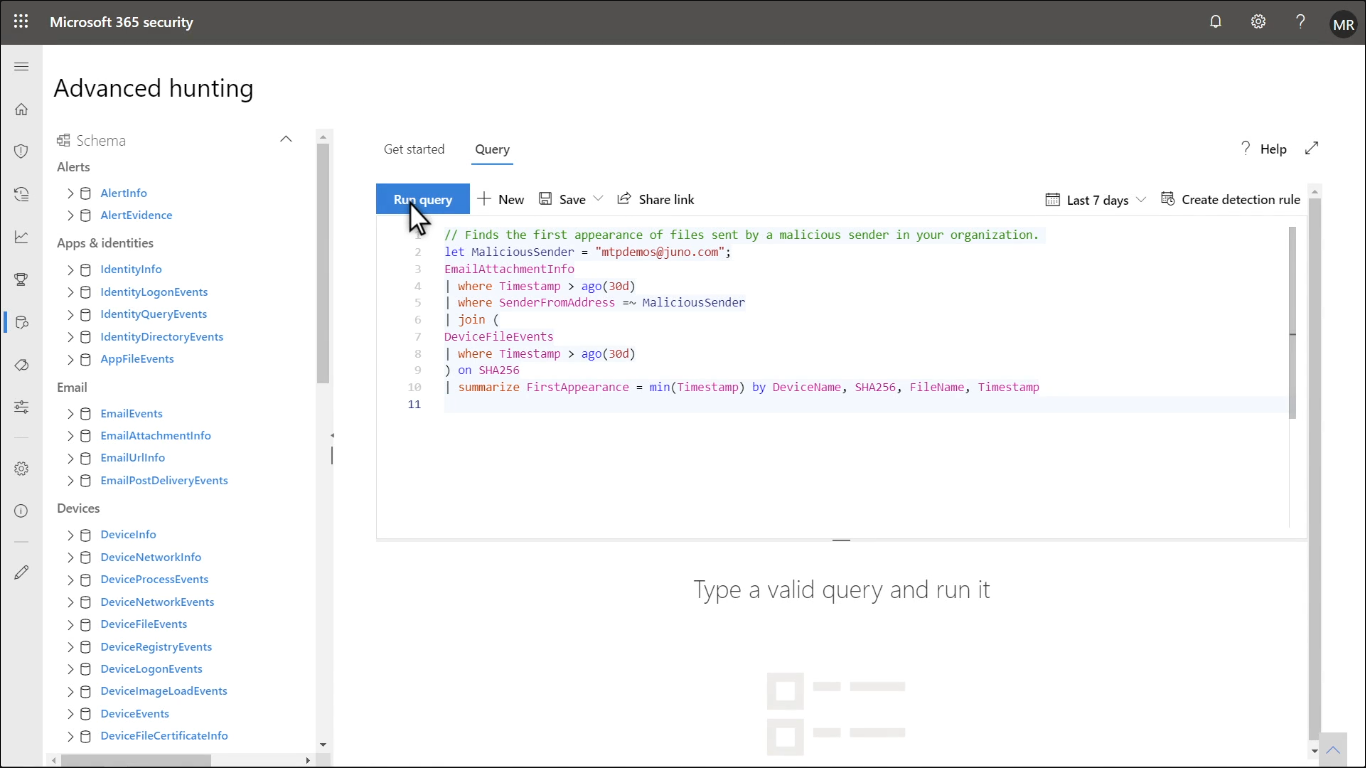
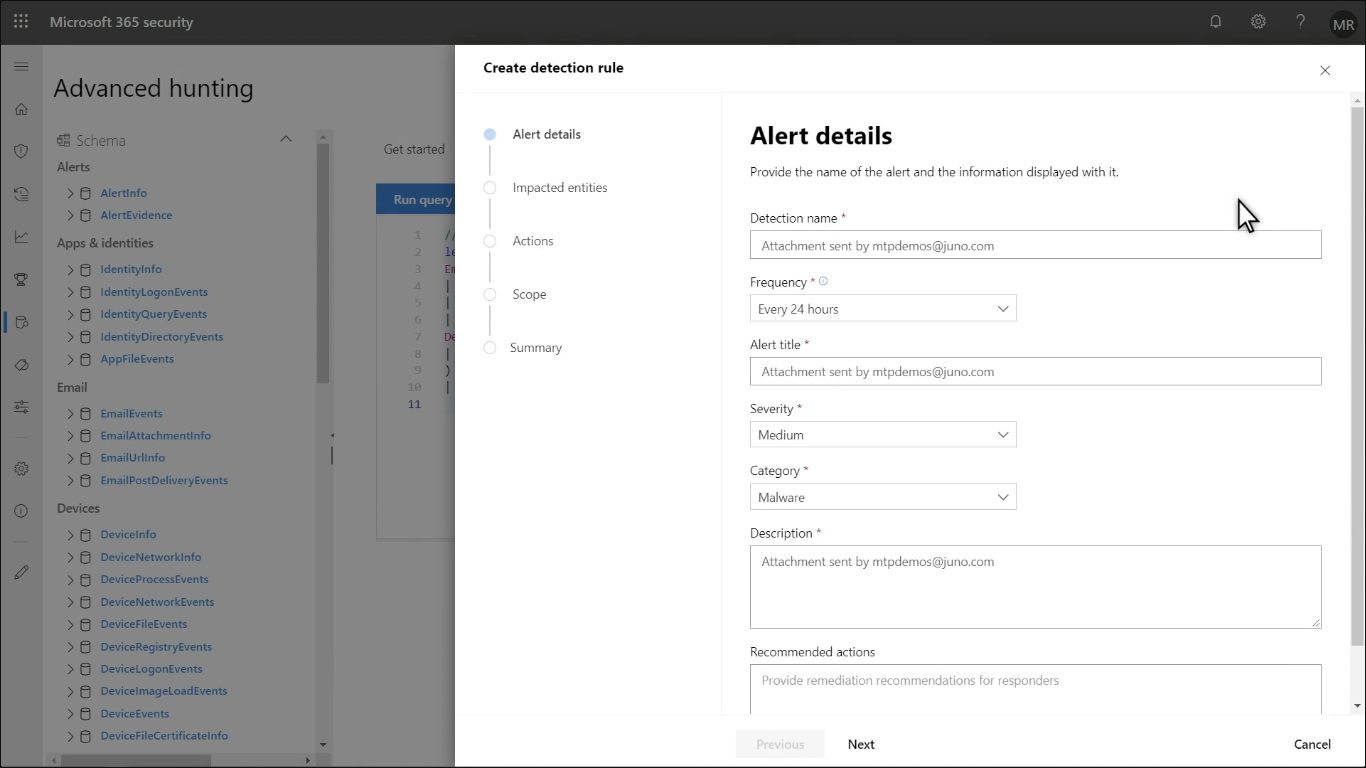
# **Advanced Hunting - Custom Detection Rule Creation**

