User Guide

The Netsurion Open XDR platform's Threats Dashboard

Publication Date:

March 30, 2023

Abstract

This guide facilitates to understand the Netsurion Open XDR platform's Threats Dashboard to detect suspicious activity, such as spam or viruses originating from the IP address.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Audience

This guide is intended for all the Netsurion Open XDR platform users responsible for investigating and managing network security.

Product Terminology

The following are the terms used throughout this guide:

- The term "Netsurion's Open XDR platform" or "the Netsurion Open XDR platform" or "the Open XDR platform" refers to EventTracker.
- The term "Data Source Integrations" refers to Knowledge Packs.
- The term "Netsurion Threat Center" refers to EventTracker Threat Center.

Table of Contents

1 Netsurion Threat Center

The Open XDR platform provides the Netsurion Threat Center Platform which is an alternate IP reputation provider. The Netsurion Threat Center is a repository of threat indicators. It accumulates a series of different threat feeds, gathers information about IP addresses, scans an IP address with multiple IP unsafe lists and finds security threats. The Netsurion Threat Center is used as an alternate IP reputation provider and is maintained by Netsurion. The Netsurion Threat Center Platform is an alternate Hash reputation provider that determines the badness/reputation of the Hash. It accumulates a series of different threat feeds, gathers information about the Hash details, scans the detected Hash value with multiple other Hash details to find the security threats.

2 Attackers and Targets dashboard

2.1 Attacker pane

The Attackers Dashboard option helps to view the Top 20 geographic location pins. Each of these top 20 pins may contain an '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 have an IP address with a negative reputation, as those systems may have been compromised. Reputation scores are measured from 0 to 100 and the greater the score, the higher the suspicious activity and the level of danger.

The Netsurion Open XDR platform uses the services provided by **Netsurion Threat Center,** and **IBM XFE** to locate the unsafe listed IPs.

Note:

Attackers Dashboard feature uses the following websites:

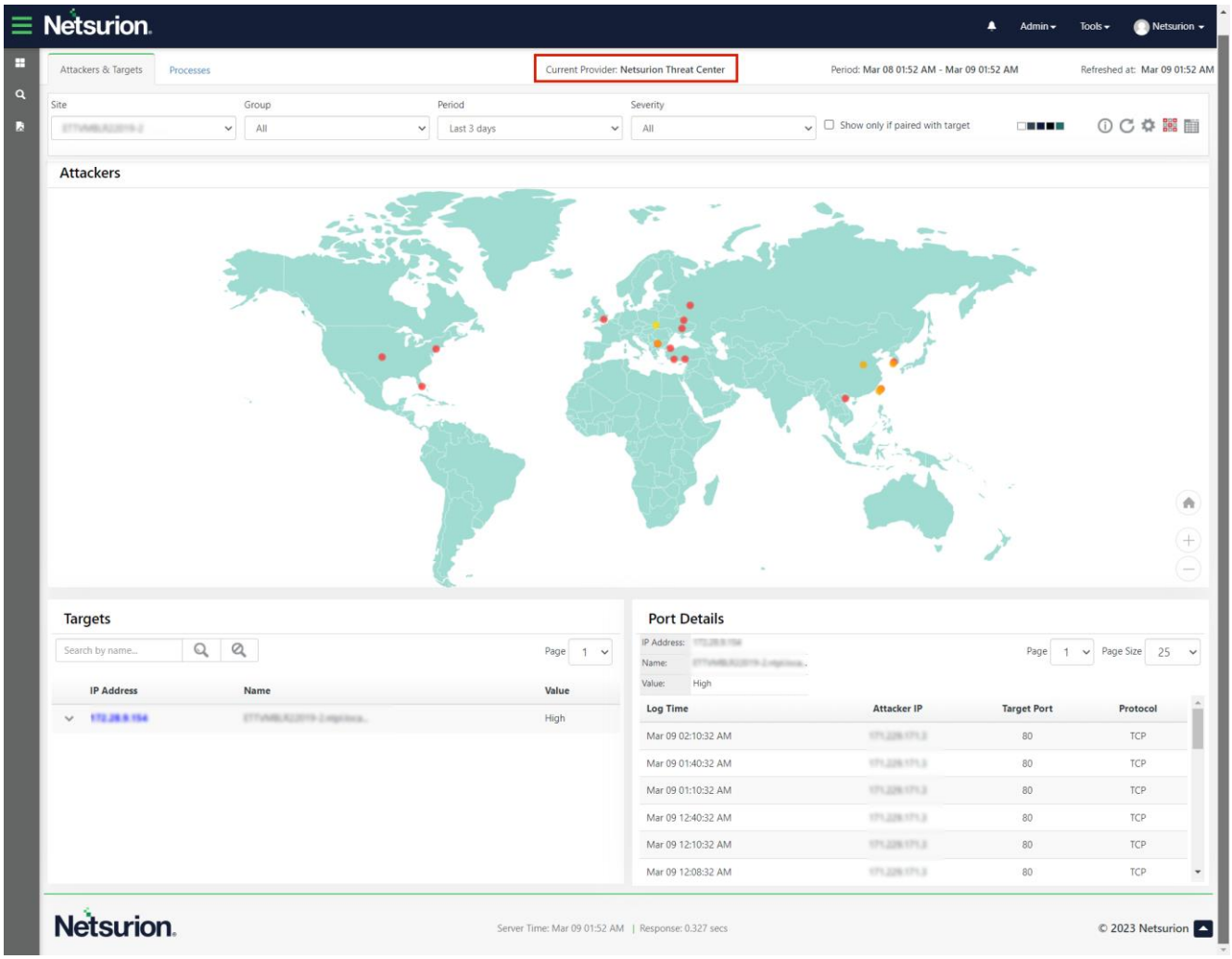
- **Netsurion Threat Center**
- **IBM XFE**

Access must be made available for these websites in order to populate the data on the Dashboard. Ensure that the above URLs are excluded from the firewall.

