Threat Control System User Guide 5.0.1

November, 2024

Table of Contents

Getting Started

Introduction

Organizations face innumerable security threats of several types. Any security software or hardware may have vulnerabilities, or the attackers may develop new ways of breaching the security layers using weapons such as DDoS, ransomware, malware, and new emerging cyber threats. If the organizations have a clear picture of these attacks, they can mitigate the risks and implement the necessary solutions to prevent future threats.

With Threat Control System, Organization provides in-depth descriptive analytics on security attacks occurring across security devices and networks in real time.

Threat Control System is a centralized threat intelligence platform. It collects, processes, and analyzes data on security threats in different organizations based on different parameters. Threat Control System helps to investigate security threats and vulnerabilities in the organizations where network security solutions are implemented.

Security analysts can analyze weapons, motives, targets, and behavior of the attackers. Such analysis helps to create an actionable plan for an organization. Additionally, it is designed to work with the existing infrastructure enabling you to implement threat-prevention solutions.

The threats are analyzed based on the following factors:

- Attack types
- Autonomous System Numbers (ASN)
- Countries
- Sectors

Key Features

Threat Control System empowers security analysts with the following benefits:

- Read the security breaches and attacks on all security devices and networks in real time.
- Investigate the attacks, vulnerabilities, security threats, and malicious actors and their behavior.
- Analyze the implications of security threats and breaches, indicators of compromise (IOCs), indicators of attacks (IOAs), and threat complexity.
- Respond to the security threats on time before they leave an impact.
- Plan pertinent actions and security measures to prevent threats in future.
- Proactively create a security system to reduce the security risks.
- Download the threat analysis report to share with the responsible stakeholders.

System Requirements

Threat Control System is a web-based portal. The web portal can run on any latest browser including,

- Microsoft Edge
- Google Chrome
- Mozilla Firefox

Login to Threat Control System Application

Logging using Single Sign On (SSO)

To log in to the Threat Control System portal using Single Sign On (SSO) with Azure IDP or Okta IDP:

1. Go to www.defend.a10networks.com.
2. Enter the organization name and click **Next**.

NOTE: The organization name is the name of the entity that purchases the threat insight intelligence application.

3. Enter your corporate email address and click **Next**.
4. Enter your corporate password and click **Sign In**.
5. Click **Yes**.

Logging using Organization's Keycloak

To log in to the Threat Control System portal using the Organization's Keycloak IDP:

1. Go to www.defend.a10networks.com.
2. Enter the organization name and click **Next**.

NOTE: The organization name is the name of the entity that purchases the threat insight intelligence application.

3. Enter your username or email address, password, and then click **Sign In**.
4. Click the product name to enter the Threat Control System application.

Dashboard

After logging in to Threat Control System, the default Dashboard menu presents various threat analytics widgets and components.

Dashboard displays all the attack analytics occurring across organizations in different countries in real time as per the default setting. However, you can customize the Search Widgets to zero in on your analysis according to the requirement of your organization, country, or other factors. Using these attributes, you can analyze the attacks on the security weapons more effectively and take the required actions to minimize the security risks on time.

You can generate and download reports in PDF format based on your search attributes. You can also share the reports with the respective stakeholders for further analysis and for designing a mitigation plan.

Menu Options

The following GUI menu options are available on the dashboard:

Table 1 : Threat Control System Menu

Menu	Description
Dashboard	Allows you to customize and view the attack analytics happening in real time.
Attack Research	Allows you to customize and view the incident analytics based on the IP address, organization, attack type, country, and duration. This menu includes the following sub-menus: • **Attack Victims** — Displays all the attacks. • **Weaponized Nodes** — Allows you to search an attack by an IP address and network. • **Traffic Analysis** — Allows you to analyze the PCAP files and give insights of the attacks on a network. For more information, see Attack Research.

Table 1 : Threat Control System Menu

Menu	Description
Weapons & Activities	Allows you to customize and view the reports based on the incidents of various attributes. This menu includes the following sub-menus: • **Summary** — Includes a summary of trending attacks. • **Reflectors** — Includes a report on DDoS weapons. • **Botnets** — Includes a report on botnet tools. • **IOCs** — Includes a report on indicators of compromises (IOC). For more information, see Weapons & Activities.
Alerts	Allows you to view all the alerts generated, create rules for triggering alerts and send email notifications for the incidents. This menu includes the following sub-menus: • **Generated Alerts** — Displays all the alerts generated till date. • **Alert Configuration** — Allows you to create rules for generating alerts and sending email notifications. • **Triggers** — Allows you to create rules for generating triggers. For more information, see Alerts.
IP Block List	Allows you to view and download all IP addresses that have been attacked and are currently under attacks. Such IP addresses are blocked to prevent malicious attacks in future. This menu includes the following sub-menus: • **IP Block List** — Displays all the IP blocklists added on your security device. • **Custom IP Block List** — Displays all the curated

Table 1 : Threat Control System Menu

Menu	Description
	IP blocklists that you added for specific reasons. For more information, see IP Block List.
Reports & Advisories	Allows you to view the reports on cybersecurity concerns and DDoS weapon attacks published by Threat Control System. This menu includes the following sub-menu: • **Reports & Advisories** — Allows you to view the reports and advisories in card and list views. • **Periodic IP Check Reports** — Allows you to download the complete Periodic IP Check Reports for triggers and alerts both in PDF and CSV formats. For more information, see Reports & Advisories.
Administrator	Allows you to view and manage the following: • **Audit Trail** — Allows you to view logs by a username, action, and module. • **User Management** — Allows you to create a new user, edit user information, and add users to groups. • **Session Management** — Allows you to view the list of current sessions along with the history of the logged in sessions.
Help Icon	Allows you to access the Threat Control System Help and send emails to the A10 support team.
Share Feedback	Allows you to share your feedback about Threat Control System service.
Profile Icon	Allows you to view the Threat Control System application version and log out from the SecDevice application.

Search Options

Search options include the following:

Search Widgets

Threat Control System provides some common search widgets and buttons on the dashboard.

