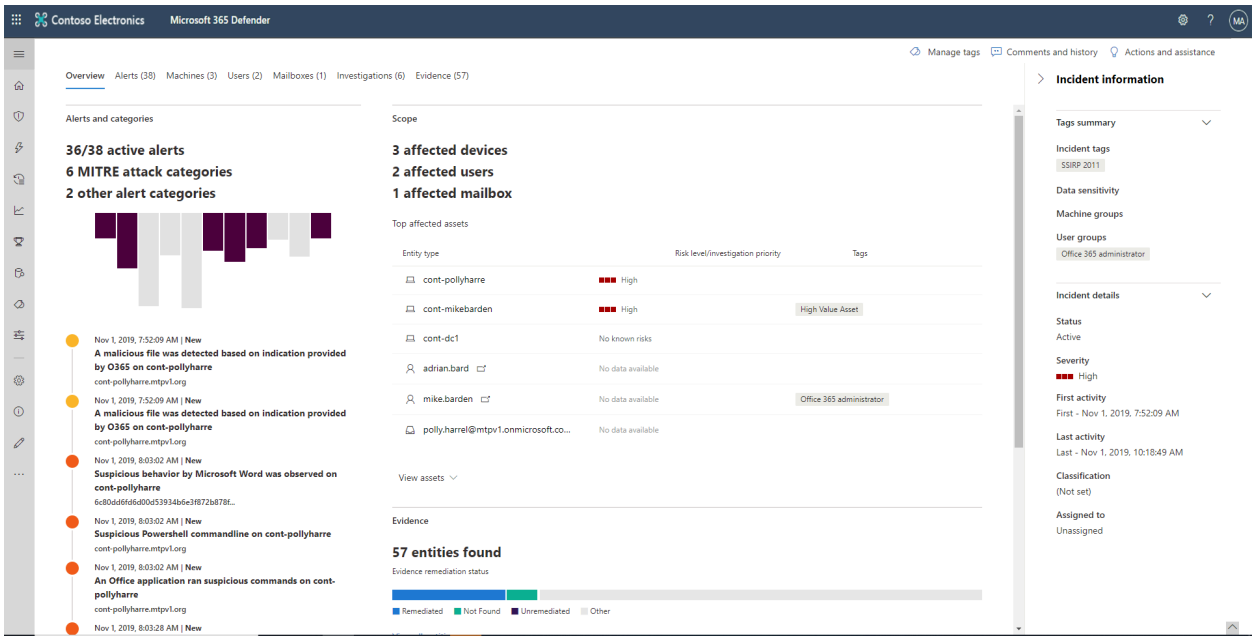
Investigate incidents

By: Ryan Stewart

Incident overview

The overview page gives you a snapshot glance into the top things to notice about the incident.



The attack categories provide both a visual and numeric representation of the attack's advancement throughout the kill chain. Microsoft Defender XDR aligns seamlessly with the MITRE ATT&CK™ framework, in line with other Microsoft security products.

In the scope section, you'll find a comprehensive list of the primary impacted assets within the incident. Specific details related to these assets, such as risk level, investigation priority, and any associated tags, are also highlighted.

The alerts timeline offers a **chronological overview** of the alert sequence, detailing the reasons each alert is linked to the incident. This chronological order provides valuable **insights into the attack's progression.**

The **evidence section** summarizes the various artifacts involved in the incident and their current remediation status. This section allows for quick identification of any necessary actions on your part.

This overview **streamlines** the initial triage of the incident, offering insights into its key characteristics. Now, let's delve into specific sections:

Alerts:

Explore all incident-related alerts, including severity, involved entities, alert sources (Microsoft Defender for Identity, Microsoft Defender for Endpoint, Microsoft Defender for Office 365), and the rationale for their linkage. Alerts are chronologically ordered, facilitating an understanding of the attack's timeline.

Devices:

The devices tab provides a list of all devices with related incident alerts. Clicking on a machine's name navigates you to its Device page, offering a detailed view of triggered alerts and relevant events for thorough investigation.

Users:

Identify users associated with the incident. By clicking on a username, you can access the user's Microsoft Defender for Cloud Apps page for further investigation.

Mailboxes and Apps:

Investigate **mailboxes** and **apps** linked to the incident to gain a comprehensive understanding of their involvement.

Investigations:

Review automated investigations triggered by alerts in the incident. Investigations may execute remediation actions or await analyst approval. Navigate to the Investigation details page for full information, including pending actions.

Evidence and Responses:

Microsoft Defender XDR automatically investigates supported events and entities, providing auto response and information on files, processes, services, emails, and more. Each analyzed entity is marked with a verdict (**Malicious, Suspicious, Clean**) and a **remediation status**.

Graph:

Visualize cybersecurity threat information through the incident graph, highlighting patterns and correlations from various data points. The graph illustrates the cybersecurity attack's narrative, including entry points, indicators of compromise, and observed activities on specific devices. Select circles on the incident graph for detailed information on malicious files, associated detections, and global instances.