2.2 Viewing the Dashboard

1. In the Open XDR platform, click the **Dashboard** icon and click **Threats** from the dropdown list to go to the **Attackers & Targets** interface. By default, each IP's summary will be displayed in map view, wherein it can also be viewed in a Tabular format.

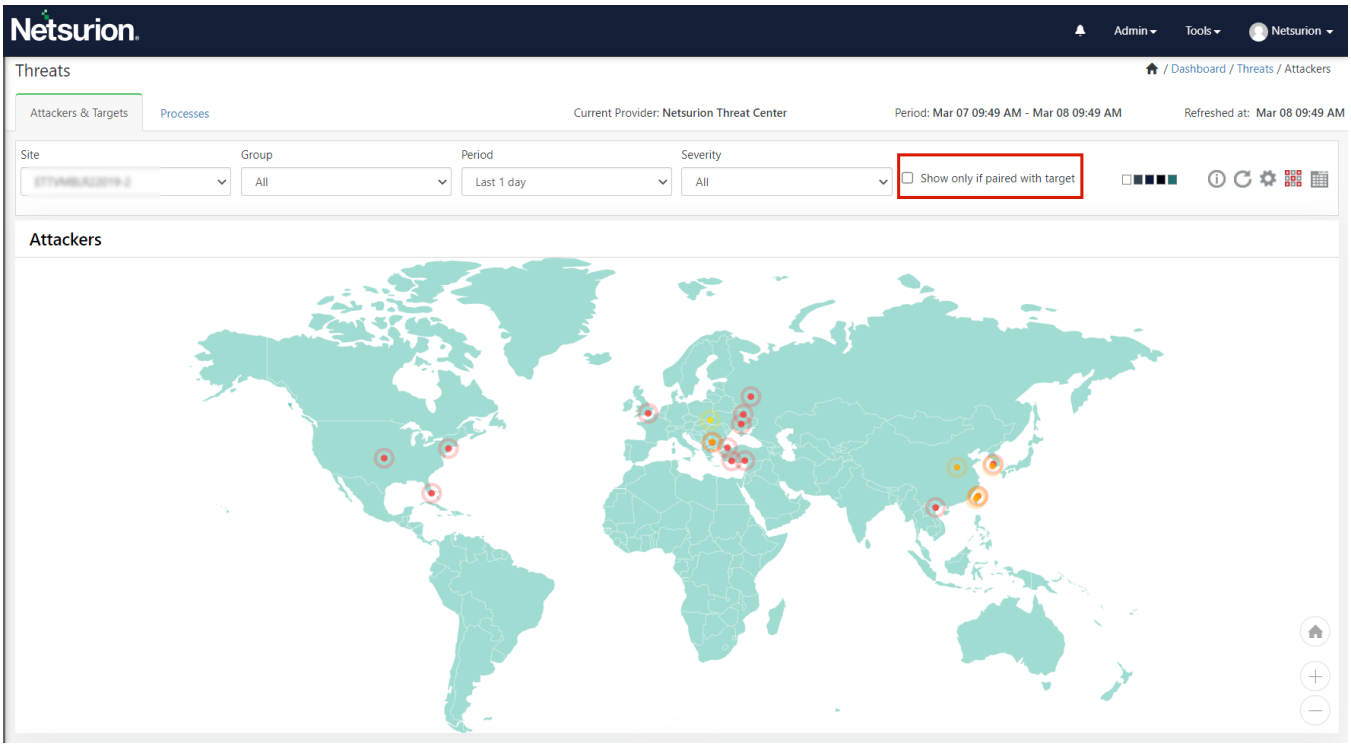
Depending on the selected service provider in the Manager Configuration, the details of the Attackers will be displayed.



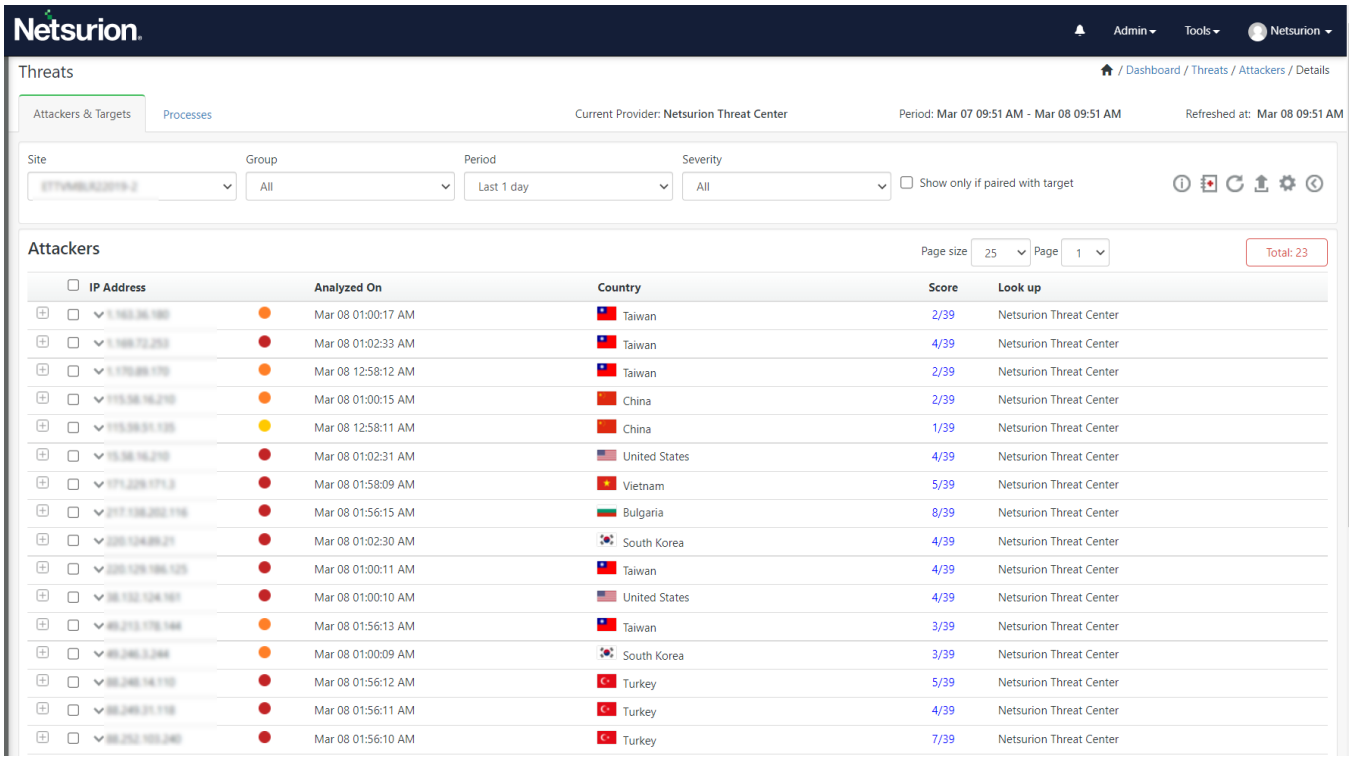
Note:

The dashboard populates data based on the default reputation service provider, that is, Netsurion 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.

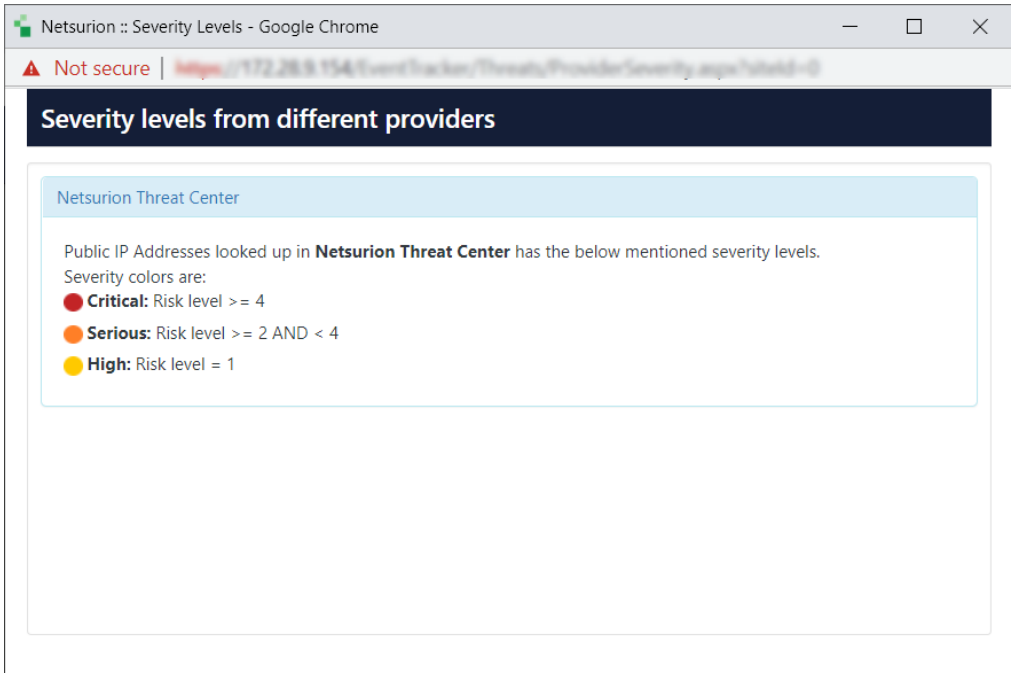
2. Select the **Show only if paired with target** check box to display only the paired IPs in the dashboard and click the Tabular icon to get the information for the IP paired with the targets in a tabular format.



3. Then, click the **Information** icon to view the severity level of the different service providers.



The threat level of the IP addresses is implied by severity, and the severity is defined on the list.

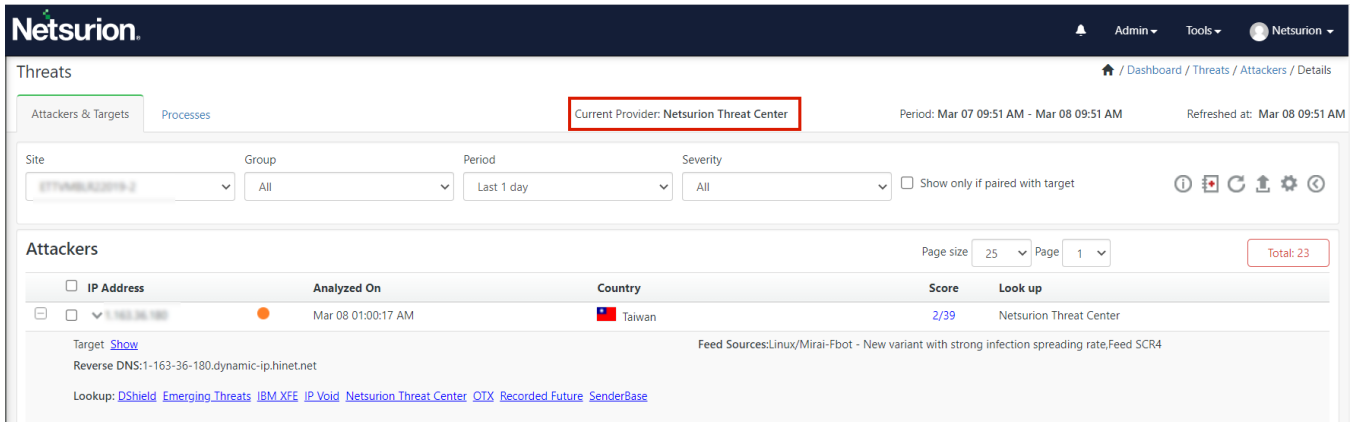


4. Select an IP address from the list and click **Add** Casebook to add a New Casebook to investigate a particular issue.
5. Click the **Refresh** icon to refresh the dashboard.
6. Click **Export** to export the details to Excel.