Table 2 : Search Widgets and Buttons

Search Widgets/Buttons	Description
Filters	The dashboard view changes based on the filtering criteria that you select using the Filters button. Select the filtering criteria according to your requirement. • Duration • Attack Type • ASN • AS Organization • Country To know more details about the search filters, see Filters.
Persist Filters & Time Frame	Enables you to save the searched filters along with search time frame. For example, if you enable **Persist Filters & Time Frame**, and select any filters from the Filters option and the duration for result, the selected filters and result time frame will be visible on the **Dashboard**, the **Attack Victims** and **Weaponized Nodes** pages of Attack Research, and the **Summary** page of Weapons & Activities. The searched filers will be visible even after navigating to other SecDevice Threat Control features, and then

Table 2 : Search Widgets and Buttons

Search Widgets/Buttons	Description
	revisiting these pages again. This feature helps to save the searched filters for future use and eliminates the effort of recreating required filters from time to time. **NOTE:** Some filters may or may not be available under certain menus.
Search time frame	Click the search time frame for which you want to view the attack incidents. The following search time frames are available: • Last 6 Hours • Last 24 Hours • Last 72 Hours • Today • Yesterday • Last 7 Days • Last 30 Days • Last 90 Days • Last 365 Days • Custom Range **NOTE:** If you select less than 24 hours from the calendar picker, the time format displayed in the chart is in date and time. For example, Dec 13-13:00. If you select more than 24 hours, the format will only be displayed in date. The timestamp is not displayed.
Time Zone	Enables you to switch to UTC or your local

Table 2 : Search Widgets and Buttons

Search Widgets/Buttons	Description
	time zone, as per requirement. Time zone impacts all the reports in the application that contain dates. This facility helps users from different geographies to get the same view of the application.
Download PDF	You can download the report in PDF format. The report is generated based on the search factors that you select.
Download All	You can download the reports in PDF format. The report is generated based on the search factors that you have selected and include all the attributes such as reflectors and botnets. This button is available only on the Weapons & Activities menu.

Table 3 : Dashboard Widget

Widget	Description
Attack Map	This map gives a view of the countries under attack on the world map. If you hover over the affected spot, the country names appear with links. You can click the links to the country names to analyze the attack details. You are redirected to the attack details page (Attack Research > Attack Victims). Moreover, you can analyze the details of attacks for **Attacks By Target Country** and **Attack Distribution By Duration** options also. To know more details about the attack details, see Attack Victims.

Table 3 : Dashboard Widget

Widget	Description
Filter by	Allows you to filter the world map insight based on the following selections: • **Ongoing** — Includes the ongoing threats in red color. • **Stopped** — Includes the stopped or blocked threats in blue color.
Attacks Over Time	Displays attacks based on the time range that you select using the search time frame. You can view this attack type in both logarithmic and linear charts.
Attacks By Target Country	Displays top countries impacted by the attacks. The countries are displayed based on the search filter.
Attack Distribution By Duration	Displays attacks based on durations selected in the search filter.

Filters

Duration

The Duration option in the Filters drop-down list allows you to narrow down the analytics based on the duration of the attack. The available search options are:

- < 5 min
- 5 min – 10 min
- 10 min – 1 hour
- > 1 hour

Attack Type

Attack types capture every kind of emerging DDoS attacks and vulnerabilities whether they are related to network connection (TCP/UDP), volumetric attack, fragmentation, application, or ports.

You can narrow down your search if you suspect your organization is under attack by weapons such as ARM, ASN, or others. This helps you to capture the exact attack attempts.

To know more about the attack types, see Appendix: Attack Types.

ASN

The ASN (Autonomous System Number) attacks in the Filters drop-down list enable you to narrow the analytics report based on the attacks originating from an ASN port in a network.

If you know the exact port number, you can type that port number in the ASN search box and search for the attacks on the network. ASN can be between 0-65535. You can search for a maximum of ten ASN in one try.

AS Organization

The AS (Autonomous System) Organization attacks in the **Filters** drop-down list enable you to analyze the attacks on a network of an organization.

Country

The Country option in the Filters drop-down list enables you to narrow the analytics report based on the attacks from a single country, a combination of countries, or all countries of the world in one graph.

Attack Research

Attack Research allows you to customize and view the incident analytics based on the IP address, organization, attack type, country, and duration.

The following topics are covered:

Attack Victims

Attack Victims gives you an insight into the vulnerability of your network to various kinds of attacks by IP address or subnets.

To mitigate DDoS attacks received in a network, it is important to analyze the affected IP addresses, ports, and hostnames within your organization. This helps in knowing the complexity of attacks, malicious traffic, and vulnerabilities. You can also know the duration and specific times of these attacks.

Attack Victims has the same analytical attributes as those present on the dashboard. For more information, see Dashboard.

Analyzing Attacks at Organization Level

To analyze the attacks at the organization level:

1. Navigate to **Attack Research > Attack Victims**.

   The report is displayed based on the selected attributes such as attack duration, attack types, ASN, AS Organization, and countries. By default, all the search

factors are selected. However, you can change these attributes according to the analytical requirement of your organization.

In the **Attack Victims** view, you can expand every attack to find its specific details, such as - hostname, ASN, attacked port numbers, victim sector, current attack status, and name of city. The following table describes the attack details.

Table 4 : Attack Victims Widgets

Widget	Description
Time	Displays time when the attack occurred. You can inspect an attack more effectively by the factors such as hostname, attacked port number, current attack status, and ASN. To view the attack details, click the expand arrow icon available next to the incident.
Complexity	Displays how complex an attack is. The complexity may be low, medium, or high as per criticality of the attack.
Attacked IP Range	Displays the impacted IP address range in the network.
Attacked IP	Displays the impacted IP address in the network.
AS Organization	Displays the name of the impacted organization.
Attack Type	Describes what type of attack occurred such as ARM, CoAP, and so on. Attack types indicate severity of the malware attack. To know more about the attack types, see Appendix: Attack Types.
Attack Duration	Displays how long the attacks occurred.
Country	Displays the names of countries which have been affected.

