Netsurion | EventTracker®

EventTracker Threat Center Integration

EventTracker v9.3

Publication Date: May 7, 2020

Abstract

This guide helps you to know more about EventTracker Threat Center. EventTracker Threat Center is Netsurion' s Threat Center Platform.

EventTracker Threat Center is a repository of threats indicators. It accumulates series of different threat feeds, gathers information about IP addresses, scans an IP address with multiple IP blacklist and finds security threats. EventTracker Threat Center is used as an alternate IP reputation provider and is maintained by Netsurion.

Audience

This guide is intended for all the EventTracker v9.3 users responsible for investigating and managing the network security.

Table of Contents

1. EventTracker Threat Center 3
2. Attackers and Targets dashboard 3
2.1 Attackers pane 3
2.2 Viewing the Dashboard 3
2.3 Getting information about the bad IP 6
2.4 Targets pane 9

1. EventTracker Threat Center

The current IP reputation providers such as IP Void or BorderWare (that determines the badness/reputation of an IP address) has limitations when scanning numerous IP addresses.

Netsurion has developed Threat Center Platform which can be used as an alternate IP reputation provider. It accumulates series of different threat feeds, gathers information about IP addresses, scans an IP address with multiple IP blacklist and finds security threats.

2. Attackers and Targets dashboard

2.1 Attackers pane

The Attackers Dashboard option helps to view the Top 20 geographic location pins. Each of these top 20 pins may contain 'N' number of bad IPs.

An IP address earns a negative reputation when it is found with suspicious activity, such as spam or viruses originating from that address. It is strongly recommended to perform a security audit on any systems that has an IP address with a negative reputation, as those systems may have been compromised. Reputation scores are measured from 0 to 100 and greater the score, higher is the suspicious activity and the level of danger.

EventTracker uses the services provided by **EventTracker Threat Center**, **IP Void**, **IBM XFE and BorderWare** to locate the blacklisted IPs.

NOTE: Attackers Dashboard feature uses the following websites:

- **EventTracker Threat Center**
- **IP void**
- **IBM XFE**
- **BorderWare**

To get the data populated on the Dashboard, access needs to be provided for these websites. Ensure that the above URLs are excluded from the firewall.

2.2 Viewing the Dashboard

1. To view Dashboard, click the **Dashboard** icon and select **Threats** from the dropdown list.

   By default, the summary of the IPs is shown in map view, it can also be viewed in a Tabular format.

Depending on the service provider selected in the Manager Configuration, the Attackers are displayed.

