Cloud Security Automation with Python/Boto3 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

In today's hyper-scale, multi-cloud environment, manual security processes are a significant liability, contributing to misconfigurations, compliance drift, and delayed incident response. The imperative for modern enterprises is a definitive shift to DevSecOps and Security Automation. This transition is critically powered by scripting languages, with Python and the AWS Boto3 SDK at the forefront. Cloud Security Automation with Python/Boto3 Training Course is meticulously designed to equip security professionals, DevOps engineers, and Cloud Architects with the advanced, hands-on skills needed to architect, implement, and maintain immutable security guardrails and auto-remediation workflows on the Amazon Web Services (AWS) platform. Mastering this skillset is not merely an efficiency gain; it is a business-critical requirement for achieving Zero Trust architectures and ensuring continuous compliance in a world where Infrastructure as Code (IaC) defines the modern data center.

The focus of this specialized training is to transcend theoretical knowledge and drive immediate, practical competence. We delve deep into automating core security services like AWS IAM, Config, CloudTrail, and GuardDuty using robust Python scripts. Participants will work through real-world case studies centered on preventing common security threats, such as public S3 bucket exposure and overly permissive IAM roles. By the conclusion of this program, you will be fluent in developing and deploying scalable, production-ready security solutions, transforming from a reactive security respondent to a proactive Cloud Security Automation Expert, dramatically reducing human-error risk, and strengthening your organization's overall Cloud Native Security Posture.

Programme Curriculum

Cloud Security Automation with Python/Boto3 Training Course

Introduction

In today's hyper-scale, multi-cloud environment, manual security processes are a significant liability, contributing to misconfigurations, compliance drift, and delayed incident response. The imperative for modern enterprises is a definitive shift to DevSecOps and Security Automation. This transition is critically powered by scripting languages, with Python and the AWS Boto3 SDK at the forefront. Cloud Security Automation with Python/Boto3 Training Course is meticulously designed to equip security professionals, DevOps engineers, and Cloud Architects with the advanced, hands-on skills needed to architect, implement, and maintain immutable security guardrails and auto-remediation workflows on the Amazon Web Services (AWS) platform. Mastering this skillset is not merely an efficiency gain; it is a business-critical requirement for achieving Zero Trust architectures and ensuring continuous compliance in a world where Infrastructure as Code (IaC) defines the modern data center.

The focus of this specialized training is to transcend theoretical knowledge and drive immediate, practical competence. We delve deep into automating core security services like AWS IAM, Config, CloudTrail, and GuardDuty using robust Python scripts. Participants will work through real-world case studies centered on preventing common security threats, such as public S3 bucket exposure and overly permissive IAM roles. By the conclusion of this program, you will be fluent in developing and deploying scalable, production-ready security solutions, transforming from a reactive security respondent to a proactive Cloud Security Automation Expert, dramatically reducing human-error risk, and strengthening your organization's overall Cloud Native Security Posture.

Course Duration

5 days

Course Objectives

1. Architect and write resilient, modular Boto3 scripts for programmatic management of all core AWS security services.
2. Implement security checks and controls directly within Infrastructure as Code (IaC) pipelines using Python and associated tools.
3. Develop and enforce enterprise-wide Security Guardrails and Compliance-as-Code for governance.
4. Design and deploy event-driven Automated Remediation workflows using AWS Lambda and Python to fix misconfigurations in real-time.
5. Programmatically manage Identity and Access Management users, roles, and policies to enforce the Principle of Least Privilege.
6. Configure AWS Config rules and integrate custom Python logic to ensure continuous compliance against standards like CIS Benchmarks.
7. Secure serverless and containerized workload through automated security configuration.
8. Automate the scanning, reporting, and ticketing of vulnerabilities identified by tools like Amazon Inspector and Python scripts.
9. Integrate Python automation with Amazon GuardDuty and AWS Security Hub for enhanced Threat Intelligence and analysis.
10. Implement automated S3 bucket security, including encryption, public access blocking, and lifecycle policy enforcement.
11. Programmatically integrate and rotate sensitive data using AWS Secrets Manager and AWS Parameter Store within automation scripts.
12. Embed security scripts into CI/CD Pipelines for a true Shift-Left Security approach.
13. Use Python scripts to identify and terminate unused or non-compliant, costly resources

Target Audience

1. Cloud Security Engineers.
2. DevOps & DevSecOps Engineers.
3. Cloud Architects.
4. Security Analysts.
5. System Administrators.
6. Penetration Tester.
7. Software Developers.
8. Technical Leaders/Managers.

