Integrate Cb Defense

EventTracker v8.x and above

Publication Date: June 18, 2018
Abstract

This guide helps you in configuring Cb Defense with EventTracker to receive Cb Defense events. In this guide, you will find the detailed procedures required for monitoring Cb Defense.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 8.x and later, Cb Defense Next-Generation Antivirus + EDR.

Audience

Administrators who are assigned the task to monitor and manage Cb Defense events using EventTracker.
# Table of Contents

Abstract ............................................................................................................................................................. 1  
Scope ................................................................................................................................................................. 1  
Audience ............................................................................................................................................................ 1  
Overview ................................................................................................................................................................ 3  
Prerequisites .......................................................................................................................................................... 3  
Integration of Cb Defense events to EventTracker server .................................................................................... 3  
Verify Cb Defense Integration in EventTracker ..................................................................................................... 7  
EventTracker Knowledge Pack ................................................................................................................................ 11  
  Flex Reports ..................................................................................................................................................... 11  
  Knowledge Objects .......................................................................................................................................... 18  
Import Cb Defense knowledge pack into EventTracker ........................................................................................... 18  
  Parsing Rules .................................................................................................................................................... 19  
  Flex Reports ..................................................................................................................................................... 20  
  Knowledge Objects .......................................................................................................................................... 22  
Verify Cb Defense knowledge pack in EventTracker ............................................................................................... 23  
  Parsing Rules .................................................................................................................................................... 23  
  Flex Reports ..................................................................................................................................................... 24  
  Knowledge Objects .......................................................................................................................................... 25  
Create Flex Dashboards in EventTracker ............................................................................................................. 26  
  Schedule Reports ............................................................................................................................................. 26  
  Create Dashlets ............................................................................................................................................... 28  
  Sample Flex Dashboards .................................................................................................................................. 32
Overview

Cb Defense is the Carbon Black’s next-generation antivirus solution which provides complete antivirus efficacy to directly meet PCI DSS requirements. It uses behavior-based techniques to prevent attacks from getting started and blends in attack-detection and response to halt ongoing attacks.

EventTracker integrates Cb defense logging through REST API and provides reports, knowledge objects and dashboards for all generated events including attacks, network connections, registry access, file auditing etc. EventTracker will also monitor antivirus sensors and process execution statuses for all workstations in the network.

Prerequisites

- EventTracker v8.x should be installed.
- Cb Defense must be deployed.
- Contact support to get the Hostname associated with your Cb Defense API backend.

Integration of Cb Defense events to EventTracker server

EventTracker utilizes Cb Defense API to fetch events from Cb Defense console in JSON format. The Cb Defense API is accessible through a special hostname assigned to your organization. Authentication is handled by an API key and Connector ID, which is generated from the Connectors page of the Cb Defense console.

Connector configuration for Cb Defense API is explained below:

1. Logon to the Cb Defense console.
2. Click on Settings and select Connectors from drop-down.
3. Define a new connector and note down its `apiKey` and `connectorId`.
4. Use an appropriate name for the connector.
5. Choose `API` as `Connector Type`. Notifications can also be configured by adding a new connector with connector type `SIEM`.
6. Enter the IP address of EventTracker machine under `Authorized IP Addresses`.
7. Click `Save`.

**Note:** If authentication failures happen for API calls, remove ip address from Authorized IP Addresses.
Following are the steps to integrate Cb Defense to EventTracker:

- Please Contact the EventTracker support team for obtaining Cb Defense Integrator pack.
- The Integrator package will be obtained in a Zip file format, extract the files to get the below file contents as shown in the image.

- Double-click on the `CBScript.bat` to initialize configuration.

CB Integrator configuration window will pop-up.
In the CB Integrator configuration window, enter the following details:
- **API Key** – Enter the API key of the configured connector.
- **Connector ID** - Enter the connector ID of the configured connector.
- **API HostName** – Enter the API backend hostname.

**Note:** Configure SIEM api key details only if connector has been made for the same.

- Click **OK** to proceed.
- In the next window, enter admin credentials for scheduling the task.

- Click **OK** to proceed.

