Training Course on Cloud Environment Threat Hunting

Professional Development Training Course Outline

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

Course Introduction

Training Course on Cloud Environment Threat Hunting provides a comprehensive deep dive into **proactive cybersecurity** strategies for **Cloud Environments**, equipping security professionals with the essential skills and methodologies for **threat detection** and **incident response**. As organizations rapidly migrate to the cloud, the attack surface expands, demanding specialized expertise in identifying and neutralizing **advanced persistent threats (APTs)** and **emerging cyber threats** that bypass traditional security controls. Participants will master **hypothesis-driven threat hunting**, leveraging **cloud-native tools** and **cutting-edge analytics** to uncover hidden malicious activities, strengthen **cloud security posture**, and significantly reduce organizational risk in complex **multi-cloud infrastructures**.

The modern cyber landscape is characterized by increasingly sophisticated adversaries targeting dynamic **cloud workloads** and **containerized environments**. This course addresses the critical need for skilled **threat hunters** who can proactively search for anomalies, indicators of compromise (IOCs), and indicators of attack (IOAs) across vast cloud telemetry data. Through practical, **hands-on labs** and **real-world case studies**, attendees will gain proficiency in **cloud forensics**, **log analysis**, and leveraging **threat intelligence** to predict and preempt cyberattacks, ultimately building resilient **cloud security operations** and enhancing overall organizational **cyber resilience**.

Programme Curriculum

Training Course on Cloud Environment Threat Hunting

Introduction

Training Course on Cloud Environment Threat Hunting provides a comprehensive deep dive into **proactive cybersecurity** strategies for **Cloud Environments**, equipping security professionals with

the essential skills and methodologies for **threat detection** and **incident response**. As organizations rapidly migrate to the cloud, the attack surface expands, demanding specialized expertise in identifying and neutralizing **advanced persistent threats (APTs)** and **emerging cyber threats** that bypass traditional security controls. Participants will master **hypothesis-driven threat hunting**, leveraging **cloud-native tools** and **cutting-edge analytics** to uncover hidden malicious activities, strengthen **cloud security posture**, and significantly reduce organizational risk in complex **multi-cloud infrastructures**.

The modern cyber landscape is characterized by increasingly sophisticated adversaries targeting dynamic **cloud workloads** and **containerized environments**. This course addresses the critical need for skilled **threat hunters** who can proactively search for anomalies, indicators of compromise (IOCs), and indicators of attack (IOAs) across vast cloud telemetry data. Through practical, **hands-on labs** and **real-world case studies**, attendees will gain proficiency in **cloud forensics**, **log analysis**, and leveraging **threat intelligence** to predict and preempt cyberattacks, ultimately building resilient **cloud security operations** and enhancing overall organizational **cyber resilience**.

Course Duration

5 days

Course Objectives

1. Master Cloud Security Posture Management (CSPM) and identify misconfigurations.
2. Develop Hypothesis-Driven Threat Hunting methodologies for diverse cloud platforms (AWS, Azure, GCP).
3. Utilize Cloud-Native Security Tools for advanced threat detection and response.
4. Conduct comprehensive Cloud Log Analysis and leverage Security Information and Event Management (SIEM) for anomaly detection.
5. Apply the MITRE ATT&CK Framework to map adversary tactics, techniques, and procedures (TTPs) in cloud environments.
6. Perform Container Security Monitoring and identify malicious images and runtime behaviors.
7. Investigate Serverless Security vulnerabilities and threat vectors.
8. Implement Data Exfiltration Detection and prevention strategies in cloud storage.
9. Analyze Network Traffic Patterns and detect lateral movement within cloud VPCs.
10. Develop effective Incident Response Playbooks specifically tailored for cloud breaches.
11. Integrate Threat Intelligence Feeds to enrich hunting activities and predict emerging threats.
12. Automate Cloud Threat Hunting Workflows using scripting and orchestration tools.
13. Conduct Cloud Forensics Investigations to reconstruct attack chains and identify root causes.

Organizational Benefits

- Detect and neutralize sophisticated cyber threats before they escalate into full-blown breaches, significantly reducing potential financial and reputational damage.
- Identify and remediate critical vulnerabilities and misconfigurations across diverse cloud environments, strengthening overall defense capabilities.
- Develop highly effective cloud-specific incident response plans, leading to faster containment and recovery times.
- Equip security teams with the skills to rapidly identify and address threats, minimizing their impact.
- Leverage cloud-native security features and existing tools more effectively, maximizing ROI on security infrastructure.

- Ensure adherence to industry regulations and compliance frameworks by proactively identifying and addressing security risks.
- Build a more robust and adaptive security program capable of withstanding evolving cyber threats.
- Empower security analysts and incident responders with specialized cloud security expertise, addressing the industry's skills gap.

