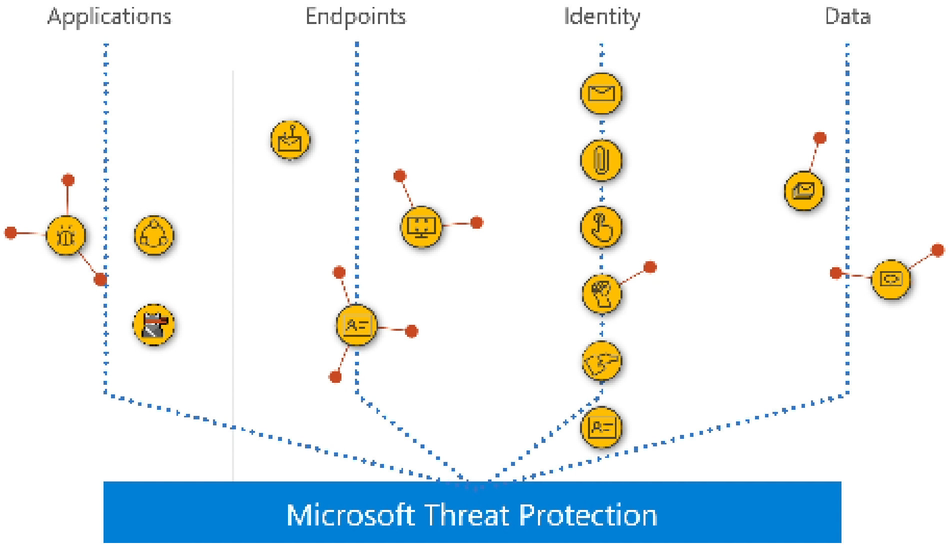
Mitigate incidents using Microsoft 365 Defender

By: Ryan Stewart

Microsoft Defender XDR delivers a cross-domain threat correlation platform and a purpose-driven portal designed for in-depth threat investigation. Incidents are formulated from correlated alerts triggered upon the detection of malicious events or activities within your network. While individual alerts offer valuable insights into ongoing attacks, the complexity arises from attacks utilizing diverse vectors and techniques to execute a breach. Assembling these individual clues can pose challenges and consume considerable time.

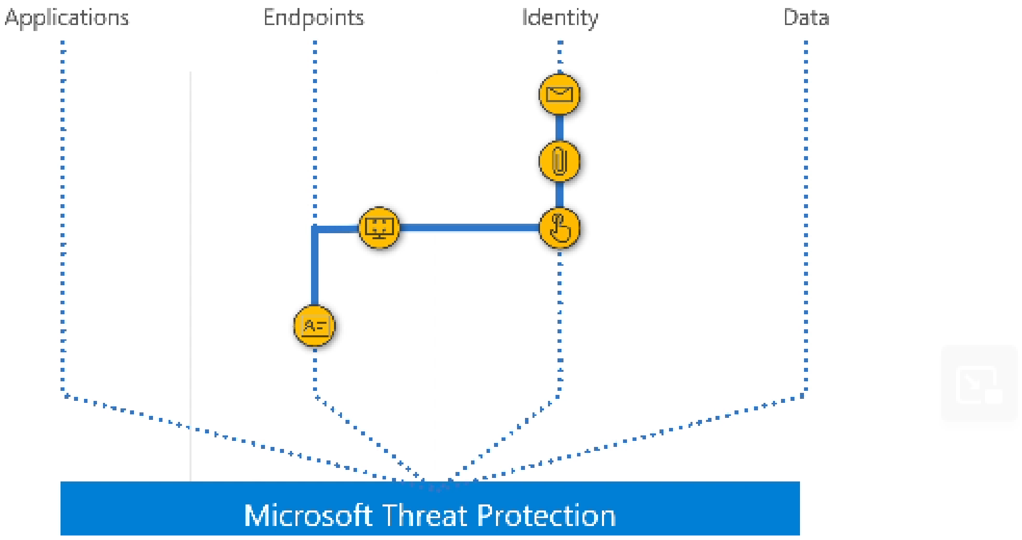


An incident comprises a set of correlated alerts that weave together the narrative of an attack. Microsoft Defender XDR **seamlessly consolidates** malicious and suspicious events detected across various device, **user**, and **mailbox entities** in the network. The grouping of related alerts into an incident offers security defenders a comprehensive view of an attack.

