APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Microsoft Security Operations Analyst Training

Microsoft Authorized Training · Applied Technology Academy

This course trains security professionals to investigate, respond to, and hunt for threats using Microsoft's primary security tools: Microsoft Sentinel (SIEM/SOAR), Microsoft Defender XDR, and Microsoft Defender for Cloud. You will master Kusto Query Language (KQL) for detection and reporting, and learn to reduce organizational risk by rapidly remediating active attacks and advising on improvements to threat protection practices.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Intermediate	**4 Days**	**1 year: Microsoft**	**$135,000**	**Yes**

Course Overview

- Mitigate threats across endpoints, identity, email, and cloud apps using the Microsoft Defender XDR suite.
- Configure and utilize Microsoft Sentinel (SIEM) for log ingestion, alert creation, and incident investigation.
- Perform advanced threat hunting using Kusto Query Language (KQL) and specialized Sentinel tools.
- Manage and mitigate risks related to information protection, data loss, and insider threats using Microsoft Purview.
- Understand and utilize Microsoft Security Copilot for faster threat analysis and response leveraging Generative AI.

Course Outline

- **Module 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
- **Module 2: Mitigate threats using Microsoft Security Copilot**
  - Fundamentals of Generative AI
  - Describe Microsoft Security Copilot
  - Describe the core features of Microsoft Security Copilot
  - Describe the embedded experiences of Microsoft Security Copilot
  - Explore use cases of Microsoft Security Copilot
- **Module 3: Mitigate threats using Microsoft Purview**

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

  - 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
- **Module 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
  - Configure and manage automation
  - Configure alerts and detections
  - Utilize Vulnerability Management
- **Module 5: Mitigate threats using Microsoft Defender for Cloud**
  - Plan for cloud workload protections
  - Connect Azure assets to Microsoft Defender for Cloud
  - Connect non-Azure resources
  - Manage cloud security posture
  - Explain cloud workload protections
  - Remediate security alerts
- **Module 6: Create queries for Microsoft Sentinel using KQL**
  - Construct KQL statements
  - Analyze query results
  - Build multi-table statements
  - Work with data in Microsoft Sentinel using KQL
- **Module 7: Configure your Microsoft Sentinel environment**
  - Introduction to Microsoft Sentinel
  - Create and manage Sentinel workspaces
  - Query logs
  - Use watchlists
  - Utilize threat intelligence
  - Integrate Microsoft Defender XDR with Sentinel
- **Module 8: Connect logs to Microsoft Sentinel**
  - Connect data using data connectors
  - Connect Microsoft services
  - Connect Microsoft Defender XDR

  - Connect Windows hosts
  - Connect Common Event Format logs
  - Connect syslog data sources
  - Connect threat indicators
- **Module 9: Create detections and perform investigations using Microsoft Sentinel**
  - Threat detection with analytics
  - Automation in Sentinel
  - Threat response with playbooks
  - Security incident management
  - Identify threats with Behavioral Analytics
  - Data normalization in Microsoft Sentinel
  - Query, visualize, and monitor data in Microsoft Sentinel
  - Manage content in Microsoft Sentinel
- **Module 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

Intended Audience

Security Operations Analysts, Security Engineers, and other professionals focused on threat management, monitoring, and incident response within the Microsoft security ecosystem.

Prerequisites

- Microsoft Azure
- Microsoft 365 services and workloads
- Active Directory Domain Services (AD DS)
- PowerShell and Kusto Query Language (KQL)

Follow-On Courses

- SC-300: Identity and Access Administrator
- CISSP

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.