Training: AWS
Security Engineering on AWS with AWS Jam

TRAINING GOALS:

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.

The final day is an AWS Jam, a gamified event, with teams competing to score points by completing a series of challenges according to established best practices based on concepts covered in the course. You get to experience a wide range of AWS services in a series of real-world scenarios that represent common operational and troubleshooting tasks. The end result is developing, enhancing, and validating your skillsets in the AWS Cloud through real-world problem solving, exploring new services, features, and understanding how they interoperate.

Activities

This course includes presentations, hands-on labs, demonstrations, group exercises, and team-based gamified challenge.

Course objectives

In this course, you will:

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

Intended audience

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

This course is intended for:

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

CONSPECT:

- Day 1
  - Module 1: Security Overview and Review
    - Explain Security in the AWS Cloud.
    - Explain AWS Shared Responsibility Model.
    - Summarize 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 analyze 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 Organizations 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.
    - 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
- Day 2
  - Module 4: Secrets Management on AWS
    - Describe and list the features of AWS KMS, CloudHSM, AWS Certificate Manager (ACM), and AWS Secrets Manager.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- 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
  - 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 centralized deployment for AWS Firewall Manager can enhance security.
  - Hands-on lab: Lab 5: Using AWS WAF to Mitigate Malicious Traffic

- Day 3
  - 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.
    - Detect threats using AWS services.
    - Analyze and respond to security findings.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

        - Hands-on lab: Lab 7: Incident Response
    - Day 4
        - AWS Jam
            - Participate in team-based challenges in a real AWS environment
            - Compete with your colleagues in a gamified, hands-on learning experience
            - Apply your learning from the course on various AWS services

REQUIREMENTS:

We recommend that attendees of this course have:

- Completed the following courses:
    - AWS Security Essentials (Classroom training) or
    - AWS Security Fundamentals (Second Edition) (digital) and
    - Architecting on AWS (Classroom Training)
- Working knowledge of IT security practices and infrastructure concepts.
- Familiarity with the AWS Cloud.

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by AWS (course completion).

This course also helps you prepare for the AWS Certified Security - Specialty SCS-C01exam and this way gain the AWS Certified Security - Specialty title – specialty level. AWS certification exams are offered at Pearson Vue test centers worldwide https://home.pearsonvue.com/Clients/AWS.aspx

TRAINER:

AWS Authorized Instructor (AAI)

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007