For example, security defenders gain insights into the **attack's origin**, **employed tactics**, and the **extent of penetration** into the network. They can assess the attack's scope, including the number of impacted devices, users, and mailboxes, the **severity of the impact,** and other pertinent details about affected entities.

If configured, Microsoft Defender XDR can **autonomously** investigate and resolve individual alerts through **automation** and artificial intelligence. Security defenders also have the capability to execute additional remediation steps directly from the incidents view.

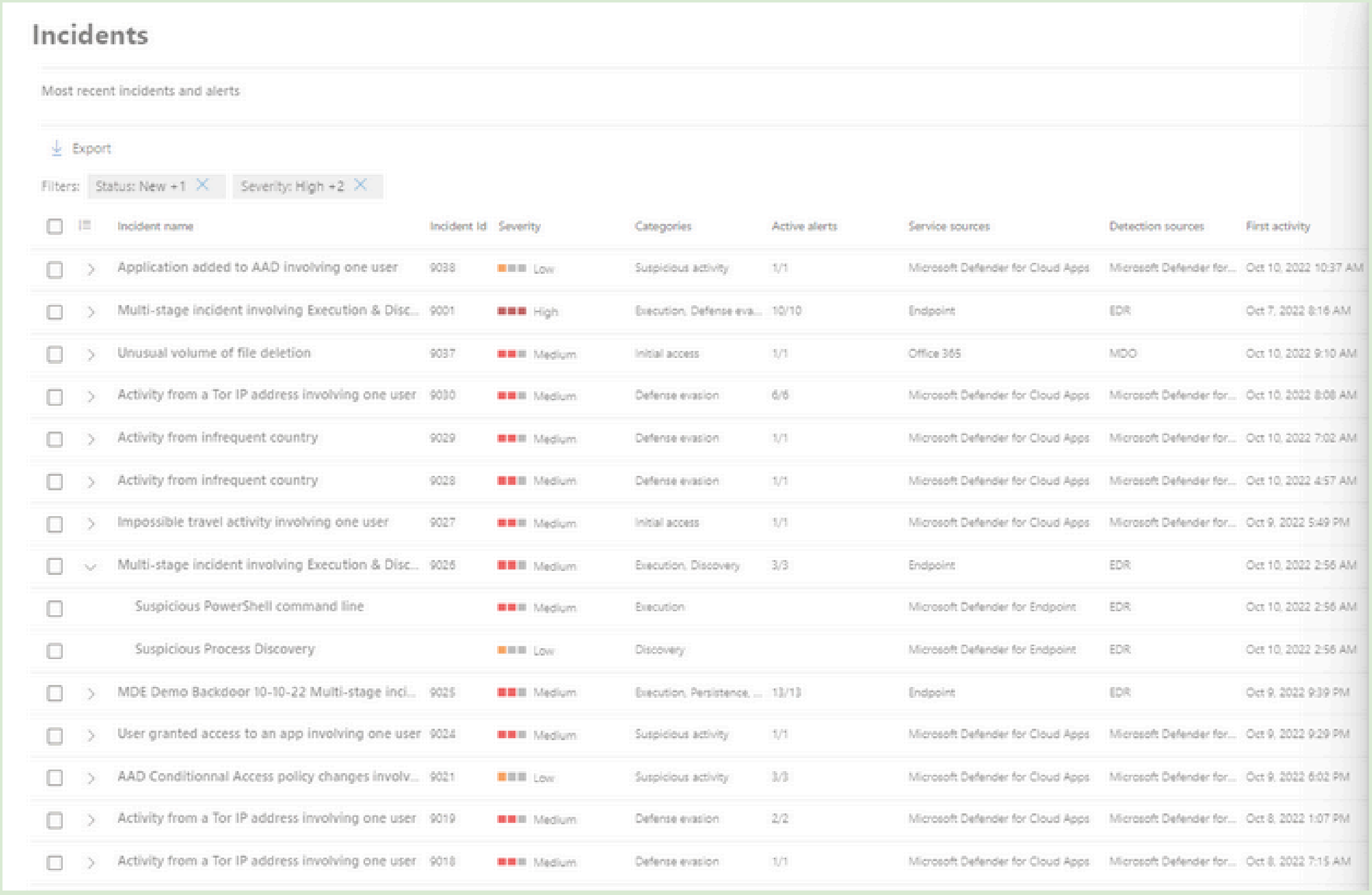
Incidents from the last 30 days are accessible in the incident queue, allowing security defenders to prioritize based on risk level and other factors. Furthermore, security defenders can enhance their incident management experience by renaming incidents, assigning them to specific analysts, classifying, and adding tags for a more tailored and efficient workflow.