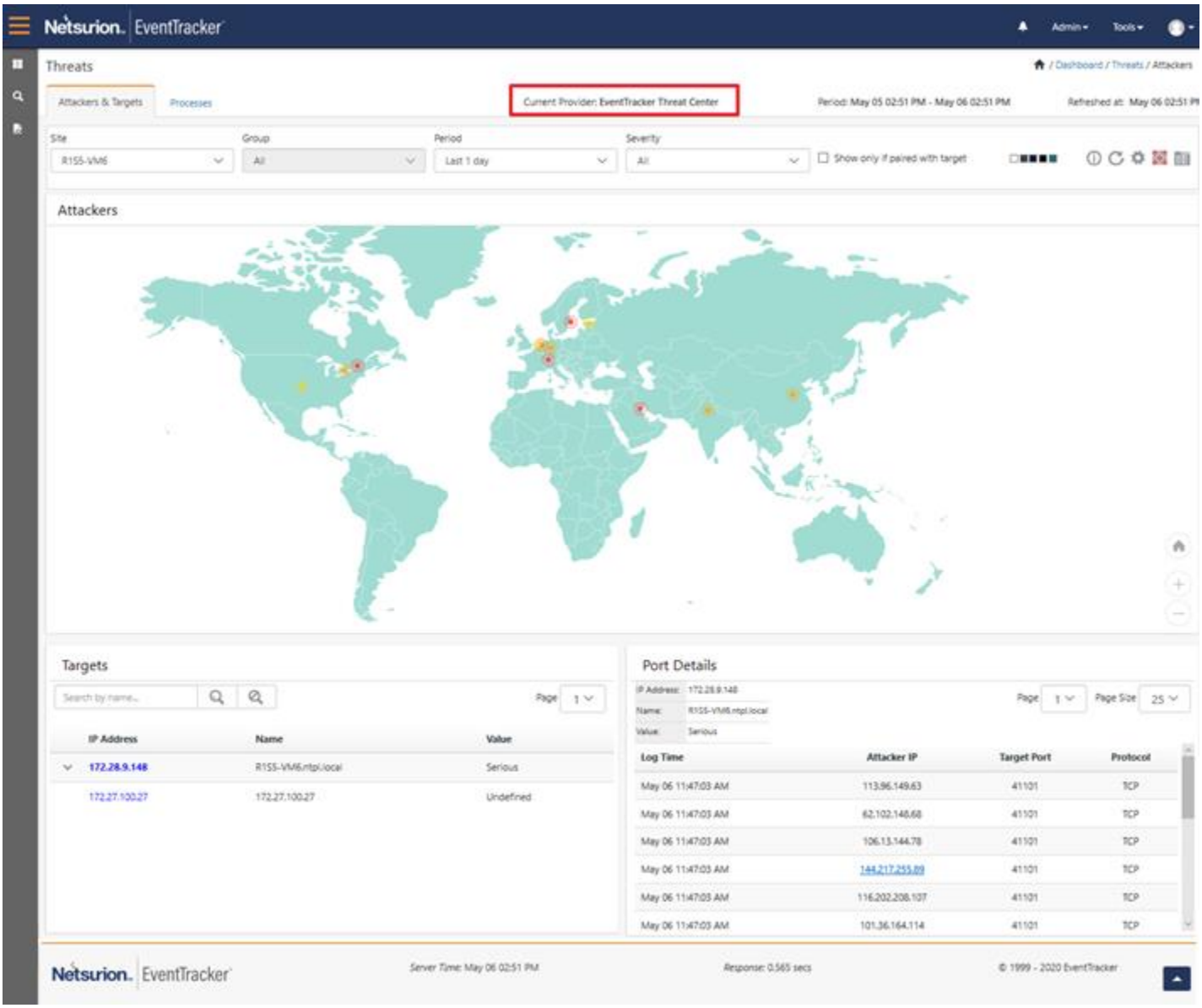


Figure 1

NOTE

The dashboard will populate data based on the default reputation service provider, i.e. EventTracker Threat Center. Once the user changes the service provider, the initial data will be intact and will continue populating data based on the new service provider, for the new IPs.

