EventTracker

Actionable Security Intelligence

Identifying dormant executable files in the network

EventTracker Enterprise

Publication Date: June 7, 2017

Abstract

The update is designed to display the executed and non-executed files in the Unknown process dashboard.

Who should read this document?

Customers who use v8.2 Build 14

Why to apply the Update?

This Update will support the user(s) for identifying the unknown executable and non-executable files in the network based on the last Change Audit snapshot taken.

Process to be followed after applying the update

After applying the update, the user(s) will get an option "**Show**" in the Unknown Process Dashboard.

- Login to **EventTracker web** and navigate to **Dashboard->Threats->Unknown Processes**.

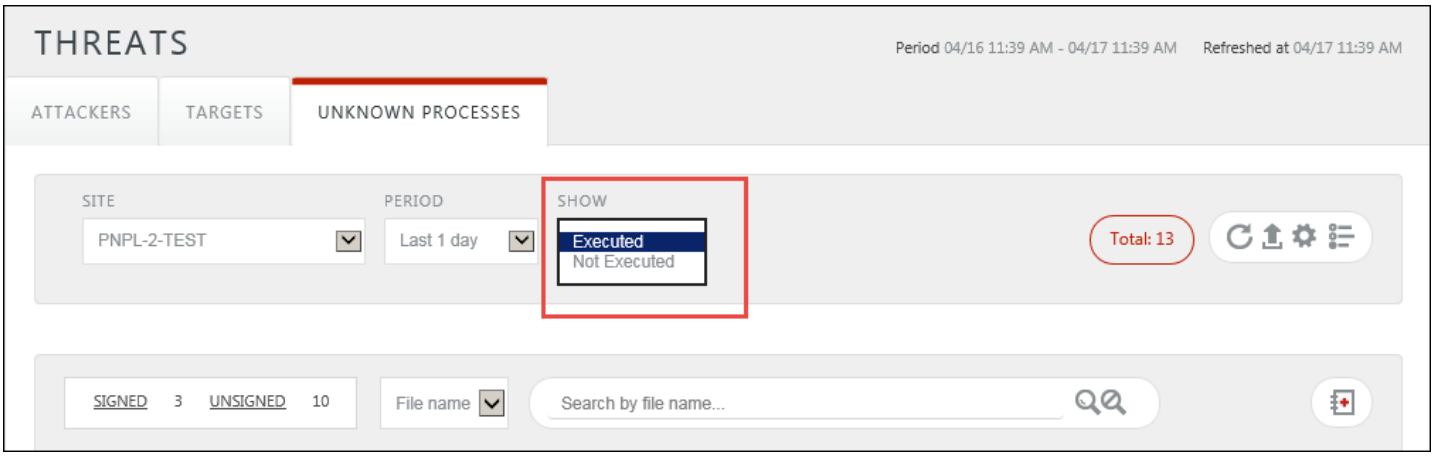

Figure 1

- The "**Show**" option is available with dropdown selections as **Executed** and **Not Executed**.

For the executed option selected, it will display all the files which were executed on remote agent.

An example for executed files is shown below:

