# How to Build a Threat Detection Strategy in AWS

**Modality: Self-Paced Learning**

**Duration: 1 Hour**

## *About this course:*

This webinar will be conducted by speaker Joseph Holbrook, who is an AWS Subject Matter Expert (SME). He will be delivering lecture on “How to Build a Threat Detection Strategy in AWS” which is important for every AWS Cloud administrator to know. Having a strong Threat Detection Strategy will serve as very much helpful for your organization as it will protect them from the common exploits in the system. Not only this, the strategy will also secure your AWS resources which will decrease any sort of impact of a potential breach, even if one occurs. This webinar will teach about various different Intrusion Detection Systems, Advanced Threat Detection Systems and several other security tools that give an active response to the oncoming threats of the system. The lecture will also cover the topic of Amazon GuardDuty. Amazon GuardDuty is a threat detection service that performs the role of constantly regulating the system for any sort of dangerous activity and unauthorized actions to protect the AWS accounts and information. In the lecture, we will also go over the aspect of how this can provide us with great value by taking in several metadata streams at organizational level from several different sources. The sources can include programs like AWS CloudTrail, VPC Flow Logs, and DNS logs.

There will be an additional bonus in this course too. The lecture will also talk over the ways in which AWS Lambda can be utilized to automate activities like, changing security groups, isolating instances, or rotating credentials to ease administrative workload.

*Did you know?*

- AWS has direct and concise Cloud Adoption Framework (CAF) Security Perspective Controls which enables the organizations to quickly decrease their threat footprint.
- Majorly, the reason for the occurring of security instances are due to credential theft (according to the 2018 Verizon Data Breach Investigations Report), and not because of compliacted zero-day attacks against cloud providers themselves.
- In the span of within three months, AWS has made upgrades of adding twelve more anomaly detections in the system. Nine of them are CloudTrail-based anomaly detections that accurately pinpoint highly suspicious activity in your accounts.
- The VPC Flow log entries can be scanned by GuardDuty service in order to detect both specific and anomalous attack patterns.

## *Learning objectives:*

The course has the following learning objectives:

- Gaining understanding of Shared Security Model
- Getting an introduction to Threat Detection
- Gaining skills regarding Intrusion Detection Systems, Advanced Threat Detection Systems

and several other security programs that provide the benefit of an active response to the oncoming threats for the system
- Knowing how to build a Threat Reduction Strategy
- Learning about Cloud Adoption Framework (CAF) Security Perspective Controls
- Understanding AWS GuardDuty Monitoring (a demo)
- Learning the objectives of AWS Security Specialty Certification
- Gaining the understanding of what the course is for fundamentally i.e. a course summary

## *Audience:*

The course has been intended for the following groups:

- Security practitioners like, security analysts, architects, senior security engineers etc.
- Cloud Security Architects
- The office of the CISO

## *Requirements:*

None.

## Course Outline: