kod szkolenia: AWS-SEC-BP / PL AA 1d

AWS Security Best Practices

Currently, the average cost of a security breach can be upwards of $4 million. AWS Security Best Practices provides an overview of some of the industry best practices for using AWS security and control types. This course helps you understand your responsibilities while providing valuable guidelines for how to keep your workload safe and secure. You will learn how to secure your network infrastructure using sound design options. You will also learn how you can harden your compute resources and manage them securely. Finally, by understanding AWS monitoring and alerting, you can detect and alert on suspicious events to help you quickly begin the response process in the event of a potential compromise.

Przeznaczenie szkolenia

This course is intended for:

- Solutions architects, cloud engineers, including security engineers, delivery and implementation engineers, professional services, and Cloud Center of Excellence (CCOE

Korzyści wynikające z ukończenia szkolenia

In this course, you will learn to:

- Design and implement a secure network infrastructure
- Design and implement compute security
- Design and implement a logging solution

Oczekiwane przygotowanie słuchaczy

Before attending this course, participants should have completed the following:

- AWS Security Fundamentals
- AWS Security Essentials

Język szkolenia

- Szkolenie: polski
- Materiały: angielski

Czas trwania

1 dni / 7 godzin

Agenda szkolenia

Module 1: AWS Security Overview

- Shared responsibility model
- Customer challenges
- Frameworks and standards
- Establishing best practices
- Compliance in AWS

Module 2: Securing the Network

- Flexible and secure
- Security inside the Amazon Virtual Private Cloud (Amazon VPC)
- Security services
- Third-party security solutions

Module 3: Amazon EC2 Security

- Compute hardening
- Amazon Elastic Block Store (EBS) encryption
- Secure management and maintenance
- Detecting vulnerabilities
- Using AWS Marketplace

Module 4: Monitoring and Alerting

- Logging network traffic

- Logging user and Application Programming Interface (API) traffic
- Visibility with Amazon CloudWatch
- Enhancing monitoring and alerting
- Verifying your AWS environment