Course Modules

Module 1: Python & Boto3 Security Foundation

- Python best practices for security scripting.
- Configuring secure AWS credentials for Boto3.
- Understanding Boto3 Clients and Resources and common methods
- Case Study: Programmatic secure setup of IAM users with enforced MFA and temporary access keys.
- Introduction to core Boto3 libraries for security.

Module 2: Automated Identity and Access Management (IAM)

- Scripting the audit of overly permissive IAM policies to enforce PoLP.
- Automating the identification and deactivation of unused or aged access keys.
- Using Boto3 to programmatically manage and attach Service Control Policies across an organization.
- Case Study: Building an IAM Role Audit script that flags roles without Trust Relationships limits.
- Implementing temporary, assumed roles using the AWS STS with Python.

Module 3: Storage and Data Protection Automation (S3 & KMS)

- Creating an automated script to detect and block all public access to S3 buckets globally.
- Automating default server-side encryption and versioning on all new S3 buckets via Python-driven S3 Policy application.
- Programmatic auditing of KMS Key Policies to restrict cross-account access.
- Case Study: A data exfiltration prevention script that monitors CloudTrail for unusual S3 object downloads and quarantines the source user.
- Using Boto3 waiters and paginators for large-scale storage inventory and compliance checks.

Module 4: Compliance-as-Code and Configuration Management

- Creating custom AWS Config rules using Python and Lambda to check for specific security configurations.
- Automating the deployment of security baseline configurations using AWS CloudFormation or Terraform and Python validation.
- Developing a reporting engine that aggregates and scores compliance status from AWS Security Hub.
- Case Study: Auto-remediation script to delete or tag EC2 instances missing a mandatory "Data Classification" tag.
- Scripting checks against the CIS AWS Foundations Benchmark

Module 5: Event-Driven Auto-Remediation with Lambda

- Designing event-driven security architectures using CloudWatch Events/EventBridge and Lambda.
- Writing Python Lambda functions for immediate, non-compliant resource termination or modification.

- Implementing retry logic, logging, and monitoring for all auto-remediation workflows.
- Case Study: A security group enforcement Lambda that automatically revokes "0.0.0.0/0" access on ports 22/3389 within seconds of creation.
- Integrating Python scripts with SNS for automated security alerting and notification.

Module 6: Threat Detection and Incident Response Automation

- Using Boto3 to enable, configure, and manage Amazon GuardDuty across multiple accounts.
- Automating the response to GuardDuty findings.
- Building a basic Python Security Orchestration, Automation, and Response (SOAR)-like workflow.
- Case Study: An Incident Response (IR) script that takes an EC2 Instance ID from a GuardDuty finding, takes a forensic snapshot (EBS), and modifies its security group to isolate it.
- Scripting the collection and analysis of security-relevant CloudTrail and VPC Flow Logs.

Module 7: DevSecOps and Secure Secrets Management

- Integrating Python security scripts as mandatory gates within a CI/CD Pipeline.
- Programmatic management of application secrets and credentials using AWS Secrets Manager and Parameter Store.
- Automating the forced rotation of database and service user passwords using Python Lambda functions.
- Case Study: Deploying an application via CodePipeline that automatically injects credentials using Secrets Manager, validated by a Boto3 script.
- Securing Python code and dependencies for automation scripts.

Module 8: Advanced Security Automation and Future Trends

- Automating security for Serverless and Container workloads.
- Scripting the use of Amazon Inspector for vulnerability assessment and automated report generation.
- Introduction to AI/ML in security automation
- Case Study: Scripting an automated cleanup and cost optimization solution that identifies and terminates unused resources with proper logging.
- Scaling security automation across a Multi-Account/Multi-Region AWS organization.

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.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	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now