multisoft
Systems

SC-5001: Configure SIEM security operations using Microsoft 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

The SC-5001: Configure SIEM security operations using Microsoft Sentinel training by Multisoft Systems is designed for IT professionals seeking to enhance their skills in security operations using Microsoft's cutting-edge SIEM technology, Microsoft Sentinel.

Module 1: Create and manage Microsoft Sentinel workspaces

- ✓ Plan for the Microsoft Sentinel workspace
- ✓ Create a Microsoft Sentinel workspace
- ✓ Manage workspaces across tenants using Azure Lighthouse
- ✓ Understand Microsoft Sentinel permissions and roles
- ✓ Manage Microsoft Sentinel settings
- ✓ Configure logs
- ✓ Knowledge check
- ✓ Summary and resources

Module 2: Connect Microsoft services to Microsoft Sentinel

- ✓ Plan for Microsoft services connectors
- ✓ Connect the Microsoft Office 365 connector
- ✓ Connect the Microsoft Entra connector
- ✓ Connect the Microsoft Entra ID Protection connector
- ✓ Connect the Azure Activity connector
- ✓ Knowledge check
- ✓ Summary and resources

Module 3: Connect Windows hosts to Microsoft Sentinel

- ✓ Plan for Windows hosts security events connector
- ✓ Connect using the Windows Security Events via AMA Connector
- ✓ Connect using the Security Events via Legacy Agent Connector
- ✓ Collect Sysmon event logs
- ✓ Knowledge check
- ✓ Summary and resources

Module 4: Threat detection with Microsoft Sentinel analytics

- ✓ Exercise Detect threats with Microsoft Sentinel analytics
- ✓ What is Microsoft Sentinel Analytics?
- ✓ Types of analytics rules
- ✓ Create an analytics rule from templates
- ✓ Create an analytics rule from wizard
- ✓ Manage analytics rules
- ✓ Exercise Detect threats with Microsoft Sentinel analytics
- ✓ Summary

Module 5: Automation in Microsoft Sentinel

- ✓ Understand automation options
- ✓ Create automation rules
- ✓ Knowledge check
- ✓ Summary and resources

Module 6: Configure SIEM security operations using Microsoft Sentinel

- ✓ Exercise Configure SIEM operations using Microsoft Sentinel
- ✓ Exercise Install Microsoft Sentinel Content Hub solutions and data connectors
- ✓ Exercise Configure a data connector Data Collection Rule
- ✓ Exercise Perform a simulated attack to validate the Analytic and Automation rules
- ✓ Summary