MICROSOFT TRAINING

SC-5001: Configure SIEM Security Operations Using Microsoft Sentinel

Configure SIEM security operations with Microsoft Sentinel. Prepare for SC-5001 and secure your organization's cloud environment.

DURATION
2 hours

LEVEL
Intermediate

FORMAT
Instructor-Led

- Globally Recognized Certification
- Expert-Led Hands-On Training
- Flexible Scheduling

Computer Pride | 1st Floor, ICEA Building, Kenyatta Avenue, Nairobi | www.computer-pride.co.ke

COURSE OVERVIEW

This intermediate-level course, "SC-5001: Configure SIEM Security Operations Using Microsoft Sentinel," provides a robust foundation for professionals looking to master Microsoft's cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution. In today's complex threat landscape, organizations demand robust, scalable security operations, and Microsoft Sentinel delivers just that. Participants will gain practical, hands-on experience in configuring, operating, and optimizing Sentinel to detect, investigate, and respond to cyber threats effectively.

Throughout this intensive 2-hour program, you will delve into core technologies such as Azure Log Analytics, Kusto Query Language (KQL), Azure Logic Apps, and the comprehensive capabilities of Microsoft Sentinel. The course emphasizes practical skills development, enabling you to connect data sources, create sophisticated analytics rules, manage incidents, perform proactive threat hunting, and automate responses. By mastering these critical functions, you will transform raw security data into actionable intelligence, significantly bolstering an organization's defensive posture.

Upon completion, you will be equipped to design and implement effective security operations within an Azure environment. This certification not only enhances your technical proficiency but also significantly boosts your value to employers seeking skilled cybersecurity professionals capable of leveraging advanced cloud security tools to protect critical assets and ensure compliance, paving the way for specialized roles in security operations.

Duration	2 hours
Level	Intermediate
Vendor	Microsoft
Exam Code	SC-5001

COURSE CURRICULUM

01 Module 1: Introduction to Microsoft Sentinel and Core Concepts

- Understanding SIEM and SOAR in the Cloud
- Overview of Microsoft Sentinel Architecture and Capabilities
- Key Components: Workspaces, Data Connectors, Analytics, Incidents, Workbooks, Playbooks
- Planning a Microsoft Sentinel Deployment Strategy
- Introduction to Kusto Query Language (KQL) for Security Analysts

02 Module 2: Data Ingestion and Log Management

- Connecting Data Sources to Sentinel (Azure AD, Microsoft 365, Azure Activity, Firewalls)
- Configuring Custom Log Sources and Syslog Collection
- Utilizing Data Connectors and Data Transformations
- Managing Data Retention and Optimizing Log Analytics Workspaces
- Working with Azure Monitor Logs and KQL for Data Exploration

03 Module 3: Threat Detection and Analytics Rules

- Creating and Managing Analytics Rules (Scheduled, Microsoft Security, Fusion, Machine Learning)
- Developing Custom Detection Logic using KQL
- Understanding Incident Generation and Correlation Mechanisms
- Implementing Alert Suppression Strategies

- Leveraging Built-in Rule Templates and Best Practices for Rule Creation

04 Module 4: Incident Management and Automated Response

- Investigating Incidents in Microsoft Sentinel
- Utilizing the Investigation Graph and Entity Pages for Deep Analysis
- Orchestrating Automated Responses with Playbooks (Azure Logic Apps)
- Integrating Sentinel with Ticketing Systems and External Tools
- Managing Incident Lifecycle: Assignment, Status Updates, and Closure

05 Module 5: Proactive Threat Hunting and Visualization

- Performing Proactive Threat Hunting with KQL
- Leveraging Built-in Hunting Queries and Developing Custom Ones
- Utilizing Watchlists for Contextual Threat Intelligence
- Visualizing Security Data with Azure Monitor Workbooks
- Creating Custom Dashboards and Reports for Operational Insights

CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

> **Security Operations Center (SOC) Analyst (Tier 2/3)**

> **Microsoft Sentinel Administrator/Specialist**

> **Cybersecurity Engineer specializing in Cloud Security**

> **Threat Hunter**

FREQUENTLY ASKED QUESTIONS

Q: What prior knowledge or experience is recommended to successfully complete the SC-5001: Configure SIEM Security Operations Using Microsoft Sentinel course?

To gain the most from this course, participants should have a foundational understanding of Azure services, including Azure Active Directory, and general networking concepts. Basic familiarity with cybersecurity principles, such as common attack vectors and threat mitigation strategies, is highly beneficial. While Kusto Query Language (KQL) will be introduced, prior exposure to query languages or scripting will aid in rapid comprehension. This course is designed for intermediate-level IT professionals looking to specialize in cloud security operations.

Q: How will this SC-5001 course specifically enhance my ability to perform active threat hunting and incident response within a Microsoft Azure environment?

This course is intensely focused on practical application. You will learn to construct complex KQL queries to proactively hunt for threats that bypass standard detections. Furthermore, you will master the Sentinel investigation graph to visualize attack paths, understand entity relationships, and efficiently manage incident queues. The curriculum also extensively covers building and deploying Azure Logic Apps as playbooks, empowering you to automate incident response actions, thereby significantly reducing mean time to respond (MTTR) and enhancing your organization's security posture against emerging threats.

Q: Beyond the SC-5001 course, what further Microsoft security certifications or career paths can this

training prepare me for?

Completing the SC-5001 course is an excellent step towards specializing in cloud security operations and serves as a strong foundation for various advanced roles. It aligns closely with the skills required for the Microsoft Certified: Security Operations Analyst Associate (SC-200) certification. Furthermore, the expertise gained in Sentinel is highly valuable for aspiring Cybersecurity Architects (SC-100) and Identity and Access Administrators (SC-300), as Sentinel often integrates with these domains. Professionally, it opens doors to roles such as Advanced Security Analyst, SIEM Engineer, or Cloud Security Consultant, building on your ability to deploy and manage enterprise-grade security solutions.

ABOUT COMPUTER PRIDE

East Africa's Premier IT Training Center

With over 15 years of excellence, Computer Pride delivers globally recognized certification programs from leading technology vendors. Located on Kenyatta Avenue in Nairobi's CBD, our state-of-the-art facilities and expert instructors have empowered thousands of professionals across East Africa.

15+	10,000+	50+
Years of Excellence	Professionals Trained	Vendor Certifications

READY TO ENROL?

Take the next step in your technology career.

Location
1st Flr, ICEA Building
Kenyatta Ave, Nairobi

Email
info@computer-pride.co.ke

Phone
+254 705 900 900

www.computer-pride.co.ke