

KOENIG SOLUTIONS • COURSE OUTLINE

Azure Sentinel

Learn to collect, detect, investigate and respond to threats using Microsoft Azure Sentinel, from KQL queries to automated playbooks.

3 Days

24 HOURS

29

TOPICS

3

HANDS-ON LABS

COURSE OVERVIEW

The Azure Sentinel course is designed to equip learners with comprehensive knowledge about Microsoft's cloud-native Security Information and Event Management (SIEM) solution, Microsoft Azure Sentinel. This course will take participants through the core aspects of Azure Sentinel, starting from data collection to threat detection, investigation, and response. In Phase 1: Collect, learners will delve into data ingestion, understanding Azure Analytics, and the fundamentals of Microsoft 365 Sentinel. They will compare traditional SIEMs with cloud-native solutions and learn how to visualize and query logs using the Kusto Query Language (KQL). Phase 2: Detect focuses on identifying threats through correlation rules and custom detections, highlighting real-time cloud use cases and advanced threat hunting techniques. In Phase 3: Investigate, students will learn about threat investigation methods and utilize graphical tools to analyze incidents. Lastly, Phase 4: Respond introduces Security Orchestration, Automation, and Response (SOAR) concepts, where learners will create security playbooks and automate threat responses using Logic App Designer. Overall, this course will provide learners with the skills needed to effectively use Azure Sentinel for enhancing an organization's security posture.

Who Should Attend

Azure Sentinel course by Koenig Solutions offers comprehensive training on leveraging Microsoft's cloud-native SIEM for enhanced security operations. Target audience for the Azure Sentinel course includes:

- IT Security Professionals
- Security Analysts
- Security Engineers
- Security Architects
- Incident Responders
- System Administrators managing security solutions
- Cloud Security Specialists
- Cybersecurity Consultants
- IT Professionals looking to specialize in security operations
- Network Administrators focusing on security
- Threat Intelligence Analysts
- Compliance Officers dealing with security frameworks
- SOC (Security Operations Center) staff
- DevOps and DevSecOps Professionals dealing with security automation
- CTOs and CISOs looking to understand Azure Sentinel's capabilities for organizational security
- IT Managers and Directors responsible for security strategy and implementation
- Professionals seeking to learn about modern SIEM solutions in the cloud
- Technical Auditors and Forensic Specialists interested in cloud security and incident investigations

LEARNING OBJECTIVES

- Compare traditional SIEM with cloud-native SIEM solutions
- Query and visualise logs using Kusto Query Language
- Identify threats through correlation rules and custom detections
- Analyse real-time use cases and user behaviour patterns
- Apply threat hunting techniques using notebooks
- Investigate incidents using the investigation graph
- Explain Security Orchestration, Automation and Response concepts
- Build security playbooks using Logic App Designer

COURSE SYLLABUS

29 Topics

DAY 1

TOPICS

Introduction to Azure Analytics · Introduction to Azure Sentinel · Traditional SIEM vs Cloud native SIEM · Phases of Azure Sentinel · Introduction to Workbook

Phase 1: Collect

Lab

TOPICS

Data Collection · Visualization · Querying the logs · Introduction to Kusto Query Language (KQL) · Useful Queries in KQL · Advanced Queries in KQL

Phase 2: Detect

Lab

TOPICS

- Detecting Threats using correlation Rules
- Out of the box Detection
- Custom threat detection rules
- Advanced multistage attack detection
- Intro to Use cases
- Real time use cases for Cloud
- User Behavior related use cases
- Introduction to Threat hunting
- Life cycle of Threat hunting
- Use Notebooks to hunt

Phase 3: Investigate

TOPICS

Introduction to Threat investigation · Investigating Incidents · Use the investigation graph to deep dive

Phase 4: Respond

Lab

TOPICS

Introduction to SOAR · Introduction to Play Books · Creating Security Play Books · Creating Logic through Logic App Designer · Threat Response Automation

HANDS-ON LABS

Practise What You Learn

MODULE	ACTIVITY
Phase 1: Collect	Lab
Phase 2: Detect	Lab
Phase 4: Respond	Lab

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com

✉ info@koenig-solutions.com