AWS Secure Builder Micro-Credential (SANS) 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 AWS Secure Builder Micro-Credential training course provides a focused, hands-on path to validating competency in securing and managing Amazon Web Services environments. This training is crucial for engineering and development teams to shift security left, embedding secure-by-design principles directly into the build process. By mastering key areas like Identity and Access Management, DevSecOps pipeline security, and effective workload hardening, participants significantly reduce an organization's cloud risk posture and accelerate time-to-market. The course emphasizes practical, immediately applicable skills to tackle modern threats, including those related to the supply chain and complex misconfigurations.

This micro-credential, aligned with the GIAC AWS Secure Builder certification, goes beyond theoretical knowledge, offering technical staff the essential skills to build and deploy resilient, compliant workloads from the outset. AWS Secure Builder Micro-Credential (SANS) Training Course is designed to empower builder?ÇÖs developers, cloud engineers, and architects to own security within the Shared Responsibility Model. It features extensive hands-on labs focused on real-world scenarios in security monitoring, incident response best practices, and implementing Zero Trust principles. Successful completion validates an individual's ability to proactively defend against common AWS attack vectors, ensuring a robust and defensible cloud infrastructure.

Programme Curriculum

AWS Secure Builder Micro-Credential (SANS) Training Course

Introduction

The AWS Secure Builder Micro-Credential training course provides a focused, hands-on path to validating competency in securing and managing Amazon Web Services environments. This training is crucial for engineering and development teams to shift security left, embedding secure-by-design principles directly into

the build process. By mastering key areas like Identity and Access Management, DevSecOps pipeline security, and effective workload hardening, participants significantly reduce an organization's cloud risk posture and accelerate time-to-market. The course emphasizes practical, immediately applicable skills to tackle modern threats, including those related to the supply chain and complex misconfigurations.

This micro-credential, aligned with the GIAC AWS Secure Builder certification, goes beyond theoretical knowledge, offering technical staff the essential skills to build and deploy resilient, compliant workloads from the outset. AWS Secure Builder Micro-Credential (SANS) Training Course is designed to empower builder?ÇÖs developers, cloud engineers, and architects to own security within the Shared Responsibility Model. It features extensive hands-on labs focused on real-world scenarios in security monitoring, incident response best practices, and implementing Zero Trust principles. Successful completion validates an individual's ability to proactively defend against common AWS attack vectors, ensuring a robust and defensible cloud infrastructure.

Course Duration

5 days

Course Objectives

1. Master AWS IAM best practices and secure access controls to enforce the principle of least privilege across all AWS resources.
2. Apply advanced configuration and workload hardening techniques for core services like Amazon S3, EC2, RDS, and API Gateway.
3. Integrate security tooling and checks into DevSecOps and CI/CD pipelines to prevent misconfigurations and supply chain vulnerabilities.
4. Identify and remediate the most common and high-impact AWS cloud misconfigurations leading to data exposure and breaches.
5. Deeply understand and effectively implement security controls in line with the AWS Shared Responsibility Model for maximum coverage.
6. Implement centralized security monitoring, logging, and alerting using AWS services like CloudTrail, GuardDuty, and Security Hub.
7. Design and implement Zero Trust architecture concepts within an AWS environment to enhance perimeter and micro-segmentation security.
8. Understand and apply controls to mitigate risks from third-party reliance and supply chain attacks within cloud deployments.
9. Design and implement robust data protection strategies using AWS KMS and encryption mechanisms for data at rest and in transit.
10. Use Open-Source Intelligence and attack surface analysis to proactively identify and defend against likely cloud attack vectors.
11. Execute the six-step incident response process tailored for AWS environments, including containment and recovery best practices.
12. Leverage AWS Lambda and other services to implement security automation and streamline repetitive security tasks.
13. Apply security controls that meet industry standards and regulatory compliance requirements within AWS deployments.

Target Audience

1. Cloud Engineers and Developers
2. DevSecOps Practitioners

3. Cloud Architects and Solutions Architects
4. Security Operations Analysts
5. Site Reliability Engineers
6. Software Engineers building on AWS
7. Technical Leaders and Engineering Managers
8. Vulnerability Analysts transitioning to Cloud

Course Modules

Module 1: AWS Shared Responsibility & Foundation Security

- Understanding the Shared Responsibility Model and its business impact.
- Securely configuring the AWS Root Account and organization structure.
- Implementing Security Best Practices for initial account setup
- Case Study: Analyzing a major S3 bucket breach due to misunderstanding of the shared model.
- Securing foundational network services like VPC, Security Groups, and NACLs.

Module 2: Identity & Access Management (IAM) Deep Dive

- Designing and implementing Least Privilege policies using IAM roles and resource policies.
- Mastering AWS STS and temporary credentials for cross-account access.
- Securing and auditing IAM Users, Groups, and Roles for compliance.
- Case Study: Reviewing a privilege escalation attack stemming from an overly permissive IAM policy.
- Implementing Identity Federation with AWS IAM Identity Centre

Module 3: Workload Hardening for Compute & Data Services

- Hardening Amazon **EC2** instances and associated launch templates.
- Securing relational and non-relational databases
- Implementing encryption and secure access controls for Amazon S3 and data lakes.
- Case Study: Mitigating a server-side request forgery vulnerability in an EC2 metadata service exploitation.
- Using AWS WAF and Shield for application-level protection.

Module 4: Secure Continuous Integration/Continuous Delivery

- Integrating SAST/DAST and Secret Scanning into the CI/CD pipeline.
- Securing code repositories and build environments
- Implementing Infrastructure as Code Security using tools like Terraform/CloudFormation with security linters.
- Case Study: Preventing a malicious code injection attack on a deployment pipeline by enforcing branch protection and least-privilege runners.
- Automating security policy enforcement using Service Control Policies

Module 5: Security Monitoring, Logging, and Alerting

- Centralized logging with CloudTrail and VPC Flow Logs for visibility.
- Implementing threat detection with Amazon GuardDuty and automated responses.
- Consolidating and analyzing findings using AWS Security Hub and Amazon Detective.
- Case Study: Tracing an unauthorized API call from detection in CloudTrail logs to containment.
- Setting up custom, actionable CloudWatch Alarms and Events for key security metrics.

Module 6: Cloud Data Protection and Encryption

- Implementing and managing keys with AWS Key Management Service and CloudHSM.
- Enforcing encryption-at-rest and in-transit for sensitive data stores.
- Discovering and protecting sensitive data using Amazon Macie.
- Case Study: Designing a solution for a PCI-DSS compliant application requiring strict key rotation and separation of duties for cryptographic operations.
- Securely managing application secrets with AWS Secrets Manager and AWS Parameter Store.

Module 7: Incident Response and Mitigation

- Developing a concise Cloud-Specific Incident Response Plan and playbooks.
- Executing the containment, eradication, and recovery phases in an AWS context.
- Securely isolating and performing forensics on a compromised EC2 instance.
- Case Study: Responding to a compromised AWS Access Key and the necessary steps for remediation and blast radius reduction.
- Utilizing AWS services for automated response actions.

Module 8: Zero Trust, Supply Chain, and Emerging Risks

- Applying Zero Trust principles to network segmentation and user access models.
- Assessing vendor reliance and third-party risk for the cloud supply chain.
- Securing Serverless workloads against emerging vectors.
- Case Study: Evaluating the risk of using a vulnerable third-party container image from a public registry and implementing a secure vetting process.
- Introduction to Cloud Security Posture Management tools and continuous audit.

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