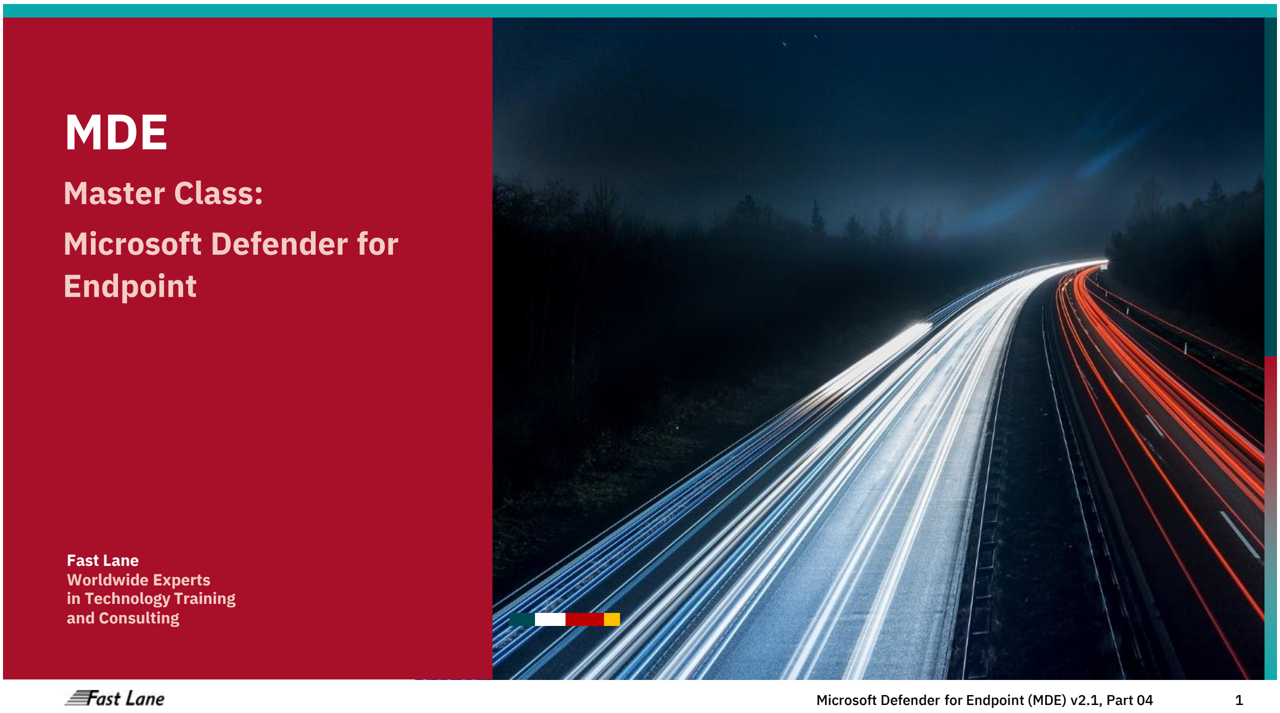


MDE

Master Class: Microsoft Defender for Endpoint

Fast Lane
Worldwide Experts
in Technology Training
and Consulting