1. **Run Query in Advanced Hunting**
   * Navigate to Microsoft Defender Security Center → Advanced Hunting.
   * Construct and execute the query to ensure it returns the required columns: Timestamp, DeviceId, ReportId.
   * Example Query:

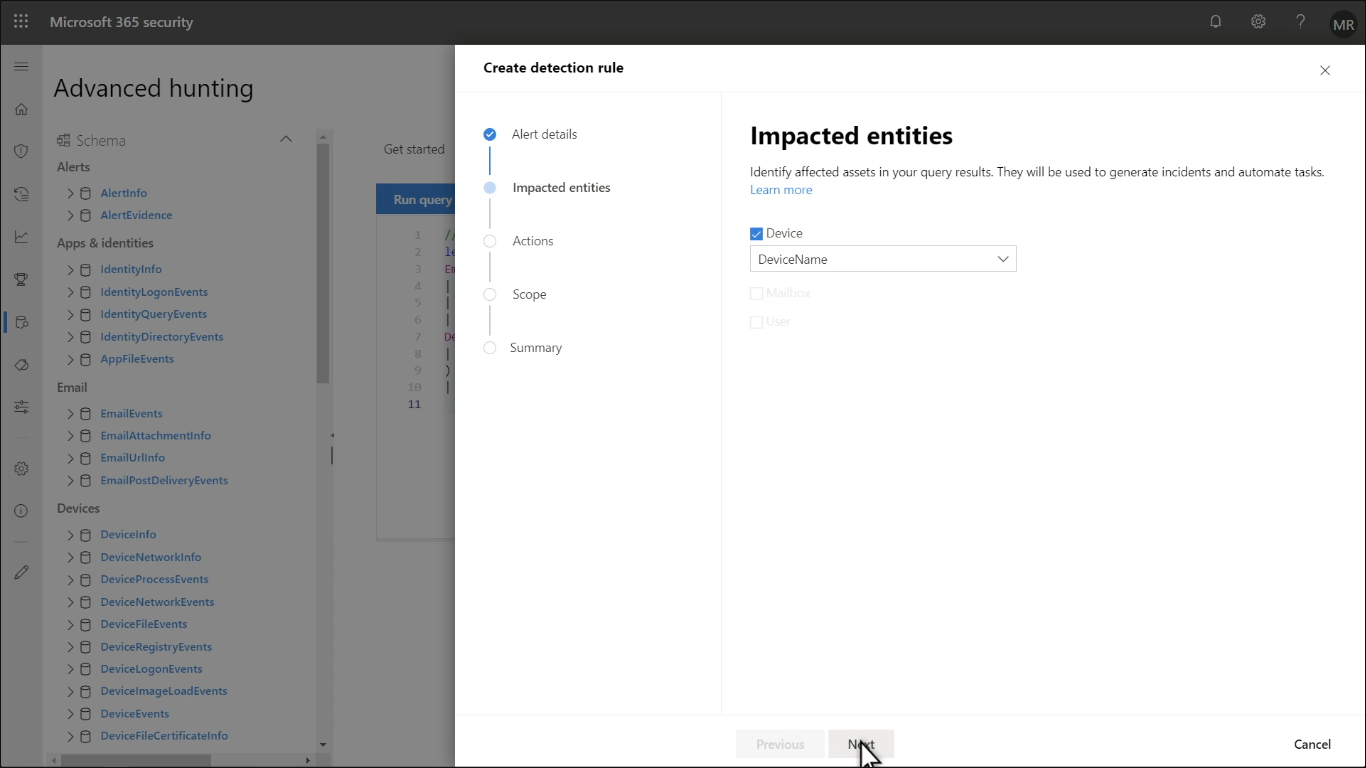


* + Verify that the query results match expectations before proceeding.

1. **Create Detection Rule**
   * Click **Create detection rule** with the query loaded.
   * Provide alert details:
     + **Detection Name**: Meaningful name for identification.
     + **Alert Title**: Clearly describes the detection.
     + **Severity**: Assign severity (Low, Medium, High, Severe).
     + **Category**: Select appropriate threat category.
     + **MITRE ATT&CK Techniques**: Link to known attack techniques if applicable.
     + **Description**: Additional information about the rule.
     + **Recommended Actions**: Steps to take when triggered.

