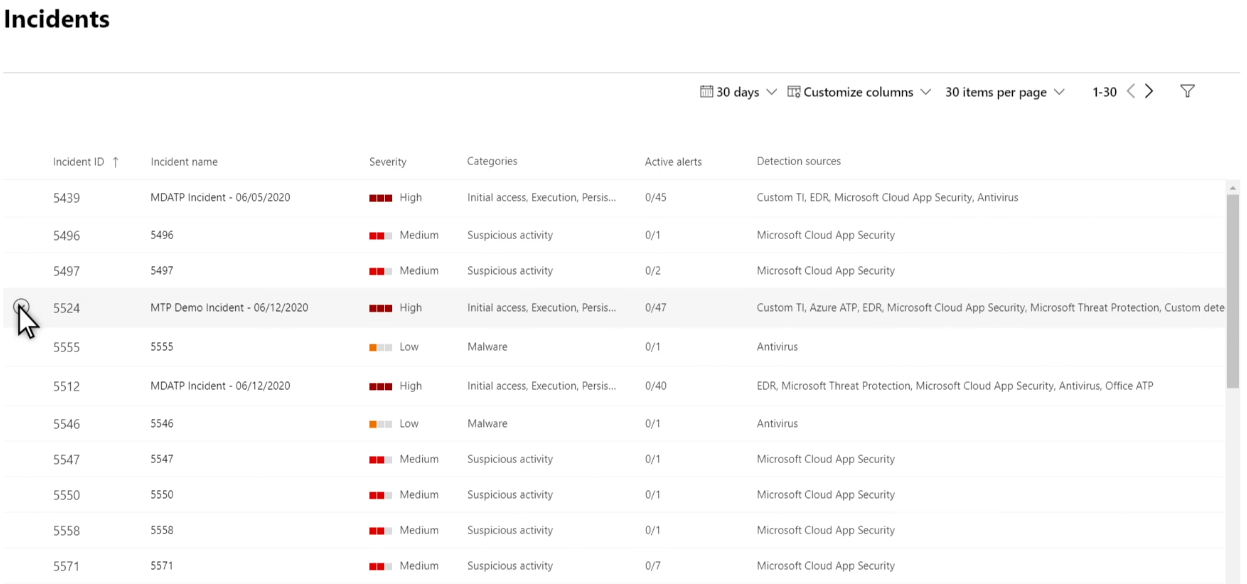
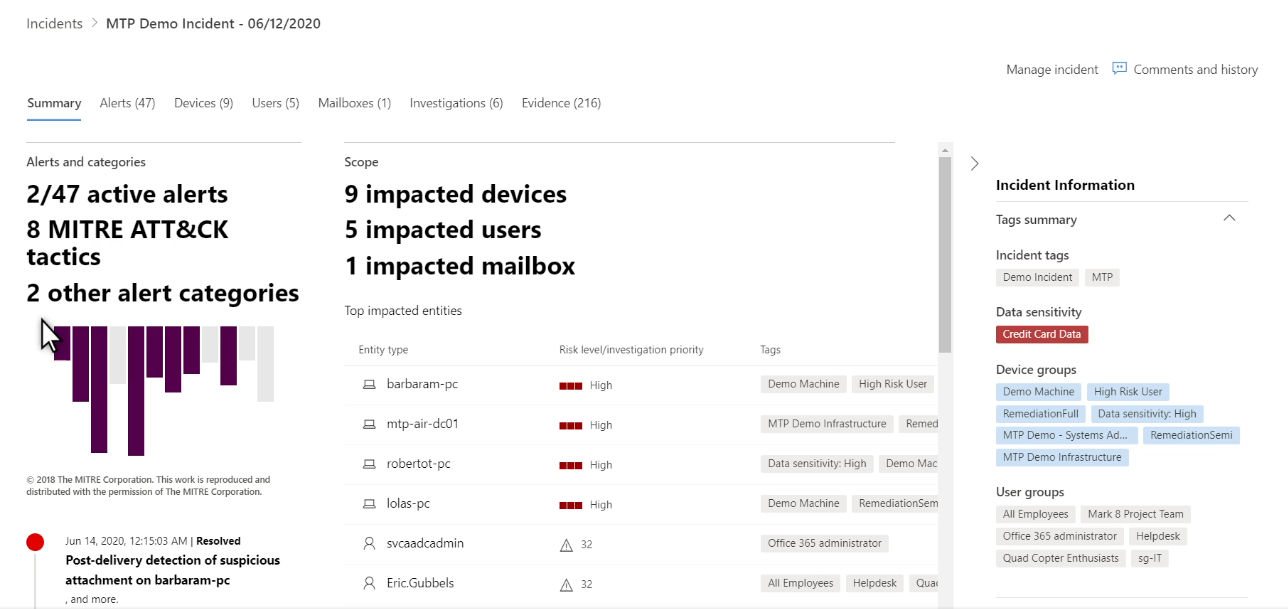
### **Incident Management Using Microsoft Defender XDR**