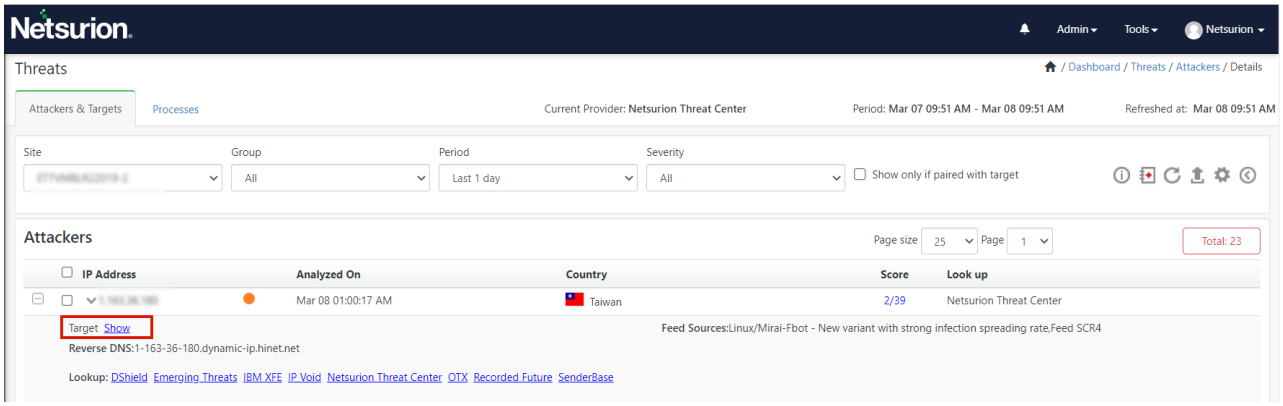
2.3 Getting information about bad IP

1. In the **Attackers** section, click **Lookup** to get the information about the bad IP.

Based on the Service Provider, the following window appears in the **Netsurion Threat Center**.

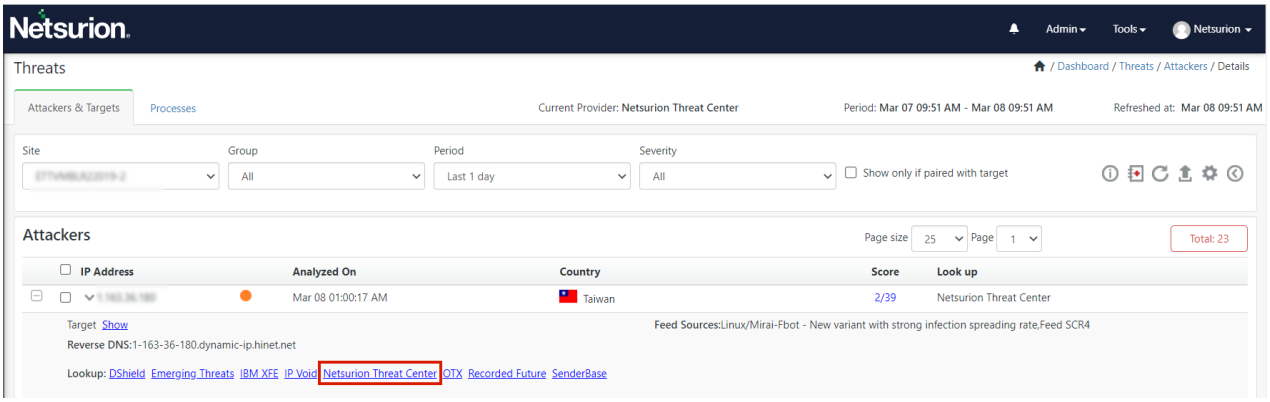


2. Click **Show** hyperlink.

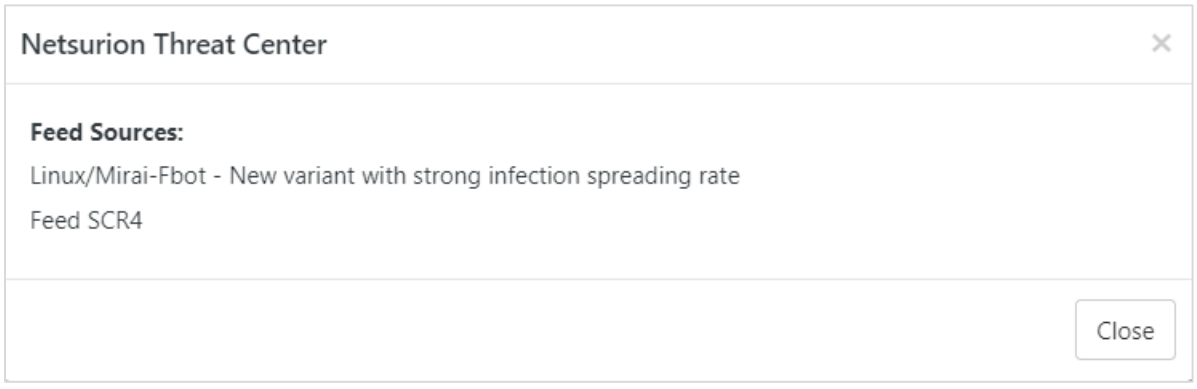


Target information page will be displayed, and you can view the targets details.

