Manage alerts and incidents in Microsoft Defender for Endpoint

# Defender for Endpoint terminology

**Device:** Each endpoint is considered a Device.

**Evidence:** Defender for endpoint collects forensics information on artifacts, including accounts, processes, network information and others.

**Alert:** Defender for endpoint uses detection rules based on Microsoft expertise and that are continually updated looks for suspicious activities. If found it’ll generate an alert.

**Incident:**  Defender for endpoint groups the alerts into incidents.

**Investigation:** Automated Investigation performed by defender for endpoint

# SOC Dashboard

SOC dashboard provides a high-level overview of:

* Active Alerts
* Devices at risk
* Sensor health
* Service health
* Daily devices reporting
* Active automated investigations
* Automated investigations statistics
* Users at risk
* Suspicious activities

# Automation levels in automated investigation and remediation (AIR) capabilities

* **Full automation(recommended):**  means remediation actions are taken automatically on artifacts determined to be malicious
* **Semi automation:** Means some remediation actions are taken automatically, but other remediation actions await approval before being taken
* **No automated response**
* All remediation actions, whether pending or completed are tracked in the Action Centre.

# Levels of automation

* **Full automation – Remediate threats automatically**

All remediation actions are performed automatically and can be viewed in the action centre on the history tab. If necessary, a remediation action can be undone.

* **Semi automation – require approval for any remediation**

Approval is required for any remediation action. Such pending actions can be viewed and approved in the action centre on the pending tab.

* **Semi automation – require approval for core folders remediation**

Approval is required for any remediation actions needed on files or executables tat are in core folders.

* **Semi automation – require approval for non-temp folders remediation**

Approval required for any remediation actions needed on files or executables that are not in temp folders like:

\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\*

* **No automated response**

AIR does not run on your organisation’s devices. However other threat protection features, such as protection from potentially unwanted applications can be in effect depending on antivirus and next-gen protections features are configured.

# Action Centre

* **Pending Actions** – displays a list of ongoing investigations that require attention. Recommended actions are presented that your SOC team can approve or reject. Pending tab appears only if there are pending actions to be approved (or rejected).
* **History Acts** – as an audit log for all of the following items:
  + Remediation actions taken as a result of automated investigation
  + Remediation actions that were approved by your SOC team
  + Commands that were run and remediation actions that were applied in Live Response sessions
  + Remediation actions that were applied by Microsoft Defender Antivirus