2. Enable the checkbox **Show only if paired with target** to display only the paired IPs in the dashboard.

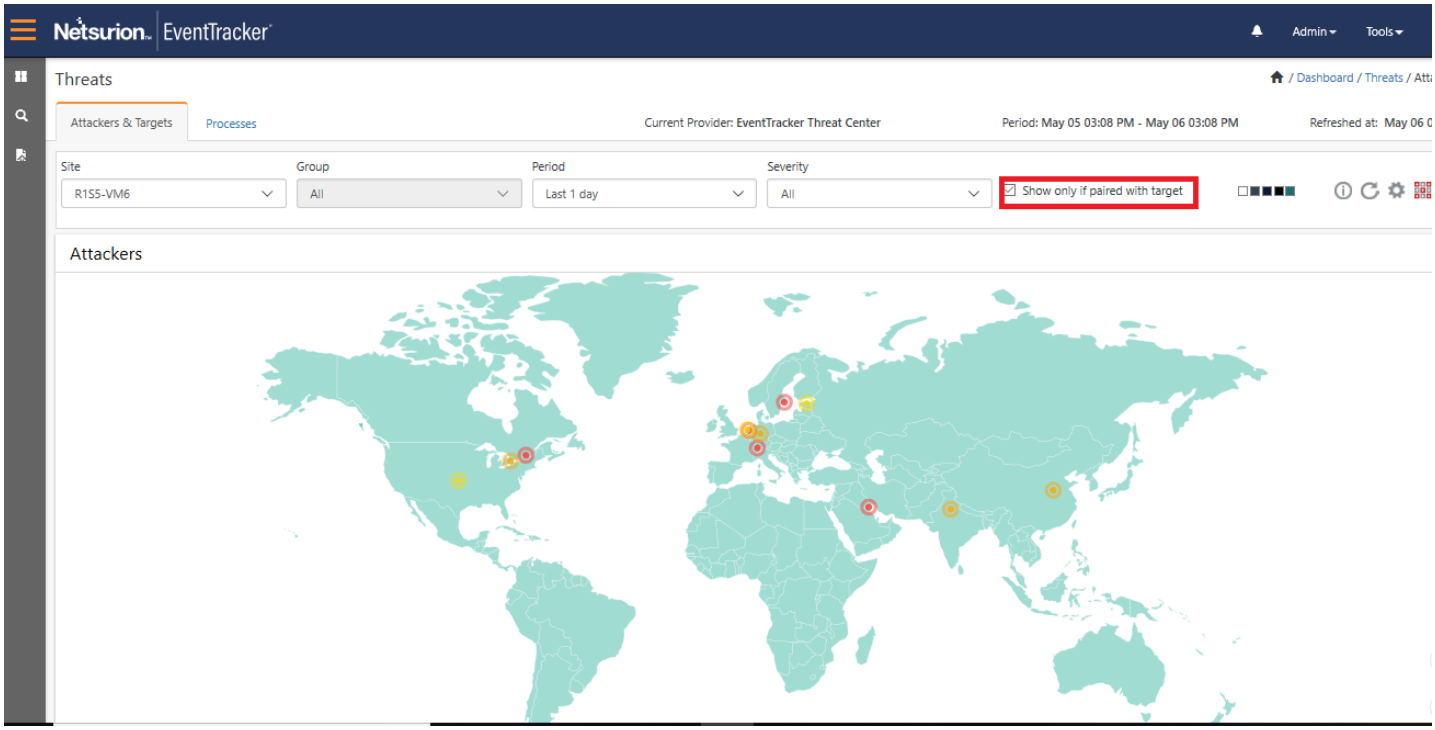


Figure 2

3. To get the information for the IP paired with the targets in a tabular format, enable the checkbox and select the Tabular icon . This is shown in the figure below:

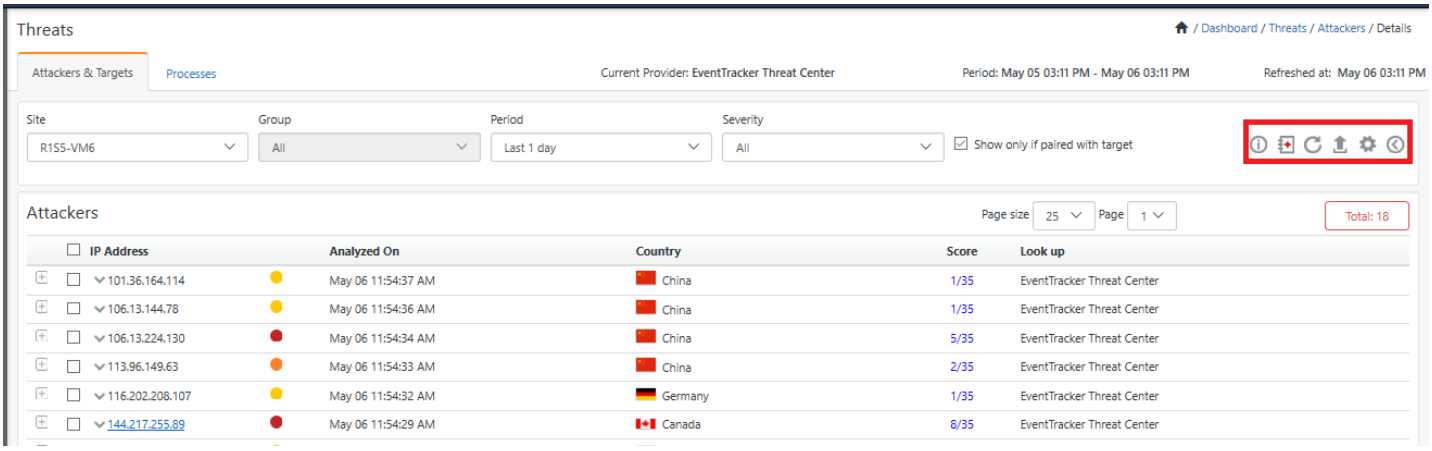


Figure 3

4. Click the Information icon to view the severity level of the different service providers. Severity implies the threat level of the IP Addresses, where the severity is calculated on the list.

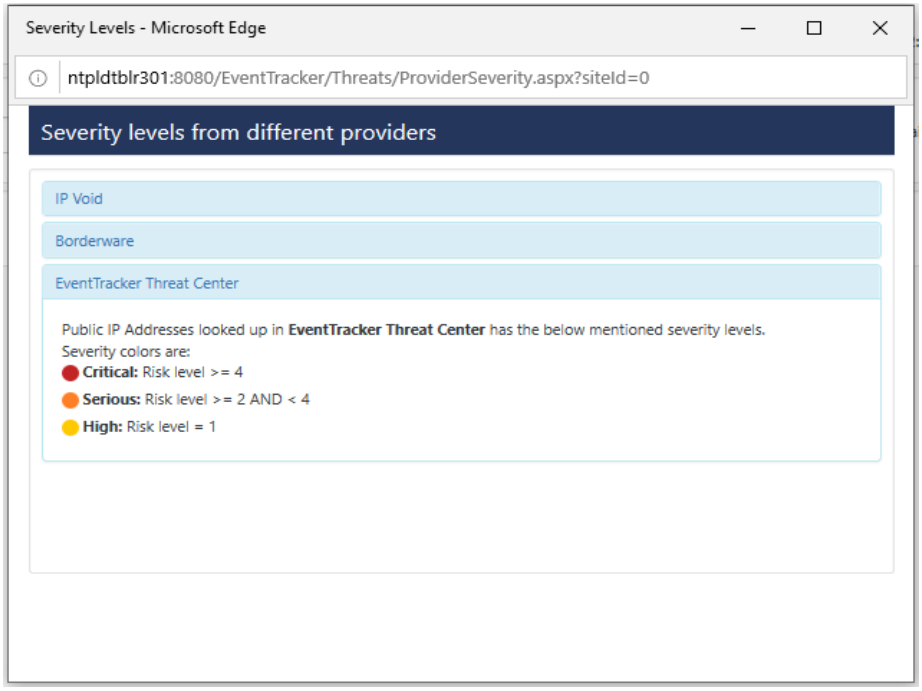


Figure 4

5. Select an IP address and click **Add** Casebook to add a New Casebook.
6. Click the icon to refresh the dashboard.
7. Click Export to export the details to Excel.