Search Options

Table 5 : Search Widgets and Download Options

Search Widgets/Buttons	Description
Filters	The attack details change based on the filtering criteria that you select using the Filters button. Select the filtering criteria

Table 5 : Search Widgets and Download Options

Search Widgets/Buttons	Description
	according to your requirement. • Duration • Attack Type • ASN • AS Organization • Country
IP search text box	Allows you to search by IP addresses or subnets. If you search by an IP address, only data from the last 24 hours is displayed. If you search by a subnet, all data of the searched subnet is displayed. By default, data of attacks is displayed for last 24 hours.
Search time frame	Click the search time frame to select the duration you want to view the incidents. You can customize your search criteria based on the following durations: • Last 6 Hours • Last 24 Hours • Last 72 Hours • Today • Yesterday • Last 7 Days • Last 30 Days • Last 90 Days • Last 365 Days • Custom Range

Table 5 : Search Widgets and Download Options

Search Widgets/Buttons	Description
	NOTE: If you select less than 24 hours from the Search time frame, the time format displayed in the chart is in date and time. For example, Dec 13-13:00. If you select more than 24 hours, the format will only be displayed in date. The timestamp is not displayed.
Download	Click the **Download** button to download the attack details report in PDF and CSV formats for the **Attack Victims** and **Weaponized Nodes** attack types The reports are generated based on the search factors selected from the **Filters** option. The report in PDF format supports the addition of 1,000 records by recent time and includes all the columns as displayed on the SecDevice app. The report in the CSV format supports the addition of 100,000 records and includes all the columns, along with the fields from the Time column.

Weaponized Nodes

Weaponized Nodes are those IP addresses that have been compromised or have become botnet weapons by any other attackers to spread DDoS attacks.

Tracking the source of compromise such as malware or potential vulnerabilities is crucial to prevent your network from becoming a botnet in future and enhance defence mechanism.

Analyzing Attack by IP Address/Network

To analyze the attack by an IP address or network:

1. Navigate to **Attack Research > Weaponized Nodes**.
2. In the search field, enter an IP address or network, as per your requirement.

   If you enter a network, make sure you add the subnet as well. The permissible search range for subnet masks for both attacked networks and weaponized networks is between /13 to /32.

3. Press **Enter**. The report is displayed.

   If an IP address is attacked from different port numbers, sectors, or other factors, several reports on the same IP address are displayed. You can download the reports in PDF and CSV formats. The report for the searched IP subnet range will be available in both the PDF and CSV formats.

NOTE: **Duration** and **Attack Type** filters are not applicable for Weaponized Nodes.

Table 6 : Weaponized Nodes

Widget	Description
Last Seen	Displays time when the attack was observed for the last time.
Weapon IP Range	Displays if the targeted IP address range has become a botnet.
Weapon IP	Displays if the targeted IP address has become a botnet.
AS Organization	Displays the name of the organization that became a botnet.
Country	Displays the name of the country where the organization is located.

You can expand every attack to find its specific details by further attributes, such as ASN, weapon type, and the name of city.

You can change the duration from the result time frame if you want attacks record for a different time frame.

Traffic Analysis

Traffic Analysis helps you analyze the attacks for the packet capture (PCAP) files. The PCAP (packet capture) file captures the traffic of your network.

The analysis gives a granular picture of the PCAP file size, packets count, attacks targeted for specific IP addresses, ports, and protocols. These factors help you to inspect the incoming traffic of your network, so you can fortify your network from the attacks. The analysis is presented in 3D modeling to give a visual presentation of the threats.

Analyzing Traffic for the PCAP File

To analyze the attacks for the packet capture (PCAP) file in the network:

1. Navigate to **Attack Research > Traffic Analysis**.
2. In the **Select File** field, upload a PCAP file.

   Only Wireshark capture file (.pcap) is supported. The maximum file size allowed is 20 MB.

3. Click **Generate Filter**.

   The following analysis is displayed.

Table 7 : Traffic Analysis

Factors	Description
Overview	Displays the PCAP file size, which is being analyzed.
Packet Count	Displays the packet counts.
BPF & JSON filters	Displays the BPF (Berkeley Packet Filter) and the JSON filters. These filters track IP packet length, time to live (TTL) duration for the IPs, destination IPs, TCP window size, packet fragment limit, TCP three-way handshake policy, TCP ACK, TCP communication, and so on. You can add this filter to your firewall protection policy to stay protected from DDoS attacks in future.

Table 7 : Traffic Analysis

Factors	Description
Filter Insights	Displays the attacks with data clustering model. You can rotate the 3D modeling, and click on the bad actors and cluster icons under **Cluster Information** to include or exclude these actors on the cluster modeling. The attacks are grouped on the basis of coherent logics and are displayed on different axes such as X-axis, Y-axis, and Z-axis. Data clustering helps in generating logical BPF syntax, which if added to the firewall protection, can prevent illegitimate traffic more effectively.

Weapons & Activities

Weapons & Activities gives you an extensive picture of the ever-expanding malware attacks across the globe, organizations, and network systems. You can investigate the malware attackers, severity of attacks, vulnerabilities, and security compromises. You can analyze DDoS weapons (reflectors), botnets, indicators of compromises (IOC), and other security threats more effectively under this feature.

You can also generate reports on the attacks according to your requirements by changing the analytical factors and download the reports.

The following topics are covered:

Summary

Summary reports include UDP amplification's top 5 trending attacks for IP ranges, countries, ASNs, and organizations. In addition, you can investigate why specific security attacks originate from certain locations or why certain IP addresses or organizations are under attack. Such analysis helps security analysts to augment the best solution for the targeted incidents.

Analyzing the Summary on Weapons & Activities

To analyze the summary:

1. Navigate to **Weapons & Activities > Summary**.

   Reports based on default setting are displayed.

   However, you can customize your reports by changing the filtering criteria using the Filters button such as attack duration, attack types, ASN, and countries. The following table describes the details of the reports.

