# Microsoft Certified: Security Operations Analyst Associate

4 – 8 January 2027
London (UK)



# Microsoft Certified: Security Operations Analyst Associate

**Ref:** 321856_300475 **Date:** 4 – 8 January 2027 **Location:** London (UK) **Fees:** 6100 GBP

## Introduction

The Microsoft Certified: Security Operations Analyst Associate course is a focused and practical training program designed for professionals who want to strengthen their capabilities in protecting modern digital environments and managing cybersecurity incidents with confidence. In today's threat landscape, organizations need specialists who can monitor security events, investigate suspicious activity, respond to incidents quickly, and support stronger operational security across systems, networks, and cloud environments.

This comprehensive 1-week course provides participants with a structured understanding of cybersecurity security operations, combining core concepts with hands-on application. It introduces the role of the Security Operations Analyst Associate, explains what is operational security in a practical context, and offers a clear operation security definition through real-world security monitoring, investigation, and response scenarios. The course also explores key tools and practices used in a modern security operations center course, with particular emphasis on Microsoft technologies such as Microsoft Sentinel and Azure Defender.

Participants will build practical knowledge in threat detection, incident investigation, security operations alerts, vulnerability management, and proactive defense. With additional focus on security operations best practices and cybersecurity operational technology, this course helps learners develop the technical and analytical skills needed to respond effectively to evolving cyber threats and prepare successfully for the certification exam.

## Course Objectives

By the end of this course, participants will be able to:



- Understand the foundations of security operations analysis and the importance of operational security in protecting organizational assets.
- Explain what is operational security and apply a practical operation security definition within daily cybersecurity activities.
- Demonstrate proficiency in configuring and using Microsoft Sentinel for effective cybersecurity security operations.
- Detect, investigate, and respond to incidents using modern monitoring and analysis techniques.
- Apply threat intelligence and proactive threat hunting methods to identify and reduce security risks before they escalate.
- Use Azure Defender to secure cloud workloads and strengthen protection for cybersecurity operational technology environments.
- Create and manage effective security operations alerts, investigate incidents thoroughly, and support structured response actions.
- Conduct security assessments, analyze vulnerabilities, and contribute to stronger operational security management.
- Develop incident response actions aligned with recognized security operations best practices.
- Build the knowledge and confidence needed to prepare for the Microsoft Certified Security Operations Analyst Associate certification exam and succeed in analyst roles across industries.

## Course Outlines

### Day 1: Security Operations Fundamentals

- Introduction to security operations analysis and its role in modern and global operations security
- Understanding the responsibilities of a Security Operations Analyst Associate
- Defining operational security and explaining its role in cybersecurity programs
- Overview of different types of security operations center environments and related cybersecurity risks
- Introduction to incident handling, escalation paths, and response processes
- Exploring the role of Microsoft Sentinel in monitoring and managing security incidents

### Day 2: Microsoft Sentinel and Threat Detection

- Configuring and using Microsoft Sentinel for cybersecurity security operations
- Techniques for log collection, correlation, and analysis
- Detecting suspicious behavior and investigating security incidents in real time
- Managing incidents, alerts, and case workflows within Microsoft Sentinel
- Improving visibility and response effectiveness across operational environments



## Day 3: Threat Intelligence and Threat Hunting

- The role of threat intelligence in strengthening security operations
- Using intelligence sources to improve visibility into emerging threats
- Applying proactive threat-hunting techniques to identify hidden risks
- Enhancing Microsoft Sentinel investigations with advanced detection methods
- Supporting early detection and faster response through informed analysis

## Day 4: Azure Defender for Cloud Security

- Introduction to Azure Defender and its security capabilities for cloud workloads
- Protecting cloud resources against evolving threats and unauthorized activity
- Techniques for monitoring Azure environments and improving resilience
- Strengthening controls for cloud-based assets and cybersecurity operational technology
- Supporting secure cloud adoption through visibility, policy, and continuous monitoring

## Day 5: Security Assessment and Incident Response

- Creating and managing security operations alerts for incident tracking and investigation
- Analyzing security data to identify patterns, weaknesses, and critical risks
- Conducting security assessments and supporting vulnerability management activities
- Developing and executing incident response plans based on security operations best practices
- Improving operational security management through assessment, review, and response planning

# Why Attend this Course: Wins & Losses!

- Gain a strong and practical understanding of security operations analysis and modern operational security principles.
- Build hands-on experience with Microsoft Sentinel and Azure Defender, two essential tools for Microsoft-based security environments.
- Learn how to detect threats, investigate incidents, and manage security operations alerts more effectively.
- Strengthen your skills in threat intelligence, threat hunting, vulnerability management, and incident response.
- Improve your readiness for work in a security operations center and for the Microsoft Certified Security Operations Analyst Associate certification exam.
- Develop knowledge that supports stronger decision-making and better alignment with security operations best practices.



## Conclusion

The Microsoft Certified: Security Operations Analyst Associate course offers a well-structured and practical pathway for professionals who want to strengthen their role in modern cybersecurity operations. It combines essential concepts, hands-on technical knowledge, and real-world security practices to help participants understand what is operational security, apply a clear operation security definition, and perform effectively in security monitoring and incident response roles.

**Throughout the course, participants develop valuable capabilities in Microsoft Sentinel, Azure Defender, threat intelligence, threat hunting, security assessments, and incident management. By integrating these topics with established security operations best practices, the course prepares participants to contribute more effectively to organizational resilience, strengthen operational security management, and advance toward successful certification and professional growth in the field of security operations.**