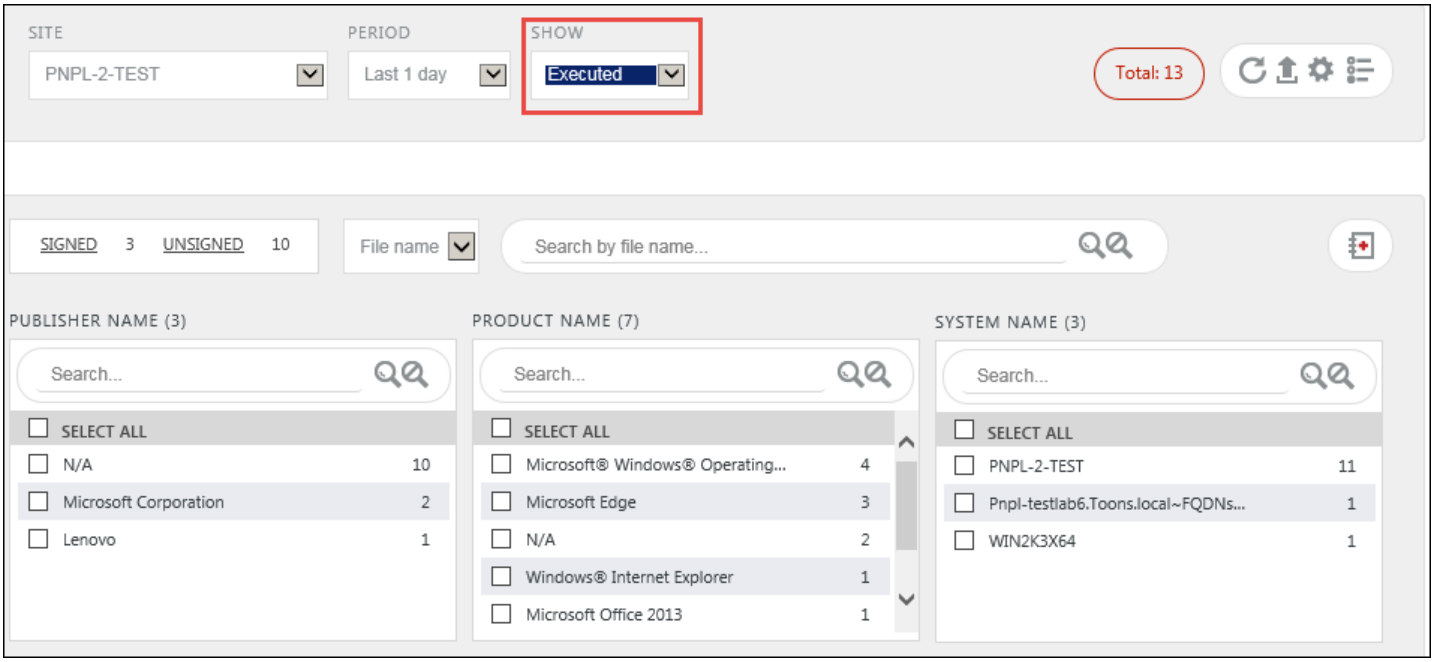

Figure 2

The files which were not executed within the enterprise will be displayed under the **not-executed** option based on the previous and last snapshot comparison taken by Change Audit.

NOTE: It will consider the Event Id 3400 (File added) and 3401 (File Modified) for displaying the not executed files in the Unknown processes not executed dashboard.

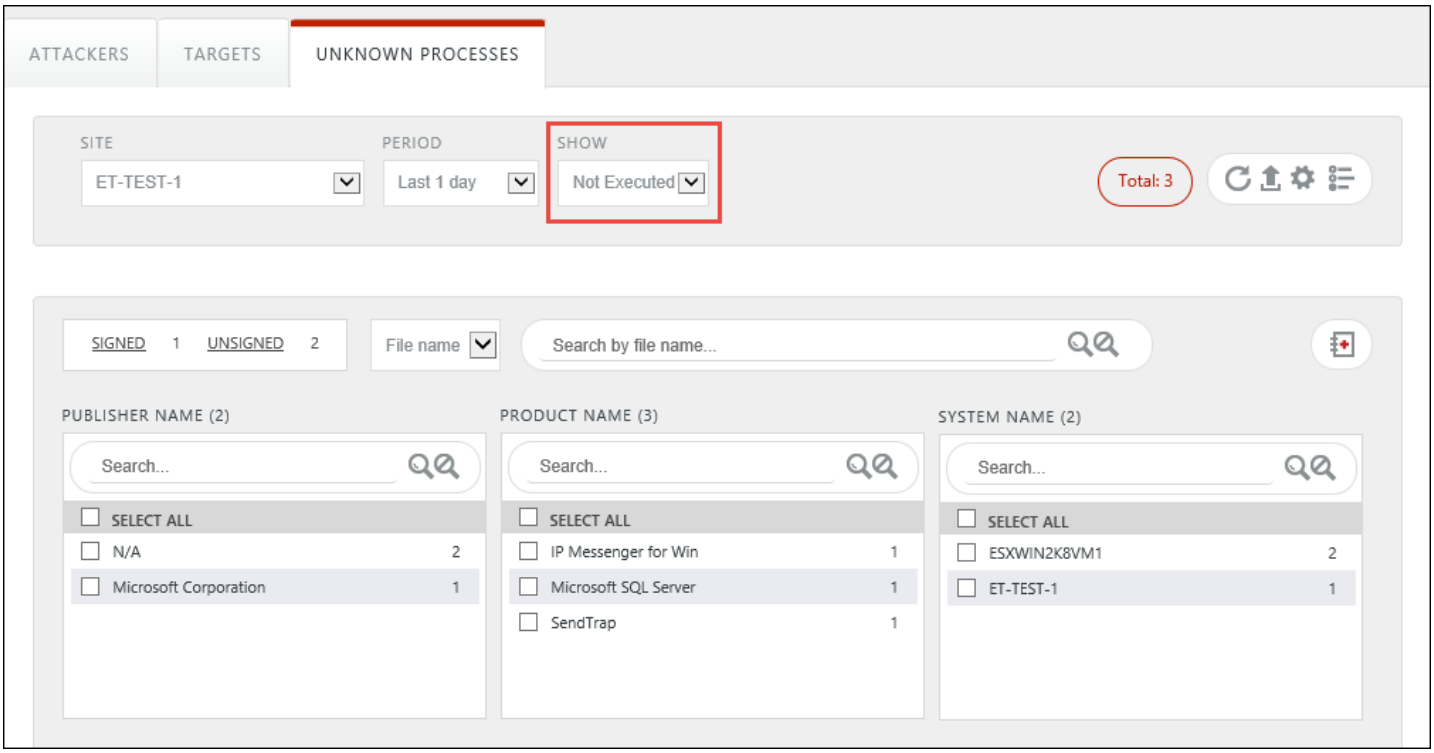

Figure 3

- The user(s) can export the result in excel by clicking the Export icon and can add unknown process filters by clicking the icon .

