cloudthat | Microsoft

SC-200: MICROSOFT SECURITY OPERATIONS ANALYST

Course Level:

Associate

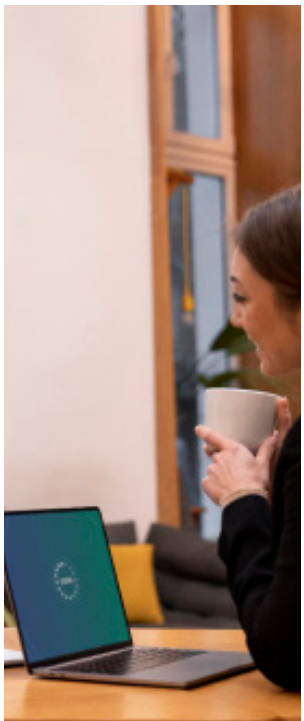
Course Duration:

4 Days

Course Overview:

This Microsoft Security Operations Analyst certification training from CloudThat teache candidates how to mitigate threats using Microsoft 365 Defender, Microsoft Defender for Cloud, and Microsoft Sentinel. Candidates taking up course SC-200 also learn to secure information technology systems, reduce organizational risk, advise best practices for threat protection, and refer violations of organizational policies to stakeholders.

The responsibilities of Azure Security Operations Analyst include threat management, response, and monitoring, using a variety of security solutions. They also use Azure Defender, Microsoft Azure Sentinel, Microsoft 365 Defender, and third-party security products to investigate, respond, and identify threats.



Prerequisites

- 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 torage
- Familiarity with Azure virtual machines and virtual networking
- Basic understanding of scripting concepts.

Objectives

- Mitigate threats using Microsoft 365 Defender
- Mitigate threats using Azure Defender
- Mitigate threats using Azure Sentinel

Learn from certified cloud security experts and become a leader in securing cloud environments with Microsoft Security Mastery Pass. Attend 5+ Microsoft Security Training at the price of 2.

Enroll Today!

Course Outline

Module 1: Mitigate Threats Using Microsoft 365 Defender

Detect, investigate, respond, and remediate threats to the productivity environment by using Microsoft Defender for Office 365

- Detect, investigate, respond, remediate Microsoft Teams, SharePoint, and OneDrive for Business threats
- Detect, investigate, respond, remediate threats to email by using Defender for Office 3
- Manage data loss prevention policy alerts
- Assess and recommend sensitivity label
- Assess and recommend insider risk policies

Detect, investigate, respond, and remediate endpoint threats by using Microsoft Defender for Endpoint

- Manage data retention, alert notification, and advanced feature
- Configure device attack surface reduction rule
- Configure and manage custom detections and alert
- Respond to incidents and alerts

Course Outline

- Manage automated investigations and remediations Assess and recommend endpoint configurations to reduce and remediate vulnerabilities by using Microsoft's Threat and Vulnerability Management solution.
- Manage Microsoft Defender for Endpoint threat indicators
- Analyze Microsoft Defender for Endpoint threat analytics

Detect, investigate, respond, and remediate identity threats

- Identify and remediate security risks related to sign-in risk policies
- Identify and remediate security risks related to conditional access events
- Identify and remediate security risks related to Azure Active Directory
- Identify and remediate security risks using Secure Score
- Identify, investigate, and remediate security risks related to privileged identities
- Configure detection alerts in Azure AD identity protection
- Identify and remediate security risks related to Active Directory Domain Services using Microsoft Defender for identity detect, investigate, respond, and remediate application threats
- Identify, investigate, and remediate security risks by using Microsoft Cloud Application Security (MCAS)
- Configure M AS to generate alerts and reports to detect threats

Course Outline

Module 2: Mitigate Risks Using Azure Defender

Manage cross-domain investigations in Microsoft 365 Defender portal

- Manage incidents across Microsoft 365 Defender products
- Manage actions pending approval across products
- Perform advanced threat hunting

Design and configure an Azure Defender implementation

- Plan and configure Azure Defender settings, including selecting target subscriptions and workspace
- Configure Azure Defender roles
- Configure data retention policies
- Assess and recommend cloud workload protection

Plan and implement the use of data connectors for ingestion of data sources in Azure Defender

- Identify data sources to be ingested for Azure Defender
- Configure utomated Onboarding for Azure resources
- Connect on-premises computers
- Connect AWS cloud resources
- Connect GCP cloud resources
- Configure data collectio

