

1. Understand the fundamentals of Python programming for cybersecurity applications.
2. Write scripts to automate security monitoring, logging, and alerting.
3. Implement network scanning, vulnerability assessment, and penetration testing using Python.
4. Integrate Python with security tools such as SIEM, IDS/IPS, and firewalls.
5. Develop malware analysis and threat intelligence automation scripts.
6. Automate incident response and reporting workflows.
7. Utilize Python libraries for encryption, hashing, and secure communication.
8. Analyze and process log files for anomaly detection and forensic investigations.
9. Implement ethical hacking techniques and security automation best practices.
10. Deploy automated phishing detection and malware classification solutions.
11. Conduct automated risk assessment and compliance checks.
12. Integrate APIs for threat intelligence and cybersecurity automation.
13. Build scalable Python-based solutions for enterprise security operations.

Organizational Benefits

- Increased cybersecurity operational efficiency through automation
- Faster detection and response to security incidents
- Improved accuracy in vulnerability scanning and threat identification
- Enhanced integration with existing security tools and platforms
- Reduced manual workload for security teams
- Scalable automation solutions for enterprise environments
- Strengthened security compliance and reporting capabilities
- Improved incident documentation and audit readiness
- Increased staff proficiency in cybersecurity scripting and automation
- Reduced organizational risk through proactive threat mitigation

Target Audiences

- Security analysts and SOC team members
- IT security engineers and network administrators
- Penetration testers and ethical hackers
- Cybersecurity consultants and auditors
- Security operations managers
- Python developers interested in security applications
- IT compliance and risk management professionals
- Students and researchers in cybersecurity and information technology

Course Duration: 10 days

Course Modules

Module 1: Python Basics for Cybersecurity

- Introduction to Python syntax, variables, and data types
- Control structures, loops, and functions
- Working with modules and packages
- File handling and basic input/output
- Error handling and debugging techniques
- Case Study: Writing a Python script to automate log parsing

Module 2: Python Libraries for Security

- Overview of cybersecurity-relevant libraries (e.g., Scapy, Requests, Paramiko)
- Automating network tasks with Python libraries
- Using cryptography and hashing libraries
- Data parsing and JSON handling for threat intelligence
- Implementing API calls for automation
- Case Study: Automating vulnerability scanning using Python libraries

Module 3: Networking & Socket Programming

- Understanding TCP/IP and OSI model concepts
- Creating network clients and servers with Python
- Automating port scanning and network mapping
- Sending and receiving network packets programmatically
- Monitoring network traffic with Python
- Case Study: Network reconnaissance automation script

Module 4: Web Application Security Automation

- Introduction to web vulnerabilities (XSS, SQLi, CSRF)
- Using Python to automate vulnerability testing
- Web scraping for reconnaissance and threat intelligence
- Automating input validation and testing scripts
- Logging and reporting detected vulnerabilities
- Case Study: Automated SQL injection scanning tool

Module 5: Malware Analysis & Automation

- Fundamentals of malware types and behaviours
- Automating static and dynamic malware analysis
- Extracting indicators of compromise (IoCs) using Python
- Automating malware classification and reporting
- Generating alerts for suspicious activities
- Case Study: Python-based ransomware signature detector

Module 6: Log Analysis & Threat Detection

- Parsing system and application logs with Python
- Detecting anomalies and suspicious patterns
- Automating alert generation and notification systems

- Aggregating log data from multiple sources
- Implementing correlation rules for threat detection
- Case Study: Automated SIEM log monitoring script

Module 7: Penetration Testing & Ethical Hacking Automation

- Python scripting for reconnaissance and scanning
- Automating enumeration and exploitation tasks
- Custom scripts for password attacks and brute force testing
- Reporting vulnerabilities in standardized formats
- Combining multiple scripts for workflow automation
- Case Study: Automated penetration testing toolkit

Module 8: Security Automation for Endpoints

- Automating endpoint monitoring and patch management
- Detecting unauthorized processes and file changes
- Scheduling security tasks with Python scripts
- Automating configuration and policy enforcement
- Collecting endpoint telemetry for analysis
- Case Study: Endpoint anomaly detection automation

Module 9: Encryption & Cryptography Automation

- Understanding symmetric and asymmetric encryption
- Implementing hashing and digital signatures in Python
- Automating encryption/decryption workflows
- Securing communications using Python scripts
- Key management and secure storage automation
- Case Study: Automating secure file transfer with encryption

Module 10: API Integration & Threat Intelligence

- Consuming threat intelligence feeds using APIs
- Automating enrichment of IoCs from external sources
- Integrating Python scripts with SIEM and alerting platforms
- Building dashboards for automated threat reporting
- Scheduling API-based threat intelligence tasks
- Case Study: Automated threat feed integration for SOC

Module 11: Incident Response Automation

- Automating alert triage and prioritization
- Developing scripts to collect forensic evidence
- Integrating Python with ticketing and response platforms
- Automating containment measures for compromised hosts
- Reporting incidents in real-time
- Case Study: Incident response automation workflow

Module 12: Malware & Phishing Detection

- Automating detection of phishing emails

- Implementing email parsing and pattern recognition
- Classifying malware and suspicious files automatically
- Generating alerts and reports for SOC teams
- Combining AI/ML scripts for threat classification
- Case Study: Python script detecting phishing campaigns

Module 13: Vulnerability Assessment Automation

- Automating vulnerability scanning with Python
- Parsing scanner results for reporting
- Scheduling regular scans and automated remediation alerts
- Integrating vulnerability data into dashboards
- Continuous monitoring of critical assets
- Case Study: Automated network vulnerability assessment

Module 14: Security Metrics & Reporting

- Automating KPI collection and security metrics
- Creating dashboards for SOC performance
- Automating compliance reporting
- Visualizing threat trends and attack vectors
- Generating automated reports for management and regulators
- Case Study: Python-based SOC metrics dashboard

Module 15: Advanced Cybersecurity Automation Projects

- Combining Python skills across modules for end-to-end automation
- Developing custom security solutions for enterprise environments
- Integrating threat intelligence, incident response, and reporting
- Testing and deploying automated workflows in simulated environments
- Documenting automation procedures and best practices
- Case Study: Full SOC automation using Python scripts

Training Methodology

- Instructor-led presentations on Python and cybersecurity concepts
- Hands-on exercises for scripting, automation, and threat simulations
- Case study discussions and real-world problem-solving
- Group projects integrating multiple Python automation techniques
- Use of virtual labs and simulation environments
- Continuous assessment, feedback, and action plan development

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com