AWS Security Hub and GuardDuty Implementation 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

An AWS Security Hub and GuardDuty Implementation Training course is a crucial offering for professionals looking to master Cloud Security Posture Management and intelligent threat detection within their Amazon Web Services environments. AWS Security Hub and GuardDuty Implementation Training Course provides the practical, hands-on experience needed to deploy, configure, and operate these two foundational AWS security services in tandem to achieve a unified security view and automated incident response.

The course delivers a deep dive into leveraging Amazon GuardDuty for real-time, AI-powered threat intelligence and correlating its findings with other security services, all aggregated and prioritized by AWS Security Hub. Participants will learn to move beyond basic enablement to implement multi-account security strategies using AWS Organizations, establish sophisticated compliance checks against industry standards like CIS and PCI DSS, and build Serverless remediation workflows using AWS EventBridge and AWS Lambda. Mastering this integration is paramount for DevSecOps and Security Operations Center teams aiming to significantly reduce their Mean Time to Detect and Mean Time to Respond to potential threats, ensuring a robust and zero-trust security architecture for critical cloud workloads.

Programme Curriculum

AWS Security Hub and GuardDuty Implementation Training Course

Introduction

An AWS Security Hub and GuardDuty Implementation Training course is a crucial offering for professionals looking to master Cloud Security Posture Management and intelligent threat detection within their Amazon Web Services environments. AWS Security Hub and GuardDuty Implementation Training Course provides the practical, hands-on experience needed to deploy, configure, and operate these two foundational AWS security services in tandem to achieve a unified security view and automated incident response.

The course delivers a deep dive into leveraging Amazon GuardDuty for real-time, AI-powered threat intelligence and correlating its findings with other security services, all aggregated and prioritized by AWS Security Hub. Participants will learn to move beyond basic enablement to implement multi-account security strategies using AWS Organizations, establish sophisticated compliance checks against industry standards like CIS and PCI DSS, and build Serverless remediation workflows using AWS EventBridge and AWS Lambda. Mastering this integration is paramount for DevSecOps and Security Operations Center teams aiming to significantly reduce their Mean Time to Detect and Mean Time to Respond to potential threats, ensuring a robust and zero-trust security architecture for critical cloud workloads.

Course Duration

5 days

Course Objectives

1. Deploy and Configure both AWS Security Hub and Amazon GuardDuty across a multi-account AWS environment using AWS Organizations.
2. Master Cloud Security Posture Management (CSPM) by enabling and customizing security standards like AWS Foundational Security Best Practices, CIS, and PCI DSS.
3. Implement centralized security finding aggregation and cross-region consolidation for a unified global security view.
4. Analyze, prioritize, and investigate GuardDuty findings within the Security Hub console.
5. Design and implement automated incident response workflows using AWS EventBridge and AWS Lambda for remediation actions.
6. Configure and manage Security Hub automation rules to suppress non-actionable findings and enrich critical alerts.
7. Integrate findings from other key security services into Security Hub for a comprehensive security data lake.
8. Utilize Trusted IP Lists and Threat Lists in GuardDuty to fine-tune threat detection accuracy and reduce false positives.
9. Apply DevSecOps principles by monitoring security compliance continuously and integrating security feedback loops into deployment pipelines.
10. Implement advanced GuardDuty features, including EKS Protection, S3 Protection, RDS Protection, and Malware Protection for EC2.
11. Generate insightful compliance reports and security posture dashboards for executive-level visibility and auditing.
12. Understand the cost implications and optimization best practices for running both Security Hub and GuardDuty at scale.
13. Establish a robust Security Operations Center workflow for triaging and escalating high-severity security alerts and achieving a lower MTTR.

Target Audience

1. Cloud Security Engineers
2. Security Operations Center Analysts
3. DevSecOps Engineers
4. AWS Solutions Architects
5. Compliance and Audit Professionals
6. Cloud System Administrators
7. Cloud Consultants/Advisors

8. Security Developers

Course Modules

Module 1: Foundational Setup & Architecture

- Introduction to the AWS Shared Responsibility Model and the role of Detective Controls.
- Enabling and delegating administrator accounts for Security Hub and GuardDuty via AWS Organizations.
- Configuring cross-region finding aggregation for global visibility.
- Reviewing initial security posture findings against the FSBP Standard.
- Case Study: Securing the Enterprise Landing Zone.

Module 2: Deep Dive into Amazon GuardDuty Threat Detection

- Understanding GuardDuty's threat intelligence and machine learning models.
- Analyzing GuardDuty data sources.
- Implementing and tuning Trusted IP Lists and Threat Lists to refine findings.
- Working with different GuardDuty finding types, severity levels, and the Finding Format.
- Case Study: Simulating Credential Compromise.

Module 3: Advanced GuardDuty Protections

- Enabling and investigating findings from GuardDuty EKS Runtime Monitoring.
- Configuring Malware Protection for EC2
- Implementing S3 Protection to detect policy changes, unauthorized data access, and suspicious API activity on buckets.
- Deploying and monitoring RDS Protection for database threat detection.
- Case Study: Data Exfiltration Prevention.

Module 4: Security Hub Posture Management and Standards

- Enabling and managing built-in Security Standards
- Reviewing and triaging Security Hub Findings for configuration drift and compliance gaps.
- Customizing and creating Security Hub automation rules for auto-archiving and suppression.
- Understanding the relationship and data flow between Security Hub, AWS Config, and AWS Config Rules.
- Case Study: Achieving CIS Compliance.

Module 5: Integration with Other AWS Security Services

- Integrating findings from Amazon Inspector into Security Hub.
- Connecting Amazon Macie for sensitive data discovery and reporting.
- Leveraging AWS IAM Access Analyzer findings within the unified dashboard.
- Configuring Custom Product Integrations for third-party security tools.
- Case Study: Vulnerability-to-Threat Correlation.

Module 6: Automated Incident Response and Remediation

- Designing the Serverless Security Automation architecture using EventBridge and Lambda.
- Creating EventBridge rules to capture high-severity Security Hub events.
- Developing and deploying Lambda functions for automated remediation

- Implementing Custom Actions in Security Hub for analyst-initiated workflows.
- Case Study: Automated EC2 Isolation.

Module 7: Security Operations and Reporting

- Building effective Security Hub dashboards and custom insights for continuous monitoring.
- Generating compliance reports and metrics for management and auditors.
- Defining a clear Security Operations Center workflow for triaging, investigation, and escalation using Security Hub's severity and workflow status fields.
- Integrating Security Hub with Amazon Detective for faster root cause analysis (RCA).
- Case Study: Executive Security Briefing

Module 8: Optimization, Governance, and Best Practices

- Cost Optimization strategies for GuardDuty and Security Hub.
- Implementing Least Privilege for the delegated administrator and SOC roles.
- Advanced Suppression Rules and Finding Filtering best practices to manage signal-to-noise ratio.
- Reviewing the AWS Security Reference Architecture for GuardDuty and Security Hub deployment.
- Case Study: Cost and Noise Reduction.

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