MICROSOFT SECURITY OPERATIONS ANALYST CERTIFICATION

SC 200

As per International Standards

UNICHRONE

Unichrone Training **Advantages**

- 4 Day Interactive Instructor –led Online/Classroom or Group Training
- Course study materials designed by subject matter experts
- Mock Tests to prepare in a best way
- Highly qualified, expert & accredited trainers with vast experience
- Enrich with Industry best practices and case studies and present trends
- End-to-end support via phone, mail, and chat
- Microsoft Security Operations Analyst Training Course adhered with International Standards
- Convenient Weekday/Weekend Microsoft Security Operations Analyst Certification Training Course schedule

Importance of Microsoft Security Operations Analyst Certification

✓ Microsoft Security Operations Analyst Certification holders acquire knowledge of several tools, such as Azure Sentinel, Microsoft Sentinel, Microsoft Defender, and Microsoft Defender for Office 365. with a comprehensive understanding of these tools, candidates are trained to apply them more effectively in an organization. Certified Security Operations Analysts utilize their expertise to implement advanced security protocols to protect organizations from cyber threats.

The certification of Microsoft Security Operations Analyst opens up various opportunities in a professional’s career, thereby entitling him/her to earn better salaries globally. It further adds value to businesses and clients searching for operations security for their organization. As security functions are the main priority in today's IT industry, the credential offers the best approach to tackle risks and puts Security Operation Analysts ahead of competitors in the employment market.

About Unichrone

✓ We are a professional training institute with an extensive portfolio of professional certification courses. Our training programs are meant for those who want to expand their horizons by acquiring professional certifications across the spectrum. We train small- and medium-sized organizations all around the world, including in USA, Canada, Australia, UK, Ireland and Germany.

Guaranteed Quality

Handpicked Trainers

Global Presence

Online Training Option

We’ve trained professionals across global companies

PHILIPS

AXCESS
FINANCIAL PRODUCT MANAGEMENT

CLARIANT

AkerSolutions

WÜRTH

baycoat

DUPONT

DASHTI

GlobalSign

TriskeleLabs

مصرف الراجحي
Al Rajhi Bank

DHL

ARASCO أراسكو

ELIGIBILITY CRITERIA

- ✓ Candidates aspiring to be Microsoft Certified Security Operations Analysts should be familiar with attack vectors, cyber threats, incident management, and Kusto Query Language (KQL). Additionally, professionals need to have command over Microsoft 365 and Azure services.

Why attend Microsoft Security Operations Analyst Certification Training?

- ✓ Microsoft Security Operations Analyst Training offered by Unichrone is imparted through highly qualified instructors. These instructors assist candidates in acquiring the knowledge and skills required to mitigate attacks using advanced Microsoft tools. Our training program offers hands-on experience that helps professionals learn these technologies in practice. Additionally, Microsoft Security Operations Analyst Training covers SC 200 Exam content which aids in preparing for the Exam and achieving the Microsoft Security Operations Analyst Certification.

Microsoft Security Operations Analyst Certification Advantages

- CERTIFIES YOUR TALENT
- HELPS BUILDING VALUES
- GLOBAL RECOGNITION
- PERFECT EXECUTION
- BUILDS CUSTOMER LOYALTY
- MORE EMPLOYABILITY OPTIONS

Syllabus of Microsoft Security Operations Analyst Training

Lesson 01 – Mitigate threats using Microsoft 365 Defender	
1.	Introduction to Microsoft 365 threat protection
2.	Mitigate incidents using Microsoft 365 Defender
3.	Protect your identities with Azure AD Identity Protection
4.	Remediate risks with Microsoft Defender for Office 365
5.	Safeguard your environment with Microsoft Defender for Identity
6.	Secure your cloud apps and services with Microsoft Defender for Cloud Apps
7.	Respond to data loss prevention alerts using Microsoft 365
8.	Manage insider risk in Microsoft Purview

