Integrate Tenable.io

EventTracker v8.x and above
Integrate Tenable.io

Abstract

This guide helps you in configuring Tenable.io and EventTracker to receive Tenable.io events. You will find the detailed procedures required for monitoring Tenable.io.

Audience

Administrators who are assigned the task to monitor and manage Tenable.io events using EventTracker.

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.
Table of Contents

Abstract .................................................................................................................................................................... 1
Audience .................................................................................................................................................................. 1
Overview .............................................................................................................................................................. 3
Prerequisites ........................................................................................................................................................ 3
Integration of Tenable events to EventTracker server ............................................................................................. 3
Verify Tenable.io Integration in EventTracker ........................................................................................................... 6
EventTracker Knowledge Pack .................................................................................................................................. 11
    Flex Reports ....................................................................................................................................................... 12
Import Tenable.io knowledge pack into EventTracker ................................................................................................... 18
    Knowledge Objects ................................................................................................................................................ 19
    Flex Reports ........................................................................................................................................................... 20
    Parsing Rule .......................................................................................................................................................... 21
Verify Tenable.io knowledge pack in EventTracker ................................................................................................... 23
    Knowledge Objects ................................................................................................................................................ 23
    Flex Reports ........................................................................................................................................................... 23
    Parsing Rule .......................................................................................................................................................... 24
Create Flex Dashboards in EventTracker ................................................................................................................... 25
    Schedule Reports .................................................................................................................................................. 25
    Create Dashlets ..................................................................................................................................................... 27
    Sample Flex Dashboards ..................................................................................................................................... 31
Overview

Tenable provides comprehensive visibility into the security posture of container images as they are developed, enabling vulnerability assessment, malware detection, policy enforcement and remediation prior to container deployment. It gains visibility into the security of web applications with safe vulnerability scanning, complete with high detection rates to ensure you understand the true risks in your web applications. It brings clarity to your security posture through a fresh, asset-based approach that provides maximum coverage of your evolving assets and vulnerabilities in ever-changing environments.

Prerequisites

- EventTracker v8.x should be installed.
- Tenable.io for cloud and Tenable.io on premises (Security Centre)
- An exception should be added into windows firewall on EventTracker machine for syslog port 514.

Integration of Tenable events to EventTracker server

Following are the steps to integrate Tenable.io to EventTracker.

- Please Contact the EventTracker support team for obtaining Tenable 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.

![Figure 1](image-url)
• Double-click on the Tenable Integrator.bat(for both cloud or Security centre) to start the integration process.
• Once the .bat starts running, you will get a pop up window as shown in below image.

![Figure 2](image)

- In the pop-up window that appeared, enter your Tenable Username and Password.
- Once you enter the details, click on OK.
- Now a task scheduler trigger pop-up window appears as shown in below image

![Figure 3](image)

- In this task scheduler window, you need to choose how you want to schedule the Tenable reports, i.e. on a Daily, Weekly or Monthly basis.
- Click on OK once scheduling period is chosen.
- Once you click OK, an authentication pop up window will appear asking for Username and password as shown below:
• Please enter your System Username and Password to proceed with the Task Scheduling.
• Click on OK to continue.

Figure 4

Figure 5

• Configuration is now complete.

Note: For the scans to be monitored, the permissions for the user scans should be set to ‘Can view’ as shown in the below image, otherwise the scans would not be saved or monitored.
Verify Tenable.io Integration in EventTracker

- Launch the EventTracker web.
- Navigate to Admin > Manager.
Go to the Direct Log Archiver Tab and check if the configurations are replicating as show in the below image.

Please select the checkbox Direct log file achieving from external sources, if not selected by default, as shown in the below image.
- Confirm if the Configurations are set right by clicking on **Edit**. You will get the below window once you click **Edit**.
• Click on **Configure** to check the Computer Name, Configuration name and system description.
• Click **Ok.**
Go to **Start** and open **Task Scheduler** to confirm if the scheduling action is created or not.

Below image shows the Tenable Task that is created for scheduling.
• Check if the Task Scheduler is configured correctly with the right conditions to trigger the task, with the specified date and time when it needs to be run.

• Tenable Integration is now completed with EventTracker to receive Tenable Events.