Incident Prioritization

Microsoft Defender XDR utilizes correlation analytics to consolidate related alerts and investigations from different products into a unified incident. Leveraging its end-to-end visibility across the entire estate and suite of products, Microsoft Defender XDR also generates distinct alerts for activities that exhibit characteristics of malicious intent. This comprehensive perspective equips **security operations analysts** with a **more extensive** understanding of the attack narrative, enabling them to adeptly manage complex threats across the organization.

The Incidents queue presents a compilation of flagged incidents encompassing devices, users, and mailboxes. This functionality assists in navigating through incidents, **streamlining the prioritization process**, and facilitating well-informed decision-making for an efficient cybersecurity response.



Incidents

Most recent incidents and alerts

Filters: Status: New +1 × Severity: High +2 ×

□		Incident name	Incident Id	Severity	Categories	Active alerts	Service sources	Detection sources	First activity
□	>	Application added to AAD involving one user	9038	■■■ Low	Suspicious activity	1/1	Microsoft Defender for Cloud Apps	Microsoft Defender for...	Oct 10, 2022 10:37 AM
□	>	Multi-stage incident involving Execution & Disc...	9001	■■■ High	Execution, Defense eva...	10/10	Endpoint	EDR	Oct 7, 2022 8:16 AM
□	>	Unusual volume of file deletion	9037	■■■ Medium	Initial access	1/1	Office 365	MDO	Oct 10, 2022 9:10 AM
□	>	Activity from a Tor IP address involving one user	9030	■■■ Medium	Defense evasion	6/6	Microsoft Defender for Cloud Apps	Microsoft Defender for...	Oct 10, 2022 8:08 AM
□	>	Activity from infrequent country	9029	■■■ Medium	Defense evasion	1/1	Microsoft Defender for Cloud Apps	Microsoft Defender for...	Oct 10, 2022 7:02 AM
□	>	Activity from infrequent country	9028	■■■ Medium	Defense evasion	1/1	Microsoft Defender for Cloud Apps	Microsoft Defender for...	Oct 10, 2022 4:57 AM
□	>	Impossible travel activity involving one user	9027	■■■ Medium	Initial access	1/1	Microsoft Defender for Cloud Apps	Microsoft Defender for...	Oct 9, 2022 5:49 PM
□	⌄	Multi-stage incident involving Execution & Disc...	9026	■■■ Medium	Execution, Discovery	3/3	Endpoint	EDR	Oct 10, 2022 2:56 AM
□		Suspicious PowerShell command line		■■■ Medium	Execution		Microsoft Defender for Endpoint	EDR	Oct 10, 2022 2:56 AM
□		Suspicious Process Discovery		■■■ Low	Discovery		Microsoft Defender for Endpoint	EDR	Oct 10, 2022 2:56 AM
□	>	MDE Demo Backdoor 10-10-22 Multi-stage inci...	9025	■■■ Medium	Execution, Persistence, ...	13/13	Endpoint	EDR	Oct 9, 2022 9:39 PM
□	>	User granted access to an app involving one user	9024	■■■ Medium	Suspicious activity	1/1	Microsoft Defender for Cloud Apps	Microsoft Defender for...	Oct 9, 2022 9:29 PM
□	>	AAD Conditionnal Access policy changes involv...	9021	■■■ Low	Suspicious activity	3/3	Microsoft Defender for Cloud Apps	Microsoft Defender for...	Oct 9, 2022 6:02 PM
□	>	Activity from a Tor IP address involving one user	9019	■■■ Medium	Defense evasion	2/2	Microsoft Defender for Cloud Apps	Microsoft Defender for...	Oct 8, 2022 1:07 PM
□	>	Activity from a Tor IP address involving one user	9018	■■■ Medium	Defense evasion	1/1	Microsoft Defender for Cloud Apps	Microsoft Defender for...	Oct 8, 2022 7:15 AM