2.3 Getting information about the bad IP

1. To get the information about the bad IP, click on the lookup location, as shown in the figure below.

   For Service Provider, **EventTracker Threat Center** the following window appears.

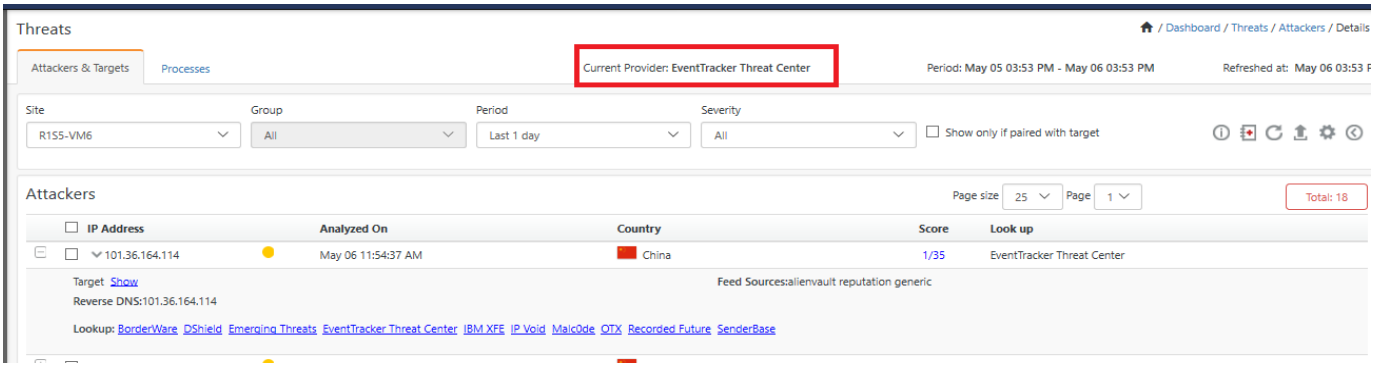


Figure 5

2. Click **Show** hyperlink.

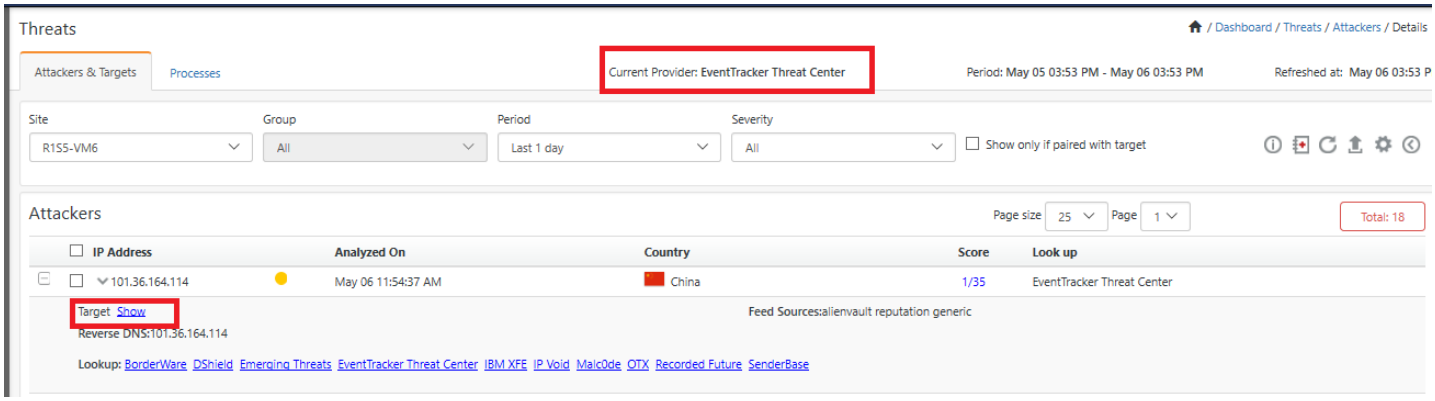


Figure 6

3. Target information page opens, and you can view the targets details.

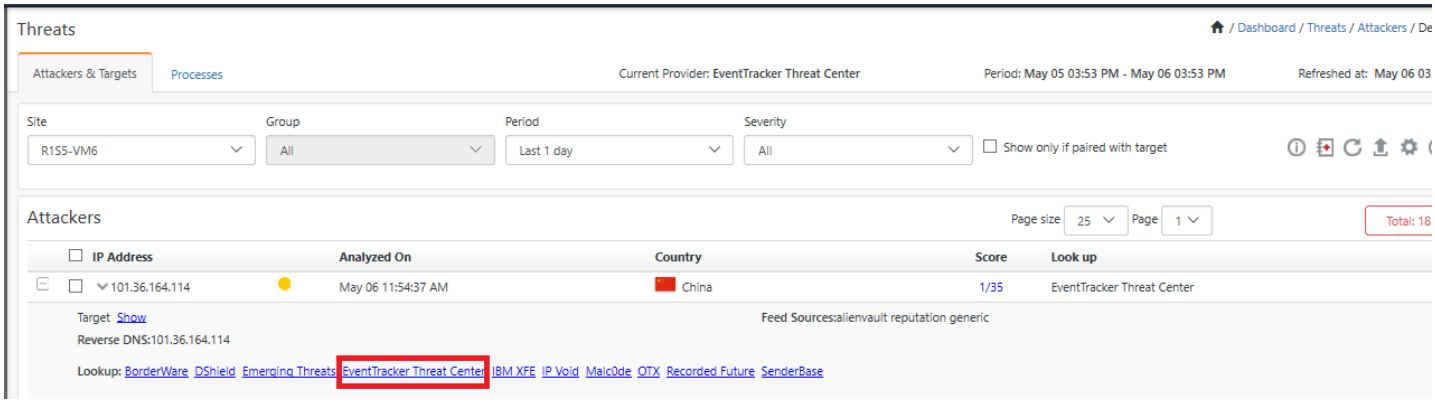


Figure 7

4. For more information on the IP, click on the respective **Lookup** provider hyperlink.

