Defend Against Cyberthreats with Microsofts Security Operations Platform Training

Duration: **4 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Learn how to investigate, respond to, and hunt for threats using Microsoft Azure Sentinel, Azure Defender, and Microsoft 365 Defender. In this course you will learn how to mitigate cyberthreats using these technologies. Specifically, you will configure and use Azure Sentinel as well as utilize Kusto Query Language (KQL) to perform detection, analysis, and reporting. The course was designed for people who work in a Security Operations job role and helps learners prepare for the exam SC-200: Microsoft Security Operations Analyst.

Audience profile

The Microsoft Security Operations Analyst collaborates with organizational stakeholders to secure information technology systems for the organization. Their goal is to reduce organizational 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. Responsibilities include threat management, monitoring, and response by using a variety of security solutions across their environment. The role primarily investigates, responds to, and hunts for threats using Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender, and third-party security products. Since the Security Operations Analyst consumes the operational output of these tools, they are also a critical stakeholder in the configuration and deployment of these technologies.

Accessing your courseware and registering attendance with Microsoft

To access your Official Curriculum (MOC) course materials you will need a Microsoft.com/Learn account. In Learn you will also be able to register your completion of the event and receive your achievement badge. You will be issued with a unique code during your event.

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

Important This course may require the use of Multifactor Authentication (MFA). Please read this page and download the Microsoft Authenticator app (or similar app) prior to attending the course

https://www.qa.com/resources/faqs/mfa-requirements/

Please see the below Microsoft article for further information on reasons for the MFA requirement:

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mandatory-multifactor-authentication

Target audience

The Microsoft Security Operations Analyst collaborates with organizational stakeholders to secure

BILGINC IT Academy

info@bilginc.com

bilginc.com

information technology systems for the organization. Their goal is to reduce organizational 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. Responsibilities include threat management, monitoring, and response by using a variety of security solutions across their environment. The role primarily investigates, responds to, and hunts for threats using Microsoft Sentinel, Microsoft Defender XDR, Microsoft Defender for Cloud, and third-party security products. Since the Security Operations Analyst consumes the operational output of these tools, they are also a critical stakeholder in the configuration and deployment of these technologies.

What You Will Learn

- Analyze threat data across domains and rapidly remediate threats with built-in orchestration and automation in Microsoft Defender XDR.
- Get started with Microsoft Security Copilot.
- Use Microsoft Purview's risk and compliance solutions that assist security operations analysts detect threats to organizations and identify, classify, and protect sensitive data, as well as monitor and report on compliance.
- Implement the Microsoft Defender for Endpoint platform to detect, investigate, and respond to advanced threats.
- Use Microsoft Defender for Cloud, for Azure, hybrid cloud, and on-premises workload protection and security.
- Write Kusto Query Language (KQL) statements to query log data to perform detections, analysis, and reporting in Microsoft Sentinel.
- Get started with Microsoft Sentinel by properly configuring the Microsoft Sentinel workspace.
- Connect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds to Microsoft Sentinel.
- Detect previously uncovered threats and rapidly remediate threats with built-in orchestration and automation in Microsoft Sentinel.
- Proactively hunt for security threats using the Microsoft Sentinel powerful threat hunting tools.

Training Outline

Learning path 1 - Mitigate threats using Microsoft Defender XDR

- Introduction to Microsoft Defender XDR threat protection
- Mitigate incidents using Microsoft Defender
- Remediate risks with Microsoft Defender for Office 365
- Manage Microsoft Entra Identity Protection
- Safeguard your environment with Microsoft Defender for Identity
- Secure your cloud apps and services with Microsoft Defender for Cloud Apps

Lab - Explore Microsoft Defender XDR

Learning path 2 - Mitigate threats using Microsoft Security Copilot

- Fundamentals of Generative AI
- Describe Microsoft Security Copilot
- Describe the core features of Microsoft Security Copilot

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Describe the embedded experiences of Microsoft Security Copilot

Lab - Explore use cases of Microsoft Security Copilot

Learning path 3 - Mitigate threats using Microsoft Purview

- Respond to data loss prevention alerts using Microsoft 365
- Manage insider risk in Microsoft Purview
- Search and investigate with Microsoft Purview Audit
- Investigate threats with Content search in Microsoft Purview