By default, the Microsoft Defender portal's incident queue displays incidents observed within the **last 30 days**, with the **most recent incident** positioned at the top for **immediate** visibility.

The incident queue provides customizable columns that offer insights into various incident characteristics or the entities involved. This additional layer of information aids in making informed decisions about incident prioritization.

For quick clarity, the automatic incident naming feature generates incident names based on alert attributes such as the number of affected endpoints, impacted users, detection sources, or categories. This automatic naming facilitates a rapid understanding of the incident's scope.

Available Filters:

1. Status:
   - Choose to view incidents based on their status, distinguishing between active or resolved cases.

2. Severity:
   - Incident severity indicates its potential impact on your assets. Higher severity levels signify more significant impacts, demanding immediate attention.

3. Incident Assignment:
   - Opt to display alerts assigned to you or those managed by automation.

4. Multiple Service Source:
   - Select No (default) or Yes to enable, filtering incidents containing alerts from various sources like Microsoft Defender for Endpoint, Microsoft Cloud App Security, Microsoft Defender for Identity, and Microsoft Defender for Office 365.

5. Tags:
   - Filter by assigned tags, with tag names appearing upon selection.

6. Multiple Category:
   - Choose to view only incidents mapped to multiple categories, potentially causing more extensive damage.

7. Categories:
   - Focus on specific tactics, techniques, or attack components by selecting relevant categories.

8. Entities:
   - Filter by entity name or ID.

9. Data Sensitivity:
   - Identify incidents involving sensitive data, particularly useful when Microsoft Purview Information Protection is active.

10. Device Group:
    - Filter by defined device groups.

11. OS Platform:
- Limit the incident queue view by operating system.

12. Classification:
- Filter incidents based on set classifications (true alerts, false alerts, or not set) associated with related alerts.