Successful configuration pop-up message is shown.
Ci\# Integrator

Configuration Complete

OK

Figure 6

- Click OK to exit Cb Integrator configuration.

Verify Cb Defense Integration in EventTracker

- Launch the EventTracker Manager.
- Select Manager under Admin drop-down.

Figure 7
• Go to the Direct Log Archiver tab and check if the configurations are replicated as shown below:

![Manager Configuration](image)

**Figure 8**

• Select Cb Defense integrator DLA configuration and click **Edit** to verify DLA configuration further.
• Verify configured settings and click **Configure** to proceed.
• Verify configured settings and click **Cancel** settings are correct.
• Go to Start and open Task Scheduler to verify **CBDefense Logging** scheduled task.
• Adjust task trigger schedule for the task as per your requirement.
• If task is altered, save it with admin credentials.

EventTracker Knowledge Pack

Once logs are received into EventTracker, Reports, Dashboards and Knowledge Objects can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Windows.

Flex Reports

• CB Defense- Processes executed: This report provides details regarding processes executed in the network with their respective counts.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Application Name</th>
<th>Event Count</th>
<th>SHA256 Hash</th>
<th>Application Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>07/05/2017 02:18:18 PM</td>
<td>svchost.exe</td>
<td>2976</td>
<td>93b2ed4004ed5ff3039dd7ecbd22 C:Windows\System32\svchost.exe c7e4e24b6373b4d9ef8d6e45a179 xe b13a5e8</td>
<td></td>
</tr>
<tr>
<td>07/05/2017 02:18:18 PM</td>
<td>chrome.exe</td>
<td>3000</td>
<td>f069d992013657aa0793e0c3b433 C:\Program Files (x86)\Google\Chrome\Application a9c6d5b</td>
<td></td>
</tr>
<tr>
<td>07/05/2017 02:18:18 PM</td>
<td>firefox.exe</td>
<td>3012</td>
<td>406f8750e2047c55ac38923844d7 C:\Program Files (x86)\Mozilla Firefox\firefox.exe 8b87d61</td>
<td></td>
</tr>
<tr>
<td>07/05/2017 02:18:18 PM</td>
<td>svchost.exe</td>
<td>5040</td>
<td>93b2ed4004ed5ff3039dd7ecbd22 C:Windows\System32\svchost.exe c7e4e24b6373b4d9ef8d6e45a179 xe b13a5e8</td>
<td></td>
</tr>
<tr>
<td>07/05/2017 02:18:18 PM</td>
<td>svchost.exe</td>
<td>2776</td>
<td>93b2ed4004ed5ff3039dd7ecbd22 C:Windows\System32\svchost.exe c7e4e24b6373b4d9ef8d6e45a179 xe b13a5e8</td>
<td></td>
</tr>
</tbody>
</table>
Sample Logs:

- **CB Defense - Device details**: This report provides details about AV sensor status of all devices in the network.
### Sample Logs:

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
</table>

- **event_log_type**: System
- **event_type**: Information
- **event_id**: 3220
- **event_source**: Cb
- **event_user_domain**: NT AUTHORITY
- **event_computer**: CB Defense-DLA
- **event_user_name**: SYSTEM

- **Cb Defense- Network activity**: This report provides information about network traffic details.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Event Type</th>
<th>Threat Indicators</th>
<th>Device Name</th>
<th>Device Location</th>
<th>Device Type</th>
<th>Device OS Version</th>
<th>Device IP Address</th>
<th>Device Priority</th>
<th>User Details</th>
<th>Source IP</th>
<th>Source Port Number</th>
<th>Destination IP</th>
<th>Destination Port Number</th>
<th>Destination Port Number</th>
</tr>
</thead>
</table>
Sample Logs:

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 30 11:00:25 AM</td>
<td>registryValue threatIndicators: NETWORK_ACCESS deviceDetails.deviceIPAddress: 110.23.55.69 deviceDetails.agentLocation: ONSITE deviceDetails.deviceName: RIPLEYS\Name-POS-01 deviceDetails.deviceVersion: Windows 7 x64 SP 1</td>
</tr>
</tbody>
</table>

**Cb Defense- Application access:** This report provides information about applications accessed by users.
### Cb Defense - File and Registry access:

This report provides information about file and registry changes by users.