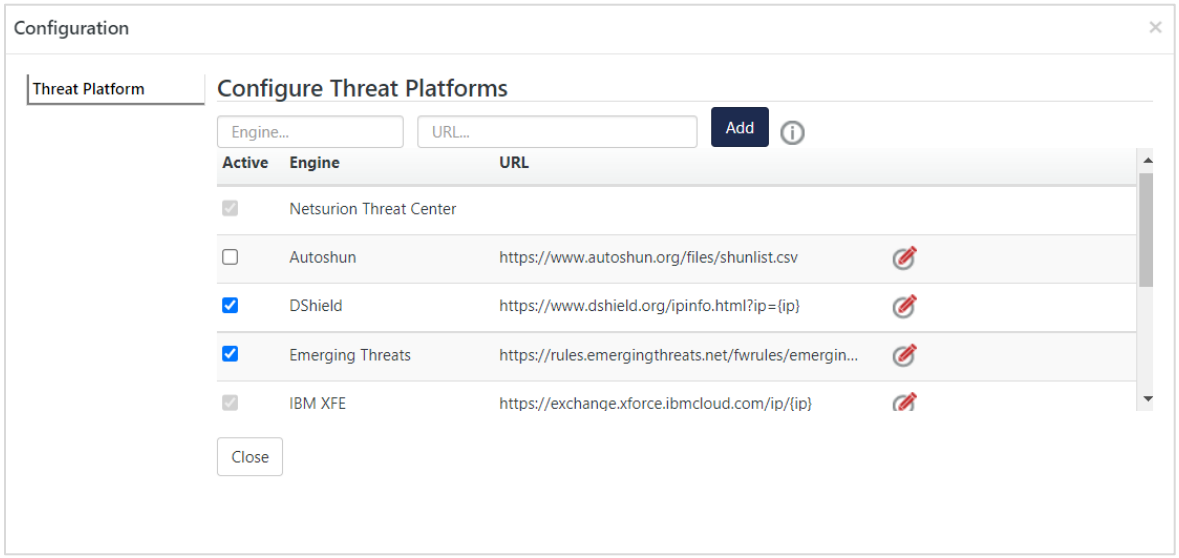
3. Click on the respective **Lookup** provider hyperlink for more information on the IP.



4. Click **Netsurion Threat Center** hyperlink to view the Netsurion feed source details.



5. In the **Attackers & Targets** tab, click the configuration icon, and click the **Threat Platform** option in the left pane.

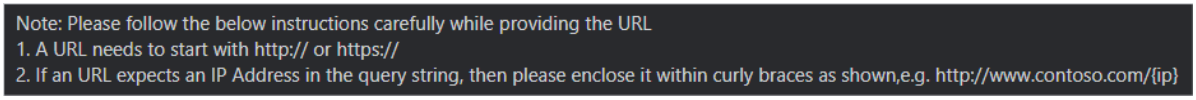


6. To custom add the threat Intelligence platforms, add the name in the Engine Box and URL name in the URL box and click **Add**. (The user can also deselect the checkbox from the available engine list.)

7. A pop-up message appears. Click **OK**.

8. Click **Edit**, to edit the Engine name.

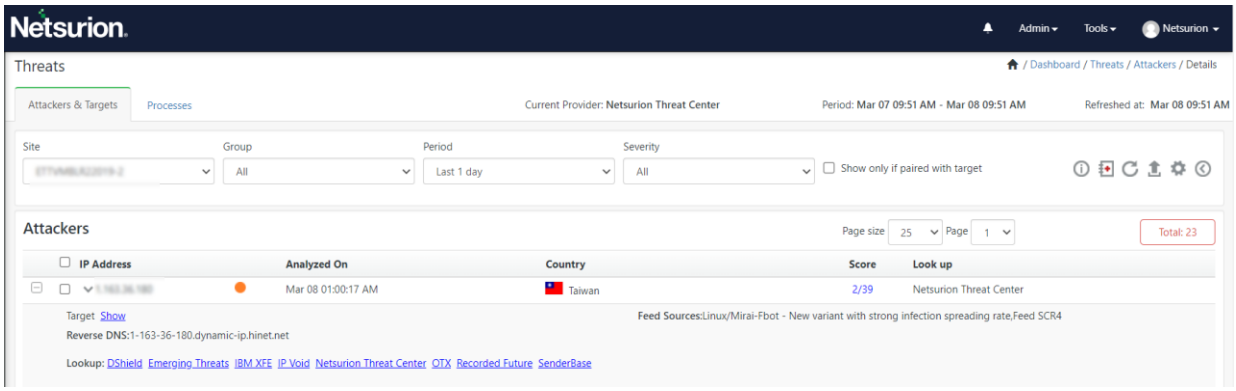
9. Click the **information** icon for more information.



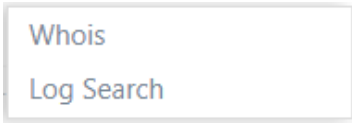
10. In the **Attackers** dashboard click the Tabular view icon to get detailed information on the bad IPs.

Here, the IPs will be listed in a tabular format.

11. Click the **Expand** ⊞ icon to view the IP details.



12. Click the **IP dropdown** ⌄ icon located next to each IP Address, and either select the **Whois** for more information on the IP or select **Log Search** to perform 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.