   Click EventTracker Threat Center hyperlink to view the EventTracker feed source details.

Figure 8

5. Click configuration icon ⚙, (fig 7) the following window appears. Click the **Threat Platform** option in the left pane.

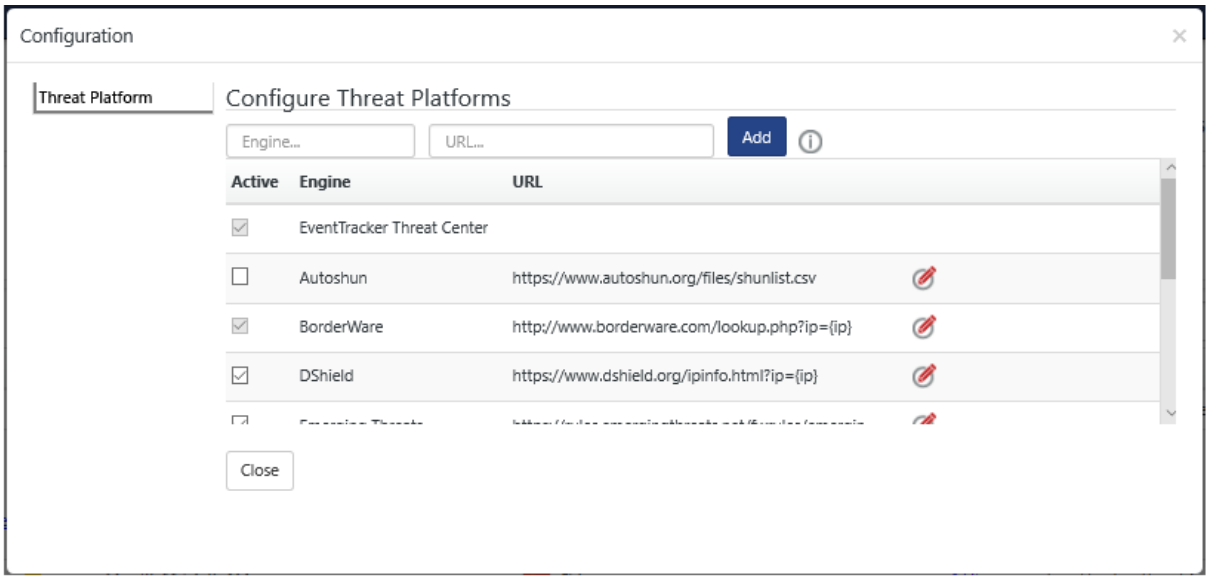


Figure 9

6. To custom add the threat Intelligence platforms add the name in the Engine Box and URL name in the URL box and click **Add**. (The user can also unselect checkbox from the engine list available.)

   A pop-up message displays. Click **OK**.

