Zielbox Advanced Security Operations Center (SOC) Analyst with Microsoft Defender– ZBS-200

Zielbox

About this course

Course Description

Learn how to investigate, respond to, and hunt for threats using Microsoft Defender for Endpoint and Cloud, and other similar products under Microsoft and Azure Security. In this course you will learn how to mitigate cyberthreats using these technologies. Specifically, you will configure and use Microsoft 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 like SC-200: Microsoft Security Operations Analyst.

ZBS-200 is internal name given by Zielbox for reference as we will be brining more security courses in coming days. ZBS stands for Zielbox Security and 200 number is our starting course in the security area as equivalent to SC-200 but it has our own customized contents that may or may not cover all items of SC-200.

Level

Intermediate

Audience

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 Defender for Endpoint (MDE) and other Microsoft Security products like Microsoft Endpoint Manager (Intune), Configuration Manager and other related Microsoft Security products like XDR and Sentinel, 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.

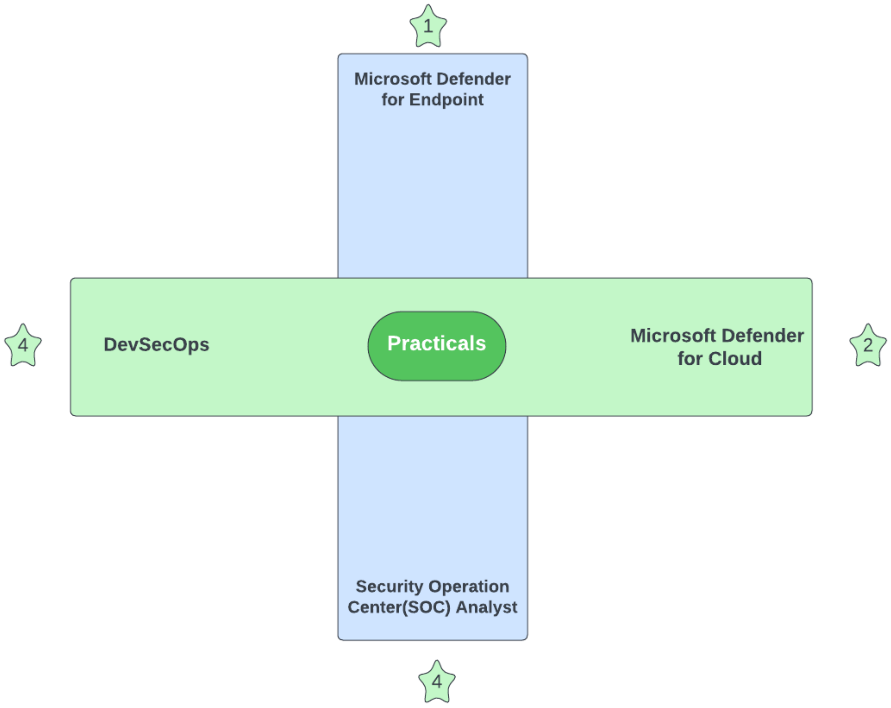
Prerequisites

- Basic understanding of Microsoft 365
- Fundamental understanding of Microsoft security, compliance, and identity products
- Intermediate understanding of Windows 10/11, Linux RHEL/Ubuntu, MacOS and similar understanding.
- Familiarity with Azure services, specifically Azure SQL Database and Azure Storage or other similar other cloud.
- Familiarity with Azure virtual machines and virtual networking or other similar cloud servies.
- Basic understanding of scripting concepts.