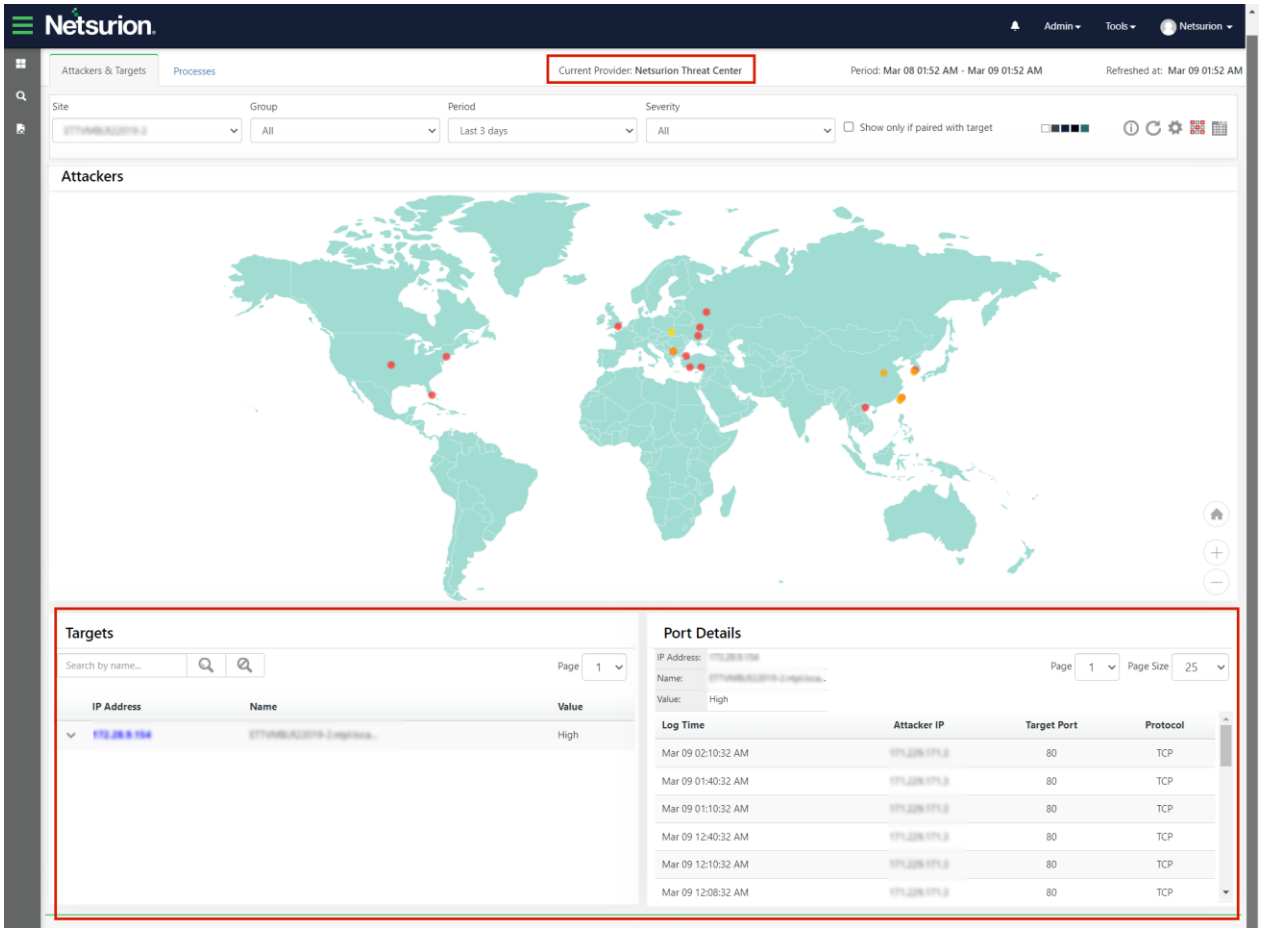
There are two ways of looking at the same pair table data. The user can view it from the attacker dashboard - "who is attacking/ how/ what port" or from the **Targets** dashboard- "what is being attacked/ by who/ which port".

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

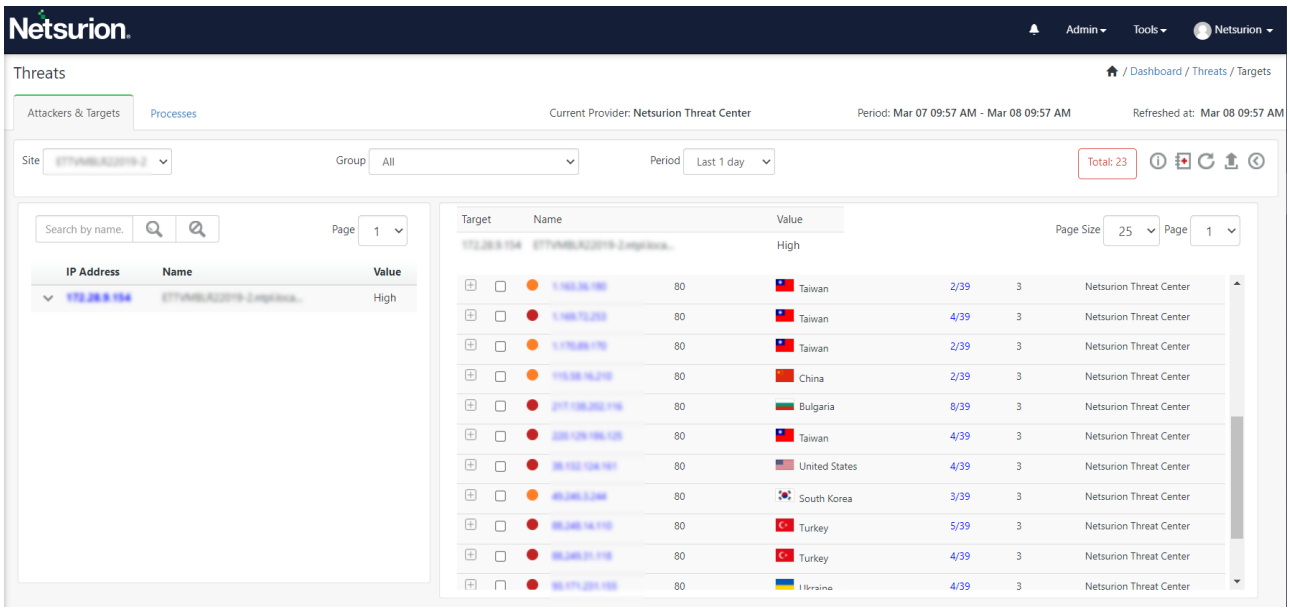
For Geo-location, the Netsurion Open XDR platform uses the **MaxMind GeoLite**.

