multisoft
Systems

Azure Sentinel Training

COURSE CONTENT

GET IN TOUCH

Multisoft Systems
B - 125, Sector - 2, Noida

(+91) 9810-306-956

info@multisoftsystems.com

www.multisoftsystems.com

About Multisoft

Train yourself with the best and develop valuable in-demand skills with Multisoft Systems. A leading certification training provider, Multisoft collaborates with top technologies to bring world-class one-on-one and certification trainings. With the goal to empower professionals and business across the globe, we offer more than 1500 training courses, which are delivered by Multisoft's global subject matter experts. We offer tailored corporate training; project Based Training, comprehensive learning solution with lifetime e-learning access, after training support and globally recognized training certificates.

About Course

Azure Sentinel, Microsoft's premier cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution, stands at the forefront of cybersecurity defenses. Multisoft Systems' Azure Sentinel Training Course is meticulously designed to equip IT professionals with the necessary skills to implement, configure, and manage Azure Sentinel efficiently.

Module 1: Introduction to Azure Analytics

- ✓ Introduction to Azure Sentinel
- ✓ Traditional SIEM vs Cloud native SIEM
- ✓ Phases of Azure Sentinel
- ✓ Introduction to Workbook
- ✓ Data Collection
- ✓ Visualization
- ✓ Querying the logs
- ✓ Introduction to Kusto Query Language (KQL)
- ✓ useful Queries in KQL
- ✓ Advanced Queries in KQL

Module 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

Module 3: Investigate

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

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