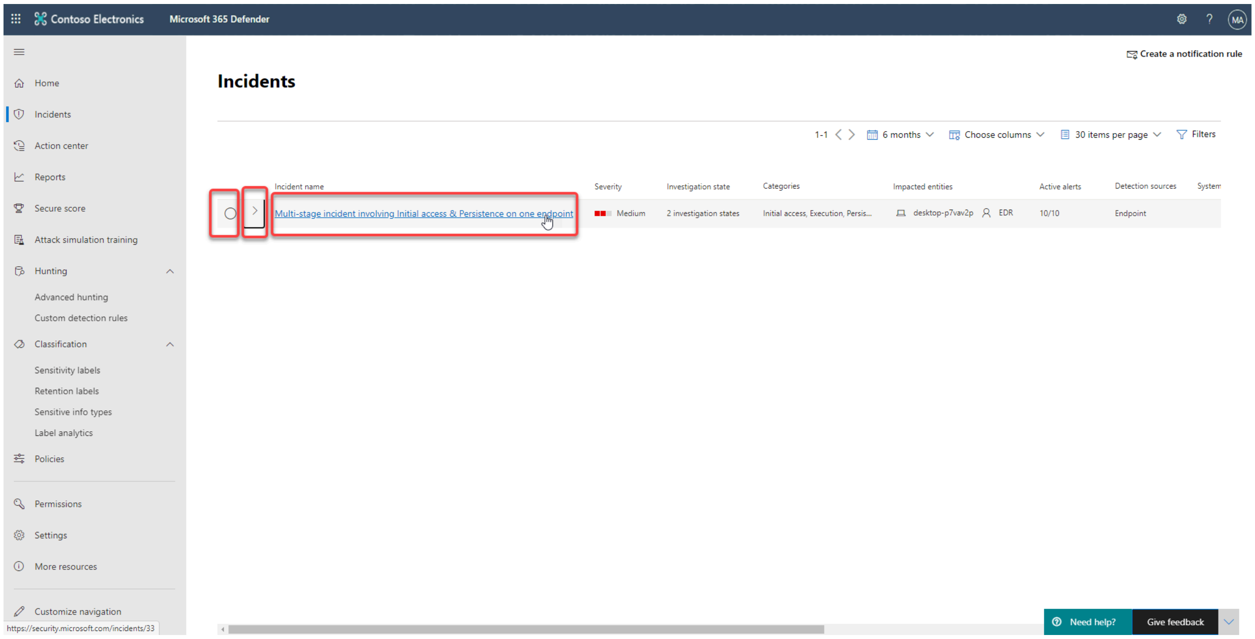
13. Automated Investigation State:
- Filter incidents by the status of automated investigations.

14. Associated Threat:
- Enter threat information and retrieve previous search criteria by selecting the Type associated threat field.

Preview incidents

The portal pages provide preview information for most list-related data.

In this screenshot, the three highlighted areas are the circle, the greater than symbol, and the actual link.