#### **1. Selecting and Reviewing the Incident**

* Open **Microsoft Defender XDR** and select an incident.

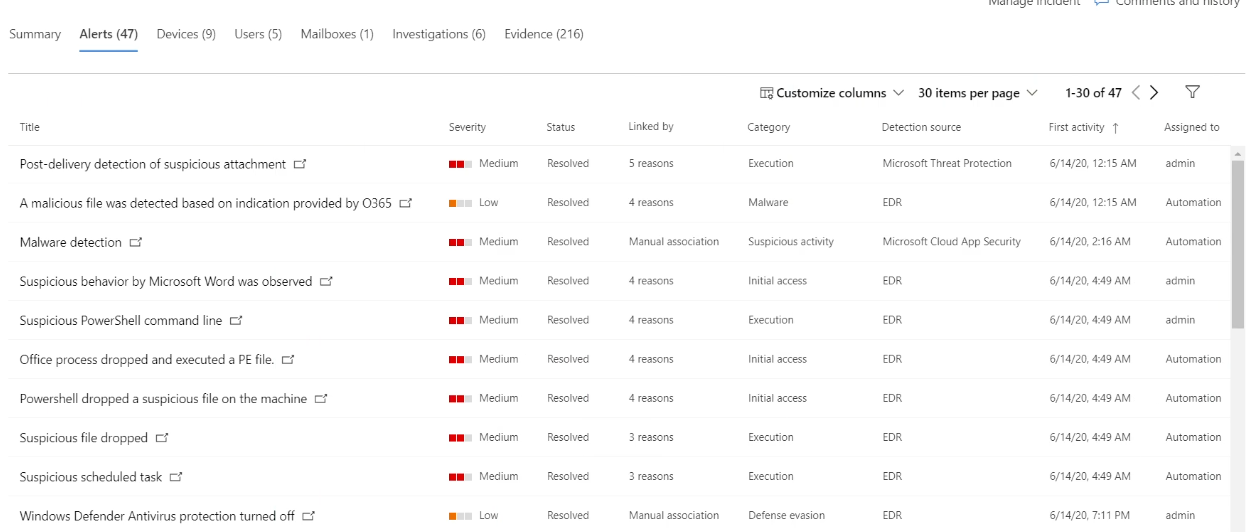


* View the **incident summary** for an overview of the issue.

