EICAR Malware Testing and Analysis in Elastic on Windows

This document provides a detailed guide for testing malware detection using the EICAR test file on a Windows machine and analyzing the results in Elastic (Kibana). The process includes downloading the EICAR file, executing it, and reviewing the detection events in Kibana to ensure proper security monitoring.

Downloading the EICAR Test File from Microsoft Edge

Testing Steps:

I. Open Microsoft Edge on your Windows machine.

II. In the search bar, type "palo alto eicar" and press Enter to search.

III. Identify and open the first result that mentions testing a sample malware file (likely titled "Test a Sample Malware File").

IV. On the webpage, locate and click the option to download the PE (Portable Executable) EICAR test file, which will be an .exe file.

V. If Microsoft Edge displays a warning such as "Malware detected" or "Virus detected" and blocks the download, or if the browser's smart protection refuses the file, select the "Keep" option to proceed with the download.

The EICAR test file will be successfully downloaded as an .exe file to your Downloads folder, despite any browser warnings.

Executing the EICAR Test File on Windows

Testing Steps:

I. Navigate to your Downloads folder on the Windows machine.

II. Locate the downloaded EICAR .exe file (e.g., eicar.com).

III. Double-click the file to execute it.

IV. Observe the terminal window that opens briefly and then closes automatically.

V. Note any antivirus alerts (e.g., from Windows Defender) that may detect the file as a virus during execution.

What it will: The EICAR test file will execute, briefly displaying a terminal window that closes itself, and may trigger an antivirus alert identifying it as a virus.

Add Screenshot Here: Insert the screenshot from page 2 of images.pdf, showing the context of the EICAR execution (adjust if you have a terminal screenshot).

Reviewing Malware Alerts in Kibana Security Section

Testing Steps:

I. Open Microsoft Edge and navigate to your Elastic (Kibana) instance (e.g., http://localhost:5601).

II. Log in using your credentials to access the Kibana dashboard.

III. On the left sidebar, scroll down to the "Security" section and click "Alerts."

IV. Look for new alerts related to the EICAR test file execution, which should indicate a malware detection event. The Alerts page in Kibana will display a new alert entry for the EICAR test file, confirming that the Elastic Security module detected the malware execution.

