

# Identifying dormant executable files in the network

## EventTracker Enterprise

## 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.

*The information contained in this document represents the current view of EventTracker. on the issues discussed as of the date of publication. Because EventTracker must respond to changing market conditions, it should not be interpreted to be a commitment on the part of EventTracker, and EventTracker cannot guarantee the accuracy of any information presented after the date of publication.*

*This document is for informational purposes only. EventTracker MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.*

*Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.*

*EventTracker may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from EventTracker, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.*

*The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.*

*© 2017 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

## 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**.

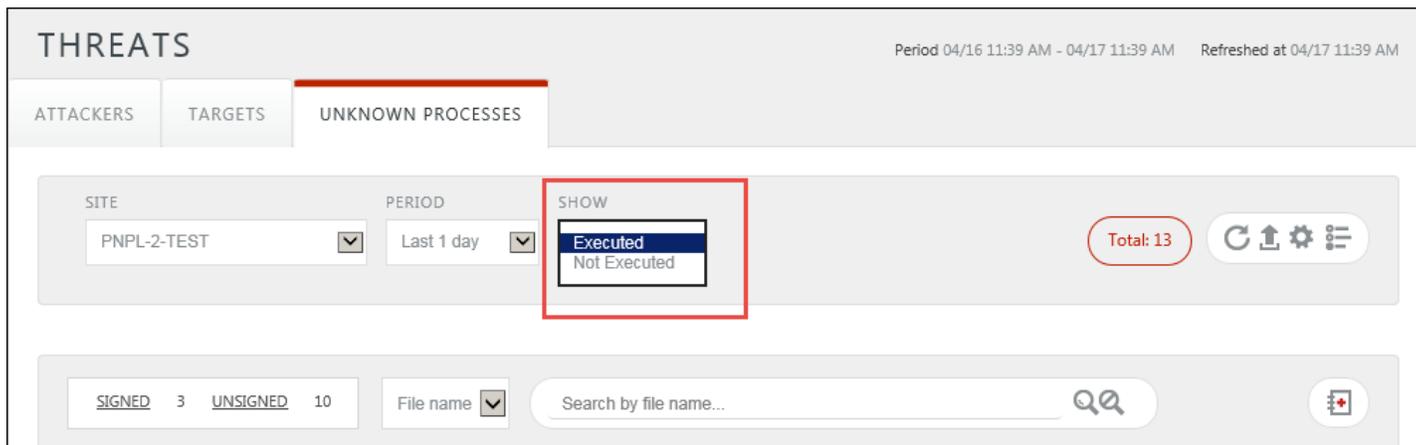


Figure 1

- 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:

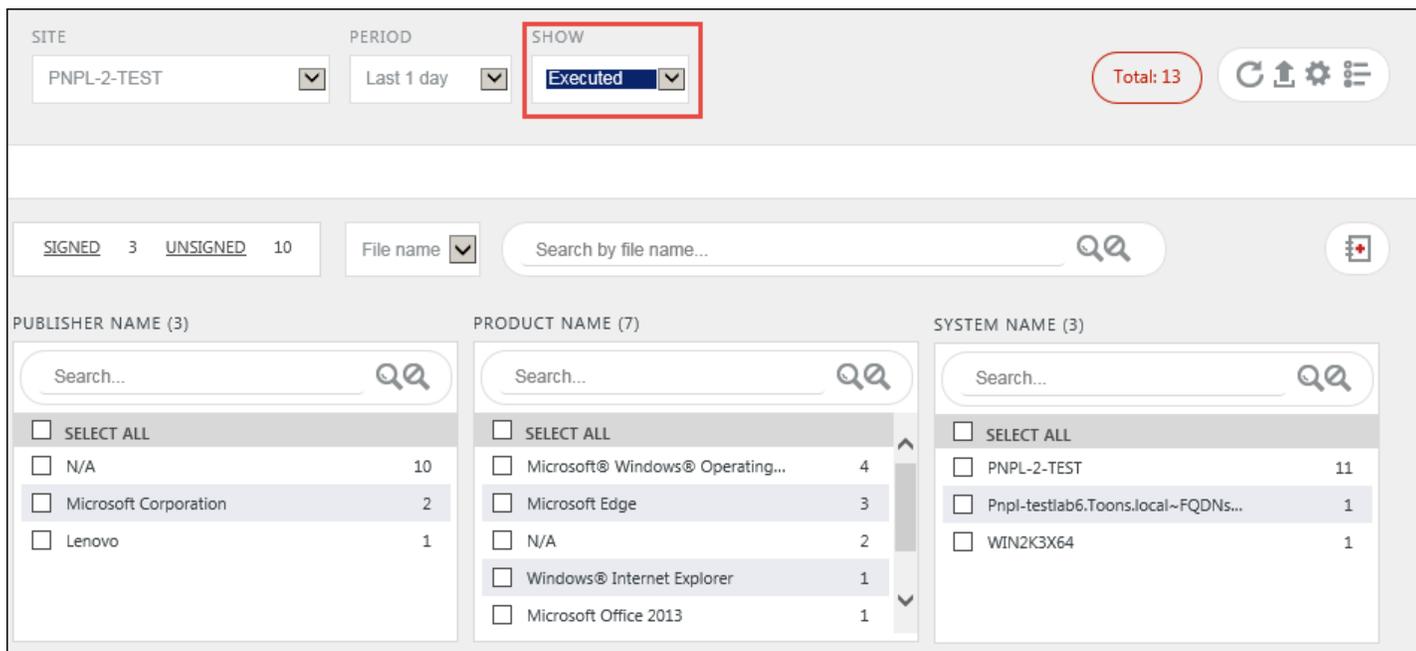


Figure 2

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.