### Sample Logs:

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 30 11:00:25 AM</td>
<td>registryValue: threatIndicators: deviceDetails.deviceIPv4Address: 11.23.125.63 deviceDetails.agent.location: OFFSITE deviceDetails.deviceIPv4Address: ...</td>
</tr>
</tbody>
</table>

- Cb Defense- File and Registry access: This report provides information about file and registry changes by users.
• Cb Defense - Data access: This report provides information about data accessed by users.

Sample Logs:

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 07 03:11:44 PM</td>
<td>registryValue threatIndicators: ACCESS_EMAIL_DATA deviceDetails.devicelp4Address: 75.125.23.2 deviceDetails.agentLocation: OFFSITE deviceDetails....</td>
</tr>
</tbody>
</table>

- event_log_type: System
- event_type: Information
- event_id: 3320
- event_source: CB
- event_user_domain: NT AUTHORITY
- event_computer: Cb Defense- OLA
- event_user_name: SYSTEM
- event_description: registryValue

threatIndicators: ACCESS_EMAIL_DATA
deviceDetails.devicelp4Address: 75.125.23.2
deviceDetails.agentLocation: OFFSITE
deviceDetails.devicelp4Address: 75.125.23.2
deviceDetails.deviceLocation: @serCode=\s=, countryName=United States; countryCode=US; dmaCode=312; latitude=39.9042; longitude=-76.5366; metroCode=141; postalCode=19114; region=MD; city=......
deviceDetails.deviceHostName
deviceDetails.devicePriorityType: MEDIUM
deviceDetails.devicePriorityCode: 1
deviceDetails.email: MS.mp

deviceDetails.deviceType: WINDOWS
deviceDetails.policyId: 20215
deviceDetails.deviceId: 2376254
deviceDetails.deviceName: MS-INF

• Cb Defense - Policy action: This report provides information about policies changed by users.
Sample Logs:

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 07 06:11:44 PM</td>
<td>registryValue: threatIndicators.POLICY_DENY deviceDetails.deviceIpAddress 75.23.1.200 deviceDetails.agentLocation OFFSITE deviceDetails.deviceIpAddress 75.23.1.200 deviceDetails.deviceLocation: {areaCode: ... countryNames: UnitedStates; countryCodes: US; dmaCode: ... latitude: 39.805; longitude: -76.614; region: MD; city: Baltimore}</td>
</tr>
<tr>
<td></td>
<td>threatIndicators.POLICY_DENY deviceDetails.deviceIpAddress 75.23.1.200 deviceDetails.agentLocation OFFSITE deviceDetails.deviceIpAddress 75.23.1.200 deviceDetails.deviceLocation: {areaCode: ... countryNames: UnitedStates; countryCodes: US; dmaCode: ... latitude: 39.805; longitude: -76.614; region: MD; city: Baltimore} deviceDetails.deviceHostName deviceDetails.deviceIpAddress deviceDetails.devicePriorityType MEDIUM deviceDetails.devicePriorityCode 1 deviceDetails.deviceName MSVWELT deviceDetails.deviceType: WINDOWS deviceDetails.policyId: 2931 deviceDetails.deviceId: 237632 deviceDetails.deviceVersion: Windows 7 x64 SP 1</td>
</tr>
<tr>
<td></td>
<td>threatIndicators.POLICY_DENY deviceDetails.deviceIpAddress 75.23.1.200 deviceDetails.agentLocation OFFSITE deviceDetails.deviceIpAddress 75.23.1.200 deviceDetails.deviceLocation: {areaCode: ... countryNames: UnitedStates; countryCodes: US; dmaCode: ... latitude: 39.805; longitude: -76.614; region: MD; city: Baltimore} deviceDetails.deviceHostName deviceDetails.deviceIpAddress deviceDetails.devicePriorityType MEDIUM deviceDetails.devicePriorityCode 1 deviceDetails.deviceName MSVWELT deviceDetails.deviceType: WINDOWS deviceDetails.policyId: 2931 deviceDetails.deviceId: 237632 deviceDetails.deviceVersion: Windows 7 x64 SP 1</td>
</tr>
</tbody>
</table>

