Training Course on Cloud Security Posture Management (CSPM) for IR

Professional Development Training Course Outline

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

Course Introduction

As cloud adoption accelerates across industries, organizations face increasingly sophisticated cyber threats targeting their cloud infrastructures. Cloud Security Posture Management (CSPM) has emerged as a critical framework to ensure continuous security and compliance across cloud environments. Training Course on Cloud Security Posture Management (CSPM) for Incident Response (IR) empowers cybersecurity professionals with the skills and tools required to proactively identify misconfigurations, automate remediation, and integrate CSPM with Incident Response (IR) workflows. With the rise of hybrid and multi-cloud ecosystems, it is imperative to adopt scalable and intelligent posture management strategies that mitigate risk exposure and enable rapid threat containment.

Designed by industry experts, this hands-on training covers best practices in cloud threat intelligence, real-time posture assessment, compliance automation, and forensics-driven response mechanisms. Participants will engage in real-world case studies, lab simulations, and scenario-based learning tailored to the most current cloud attack vectors. Whether you are a cloud security engineer, compliance officer, or IR team lead, this course will enhance your technical proficiency in cloud-native security tools, policy enforcement, and automated remediation orchestration, paving the way for secure cloud transformation.

Programme Curriculum

Training Course on Cloud Security Posture Management (CSPM) for Incident Response (IR)

Introduction

As cloud adoption accelerates across industries, organizations face increasingly sophisticated cyber threats targeting their cloud infrastructures. Cloud Security Posture Management (CSPM) has emerged as a critical framework to ensure continuous security and compliance across cloud environments. Training Course on Cloud Security Posture Management (CSPM) for Incident Response (IR) empowers cybersecurity professionals with the skills and tools required to proactively identify misconfigurations, automate remediation, and integrate CSPM with Incident Response (IR) workflows. With the

rise of hybrid and multi-cloud ecosystems, it is imperative to adopt scalable and intelligent posture management strategies that mitigate risk exposure and enable rapid threat containment.

Designed by industry experts, this hands-on training covers best practices in cloud threat intelligence, real-time posture assessment, compliance automation, and forensics-driven response mechanisms. Participants will engage in real-world case studies, lab simulations, and scenario-based learning tailored to the most current cloud attack vectors. Whether you are a cloud security engineer, compliance officer, or IR team lead, this course will enhance your technical proficiency in cloud-native security tools, policy enforcement, and automated remediation orchestration, paving the way for secure cloud transformation.

Course Objectives

1. Understand the fundamentals of Cloud Security Posture Management (CSPM).
2. Analyze common cloud misconfigurations and their impact on risk posture.
3. Integrate CSPM tools with SIEM/SOAR platforms for enhanced IR.
4. Automate detection and remediation of cloud security gaps.
5. Utilize compliance frameworks like CIS Benchmarks, NIST, and ISO in CSPM.
6. Monitor and respond to real-time cloud threats and anomalies.
7. Conduct incident response playbook development specific to CSPM alerts.
8. Implement cloud-native forensics and logging for post-incident investigation.
9. Perform continuous cloud security assessment using AI and ML.
10. Establish and enforce zero-trust policies across cloud environments.
11. Investigate and remediate IAM role escalation and privilege misuse.
12. Explore the role of DevSecOps in CSPM integration pipelines.
13. Conduct case-based analysis of major cloud data breaches.

Target Audience

1. Cloud Security Engineers
2. SOC Analysts and Incident Responders
3. Cybersecurity Architects
4. Cloud DevOps and DevSecOps Teams
5. Compliance and Risk Officers
6. IT Managers and CIOs
7. Cloud Infrastructure Teams
8. Security Consultants and Auditors

Course Duration: 5 days

Course Modules

Module 1: Introduction to CSPM and Cloud Threat Landscape

- Overview of CSPM and its role in IR
- Evolving cloud threat vectors
- CSPM architecture and core components
- Cloud visibility and asset inventory
- Risk scoring and prioritization
- **Case Study**: AWS S3 Breach Due to Public Misconfiguration

Module 2: Cloud Misconfiguration Management and Detection

- Types of cloud misconfigurations
- Automated scanning and detection techniques
- Role of Infrastructure as Code (IaC) in misconfigurations

- Alert tuning and false positive reduction
- Integrating compliance rules into CSPM
- **Case Study**: Azure Container Misconfiguration Incident

Module 3: Policy Enforcement and Compliance Mapping

- Mapping CSPM to regulatory standards (HIPAA, NIST, GDPR)
- Building policy-as-code with tools like Terraform and Open Policy Agent
- Role of CSPM in continuous compliance
- Risk scoring aligned with business objectives
- Reporting and audit readiness
- **Case Study**: GCP PCI-DSS Compliance Gap Analysis

Module 4: Incident Detection and Response with CSPM

- Role of CSPM in early incident detection
- Event correlation with SIEM/SOAR tools
- Creating incident response workflows
- CSPM alert classification and escalation
- Mitigation and rollback strategies
- **Case Study**: Cloud Ransomware Detection and Response

Module 5: Forensics and Investigation in Cloud Environments

- Capturing evidence using cloud-native tools
- Centralized logging and audit trails
- Real-time threat hunting using CSPM data
- Chain-of-custody practices in cloud forensics
- Post-incident reporting and RCA
- **Case Study**: IAM Credential Abuse Forensic Review

Module 6: Automation and Remediation Strategies

- Automated remediation scripting with Lambda, Azure Functions
- Leveraging APIs for dynamic security controls
- Real-time posture correction and rollback
- Orchestration with CI/CD pipelines
- Workflow automation with SOAR and CSPM
- **Case Study**: Auto-Remediation of Unused Security Groups

Module 7: Zero Trust and Identity-Centric Security in CSPM

- Role of IAM in CSPM effectiveness
- Least privilege enforcement and MFA policies
- Cloud identity lifecycle management
- Detecting over-privileged accounts and roles
- Aligning CSPM with Zero Trust principles
- **Case Study**: Cross-Account IAM Role Escalation Attack

Module 8: Building CSPM and IR into DevSecOps

- Integrating CSPM checks into CI/CD pipelines
- Pre-deployment misconfiguration checks
- Shift-left security strategies
- Developer-friendly security tooling
- Feedback loops between IR and DevSecOps

- **Case Study**: CloudFormation Template with Vulnerable Defaults

Training Methodology

- Instructor-led online/live sessions
- Hands-on lab environments and simulations
- Real-world case study analysis
- Interactive Q&A and whiteboard brainstorming
- Capstone project and group-based assessments
- Certification of completion and post-training support

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
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

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

Register Online Now

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