EventTracker Knowledge Pack

Once logs are received into EventTracker, Categories, reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Windows.
1. **Tenable-Basic Network Scan**: This report provides a full system scan suitable for any host.

![Figure 12](image1.png)

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Event ID</th>
<th>Site/Computer</th>
<th>User</th>
<th>Domain</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/25/2017 05:17:37 PM</td>
<td>9647</td>
<td>PNPL-6-KP / Contoso</td>
<td>N/A</td>
<td>N/A</td>
<td>Tenable</td>
</tr>
</tbody>
</table>

**Logs Considered:**

![Figure 13](image2.png)

2. **Tenable-Credentialed Patch Audit**: This report provides the ways that a host can be authenticated and enumerates missing patch updates.
3. **Tenable-Badlock Detection**: This report provides the badlock vulnerability for Windows and the Linux/Unix application Samba for network file sharing.
4. **Tenable-Host Discovery:** This report provides a simple scan to discover live host and open ports.

5. **Tenable-Malware Detection:** This report provides the scan results of malware on windows and unix systems.
6. **Tenable-Bash Shellshock Detection**: This report provides the vulnerability that affects Bash, a common component known as a shell that appears in many versions of Linux and Unix. It allows the user to type commands into a simple text-based window, which the operating system will then run.
Logs Considered:

<table>
<thead>
<tr>
<th>LOG TIME</th>
<th>EVENT ID</th>
<th>SITE / COMPUTER</th>
<th>USER</th>
<th>DOMAIN</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/10/2017 6:08:17 PM</td>
<td>3730</td>
<td>PIIPL-6-KP / Conotox</td>
<td>N/A</td>
<td>N/A</td>
<td>Tenable</td>
</tr>
</tbody>
</table>

Event Type: Information
Log Type: Application
Category Id: 0

Description:
Plugin Id: 11219
CVE: CVE-2014-6278
CVSS: Risk: None
Host: 192.168.137.236
Protocol: tcp
Port: 22

Vulnerability Description: This plugin is a SYN “half-open” port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCPFull connections against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution: Protect your target with an IP filter.

Figure 23

7. **Drown Detection**: DROWN is a serious vulnerability that affects HTTPS and other services that rely on SSL and TLS, some of the essential cryptographic protocols for Internet security.

<table>
<thead>
<tr>
<th>LOG TIME</th>
<th>EVENT ID</th>
<th>SITE / COMPUTER</th>
<th>USER</th>
<th>DOMAIN</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>08/03/2017 00:20:17 PM</td>
<td>03705</td>
<td>CVE-2016-0702</td>
<td>9.3</td>
<td>High</td>
<td>Tenable Drown detection</td>
</tr>
</tbody>
</table>

Solution: Upgrade to OpenSSL version 1.0.2g or later.

Synopsis: The remote service is affected by multiple vulnerabilities.

Figure 24

Logs Considered:

<table>
<thead>
<tr>
<th>LOG TIME</th>
<th>EVENT ID</th>
<th>SITE / COMPUTER</th>
<th>USER</th>
<th>DOMAIN</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/1/2017 6:20:17 PM</td>
<td>2230</td>
<td>NTPL01B.86 / Tenable</td>
<td>N/A</td>
<td>N/A</td>
<td>Tenable</td>
</tr>
</tbody>
</table>

Event Type: Information
Log Type: Application
Category Id: 0

Description:
Plugin Id: 83705
CVE: CVE-2016-0762
CVSS: 9.0
Risk: High
Host: 100.168.1.140
Protocol: tcp
Port: 80

Name: Tenable Drown detection

Vulnerability Description: A key disclosure vulnerability exists due to improper handling of cache-bank conflicts on the Intel Sandy-bridge microarchitecture. An attacker can exploit this to gain access to RSA key information.

Solution: Upgrade to OpenSSL version 1.0.2g or later.