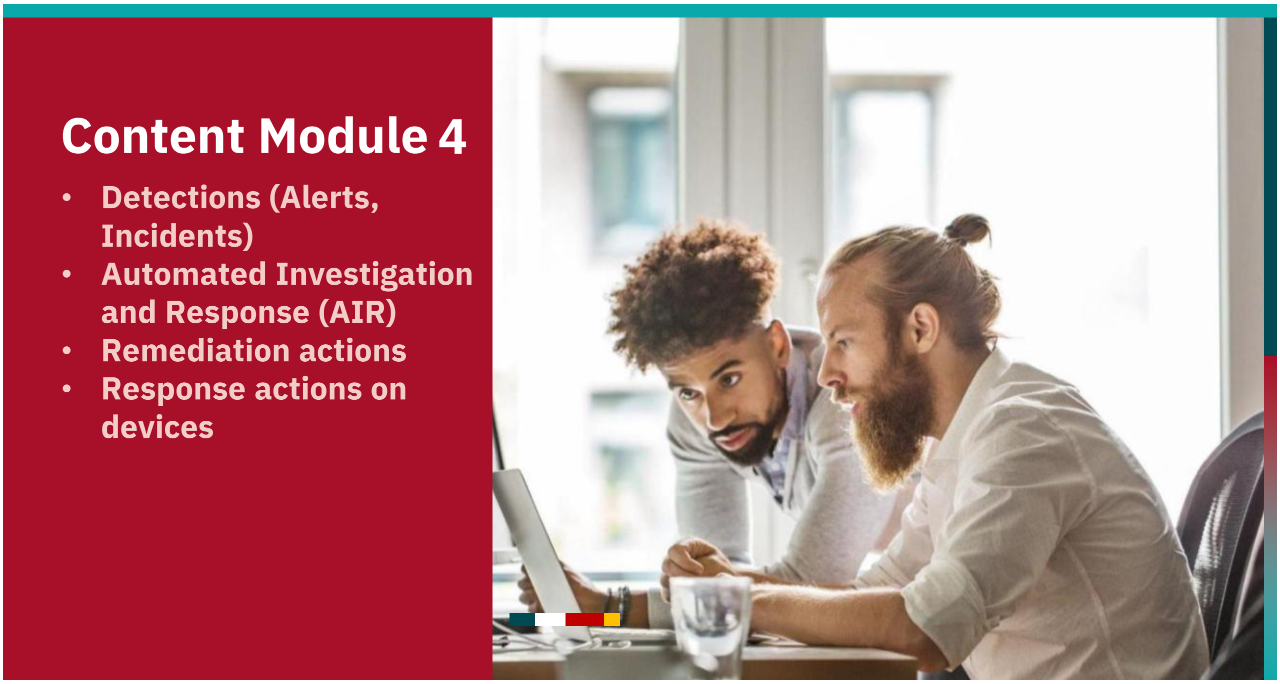
1

Module 4

Endpoint Detection and Response

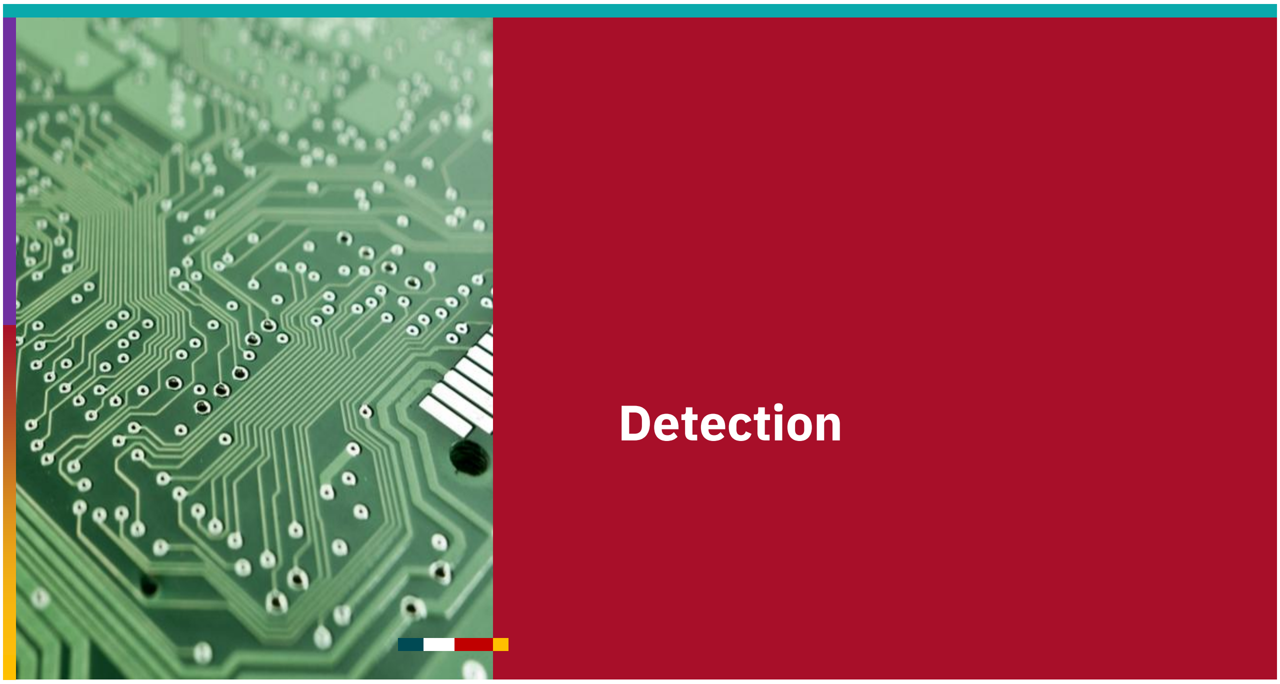
Fast Lane
Worldwide Experts
in Technology Training
and Consulting