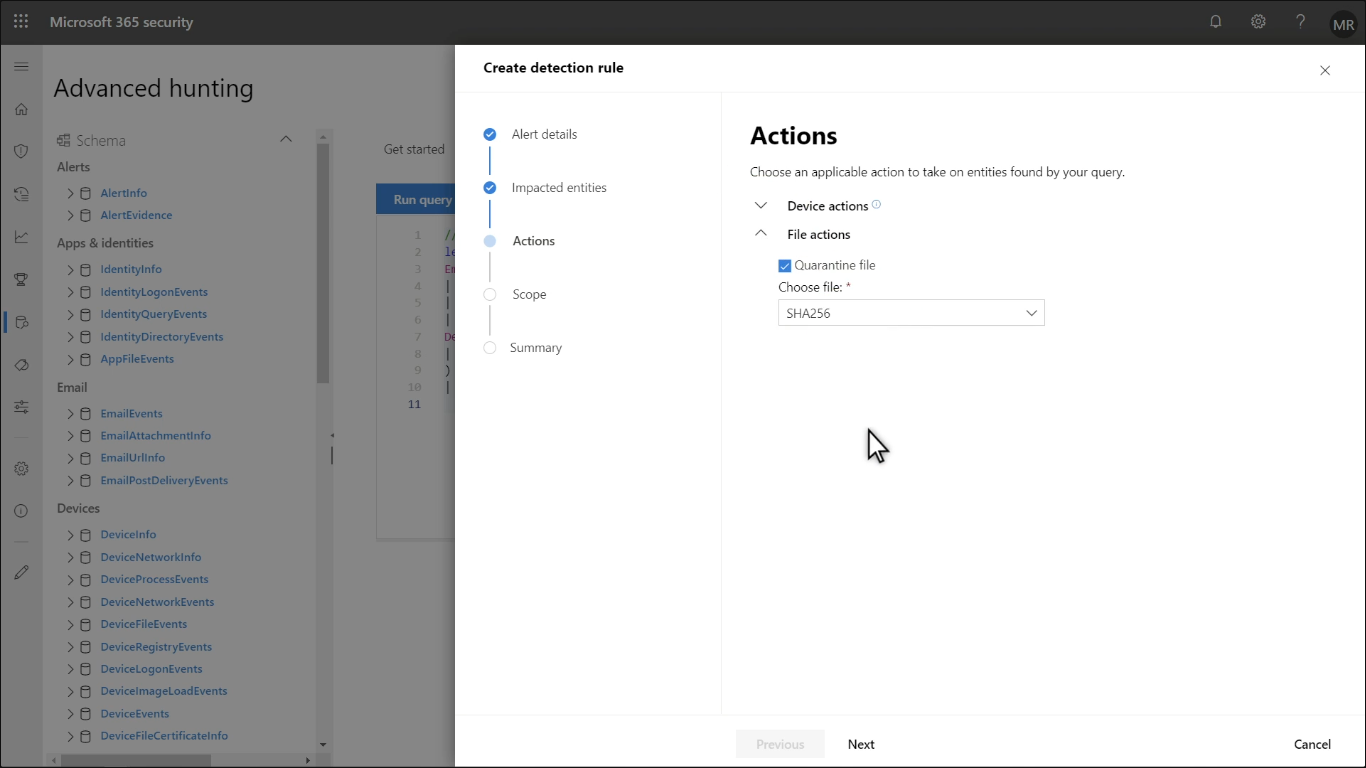


1. **Select Impacted Entities**

****

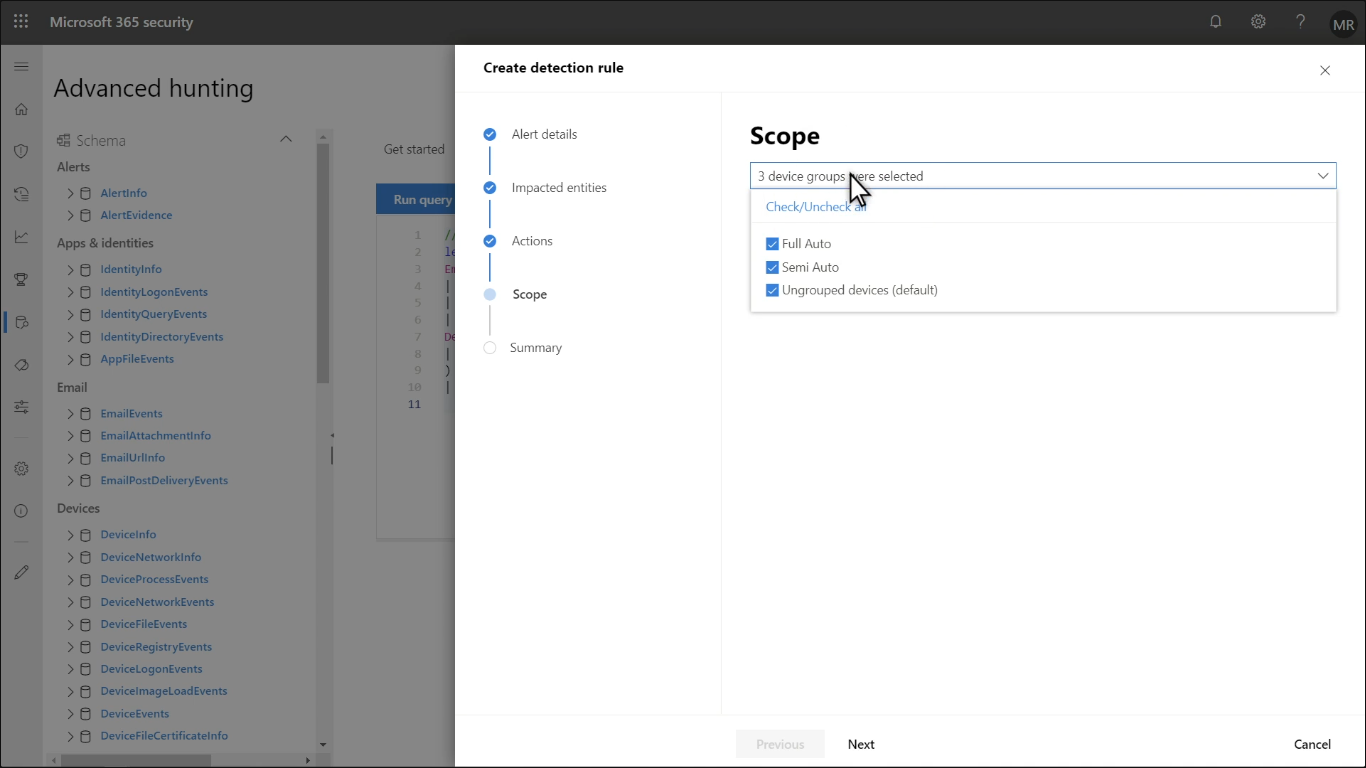
* + Identify which entity type is impacted:
    - **Devices (DeviceId)**
    - **Users (UserId)**
    - Ensuring proper correlation for alerts and incidents.

