MICROSOFT TRAINING

Planning Implementing Microsoft Sentinel Siem Soar Course

Master Microsoft Sentinel to plan, implement, and manage SIEM/SOAR solutions. Effectively protect your organization from cyber threats.

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 "Planning Implementing Microsoft Sentinel SIEM SOAR Course" is meticulously designed for IT professionals aiming to master the deployment, configuration, and operationalization of Microsoft's cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution. Participants will gain comprehensive expertise in leveraging Microsoft Sentinel to centralize security data from across their digital estate, detect sophisticated threats with intelligent analytics, and automate incident response workflows to enhance an organization's overall security posture. The course dives deep into connecting various data sources, configuring advanced analytical rules, building effective playbooks for automated remediation, and managing security incidents efficiently within a modern cloud environment. Upon completion, you will be equipped with the practical skills to significantly enhance your organization's security posture. This training empowers professionals to proactively identify and respond to cyber threats, minimize detection and response times, and reduce manual security overhead through robust automation. It's an essential program for anyone looking to bridge the gap between theoretical cybersecurity knowledge and hands-on implementation of a leading cloud security platform, preparing you for critical roles in safeguarding digital assets against an evolving threat landscape.

Duration	2 hours
Level	Intermediate
Vendor	Microsoft

COURSE CURRICULUM

01 Module 1: Introduction to Microsoft Sentinel and Core Concepts

- Understanding SIEM and SOAR principles and their importance
- Overview of Microsoft Sentinel architecture, components, and capabilities
- Key components: Data Connectors, Analytics Rules, Workbooks, Playbooks, Incidents
- Azure workspace setup and prerequisites for Sentinel deployment

02 Module 2: Planning and Deployment Strategies

- Defining security monitoring scope and identifying key use cases
- Capacity planning for log ingestion, retention, and cost optimization
- Designing a scalable and resilient Microsoft Sentinel workspace
- Implementing Role-Based Access Control (RBAC) for Sentinel operations

03 Module 3: Data Ingestion and Connectors

- Connecting Azure activity logs, Azure AD logs, and Microsoft 365 Defender logs
- Onboarding Windows and Linux server logs using Log Analytics Agents and Azure Monitor Agent
- Integrating third-party data sources (e.g., firewalls, EDR solutions) via custom connectors
- Custom log ingestion with Log Analytics custom logs and data transformation

04 Module 4: Threat Detection with Analytics and Hunting

- Creating and customizing scheduled analytics rules using Kusto Query Language (KQL)
- Understanding Fusion, Microsoft security, and ML behavior analytics rules for advanced threat detection
- Developing effective threat hunting queries and strategies
- Leveraging watchlists and integrating threat intelligence feeds for enhanced detection

05 Module 5: Incident Response and SOAR Automation

- Managing security incidents in Microsoft Sentinel: triage, investigation, and enrichment
- Building and deploying Azure Logic Apps (Playbooks) for automated response actions
- Integrating Playbooks with external security tools and services for comprehensive actions
- Orchestrating automated workflows for common security scenarios like user blocking or malware isolation

06 Module 6: Visualization, Reporting, and Optimization

- Creating custom workbooks for interactive dashboards and security visualizations
- Generating security reports and compliance views for stakeholders
- Optimizing Sentinel performance, query efficiency, and cost management strategies
- Continuous improvement strategies and maintenance best practices for a healthy Sentinel deployment

CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

> **Cloud Security Engineer (Azure Specialist)**

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

> **Cybersecurity Incident Response Lead**

FREQUENTLY ASKED QUESTIONS

Q: What specific technical skills will I gain that are directly applicable to a SOC Analyst role after completing this course?

This course will equip you with the ability to build, manage, and optimize Microsoft Sentinel for real-time threat detection and response. You'll gain hands-on expertise in crafting KQL queries for advanced hunting, configuring analytics rules to identify suspicious activities, triaging security incidents efficiently, and automating response actions using Azure Logic Apps (Playbooks). These are fundamental skills for any modern SOC Analyst operating in a cloud-centric environment, allowing you to proactively defend against complex cyber threats.

Q: Is prior experience with Azure or cybersecurity concepts required to benefit from this intermediate-level course?

While this is an intermediate course, a foundational understanding of basic networking, cloud computing concepts (preferably Azure), and general cybersecurity principles (like common attack vectors or security tools) will be highly beneficial. The course focuses on implementing Microsoft Sentinel, so prior hands-on exposure to other SIEM solutions or a basic grasp of Azure services will allow you to maximize your learning and practical application of the course material.

Q: How does mastering Microsoft Sentinel through this course improve an organization's overall cybersecurity posture and incident response capabilities?

Mastering Microsoft Sentinel through this course significantly enhances an organization's cybersecurity posture by enabling centralized log management from diverse sources, intelligent threat detection through AI and machine learning capabilities, and rapid, automated incident response. You'll learn to reduce Mean-Time-To-Detect (MTTD) and Mean-Time-To-Respond (MTTR) by implementing effective analytics, proactive threat hunting strategies, and robust SOAR playbooks, thereby minimizing the impact of security breaches and ensuring a more resilient defense against evolving cyber threats.

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