Microsoft Security

SC-200 Microsoft Security Operations Analyst

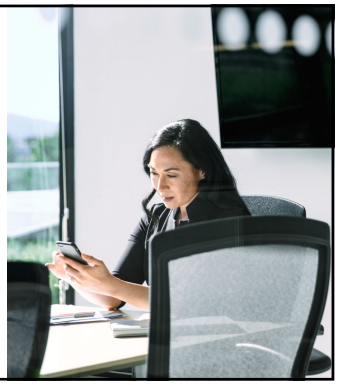
Ben McGee
11/20/2022

1

Microsoft Security

MSRP → $10/$3
50

Module 2: Mitigate threats using Microsoft Defender for Endpoint



2

Module agenda

- Protect against threats with Microsoft Defender for Endpoint
- Deploy the Microsoft Defender for Endpoint environment
- Implement Windows security enhancements
- Perform device investigations
- Perform actions on a device
- Perform evidence and entities investigations
- Configure and manage automation
- Configure for alerts and detections
- Utilize Threat and Vulnerability Management

3

Lesson 1: Protect against threats with Microsoft Defender for Endpoint

4

Lesson introduction

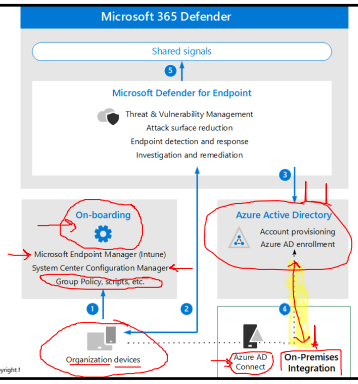
After this lesson, you will be able to:

- Define the capabilities of Microsoft Defender for Endpoint
- Describe how to hunt threats within your network.
- Explain how Microsoft Defender for Endpoint can remediate risks in your environment

5

Microsoft Defender for Endpoint explained

Microsoft Defender for Endpoint is a platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats on their endpoints.



6

Explain security operations in Microsoft Defender for Endpoint

- Defender for Endpoint detection and response capabilities provide advanced attack detections that are near real-time and actionable.
- When a threat is detected, alerts are created in the system for an analyst to investigate. Alerts with the same attack techniques or attributed to the same attacker are aggregated into an entity called an incident. Aggregating alerts in this manner makes it easy for analysts to investigate and respond to threats collectively.
- Inspired by the "assume breach" mindset, Defender for Endpoint continuously collects behavioral cyber telemetry. This includes process information, network activities, deep optics into the kernel and memory manager, user sign in activities, registry and file system changes, and others.

7

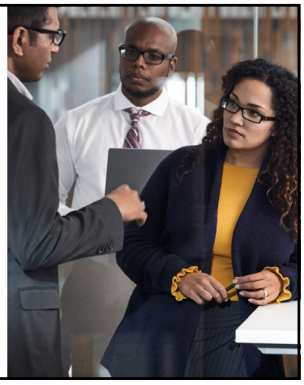
Lesson 2: Deploy the Microsoft Defender for Endpoint environment

8

Lesson introduction

After this lesson, you will be able to:

- Create a Microsoft Defender for Endpoint environment
- Onboard devices to be monitored by Microsoft Defender for Endpoint
- Configure Microsoft Defender for Endpoint environment settings



9

Create your environment

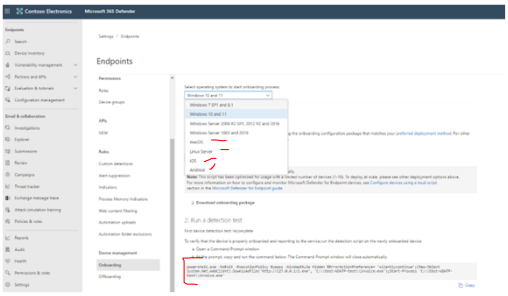
Microsoft 365 Defender portal https://security.microsoft.com

Data storage location:	Data retention:	Enable preview features:
Determine where you want to be hosted. You cannot change the location after this set up.	The default is six months.	The default is on, can be changed later.

10

Onboard devices

You'll need to go to the onboarding section of the Defender for Endpoint portal to onboard any of the supported devices. Depending on the device, you'll be guided with appropriate steps and provided management and deployment tool options suitable for the device.



11

Manage access

Defender for Endpoint RBAC is designed to support your tier- or role-based model of choice and gives you granular control over what roles can see, devices they can access, and actions they can take.

Control who can take specific actions:	Control who can see information on a specific device group or groups:
Create custom roles and control what Defender for Endpoint capabilities they can access with granularity.	Create device groups by specific criteria such as names, tags, domains, and others, then grant role access to them using a specific Azure Active Directory (Azure AD) user group.

12

Create and manage roles for role-based access control

Permission options

RBAC ← Lab

- View data: Security operations
- View data: Threat and vulnerability management (TVM)
- Active remediation actions: Security operations
- Active remediation actions: TVM - Exception handling
- Active remediation actions: TVM - Remediation handling
- Alerts investigation
- Manage portal system settings
- Manage security settings in the security center
- Live response: Basic commands
- Live response: Advanced commands

13

Configure device groups

create device groups and use them to:

- Limit access to related alerts and data to specific Azure AD user groups with assigned RBAC roles
- Configure different auto-remediation settings for different sets of devices
- Assign specific remediation levels to apply during automated investigations
- In an investigation, filter the Devices list to just specific device groups by using the Group filter.

As part of the process of creating a device group, you'll:

- Set the automated remediation level for that group.
- Specify the matching rule that determines which device group belongs to the group based on the device name, domain, tags, and OS platform.
- Select the Azure AD user group that should have access to the device group.
- Rank the device group relative to other groups after it is created.

14

Lesson 3: Implement Windows security enhancements

15

Lesson introduction

After this lesson, you will be able to:

- Explain attack surface reduction in Windows
- Enable attack surface reduction rules on Windows devices
- Configure attack surface reduction rules on Windows devices

16

Explain attack surface reduction

ASR

- Attack surface reduction rules
- Hardware-based isolation
- Application control
- Exploit protection
- Network protection
- Web protection
- Controlled folder access
- Device control

17

Enable attack surface reduction rules

Sample ASR Rules:

- Block executable content from email client and webmail
- Block all Office applications from creating child processes
- Block Office applications from creating executable content
- Block Office applications from injecting code into other processes
- Block execution of potentially obfuscated scripts
- Use advanced protection against ransomware

Rule options:

Disable = 0
Block (enable ASR rule) = 1
Audit = 2
Warn = 6

MACRO

Deployment options:

- Microsoft Endpoint
- Configuration Manager
- Group Policy
- PowerShell cmdlets
- Microsoft Intune
- Mobile Device Management (MDM)

18

Lesson 4: Perform device investigations

19

Lesson introduction

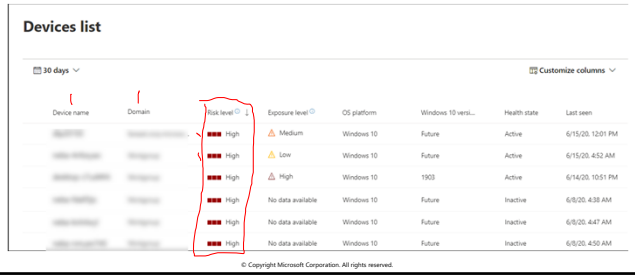
After this lesson, you will be able to:

- Use the device page in Microsoft Defender for Endpoint
- Describe device forensics information collected by Microsoft Defender for Endpoint
- Describe behavioral blocking by Microsoft Defender for Endpoint

20

Use the device inventory list

The Device inventory page shows a list of the devices in your network where alerts were generated. By default, the queue displays devices with alerts seen in the last 30 days.



21

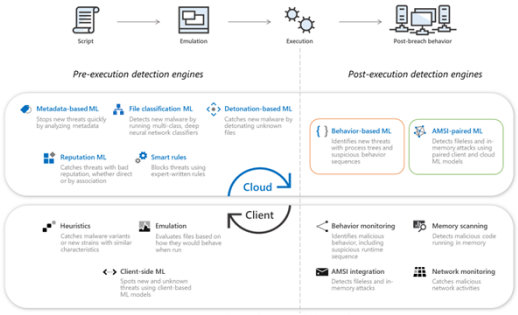
Investigate the device

When you investigate a specific device, you'll see the following:

- Device details
- Response actions
- Tabs for (overview, alerts, timeline, security recommendations, software inventory, discovered vulnerabilities, missing KBs)
- Cards for (active alerts, logged on users, security assessment)

22

Use behavioral blocking



23

Lesson 5: Perform actions on a device

24

Lesson introduction

After this lesson, you will be able to:

- Perform actions on a device using Microsoft Defender for Endpoint
- Conduct forensics data collection using Microsoft Defender for Endpoint
- Access devices remotely using Microsoft Defender for Endpoint

25

Explain device actions

When investigating a device, you can perform actions, collect data, or remotely access the machine. Defender for Endpoint provides the device control required.

