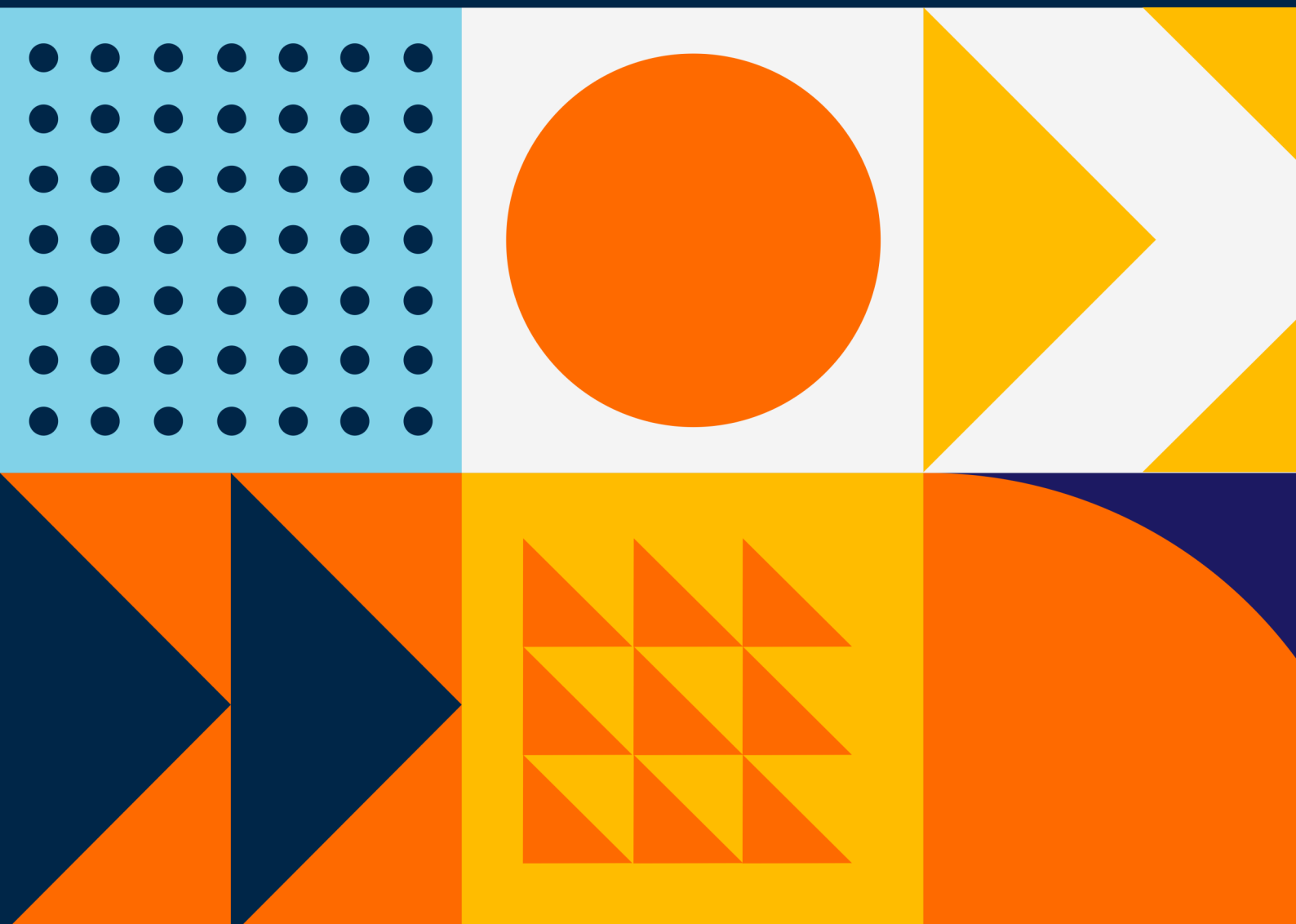
AVEREST

We do IT
to inspire.

Cloud Computing:

Microsoft Security Operations Analyst Training (SC-200)



About Us

who we **are.**

Averest is one of the leading and fast-growing companies specialising in Information Technologies, Cyber Security, Cloud Computing, DevOps, Artificial Intelligence, Agile and Scrum, and Project Management, which is based in the United Kingdom and Turkey. Averest provides high-quality tech-accredited training and business solutions to its clients on these topics and more.

Why You Should Learn With Us?

We offer accredited Programs that are available for anyone wishing to acquire skills and gain professional certification to take their career to the next level.

- **100+ Premium Programs**

  Choose the appropriate program, date and region for your occupation.

- **50+ World-Wide Accredited Certifications**

  Get certified by global certification bodies and deepen your expertise.

- **500+ Expert Advisors**

  Get together with professional trainers who are experts in their professions.

- **100.000+ Professionals Trained**

  We help many of the world's leading companies to build their tech and digital capabilities.

Our partners.

ISACA

EC-Council

DevOps INSTITUTE

Project Management Institute.

(ISC)²

IIBA®

OFFENSIVE security

CERTNEXUS

PECB

CompTIA

Microsoft

PeopleCert®
All talents, certified.

Scrum.org

aws

apm

ITIL®

To Explore More Please Visit **Our Website**

Program

Microsoft Security Operations Analyst Training (SC-200)

Overview

The role of the Microsoft Security Operations Analyst is to collaborate with organizational stakeholders to secure information technology systems for the organization and reduce corporate risk by rapidly remediating active attacks in the environment, advising on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders.

What You Will Learn?

