SC-5001 Configure SIEM security operations using Microsoft Sentinel

Category: Networking & Security | **Vendor:** Microsoft Technical

Duration: 8.00 hours (1 days) **6.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format:	Instructor Led - Online
Certification:	Microsoft Applied Skills: Configure SIEM security operations using Microsoft Sentinel
Related Exam:	SC-5001

Course 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

About This Course

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

Who Should Attend

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.

Prerequisites & Entry Requirements

General Prerequisites:

- Fundamental understanding of Microsoft Azure
- Basic understanding of Microsoft Sentinel
- Experience using Kusto Query Language (KQL) in Microsoft Sentinel

Learning Outcomes

Upon successful completion of this course, participants will be able to:

Course ObjectivesCreate and manage Microsoft Sentinel workspacesConnect Microsoft services to Microsoft SentinelConnect Windows hosts to Microsoft SentinelThreat detection with Microsoft Sentinel analyticsAutomation in Microsoft SentinelConfigure SIEM security operations using Microsoft Sentinel, Course ObjectivesCreate and manage Microsoft Sentinel workspacesConnect Microsoft services to Microsoft SentinelConnect Windows hosts to Microsoft SentinelThreat detection with Microsoft Sentinel analyticsAutomation in Microsoft SentinelConfigure SIEM security operations using Microsoft Sentinel, Course ObjectivesCreate and manage Microsoft Sentinel workspacesConnect Microsoft services to Microsoft SentinelConnect Windows hosts to Microsoft SentinelThreat detection with Microsoft Sentinel analyticsAutomation in Microsoft SentinelConfigure SIEM security operations using Microsoft Sentinel, Course ObjectivesCreate and manage Microsoft Sentinel workspacesConnect Microsoft services to Microsoft SentinelConnect Windows hosts to Microsoft SentinelThreat detection with Microsoft Sentinel analyticsAutomation in Microsoft SentinelConfigure SIEM security operations using Microsoft Sentinel, Course ObjectivesCreate and manage Microsoft Sentinel workspacesConnect Microsoft services to Microsoft SentinelConnect Windows hosts to Microsoft SentinelThreat detection with Microsoft Sentinel analyticsAutomation in Microsoft SentinelConfigure SIEM security operations using Microsoft Sentinel, Course ObjectivesCreate and manage Microsoft Sentinel workspacesConnect Microsoft services to Microsoft SentinelConnect Windows hosts to Microsoft SentinelThreat detection with Microsoft Sentinel analyticsAutomation in Microsoft SentinelConfigure SIEM security operations using Microsoft Sentinel, Course ObjectivesCreate and manage Microsoft Sentinel workspacesConnect Microsoft services to Microsoft SentinelConnect Windows hosts to Microsoft SentinelThreat detection with Microsoft Sentinel analyticsAutomation in Microsoft SentinelConfigure SIEM security operations using Microsoft Sentinel, Course ObjectivesCreate and manage Microsoft Sentinel workspacesConnect Microsoft services to Microsoft SentinelConnect Windows hosts to Microsoft SentinelThreat detection with Microsoft Sentinel analyticsAutomation in Microsoft SentinelConfigure SIEM security operations using Microsoft Sentinel, Course ObjectivesCreate and manage Microsoft Sentinel workspacesConnect Microsoft services to Microsoft SentinelConnect Windows hosts to Microsoft SentinelThreat detection

with Microsoft Sentinel analyticsAutomation in Microsoft SentinelConfigure SIEM security operations using Microsoft Sentinel, Course ObjectivesCreate and manage Microsoft Sentinel workspacesConnect Microsoft services to Microsoft SentinelConnect Windows hosts to Microsoft SentinelThreat detection with Microsoft Sentinel analyticsAutomation in Microsoft SentinelConfigure SIEM security operations using Microsoft Sentinel

Detailed Course Outline

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
- Module assessment

2 - Connect Microsoft services to Microsoft Sentinel

- Plan for Microsoft services connectors
- Connect the Microsoft 365 connector
- Connect the Microsoft Entra connector
- Connect the Microsoft Entra ID Protection connector
- Connect the Azure Activity connector
- Module assessment

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
- Module assessment

4 - Threat detection 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

5 - Automation in Microsoft Sentinel

- Understand automation options
- Create automation rules
- Module assessment

6 - Configure SIEM security operations using Microsoft Sentinel

, 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

□□ Certification Path

Microsoft Applied Skills: Configure SIEM security operations using Microsoft Sentinel

Exam: SC-5001

Upcoming Schedule

Available training dates for SC-5001 Configure SIEM security operations using Microsoft Sentinel:

Start Date	End Date	Location	Delivery	Price
24 Nov 2026	24 Nov 2026	Online	Virtual	€695.00

Frequently Asked Questions

Q: What delivery options are available for SC-5001 Configure SIEM security operations using Microsoft Sentinel?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: What certification does this course prepare me for?

The SC-5001 Configure SIEM security operations using Microsoft Sentinel course helps prepare you for the Microsoft Applied Skills: Configure SIEM security operations using Microsoft Sentinel certification path.

Q: Which exam does this course prepare me for?

This course prepares you for the SC-5001 official exam. You can take this exam at any exam center across United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online wherever you are located.

Q: How many CPD hours does this course provide?

The 1-day SC-5001 Configure SIEM security operations using Microsoft Sentinel course provides up to 6.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the SC-5001 Configure SIEM security operations using Microsoft Sentinel training?

The training takes place over 1 day(s), with each day lasting approximately 8.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for SC-5001 Configure SIEM security operations using Microsoft Sentinel?

Yes, we provide corporate training, dedicated training, and closed classes for SC-5001 Configure SIEM security operations using Microsoft Sentinel. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: SC-5001: Configure SIEM Security Operations Using Microsoft Sentinel, Microsoft, vILT, SC-5001

Q: Why choose Nexus Human for SC-5001 Configure SIEM security operations using Microsoft Sentinel?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your SC-5001 Configure SIEM security operations using Microsoft Sentinel training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)