Integrate Kaspersky Security Center
EventTracker v9.0 and above

Publication Date: December 5, 2019
Abstract

This guide will facilitate a Kaspersky Security Center user to send logs to EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker 9.x or later and Kaspersky Security Center 10 and later.

Audience

Administrators who want to monitor the Kaspersky Security Center using EventTracker.

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

This document is for informational purposes only. Netsurion 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 Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion 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 Netsurion, 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.

© 2019 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
# Table of Contents

1. Introduction .......................................................................................................................... 3  
   1.1 Pre-requisites ................................................................................................................. 3  
   1.2 Enabling Kaspersky Event Logs and Send logs to EventTracker ................................ 3  
2. EventTracker Knowledge Pack ............................................................................................ 5  
   2.1 Categories ...................................................................................................................... 6  
   2.2 Alerts ............................................................................................................................... 6  
   2.3 Report .............................................................................................................................. 7  
   2.4 Dashboards ..................................................................................................................... 10  
3. Importing knowledge pack into EventTracker ................................................................. 15  
   3.1 Categories ...................................................................................................................... 16  
   3.2 Alerts ............................................................................................................................... 17  
   3.3 Parsing Rule ................................................................................................................... 18  
   3.4 Flex Reports .................................................................................................................. 19  
   3.5 Knowledge Objects ....................................................................................................... 21  
   3.6 Dashboards ..................................................................................................................... 22  
4. Verifying knowledge pack in EventTracker ...................................................................... 23  
   4.1 Categories ...................................................................................................................... 23  
   4.2 Alerts ............................................................................................................................... 24  
   4.3 Parsing Rules ................................................................................................................ 25  
   4.4 Flex Reports .................................................................................................................. 25  
   4.5 Knowledge Objects ....................................................................................................... 25  
   4.6 Dashboards ..................................................................................................................... 26
1. Introduction

Kaspersky Security Center offers consumer security products, such as anti-virus, anti-malware and firewall applications. Besides, to the security systems designed for small businesses, corporations, and large enterprises.

Kaspersky Security Center can be integrated with EventTracker via syslog. EventTracker can fetch the device management, object management, virus detected, vulnerabilities detected events on endpoints.

Dashboards provide a view of unmanaged endpoints, inactive endpoints and threat detected on the endpoint.

By using a detailed report, we can understand which endpoint is infected by malware, endpoints which are inactive for more than seven days and provide information about the unmanaged endpoint in the environment. Alerts are triggered whenever malware is detected, device blocked on endpoints, etc.

1.1 Pre-requisites

- **EventTracker 9.x or later** should be installed.
- **EventTracker Agent** to be installed on Kaspersky Security Center administrative server.
- **Advance licensed Kaspersky** is required to forward the syslog.

1.2 Enabling Kaspersky Event Logs and Send logs to EventTracker

1. Open Kaspersky Security Center 10 and Go to **Administration Server**.

![Figure 1](image-url)
2. In Admin Administration Server, select Events in the right frame.
3. Click on Configure notifications and event export.

![Figure 2](image1.png)

4. Select Configure export to the SIEM system.

![Figure 3](image2.png)

5. Select the checkbox Automatically export events to the SIEM system database.
6. Choose the **SIEM** system. Specify the EventTracker Manager address.
7. Click **OK**.

**2. EventTracker Knowledge Pack**

Once Kaspersky Security Center events are enabled and Kaspersky Security Center events are received in EventTracker, Alerts, and Reports can be configured in EventTracker.
The following Knowledge Packs are available in EventTracker to support the Kaspersky Security Center monitoring.

2.1 Categories

**Kaspersky Security Center - Application management**: This category provides information related to the application installed, application uninstalled, and application modified, application package added on endpoints.

**Kaspersky Security Center - Endpoint management**: This category provides information related to the endpoint added to the admin group, endpoint removed from the admin group, etc.

**Kaspersky Security Center - Device connection blocked**: This category provides information related to removable disks connected to devices, mobile phones connected to devices.

**Kaspersky Security Center - Endpoint license status**: This category provides information related to what are the endpoint license expired.