Course Outline

Manage Azure Defender alert rules

- Validate alert configuration
- Setup email notifications
- Create and manage alert suppression rules

Configure automation and remediation

- Configure automated responses in Azure Security Cente
- Design and configure playbook in Azure Defende
- Remediate incidents by using Azure Defender recommendations
- Create an automatic response using an Azure Resource Manager Template Investigate Azure Defender alerts and incidents
- Describe alert types for Azure workloads
- Manage security alerts
- Manage security incidents
- Analyze Azure Defender threat intelligence
- Respond to Azure Defender for Key Vault alerts
- Manage user data discovered during an investigation

Course Outline

Module 3: Mitigate Risks Using Azure Sentinel

Design and configure an Azure Sentinel workspace

- Plan an Azure Sentinel workspace
- Configure Azure Sentinel role
- Design Azure Sentinel data storage
- Configure Azure Sentinel service securit

Plan and Implement the use of Data Connectors for Ingestion of Data Sources in Azure Sentinel

- Identify data sources to be ingested for Azure Sentinel
- Identify the prerequisites for a data connector
- Configure and use Azure Sentinel data connector
- Configure data connectors by using Azure olicy
- Design and configure yslog and CEF event collections
- Design and Configure Windows Events collection
- Configure custom threat intelligence connector
- Create custom logs in Azure Log Analytics to store custom data

Course Outline

Manage Azure Sentinel analytics rules

- Design and configure analytics rules
- Create custom analytics rules to detect threats
- Activate Microsoft security analytical rules
- Configure connector provided scheduled querie
- Configure custom scheduled queries
- Define incident creation logic

Configure Security Orchestration Automation and Response (SOAR) in Azure Sentinel

- Create Azure Sentinel playbooks
- Configure rules and incidents to trigger playboo s
- Use playbooks to remediate threats
- Use playbooks to manage incidents
- Use playbooks across Microsoft Defender solutions

Manage Azure Sentinel Incidents

- Investigate incidents in Azure Sentinel
- Triage incidents in Azure Sentinel
- Respond to incidents in Azure Sentinel
- Investigate multi-workspace incidents
- Identify advanced threats with User and Entity Behavior Analytics (UEBA)

Course Outline

Use Azure Sentinel workbooks to analyze and interpret data

- Activate and customize Azure Sentinel workbook templates
- Create custom workbooks
- Configure advanced visualizations
- View and analyze Azure Sentinel data using workbooks
- Track incident metrics using the security operations efficiency workboo

Hunt for threats using the Azure Sentinel portal

- Create custom hunting queries
- Run hunting queries manually
- Monitor hunting queries by using Livestream
- Perform advanced hunting with notebooks
- Track query results with bookmarks
- Use hunting bookmarks for data investigations
- Convert a hunting query to an analytical

Who should attend this course?

The Microsoft Security Operations Analyst Associate collaborates with organizational stakeholders to secure information technology systems for the organization.

Who Should Attend

The Microsoft Security Operations Analyst Associate collaborates with organizational stakeholders to secure information technology systems for the organization.

About CloudThat

CloudThat is the first company in India to offer Cloud Training & Consulting services for mid-market & enterprise clients from across the globe. Since our inception in 2012, we have trained over 500K IT professionals from fortune 500 companies on technologies such as Microsoft Azure, Amazon Web Services, VMware, Artificial Intelligence, Machine Learning, Google Cloud, IoT, Dynamics 365, Power Platform, Power BI, HPE AI, DevOps, Big Data, Kubernetes, Terraform and more.

With expertise in all the major Cloud platforms, CloudThat is a proud Microsoft Gold Partner, AWS Authorized Training Partner, VMware Authorized Training Reseller, Google Cloud Platform Partner and HPE Learning Partner. Through sheer dedication and commitment towards customer excellence, we have been the winner of the Microsoft Asia Superstar Campaign for India – 2021 as well as recognized as the winner of Microsoft Learning Partner of the Year 2021 Finalist award. Recently, we have been recognized as the Microsoft 2022 Partner of the Year Finalist - Learning Award.

Our Success Track

11+ Years of Experience	100+ Corporates served	28+ countries catered
650K+ Professionals trained	300+ Projects delivered	500+ Cloud certification

To know more about our VMware certification training, email a **sales@cloudthat.com** or call us at **+918880002200.**