Table 8 : Summary Reports Widgets

Widget	Description
Attacks Over Time	Displays the attack trends based on the selected duration. • X-axis: Includes attack count. • Y-axis: Includes attack duration (date and time). You can view this attack type in both logarithmic and linear charts.
UDP Amplification Top 5 Victim IP Ranges	Displays the insight into the top five UDP amplification attacks based on the IP ranges.
UDP Amplification Top 5 Victim Countries	Displays the insight into the top five UDP amplification attacks based on the countries.
UDP Amplification Top 5 Victim ASNs	Displays the insight into the top five UDP amplification attacks based on the ASNs.
UDP Amplification Top 5 Victim Orgs	Displays the insight into the top five UDP amplification attacks based on the organizations.

Reflectors

Reflectors capture the attacks carried out by various weapons such as DDoS, OpenDNS, TelNet, SSDP, SNMP, DNS, OpenVPN, NATPMP, NTP, and MSSQL. In addition, you can generate reports on trending attacks in the last seven days, incidents happening in countries and organizations, mitigation size and complexity, and other factors. The attacks on security weapons are displayed in a pie chart.

Analyzing the Reflectors

To analyze the reflectors:

1. Navigate to **Weapons & Activities > Reflectors**.

   Reports are displayed. You can customize your reports by changing various filtering criteria such as Known Low Port, Known High Port, and Random High Port. The following table describes the reflectors.

Table 9 : Reflectors Widgets

Widget	Description
Total DDoS Weapons	Displays the total number of DDoS weapons.
Attacks Attempted In Last 7 Days	Displays the pie chart of the attacks attempted in the last seven days. You can include or exclude attack types by clicking the legends available next to the pie chart.
UDP Amplification Weapons By Country	Displays the geographical heat map and insights of the UDP amplification weapons of top five countries.
UDP Amplification Weapons By Organization	Displays the treemap insight of the UDP amplification weapons based on the organization.
UDP Amplification Categories By Size And Mitigation Complexity	Displays the treemap insight of the UDP amplification weapons based on the size and mitigation complexity.
Filter by	Displays the treemap

Table 9 : Reflectors Widgets

Widget	Description
	insight of the UDP amplification weapons that can be filtered based on the following factors: • Known Low Port – Includes the known low ports in blue color. • Known High Port – Includes the known high ports in purple color. • Random High Port – Includes the random high ports in green color.

Botnets

Botnets lets you view how botnet attacks happen by botnet tools, organizations, and countries.

Analyzing the Botnets

To analyze the botnets:

1. Navigate to **Weapons & Activities > Botnets**.

   Reports are displayed. The following table describes the botnets.

Table 10 : Botnet Reports Widgets

Widget	Description
Top 10 Port Scanned By Botnets (Last 30 Days)	Displays the treemap insight of the top 10 ports scanned by the botnets.

Table 10 : Botnet Reports Widgets

Widget	Description
Bots By Organization	Displays the treemap insight of the combined bots for different organizations.
Bots By Country	Displays the geographical heat map and insights of the combined bots of top five countries.

IOCs

Indicators of Compromises (IOCs) allows you to analyze the nature of security compromises, frequency of attacks, and their complexity that occurred in the last 30 days. For example, you can scrutinize highly targeted organizations and countries, types of vulnerabilities in the settings of computers, routers, IP protocols, and networks.

This analysis helps you know the trending attackers, draws your attention to the vulnerabilities in your systems, and analyzes the impacts they can leave on your business. You can plan an effective security strategy to prevent any kind of unknown attacks.

Analyzing IOC Reports

To analyze IOC reports:

1. Navigate to **Weapons & Activities > IOCs**.

   BOT IOC Analysis is displayed. The following table describes the details of security compromises.

Table 11 : Summary of IOC Reports

Widget	Description
C2/Droppers By Country	Displays the locations of command & control (C2) servers and droppers by countries on a global map, along with five trending countries.
Top	Displays the top vulnerability exploitation attempts in the

Table 11 : Summary of IOC Reports

Widget	Description
Vulnerability Exploitation Attempts	last 30 days. This data helps you analyze the vulnerabilities and fix them.
Top 5 Malware Hashes	Displays the complexity of malware hashes that attempted to compromise the networks.
C2/Droppers By Organization	Displays the organizations impacted by command & control (C2) servers and droppers on their networks.

Alerts

Alerts allows you to view all the alerts configured in Threat Control System and create new alerts and triggers.

To ensure the security of your network systems and prevent cybersecurity attacks, the ability to proactively identify and resolve potential threats serves as the primary line of defense. The Alert Configuration feature enables you to enforce security measures that you create for your networks by tracking the attacks happening within your network system. SecDevice captures a large list of about 150 thousand subnets of an organization that may be suspected to be under attack. It then promptly dispatches email notifications to the concerned security mitigators.

You can create triggers to plan when alerts should be generated. The Alert Configuration feature will send out email notifications automatically to the designated stakeholders. Timely reception of these notifications equips you to not only assess attack threats promptly but also make informed decisions that reinforce your defense strategy against future attacks.

Following are the advantages of alerts and triggers:

- **Early Attack Trends**: Early trends of attacks by industry and country help you understand vulnerability to new attacks and prepare for emerging threats.
- **Attack Identification**: Find if you have been attacked or you have been part of an attack and assess risks relevant to your industry or country.
- **Trigger Rule Setting**: Create customized trigger rules to secure your network against potential threats.
- **Email Notifications**: Send email notifications automatically to the security mitigators.
- **Risk Assessment and Mitigation**: Assess threat severity and reinforce the security measures.

The following topics are covered:

Generated Alerts

In the Generated Alerts menu, you can view all the alerts generated till date. Alerts include the triggers for which the alerts are generated and the time when they are generated.

To view generated alerts:

1. Navigate to **Alerts > Generated Alerts**.

   You can view the alerts by alert names, trigger types, and time when they were generated.

   The following table describes the alerts:

Table 12 : Alerts

Alert Factors	Description
Search options	You can search alerts by using various filtering options such as the Filters option, search time frame, and timestamp. **Filters**: You can search the triggers by using the Filters options such as **Alert Name**, **Trigger Name**, and **Trigger Type**. **Search time frame**: You can search the triggers by using the search time frame, which includes different periods such as Last 6 Hours, Last 24 Hours, and so on. **Timestamp**: You can change the triggers result by using the timestamp such as 1 Min, 5 Min, and so on.
Timestamp	Displays the date and time when an alert was generated.
Alert Name	Displays the alert name.
Trigger Name	Displays the trigger name.