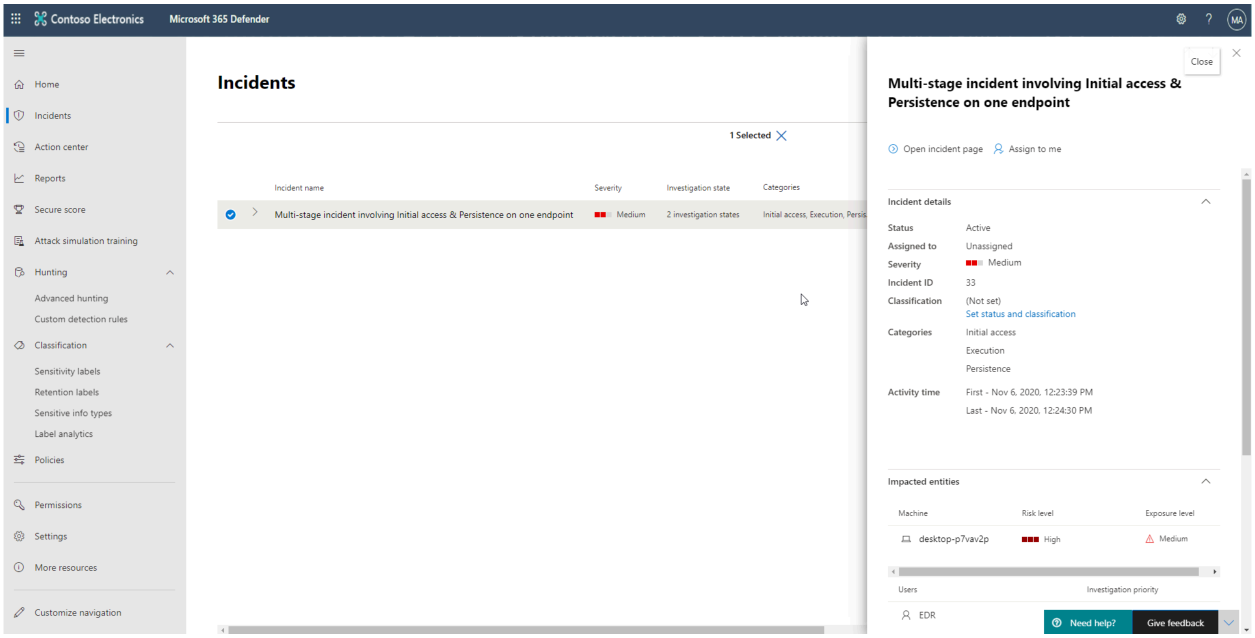


Incidents

		Incident name	Severity	Investigation state	Categories	Impacted entities	Active alerts	Detection sources	System
○	>	Multi-stage incident involving Initial access & Persistence on one endpoint	Medium	2 investigation states	Initial access, Execution, Persis...	desktop-p7vav2p EDR	10/10	Endpoint	

Circle

Selecting the circle will open a details window on the right side of the page with a preview of the line item with an option to open the full page of information.



Incidents

Incident name	Severity	Investigation state	Categories
Multi-stage incident involving Initial access & Persistence on one endpoint	Medium	2 investigation states	Initial access, Execution, Persis

Multi-stage incident involving Initial access & Persistence on one endpoint

Incident details

Status	Active
Assigned to	Unassigned
Severity	Medium
Incident ID	33
Classification	(Not set) Set status and classification
Categories	Initial access Execution Persistence
Activity time	First - Nov 6, 2020, 12:23:39 PM Last - Nov 6, 2020, 12:24:30 PM

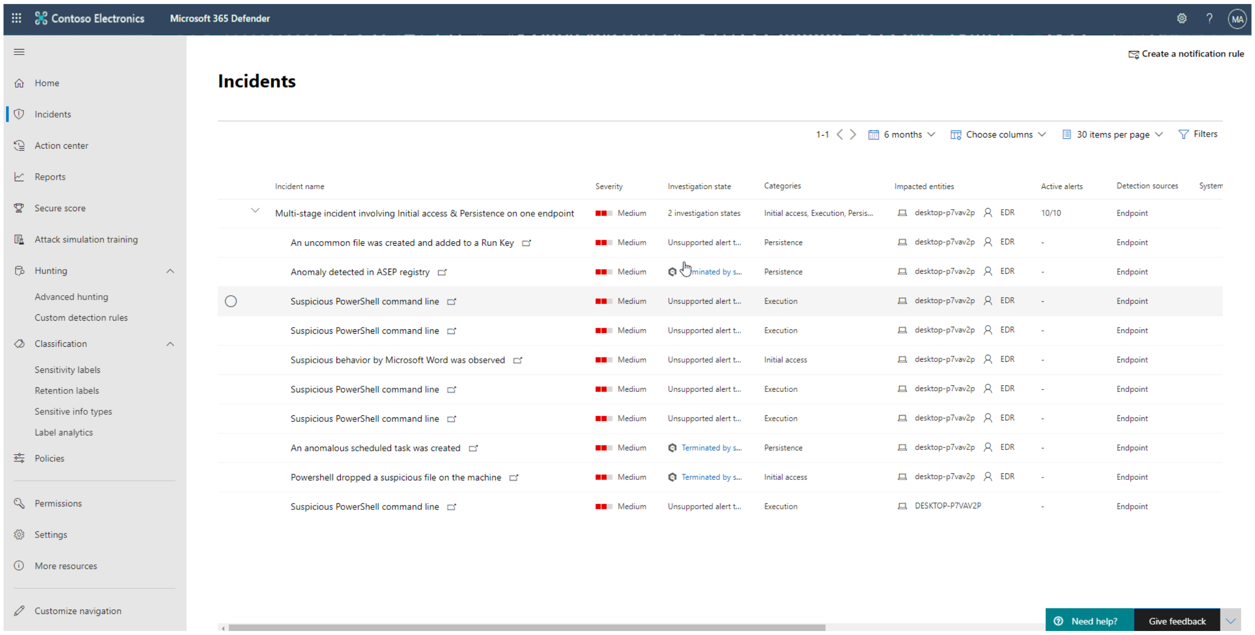
Impacted entities

Machine	Risk level	Exposure level
desktop-p7vav2p	High	Medium

Users	Investigation priority
EDR	

Greater than symbol

If there are related records that can be displayed, selecting the greater than sign will display the records below the current record.