1. In the Threats interface, scroll down to the **Targets** pane to view the targets that are attacked.

Here, Targets are in the left pane and the Port details are in the right pane.

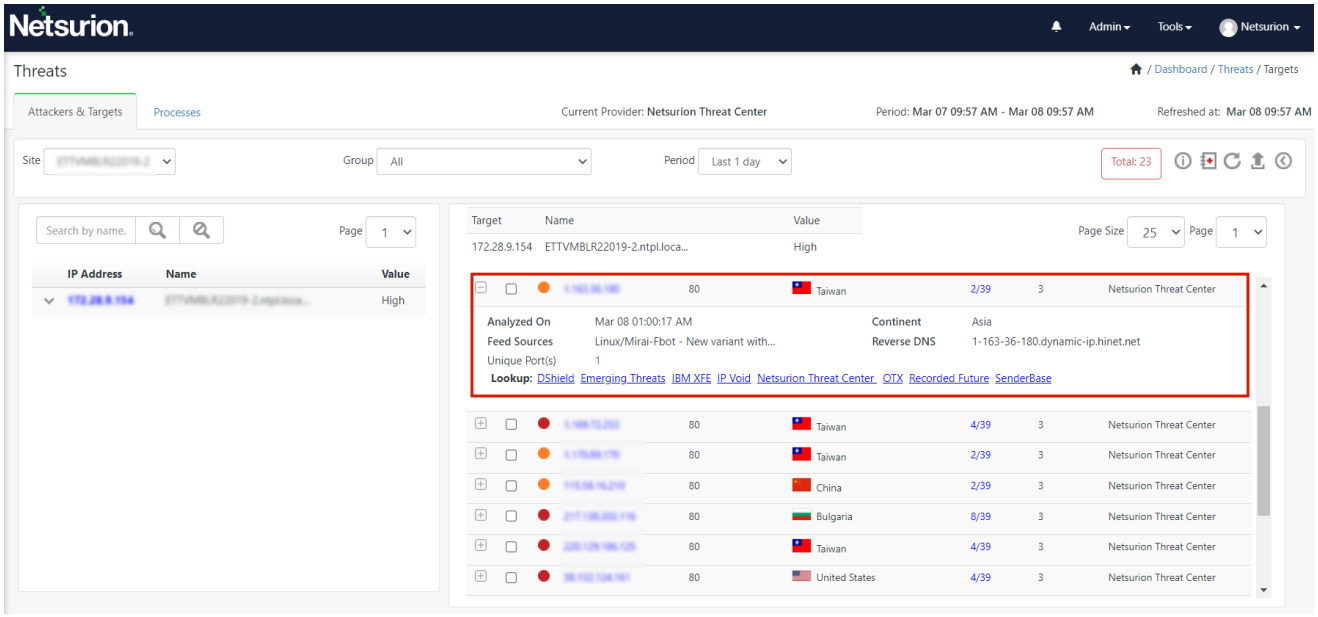


2. Within the **Attackers & Targets** tab, click the **View targets data** icon to view the Target data details.



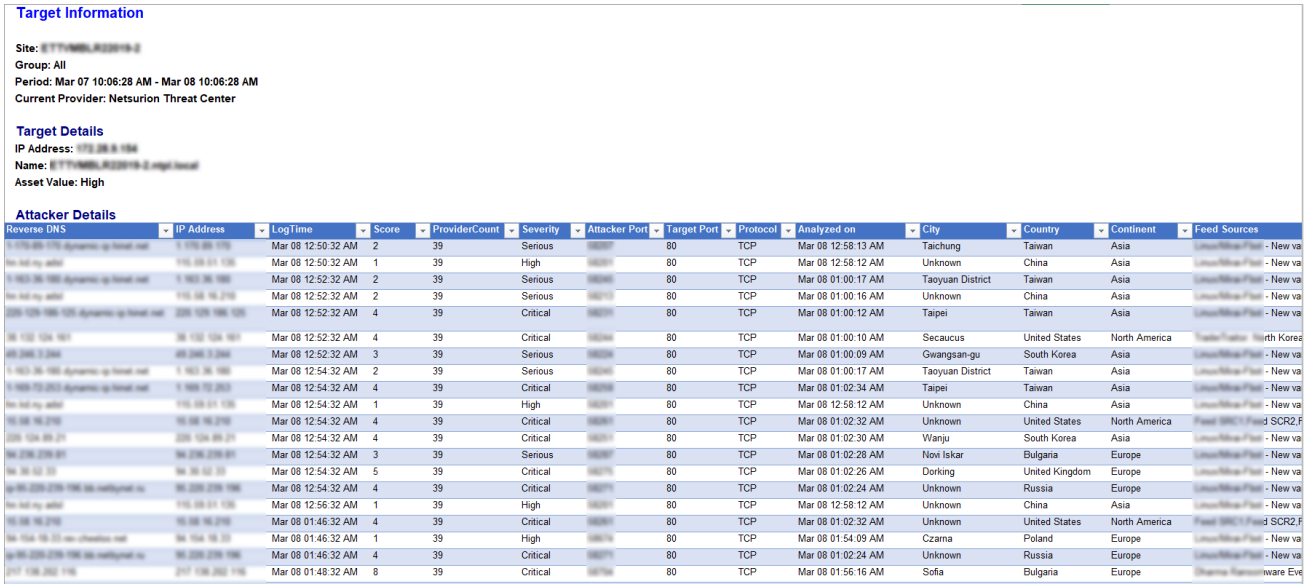
The targets show the attacks on the systems in the form of a pair table. The left pane will list down the multiple targets with their asset value and host name (if any). The respective attackers are listed in the right pane along with the critical reputation information.