**Kaspersky Security Center - Inactive endpoints**: This category provides information related to endpoint inactive from seven days.

**Kaspersky Security Center - Unmanaged endpoints**: This category provides information related to endpoints not manageable by Kaspersky Security Center for some reason.

**Kaspersky Security Center - Malware found**: This category provides information related to virus detected, suspicious object blocked, deleted, and disinfection impossible on endpoints.

**Kaspersky Security Center - Virus scan not performed on endpoints**: This category provides information related to virus scan not performed on endpoints due to too many malicious objects detected on endpoints.

2.2 Alerts

**Kaspersky Security Center: Device connection blocked** – This alert is generated when removable disks connected on endpoints.

**Kaspersky Security Center: Inactive endpoints** - This alert is generated when an endpoint not responding for more than seven days.

**Kaspersky Security Center: Malware detected** – This alert is generated when a virus detected on endpoints.
2.3 Report

**Kaspersky Security Center - Endpoint management:** This report provides information related to endpoint added and removed, destination hostname, message, endpoint added to the admin group, endpoint removed from the admin group, endpoint name, endpoint IP address, etc.

**Log Considered**

Nov 21 08:36:04 contoso-qbwk06
CEF:0|KasperskyLab|SecurityCenter|11.0.0.1131|KLNAG_EVDEVICE_REMOVE|Device removed|1|msg=Device "Generic PnP Monitor" removed. rt=1574343362000 dhost= contosowork4534 dst= 10.10.20.17 cs2=1103 cs2Label=ProductName cs3=1.0.0.0 cs3Label=ProductVersion deviceExternalId=Generic PnP Monitor

**Sample Report**

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Product Name</th>
<th>Product ID</th>
<th>Product Version</th>
<th>Destination Host Name</th>
<th>Destination IP Address</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/27/2019 02:03:01 PM</td>
<td>Generic PnP Monitor</td>
<td>1103</td>
<td>1.0.0.0</td>
<td>contosowork4534</td>
<td>10.10.20.17</td>
<td>Device &quot;Generic PnP Monitor&quot; has been removed.</td>
</tr>
<tr>
<td>11/27/2019 02:03:01 PM</td>
<td>Intel(R) Display Audio</td>
<td>1103</td>
<td>1.0.0.0</td>
<td>contosowork4536</td>
<td>10.10.20.21</td>
<td>Device &quot;Intel(R) Display Audio&quot; has been added.</td>
</tr>
</tbody>
</table>

**Kaspersky Security Center - Unmanaged endpoints:** This report provides information related to an endpoint not manageable by Kaspersky Security center for some reason.

**Log Considered**

Nov 20 14:50:46 contoso-qbwk06
CEF:0|KasperskyLab|SecurityCenter|11.0.0.1131|KLSRV_HOST_STATUS_CRITICAL|Device status is Critical.|4|msg=Status of device "Contosowork5436" has changed to Critical: Device has become unmanaged; Protection is disabled. rt=1574279421000 dhost= contoso-qbwk06 dst=127.0.0.1 cs2=1093 cs2Label=ProductName cs3=1.0.0.0 cs3Label=ProductVersion

**Sample Report**

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Source Device Name</th>
<th>Destination Host Name</th>
<th>Destination IP Address</th>
<th>Product Name</th>
<th>Product Version</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/27/2019 03:17:28 PM</td>
<td>contosowork5436</td>
<td>contoso-qbwk06</td>
<td>127.0.0.1</td>
<td>1093</td>
<td>1.0.0.0</td>
<td>Status of device &quot;Contosowork5436&quot; has changed to Critical Device has become unmanaged; Protection is disabled.</td>
</tr>
</tbody>
</table>

**Kaspersky Security Center - Inactive endpoints:** This report provides information related to endpoint inactive for more than seven days.