- **Cb Defense- Threat detection:** This report provides information about threats detected.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Threat Indicators</th>
<th>Device Name</th>
<th>Device Location</th>
<th>Device Type</th>
<th>Device OS Version</th>
<th>Device IP Address</th>
<th>Device Priority</th>
<th>Threat Details</th>
<th>Process Name</th>
<th>Application Path</th>
<th>Application sha256 Hash</th>
<th>Target Command Line</th>
<th>Parent Command Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/7/2018 12:16:11 AM</td>
<td>inject_code</td>
<td>JELUR</td>
<td>United States</td>
<td>WINDOWS</td>
<td>Windows 7 x64</td>
<td>55.216.58.156</td>
<td>SP 1</td>
<td>MEDIUM</td>
<td>Inject</td>
<td>ndriver.exe</td>
<td>3699565598562996540374</td>
<td>C:\Program Files (x86)\WebContent\001\kernel\ntnt打进.exe</td>
<td>17</td>
</tr>
<tr>
<td>5/7/2018 12:18:08 AM</td>
<td>inject_code</td>
<td>JELUR</td>
<td>United States</td>
<td>WINDOWS3</td>
<td>Windows 7 x64</td>
<td>55.216.58.158</td>
<td>SP 1</td>
<td>MEDIUM</td>
<td>Inject</td>
<td>ndriver04.exe</td>
<td>3699565598562996540374</td>
<td>C:\Program Files (x86)\WebContent\001\kernel\ntnt打进.exe</td>
<td>17</td>
</tr>
<tr>
<td>5/7/2018 12:19:33 AM</td>
<td>inject_code</td>
<td>JELUR</td>
<td>United States</td>
<td>WINDOWS</td>
<td>Windows 7 x64</td>
<td>55.216.58.150</td>
<td>SP 1</td>
<td>MEDIUM</td>
<td>Inject</td>
<td>ndriver04.exe</td>
<td>3699565598562996540374</td>
<td>C:\Program Files (x86)\WebContent\001\kernel\ntnt打进.exe</td>
<td>17</td>
</tr>
</tbody>
</table>
Sample Logs:

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 07 11:49 PM</td>
<td>registryValue: threatIndicators INJECT_CODE deviceDetails devAddress 75.23.1.200 deviceDetails agentLocation OFFSITE deviceDetails devName A...</td>
</tr>
</tbody>
</table>

- **event_log_type**: System
- **event_type**: Information
- **event_id**: 3320
- **event_source**: CB
- **event_user_domain**: NT AUTHORITY
- **event_computer**: CB Defense DLA
- **event_user_name**: SYSTEM
- **event_description**: registryValue:
  - threatIndicators: INJECT_CODE
devices deviceDetails.devAddress: 75.23.1.200
deviceDetails.agentLocation: OFFSITE
deviceDetails.devAddress: 75.23.1.200
deviceDetails.devLocation: @areaCode ... country=United States countyCode=US adminCode= ... latitude=39.7... longitude=... region=MD city=Baltimore
deviceDetails.devHostName
deviceDetails.devDomainName
deviceDetails.devPriorityType: MEDIUM
deviceDetails.devPriorityCode: 1
deviceDetails.email= MSWelt
deviceDetails.devType: WINDOW

time=2011/06/23 11:48:32

deviceDetails.devId: 327632
deviceDetails.devName: MSWelt
deviceDetails.devVersion: Windows 7

Knowledge Objects

- **CB Defense - Processes executed**: This KO helps in evaluating processes executed in the network with their respective counts. It identifies frequently and rarely used process with their respective paths.
- **CB Defense - Device details**: This KO helps in identifying AV sensor details of all workstations in the network. It provides AV database versions; AV status and AV scan status for all integrated devices.
- **CB Defense - All events**: This KO helps in analyzing all events generated on CB Defense. This includes events for attacks, network traffic, data audit etc.

Import Cb Defense knowledge pack into EventTracker

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

- Parsing Rules
- Flex Reports
- Knowledge Objects

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

### Parsing Rules

1. Click **Token Value** option, and then click the browse button.
2. Locate the **Cb Defense Parsing Rules.istoken** file, and then click the *Open* button.
3. Click the **Import** button to import the tokens. EventTracker displays success message.