1. **Define Actions on Detection**
   * Actions on **Devices**:
     + Isolate device (Full network isolation).
     + Collect investigation package.
     + Run antivirus scan.
     + Initiate automated investigation.
   * Actions on **Files**:
     + **Quarantine file** – Removes file and places it in quarantine.



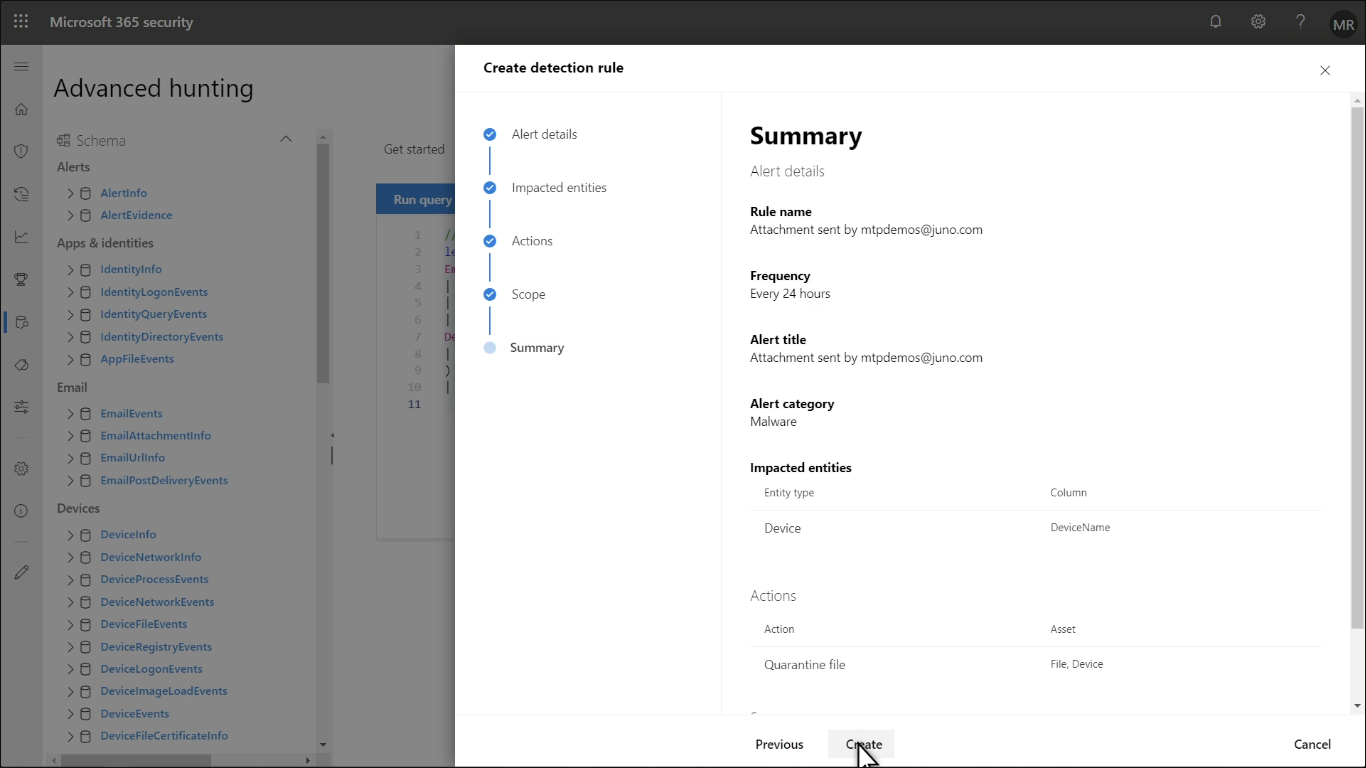
* + - **Allow/Block file** – Adds to custom indicator list.