**Log Considered**

Nov 20 14:48:46 contoso-qb06
CEF:0|KasperskyLab|SecurityCenter|11.0.0.1131|KLSRV_EVENT_HOSTS_NOT_VISIBLE|Inactive device. |2|msg=Device "contosowork4567" has not been visible for "7" days. rt=157427907000 dhost= contoso-qb06 dst=127.0.0.1 cs2=1093 cs2Label=ProductName cs3=1.0.0.0 cs3Label=ProductVersion

**Sample Report**

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Source Device Name</th>
<th>Destination Host Name</th>
<th>Destination IP Address</th>
<th>Product Name</th>
<th>Product Version</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/27/2019 10:12:28 PM</td>
<td>contosowork4567</td>
<td>contoso-qb06</td>
<td>127.0.0.1</td>
<td>1093</td>
<td>1.0.0.0</td>
<td>Status of device &quot;contosowork4567&quot; has not been visible for &quot;7&quot; days. Protection is disabled.</td>
</tr>
</tbody>
</table>
**Kaspersky Security Center - Application management:** This report provides information related to what is the application installed and uninstalled on endpoints, application names, destination hostname, etc.

Log Considered

Nov 21 09:50:45 contoso-qb06
CEF:0|KasperskyLab|SecurityCenter|11.0.0.1131|KLNAG_EV_INV_APP_INSTALLED|Application has been installed.|1|msg="Kaspersky Endpoint Security for Windows" version "11.1.0.15919" has been installed. rt=1574347798000 dhost=contosowork5467 dst=10.10.20.46 cs2=1103 cs2Label=ProductName cs3=1.0.0.0 cs3Label=ProductVersion fname=Kaspersky Endpoint Security for Windows fileType=application

Sample Report

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Source Device Name</th>
<th>Product Name</th>
<th>Product Version</th>
<th>Destination Host Name</th>
<th>Destination IP Address</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/03/2019 10:27:59 AM</td>
<td>contosowork4567</td>
<td>1093</td>
<td>1.0.0.0</td>
<td>contoso-qb06</td>
<td>127.0.0.1</td>
<td>Device &quot;contosowork4567&quot; has not been visible for &quot;7&quot; days.</td>
</tr>
</tbody>
</table>

**Kaspersky Security Center - Device connection blocked:** This report provides information related to removable disks connected to endpoints and connections blocked by Kaspersky Security Center, removable disk names, endpoint names, endpoint IP address, etc.

Log Considered

Nov 20 11:08:37 contoso-qbwk06
CEF:0|KasperskyLab|SecurityCenter|11.0.0.1131|GNRL_EV_DEVCTRL_DEV_PLUG_DENIED|Device connection blocked|2|msg=Event type:     Device connection blocked
Device category:     Device
Device type/Bus type:     Portable devices (MTP)
Device ID:
VID/PID:     VID_04E8&PID_6860
Device ExternalId=

Sample Report

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Destination Host Name</th>
<th>Destination IP Address</th>
<th>Product Name</th>
<th>Product Version</th>
<th>File Name</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/27/2019 02:49:50 PM</td>
<td>contosowork5467</td>
<td>10.10.20.46</td>
<td>1103</td>
<td>1.0.0.0</td>
<td>FileZilla Client 3.29.0</td>
<td>&quot;FileZilla Client 3.29.0&quot; has been removed.</td>
</tr>
<tr>
<td>11/28/2019 12:18:35 PM</td>
<td>contosowork5468</td>
<td>10.10.20.53</td>
<td>1103</td>
<td>1.0.0.0</td>
<td>Kaspersky Endpoint Security for Windows</td>
<td>&quot;Kaspersky Endpoint Security for Windows&quot; version &quot;11.1.0.15919&quot; has been installed.</td>
</tr>
</tbody>
</table>

**Kaspersky Security Center - Endpoint License status:** This report provides information related to endpoint license status, endpoint names, endpoint IP address, etc.

