INFOSECTRAIN

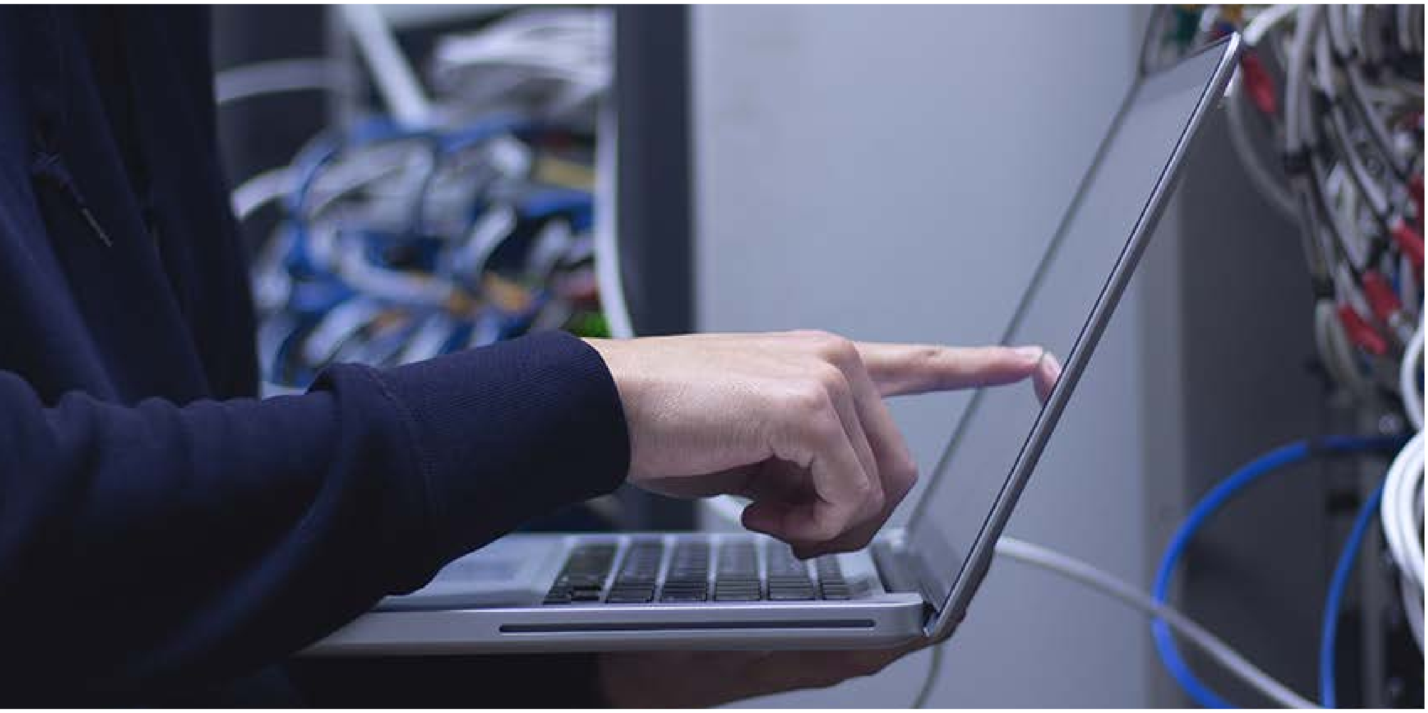
Azure Sentinel

TRAINING COURSE

Course description

Azure Sentinel is a cloud-native Security Information and Event manager (SIEM) with built-in AI to enable enterprises quickly analyse enormous amounts of data. Azure Sentinel gathers data from all sources, including people, apps, servers, and devices running on-premises or in the cloud, and allows you to quickly analyse 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 Azure Sentinel Training Course with InfosecTrain teaches you the basics of Azure Sentinel, its components and functionalities. It will take you through the Azure Analytics, explain the difference between Traditional SIEM and Cloud native SIEM. This course will also provide an in-depth knowledge of the various phases of Azure Sentinel.



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

Why Infosec Train?