Lesson 02 – Mitigate threats using Microsoft Defender for Endpoint	
1.	Protect against threats with Microsoft Defender for Endpoint
2.	Deploy the Microsoft Defender for Endpoint environment
3.	Implement Windows security enhancements with Microsoft Defender for Endpoint
4.	Perform device investigations in Microsoft Defender for Endpoint
5.	Perform actions on a device using Microsoft Defender for Endpoint
6.	Perform evidence and entities investigations using Microsoft Defender for Endpoint
7.	Configure and manage automation using Microsoft Defender for Endpoint
8.	Configure for alerts and detections in Microsoft Defender for Endpoint
9.	Utilize Vulnerability Management in Microsoft Defender for Endpoint

Syllabus of Microsoft Security Operations Analyst Training

Lesson 03 – Mitigate threats using Microsoft Defender for Cloud	
1.	Plan for cloud workload protections using Microsoft Defender for Cloud
2.	Connect Azure assets to Microsoft Defender for Cloud
3.	Connect non-Azure resources to Microsoft Defender for Cloud
4.	Manage your cloud security posture management
5.	Explain cloud workload protections in Microsoft Defender for Cloud
6.	Remediate security alerts using Microsoft Defender for Cloud

Lesson 04 – Create queries for Microsoft Sentinel using Kusto Query Language (KQL)	
1.	Construct KQL statements for Microsoft Sentinel
2.	Analyze query results using KQL
3.	Build multi-table statements using KQL
4.	Work with data in Microsoft Sentinel using Kusto Query Language

Syllabus of Microsoft Security Operations Analyst Training

Lesson 05 – Configure your Microsoft Sentinel environment	
1.	Introduction to Microsoft Sentinel
2.	Create and manage Microsoft Sentinel workspaces
3.	Query logs in Microsoft Sentinel
4.	Use watchlists in Microsoft Sentinel
5.	Utilize threat intelligence in Microsoft Sentinel

Lesson 06 – Connect logs to Microsoft Sentinel	
1.	Connect data to Microsoft Sentinel using data connectors
2.	Connect Microsoft services to Microsoft Sentinel
3.	Connect Microsoft 365 Defender to Microsoft Sentinel
4.	Connect Windows hosts to Microsoft Sentinel
5.	Connect Common Event Format logs to Microsoft Sentinel
6.	Connect syslog data sources to Microsoft Sentinel
7.	Connect threat indicators to Microsoft Sentinel

Syllabus of Microsoft Security Operations Analyst Training

Lesson 07 – Create detections and perform investigations using Microsoft Sentinel	
1.	Threat detection with Microsoft Sentinel analytics
2.	Automation in Microsoft Sentinel
3.	Threat response with Microsoft Sentinel playbooks
4.	Security incident management in Microsoft Sentinel
5.	Identify threats with Behavioral Analytics
6.	Data normalization in Microsoft Sentinel
7.	Query, visualize, and monitor data in Microsoft Sentinel
8.	Manage content in Microsoft Sentinel

Lesson 08 – Perform threat hunting in Microsoft Sentinel	
1.	Explain threat-hunting concepts in Microsoft Sentinel
2.	Threat hunting with Microsoft Sentinel
3.	Use Search jobs in Microsoft Sentinel
4.	Hunt for threats using notebooks in Microsoft Sentinel

Format of Exam SC 200: Microsoft Security Operations Analyst

Examination Format	
Exam Name	**Exam SC 200: Microsoft Security Operations Analyst**
Exam Format	Multiple-choice and Scenario-based questions
Total Questions & Duration	40-60 Questions, 120 minutes
Passing Score	700/1000
Exam Cost	USD 165

To get you fully prepared with the knowledge and skills for the SC 200 examination, a training session at Unichrone gives immense importance to mock questions at the end of every module and problem-solving exercises within the session. Prepared by highly qualified faculty, the practice tests are a true simulation of the Microsoft Security Operations Analyst Certification Examination

Contact Us

support@unichrone.com ✉

https://unichrone.com/ 🌐