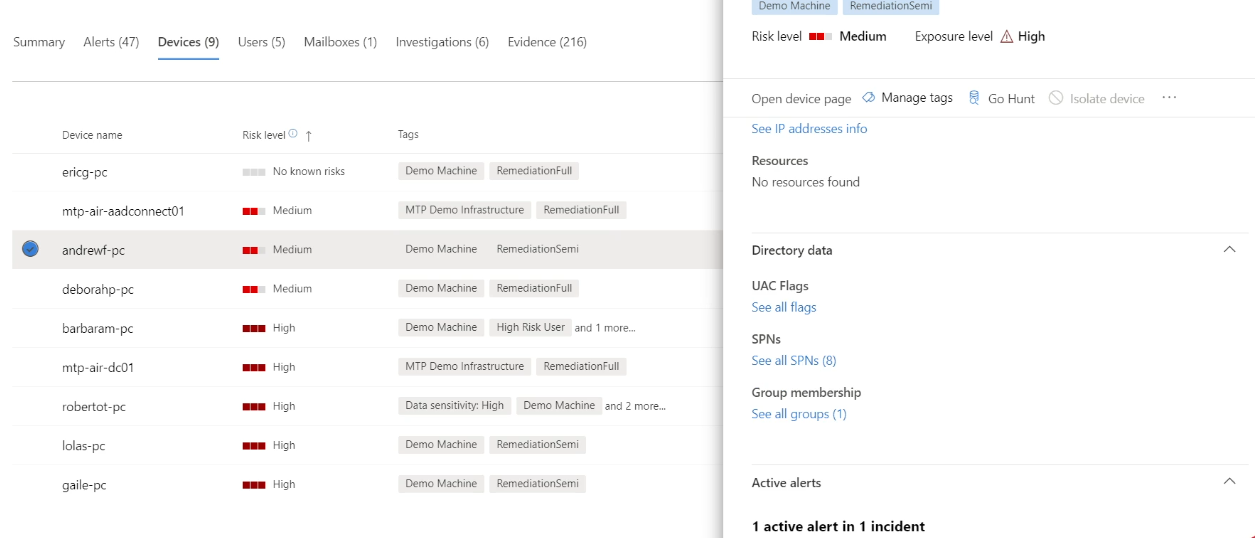


#### **2. Analyzing Incident Details**

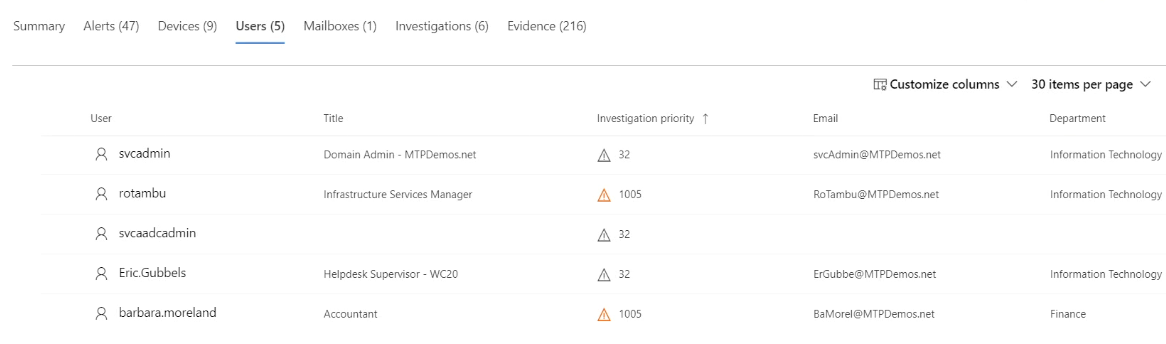
* **Alerts Section:** Displays details about security alerts.



* **Devices Section:** Lists affected devices.



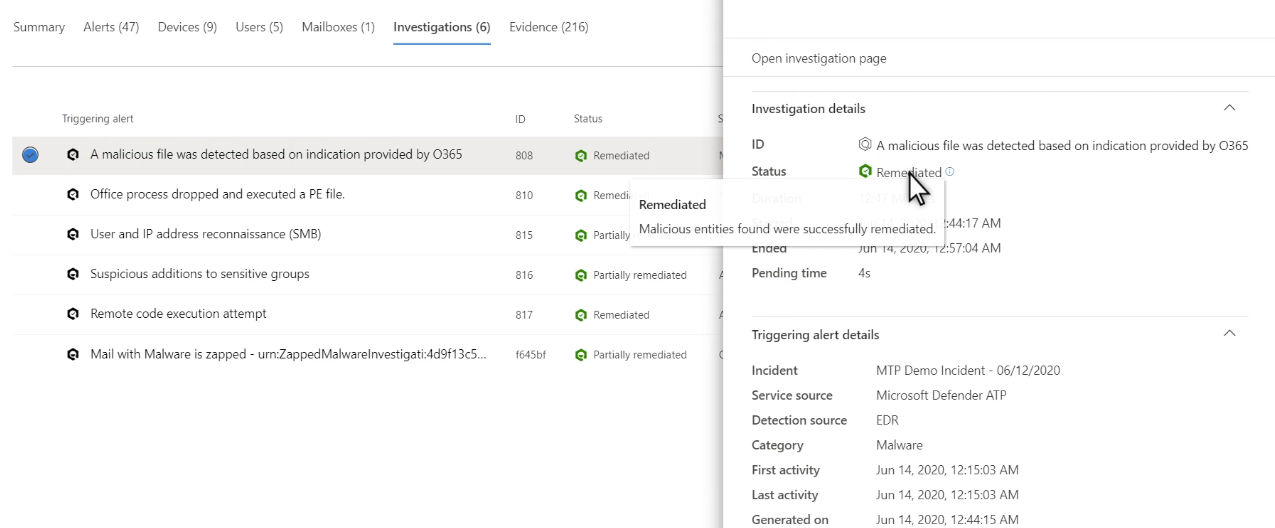
* **Users Section:** Shows impacted user accounts.