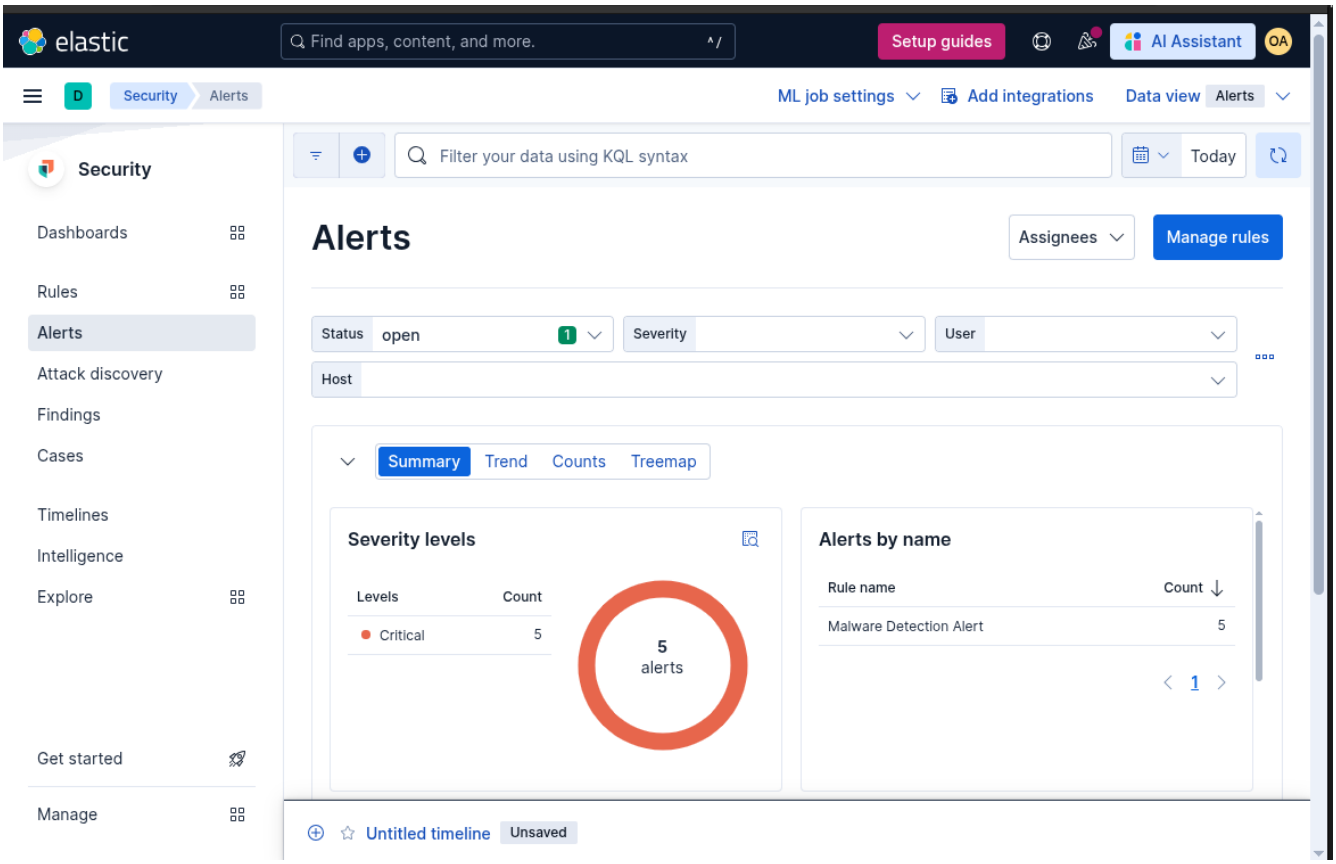

Figure 1.1 :Alerts page in Kibana with the EICAR detection.

Analyzing Alert Timestamp and Event Details in Kibana

Testing Steps:

I. On the Alerts page in Kibana, scroll down to the section where timestamps are displayed for the EICAR alert.

II. Click on the alert to view the full details of the event, including the timestamp, source, and detection information.

III. Analyze the event details to understand the malware behavior, such as the process that triggered the alert.

The alert details will display the exact timestamp of the EICAR detection (e.g., around 02:29 AM EAT on May 29, 2025), along with specific event details like the process name and detection rule.

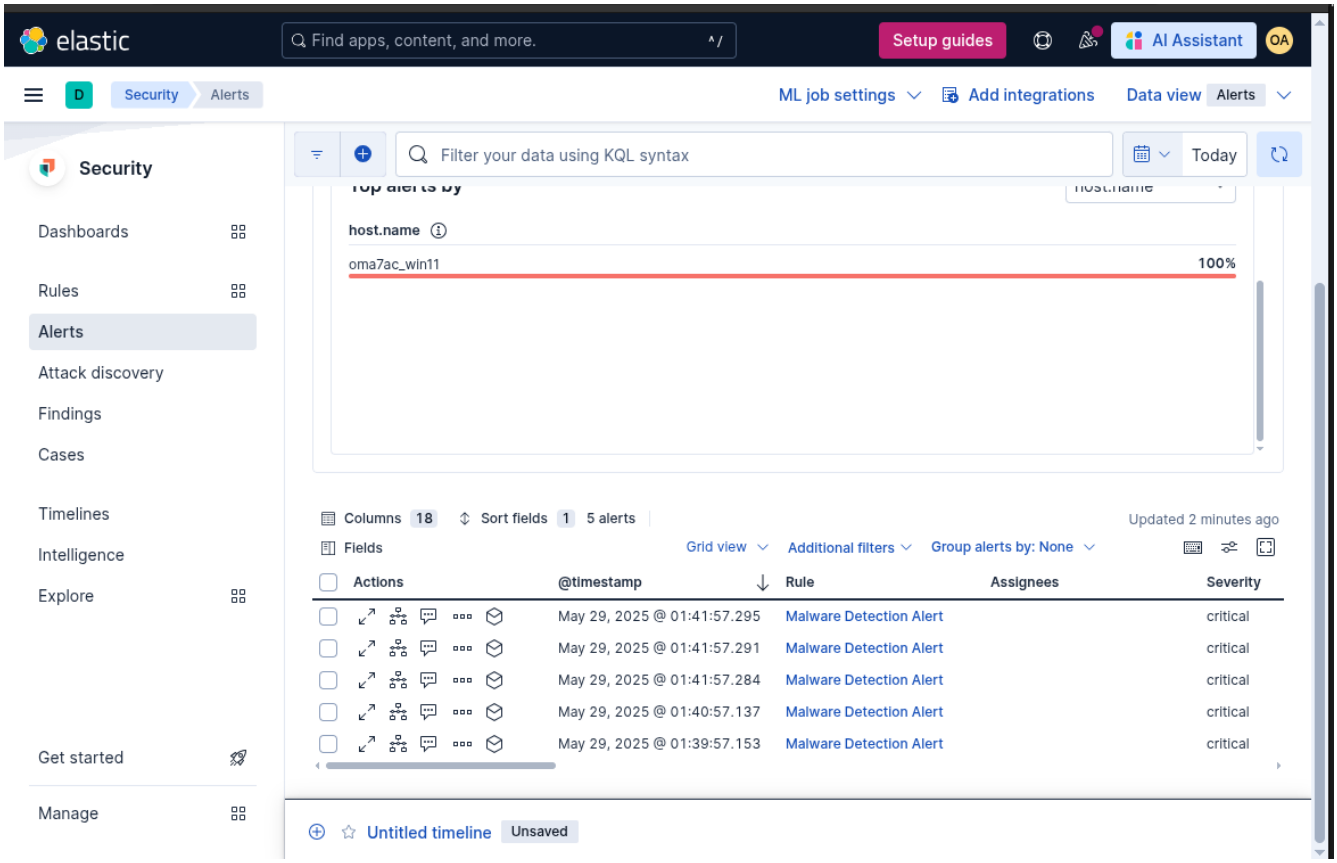

Figure 1.2: showing the alert details with the timestamp in Kibana.

