INFOSECTRAIN

MICROSOFT SENTINEL

TRAINING COURSE

Course description

Microsoft Sentinel is a cloud-native Security Information and Event Manager (SIEM) with built-in AI to enable enterprises quickly analyze enormous amounts of data. It gathers data from all sources, including people, apps, servers, and devices running on-premises or in the cloud, and allows you to quickly analyze millions of records. It comes with built-in connections that make integrating popular security systems a breeze. With support for open standard formats like CEF and Syslog, you may collect data from any source.

The Microsoft Sentinel Training Course with InfosecTrain teaches you the basics of Microsoft Sentinel, its components, and its functionalities. It will take you through Azure Analytics, explain the difference between Traditional SIEM and Cloud-native SIEM.

Target Audience

This course is intended for candidates interested in beginning their career in Azure Security.

Prerequisites

- Participants must have a basic grasp of Azure Cloud and services
- Familiarity with security operations in an organization

Azure Sentinel Course Objectives

- Recognize Microsoft Sentinel's many components and features
- Determine which scenarios Microsoft Sentinel might be a good fit for.

Note

- This course is a beginner to intermediate level. This course is suitable for candidates who want to understand what is Microsoft Sentinel? and how it works?
- This course is also ideal for candidates who want to start learning about SIEM solutions.
- This course will be having hands-on labs as well. For the demonstration purpose, we will be using all the generic examples. For LAB we will be using free tier and trial license products, so, demonstrations will be limited to those scenarios.

INFOSECTRAIN

Why Azure Sentinel with InfosecTrain?

InfosecTrain is one of the finest security and technology training and consulting organizations, focusing on a range of IT security training and Information Security services. InfosecTrain offers complete training and consulting solutions to its customers globally. Whether the requirements are technical services, certification, or customized training, InfosecTrain is consistently delivering the highest quality and best success rate in the industry.

- Certified & Experienced Instructor
- Flexible Schedule
- Post Training Support
- Interactive Q & A session

Course Content

INFOSECTRAIN

Let's Go with Microsoft Sentinel

- Introduction
- What Is Microsoft Sentinel?
- Do you Know SIEM?
- Why Should we care?
- Tour de Sentinel
- Pricing related to Sentinel

KQL: Basic you Need for Sentinel and Security

- Introduction
- Most Used Operators
- Analyse Query result
- Build multi-table statements using KQL
- Work with string data using

Start Working with Sentinel- Collect

- What is LAW(Log Analytic Workspace)
- How to collect the Log?
- Start using the connector
- What is Sentinel Workbook

Start Working with Sentinel- Detect

- What are Analytic Rules?
- How to detect suspicious activity?
- Generating an incident

Start Working with Sentinel- Manage and Investigate

- What are Incidents?
- Incident Management Lifecycle
- Managing and Investigating Incidents with sentinel
- Threat Hunting with sentinel

Start Working with Sentinel- Respond

- Why Automation is needed?
- Let's talk about SOAR?
- Get to know about Logic App.
- What is Playbook?
- Implement of Automation in the Sentinel

Additional Feature

- Introduction of Watchlist.
- Introduction of UEBA.
- Introduction of Notebook.

Handle Security operation in Azure

- What are Azure Policies?
- Learn to configure Azure Policies
- Introduction to Azure Security Centre
- Work with security Centre

www.infosectrain.com | sales@infosectrain.com