MICROSOFT TRAINING

SC-200T00: Microsoft Security Operations Analyst

Become a Microsoft Security Operations Analyst (SC-200) by mastering threat detection and response using Microsoft 365 Defender and Azure Sentinel.

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

The SC-200T00: Microsoft Security Operations Analyst course equips IT professionals with the essential skills to proactively detect, prevent, and respond to cyber threats within a Microsoft ecosystem. This intensive training dives deep into leveraging Microsoft's comprehensive security suite, including Microsoft 365 Defender, Microsoft Defender for Cloud, and Microsoft Sentinel. Participants will learn to configure and manage these powerful tools, enabling them to analyze security data, identify vulnerabilities, and execute effective incident response strategies to protect organizational assets.

By completing this course, you will gain hands-on expertise in critical security operations functions. You will master threat mitigation techniques across various platforms, from endpoints and identities to email, collaboration, and cloud workloads. The professional benefits are immense, as this certification validates your ability to operate advanced security solutions, making you an invaluable asset in safeguarding digital infrastructures against evolving cyber threats. It's designed to enhance your career trajectory in a rapidly growing field, ensuring you possess the practical, in-demand skills required by modern Security Operations Centers (SOCs).

Duration	2 hours
Level	Intermediate
Vendor	Microsoft
Exam Code	SC-200

PREREQUISITES

- Understanding of cloud computing concepts
- Familiarity with Azure portal
- Basic PowerShell or CLI experience
- Understanding of virtualization concepts

COURSE CURRICULUM

01 Module 1: Mitigate Threats Using Microsoft 365 Defender

- Implementing and managing Microsoft 365 Defender components
- Detecting and investigating threats using Microsoft Defender for Endpoint
- Responding to incidents and alerts with Defender for Office 365
- Managing identities and access with Defender for Identity and Azure AD Identity Protection
- Securing cloud applications with Microsoft Defender for Cloud Apps

02 Module 2: Mitigate Threats Using Microsoft Defender for Cloud

- Onboarding and configuring Microsoft Defender for Cloud
- Managing security posture and recommendations
- Protecting Azure workloads (VMs, SQL, Storage, Containers)
- Responding to threats within Microsoft Defender for Cloud
- Integrating with other security services

03 Module 3: Mitigate Threats Using Microsoft Sentinel

- Designing and deploying Microsoft Sentinel workspaces
- Connecting data sources and ingesting security logs

- Creating and managing analytics rules for threat detection
- Investigating incidents and alerts in Microsoft Sentinel
- Automating threat response with Playbooks (Azure Logic Apps)
- Leveraging threat intelligence in Sentinel

CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

> **Security Operations Center (SOC) Analyst**

> **Incident Response Specialist (Microsoft Ecosystem)**

> **Threat Hunter utilizing Microsoft Security Solutions**

FREQUENTLY ASKED QUESTIONS

Q: What foundational knowledge should I possess before enrolling in the SC-200T00 course to maximize my learning experience?

To get the most out of the SC-200T00 course, it is highly recommended that you have a foundational understanding of Microsoft 365 services, Azure services, and basic networking concepts. Familiarity with general security best practices and an understanding of security concepts like threat vectors, attack types, and incident response methodologies will also be beneficial. Experience with PowerShell or Kusto Query Language (KQL) will be an advantage, particularly for working with Microsoft Sentinel.

Q: How does the SC-200T00 certification specifically enhance my ability to perform threat hunting and incident response in a cloud-centric environment?

The SC-200T00 certification directly addresses the nuances of cloud security operations. It trains you to use cloud-native tools like Microsoft Defender for Cloud to secure Azure workloads and Microsoft Sentinel for comprehensive SIEM/SOAR capabilities across hybrid and multi-cloud environments. You will learn to leverage advanced analytics, automation, and threat intelligence unique to Microsoft's cloud platform to proactively hunt for threats and orchestrate rapid, effective incident responses, which is critical in today's cloud-first security landscape.

Q: What practical, hands-on skills will I acquire from this course that I can immediately apply in a Security Operations Center (SOC) role?

Upon completing the SC-200T00 course, you will acquire practical skills such as configuring and monitoring security alerts across Microsoft 365 Defender components (Endpoint, Identity, Office 365, Cloud Apps), analyzing security recommendations and vulnerabilities in Microsoft Defender for Cloud, and creating custom detection rules and automated response playbooks within Microsoft Sentinel. You'll be proficient in correlating disparate security data, investigating complex incidents using built-in tools, and generating actionable security insights crucial for day-to-day SOC operations.

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