MICROSOFT TRAINING

Azure Sentinel Course

Master threat detection and incident response using Microsoft Azure Sentinel. Secure your cloud environment with advanced SIEM capabilities.

DURATION
8 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 intensive 8-hour Azure Sentinel course is designed for IT professionals seeking to master Microsoft's cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution. Participants will gain hands-on experience in deploying, configuring, and utilizing Azure Sentinel to effectively detect, investigate, and respond to cyber threats across their hybrid and cloud environments. The course delves into core technologies such as Azure Log Analytics for data collection, the powerful Kusto Query Language (KQL) for crafting advanced detection rules and performing threat hunting, and the integration of various data connectors to centralize security logs.By completing this course, you will develop a robust understanding of modern threat detection methodologies and incident response workflows within the Azure ecosystem. You'll learn to leverage Azure Sentinel's capabilities for proactive threat intelligence integration, automate security tasks, and visualize security posture through custom workbooks. This specialized knowledge not only enhances an organization's security resilience but also positions participants as invaluable assets in the rapidly evolving field of cloud cybersecurity, opening doors to specialized roles focused on securing Microsoft Azure environments.

Duration	8 hours
Level	Intermediate
Vendor	Microsoft

COURSE CURRICULUM

01 Module 1: Introduction to Azure Sentinel

- What is Azure Sentinel? Cloud-native SIEM & SOAR capabilities
- Azure Sentinel architecture and key components
- Understanding the role of Azure Log Analytics workspace
- Key concepts: Incidents, Analytics Rules, Playbooks, Workbooks
- Planning and deployment considerations for Azure Sentinel

02 Module 2: Data Ingestion and Connectors

- Connecting data sources to Azure Sentinel
- Common data connectors: Azure Activity, Azure AD, M365 Defender, Firewalls, Servers
- Custom log ingestion using Log Analytics Agent and Data Connectors
- Managing data ingestion and data retention policies
- Introduction to Kusto Query Language (KQL) for data exploration

03 Module 3: Threat Detection with KQL and Analytics Rules

- Mastering Kusto Query Language (KQL) for security analysis
- Creating and managing analytics rules for automated threat detection
- Understanding different rule types: Scheduled, Microsoft Security, Fusion
- Customizing detection logic and entity mapping
- Leveraging built-in detections and community-contributed rules

04 Module 4: Incident Management and Automation (SOAR)

- Working with incidents in Azure Sentinel
- Investigating incidents using the investigation graph
- Understanding playbooks and logic apps for automated response
- Creating and deploying security orchestration automation playbooks
- Manual and automated incident response workflows

05 Module 5: Threat Hunting and Workbooks

- Proactive threat hunting methodologies in Azure Sentinel
- Using KQL for advanced threat hunting queries
- Leveraging threat intelligence in Sentinel
- Creating custom workbooks for security visualization and reporting
- Monitoring security posture and compliance with Sentinel

06 Module 6: Advanced Concepts and Best Practices

- Integrating Azure Sentinel with other Microsoft security services (Azure Security Center, Microsoft Defender)
- Role-Based Access Control (RBAC) in Sentinel
- Performance tuning and cost management considerations
- Best practices for deploying and operating Azure Sentinel
- Future trends in cloud SIEM and security operations

CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

> **Azure Cloud Security Analyst**

> **Security Operations Center (SOC) Engineer (Azure Focus)**

> **Azure Threat Hunter & Incident Responder**

FREQUENTLY ASKED QUESTIONS

Q: What specific types of advanced cyber threats will I be able to detect and respond to after completing this Azure Sentinel course?

Upon completion, you will be equipped to detect a wide array of advanced threats, including sophisticated phishing campaigns, insider threats, privilege escalation attempts, data exfiltration, brute-force attacks against Azure AD, malware propagation within cloud environments, and suspicious activities indicative of advanced persistent threats (APTs). You'll learn to craft custom KQL queries and analytics rules that specifically target these threat patterns, enabling proactive identification and automated responses.

Q: Is prior experience with Microsoft Azure or Kusto Query Language (KQL) required to enroll in this course?

While not strictly mandatory, an intermediate understanding of fundamental cybersecurity concepts, general cloud computing principles (preferably Azure basics), and familiarity with command-line interfaces or scripting will be highly beneficial. This course provides an introduction to KQL specifically for security analysis, but prior exposure to query languages can accelerate your learning. If you have no prior Azure experience, we recommend reviewing basic Azure services before attending.

Q: How does this Azure Sentinel course integrate with other Microsoft security tools I might already be using, such as Microsoft 365 Defender or Azure Security Center?

This course extensively covers how Azure Sentinel acts as the central SIEM for your entire Microsoft security ecosystem. You will learn how to seamlessly ingest alerts and logs from Microsoft 365 Defender (including Defender for Endpoint, Identity, Cloud Apps, and Office 365) and Azure Security Center (now Microsoft Defender for Cloud). We'll demonstrate

how Sentinel correlates these diverse signals, provides a unified view for investigation, and orchestrates automated responses, significantly enhancing your overall security posture by bringing together insights from all your Microsoft security investments.

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