Target Audience

1. Security Analysts and SOC Analysts
2. Incident Responders and Digital Forensics Professionals
3. Cloud Security Engineers and Architects
4. Cybersecurity Professionals seeking cloud specialization
5. DevSecOps Engineers
6. IT Security Managers and Leaders
7. Threat Intelligence Analysts
8. Anyone responsible for Securing Cloud Environments

Course Outline

Module 1: Introduction to Cloud Threat Hunting

- Understanding the Cloud Shared Responsibility Model and its implications for threat hunting.
- Defining threat hunting in the context of cloud environments (proactive vs. reactive).
- Key differences in threat hunting methodologies for On-Premise vs. Cloud.
- Leveraging the Cyber Kill Chain and MITRE ATT&CK for cloud attack scenarios.
- Case Study: Analyzing a public cloud data breach (e.g., Capital One breach) to understand initial access and lateral movement in the cloud.

Module 2: Cloud Platform Fundamentals for Threat Hunters

- Overview of major cloud providers: AWS, Azure, and Google Cloud Platform (GCP).
- Understanding core cloud services relevant to security: Compute, Storage, Networking, Identity and Access Management (IAM).
- Exploring cloud-native logging and monitoring services (e.g., CloudTrail, Azure Monitor, Cloud Logging).
- Introduction to Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platforms (CWPP).
- Case Study: Identifying misconfigurations in S3 buckets leading to data exposure and how a threat hunt could have prevented it.

Module 3: Cloud Data Sources and Log Analysis

- Collecting and centralizing cloud logs for effective threat hunting.
- Analyzing VPC Flow Logs, CDN logs, DNS logs, and API activity logs.
- Utilizing SIEM/SOAR platforms for log correlation and anomaly detection in cloud environments.
- Leveraging Cloud-native security services for log enrichment and threat feeds.
- Case Study: Hunting for unusual API calls and access patterns indicative of compromised cloud credentials.

Module 4: Hypothesis-Driven Cloud Threat Hunting

- Developing effective threat hunting hypotheses based on threat intelligence and common cloud attack vectors.
- Techniques for proactive searching: statistical analysis, behavioral analytics, and clustering.
- Building custom queries and rules for detecting evasive threats.
- Iterative refinement of hypotheses based on hunt outcomes.
- Case Study: Formulating and testing hypotheses around cryptojacking activities in compromised cloud compute instances.

Module 5: Threat Hunting in Cloud Compute and Container Environments

- Hunting for malicious activity in EC2, Azure VMs, and GCP Compute Engine instances.
- Container security: Image scanning, runtime protection, and monitoring container orchestration platforms (Kubernetes).
- Detecting living-off-the-land techniques and compromised binaries in cloud workloads.
- Analyzing process execution and network connections within cloud virtual machines.
- Case Study: Uncovering a sophisticated supply chain attack targeting container images in a Kubernetes cluster.

Module 6: Hunting for Threats in Cloud Identity and Data Storage

- Investigating suspicious IAM activities, privilege escalation attempts, and compromised roles/users.
- Detecting unauthorized access and data manipulation in cloud storage services (e.g., S3, Azure Blob Storage, Cloud Storage).
- Hunting for sensitive data exposure and exfiltration attempts.
- Analyzing access control lists (ACLs) and security policies for misconfigurations.
- Case Study: Tracing an insider threat who exfiltrated sensitive customer data from a cloud database using legitimate but abused credentials.

Module 7: Advanced Cloud Threat Hunting Techniques

- Automating threat hunting with serverless functions and orchestration tools.
- Applying machine learning and behavioral analytics for advanced anomaly detection.
- Reverse engineering cloud-specific malware and attack tools.
- Red teaming and purple teaming exercises in cloud environments to validate hunting capabilities.
- Case Study: Implementing automated detection rules for a newly discovered cloud-specific vulnerability using serverless functions.

Module 8: Cloud Incident Response and Post-Hunt Actions

- Developing cloud-specific incident response plans and playbooks.
- Containment, eradication, and recovery strategies for cloud breaches.
- Post-incident analysis, lessons learned, and hardening cloud environments.
- Integrating threat hunting findings into continuous security improvement.
- Case Study: Responding to a ransomware attack on cloud-hosted data, including data recovery and forensic investigation steps.

Training Methodology

This course adopts a highly interactive and **hands-on training methodology** to ensure practical skill development and immediate applicability.

- **Instructor-Led Sessions:** Expert-led discussions on core concepts, advanced techniques, and real-world scenarios.
- **Interactive Labs:** Extensive practical exercises using simulated cloud environments (AWS, Azure, GCP) to apply learned concepts. Participants will gain direct experience with cloud security tools and platforms.
- **Case Studies and Group Discussions:** In-depth analysis of real-world cloud breaches and attack scenarios to foster critical thinking and problem-solving.
- **Hypothesis-Driven Exercises:** Participants will develop and execute their own threat hunts based on provided scenarios and datasets.
- **Tool Demonstrations:** Live demonstrations of industry-leading cloud security and threat hunting tools.
- **Q&A and Collaborative Learning:** Encouraging active participation, peer-to-peer learning, and addressing specific challenges faced by attendees.

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
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