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



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

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



Target Information

Site: [redacted]
Group: All
Period: Mar 07 10:06:28 AM - Mar 08 10:06:28 AM
Current Provider: Netsurion Threat Center

Target Details
IP Address: [redacted]
Name: [redacted]
Asset Value: High

Attacker Details

Reverse DNS	IP Address	LogTime	Score	ProviderCount	Severity	Attacker Port	Target Port	Protocol	Analyzed on	City	Country	Continent	Feed Sources
[redacted]	[redacted]	Mar 08 12:50:32 AM	2	39	Serious	[redacted]	80	TCP	Mar 08 12:58:13 AM	Taichung	Taiwan	Asia	[redacted] - New va
[redacted]	[redacted]	Mar 08 12:50:32 AM	1	39	High	[redacted]	80	TCP	Mar 08 12:58:12 AM	Unknown	China	Asia	[redacted] - New va
[redacted]	[redacted]	Mar 08 12:52:32 AM	2	39	Serious	[redacted]	80	TCP	Mar 08 01:00:17 AM	Taoyuan District	Taiwan	Asia	[redacted] - New va
[redacted]	[redacted]	Mar 08 12:52:32 AM	2	39	Serious	[redacted]	80	TCP	Mar 08 01:00:16 AM	Unknown	China	Asia	[redacted] - New va
[redacted]	[redacted]	Mar 08 12:52:32 AM	4	39	Critical	[redacted]	80	TCP	Mar 08 01:00:12 AM	Taipei	Taiwan	Asia	[redacted] - New va
[redacted]	[redacted]	Mar 08 12:52:32 AM	4	39	Critical	[redacted]	80	TCP	Mar 08 01:00:10 AM	Secaucus	United States	North America	[redacted]
[redacted]	[redacted]	Mar 08 12:52:32 AM	3	39	Serious	[redacted]	80	TCP	Mar 08 01:00:09 AM	Gwangsan-gu	South Korea	Asia	[redacted] - New va
[redacted]	[redacted]	Mar 08 12:54:32 AM	2	39	Serious	[redacted]	80	TCP	Mar 08 01:00:17 AM	Taoyuan District	Taiwan	Asia	[redacted] - New va
[redacted]	[redacted]	Mar 08 12:54:32 AM	4	39	Critical	[redacted]	80	TCP	Mar 08 01:02:34 AM	Taipei	Taiwan	Asia	[redacted] - New va
[redacted]	[redacted]	Mar 08 12:54:32 AM	1	39	High	[redacted]	80	TCP	Mar 08 12:58:12 AM	Unknown	China	Asia	[redacted] - New va
[redacted]	[redacted]	Mar 08 12:54:32 AM	4	39	Critical	[redacted]	80	TCP	Mar 08 01:02:32 AM	Unknown	United States	North America	[redacted]
[redacted]	[redacted]	Mar 08 12:54:32 AM	4	39	Critical	[redacted]	80	TCP	Mar 08 01:02:30 AM	Wanju	South Korea	Asia	[redacted] - New va
[redacted]	[redacted]	Mar 08 12:54:32 AM	3	39	Serious	[redacted]	80	TCP	Mar 08 01:02:28 AM	Novi Iskar	Bulgaria	Europe	[redacted] - New va
[redacted]	[redacted]	Mar 08 12:54:32 AM	5	39	Critical	[redacted]	80	TCP	Mar 08 01:02:26 AM	Dorking	United Kingdom	Europe	[redacted] - New va
[redacted]	[redacted]	Mar 08 12:54:32 AM	4	39	Critical	[redacted]	80	TCP	Mar 08 01:02:24 AM	Unknown	Russia	Europe	[redacted] - New va
[redacted]	[redacted]	Mar 08 12:56:32 AM	1	39	High	[redacted]	80	TCP	Mar 08 12:58:12 AM	Unknown	China	Asia	[redacted] - New va
[redacted]	[redacted]	Mar 08 01:46:32 AM	4	39	Critical	[redacted]	80	TCP	Mar 08 01:02:32 AM	Unknown	United States	North America	[redacted]
[redacted]	[redacted]	Mar 08 01:46:32 AM	1	39	High	[redacted]	80	TCP	Mar 08 01:54:09 AM	Czarna	Poland	Europe	[redacted] - New va
[redacted]	[redacted]	Mar 08 01:46:32 AM	4	39	Critical	[redacted]	80	TCP	Mar 08 01:02:24 AM	Unknown	Russia	Europe	[redacted] - New va
[redacted]	[redacted]	Mar 08 01:48:32 AM	8	39	Critical	[redacted]	80	TCP	Mar 08 01:56:16 AM	Sofia	Bulgaria	Europe	[redacted]

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. https://www.dshield.org/
4. https://rules.emergingthreats.net/
5. https://www.autoshun.org/files/
6. https://otx.alienvault.com/
7. https://www.senderbase.org/
8. http://certificates.eventtracker.com/
9. Netsurion Threat center

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's managed offering includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers Managed Threat Protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection and Response (MDR) and a Top 25 Global MSSP. Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Direct Enterprise	SOC@Netsurion.com	1 (877) 333-1433 Option 1, Option 1
MSP Enterprise	SOC-MSP@Netsurion.com	1 (877) 333-1433 Option 1, Option 2
Essentials	Essentials-Support@Netsurion.com	1 (877) 333-1433 Option 1, Option 3
Self-Serve	EventTracker-Support@Netsurion.com	1 (877) 333-1433 Option 1, Option 4

https://www.netsurion.com/eventtracker-support