Searching for EICAR-Related Processes in Kibana Discover

Testing Steps:

I. Return to the left sidebar in Kibana and click "Discover."

II. In the search bar, apply the filter process.name: "wild" to search for processes related to the EICAR execution.

III. In the field list on the left, locate and select the field event.dataset: endpoint.events.process to filter events specifically for process-related data.

IV. Review the results to identify the processes involved in the EICAR execution.

The Discover page will display process events matching the wild process name, filtered by endpoint.events.process, revealing the processes triggered by the EICAR file.

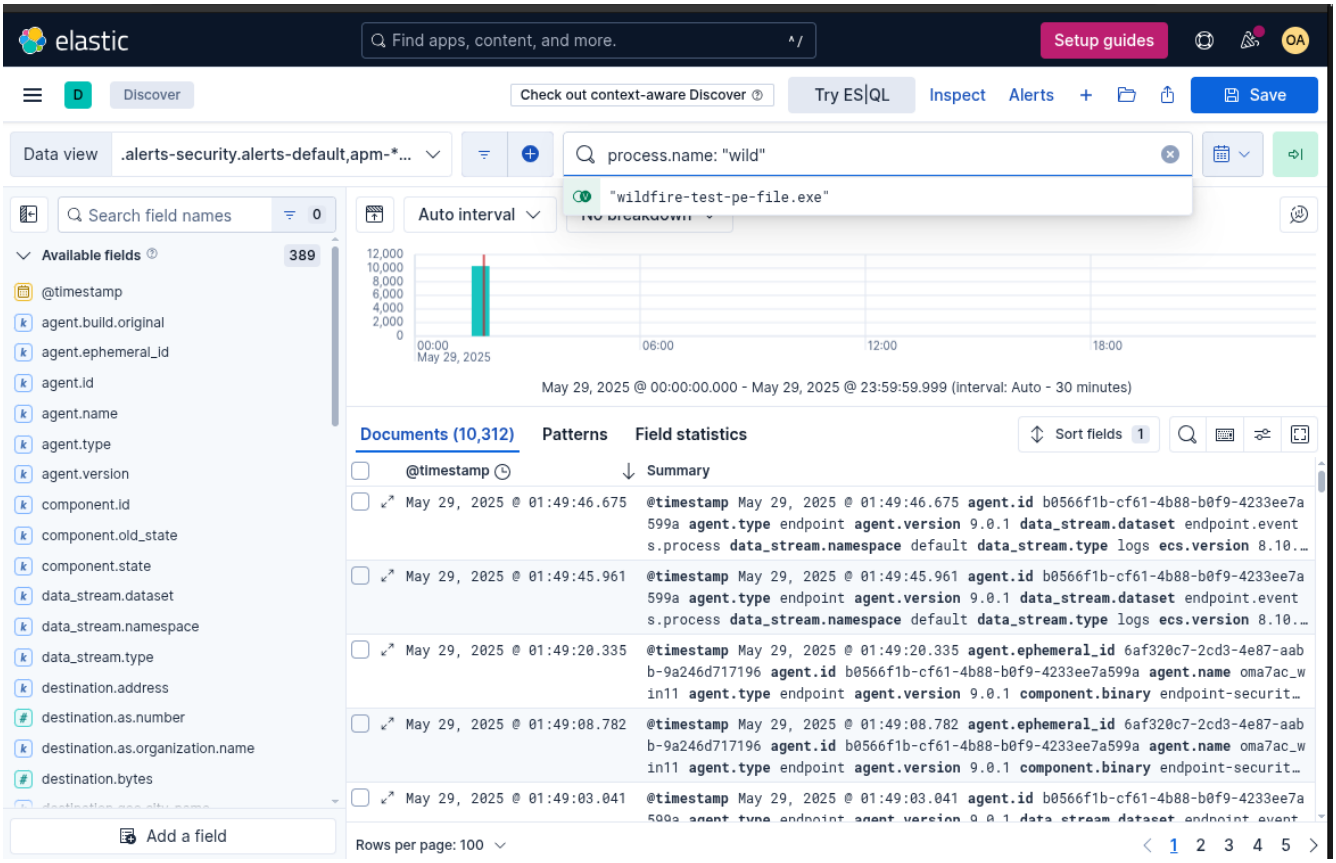

Figure 1.3: iscover page with process search results in Kibana.