Security Engineers, watch your traffic!

AWS Classroom Training

Course description

This course allows security engineers to explore and implement best practices for logging and monitoring to help detect threats in their AWS environments. This includes using custom fields in Flow Logs, Traffic Mirroring for deep packet inspection, and Amazon CloudWatch Alarms. You will learn important solutions for detecting traffic anomalies using various AWS services and features. The hands-on exercises will challenge you to implement custom, targeted monitoring and analyze traffic to find anomalies and potential security threats.

- Course level: Intermediate
- Duration: 4 hours

Activities

This course includes presentations, demonstrations, and labs.

Course objectives

In this course, you will learn to:

- Configure logging and monitoring using AWS services
- Analyze logs, traffic, and alarms to detect anomalies or malicious activities
- Review AWS services and features available to implement security monitoring and analysis.

Intended audience

This course is intended for:

- Security Engineers
- Cloud Developers
- Solutions Architects

Prerequisites

We recommend that attendees of this course have:

- Familiarity with the basics of AWS Cloud architecture and security controls.
- Basic knowledge of logging and traffic monitoring and AWS services such as AWS CloudTrail, Amazon CloudWatch and VPC Flow Logs.

Security Engineers, watch your traffic!

AWS Classroom Training

Course outline

Introduction

- Introduction to the course
- Access to resources (Hands-on lab interface, instructions)

Module 1: Understanding the threat

- Indicators of compromise in network traffic
- Indicators of compromise in compute resources
- Benefits of logging and monitoring in the cloud

Module 2: Logging network, user and API activity

- VPC Flow log best practices
- Anatomy of a flow log: custom fields for targeting suspicious traffic
- Hands-on Lab: Custom fields in Flow Logs for anomaly monitoring
- AWS CloudTrail Best practices
- Centralizing logging solution review

Module 3: Visibility and Alarms

- Amazon CloudWatch Alarms best practices
- Using composite alarms to reduce alert fatigue
- Using Amazon CloudWatch anomaly detection
- CloudWatch Logs versus Kinesis Firehose
- Hands-on Lab: Security monitoring with Amazon CloudWatch

Module 4: Mirroring Traffic for fine grained analysis

- Compare and contrast VPC Flow Logs and Traffic Mirroring
- Examine how traffic mirroring is used for deep packet inspection
- Hands-on Lab: Implement traffic mirroring for deep packet inspection

Module 5: Wrap Up

- Recap