Table 12 : Alerts

Alert Factors	Description
Trigger Type	Displays the trigger type.
Lookback Period	Displays a time for which the triggers should be displayed.

Alert Configuration

In the Alert Configuration menu, you can view the alerts by alert name, trigger name, trigger type, lookback period, email notification frequency set to an alert, name of the alert creator, and time of alert creation.

Trigger Name, Trigger Type, and Lookback Period are associated together and must be created carefully.

For more information on how to create a trigger rule, see Triggers.

Creating Alerts

To create a new alert:

1. Navigate to **Alerts > Alert Configuration**. The following table describes the configured alerts:

Table 13 : Alerts

Alert Factors	Description
Name	Displays an alert name.
Trigger Name	Displays the trigger name.
Trigger Type	Displays the trigger type.
Lookback Period	Displays number of days for which the triggers should be displayed.
Notification Frequency	Displays frequency such as day and time when the notification should be sent.
Created By	Displays the names of the alert creator.

Table 13 : Alerts

Alert Factors	Description
Created Time	Displays when an alert was created.
Actions	Displays the following actions: • **Delete**: Use to delete an alert. This option is available to the organization administrators for all alerts. • **Edit**: Use for modifying the alert setting. The Edit option is available to the alerts **My network has been attacked** and **My network is used for the attack** only. While editing an alert, only the **Recipient's Email** and **Notification Frequency** fields can be modified. Only organization administrators can create, edit, and delete the triggers — **My network has been attacked** and **My network is used for the attack**. Moreover, organization administrators can create only one alert for each of these triggers. Organization non-administrator users can select a day of their choice and add recipients. The Lookback period for these alerts is set to **7 days** by default.

2. Click the **+ Create** link.
3. On the **Create Alert** screen, do the following:

Table 14 : Alert Fields

Fields	Description
Alert Name	Enter an alert name. You can give any name to your alert and then group it with a trigger name. Hence, you must first create a trigger to associate with an alert.
Trigger Name	Select a trigger name. Trigger names appear from the trigger list that you create under the Triggers option.
Trigger Type	Displays a trigger type. A trigger type is associated with

Table 14 : Alert Fields

Fields	Description
	a trigger name that you create under the Triggers option.
Lookback Period	Displays number of days for which the triggers should be displayed.
Recipient's Email	Enter an email address to which the alerts will be sent. **NOTE:** If you have the admin rights, you can add multiple email addresses. If you do not have the admin rights, your own email address will be added automatically.
Notification Frequency	Select either of the following options: • **Daily**: If you select the Daily option, you must also set the time by using the clock icon. The Daily option with 12:00 AM frequency is the default frequency. Alerts with daily frequency will get generated as per local time of the administrators who configure the alert. • **Weekly**: If you select the Weekly option, you must select a day. • **Monthly**: If you select the Monthly option, you must select whether the alert should be generated in the beginning, middle, or end of the month. For weekly and monthly notification frequencies, 11 AM PST is set as the default time.

4. To save the alert configuration, click **Create**.

   Click **Cancel** to cancel creating a new alert.

Triggers

The Triggers feature enables you to establish specific conditions that send alerts. These triggers are pivotal indicators of potential threats that demand immediate

attention. Consider scenarios where vigilance is necessary to detect potential network attacks, trace the weaponization of your IP addresses, or analyze specific attacks categorized by industry, continent, or country. These triggers serve as the foundation of your alert system, ensuring that you receive timely updates about critical security incidents.

As the trigger types are predefined, you may require creating multiple trigger rules to calibrate the trigger types to track every kind of attack.

Creating Triggers

To create a new trigger:

1. Navigate to **Alerts > Triggers**.

   All the configured triggers are displayed.

2. Click the **+ Create** link.

3. On the **Create Trigger** screen, do the following:

Table 15 : Triggers

Triggers	Description
Trigger Name	Enter a trigger name.
Trigger Type	Select a trigger type. Triggers are the reasons when a certain type of attack happens. The following are the trigger types: • New Attack • Attack campaigns that target my industry • Attack campaigns that target my country • Attack campaigns that target my continent • My network has been attacked • My network is used for the attack If you select either the **My network has been attacked** or **My network is used for the attack** option, you must also configure a lookback period. Lookback period is applicable only to these two options. **NOTE:** SecDevice Threat Control can provide periodic IP check reports for up to 10 million IPs for both **My network has been attacked** and **My network is used for the attack** trigger types.
Look Back Period	The lookback period **Last 7 Days** appears by default. A lookback period is a history of the records of triggers for the specified period.

4. Click **Create**.

IP Block List

IP Block List identifies malicious IP addresses originating from suspicious sources. Identifying malicious IP addresses fortifies your network infrastructure to the emerging threats.

IP Block List captures various categories of DDoS weapons including bots, reflectors, command and control (C2) servers, malware droppers, and more. The suspected IP addresses are added to the curated blocklists such as threat lists, network versus host lists, size-variant lists, and so on.

You can download these IP addresses and add them to the blocklists on the security devices either manually or automatically.

To know how to download the IP Block Lists on your security devices automatically, see *SecDevice Administrator's Guide*.

The following topics are covered:

IP Block List

To view the IP Block List:

1. Navigate to **IP Block List > IP Block List**.

   The following IP Block List report appears. The blocklists are the lists that you added on your security device. You can search a blocklist by its name.

Table 16 : IP Block List

Block List Attributes	Description
Last	Displays the time when the blocklist was last updated.

Table 16 : IP Block List

Block List Attributes	Description
Modified Time	
List Name	Displays the blocklist name.
Description	A brief description of the weapon categories that the blocklist captures.
Aggregated List Size (Records/IPs)	The size of the aggregated list includes the following: • The number of records/lines in the list. Each record can be either a network IP / mask or a host IP/32. • Worst case number of IP addresses if the network records were to be expanded into individual IPs by the security device that you will deploy it on.
Host List Size	Displays the size of the host list expressed as the number of host records (/32s).
Actions	You can take the following actions for an IP Block List: • **Download**: Allows you to download the IP Block List report. For more details, see IP Block List. • **Copy URL**: Allows you to generate a URL link for a blocklist and configure the URL link on the security devices using APIs with Basic Authentication.
Custom IP Blocklist	Allows you to create an IP blocklist based on geography, weapon categories, and other parameters. You can download the curated IP blocklist to configure the list on the security device in your network manually. You can also generate a URL link as an API to configure the blocklist on the security device with Basic Authentication to allow automatic blocking of the listed IP addresses.