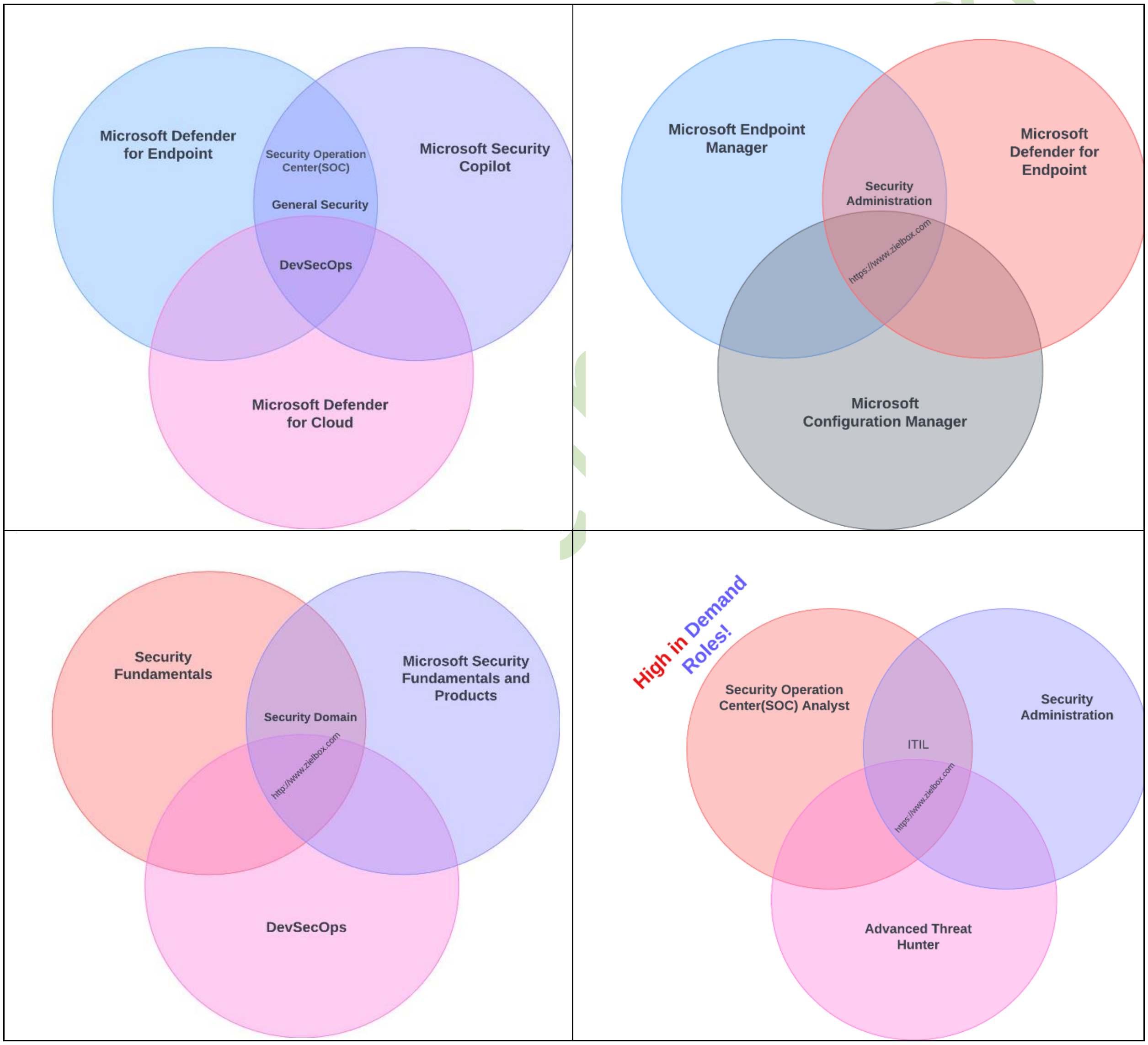
References:

Usually training institutes gives text as given above but we would like to build your high-level understanding through over custom contents so that you can quickly understand the domain and technologies.

- **On high level during course, you are going to learn below areas:**


1
Microsoft Defender for Endpoint
4
DevSecOps
Practicals
Microsoft Defender for Cloud
2
Security Operation Center(SOC) Analyst
4

- **Below is some more representation of the same thing that you are going to learn after the course:**



Microsoft Defender for Endpoint
Security Operation Center(SOC)
Microsoft Security Copilot
General Security
DevSecOps
Microsoft Defender for Cloud
Microsoft Endpoint Manager
Microsoft Defender for Endpoint
Security Administration
https://www.zielbox.com
Microsoft Configuration Manager
Security Fundamentals
Microsoft Security Fundamentals and Products
Security Domain
http://www.zielbox.com
DevSecOps
High in Demand Roles!
Security Operation Center(SOC) Analyst
Security Administration
ITIL
https://www.zielbox.com
Advanced Threat Hunter

- *Note: Products like Security Copilot are currently not available Publicly so practical will not be possible but we have references and screenshots that will help you to build the understanding.*

Expected learning

- 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 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
- 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 a Microsoft Sentinel workspace
- Use KQL to access the watchlist in Microsoft Sentinel
- Manage threat indicators in MDE Advanced Hunting features.
- Explain the Common Event Format and Syslog connector differences in Microsoft Sentinel.

- **Other Microsoft Security Product understanding:**
    - Microsoft **Endpoint Manager** integration with MDE.
    - Microsoft **Configuration Manager** integration with MDE.
    - **Azure Arc for Hybrid or Multi cloud** Management.
    - **Microsoft Defender for Cloud (MDFC)** understanding and other cloud VM onboarding.

- **Extended Learning:**
  - **DevSecOps**
    - **Container Security –**
      - Container Security,
      - Dockerfile Understanding and area of security management.
      - Code Linting,
      - Shift Left Approach,

        - Vulnerability Identification in Container Docker Images.