NOTE: The Unknown Process filter will now have 9 default filter rules. The user(s) can select from the default rules, if required.

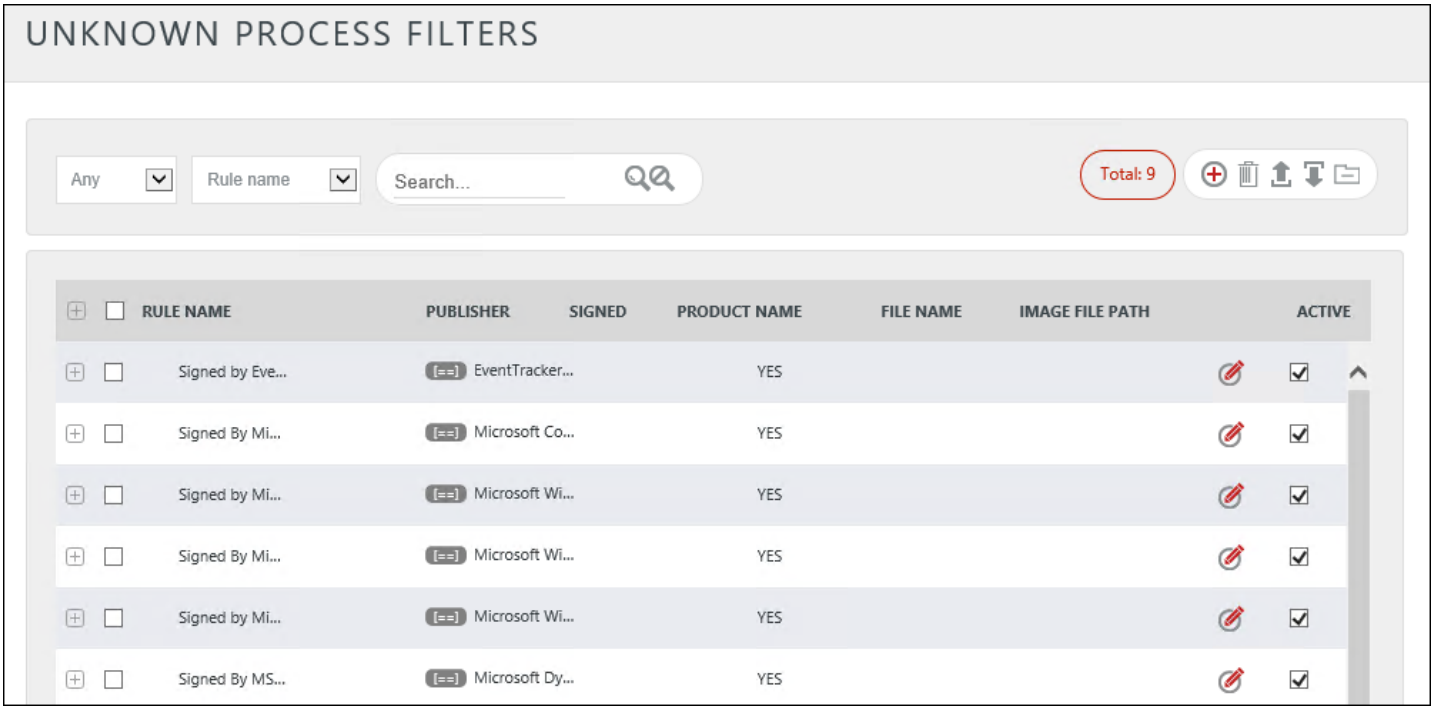

Figure 4

- The User(s) can also add the executable/not-executable files to the safe/unsafe list by clicking the respective icons and .

Limitations:

- The Unknown Process dashboard not executed option requires the Change Audit feature.
- It is mandatory to apply all the change audit updates as this feature is based on change audit.
- This feature is available for 8.2 and 8.3 agents. To utilize the feature for lower version agent machines, change audit agents should be upgraded to 8.2 or 8.3.
- If only change audit agent is deployed in a machine, then the user should enable the option to "**send directly to EventTracker as Trap**" to send the change audit events to manager. This option is available under the system configuration.