Configure SIEM security operations using Microsoft Sentinel

content

Module 1: Create and Manage Microsoft Sentinel Workspaces

- Describe the Microsoft Sentinel workspace architecture.
- Install a Microsoft Sentinel workspace.
- Manage a Microsoft Sentinel workspace.

Module 2: Connect Microsoft Services to Microsoft Sentinel

- Connect Microsoft service connectors.
- Explain how connectors auto-create incidents in Microsoft Sentinel.

Module 3: Connect Windows Hosts to Microsoft Sentinel

- Connect Azure Windows Virtual Machines to Microsoft Sentinel.
- Connect non-Azure Windows hosts to Microsoft Sentinel.
- Configure Log Analytics agent to collect Sysmon events.

Module 4: Threat Detection with Microsoft Sentinel Analytics

- Explain the importance of Microsoft Sentinel Analytics.
- Understand different types of analytics rules.
- Create rules from templates.
- Create new analytics rules and queries using the analytics rule wizard.
- Manage rules with modifications.

Module 5: Automation in Microsoft Sentinel

- Explain automation options in Microsoft Sentinel.
- Create automation rules in Microsoft Sentinel.

Module 6: Configure SIEM Security Operations Using Microsoft Sentinel

- Create and configure a Microsoft Sentinel workspace.
- Deploy Microsoft Sentinel Content Hub solutions and data connectors.
- Configure Microsoft Sentinel Data Collection rules, NRT Analytics rule, and Automation.
- Perform a simulated attack to validate Analytics and Automation rules.