Log Considered

Nov 20 11:08:37 contoso-qbwk06
CEF:0|KasperskyLab|SecurityCenter|11.0.0.1131|GNRL_EV_DEVCTRL_DEV_PLUG_DENIED|Device connection blocked|2|msg=Event type:     Device connection blocked
Device category:     Device
Device type/Bus type:     Portable devices (MTP)
Device ID:
VID/PID:     VID_04E8&PID_6860
Device ExternalId=

Sample Report

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Destination User Name</th>
<th>Destination Host Name</th>
<th>Destination IP Address</th>
<th>Device ID</th>
<th>Device Type</th>
<th>Device VID and PID</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/27/2019 03:31:15 PM</td>
<td>contoso\maxx</td>
<td>contosowork4567</td>
<td>10.10.20.11</td>
<td>USB\VID_04E8\PID_6860\MS_COMP_MTP\SAMSUNG_ANDROID\8&amp;3E0AE13\0&amp;0000</td>
<td>Portable devices (MTP)</td>
<td>YD_04E8&amp;PID_0600</td>
<td>Device connection blocked</td>
</tr>
</tbody>
</table>
Integrate Kaspersky Security Center

Log Considered

Nov 21 08:26:33 contoso-qbwk06
CEF:0|KasperskyLab|SecurityCenter|11.0.0.1131|GNRL_EV_LICENSE_EXPIRATION|License Agreement violated
msg=Event type: License Agreement violated
\nApplication\Name: Kaspersky Endpoint Security 10 for Windows\nApplication Path: C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows SP2\nUser: NT AUTHORITY\SYSTEM (System user)\nComponent: Protection\nResult\Description: License has expired \nrt=1574342735000 dhost= contosowork5435
dst=10.10.20.34 cs2=KES cs2Label=ProductName cs3=10.3.0.0 cs3Label=ProductVersion

Sample Report

Kaspersky Security Center – Malwares found: This report provides information suspicious object deleted, disinfection not possible, and blocked object name, the action was taken on the object, file path, etc.

Log Considered

Nov 21 09:26:12 contoso-qbwk06
CEF:0|KasperskyLab|SecurityCenter|11.0.0.1131|GNRL_EV_OBJECT_DELETED|Object deleted\nmsg=Result: Deleted: not-a-virus:AdWare.JS.ChromeExt.i
\nUser: contoso\maxx (Active user)\nObject: C:\Users\tparker\AppData\Local\Google\Chrome\User Data\Default\Extensions\giggggbonkbaehinhgknbhabalmkn\1.0_0\js\popup\popup.js\nHash: 78c106d9fa76fe836ad45637e116771160dd81960b5d11e8fa4e3c3891b3c
\nrt=1574346357000 dhost= contosowork4535
dst=10.10.20.41 cs2=KES cs2Label=ProductName cs3=11.0.0.0 cs3Label=ProductVersion

Sample Report

Kaspersky Security Center - User connected admin server: This report provides information related to the user accessed administration server, user name, IP address, etc.

Log Considered

Nov 21 09:55:55 contoso\maxx
CEF:0|KasperskyLab|SecurityCenter|11.0.0.1131|GNRL_EV_OBJECT_DELETED|Object deleted\nmsg=Result: Deleted: \nUser: contoso\maxx\nObject: C:\Users\tparker\AppData\Local\Google\Chrome\User Data\Default\Extensions\giggggbonkbaehinhgknbhabalmkn\1.0_0\js\popup\popup.js duser= contoso\maxx

Sample Report

Kaspersky Security Center - User connected admin server: This report provides information related to the user accessed administration server, user name, IP address, etc.
Log Considered

Nov 21 09:24:11 contoso-qbwk06
CEF:0|KasperskyLab|SecurityCenter|11.0.0.1131|KLAUD_EV_SERVERCONNECT|Audit (connection to the Administration Server)|1|msg=User "contoso\maxx" has connected to the Administration Server from "10.10.12.25". rt=1574346241000 dhost=contosowork3245 dst=127.0.0.1 cs2=1093 cs2Label=ProductName cs3=1.0.0.0 cs3Label=ProductVersion

Sample Report

<table>
<thead>
<tr>
<th>Source User Name</th>
<th>Source IP Address</th>
<th>Product Name</th>
<th>Product Version</th>
<th>Destination Host Name</th>
<th>Destination IP Address</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>contoso\maxx</td>
<td>10.10.12.25</td>
<td>1093</td>
<td>1.0.0.0</td>
<td>contosowork3245</td>
<td>127.0.0.1</td>
<td>User &quot;contoso\work3245&quot; has connected to the Administration Server from &quot;10.10.12.25&quot;</td>
</tr>
</tbody>
</table>

Kaspersky Security Center - Vulnerabilities detected and fixed with updates: This report provides the information related to the vulnerabilities detected on endpoints and fixing them installing with new updates.