7. Click **Edit** , to edit Engine name.

8. Click **information** for more information.

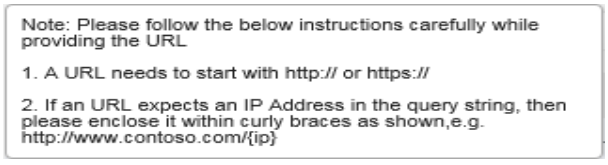


Figure 10

9. To get detailed information of the bad IPs, click Tabular view in the Attackers dashboard. The IPs are listed in a tabular format.

10. Click to view details about an IP.

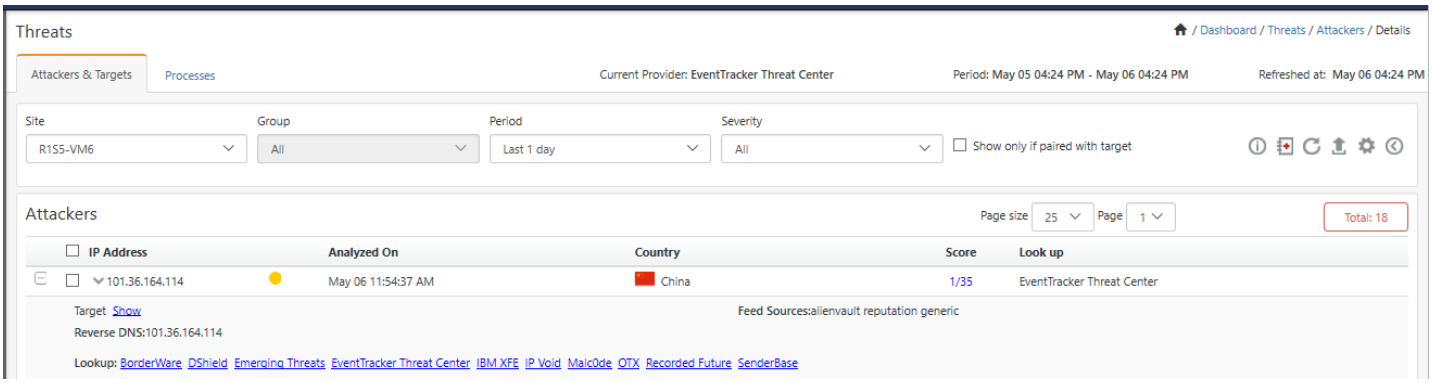
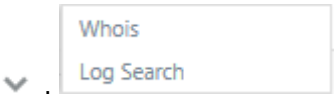


Figure 11

11. Click on the IP dropdown icon 

- Select the **WHOIS** option for more information on the IP.
- Select **Log Search**, for performing a search.

2.4 Targets pane

With the advent of the feature “Attackers” where the bad reputation IPs are pinned on the geolocation, it becomes necessary to display the information as to where these bad IPs have ventured into the network. The targets feature will suffice the requirement, displaying those targets within the enterprise which are being attacked, along with the details like-How (Port/Protocol), By Whom (IP/Host Name) and When/ How often.

There are two different ways of looking at same pair table data. The user can view it from the attacker dashboard - "who is attacking/how/what port" or from the targets dashboard- "what is being attacked/by who/which port".

In both the cases, user plays the defender job where he/she can protect the assets, react in a timely way and defend in a proper manner.

For Geo-location, EventTracker is using the **MaxMind GeoLite**.

1. For viewing the targets that has been attacked, scroll down to the **Targets** pane, shown in the figure 13. The Targets are in the left pane and the Port details are in the right pane.

