Course duration

- 4 days

Course Benefits

- Explain how Microsoft Defender for Endpoint can remediate risks in your environment
- Create a Microsoft Defender for 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
- Explain the types of 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
- Extract data from unstructured string fields using KQL
- Manage an Azure Sentinel workspace
- Use KQL to access the watchlist in Azure Sentinel
- Manage threat indicators in Azure Sentinel
- Explain the Common Event Format and Syslog connector differences in Azure Sentinel
- Connect Azure Windows Virtual Machines to Azure Sentinel
- Configure Log Analytics agent to collect Sysmon events
- Create new analytics rules and queries using the analytics rule wizard
- Create a playbook to automate an incident response
- Use queries to hunt for threats
- Observe threats over time with livestream

Microsoft Certified Partner

Webucator is a Microsoft Certified Partner for Learning Solutions (CPLS). This class uses official Microsoft courseware and will be delivered by a Microsoft Certified Trainer (MCT).

Course Outline

1. 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 10 security enhancements with Microsoft Defender for Endpoint
    4. Manage alerts and incidents in Microsoft Defender for Endpoint
    5. Perform device investigations in Microsoft Defender for Endpoint
    6. Perform actions on a device using Microsoft Defender for Endpoint
    7. Perform evidence and entities investigations using Microsoft Defender for Endpoint
    8. Configure and manage automation using Microsoft Defender for Endpoint
    9. Configure for alerts and detections in Microsoft Defender for Endpoint
    10. Utilize Threat and Vulnerability Management in Microsoft Defender for Endpoint
    11. Lab: Mitigate threats using Microsoft Defender for Endpoint
        1. Deploy Microsoft Defender for Endpoint
        2. Mitigate Attacks using Defender for Endpoint
2. Mitigate threats using Microsoft 365 Defender
    1. Introduction to threat protection with Microsoft 365
    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 Cloud App Security
    7. Respond to data loss prevention alerts using Microsoft 365
    8. Manage insider risk in Microsoft 365
    9. Lab: Mitigate threats using Microsoft 365 Defender
        1. Explore Microsoft 365 Defender
3. Mitigate threats using Azure Defender
    1. Plan for cloud workload protections using Azure Defender
    2. Explain cloud workload protections in Azure Defender
    3. Connect Azure assets to Azure Defender
    4. Connect non-Azure resources to Azure Defender
    5. Remediate security alerts using Azure Defender
    6. Lab: Mitigate threats using Azure Defender
        1. Deploy Azure Defender
        2. Mitigate Attacks with Azure Defender
4. Create queries for Azure Sentinel using Kusto Query Language (KQL)
    1. Construct KQL statements for Azure Sentinel
    2. Analyze query results using KQL
    3. Build multi-table statements using KQL
    4. Work with data in Azure Sentinel using Kusto Query Language
    5. Lab: Create queries for Azure Sentinel using Kusto Query Language (KQL)
        1. Construct Basic KQL Statements

    2. Analyze query results using KQL
    3. Build multi-table statements in KQL
    4. Work with string data in KQL
5. Configure your Azure Sentinel environment
    1. Introduction to Azure Sentinel
    2. Create and manage Azure Sentinel workspaces
    3. Query logs in Azure Sentinel
    4. Use watchlists in Azure Sentinel
    5. Utilize threat intelligence in Azure Sentinel
    6. Lab: Configure your Azure Sentinel environment
        1. Create an Azure Sentinel Workspace
        2. Create a Watchlist
        3. Create a Threat Indicator
6. Connect logs to Azure Sentinel
    1. Connect data to Azure Sentinel using data connectors
    2. Connect Microsoft services to Azure Sentinel
    3. Connect Microsoft 365 Defender to Azure Sentinel
    4. Connect Windows hosts to Azure Sentinel
    5. Connect Common Event Format logs to Azure Sentinel
    6. Connect syslog data sources to Azure Sentinel
    7. Connect threat indicators to Azure Sentinel
    8. Lab: Connect logs to Azure Sentinel
        1. Connect data to Azure Sentinel using data connectors
        2. Connect Windows devices to Azure Sentinel using data connectors
        3. Connect Linux hosts to Azure Sentinel using data connectors
        4. Connect Threat intelligence to Azure Sentinel using data connectors
7. Create detections and perform investigations using Azure Sentinel
    1. Threat detection with Azure Sentinel analytics
    2. Threat response with Azure Sentinel playbooks
    3. Security incident management in Azure Sentinel
    4. Use entity behavior analytics in Azure Sentinel
    5. Query, visualize, and monitor data in Azure Sentinel
    6. Lab: Create detections and perform investigations using Azure Sentinel
        1. Activate a Microsoft Security rule
        2. Create a Playbook
        3. Create a Scheduled Query
        4. Understand Detection Modeling
        5. Conduct attacks
        6. Create detections
        7. Investigate incidents
        8. Create workbooks
8. Perform threat hunting in Azure Sentinel
    1. Threat hunting with Azure Sentinel
    2. Hunt for threats using notebooks in Azure Sentinel
    3. Lab: Threat hunting in Azure Sentinel
        1. Perform Threat Hunting in Azure Sentinel
        2. Threat Hunting using Notebooks with Azure Sentinel

Class Materials

Each student will receive a comprehensive set of materials, including course notes and all the class examples.

Class Prerequisites

Experience in the following *is required* for this Microsoft Security class:

- 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.