Log Considered

Nov 20 10:55:05 contoso-qbwk06 CEF:0|KasperskyLab|SecurityCenter|11.0.0.1131|KLPRCI_TaskState|Completed with warning|2|msg=Find vulnerabilities and required updates has been completed (with errors). Vulnerabilities detected: critical severity level - 3, high severity level - 1, medium severity level - 0. rt=1574265039000 dhost=contosowork4534 dst=10.10.20.12 cs2=1103 cs2Label=ProductName cs3=1.0.0.0 cs3Label=ProductVersion cs5=Find vulnerabilities and application updates cs5Label=TaskName cs4=103 cs4Label=TaskId cn2=4 cn2Label=TaskNewState cn1=1 cn1Label=TaskOldState

Sample Report

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Destination Host Name</th>
<th>Destination IP Address</th>
<th>Task Name</th>
<th>Message</th>
<th>Task Old State</th>
<th>Task State</th>
<th>Task New State</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/03/2019 10:28:04 AM</td>
<td>Contosowork4534</td>
<td>10.10.20.12</td>
<td>Find vulnerabilities and application updates</td>
<td>Find vulnerabilities and required updates completed successfully</td>
<td></td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>12/03/2019 16:28:05 AM</td>
<td>Contosowork4565</td>
<td>10.18.20.41</td>
<td>Find vulnerabilities and application updates</td>
<td>Windows Update test synchronized: 10-11-2019 13:56:06:0.0 Find vulnerabilities and required updates has been completed (with errors). Vulnerabilities detected: critical severity level - 0, high severity level - 0, medium severity level - 0.</td>
<td></td>
<td>Completed</td>
<td></td>
</tr>
</tbody>
</table>

2.4 Dashboards

Kaspersky Security Center - Inactive endpoints: This dashboard shows inactive endpoint names for more than seven days.
Kaspersky Security Center – Malware detected: This dashboard shows information of virus detected on endpoints.

Kaspersky Security Center – Threat management: This dashboard shows information about suspicious objects deleted, blocked and disinfection impossible.
**Kaspersky Security Center - Endpoint license expired:** This dashboard shows information about Kaspersky Security Center license expired for endpoints.

**Kaspersky Security Center - Endpoint audit changes:** This dashboard shows information about audit changes on devices.
**Kaspersky Security Center - Unmanaged endpoints:** This dashboard shows information about unmanaged endpoint by Kaspersky Security Center.

**Kaspersky Security Center - Device connection blocked:** This dashboard shows information of removable disks connected to endpoints and connections blocked by Kaspersky Security Center.
**Kaspersky Security Center - Application installed:** This dashboard shows the information of installed application names on endpoints.

**Kaspersky Security Center - Application uninstalled:** This dashboard shows the information of uninstalled applications on endpoints.
3. Importing knowledge pack into EventTracker

**NOTE:** Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token Template/ Parsing Rules
- Flex Reports
- Knowledge Objects
- Dashboards

1. Launch the EventTracker Control Panel.
2. Double click Export-Import Utility.
3. Click the **Import** tab.

### 3.1 Categories

1. Once you have opened “Export-Import Utility” via “EventTracker Control Panel”, click the **Category** option, and then click the browse button.
2. Navigate to the knowledge pack folder and select the file with the extension “.iscat”, like “Categories_Kaspersky Security Center. iscat” and then click on the “**Import**” button:
EventTracker displays a success message:

Figure 17

3.2 Alerts

1. Once you have opened “Export-Import Utility” via “EventTracker Control Panel”, click Alert option, and then click the browse button.
2. Navigate to the knowledge pack folder and select the file with the extension “.isalt”, e.g. “Alerts_Kaspersky Security Center.isalt” and then click on the “Import” button:
3.3 Parsing Rule

1. Once you have opened "Export-Import Utility" via "EventTracker Control Panel", click the Token Value option, and then click the browse button.

