How to Build a Threat Detection Strategy in AWS

Modality: Self-Paced Learning

Duration: 1 Hour

SATV Value:

CLC:

NATU:

SUBSCRIPTION: Learn, Master

About this course:

In this webinar Joseph Holbrook, an AWS Subject Matter Expert(SME) will provide insight into "How to Build a Threat Detection Strategy in AWS" that every AWS Cloud administrator should know. Having a well implemented Threat Detection Strategy will enable your enterprise to prevent common exploits but also secure your AWS resources so that your minimizing the impact of any potential breaches that do occur as well. In this webinar we will review several common Intrusion Detection Systems, Advanced Threat Detection Systems and other security tools that enable a proactive response to threats. Also, covered will be Amazon GuardDuty, which is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads. We will review how it can immediately provide value by consuming multiple metadata streams at enterprise scale from numerous sources such as AWS CloudTrail, VPC Flow Logs, and DNS logs.

As an added bonus—We will discuss how AWS Lambda can be used to automate actions such as changing security groups, isolating instances, or rotating credentials to ease administrative burden.

Did you know?

AWS has direct and concise Cloud Adoption Framework (CAF) Security Perspective Controls that most enterprise could follow immediately to reduce their threat footprint.
That most security incidents actually occur because of credential theft (according to the 2018 Verizon Data Breach Investigations Report) not sophisticated zero-day attacks against cloud providers themselves.
In less than three months AWS has added twelve more anomaly detections of which nine are CloudTrail-based anomaly detections that identify highly suspicious activity in your accounts.
VPC Flow log entries can be scanned by GuardDuty to detect both specific and anomalous attack patterns.

Course Objective:

By the end of this Course you should be able to understand

- Shared Security Model
- Introduction to Threat Detection
- Intrusion Detection Systems, Advanced Threat Detection Systems and other security tools

that enable a proactive response to threats.
- Building a Threat Reduction Strategy
- Cloud Adoption Framework (CAF) Security Perspective Controls
- AWS GuardDuty Monitoring (Demo)
- AWS Security Specialty Certification
- Course Summary

Audience:

- Security practitioners (Security Analysts, Security Architects, Senior Security Engineers, etc.), Cloud Security Architects, and the office of the CISO.

Prerequisite:

- There are no prerequisites required for this course

Course Outline: