



Microsoft Defender for Endpoint

Master Class

Trainer DI Thomas Schleich

November 2024

Fast Lane Worldwide Experts in Technology Training and Consulting | Learn.Transform.Succeed.

1



Module 4

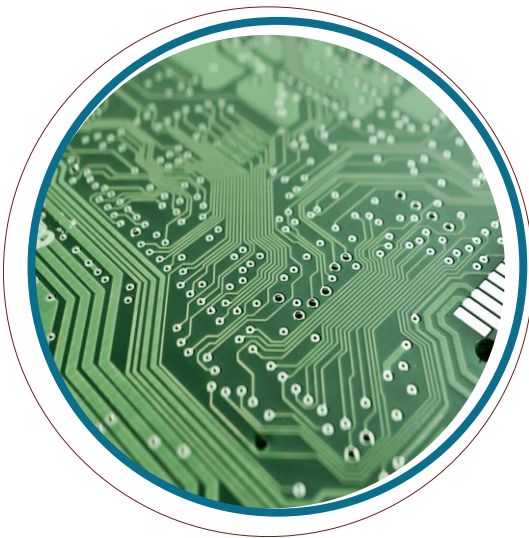
Endpoint Detection and Response

Fast Lane Worldwide Experts in Technology Training and Consulting | Learn.Transform.Succeed.

2

Module 4 Contents:

- **Detections (Alerts, Incidents)**
- **Automated Investigation and Response (AIR)**
- **Remediation actions**
- **Response actions on devices**



Detection

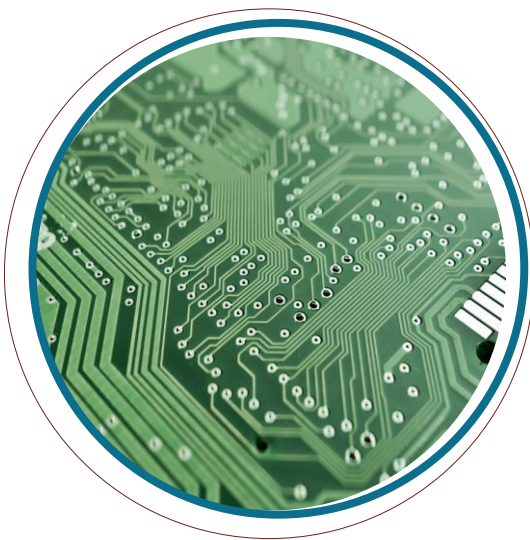
Detections

Alerts

- Organize queue
- Review, manage, investigate
- Investigate
 - Device
 - User/Identity
 - Files
 - IPs

Incidents

- Organize queue
- Manage
- Investigate



Automated Investigation

Automated Investigation and Response (AIR)

'AIR capabilities are designed to examine alerts and take immediate action to resolve breaches. AIR capabilities significantly reduce alert volume, allowing security operations to focus on more sophisticated threats and other high-value initiatives.'

- Remediation actions tracked in Action Center
- available with license
 - MDE P2
 - MDfB

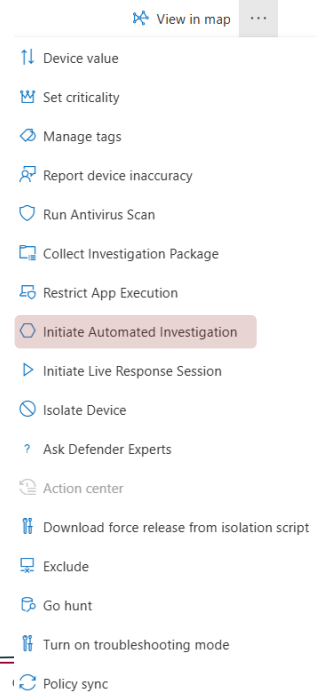
AIR - Process



- If alert is triggered, AIR starts
- For all evidences, a verdict is generated
- Remediation actions will be executed
 - automatically or
 - upon approval

AIR - Initiate manually

- Navigate to a device page
- open Device Action menu
- click 'Initiate Automated Investigation'



© 2023 Fast Lane

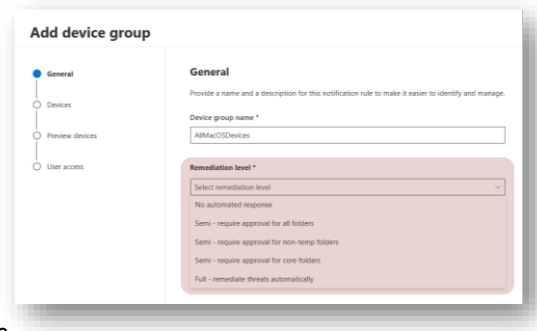
9

9

Source: <https://learn.microsoft.com/en-us/defender-endpoint/automation-levels>

AIR - Automation Levels

- only in MDE P2 available
- set for Device Groups
- Levels
 - Full - remediate threats automatically
 - Semi - require approval for all folders
 - Semi - require approval for core folders
 - Semi - require approval for non-temp folders
 - No automated response



```
\users\*\appdata\local\temp\*
\documents and settings\*\local settings\temp\*
\documents and settings\*\local settings\temporary\*
\windows\temp\*
\users\*\downloads\*
\program files\
\program files (x86)\*
\documents and settings\*\users\*
```

© 2023 Fast Lane

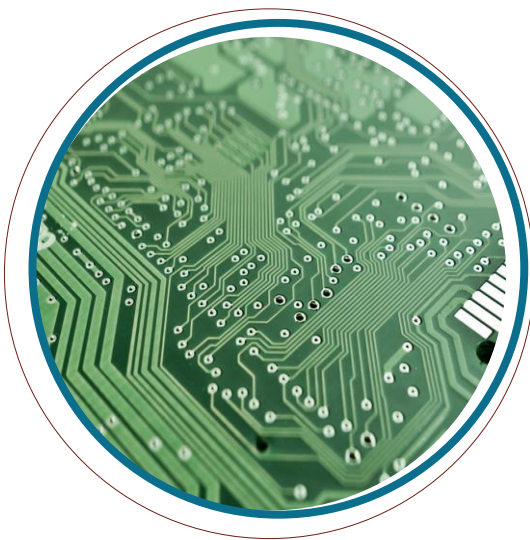
CourseName (FL-XXX) vx.x, Modulename

10

10

Remediation Actions

- Quarantine a file
- Remove a registry key
- Kill a process
- Stop a service
- Disable a driver
- Remove a scheduled task



Response Actions

View in map ...

- Device value
- Set criticality
- Manage tags
- Report device inaccuracy
- Run Antivirus Scan
- Collect Investigation Package
- Restrict App Execution
- Initiate Automated Investigation
- Initiate Live Response Session
- Isolate Device
- Ask Defender Experts
- Action center
- Download force release from isolation script
- Exclude
- Go hunt
- Turn on troubleshooting mode
- Policy sync

13

Response Actions

- on top of specific device page
- MDE P1 only:
 - Run antivirus scan
 - Isolate device

Coursename (FL-XXX) vx.x, Modulename

13

View in map ...

- Device value
- Set criticality
- Manage tags
- Report device inaccuracy
- Run Antivirus Scan
- Collect Investigation Package
- Restrict App Execution
- Initiate Automated Investigation
- Initiate Live Response Session
- Isolate Device
- Ask Defender Experts
- Action center
- Download force release from isolation script
- Exclude
- Go hunt
- Turn on troubleshooting mode
- Policy sync

14

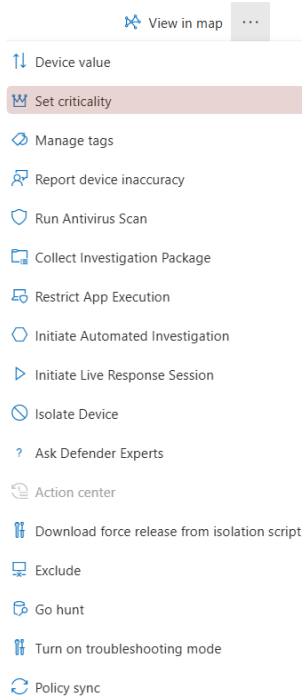
Response Actions

Device value

- 'The device value is used to incorporate the risk appetite of an individual asset into the Defender Vulnerability Management exposure score calculation.'*
- Values: Low - Normal - High
- Exposure score:
 - 'reflects how vulnerable your organization is to cybersecurity threats. Low exposure score means your devices are less vulnerable to exploitation.'*
 - the lower the better ...

Coursename (FL-XXX) vx.x, Modulename

14



15

Source: <https://learn.microsoft.com/en-us/security-exposure-management/critical-asset-management>

Response Actions

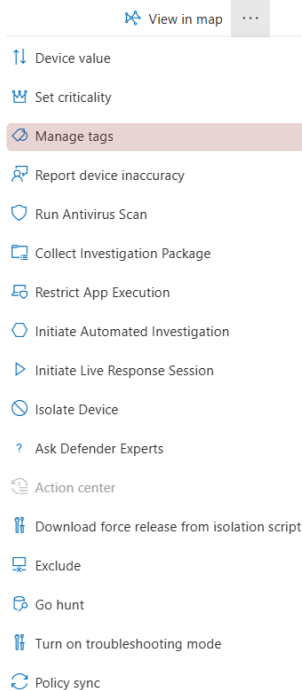
Set criticality - part of exposure management

- 'You can prioritize security investigations, posture recommendations, and remediation steps to focus on critical assets first.'
- Help to filter for critical devices
- used in attack path analysis
- Predefined levels for devices used - refer to source
- Values

Set manual criticality level *

- ☐ Very high - tier 0
- ☐ High - tier 1
- ☐ Medium - tier 2
- ☐ Low - tier 3
- ☐ None

ne 15



16

Source: <https://learn.microsoft.com/en-us/defender-endpoint/machine-tags#add-device-tags-by-setting-a-registry-key-value>

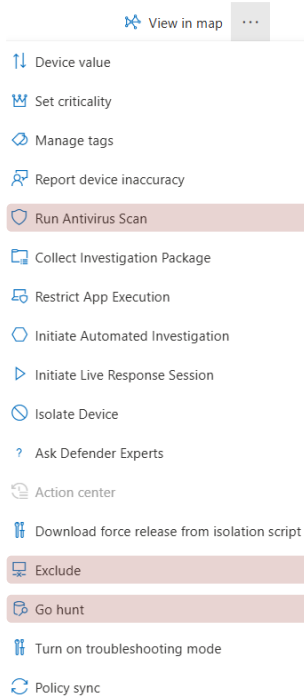
Response Actions

Manage tags

- additional custom information for devices
- useful for filtering device list
- useful for indication of devices (MDE-Management)
- can also be set by Registry
- Types
 - Manual
 - Rule-based
 - Rules: Settings | MS Defender XDR | Asset rule mgmt
 - System
 - like 'Internet facing'

Course name (FL-XXX) vx.x, Modulename

16



17

Response Actions

Run Antivirus Scan

- Select a quick or full scan
- provide a comment
- see the result in Action center

Exclude

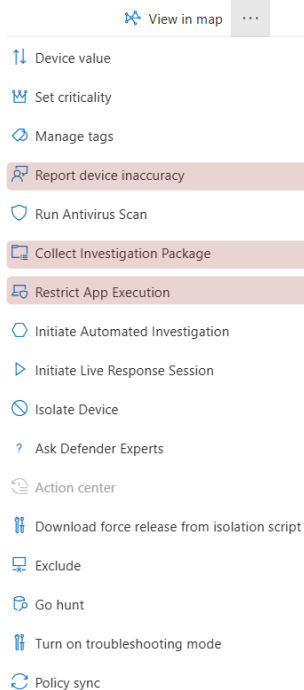
- Sets device to excluded and could be filtered out in device list
- necessary for removed or renamed devices

Go hunt

- Creates a KQL query and opens an editor with it
- for further investigation

Course name (FL-XXX) vx.x, Modulename

17



18

Response Actions

Report device inaccuracy

- Report inaccurate device information to Microsoft

Collect Investigation Package

- Starts the collection of important information
- Download result from Action center

Restrict App Execution

- Only apps signed by Microsoft can be started on device
- Click 'Remove App Restriction' to allow all apps again

Course name (FL-XXX) vx.x, Modulename

18

View in map ...

- Device value
- Set criticality
- Manage tags
- Report device inaccuracy
- Run Antivirus Scan
- Collect Investigation Package
- Restrict App Execution
- Initiate Automated Investigation
- Initiate Live Response Session
- Isolate Device**
- Ask Defender Experts
- Action center
- Download force release from isolation script
- Exclude
- Go hunt
- Turn on troubleshooting mode
- Policy sync

19

Response Actions

Isolate Device

- disconnects device from network
- connectivity to MDE retained
- Outlook, Teams and Skype communication optionally allowed
- User gets message 'Network disabled'

Enable Network on device again

- Click 'Release from isolation' in device action menu
- or: Download force release from isolation script
 - must be put to device and executed as administrator
 - a registry entry is created to start unisolation

Course name (FL-XXX) vx.x, Module name

19

View in map ...

- Device value
- Set criticality
- Manage tags
- Report device inaccuracy
- Run Antivirus Scan
- Collect Investigation Package
- Restrict App Execution
- Initiate Automated Investigation
- Initiate Live Response Session
- Isolate Device
- Ask Defender Experts
- Action center
- Download force release from isolation script
- Exclude
- Go hunt
- Turn on troubleshooting mode**
- Policy sync

20

Response Actions

Troubleshooting mode

- Tamper protection is on by default, so no changes to the Windows Defender settings are possible
- but, with Troubleshooting mode turned on, an administrator is allowed to turn off Tamper protection on a device.

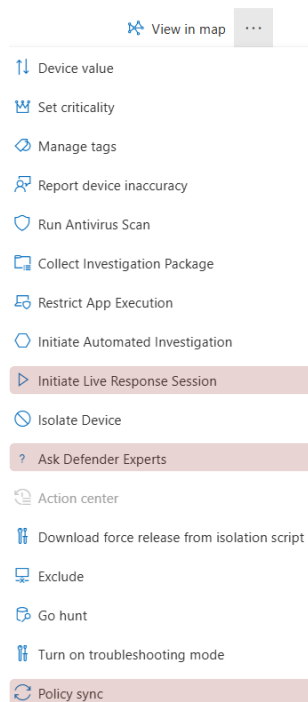
```
Set-MpPreference -DisableTamperProtection $true
```

Examples could be found [here](#)

- Unable to install application
- Microsoft Office plugin blocked by ASR

Course name (FL-XXX) vx.x, Module name

20



Response Actions

Ask Defender Experts

- Start talking with a human expert of Microsoft

Policy sync

- starts sync of new or change Endpoint Security Policies

Initiate Live Response Session

- continued on next slides

Coursename (FL-XXX) vx.x, Modulename

21

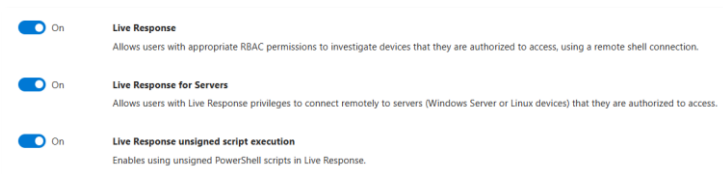
21

Live Response

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

Requirements

- Device OS: Windows 10, 11, Server, Linux, macOS
- Enabling: Settings | Endpoint | Adv Features
- RBAC Permissions



© 2023 Fast Lane

Coursename (FL-XXX) vx.x, Modulename

22

22

Live Response

- Initiated in XDR portal as device action

Commands - Basic



Commands - Adv



analyze	library
collect	putfile
isolate	remediate
release	scan
run	undo

od	persistence
connect	processes
persistence	registry
processes	scheduledtasks
registry	services
scheduledtasks	startupfolders
services	status
startupfolders	trace
status	jobs
trace	

```
C:\> help_
```

```
C:\> help services_
```

Live Response

Demo

- Using help
- Find a file
- Get file from device
- Put file to device
- Run a script from library
- Run a script from library with parameters
- Clean up library
- Get registry entries
- Redirection



End of Module 4