1. **Set Rule Scope**

****

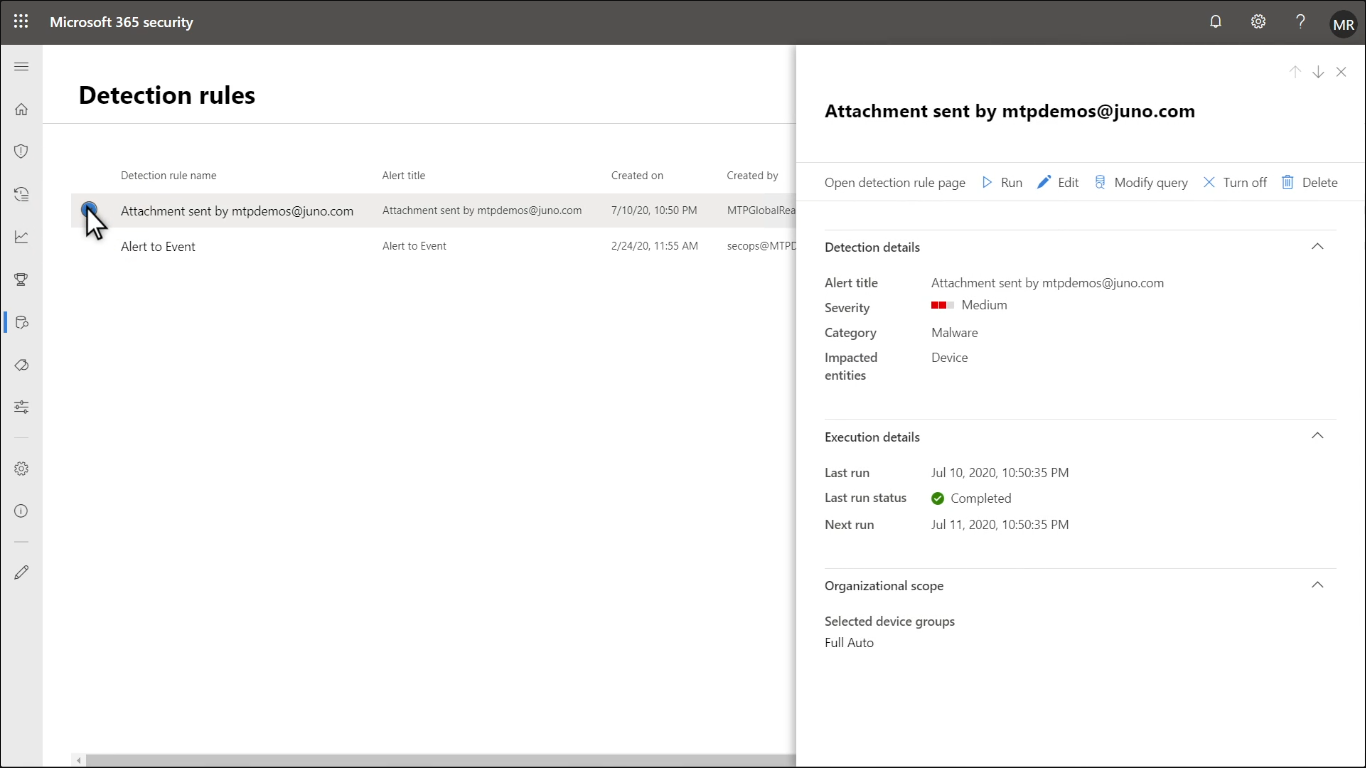
* + Choose which devices the rule applies to:
    - **Full auto** – Automatically enforces actions.
    - **Semi auto** – Requires manual confirmation for enforcement.
    - **Ungrouped devices (default)** – Applies to all devices by default.

