Python for Security Operations and Automation Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The proliferation of cyber threats and the sheer volume of security alerts necessitate a shift from manual security processes to hyper-automated Security Operations. Python for Security Operations and Automation Training Course is designed to transform security professionals into Automation Engineers, leveraging the power of Python scripting to build robust, scalable, and efficient security tools. You will master the DevSecOps philosophy, integrating automated security testing, Incident Response workflows, and Threat Intelligence feeds to achieve Security Orchestration, Automation, and Response. This is an essential skill upgrade for modern security teams seeking to maximize efficiency, reduce human error, and accelerate response times in the face of evolving Cyber Defense challenges.

The training emphasizes practical, hands-on application of Python to solve real-world security challenges, moving beyond theoretical programming to develop production-ready, object-oriented scripts for vulnerability management, log analysis, and network packet manipulation. By the end of this program, you will not only be proficient in Python but will be able to design and implement end-to-end security automation solutions, making you a critical asset in any contemporary Cybersecurity or environment.

Programme Curriculum

Python for Security Operations and Automation Training Course

Introduction

The proliferation of cyber threats and the sheer volume of security alerts necessitate a shift from manual security processes to hyper-automated Security Operations. Python for Security Operations and Automation Training Course is designed to transform security professionals into Automation Engineers, leveraging the power of Python scripting to build robust, scalable, and efficient security tools. You will master the DevSecOps philosophy, integrating automated security testing, Incident Response workflows, and Threat Intelligence feeds

to achieve Security Orchestration, Automation, and Response. This is an essential skill upgrade for modern security teams seeking to maximize efficiency, reduce human error, and accelerate response times in the face of evolving Cyber Defense challenges.

The training emphasizes practical, hands-on application of Python to solve real-world security challenges, moving beyond theoretical programming to develop production-ready, object-oriented scripts for vulnerability management, log analysis, and network packet manipulation. By the end of this program, you will not only be proficient in Python but will be able to design and implement end-to-end security automation solutions, making you a critical asset in any contemporary Cybersecurity or environment.

Course Duration

5 days

Course Objectives

1. Achieve Python scripting mastery for security tasks and tool development.
2. Automate interaction with security tools and platforms using RESTful APIs.
3. Design and implement Security Orchestration, Automation, and Response playbooks.
4. Automate key steps in Incident Response (IR) and digital forensics workflows.
5. Parse, analyze, and visualize large volumes of security logs using Python libraries.
6. Automate the ingestion and enrichment of Threat Intelligence (TI) feeds.
7. Utilize Python for network scanning, packet manipulation, and security auditing.
8. Develop custom scripts for vulnerability scanning and prioritization.
9. Apply secure coding practices to develop robust and attack-resistant automation scripts.
10. Automate security tasks and compliance checks in Cloud Environments.
11. Use Python to automate security-related system configuration and compliance enforcement.
12. Script basic malware triage and analysis tasks.
13. Integrate security automation scripts into CI/CD pipelines for proactive security.

Target Audience

1. Security Analysts
2. Security Operations Engineers
3. Incident Responders
4. Threat Hunters
5. Penetration Testers and Ethical Hackers
6. DevSecOps Engineers
7. Network Engineers
8. System Administrators

Course Modules

Module 1: Python Fundamentals for Cybersecurity

- Review of core Python concepts.
- Setting up a secure Virtual Environment and managing dependencies.
- Reading, writing, and parsing common log and configuration formats.
- Introduction to basic CLI Tool Creation using Python's argparse.
- Case Study: Automating the daily collection and aggregation of VPN connection logs for initial security review.

Module 2: Network & Protocol Analysis with Python

- Scapy fundamentals: Packet crafting, sniffing, and manipulation.
- Building a custom Port Scanner and service banner grabber.
- Automating network flow analysis and baseline deviation detection.
- Writing scripts to interact with network devices using Paramiko
- Case Study: Developing a script to detect and report ARP spoofing attempts by analyzing network traffic captures.

Module 3: Security Tool Integration and REST APIs

- Fundamentals of interacting with RESTful APIs using the requests library.
- Automating data submission and retrieval from SIEM and SOAR platforms.
- Parsing JSON and XML responses for meaningful security data.
- Handling authentication securely
- Case Study: Building an automated threat indicator submission tool that pushes newly identified IOCs to a firewall's blocklist via its API

Module 4: Automating Vulnerability Management

- Scripting wrappers for popular scanners like Nmap and Nikto for large-scale scanning.
- Automating the parsing and prioritization of vulnerability reports
- Developing custom scripts to check for specific, common misconfigurations.
- Integration with Vulnerability Management platforms via their APIs.
- Case Study: Creating a pipeline that automatically scans newly deployed cloud instances and opens tickets in JIRA for high-severity vulnerabilities.

Module 5: Incident Response and Digital Forensics Automation

- Automating the collection of volatile and non-volatile forensic data from endpoints.
- Scripting log enrichment from multiple sources
- Using Python for memory forensics
- Developing automated threat containment scripts
- Case Study: Building a phishing email triage script that automatically extracts URLs and attachments for sandbox submission and blocks sender domains.

Module 6: Threat Intelligence Automation

- Automating the aggregation of from public and private Threat Intelligence feeds.
- Data normalization and de-duplication for efficient storage and lookup.
- Creating scripts for automated lookup and scoring of addresses and hashes against databases.
- Integration of data for enhanced alert enrichment within a SIEM
- Case Study: Developing a reputation checker that automatically queries VirusTotal and Shodan APIs for suspicious IPs identified in access logs.

Module 7: Advanced Scripting and DevSecOps

- Implementing Object-Oriented Programming (OOP) for modular and reusable security tools.
- Using Unit Testing and robust Error Handling for production-ready code.
- Introduction to integrating Python scripts into CI/CD pipelines for automated SAST/DAST
- Basic data visualization of security metrics using libraries like Matplotlib or Plotly.

- Case Study: Creating a Python class structure for a generic security scanner that can be easily extended to check for new security policies.

Module 8: Security Orchestration (SOAR) Playbook Development

- Designing end-to-end SOAR Playbooks for common security events.
- Using conditionals and complex logic in automation workflows.
- Developing Python functions for playbook steps
- Best practices for developing scalable and maintainable automation solutions.
- Case Study: Mapping out and implementing a full malware alert response playbook, from initial alert to final ticketing and reporting.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com **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
07 Sep 2026	11 Sep 2026	Online	$1,100
14 Sep 2026	18 Sep 2026	Online	$1,100
21 Sep 2026	25 Sep 2026	Online	$1,100
28 Sep 2026	02 Oct 2026	Online	$1,100
05 Oct 2026	09 Oct 2026	Online	$1,100
12 Oct 2026	16 Oct 2026	Online	$1,100
19 Oct 2026	23 Oct 2026	Online	$1,100
26 Oct 2026	30 Oct 2026	Online	$1,100

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

Register Online Now

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