Hacking and Defending the Cloud 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 rapid acceleration of digital transformation has solidified the Cloud as the new data center, but this shift has simultaneously introduced an unprecedented and complex attack surface. Traditional security perimeters are obsolete; modern threats like Cloud Misconfigurations, Excessive IAM Permissions, and Supply Chain Vulnerabilities are now the primary vectors for devastating data breaches. This training is not a theoretical review it?ÇÖs a hands-on, dual-perspective program that forces participants to think like a Red Team attacker to effectively build Blue Team defenses. By simulating real-world Cloud Penetration Testing scenarios across platforms like AWS, Azure, and GCP, we ensure participants master the art of exploiting weaknesses, which is the only way to truly understand and implement a robust Zero Trust security architecture.

Hacking and Defending the Cloud Training Course directly addresses the most in-demand skills for the next generation of Cloud Security Engineers, DevSecOps Professionals, and Cloud Architects. It integrates the latest security frameworks, including MITRE ATT&CK Cloud Matrix and OWASP Top 10 for Cloud, focusing on practical skills such as securing Infrastructure as Code (IaC), implementing Cloud-Native Application Protection Platforms (CNAPP), and managing container security with Kubernetes and Docker. Graduates will move beyond check-box compliance, mastering Threat Modeling and automated Incident Response to build truly resilient, multi-cloud defenses. This specialization is the crucial step in transitioning from a general security practitioner to a highly valued Cloud Cyber Defense expert, prepared to lead security initiatives in any modern enterprise.

Programme Curriculum

Hacking and Defending the Cloud Training Course

Introduction

The rapid acceleration of digital transformation has solidified the Cloud as the new data center, but this shift has simultaneously introduced an unprecedented and complex attack surface. Traditional security perimeters are obsolete; modern threats like Cloud Misconfigurations, Excessive IAM Permissions, and Supply Chain Vulnerabilities are now the primary vectors for devastating data breaches. This training is not a theoretical review it?ÇÖs a hands-on, dual-perspective program that forces participants to think like a Red Team attacker to effectively build Blue Team defenses. By simulating real-world Cloud Penetration Testing scenarios across platforms like AWS, Azure, and GCP, we ensure participants master the art of exploiting weaknesses, which is the only way to truly understand and implement a robust Zero Trust security architecture.

Hacking and Defending the Cloud Training Course directly addresses the most in-demand skills for the next generation of Cloud Security Engineers, DevSecOps Professionals, and Cloud Architects. It integrates the latest security frameworks, including MITRE ATT&CK Cloud Matrix and OWASP Top 10 for Cloud, focusing on practical skills such as securing Infrastructure as Code (IaC), implementing Cloud-Native Application Protection Platforms (CNAPP), and managing container security with Kubernetes and Docker. Graduates will move beyond check-box compliance, mastering Threat Modeling and automated Incident Response to build truly resilient, multi-cloud defenses. This specialization is the crucial step in transitioning from a general security practitioner to a highly valued Cloud Cyber Defense expert, prepared to lead security initiatives in any modern enterprise.

Course Duration

5 days

Course Objectives

1. Master Cloud Penetration Testing methodologies across AWS, Azure, and GCP.
2. Identify and exploit the Top 10 Cloud Misconfigurations
3. Execute Identity and Access Management (IAM) attacks and privilege escalation in all major clouds.
4. Develop Cloud Threat Modeling skills to proactively assess and mitigate risk in new deployments.
5. Implement DevSecOps security controls into CI/CD Pipelines and Infrastructure as Code
6. Perform comprehensive security assessments on Serverless Functions
7. Design and deploy a Zero Trust architecture utilizing micro-segmentation and continuous verification.
8. Analyze and defend against attacks targeting Container Orchestration systems, specifically Kubernetes.
9. Configure and utilize Cloud-Native Security Tools and CNAPP solutions for unified defense.
10. Practice Incident Response (IR) and Cloud Forensics using platform-specific logging and SIEM tools.
11. Secure Data-at-Rest and Data-in-Transit using advanced Key Management Service (KMS) techniques.
12. Automate defensive tasks using Python scripting, Cloud Formation/Terraform, and Security Automation.
13. Apply the MITRE ATT&CK Cloud Matrix to map attacker tactics, techniques, and procedures (TTPs).

Target Audience

1. Cloud Security Engineers
2. Penetration Testers
3. Security Architects
4. DevSecOps Engineers
5. Security Operations Center Analysts
6. Cloud Engineers/Administrators
7. Cybersecurity Consultants
8. Technical Auditors

Course Modules

Module 1: Foundational Cloud Security Architecture & Recon

- Cloud Service Models and Shared Responsibility Model deep dive.
- Understanding the Attack Surface of major clouds.
- Cloud Enumeration techniques for target discovery
- Threat Modeling a new cloud application using STRIDE and the MITRE ATT&CK Cloud Matrix.
- Case Study: The Capital One Breach.

Module 2: Identity and Access Management (IAM) Hacking and Defense

- Attacking Over-Privileged Roles/Users and service principals
- Azure AD/Entra ID enumeration, token theft, and lateral movement techniques.
- Implementing Least Privilege Access and automated IAM Policy Auditing.
- Securing and monitoring Root/Global Administrator Accounts with MFA and conditional access.
- Case Study: The Okta Breach

Module 3: Storage and Networking Misconfigurations

- Hacking and hardening object storage.
- Attacking and defending Virtual Private Cloud and network segmentation.
- Exploiting exposed ports, public snapshots, and weak firewall rules
- Implementing Data Loss Prevention and native encryption services (KMS/Vault).
- Case Study: Unsecured Public Snapshots.

Module 4: Infrastructure as Code (IaC) and DevSecOps Security

- Auditing Terraform and CloudFormation templates for insecure configurations
- Injecting security testing tools into CI/CD Pipelines
- Vulnerability management and artifact security in Container Registries
- Best practices for Secrets Management and injecting credentials into deployment.
- Case Study: CI/CD Pipeline Hijacking.

Module 5: Container and Kubernetes Security

- Docker security flaws.
- Hacking Kubernetes.
- Implementing Pod Security Policies/Standards and network policies for micro-segmentation.
- Utilizing a Cloud-Native Application Protection Platform for full lifecycle container security.
- Case Study: Exploiting Kubelet API.

Module 6: Serverless and Application Security

- Insecure API Gateway configurations, throttling, and authentication bypass.
- Serverless Function execution attacks and resource exhaustion.
- Securing function code against dependency attacks and insecure logging.
- Implementing OWASP Top 10 controls in cloud-native Web Application Firewalls
- Case Study: Serverless Vulnerable Function.

Module 7: Cloud Incident Response (IR) and Forensics

- Designing and testing a Cloud Incident Response Plan
- Collecting and analyzing CloudTrail/Audit Log/Activity Log data using SIEM tools

- Containment strategies: network isolation, key rotation, and rolling back IaC.
- Deep-dive into Cloud Forensics capturing disk snapshots and memory for analysis.
- Case Study: Live Ransomware Containment

Module 8: Advanced Defense, Automation, and Regulatory Compliance

- Implementing Security Automation via Python and Serverless event-driven responses.
- Compliance Mapping
- Advanced Cloud Security Posture Management techniques for continuous auditing.
- Building a Zero Trust Network Access model in a hybrid cloud environment.
- Case Study: Automating Policy-as-Code.

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

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