1. **Review and Create Rule**

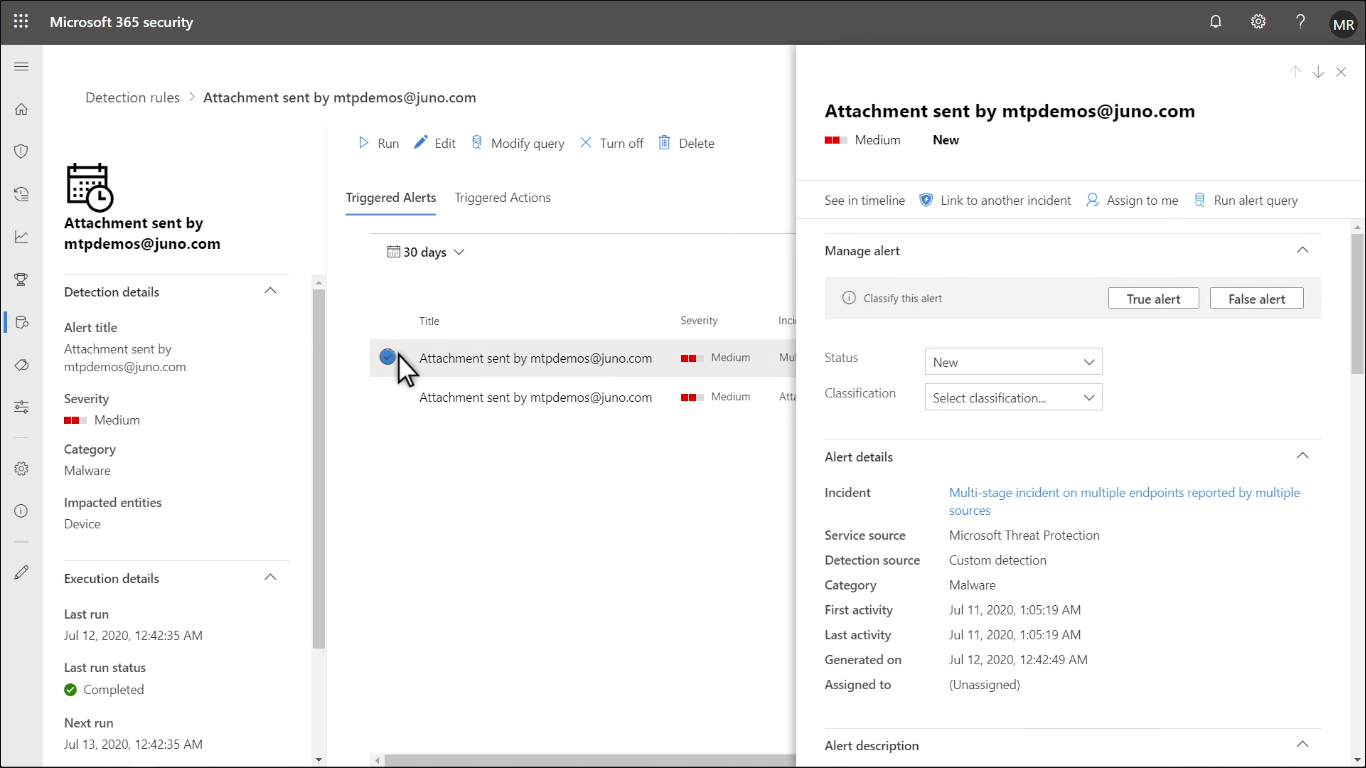


* + Check the summary and ensure all configurations are correct.
  + Click **Create** to activate the detection rule.