![Figure 14](image1.png)

**Flex Reports**

1. Click **Reports** option, and then click the browse button.

![Figure 15](image2.png)

3. Locate the **Cb Defense reports.issch** file, and then click the **Select file** button.

4. Select all reports and click **OK** button. EventTracker displays success message.

---

**Figure 16**

**Figure 17**
Knowledge Objects

1. Logon to EventTracker Enterprise.
2. Click the Admin menu and then click the Knowledge Objects.

3. Click the Import button.

Figure 18

Figure 19
4. Click browse and locate the file named **Cb Defense Knowledge Objects.etko**.

5. Click on **UPLOAD** button.

![Figure 20](import.png)

6. Select associated knowledge objects and click on **Overwrite** button.

![Figure 21](overwrite.png)

7. Click **OK**.

**Verify Cb Defense knowledge pack in EventTracker**

**Parsing Rules**

1. Logon to **EventTracker Enterprise** web interface.
2. Click the **Admin** menu, and then click **Parsing Rules**.
Flex Reports

1. In the EventTracker Enterprise web interface, click the Reports menu, and then select Configuration.
2. In Reports Configuration pane, select Defined option.
   EventTracker displays Flex reports of ‘CB Defense’.
Knowledge Objects

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu and then click the **Knowledge Objects**.

![Figure 24](image)

3. Scroll down and select Cb Defense from Groups section. Imported knowledge objects are shown in the right pane.
Create Flex Dashboards in EventTracker

**NOTE:** To configure the flex dashboards, schedule and generate the reports. Flex dashboard feature is available from EventTracker Enterprise v8.0.

**Schedule Reports**

1. Open *EventTracker* in browser and logon.

2. Navigate to *Reports* > *Configuration*.

4. Click on ‘schedule’ to plan a report for later execution.
5. Click Next button to proceed.
6. In review page, check Persist data in EventVault Explorer option.
7. In next page, check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.

![Figure 29](image)

8. Proceed to next step and click **Schedule** button.
9. Wait till the reports get generated.

**Create Dashlets**

1. Open **EventTracker Enterprise** in browser and logon.
2. Navigate to Dashboard>Flex. 
   Flex Dashboard pane is shown.

3. Fill suitable title and description and click Save button.
4. Click to configure a new flex dashlet. Widget configuration pane is shown.
5. Locate earlier scheduled report in **Data Source** dropdown.
6. Select **Chart Type** from dropdown.
7. Select extent of data to be displayed in **Duration** dropdown.
8. Select computation type in **Value Field Setting** dropdown.
9. Select evaluation duration in **As Of** dropdown.
10. Select comparable values in **X Axis** with suitable label.
11. Select numeric values in **Y Axis** with suitable label.
12. Select comparable sequence in **Legend**.
13. Click **Test** button to evaluate. Evaluated chart is shown.
14. If satisfied, click **Configure** button.

15. Click ‘customize’ to locate and choose created dashlet.

16. Click to add dashlet to earlier created dashboard.
Sample Flex Dashboards

- **REPORT: CB Defense- Process executed**
  
  **WIDGET TITLE:** Cb Defense – Top executed processes
  **CHART TYPE:** Column
  **AXIS LABELS [X-AXIS]:** Device Name
  **VALUES [Y-AXIS]:** Event Count

![CB DEFENSE- TOP EXECUTED PROCESSES](image1)

*Figure 35*

- **REPORT: CB Defense-Device details**

  **WIDGET TITLE:** CB Defense- AV Sensor status
  **CHART TYPE:** Pie
  **AXIS LABELS [X-AXIS]:** Device Name
  **VALUES [Y-AXIS]:** Event Count

![CB DEFENSE- AV SENSOR STATUS](image2)

*Figure 36*
• REPORT: CB Defense-All Events
  WIDGET TITLE: CB Defense- Network access
  CHART TYPE: Donut
  AXIS LABELS [X-AXIS]: Source Address
  LEGEND [SERIES]: Event Type

Figure 37