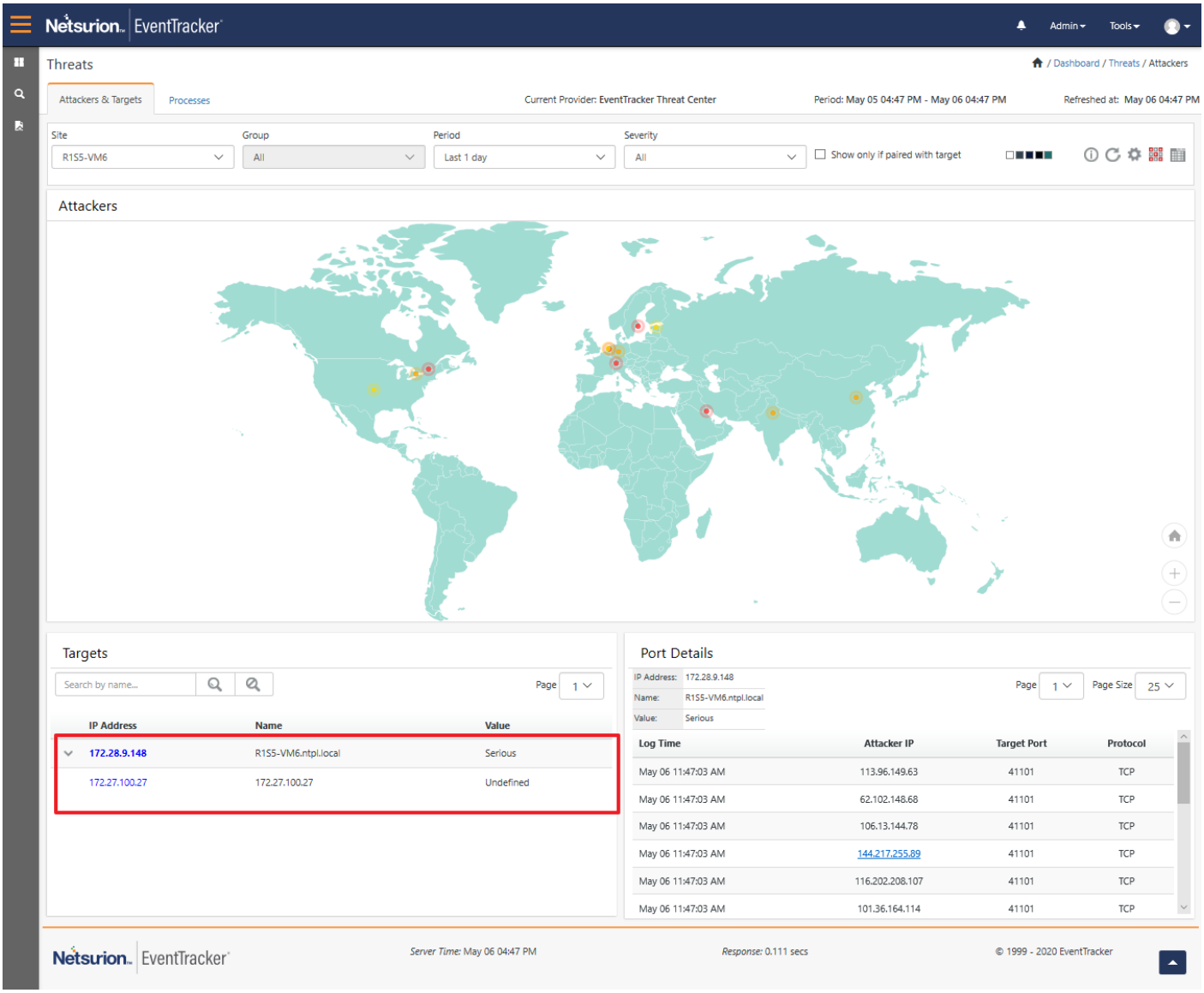


Figure 12

2. Click the icon to view the Target data details.

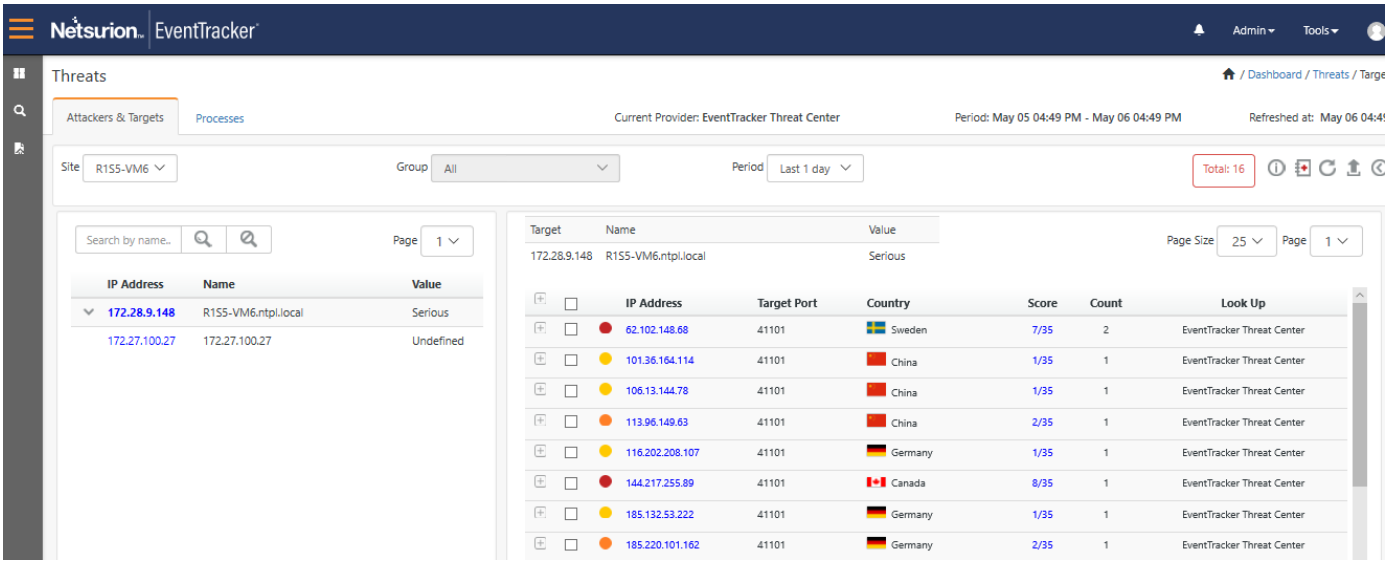


Figure 13

The targets show the attacks on the systems in the form of a pair table. The left pane will list down the multiple targets with their asset value and host name (if any). The respective attackers are listed in the right pane along with the critical reputation information.