    - **FaaS (Function as a Service Security)**

    - **Container Orchestrator Security (Kubernetes)**
        - Basis understanding of Kubernetes so that you can build security around it.

Module 1 Mitigate threats using Microsoft 365 Defender

- Introduction to Microsoft 365 threat protection
- Mitigate incidents using Microsoft 365 Defender
- Protect your identities with Azure AD Identity Protection
- Safeguard your environment with Microsoft Defender for Identity
- Respond to data loss prevention alerts using Microsoft 365
- Knowledge check
- Lab - Mitigate threats using Microsoft 365 Defender

Module 2 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 Threat and Vulnerability Management(TVM) in Microsoft Defender for Endpoint
- Knowledge check
- Lab - Mitigate threats using Defender for Endpoint

Module 3 Mitigate threats using Microsoft Defender for Cloud

- Plan for cloud workload protections using Microsoft Defender for Cloud
- Explain cloud workload protections in 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
- Remediate security alerts using Microsoft Defender for Cloud
- Knowledge check
- Lab - Mitigate threats using Microsoft Defender for Cloud

Module 4 Create queries for Microsoft Sentinel or MDE Advanced Hunting using Kusto Query Language

- Construct KQL statements for Microsoft Sentinel or MDE Advanced Hunting
- Analyze query results using KQL
- Build multi-table statements using KQL
- Work with string data using KQL statements
- Knowledge check
- Lab - Create queries for Microsoft Sentinel using KQL

~~Module 5 Configure your Microsoft Sentinel environment~~

- ~~Introduction to Microsoft Sentinel~~
- ~~Create and manage Microsoft Sentinel workspaces~~
- ~~Query logs in Microsoft Sentinel~~
- ~~Use watchlists in Microsoft Sentinel~~
- ~~Utilize threat intelligence in Microsoft Sentinel~~
- ~~Knowledge check~~
- ~~Lab - Configure your Microsoft Sentinel environment~~
- ~~Connect Microsoft services to Microsoft Sentinel~~
- ~~Connect Microsoft 365 Defender 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~~
- ~~Knowledge check~~
- ~~Lab - Connect logs to Microsoft Sentinel~~

~~Module 6 Connect logs to Microsoft Sentinel~~

- ~~Connect data to Microsoft Sentinel using data connectors~~
- ~~Connect Microsoft services to Microsoft Sentinel~~
- ~~Connect Microsoft 365 Defender 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~~
- ~~Knowledge check~~
- ~~Lab - Connect logs to Microsoft Sentinel~~

Module 7 Create detections and perform investigations using Microsoft Defender for Endpoint Web portal

- Threat detection with Microsoft Defender Endpoint analytics
- Security incident management in Microsoft Defender Endpoint
- Security incident management in MDE
- Identify threats with Behavioral Analytics
- Query, visualize, and monitor data in MDE
- Manage content in MDE
- Knowledge check
- Lab - Create detections and perform investigations

Module 8 Perform threat hunting in Microsoft Sentinel or **MDE Advanced Hunting**

- 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
- Knowledge check
- Lab - Threat hunting in Microsoft Sentinel

Module 9 DevSecOps

- **DevSecOps**
    - **Container Security –**
        - Container Security,
        - Dockerfile Understanding and area of security management.
        - Code Linting,
        - Shift Left Approach,
        - Vulnerability Identification in Container Docker Images.

    - **FaaS (Function as a Service Security)**

    - **Container Orchestrator Security (Kubernetes)**

Module 10 – General Security Market understanding and other Security Products

- Symantec Solutions
- Splunk SIEM understanding
- Security Market big picture
- Microsoft Security and Azure Security Understanding
- Penetration testing tools
- Social Engineering Toolkit (SET)

Note: Below Certification is just a reference and our goal is to give you strong understanding of technologies around this and we will cover beyond SC-200.

SC-200 Certification Exam

The **SC-200 Microsoft Security Operations Analyst** certification exam is designed to 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 Sentinel, Microsoft Defender for Cloud, 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.

Candidates for this role should be familiar with attack vectors, cyberthreats, incident management, and Kusto Query Language (KQL). Candidates should also be familiar with Microsoft 365 and Azure services.

You may be eligible for ACE college credit if you pass this certification exam. See ACE college credit for certification exams for details.

SC-200 Study Areas	Weights
Mitigate threats using Microsoft 365 Defender	25-30%
Mitigate threats using Microsoft Defender for Cloud	20-25%
Mitigate threats using Microsoft Sentinel	50-55%

Last updated on - *12/March/2024*