2



Content Module 4

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



Detection

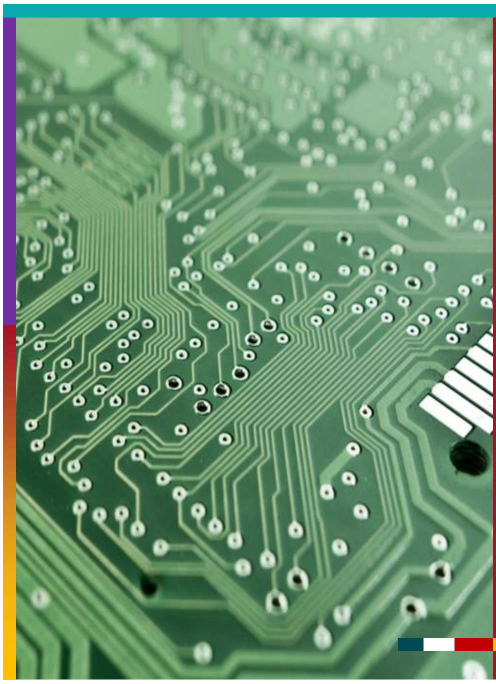
Detections

Alerts

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

Incidents

- Organize queue
- Manage
- Investigate



Automated Investigation

Source: https://learn.microsoft.com/en-us/defender-endpoint/automated-investigations

Automated Investigation and Response (AIR)

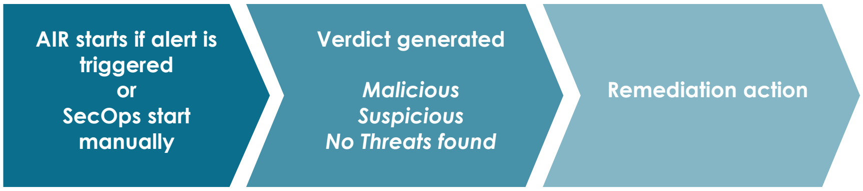
'AIR capabilities are designed to examine alerts and take immediate action to resolve breaches. AIR capabilities significantly reduce alert volume, allowing security operations to focus on more sophisticated threats and other high-value initiatives.'

- 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 starts if alert is triggered
or
SecOps start manually

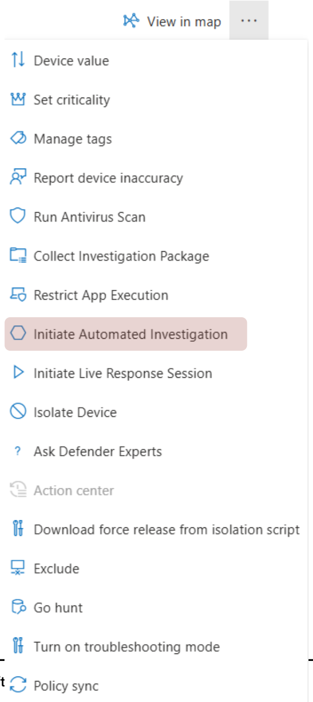
Verdict generated

Malicious
Suspicious
No Threats found

Remediation action

AIR - Initiate manually

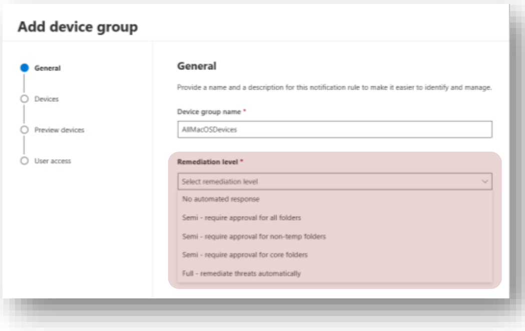
- Navigate to a device page
- open Device Action menu
- click 'Initiate Automated Investigation'



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



Add device group

General

Provide a name and a description for this notification rule to make it easier to identify and manage.

