kod szkolenia: AWS-SEC / PL DL 3d

Security Engineering on AWS

Sztuczna inteligencja w chmurze – wyzwania i innowacje według AWS

Zobacz film: https://youtu.be/2PddkjDfIQ4

Odbiorcy szkolenia

This course is intended for security engineers, security architects, and information security professionals.

Korzyści

In this course, you will:

- Identify security benefits and responsibilities of using the AWS Cloud
- Build secure application infrastructures
- Protect applications and data from common security threats
- Perform and automate security checks
- Configure authentication and permissions for applications and resources
- Monitor AWS resources and respond to incidents
- Capture and process logs
- Create and configure automated and repeatable deployments with tools such as AMIs and AWS CloudFormation

Program szkolenia

Module 1: Security on AWS

- Security in the AWS cloud

- AWS Shared Responsibility Model
- Incident response overview
- DevOps with Security Engineering

Module 2: Identifying Entry Points on AWS

- Identify the different ways to access the AWS platform
- Understanding IAM policies
- IAM Permissions Boundary
- IAM Access Analyzer
- Multi-factor authentication
- AWS CloudTrail
- Lab 01: Cross-account access

Module 3: Security Considerations: Web Application Environments

- Threats in a three-tier architecture
- Common threats: user access
- Common threats: data access
- AWS Trusted Advisor

Module 4: Application Security

- Amazon Machine Images
- Amazon Inspector
- AWS Systems Manager
- Lab 02: Using AWS Systems Manager and Amazon Inspector

Module 5: Data Security

- Data protection strategies
- Encryption on AWS
- Protecting data at rest with Amazon S3, Amazon RDS, Amazon DynamoDB
- Protecting archived data with Amazon S3 Glacier
- Amazon S3 Access Analyzer
- Amazon S3 Access Points

Module 6: Securing Network Communications

- Amazon VPC security considerations
- Amazon VPC Traffic Mirroring
- Responding to compromised instances
- Elastic Load Balancing
- AWS Certificate Manager

Module 7: Monitoring and Collecting Logs on AWS

- Amazon CloudWatch and CloudWatch Logs
- AWS Config
- Amazon Macie
- Amazon VPC Flow Logs
- Amazon S3 Server Access Logs
- ELB Access Logs

- Lab 03: Monitor and Respond with AWS Config

Module 8: Processing Logs on AWS

- Amazon Kinesis
- Amazon Athena
- ab 04: Web Server Log Analysis

Module 9: Security Considerations: Hybrid Environments

- AWS Site-to-Site and Client VPN connections
- AWS Direct Connect
- AWS Transit Gateway

Module 10: Out-Of-Region Protection

- Amazon Route 53
- AWS WAF
- Amazon CloudFront
- AWS Shield
- AWS Firewall Manager
- DDoS mitigation on AWS

Oczekiwane przygotowanie uczestnika

We recommend that attendees of this course have:

- Working knowledge of IT security practices and infrastructure concepts
- Familiarity with cloud computing concepts
- Completed AWS Security Essentials and Architecting on AWS instructor-led course

Szkolenie obejmuje

- 3 dni pracy z trenerem
- Nadzór trenera
- Kontakt ze społecznością
- Podręcznik w wersji elektronicznej
- Środowisko laboratoryjne

Metoda szkolenia

- wykład
- warsztaty

Czas trwania

3 dni / 21 godzin

Język

- Szkolenie : polski
- Materiały: angielski