Lab - Explore Microsoft Purview Audit logs

Learning path 4 - Mitigate threats using Microsoft Defender for Endpoint

- Protect against threats with Microsoft Defender for Endpoint
- Deploy the Microsoft Defender for Endpoint environment
- Implement Windows security enhancements with 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 Vulnerability Management in Microsoft Defender for Endpoint

Lab - Deploy Microsoft Defender for Endpoint

Lab - Mitigate Attacks with Microsoft Defender for Endpoint

Learning path 5 - Mitigate threats using Microsoft Defender for Cloud

- Plan for cloud workload protections using Microsoft Defender for Cloud
- Connect Azure assets to Microsoft Defender for Cloud
- Connect non-Azure resources to Microsoft Defender for Cloud
- Manage your cloud security posture management
- Explain cloud workload protections in Microsoft Defender for Cloud
- Remediate security alerts using Microsoft Defender for Cloud

Lab - Enable Microsoft Defender for Cloud

Lab - Mitigate threats using Microsoft Defender for Cloud

Learning path 6 - Create queries for Microsoft Sentinel using Kusto Query Language (KQL)

- Construct KQL statements for Microsoft Sentinel
- Analyze query results using KQL
- Build multi-table statements using KQL
- Work with data in Microsoft Sentinel using Kusto Query Language

Lab - Create queries for Microsoft Sentinel using Kusto Query Language (KQL)

Learning path 7 - Configure your Microsoft Sentinel environment

- Introduction to Microsoft Sentinel

BILGINÇ IT Academy

info@bilginc.com

bilginc.com

- Create and manage Microsoft Sentinel workspaces
- Query logs in Microsoft Sentinel
- Use watchlists in Microsoft Sentinel
- Utilize threat intelligence in Microsoft Sentinel
- Integrate Microsoft Defender XDR with Microsoft Sentinel

Lab - Configure your Microsoft Sentinel environment

Learning path 8 - Connect logs to Microsoft Sentinel

- Connect data to Microsoft Sentinel using data connectors
- Connect Microsoft services to Microsoft Sentinel
- Connect Microsoft Defender XDR to Microsoft Sentinel
- Connect Windows hosts to Microsoft Sentinel
- Connect Common Event Format logs to Microsoft Sentinel
- Connect syslog data sources to Microsoft Sentinel
- Connect threat indicators to Microsoft Sentinel

Lab - Connect data to Microsoft Sentinel using data connectors

Lab - Connect Windows devices to Microsoft Sentinel using data connectors

Lab - Connect Linux hosts to Microsoft Sentinel using data connectors

Learning path 9 - Create detections and perform investigations using Microsoft Sentinel

- Threat detection with Microsoft Sentinel analytics
- Automation in Microsoft Sentinel
- Threat response with Microsoft Sentinel playbooks
- Security incident management in Microsoft Sentinel
- Identify threats with Behavioural Analytics
- Data normalization in Microsoft Sentinel
- Query, visualize, and monitor data in Microsoft Sentinel
- Manage content in Microsoft Sentinel

Lab - Modify a Microsoft Security rule

Lab - Create a Playbook

Lab - Create a Scheduled Query from a template

Lab - Explore Entity Behavior Analytics

Lab - Prepare to perform simulated attacks

Lab - Conduct attacks

Lab - Create Detections

Lab - Investigate Incidents

Lab - Create ASIM parsers

Lab - Create workbooks

BILGINÇ IT Academy

info@bilginc.com

bilginc.com

Lab - Use Repositories in Microsoft Sentinel

Learning path 10 - Perform threat hunting in Microsoft Sentinel

- Explain threat hunting concepts in Microsoft Sentinel
- Threat hunting with Microsoft Sentinel
- Use Search jobs in Microsoft Sentinel
- Hunt for threats using notebooks in Microsoft Sentinel

Lab - Perform Threat Hunting in Microsoft Sentinel

Lab - Threat Hunting using Notebooks with Microsoft Sentinel