* **Mailboxes Section:** Allows further investigation by opening in a browser.

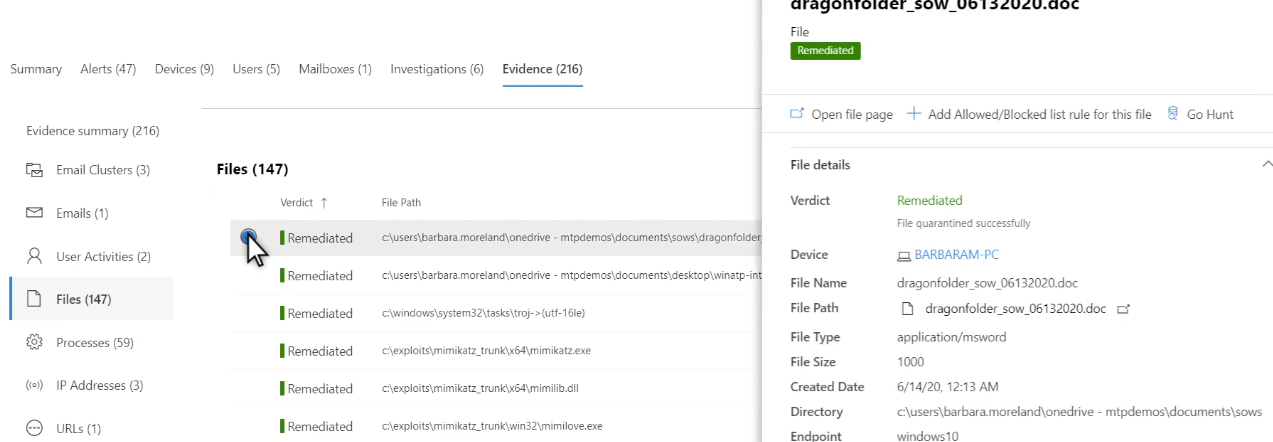


* **Investigations Section:** Provides deep-dive analysis into the incident.



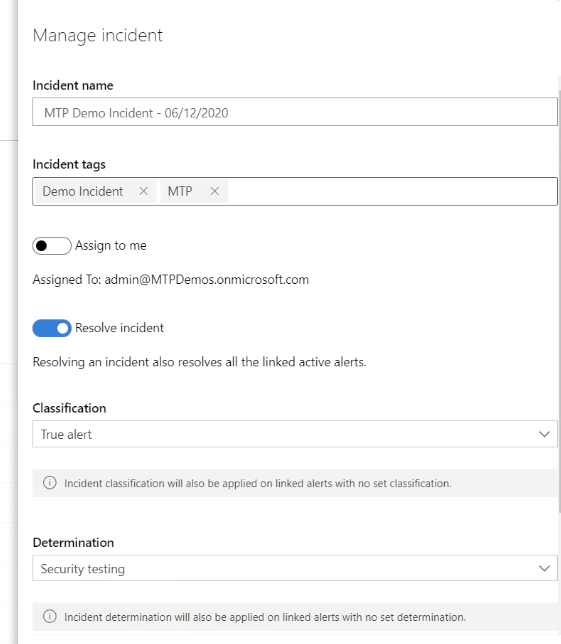
#### **3. Investigating and Remediating**

* Select an alert to **view more details and remediation options**.
* **Evidence Section:** Summarizes findings, allowing file selection for deeper inspection.



* Click **"Go Hunt"** to perform a threat-hunting query.

#### **4. Resolving the Incident**



* Click **"Manage Incident"** to take final actions:  
   ✅ Change **classification** ✅ Update **determination** ✅ Apply other necessary remediation steps

🔹 **Outcome:** Incident is reviewed, analyzed, and resolved effectively.