Certified & Experienced Instructor

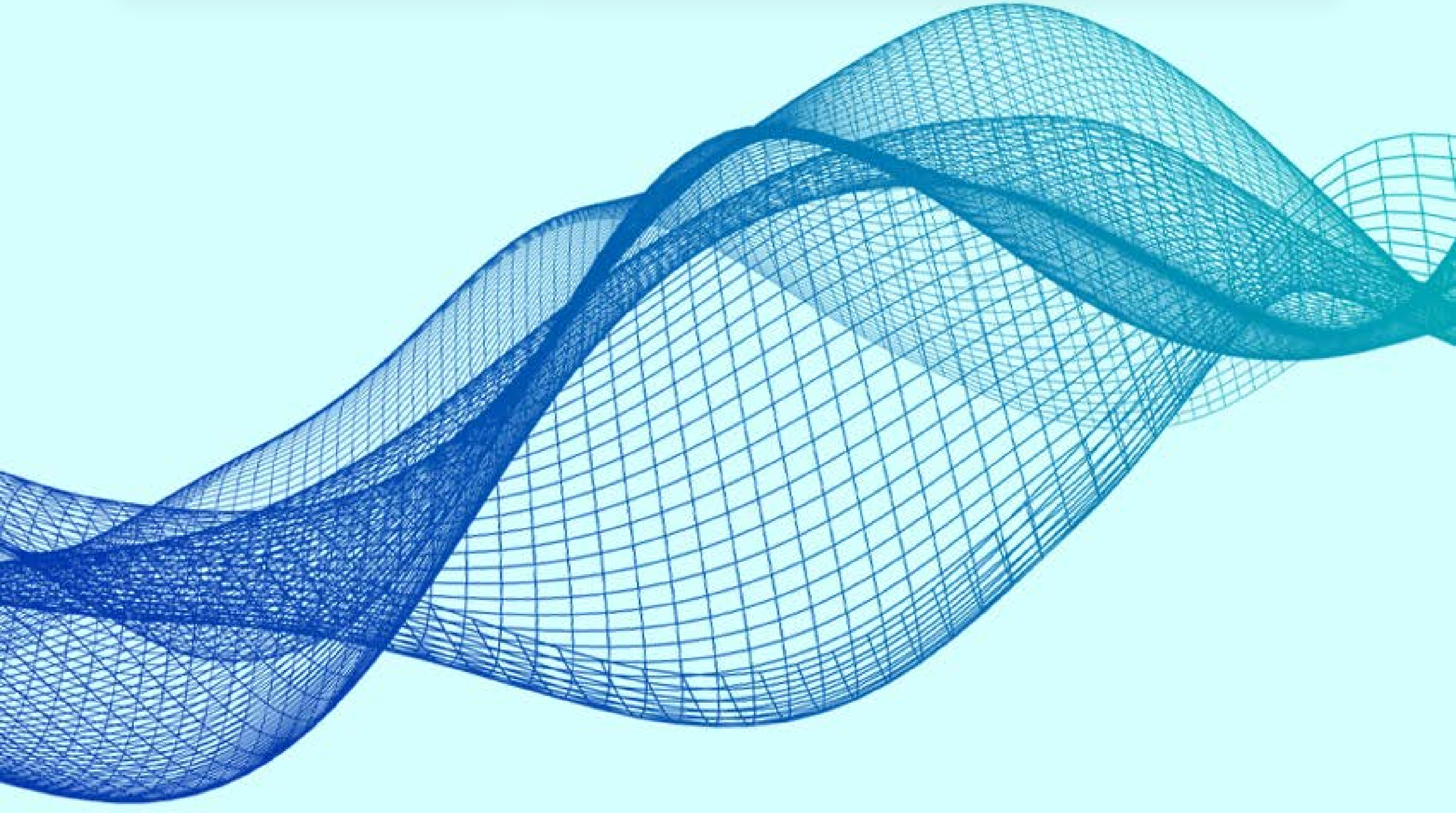
Flexible Schedule

Access to the recorded sessions

Post Training Support

Tailor Made Training

4 hrs/day in Weekend/ Weekday



Course Content

Introduction to Azure Analytics

Introduction to Azure Sentinel

Traditional SIEM vs Cloud native SIEM

Phases of Azure Sentinel

Introduction to Workbook

Phase 1: Collect

- Data Collection
- Visualization
- Querying the logs
- Introduction to Kusto Query Language (KQL)
- useful Queries in KQL
- Advanced Queries in KQL

Phase 2: Detect

- Detecting Threats using correlation Rules
- Out of the box Detection
- Custom threat detection rules
- Advanced multistage attack detection
- Intro to Use cases
- Real time use cases for Cloud
- User Behavior related use cases
- Introduction to Threat hunting
- Life cycle of Threat hunting
- Use Note books to hunt

Phase 3: Investigate

- Introduction to Threat investigation
- Investigating Incidents
- Use the investigation graph to deep dive

Phase 4: Respond

- Introduction to SOAR
- Introduction to Play Books
- Creating Security Play Books
- Creating Logic through Logic App Designer
- Threat Response Automation

INFOSECTRAIN

www.infosectrain.com | sales@infosectrain.com