Training Course on Cloud Incident Response Playbooks

Professional Development Training Course Outline

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

Course Introduction

In the dynamic landscape of cloud computing, organizations face a growing wave of cybersecurity threats. Cloud Incident Response (CIR) Playbooks have become essential to identify, mitigate, and recover from breaches across leading platforms such as AWS (Amazon Web Services), Microsoft Azure, and Google Cloud Platform (GCP). Training Course on Cloud Incident Response Playbooks empowers IT professionals, security engineers, and cloud architects to master industry-proven response strategies tailored for multi-cloud environments. With a strong focus on cybersecurity best practices, cloud-native tools, and real-time incident handling, this course prepares learners for fast, strategic, and automated response management.

Whether you're building a SOC (Security Operations Center) or integrating threat intelligence across cloud environments, this training delivers actionable knowledge. Participants will gain hands-on experience designing, customizing, and deploying cloud incident response playbooks using tools like AWS Lambda, Azure Sentinel, and GCP Security Command Center. Emphasizing regulatory compliance (e.g., ISO 27001, GDPR, CIS Benchmarks), this course enables teams to minimize downtime, improve cloud resilience, and meet incident response SLAs efficiently.

Programme Curriculum

Training Course on Cloud Incident Response Playbooks

Introduction

In the dynamic landscape of cloud computing, organizations face a growing wave of cybersecurity threats. Cloud Incident Response (CIR) Playbooks have become essential to identify, mitigate, and recover from breaches across leading platforms such as AWS (Amazon Web Services), Microsoft Azure, and Google Cloud Platform (GCP). Training Course on Cloud Incident Response Playbooks empowers IT professionals, security engineers, and cloud architects to master industry-proven response strategies tailored for multi-cloud environments. With a strong focus on cybersecurity best practices, cloud-native tools, and real-time incident handling, this course prepares learners for fast, strategic, and automated response

management.

Whether you're building a SOC (Security Operations Center) or integrating threat intelligence across cloud environments, this training delivers actionable knowledge. Participants will gain hands-on experience designing, customizing, and deploying cloud incident response playbooks using tools like AWS Lambda, Azure Sentinel, and GCP Security Command Center. Emphasizing regulatory compliance (e.g., ISO 27001, GDPR, CIS Benchmarks), this course enables teams to minimize downtime, improve cloud resilience, and meet incident response SLAs efficiently.

Course Objectives

1. Understand cloud incident response lifecycle across AWS, Azure, and GCP
2. Learn to build automated incident response playbooks using native and third-party tools
3. Master multi-cloud threat detection and alerting mechanisms
4. Implement real-time remediation workflows using serverless functions
5. Design cloud-native security architectures for proactive incident management
6. Integrate SIEM tools (e.g., Splunk, Azure Sentinel) into cloud environments
7. Apply forensics and log analysis techniques for cloud-native services
8. Establish compliance-driven response protocols (GDPR, HIPAA, ISO 27001)
9. Perform root cause analysis and cloud breach investigations
10. Configure security automation pipelines using infrastructure as code (IaC)
11. Manage incident communications and escalation processes
12. Utilize threat intelligence feeds in a cloud-native SOC environment
13. Leverage machine learning and AI for predictive incident response

Target Audiences

- Cloud Security Engineers
- DevSecOps Teams
- SOC Analysts and Incident Responders
- Compliance Officers and Risk Managers
- Cloud Architects and Infrastructure Leads
- IT Managers and CTOs
- Cybersecurity Consultants
- Security-Auditors and Penetration Testers

Course Duration: 5 days

Course Modules

Module 1: Fundamentals of Cloud Incident Response

- Define incident response in cloud environments
- Understand shared responsibility model
- Key phases: Preparation, Detection, Containment, Recovery, Post-Incident
- Identify common threats in AWS, Azure, and GCP
- Tools overview: AWS CloudTrail, Azure Monitor, GCP Audit Logs
- **Case Study:** Misconfigured S3 bucket exposes sensitive data

Module 2: AWS Incident Response Playbooks

- Setting up detection with AWS GuardDuty and CloudWatch
- Automating responses with AWS Lambda
- Role of AWS Security Hub and Inspector
- Creating custom response workflows using Step Functions
- Integrating with external SIEM and SOAR tools

- **Case Study:** Ransomware mitigation via Lambda-triggered quarantine

Module 3: Azure Incident Response Playbooks

- Utilizing Azure Sentinel and Microsoft Defender for Cloud
- Setting up alert rules and analytic rules
- Automation with Logic Apps and Playbook templates
- Azure Monitor integration and log analytics
- Role-based access control (RBAC) in incident handling
- **Case Study:** Detecting and mitigating lateral movement in Azure AD

Module 4: GCP Incident Response Playbooks

- Using Security Command Center for threat detection
- Real-time monitoring with Stackdriver
- Playbook automation using Cloud Functions
- IAM policy auditing and enforcement
- Logging and forensic tools (Cloud Audit Logs, Chronicle)
- **Case Study:** Phishing attack via compromised GCP account

Module 5: Multi-Cloud Incident Response Strategy

- Coordinating response across AWS, Azure, and GCP
- Setting up federated threat detection
- Unified SIEM/SOAR integration
- Synchronizing playbooks and compliance measures
- Cloud-native vs hybrid approaches
- **Case Study:** Coordinated response to crypto-mining malware in multi-cloud

Module 6: Cloud Security Automation & Orchestration

- Introduction to SOAR platforms (Splunk Phantom, Palo Alto Cortex XSOAR)
- Writing automated playbooks using Python and YAML
- Event-driven automation using serverless technologies
- CI/CD pipeline integration for rapid mitigation
- Alert fatigue reduction via machine learning
- **Case Study:** Using AI to suppress false positives in alerting system

Module 7: Compliance and Regulatory Response Playbooks

- Mapping cloud IR to ISO 27001, SOC 2, and NIST
- Handling Personally Identifiable Information (PII) breaches
- Legal implications and breach notification workflows
- Documentation and audit readiness
- Third-party cloud compliance tools
- **Case Study:** GDPR breach response involving Azure-hosted application

Module 8: Advanced Threat Intelligence and Response

- Integrating threat feeds into cloud playbooks
- MITRE ATT&CK framework mapping
- Using threat intel for proactive defense
- Behavioral analytics and anomaly detection
- Cloud honeypots and deception technologies
- **Case Study:** Insider threat detected via anomaly-based alerting in GCP

Training Methodology

- Hands-on labs with real-time cloud platform simulations
- Interactive demos for AWS, Azure, and GCP environments
- Scenario-based learning with guided playbook development
- Group activities to encourage collaborative problem-solving
- Expert-led walkthroughs of actual incident response cases
- Assessment quizzes and capstone project for practical validation

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	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500

Start Date	End Date	Location	Price
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

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

Register Online Now

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