2. Navigate to the knowledge pack folder and select the file with the extension ".iscat", like "Parsing Rule_Kaspersky Security Center. istoken" and then click on the "Import" button:

EventTracker displays a success message:

Selected alert configurations are imported successfully.
3.4 Flex Reports

1. In the EventTracker control panel, select “Export/ Import utility” and select the “Import tab”. Then, click Reports option, and choose “New (*.etcrx)”: 

![Figure 21](image1)

![Figure 22](image2)
2. Once you have selected “New (*.etcrx)”, a new pop-up window will appear. Click the “Select File” button and navigate to the knowledge pack folder and select file with the extension “.etcrx”, e.g. “Reports_Kaspersky Security Center.etcrx”.

3. Wait while reports are being populated in the below tables. Now, select all the relevant reports and then click the Import button.
EventTracker displays a success message:

![Success message](image)

3.5 Knowledge Objects

1. Click **Knowledge objects** under the **Admin** option in the EventTracker web interface.

![Admin interface](image)

2. Next, click the “import object” icon:

![Import objects](image)
3. A pop-up box will appear, click “Browse” in that and navigate to the knowledge packs folder (type “C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs” in the navigation bar) with the extension “.etko”, e.g. “KO_Kaspersky Security Center.etko” and then click the “Upload” button.

![Figure 29](image)

4. Wait while EventTracker populates all the relevant knowledge objects. Once the objects are displayed, select the required ones and click on the “Import” button:

![Figure 30](image)

### 3.6 Dashboards

1. Login to the EventTracker web interface.
2. Navigate to Dashboard → My Dashboard.
3. In “My Dashboard”, Click Import Button:

![Figure 31](image)
Integrate Kaspersky Security Center

4. Select the browse button and navigate to the knowledge pack folder (type “C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs” in the navigation bar) where “.etwd”, e.g. “Dashboard_Kaspersky Security Center.etwd” is saved and click on “Upload” button.

5. Wait while EventTracker populates all the available dashboards. Now, choose “Select All” and click on “Import” Button.

4. Verifying knowledge pack in EventTracker

4.1 Categories

1. Login to the EventTracker web interface.
2. Click Admin dropdown, and then click Categories.
3. In **Category Tree** to view imported categories, please click on “**Search**” and search with the “**Kaspersky Security Center**”. You will see the below results:

![Category Tree](image)

**Figure 35**

4.2 **Alerts**

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Alerts**.
2. In search box enter “**Kaspersky Security Center**” and then click the **Search** button.

EventTracker displays an alert related to Kaspersky Security Center:

![Alerts](image)

**Figure 36**
4.3 Parsing Rules

1. In the EventTracker web interface, click the Admin dropdown, and then click Parsing Rule.
2. In the Parsing Rule tab, click on the “Kaspersky Security Center” group folder to view the imported Token Values.

![Parsing Rules](image)

Figure 37

4.4 Flex Reports

1. In the EventTracker web interface, click the Reports menu, and then select the Report Configuration.

![Report Configuration](image)

Figure 38

2. In Reports Configuration pane, select the Defined option.
3. Click on the “Kaspersky Security Center” group folder to view the imported reports.

![Report Configuration](image)

Figure 39

4.5 Knowledge Objects

1. In the EventTracker web interface, click the Admin dropdown, and then click Knowledge Objects.
2. In the **Knowledge Object** tree, expand the “**Kaspersky Security Center**” group folder to view the imported Knowledge objects.

![Knowledge Objects](image1)

**Figure 40**

### 4.6 Dashboards

1. In the EventTracker web interface, Click on Home Button 🏛️ and select **“My Dashboard”**.

![Dashboard](image2)

**Figure 41**

2. In “**Kaspersky Security Center**” dashboard you should be now able to see something like this:

![My Dashboard](image3)

**Figure 42**