This section includes the following topics:

Understanding Weapon Categories and IP Block List

The following table describes the weapon categories:

Table 17 : Weapon Categories

Weapon Category	Description
Botnet	Following are some of the common botnet attacks: • Mirai: Mirai is a type of malware that infects computers and turns them into bots that are in turn controlled by the attackers. • Gafgyt: A malware that belongs to the Mirai malware family and functions the same way. • Hajime: Like Mirai malware, Hajime infects the computers to render them as botnets. It can infect switches and webcams, particularly in an IoT environment. • Remote Code Execution: Attacks that try to access a computer in a network and make changes to the advantage of the attackers.
Killnet	Killnet unleashes DDoS attacks using proxy IP addresses to pull down the internet services of the government organizations and companies.
Command and Control Servers	Attackers use command & control (C2) servers to control their botnets and launch attacks against their targets.
Reflectors-Critical	Reflector servers that enable DDoS attacks from random high ports increase the complexity of mitigating such attacks.
TOR Exit Nodes	Bad actors often use Known TOR Exit Nodes to commit other nefarious activities. These are not part of any specific DDoS weapons infrastructure. So, blocking these is up to the discretion of the security administrator.
Bogons	Bogons are unassigned IP addresses that attackers may use to mask their identity when carrying out malicious activity.

Host vs. Host & Network Lists

The page displays all the IP blocklists with their sizes. Most of the blocklists are available in two formats:

- Aggregated List (or CIDR Networks & Hosts): DDoS weapons are recorded as a mix of malicious networks (network IP/mask) and malicious hosts (host IP/32). This is a summarized form of the blocklist that includes the least number of records (lines).
- Host List (or CIDR Hosts): All DDoS weapons are captured as individual IP addresses (host IP/32).

The sizes of the blocklists in each of these formats are displayed. You can select the specific blocklist and format that fits the capability of the security device in your network.

Downloading IP Block List

Blocking the malicious IP addresses proactively can help you fortify your defense against the DDoS attacks.

It can further help you prevent the internal nodes from downloading DDoS malware or your networks being commandeered by external C2 servers to execute DDoS attacks against other organizations.

To download a blocklist manually:

1. On the **IP Block List** screen, under the **Actions** column, the following options for downloading are available:
   - **Download**: Allows you to download the IP list for a specific blocklist (For example, A10-Killnet-Block-List). Then you can add the IP list to the security devices manually.

     You need to repeat the same process to add the new IP addresses to the same blocklist.
   - **Copy URL**: Allows you to generate a URL link for a specific blocklist and configure the URL link on the security devices using APIs with Basic Authentication.

     The new malicious IP addresses for the same blocklist are added to the blocklist on the security device automatically based on time frequency as set on the security device.

To know how to download the IP blocklists on your security device automatically, see the "Support to Add IP Blocklists to Network Devices" section in the *SecDevice Administrator's Guide*.

2. Click the **Download** link available next to the report that you want to download.
3. On the **Download** dialog for your report, select the following options:
   - **List Format**: Select either **CIDR Hosts** or **CIDR Networks and Hosts** from the **List Format** drop-down list. The IP addresses in the CIDR Hosts contain the subnet masks, while in the CIDR Networks and Hosts format, there are no subnet masks.

     NOTE: For Bogons, you can download the CIDR Networks and Hosts report only.

     - **Hosts** - This list contains IPv4 host IP addresses with only /32 IPs.
     - **Networks & Hosts** - This list contains IPv4 networks and hosts. It reduces the number of records by providing a network address (/24) anything more than one /32 IP is detected in the same network. It contains both /24 and /32 IPs.
     - **Networks** - This list contains IPv4 networks with /24 IPs only. This list is useful when users wish to block large network ranges.
   - **File Format**: Select either **Plain IP List**, which is a text file, or **STIX 2.1** file from the **File Format** drop-down list.
4. Click the **Download** button.

NOTE: You can also manually upload the IP blocklists to the A10 Threat Protection System (TPS) using the aGalaxy management system or upload them to an A10/non-A10 firewall to block the traffic from these DDoS weapons.

Custom IP Blocklist

Custom IP Blocklist helps in creating blocklists with IP addresses based on factors such as specific weapon attacks, attacks originating from certain countries, attacks that target specific ports, and so on.

After downloading the IP blocklists, you must add them to the blocklists on the security devices. You can also generate a URL link of curated IP blocklists and configure the link on the security devices using Default IP Block List APIs. Traffic from these IP addresses will be blocked.

Benefits of custom IP Blocklists are as follows:

- Tailored Protection: Administrators can analyze the attacks and add the suspected IP addresses specific to their network environment.
- Rapid Response: Administrators can curb emerging security risks in the wild by blocking suspected IP addresses as required.
- Reduced False Positive Cases: Curation of IP addresses based on various factors reduce false positive cases as the administrators' approach is more targeted.

Creating Custom IP Blocklists

To create Custom IP Blocklists:

1. Navigate to **IP Block List > Custom IP Block List**.

   The IP blocklist report appears. These blocklists are the lists that you created based on various criteria to track the attacks.

   Table 18 : Custom IP Block List

Block List Attributes	Description
Created On	Displays the date when the blocklist was created.
List Name	Displays the blocklist name. While writing the blocklist name, you must keep the name unique.
Description	Displays the blocklist description. While writing the description, you should differentiate between blocklists.
Created By	Displays the user name who created a blocklist in the organization.
Last Seen	Displays the attacks for the IP addresses for

Table 18 : Custom IP Block List

Block List Attributes	Description
	as many days as listed.
Max. List Size	Displays the number of IP addresses added in a single blocklist.
List Format	Displays the list format that you selected for the blocklist. The list format can be CIDR Hosts, CIDR Network and Hosts, or CIDR Network.
File Format	Displays the file formats as such Plain IP List, which a text file and STIX 2.1 file.
Actions	Allows you to do the following actions: • **Download**: Allows to download the curated IP blocklist. • **Copy URL**: Allows to generate a URL link for the blocklist and configure it on the security devices using APIs with Basic Authentication. • **Delete**: Allows to delete the blocklist. if required.

