



Security Engineering on AWS

AWS AT LUMIFY WORK

Lumify Work is an official AWS Training Partner for Australia, New Zealand, and the Philippines. Through our Authorised AWS Instructors, we can provide you with a learning path that's relevant to you and your organisation, so you can get more out of the cloud. We offer virtual and face-to-face classroom-based training to help you build your cloud skills and enable you to achieve industry-recognised AWS Certification.



LENGTH

3 days

WHY STUDY THIS COURSE

Security is a concern for both customers in the cloud, and those considering cloud adoption. An increase in cyberattacks and data leaks remains top of mind for most industry personnel. The Security Engineering on AWS course addresses these concerns by helping you better understand how to interact and build with Amazon Web Services (AWS) in a secure way.

In this course, you will learn about managing identities and roles, managing and provisioning accounts, and monitoring API activity for anomalies. You will also learn about how to protect data stored on AWS. The course explores how you can generate, collect, and monitor logs to help identify security incidents. Finally, you will review detecting and investigating security incidents with AWS services.

This intermediate-level course is delivered through a mix of instructor-led training (ILT), hands-on labs, and group exercises.

We also offer a one-day AWS Jam Session to complement this course and enhance your learning. The AWS Jam is a gamified event, with teams competing to score points by completing a series of challenges based on concepts covered in the course.

See more information and scheduled dates [here](#).

WHAT YOU'LL LEARN

This course is designed to teach participants how to:

- › State an understanding of AWS cloud security based on the CIA triad.
- › Create and analyse authentication and authorisations with IAM.
- › Manage and provision accounts on AWS with appropriate AWS services.
- › Identify how to manage secrets using AWS services.

<https://www.lumifywork.com/en-ph/courses/security-engineering-on-aws/>





Security Engineering on AWS



My instructor was great being able to put scenarios into real world instances that related to my specific situation.

I was made to feel welcome from the moment I arrived and the ability to sit as a group outside the classroom to discuss our situations and our goals was extremely valuable.

I learnt a lot and felt it was important that my goals by attending this course were met.

Great job Lumify Work team.



AMANDA NICOL
IT SUPPORT SERVICES
MANAGER - HEALTH WORLD
LIMITED

- › Monitor sensitive information and protect data via encryption and access controls.
- › Identify AWS services that address attacks from external sources.
- › Monitor, generate, and collect logs.
- › Identify indicators of security incidents.
- › Identify how to investigate threats and mitigate using AWS services

<https://www.lumifywork.com/en-ph/courses/security-engineering-on-aws/>





Security Engineering on AWS

COURSE SUBJECTS

Module 1: Security Overview and Review

- Explain Security in the AWS Cloud.
- Explain AWS Shared Responsibility Model.
- Summarise IAM, Data Protection, and Threat Detection and Response.
- State the different ways to interact with AWS using the console, CLI, and SDKs.
- Describe how to use MFA for extra protection.
- State how to protect the root user account and access keys.

Module 2: Securing Entry Points on AWS

- Describe how to use multi-factor authentication (MFA) for extra protection.
- Describe how to protect the root user account and access keys.
- Describe IAM policies, roles, policy components, and permission boundaries.
- Explain how API requests can be logged and viewed using AWS CloudTrail and how to view and analyse access history.
- Hands-On Lab: Using Identity and Resource Based Policies.

Module 3: Account Management and Provisioning on AWS

- Explain how to manage multiple AWS accounts using AWS Organisations and AWS Control Tower.
- Explain how to implement multi-account environments with AWS Control Tower.
- Demonstrate the ability to use identity providers and brokers to acquire access to AWS services.

Lumify Work Customised Training

We can also deliver and customise this training course for larger groups saving your organisation time, money and resources.

For more information, please contact us on [02 8286 9429](tel:0282869429).

<https://www.lumifywork.com/en-ph/courses/security-engineering-on-aws/>



Security Engineering on AWS

- Explain the use of AWS IAM Identity Center (successor to AWS Single Sign-On) and AWS Directory Service.
- Demonstrate the ability to manage domain user access with Directory Service and IAM Identity Center.
- Hands-On Lab: Managing Domain User Access with AWS Directory Service

Module 4: Secrets Management on AWS

- Describe and list the features of AWS KMS, CloudHSM, AWS Certificate Manager (ACM), and AWS Secrets Manager.
- Demonstrate how to create a multi-Region AWS KMS key.
- Demonstrate how to encrypt a Secrets Manager secret with an AWS KMS key.
- Demonstrate how to use an encrypted secret to connect to an Amazon Relational Database Service (Amazon RDS) database in multiple AWS Regions
- Hands-on lab: Lab 3: Using AWS KMS to Encrypt Secrets in Secrets Manager

Module 5: Data Security

- Monitor data for sensitive information with Amazon Macie.
- Describe how to protect data at rest through encryption and access controls.
- Identify AWS services used to replicate data for protection.
- Determine how to protect data after it has been archived.
- Hands-on lab: Lab 4: Data Security in Amazon S3

Module 6: Infrastructure Edge Protection

<https://www.lumifywork.com/en-ph/courses/security-engineering-on-aws/>





Security Engineering on AWS

- Describe the AWS features used to build secure infrastructure.
- Describe the AWS services used to create resiliency during an attack.
- Identify the AWS services used to protect workloads from external threats.
- Compare the features of AWS Shield and AWS Shield Advanced.
- Explain how centralised deployment for AWS Firewall Manager can enhance security.
- Hands-on lab: Lab 5: Using AWS WAF to Mitigate Malicious Traffic

Module 7: Monitoring and Collecting Logs on AWS

- Identify the value of generating and collecting logs.
- Use Amazon Virtual Private Cloud (Amazon VPC) Flow Logs to monitor for security events.
- Explain how to monitor for baseline deviations.
- Describe Amazon EventBridge events.
- Describe Amazon CloudWatch metrics and alarms.
- List log analysis options and available techniques.
- Identify use cases for using virtual private cloud (VPC) Traffic Mirroring.
- Hands-on lab: Lab 6: Monitoring for and Responding to Security Incidents

Module 8: Responding to Threats

- Classify incident types in incident response.
- Understand incident response workflows.
- Discover sources of information for incident response using AWS services.
- Understand how to prepare for incidents.

<https://www.lumifywork.com/en-ph/courses/security-engineering-on-aws/>





CLOUD COMPUTING AND VIRTUALISATION

Security Engineering on AWS

- Detect threats using AWS services.
- Analyse and respond to security findings.
- Hands-on lab: Lab 7: Incident Response

Please note: This is an emerging technology course. Course outline is subject to change as needed.

<https://www.lumifywork.com/en-ph/courses/security-engineering-on-aws/>





CLOUD COMPUTING AND VIRTUALISATION

Security Engineering on AWS

WHO IS THE COURSE FOR?

This course is intended for:

- Security engineers
- Security architects
- Cloud architects
- Cloud operators working across all global segments

PREREQUISITES

It is recommended that attendees have the following prerequisites:

- Working knowledge of IT security practices and infrastructure concepts
- Familiarity with the AWS cloud
- Completed [AWS Security Essentials](#) course
- Completed [Architecting on AWS](#) course

The supply of this course by Lumify Work is governed by the booking terms and conditions. Please read the terms and conditions carefully before enrolling in this course, as enrolment in the course is conditional on acceptance of these terms and conditions.

<https://www.lumifywork.com/en-ph/courses/security-engineering-on-aws/>