3. Click on the icon ⊞ in the right pane, to view more information related to the attackers in the Target dashboard.

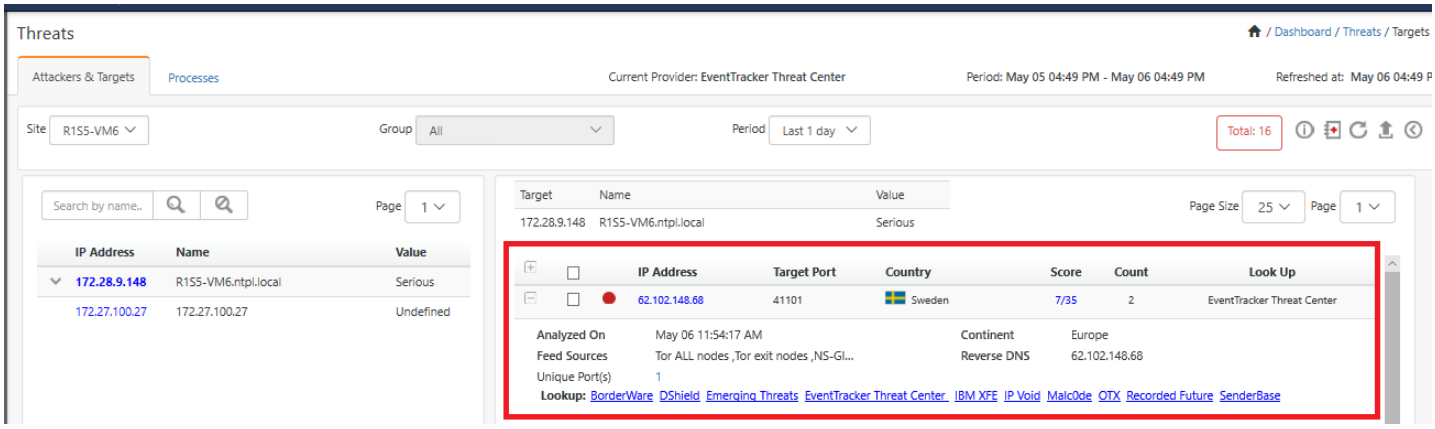


Figure 14

The user can further perform a Log Search Pair/Log Search Target for a respective target.

4. Click **Export** ⬆ to save the target information in Excel.

Attackers

Site: R1S5-VM6
Group: All
Period: May 04 01:45 PM - May 07 01:45 PM
Severity: All
Current Provider: EventTracker Threat Center

Reverse DNS	IPAddress	Latitud	Longit	City	Countrg	CountrgCode	Continent	Analgzed On	Score	Provider
111-253-9-123.dynamic-ip.hinet.net.	111.253.9.123	24.1469	120.6839	Taichung	Taiwan	TW	Asia	May 05 01:11:53 PM	70	100
static.vnpt.vn.	113.169.138.45	16.0023	105.9999	Unknown	Vietnam	VN	Asia	May 05 01:16:54 PM	70	100
static.vnpt.vn.	113.179.239.142	21.0313	105.8516	Hanoi	Vietnam	VN	Asia	May 05 01:17:53 PM	70	100
dynamic-ip-adsl.viettel.vn.	116.101.46.60	16.0023	105.9999	Unknown	Vietnam	VN	Asia	May 05 01:17:54 PM	70	100
localhost.	117.0.13.7	21.2467	106.1158	Hoang Mai	Vietnam	VN	Asia	May 05 01:17:55 PM	70	100
none	117.198.19.56	21.2092	81.428497	Bhilai	India	IN	Asia	May 05 01:17:56 PM	70	100

Figure 15

List of URLs for firewall proxy exclusion

1. https://api.xforce.ibmcloud.com/
2. http://ipinfo.io/

In Attackers,

1. http://www.ipvoid.com/
2. http://list.iblocklist.com/
3. http://www.borderware.com/
4. https://www.dshield.org/
5. https://rules.emergingthreats.net/
6. https://www.autoshun.org/files/
7. https://otx.alienvault.com/
8. https://www.senderbase.org/
9. http://certificates.eventtracker.com/
10. EventTracker Threat center