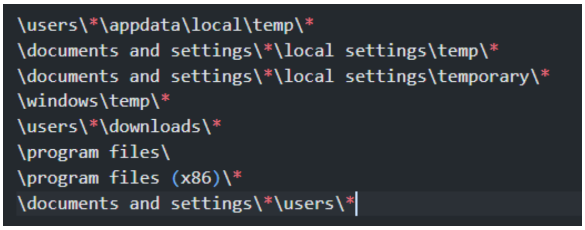
Device group name *

AllMacOSDevices

Remediation level *

Select remediation level

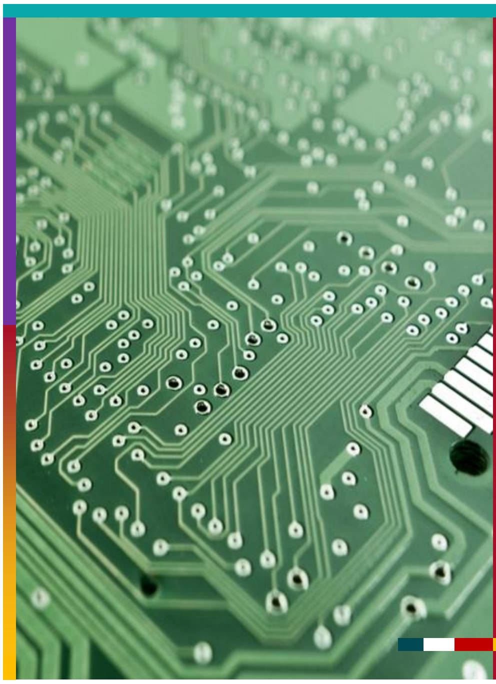
General
Devices
Preview devices
User access
No automated response
Semi - require approval for all folders
Semi - require approval for non-temp folders
Semi - require approval for core folders
Full - remediate threats automatically



```
\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\*
```

Remediation Actions

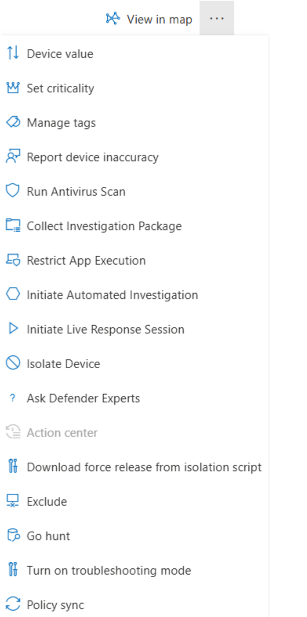
- Quarantine a file
- Remove a registry key
- Kill a process
- Stop a service
- Disable a driver
- Remove a scheduled task



Response Actions

Response Actions

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

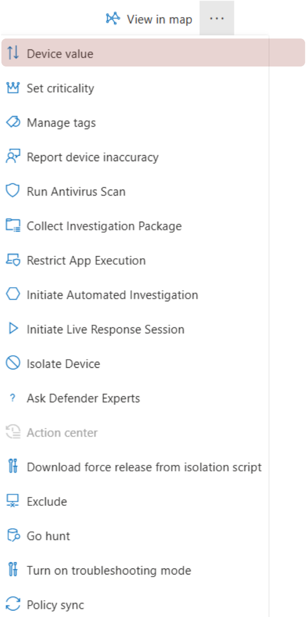


Response Actions

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 …

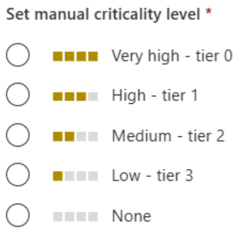


Source: https://learn.microsoft.com/en-us/security-exposure-management/critical-asset-management

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 *

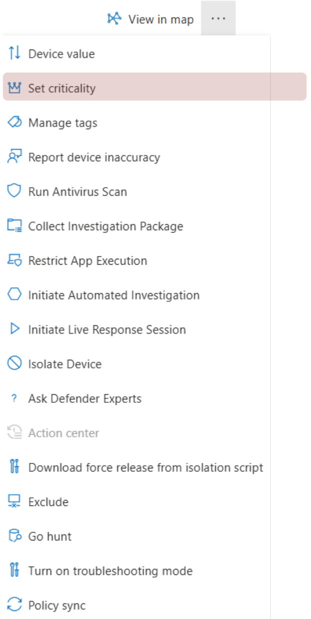
○ Very high - tier 0

○ High - tier 1

○ Medium - tier 2

○ Low - tier 3

○ None



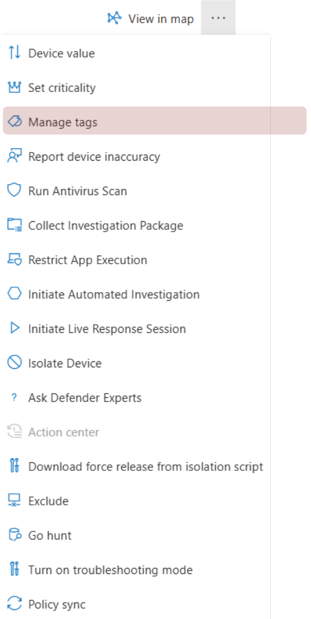
Source: https://learn.microsoft.com/en-us/defender-endpoint/machine-tags#add-device-tags-by-setting-a-registry-key-value