Synopsis: The remote service is affected by multiple vulnerabilities

Figure 25

8. **Tenable-Scap and Oval Auditing**: This report provides details about how to generate SCAP and Oval content audit scan results.
9. **Tenable-User activities:** This report provides details about all the user activities.
Logs Considered:

![Log Example](image)

**Figure 29**

Import Tenable.io knowledge pack into EventTracker

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

- Knowledge Objects
- Flex Reports
- Parsing Rule

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

- Knowledge Objects
- Flex Reports
- Parsing rule

1. Launch **EventTracker Control Panel**.

2. Double click **Export Import Utility**.
3. Click the **Import** tab.

**Knowledge Objects**

1. Click **Knowledge objects** under **Admin** option in the EventTracker manager page.

2. Locate the **All Tenable.io group of Knowledge object.** and then click **Import** button.
3. Choose the Knowledge objects that needs to be imported and click on **upload**.

![Import Knowledge Objects](image)

**Figure 32**

4. Knowledge objects are now imported successfully.

![File imported successfully](image)

**Figure 33**

**Flex Reports**

1. Click **Reports** option, and then click the browse button.
2. Locate the **All Tenable.io group of flex reports.issch** file, and then click the **Open** button.
3. Click the **Import** button to import the reports. EventTracker displays success message.

![Figure 34](image)

![Figure 35](image)

**Parsing Rule**

1. Click **Token Value** option, and then click the browse button.
2. Locate the **All Tenable.io group of Token Value.issch** file, and then click the **Open** button.
4. Click the **Import** button to import the tokens. EventTracker displays success message.
Verify Tenable.io knowledge pack in EventTracker

Knowledge Objects

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Knowledge Objects.

In the Knowledge Object tree, expand Tenable.io group folder to see the imported Knowledge objects.

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.
3. In search box enter ‘Tenable Scanner’, and then click the Search button.
   EventTracker displays Flex reports of ‘Tenable Scanner’
Parsing Rule

1. Logon to EventTracker Enterprise web interface.

2. Click the Admin menu, and then click Parsing Rules and click Parsing rule.
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.
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

For below dashboard

Report Name: Tenable-Credentialed Patch Audit

- **WIDGET TITLE:** Tenable-Credentialed Patch Audit
  - **CHART TYPE:** Stacked Column
  - **AXIS LABELS [X-AXIS]:** CVE
  - **LEGEND:** Vulnerability description

![Tenable-Credentialed Patch Audit Dashboard](image)

*Figure 49*
Report Name: Tenable-Badlock Detection

- **WIDGET TITLE:** Tenable-Badlock Detection
- **CHART TYPE:** Pie
- **AXIS LABELS [X-AXIS]:** CVE
- **LEGEND:** Host

![Tenable-Badlock Detection Chart](image)

*Figure 50*
Report Name: Tenable-Host Discovery

- WIDGET TITLE: Tenable-Host Discovery
- CHART TYPE: Stacked Column
- AXIS LABELS [X-AXIS]: IP Address
- LEGEND[SERIES]: Message

Figure 51
Report Name: Tenable-Malware Detection

- **WIDGET TITLE:** Tenable-Malware Detection
  - **CHART TYPE:** Donut
  - **AXIS LABELS [X-AXIS]:** HOST
  - **LEGEND:** Message

Figure 52

Report Name: Tenable-Bash Shellshock Detection

- **WIDGET TITLE:** Tenable-Bash Shellshock Detection
  - **CHART TYPE:** Stacked Column
  - **AXIS LABELS [X-AXIS]:** CVE
  - **LEGEND:** Risk

Figure 53
Report Name: Tenable-Drown Detection

- **WIDGET TITLE:** Tenable- Drown Detection
  - **CHART TYPE:** Donut
  - **AXIS LABELS [X-AXIS]:** CVE
  - **LEGEND[SERIES]:** Risk

![Tenable-Drown Detection Chart](image)

Figure 54
Report Name: Scap and Oval Auditing

- **WIDGET TITLE:** Tenable- Scap and Oval Auditing
- **CHART TYPE:** Donut
- **AXIS LABELS [X-AXIS]:** Mac Address
- **LEGEND[SERIES]:** Severity

![Donut Chart](image)

*Figure 55*
Report Name: Critical vulnerability score

- **WIDGET TITLE**: Critical vulnerability score
- **CHART TYPE**: PIE
- **AXIS LABELS [X-AXIS]**: CVE
- **LEGEND**: HOST

![Diagram showing critical vulnerability scores for different hosts](image-url)

*Figure 56*