1. **Monitor and Investigate Alerts**
   * Navigate to **Detection Rules** and find the newly created rule.

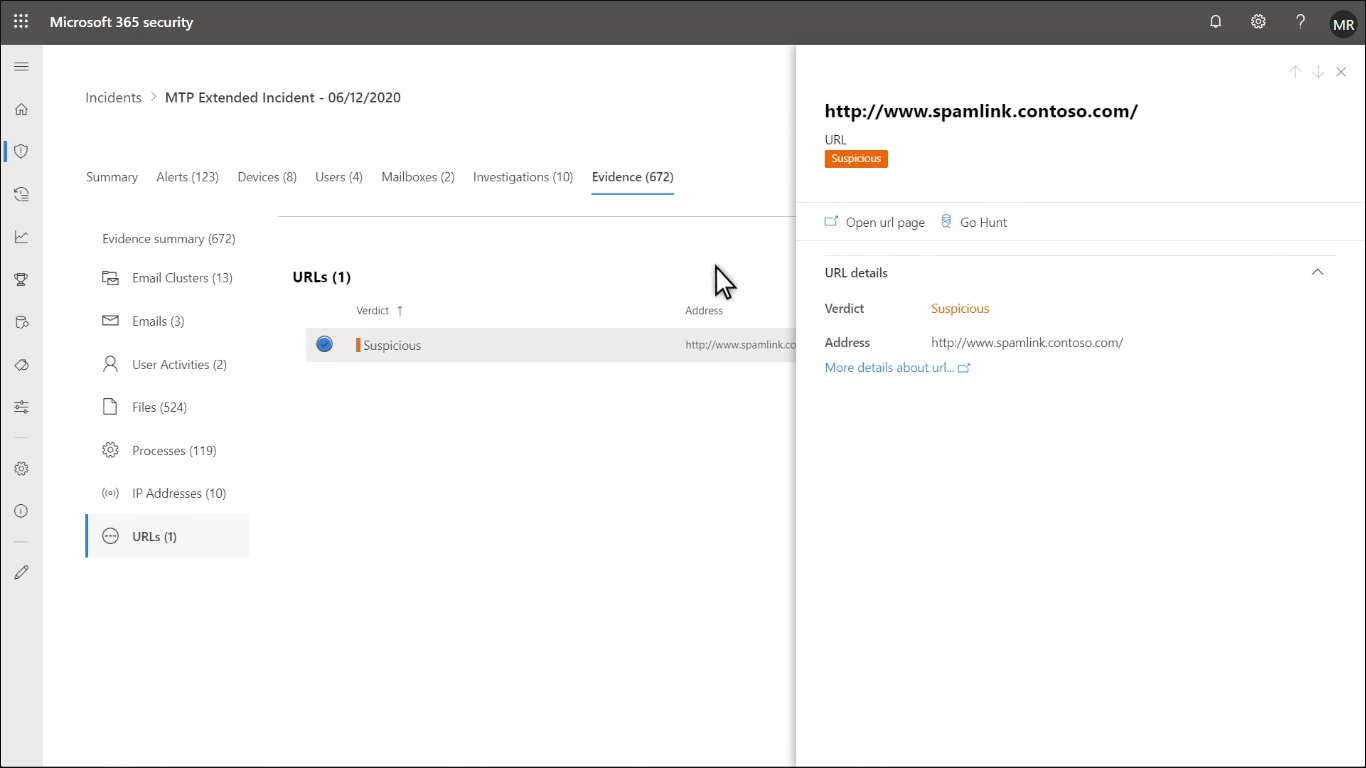


* + Continue monitoring as per security policies.



* + Any triggered detection should be investigated and marked appropriately.

1. **Mark Suspicious Evidence**
   * In the evidence section, flag items as suspicious.



* + Example: Mark spamlink.cortoso.com as suspicious and track for future occurrences.