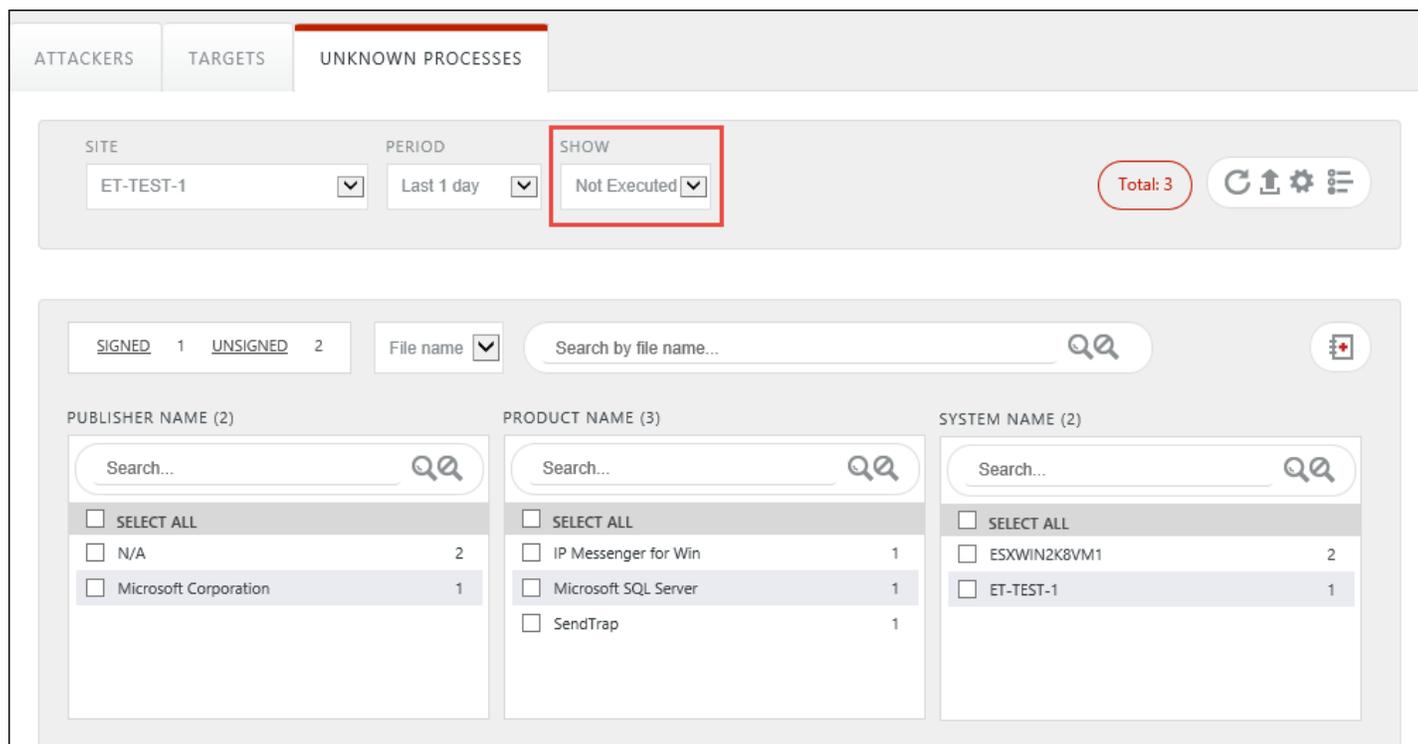


Figure 3

- 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.

UNKNOWN PROCESS FILTERS

Any  Rule name  Search...  Total: 9    

<input type="checkbox"/>	RULE NAME	PUBLISHER	SIGNED	PRODUCT NAME	FILE NAME	IMAGE FILE PATH	ACTIVE
<input type="checkbox"/>	Signed by Eve...	[==] EventTracker...		YES			 <input checked="" type="checkbox"/>
<input type="checkbox"/>	Signed By Mi...	[==] Microsoft Co...		YES			 <input checked="" type="checkbox"/>
<input type="checkbox"/>	Signed by Mi...	[==] Microsoft Wi...		YES			 <input checked="" type="checkbox"/>
<input type="checkbox"/>	Signed By Mi...	[==] Microsoft Wi...		YES			 <input checked="" type="checkbox"/>
<input type="checkbox"/>	Signed by Mi...	[==] Microsoft Wi...		YES			 <input checked="" type="checkbox"/>
<input type="checkbox"/>	Signed By MS...	[==] Microsoft Dy...		YES			 <input checked="" type="checkbox"/>

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.