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'



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

Response Actions

Run Antivirus Scan

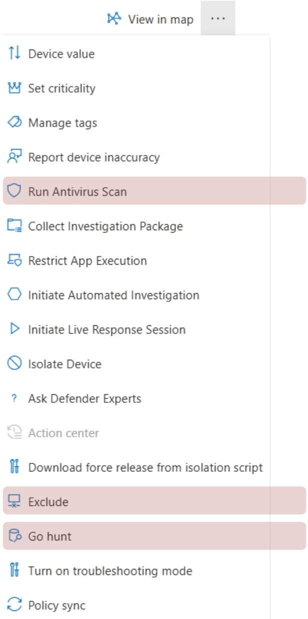
- Select a quick of full scan
- provide a comment
- see the result in Action center

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



Response Actions

Report device inaccuracy

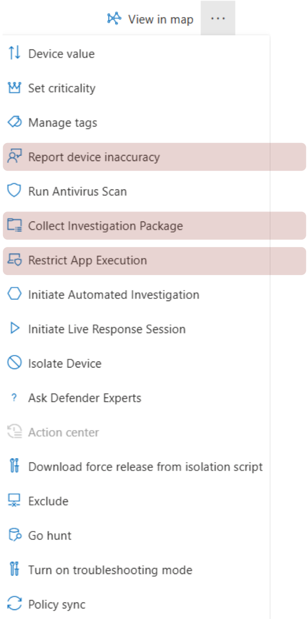
- Report inaccurate device information to Microsoft

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



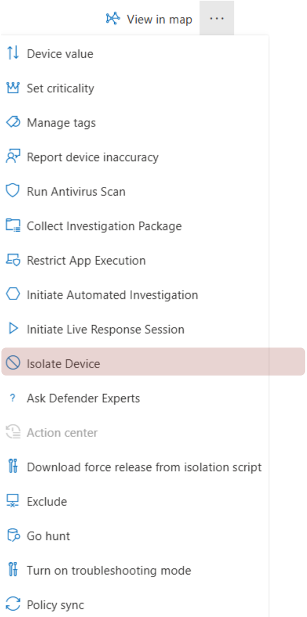
Response Actions

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

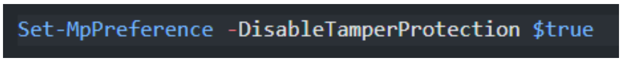
- Click 'Release from isolation' in device action menu
- or: Download force release from isolation script
  - must be put to device and executed as administrator
  - a registry entry is created to start unisolation



Response Actions

Troubleshooting mode

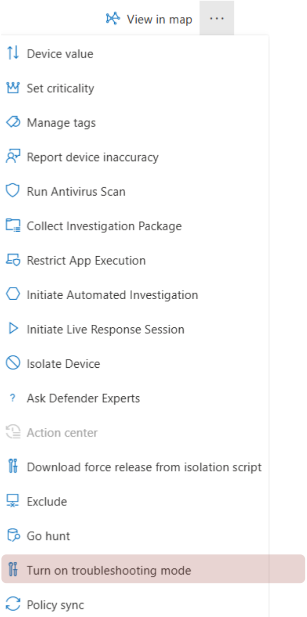
- Tamper protection is on by default, so no changes to the Windows Defender settings are possible
- but, with Troubleshooting mode turned on, an administrator is allowed to turn of Tamper protection on a device.



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

Examples could be found here

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



Response Actions

Ask Defender Experts

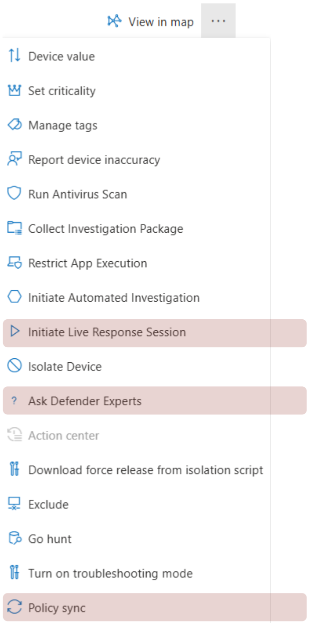
- Start talking with a human expert of Microsoft