2. Click the **Create Custom IP Block List** link, available on the top-right side.

   The Create Custom IP BlockList screen appears.

3. From the **Weapons Category** list, select one of the weapon categories.

   Following are the weapon categories: Bots, Reflectors, and Command & Control. Depending on the weapon category that you select, relevant options appear. The following table describes which options are available in a weapon category.

Table 19 : Options under Weapon Categories

Options	Description	Bots	Reflectors	Command & Control
Countries	Includes all	✓	✓	✓

Table 19 : Options under Weapon Categories

Options	Description	Bots	Reflectors	Command & Control
	the countries.			
Attacks	Includes all common attacks such as SSDP, NTP, DNS, SNMP, TFTP, Portmap, and so on.	X	✓	X
Last Seen	Allows you to enter the number of days during which the selected weapon attacks were observed for the IP addresses.	✓	✓	X
List Size	Enter the number of IP addresses to be added in a	✓	✓	✓

Table 19 : Options under Weapon Categories

Options	Description	Bots	Reflectors	Command & Control
	single blocklist. One IP address is added per line. It is advisable that while fixing the IP list size, you must keep in mind the capacity of the security devices deployed in your network. A10 includes most recent attacks in the blocklist.			
List Format	Includes list formats such as CIDR Hosts, CIDR	✓	✓	✓

Table 19 : Options under Weapon Categories

Options	Description	Bots	Reflectors	Command & Control
	Network and Hosts, and CIDR Network.			
File Format	Includes file formats such as Plain IP List and STIX 2.1, which is a JSON file.	✓	✓	✓

You can select a weapon category based on your incoming traffic and suspected attacks in your network. Following is the example of **Reflectors**.

4. From the **Countries** list, select a country.

   The IP addresses from the selected countries are included in the blocklist. You can select any number of countries as required.

5. From the **Attacks** list, select an attack.

   You can select any number of attacks as required.

6. In the **Last Seen** field, enter number of days from 1 to 30 days. This setting allows you to enter the number of days during which the selected weapon attacks were observed for the IP addresses.

7. In the **List Size** field, enter number of IP addresses to be added in the blocklist.

   The downloaded blocklist includes up-to the number of IP addresses that you specify here. It is advisable that while fixing the IP list size, you must keep in mind the capacity of the security devices deployed in your network.

NOTE: SecDevice is most likely to add recent IP addresses from all the incoming traffic.

8. From the **List Format** list, select a list type.

   Following are the list types: CIDR Hosts, CIDR Network and Hosts, and CIDR Network.

   CIDR Hosts contains only /32 IPs. CIDR Network and Hosts contains /32 IPs and /24 subnets if more than one /32 IP is in the same subnet. CIDR Network contains only /24 subnets.

9. From the **File Format** list, select a file format.

   Following are the file formats: Plain IP List, which is a text file and STIX 2.1 file.

10. Take one of the following actions after creating the blocklist.

    - **Save**: Allows you to save the blocklists to download them later.

      When you save the curated IP blocklist, you must enter the blocklist name and description. While writing the blocklist and description, make them logical to differentiate between different blocklists. Also, you can generate a URL link for the saved blocklist or delete it according to your requirement.

    - **Download**: Allows you to download the IP blocklist instantly. You must add the downloaded IP blocklist on your security device to block traffic from these IP addresses manually.

    - **Copy URL**: To automatically block the IP blocklists, generate a URL link following the same blocklist criteria and configure the blocklists on the security devices using APIs with Basic Authentication.

    - **Cancel**: Allows you to cancel creating the blocklist.

      To know difference between blocking the IP addresses manually and automatically, see Downloading IP Block List.

      For more details on how to configure security devices automatically, see the "Configuring Security Devices" section in the *SecDevice Administrators' Guide*.

Reports & Advisories

Organization publishes reports on cybersecurity concerns and DDoS weapon attacks based on various analytical studies. Such reports give insights into the origins of threat activities, the growth of DDoS weapons and botnets, and the role of malware in the propagation of DDoS weapons and attacks.

This intelligence empowers organizations to implement best practices to curb threats on time and ensure a secure business environment.

The following topics are covered:

Reports & Advisories

Reports and advisories give critical insights into growing challenges of new cybersecurity threats and DDoS attacks. These reports can be viewed in card and list formats.

- To view reports and advisories, navigate to **Reports & Advisories > Reports & Advisories**.

  All the reports and advisories and their count are displayed based on their publishing dates. You can search for the reports with report name or keywords. You can pin four reports on the top if you consider them important and want to observe them.

  The reports are available under the following tabs:

  - **Card View** — Card view gives a visual presentation of the reports and advisories. You can download reports in PDF, delete, pin, or unpin a report by using the pinning icon.

- **List View** — List view displays all the reports in tabular format. Every column in the table can be sorted as per requirement. You can download reports in PDF, delete, pin, or unpin a report from the Action column.

The following table describes the report attributes.

Table 20 : Reports & Advisories

Report Attribute	Description
Report Name	Displays the name of the report.
Description	Displays the description that you have added for a report.
Report Type	Displays the type of report, such as Advisory or DDoS Weapons Report.
Keywords	Displays the keyword that you have added for a report.
Published Date	Displays the date when the report was published, along with the timestamp.

Uploading Report

You can upload a report to the report list. The uploaded report will be listed under both the Card View and List View tabs.