Incidents

Incident name	Severity	Investigation state	Categories	Impacted entities	Active alerts	Detection sources	System
Multi-stage incident involving Initial access & Persistence on one endpoint	Medium	2 investigation states	Initial access, Execution, Persis...	desktop-p7vav2p EDR	10/10	Endpoint	
An uncommon file was created and added to a Run Key	Medium	Unsupported alert t...	Persistence	desktop-p7vav2p EDR	-	Endpoint	
Anomaly detected in ASEP registry	Medium	minated by s...	Persistence	desktop-p7vav2p EDR	-	Endpoint	
Suspicious PowerShell command line	Medium	Unsupported alert t...	Execution	desktop-p7vav2p EDR	-	Endpoint	
Suspicious PowerShell command line	Medium	Unsupported alert t...	Execution	desktop-p7vav2p EDR	-	Endpoint	
Suspicious behavior by Microsoft Word was observed	Medium	Unsupported alert t...	Initial access	desktop-p7vav2p EDR	-	Endpoint	
Suspicious PowerShell command line	Medium	Unsupported alert t...	Execution	desktop-p7vav2p EDR	-	Endpoint	
Suspicious PowerShell command line	Medium	Unsupported alert t...	Execution	desktop-p7vav2p EDR	-	Endpoint	
An anomalous scheduled task was created	Medium	Terminated by s...	Persistence	desktop-p7vav2p EDR	-	Endpoint	
Powershell dropped a suspicious file on the machine	Medium	Terminated by s...	Initial access	desktop-p7vav2p EDR	-	Endpoint	
Suspicious PowerShell command line	Medium	Unsupported alert t...	Execution	DESKTOP-P7VAV2P	-	Endpoint	

Link

The link will navigate you to the full page for the line item.

Manage incidents

Managing incidents is critical in ensuring that threats are contained and addressed. In **Microsoft Defender XDR**, you have access to managing incidents on devices, users, and mailboxes. You can manage incidents by selecting an incident from the Incidents queue.

You can edit the name of an incident, resolve it, set its classification and determination. You can also assign the incident to yourself, add incident tags and comments.

In cases where you would like to move alerts from one incident to another, during an investigation, you can also do so from the Alerts tab. Using the Alerts tab allows you to create a larger or smaller incident that includes all relevant alerts.

Edit incident name

Incidents are automatically assigned a name based on alert attributes such as the number of endpoints affected, users affected, detection sources, or categories. Naming based on alert attributes allows you to quickly understand the scope of the incident. You can modify the incident name to better align with your preferred naming convention.

Assign incidents

If an incident hasn't yet been assigned, you can select Assign to me to assign the incident to yourself. Doing so assumes ownership of not just the incident but also all the alerts associated with it.

Set status and classification

Incident status

You can categorize incidents (as Active, or Resolved) by changing their status as your investigation progresses. This ability to update status helps you organize and manage how your team can respond to incidents.

For example, your SOC analyst can review the urgent Active incidents for the day and decide to assign them to themselves for investigation.

Alternatively, your SOC analyst might set the incident as Resolved if the incident has been remediated. Resolving an incident will automatically close all open alerts that are part of the incident.

Classification and determination

You can choose not to set a classification or decide to specify whether an incident is true alert or false alert. Doing so helps the team see patterns and learn from them.

Add comments

You can add comments and view historical events about an incident to see previous changes made to it.

Whenever a change or comment is made to an alert, it's recorded in the Comments and history section.

Added comments instantly appear on the pane.

Add incident tags

You can add custom tags to an incident, for example, to flag a group of incidents with common characteristics. You can later filter the incidents queue for all incidents that contain a specific tag.