- Explain how Microsoft Defender for Endpoint can remediate risks in your environment
- Create a Microsoft Defender for the Endpoint environment
- Configure Attack Surface Reduction rules on Windows 10 devices
- Perform actions on a device using Microsoft Defender for Endpoint
- Investigate domains and IP addresses in Microsoft Defender for Endpoint
- Investigate user accounts in Microsoft Defender for Endpoint
- Configure alert settings in Microsoft Defender for Endpoint
- Explain how the threat landscape is evolving
- Conduct advanced hunting in Microsoft 365 Defender
- Manage incidents in Microsoft 365 Defender
- Explain how Microsoft Defender for Identity can remediate risks in your environment.
- Investigate DLP alerts in Microsoft Cloud App Security

Course Key Features

- Microsoft Official Course content
- After-course instructor coaching
- Exam Prep

Program

Microsoft Security Operations Analyst Training (SC-200)

- Explain the actions you can take on an insider risk management case.
- Configure auto-provisioning in Azure Defender
- Remediate alerts in Azure Defender
- Construct KQL statements
- Filter searches based on event time, severity, domain, and other relevant data using KQL

Eligibility

Basic understanding of Microsoft 365 Fundamental understanding of Microsoft security, compliance, and identity products Intermediate understanding of Windows 10 Familiarity with Azure services, specifically Azure SQL Database and Azure Storage Familiarity with Azure virtual machines and virtual networking Basic understanding of scripting concepts.

Program

Microsoft Security Operations Analyst Training (SC-200)

Program Outline

Module 1: Mitigate threats using Microsoft Defender for Endpoint

- Protect against threats with Microsoft Defender for Endpoint
- Deploy the Microsoft Defender for Endpoint environment
- Implement Windows 10 security enhancements with Microsoft Defender for Endpoint
- Manage alerts and incidents in Microsoft Defender for Endpoint
- Perform device investigations in Microsoft Defender for Endpoint
- Perform actions on a device using Microsoft Defender for Endpoint
- Perform evidence and entities investigations using Microsoft Defender for Endpoint
- Configure and manage automation using Microsoft Defender for Endpoint
- Configure for alerts and detections in Microsoft Defender for Endpoint
- Utilize Threat and Vulnerability Management in Microsoft Defender for Endpoint
- Deploy Microsoft Defender for Endpoint
- Mitigate Attacks using Defender for Endpoint

Module 2: Mitigate threats using Microsoft 365 Defender

- Introduction to threat protection with Microsoft 365
- Mitigate incidents using Microsoft 365 Defender
- Protect your identities with Azure AD Identity Protection
- Remediate risks with Microsoft Defender for Office 365
- Safeguard your environment with Microsoft Defender for Identity
- Secure your cloud apps and services with Microsoft Cloud App Security
- Respond to data loss prevention alerts using Microsoft 365
- Manage insider risk in Microsoft 365
- Mitigate Attacks with Microsoft 365 Defender

Program

Microsoft Security Operations Analyst Training (SC-200)

Module 3: Mitigate threats using Azure Defender

- Plan for cloud workload protection using Azure Defender
- Explain cloud workload protections in Azure Defender
- Connect Azure assets to Azure Defender
- Connect non-Azure resources to Azure Defender
- Remediate security alerts using Azure Defender
- Deploy Azure Defender
- Mitigate Attacks with Azure Defender

Module 4: Create queries for Azure Sentinel using Kusto Query Language (KQL)

- Construct KQL statements for Azure Sentinel
- Analyze query results using KQL
- Build multi-table reports using KQL
- Work with data in Azure Sentinel using Kusto Query Language
- Construct Basic KQL Statements
- Analyze query results using KQL
- Build multi-table statements using KQL
- Work with string data using KQL statements

Module 5: Configure your Azure Sentinel environment

- Introduction to Azure Sentinel
- Create and manage Azure Sentinel workspaces
- Query logs in Azure Sentinel
- Use watchlists in Azure Sentinel
- Utilize threat intelligence in Azure Sentinel
- Create an Azure Sentinel Workspace
- Create a Watchlist
- Create a Threat Indicator

Module 6: Connect logs to Azure Sentinel

- Connect data to Azure Sentinel using data connectors
- Connect Microsoft services to Azure Sentinel
- Connect Microsoft 365 Defender to Azure Sentinel
- Connect Windows hosts to Azure Sentinel
- Connect Common Event Format logs to Azure Sentinel
- Connect Syslog data sources to Azure Sentinel
- Connect threat indicators to Azure Sentinel
- Connect Microsoft services to Azure Sentinel
- Connect Windows hosts to Azure Sentinel

Program

Microsoft Security Operations Analyst Training (SC-200)

- Connect Linux hosts to Azure Sentinel
- Connect Threat intelligence to Azure Sentinel

Module 7: Create detections and perform investigations using Azure Sentinel

- Threat detection with Azure Sentinel analytics
- Threat response with Azure Sentinel playbooks
- Security incident management in Azure Sentinel
- Use entity behaviour analytics in Azure Sentinel
- Query, visualize and monitor data in Azure Sentinel
- Create Analytical Rules
- Model Attacks to Define Rule Logic
- Mitigate Attacks using Azure Sentinel
- Create Workbooks in Azure Sentinel

Program

Microsoft Security Operations Analyst Training (SC-200)

Program Schedule

AVEREST

LONDON

71-75 Shelton Street Covent Garden

London, United Kingdom WC2H 9JQ

+44 20 3967 83 79

ISTANBUL

Merkez Mah. Abide-i Hürriyet Cad. Blackout A Blok Kat:1

No:64 Sisli, Istanbul, Turkey 34381

+90 534 551 20 88

info@averesttraining.com