Containment actions:

- Isolate Device
- Restrict app execution
- Run antivirus scan

Investigation actions:

- Initiate Automated Investigation
- Collect investigation package
- Initiate Live Response Session

26

Collect investigation package from devices

As part of the investigation or response process, you can collect an investigation package from a device that contains:

- Autoruns
- Installed programs
- Network connections
- Prefetch files
- Processes
- Scheduled tasks
- Security event log
- Services
- Windows Server Message Block (SMB) sessions
- System information
- Temp directories
- Users and groups
- WdSupportLogs

27

Initiate live response session

Live response gives security operations teams instantaneous access to a device (also referred to as a machine) using a remote shell connection.

Live response commands (examples)

Basic commands:	Advanced commands:
connections	analyze
fileinfo	getfile
persistence	run
processes	library
registry	putfile
scheduledtasks	remediate
services	

28

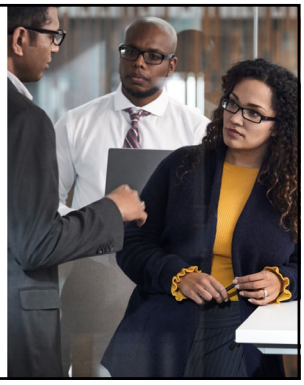
Lesson 6: Perform evidence and entities investigations

29

Lesson introduction

After this lesson, you will be able to:

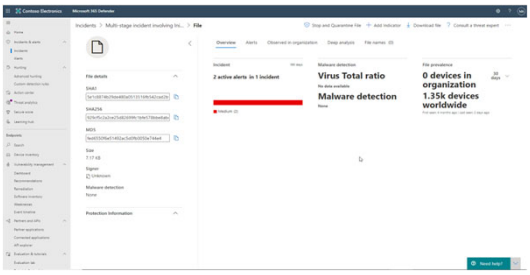
- Investigate files in Microsoft Defender for Endpoint
- Investigate domains and IP addresses in Microsoft Defender for Endpoint
- Investigate user accounts in Microsoft Defender for Endpoint



30

Investigate a file

Investigate the details of a file associated with a specific alert, behavior, or event to help determine if the file exhibits malicious activities, identify the attack motivation, and understand the potential scope of the breach.



31

Investigate a user account

Identify user accounts with the most active alerts (displayed on the dashboard as "Users at risk") and investigate cases of potentially compromised credentials, or pivot on the associated user account when investigating an alert or device to identify possible lateral movement between devices with that user account.

32

Investigate an IP address

- IP worldwide
- Reverse DNS names
- Alerts related to this IP
- IP in organization
- Prevalence

33

Investigate a domain

- URL details, Contacts, Nameservers
- Alerts related to this URL
- URL in organization
- Most recent observed devices with URL

34

Lesson 7: Configure and manage automation

35

Lesson introduction

After this lesson, you will be able to:

- Configure advanced features of Microsoft Defender for Endpoint
- Manage automation settings in Microsoft Defender for Endpoint

36

Configure advanced features

Automated Investigation

Enable EDR in block mode

The Advanced features area provides many an on/off switch for features within the product. The following are settings that are automation focused.

Automatically resolve alerts

Allow or block file

37

Manage automation upload and folder settings

File Content Analysis:
Enable the File Content Analysis capability so that certain files and email attachments can automatically be uploaded to the cloud for additional inspection in Automated investigation.

Memory Content Analysis:
Enable the Memory Content Analysis capability if you would like Microsoft Defender for Endpoint to automatically investigate memory content of processes. When enabled, memory content might be uploaded to Microsoft Defender for Endpoint during an Automated investigation.

Automation folder exclusions:
Automation folder exclusions allow you to specify folders that the Automated investigation will skip. You can control the following attributes about the folder that you'd like to be skipped:

- Folders
- Extensions of the files
- File names

38

Configure automated investigation and remediation capabilities

1. Full - remediate threats automatically
2. Semi - require approval for any remediation
3. Semi - require approval for core folders remediation
4. Semi - require approval for non-temp folders remediation
5. No automated response

39

Block at risk devices

1. Turn on the Microsoft Intune connection from Microsoft 365 Defender portal
2. Turn on the Defender for Endpoint integration in Endpoint Manager
3. Create the compliance policy in Endpoint Manager
4. Assign the policy
5. Create an Azure AD Conditional Access policy

40

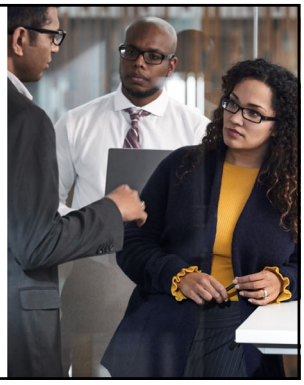
Lesson 8: Configure for alerts and detections

41

Lesson introduction

After this lesson, you will be able to:

- Configure alert settings in Microsoft Defender for Endpoint
- Manage indicators in Microsoft Defender for Endpoint



42

Configure advanced features

Live Response

Live Response unsigned script execution

The Advanced features area provides many an on/off switch for features within the product. The following are settings that are alert and detection focused.

