MICROSOFT OFFICIAL CURRICULUM

Configure SIEM security operations using Microsoft Sentinel

Microsoft

SC-5001

Official Microsoft Learn-aligned instructor-led program for Configure SIEM security operations using Microsoft Sentinel.

Security | Intermediate | Microsoft Sentinel

DURATION	LEVEL	FORMAT	CERTIFICATION
1 day	Intermediate	Virtual, On-site, or Hybrid	SC-5001

AUDIENCE PROFILE

Built for these roles

The Microsoft Security Operations Analyst collaborates with organizational stakeholders to secure information technology systems for the organization. Their goal is to reduce organizational risk by rapidly remediating active attacks in the environment, advise on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders. Responsibilities include threat management, monitoring, and response by using a variety of security solutions across their environment. The role primarily investigates, responds to, and hunts for threats using Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft Defender XDR, and third-party security products. Since the Security Operations Analyst consumes the operational output of these tools, they are also a critical stakeholder in the configuration and deployment of these technologies.

OVERVIEW

Executive overview

Get started with Microsoft Sentinel security operations by configuring the Microsoft Sentinel workspace, connecting Microsoft services and Windows security events to Microsoft Sentinel, configuring Microsoft Sentinel analytics rules, and responding to threats with automated responses. After completing this course, students will be able to: - Create and configure a Microsoft Sentinel workspace - Deploy a Microsoft Sentinel content hub solution - Connect Windows hosts to Microsoft Sentinel - Configure analytics rules in Microsoft Sentinel - Configure automation in Microsoft Sentinel

PROGRAM OUTCOMES

Capabilities your teams will gain

- Strengthen capability in security scenarios
- Strengthen capability in microsoft sentinel scenarios
- Strengthen capability in role-based scenarios

ENTERPRISE CUSTOMIZATION

Enterprise customization

Tailor this program to your organization's priorities: Builds current Microsoft credential readiness for Configure SIEM security operations using Microsoft Sentinel using the official Microsoft Learn outline.

Customization options

- Align labs to your production environment and platform priorities
- Add readiness reviews and instructor-led practice sessions
- Extend into project-specific architecture or delivery coaching

CURRICULUM

Curriculum roadmap

1

MODULE 1

Configure SIEM security operations using Microsoft Sentinel

Configure Security Information and Event Management (SIEM) operations using Microsoft Sentinel. (SC-5001)

- Create and manage Microsoft Sentinel workspaces
- Connect Microsoft services to Microsoft Sentinel
- Connect Windows hosts to Microsoft Sentinel
- Threat detection with Microsoft Sentinel analytics
- Automation in Microsoft Sentinel
- Configure SIEM security operations using Microsoft Sentinel

PRIVATE DELIVERY

Plan a private cohort for your team

Scope delivery format, role mix, and rollout timeline with our solutions team.

Plan Private Delivery

Book advisory call

vnodeites.com

TRAINING PROVIDER
VNode ITeS
MICROSOFT CERTIFIED TRAINER
vnodeites.com
linkedin.com/company/vnodeites

TALK TO US
info@vnodeites.com
+91 9779 91 4792
WhatsApp · +91 9779 91 4792
+91 9419 11 4792

OFFICE
DLF Cyber City, Gurugram
Haryana — India
Azure · AI · Data · Power Platform