MICROSOFT TRAINING

DW-301: Migrating SIEM to Microsoft Sentinel Workshop

Transform your security operations by migrating SIEM to Microsoft Sentinel. Implement advanced threat detection and response in the cloud.

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 DW-301: Migrating SIEM to Microsoft Sentinel Workshop is an essential, intermediate-level course designed for IT professionals seeking to modernize their security operations by transitioning from traditional Security Information and Event Management (SIEM) solutions to Microsoft Azure Sentinel. In today's rapidly evolving threat landscape, cloud-native SIEMs offer unparalleled scalability, intelligent threat detection, and seamless integration with the broader Azure ecosystem. This workshop provides a focused, hands-on approach to understanding the critical aspects of planning, executing, and validating such a migration, ensuring a smooth and secure transition.

Participants will delve into the core technologies and methodologies required to successfully move their security monitoring capabilities to the cloud. You'll learn how to assess existing SIEM environments, strategize data ingestion from diverse sources, translate legacy detection rules and playbooks into Sentinel's powerful analytics and automation features, and implement robust validation processes. The workshop emphasizes practical skills, enabling you to effectively leverage Microsoft Sentinel's advanced threat intelligence, machine learning, and automation capabilities to enhance an organization's security posture and incident response.

Completing this workshop will equip you with highly sought-after skills in cloud security migration and operations, making you a valuable asset in organizations embracing digital transformation. You'll be better prepared to contribute to more efficient, scalable, and cost-effective security solutions, ultimately boosting your career trajectory in the dynamic field of cybersecurity and cloud computing.

Duration	2 hours
Level	Intermediate
Vendor	Microsoft
Exam Code	DW-301

COURSE CURRICULUM

01 Module 1: Introduction to Microsoft Sentinel & Migration Foundations

- Understanding the evolution of SIEM and SOAR in the cloud era
- Overview of Microsoft Sentinel's architecture and core capabilities
- Key benefits of migrating to Microsoft Sentinel from traditional SIEMs
- Identifying crucial considerations for a successful SIEM migration project

02 Module 2: Planning Your Migration to Microsoft Sentinel

- Assessing your current SIEM environment and identifying critical data sources
- Strategies for data ingestion: Native connectors, custom logs, and Azure services
- Mapping legacy SIEM detection rules, alerts, and playbooks to Sentinel analytics
- Resource planning, cost estimation, and licensing considerations in Azure Sentinel

03 Module 3: Executing & Validating the Migration

- Hands-on deployment and initial configuration of a Microsoft Sentinel workspace
- Configuring data connectors and ensuring successful log ingestion
- Translating and implementing detection rules, queries, and threat hunting strategies
- Developing and executing testing and validation plans for migrated security content

04 Module 4: Optimizing & Managing Sentinel Post-Migration

- Leveraging Sentinel's automation with Playbooks (Logic Apps) for incident response
- Integrating threat intelligence and developing custom analytics rules
- Monitoring performance, managing costs, and optimizing queries in Sentinel
- Best practices for ongoing SIEM operations, maintenance, and continuous improvement

CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

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

> **Security Operations Center (SOC) Analyst L2/L3 (Azure Sentinel)**

> **Security Architect (Cloud Migration & Modernization)**

FREQUENTLY ASKED QUESTIONS

Q: What foundational knowledge or experience is recommended before taking the DW-301: Migrating SIEM to Microsoft Sentinel Workshop?

Participants should have a basic understanding of Security Information and Event Management (SIEM) concepts, familiarity with Azure fundamentals (e.g., Azure portal, resource groups), and some exposure to security operations or IT administration. While not strictly required, prior experience with a traditional SIEM solution would be beneficial as it provides context for the migration challenges addressed in the workshop.

Q: What specific hands-on skills will I acquire that are immediately applicable in my security role after completing this 2-hour workshop?

Upon completing this workshop, you will gain practical skills in assessing a legacy SIEM environment for migration, identifying appropriate data connectors for various log sources within Azure Sentinel, understanding the process of translating existing detection rules to Sentinel's analytics rules, and validating the successful ingestion and detection capabilities post-migration. This workshop provides a clear roadmap and initial hands-on experience crucial for SIEM modernization projects.

Q: How does this workshop specifically address common challenges faced when migrating from an on-premise or legacy SIEM to a cloud-native solution like Microsoft Sentinel?

This workshop directly addresses key migration challenges such as identifying and migrating diverse data sources, translating complex rule sets and playbooks into Sentinel's framework, managing the transition without creating security blind spots, and optimizing cloud resource consumption. It provides practical strategies for a phased migration, ensuring continuity of security monitoring, minimizing operational disruption, and maximizing the benefits of a cloud-native SIEM.

ABOUT COMPUTER PRIDE

East Africa's Premier IT Training Center

computerpride

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