Custom network indicators

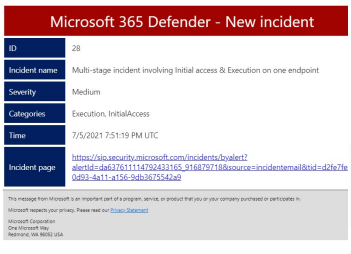
43

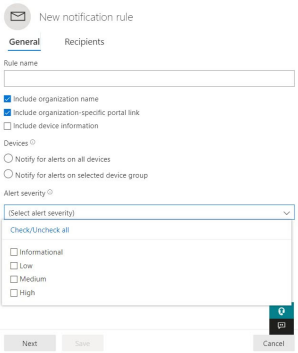
Configure advanced features (continued)

- Microsoft Defender for Identity integration
- Office 365 Threat Intelligence connection
- Microsoft Defender for Cloud Apps
- Microsoft Intune connection
- Microsoft Secure Score

44

Configure Email notifications





45

Manage alert suppression

You can create suppression rules for specific alerts known to be innocuous, such as known tools or processes in your organization. You can use the examples in the following table to help you choose the context for a suppression rule:

Context	Definition	Example scenarios
Suppress alert on this device	Alerts with the same alert title and on that specific device only will be suppressed. All other alerts on that device will not be suppressed.	• A security researcher is investigating a malicious script that has been used to attack other devices in your organization. • A developer regularly creates PowerShell scripts for their team.
Suppress alert in my organization	Alerts with the same alert title on any device will be suppressed.	• A benign administrative tool is used by everyone in your organization.

46

Manage indicators

Indicator of compromise (IoC) matching is an essential feature in every endpoint protection solution. This capability gives SecOps the ability to set a list of detection indicators and for blocking (prevention and response).

IoC type	Available actions
Files	Allow, Audit, Block and remediate
IP addresses	Allow, Audit, Block execution
URLs and domains	Allow, Audit, Block execution
Certificates	Allow, Block and remediate

47

Lesson 9: Utilize Threat and Vulnerability Management

48

Lesson introduction

After this lesson, you will be able to:

- Describe Threat and Vulnerability Management in Microsoft Defender for Endpoint
- Identify vulnerabilities on your devices with Microsoft Defender for Endpoint
- Track emerging threats in Microsoft Defender for Endpoint

49

Explain Threat and Vulnerability Management

Discover vulnerabilities and misconfigurations in real-time with sensors and without the need for agents or periodic scans. It prioritizes vulnerabilities based on the threat landscape, detections in your organization, sensitive information on vulnerable devices, and business context.

- Bridging the workflow gaps
- Real-time discovery
- Intelligence-driven prioritization
- Seamless remediation

50

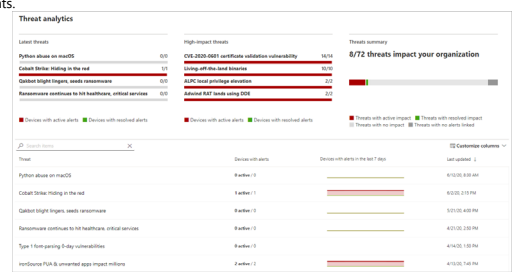
Explore vulnerabilities on your devices

- **Software inventory:** The Software inventory page opens with a list of software installed in your network.
- **Weaknesses:** The Weaknesses page lists the software vulnerabilities your devices are exposed to by listing the Common Vulnerabilities and Exposures (CVE) ID.
- **Event timeline:** The Event timeline is a risk news feed that helps you interpret how risk is introduced into the organization through new vulnerabilities or exploits.
- **Vulnerable devices report:** The report shows graphs and bar charts with vulnerable device trends and current statistics.
- **Hunt for exposed devices:** Advanced hunting is a query-based threat-hunting tool that lets you explore up to 30 days of raw data.

51

Track emerging threats with threat analytics

Assess the impact of new threats and review your resilience against or exposure to the threats.



52

Knowledge check

Check your knowledge with the module quiz in your course viewer

53

Module 2, Lab 01 – Mitigate threats using Microsoft Defender for Endpoint

54

Lab Exercises for module 2

1. Deploy Microsoft Defender for Endpoint
2. Mitigate Attacks using Defender for Endpoint

55

Microsoft Security

56