Policy sync

- starts sync of new or change Endpoint Security Policies

Initiate Live Response Session

- continued on next slides

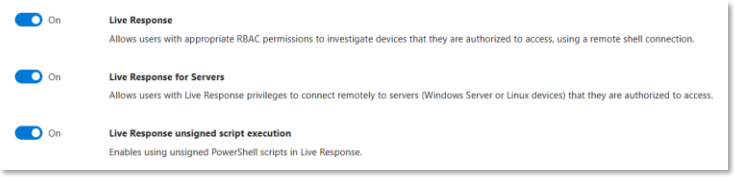


Live Response

'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



On **Live Response**
Allows users with appropriate RBAC permissions to investigate devices that they are authorized to access, using a remote shell connection.

On **Live Response for Servers**
Allows users with Live Response privileges to connect remotely to servers (Windows Server or Linux devices) that they are authorized to access.

On **Live Response unsigned script execution**
Enables using unsigned PowerShell scripts in Live Response.

Live Response

- Initiated in XDR portal as device action

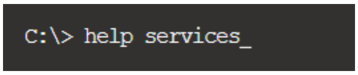
Commands - Basic

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

Commands - Adv

analyze	library
collect	putfile
isolate	remediate
release	*scan*
run	undo

```
C:\> help_
```



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

Live Response

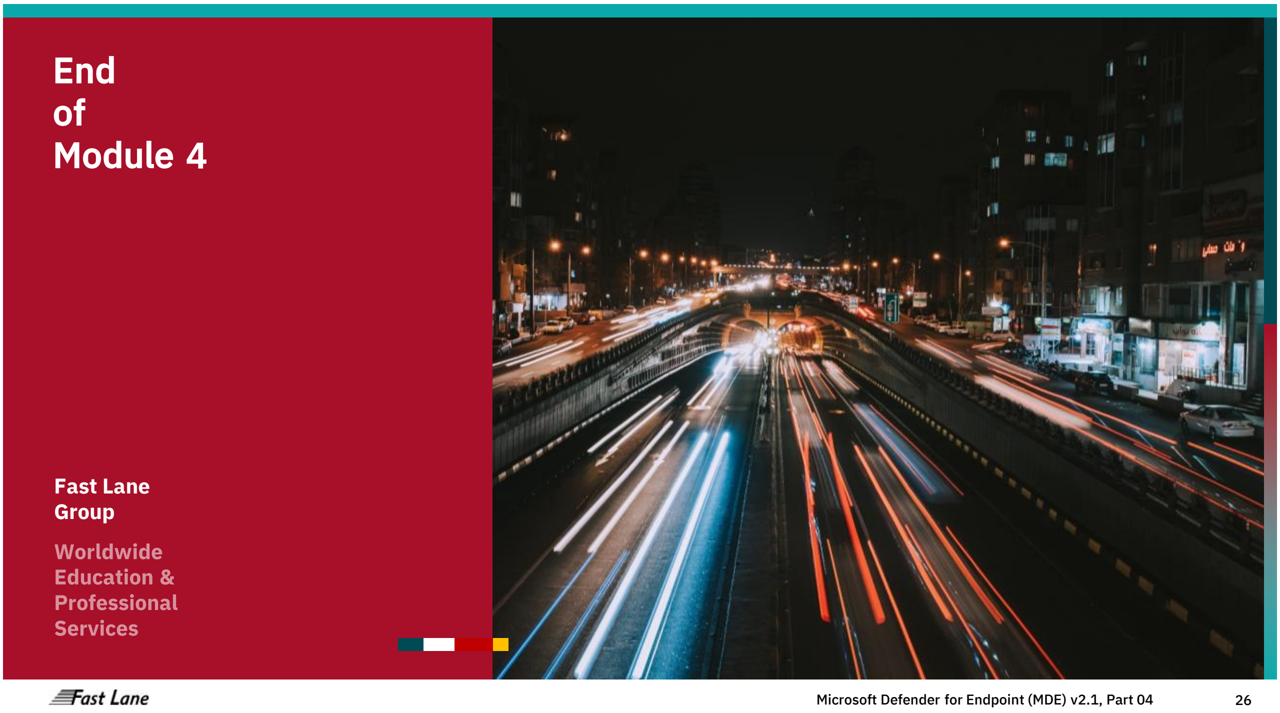
Demo

- 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

Questions?

Fast Lane Group

Worldwide Education & Professional Services



End of Module 4

Fast Lane Group

Worldwide Education & Professional Services