To upload a report:

1. On the **Reports & Advisories** page, click the **Upload** link.
2. In the **Report Name** field, enter the report name.
3. Select a Report Type from the **Advisory** and **DDoS Weapons Report**.
4. From the **Continent** drop-down list, select a continent.
5. From the **Country** drop-down list, select a country.
6. From the **Industry** drop-down list, select an industry type.
7. From the **Attack Type** drop-down list, select an attack type.
8. In the **Keyword** field, enter the keyword to the report.
9. In the **Description** field, enter a description for the report.
10. From the **File** field, select a PDF file of the report.

11. From the **Image** field, select an image for the report.

    JPEG, PNG, and GIF image formats of up to 16 MB are supported.

12. From the **Publishing Date**, select the publishing date for the report.
13. Click **Upload** to upload the image.

Periodic IP Check Reports

To view periodic IP check reports, navigate to **Reports & Advisories > Periodic IP Check Reports**

The list of Periodic IP Check Reports is generated based on the triggers and alerts as configured by the administrators. You can search for reports using report name and download the reports for future reference. All the columns in the table, except the duration column, can be sorted as per requirement. The following table describes the details in Periodic IP Check List.

Table 21 : Viewing Periodic IP Check List

Report Attribute	Description
Report Name	Displays the name of the report.
Duration	Displays the duration for which the report was executed. The time stamp is displayed in UTC.
Number of Records	Displays the count of attacks.
Published Date	Displays the date when the report was published, along with timestamp.

For every report, hovering on the ellipsis menu provides the **Download as PDF**, **Download as CSV**, and **Delete** options to administrators. Additionally, customers receive emails with separate URLs to download the PDF and CSV reports.

Appendix: Attack Types

Every attack type allows you to view if the organizations are under attack by any malware or threats. The following table describes the attack types.

Table 22 : Attack Type

Attack Type	Description
ARM	Allows you to view if the organizations using ARM are under attack by any malware or threats.
CHARGEN	Allows you to view if the organizations using CHARGEN are under attack by any malware or threats.
CLADP	Allows you to view if the organizations using LDAP are under attack by any malware or threats. LDAP is a dedicated protocol to allow people to access data in a network environment.
CoAP	Allows you to view if the organizations using CoAP are under attack by any malware or threats.
Dahua-37801	Allows you to view if the organizations using Dahua-37801 are under attack by any malware or threats.
DB2	Allows you to view if the organizations are under attack by any DB2 ransomware attacks.
DNS	Allows you to view if the organizations using DNS are under attack by any malware or threats.
DTLS	Allows you to view if the organizations using DTLS are under attack by any malware or threats.
Jenkins	Allows you to view if the organizations using Jenkins in automation server are under attack by any malware or threats.
KNX	Allows you to view if the organizations using KNX-based automation technology are under attack by any malware or threats.
LDAP	Allows you to view if the organizations using LDAP are under attack by any malware or threats. LDAP is a

Table 22 : Attack Type

Attack Type	Description
	dedicated protocol to allow people to access data in a network environment.
mDNS	Allows you to view if the organizations using mDNS are under attack by any malware or threats.
Memcache	Allows you to view if the organizations using Memcache are under attack by any malware or threats.
Mikrotik-2000	Allows you to view if the organizations using Mikrotik-based routers are under attack by any malware or threats.
MSSQL	Allows you to view if the organizations using MSSQL are under attack by any malware or threats.
Mumble	Allows you to view if the organizations using Mumble-based chat apps are under attack by any malware or threats.
NATPMP	Allows you to view if the organizations using NATPMP are under attack by any malware or threats.
NetBIOS	Allows you to view if the organizations using NetBIOS are under attack by any malware or threats.
Netis	Allows you to view if the organizations using Netis-based routers are under attack by any malware or threats.
NTP	Allows you to view if the organizations using NTP are under attack by any malware or threats. NTP is a dedicated protocol that allows the synchronization of computers.
OpenVPN	Allows you to view if the organizations using OpenVPN are under attack by any malware or threats.
Plexmedia-32414	Allows you to view if the organizations using Plex Media are under attack by any malware or threats. Plex Media is a platform to organize and stream photos, music, and videos.
Portmap	Allows you to view if the organizations using Portmap VPNs are under attack by any malware or threats.
QOTD	Allows you to view if the organizations using QOTD are under attack by any malware or threats.

Table 22 : Attack Type

Attack Type	Description
Quake3	Allows you to view if the organizations are under attack by any Quake3 malware.
RDP	Allows you to view if the organizations using RDP are under attack by any malware or threats.
Rockwell	Allows you to view if the organizations using Rockwell automation systems are under attack by any malware or threats.
SLP	Allows you to view if the organizations are under DDoS attack because of Service Location Protocol (SLP) vulnerabilities.
SNMP	Allows you to view if the organizations using SNMP are under attack by any malware or threats.
SNMPv2	Allows you to view if the organizations are under attack at Simple Network Management Protocol (SNMPv2) level.
SSDP	Allows you to view if the organizations using SSDP are under attack by any malware or threats.
TFTP	Allows you to view if the organizations using TFTP are under attack by any malware or threats.
TP240DVR	Allows you to view if the organizations are under attack by any amplified DDoS vector.
Ubiquiti	Allows you to view if the organizations using Ubiquiti are under attack by any malware or threats. Ubiquiti is a networking device used for home and enterprise networks.
VSE-21025	Allows you to view if the organizations using VSE-21025 are under attack by any malware or threats.
VSE-2303	Allows you to view if the organizations using VSE-2303 are under attack by any malware or threats. VSE-2303 is a dedicated client-server solution supporting hardware devices and operating systems.
VSE-27015	Allows you to view if the organizations using VSE-27015 are under attack by any malware or threats.

Table 22 : Attack Type

Attack Type	Description
VSE-27016	Allows you to view if the organizations using VSE-27016 are under attack by any malware or threats.
VSE-27019	Allows you to view if the organizations using VSE-27019 are under attack by any malware or threats.
VSE-28015	Allows you to view if the organizations using VSE-28015 are under attack by any malware or threats.
WDBRPC	Allows you to view if the organizations using WDBRPC are under attack by any malware or threats.
WSDiscovery	Allows you to view if the organizations using WSDiscovery are under attack by any malware or threats. WSDiscovery is a dedicated protocol for accessing different services on a local network.
Select All	Allows you to search all the attack types.

Contact Us