

20-05-2025

GÉANT NeMo User Guide (for NRENs)

NeMo Network Monitoring: High-Performance DDoS Mitigation and Analysis Tool

Version:	Version 1.9
Date of Issue:	20-05-2025
Document ID:	GN-SOC-001
Authors:	Ryan Richford, Ashley Brown, Mohammad Hussain Faqeri, Roderick Mooi (GÉANT Association) Contact: soc@geant.org
Classification:	Restricted

© GÉANT Association

Table of Contents

1	Introduction	1
1.1	Overview	1
1.2	NeMo Product Description and Key Features	1
1.3	NeMo and the GÉANT DDoS C&A Service	1
1.4	About this User Guide	2
2	GÉANT DDoS C&A Service Definition	3
2.1	Overview	3
2.2	NREN Subscription/Configuration	4
2.3	NREN User Configuration	4
2.4	Service Delivery Model	4
2.5	NeMo Alert Levels	5
2.6	NeMo Sensitivity Categories	5
2.7	NeMo Thresholds	6
3	Gaining Access to the NeMo Web UI	7
3.1	Creating a Personal Client Certificate Using TCS	7
3.2	Importing your Certificate into your Browser	9
3.3	Completing NeMo Web Registration	9
4	Email Alerts from NeMo	11
5	NeMo Analysis Using the Web UI	14
5.1	Accessing Alerts	14
5.2	Analysing Graphical Data with Visual Explorer	16
5.3	Manipulating Time Parameters within Analysis Window	18
5.4	Analysing IP Addresses of an Alert	19
5.5	NeMo Alert Aggregation	21
6	Mitigation	23
6.1	Requesting Mitigation	23
6.2	Adding IP Addresses to the Mitigation	24
6.3	Stopping Mitigation	24
7	Submitting Bug Notifications and Feature Requests	25
	References	26
	Glossary	26

Table of Tables

Table 2.1: NeMo alert levels, sensitivity categories and trigger value conditions	6
Table 2.2: NeMo default thresholds per sensitivity category	6

1 Introduction

1.1 Overview

The GÉANT Distributed Denial of Service Cleansing and Alerting (DDoS C&A) solution has been designed to enhance visibility of traffic transiting the GÉANT network and specifically to aid the detection, analysis and mitigation of (D)DoS attacks. It is based on the NeMo (Network Monitoring) software, which was originally developed by DFN-CERT to address NREN-specific network-based analysis needs and is further supported by the GÉANT project, for implementation within both the GÉANT network and NREN networks.

1.2 NeMo Product Description and Key Features

The NeMo DDoS software is a powerful tool for flow-based traffic anomaly analysis, and (D)DoS detection, alerting and mitigation. The software has been deployed by GÉANT but can also be obtained and installed locally by NRENs to enhance backbone traffic visibility and enable DDoS workflows for NREN networks and customers.

Key features of NeMo include:

- Royalty-free open-source software without any volume-based licence fees.
- High-performance NetFlow analysis, capable of handling NREN traffic patterns and modelling complex backbone architectures.
- Low software requirements: NeMo can run on most current Linux distributions, either in containers or native.
- Sensitive data will stay local, with no need for external data processing.

For deploying NeMo in your own network, please contact: nemo@lists.geant.org.

Access more information on the NeMo page of the GÉANT Security website [[NeMo](#)].

1.3 NeMo and the GÉANT DDoS C&A Service

NeMo is a key component of the GÉANT DDoS Cleansing and Alerting (DDoS C&A) service, a DDoS attack detection and mitigation solution that aims to:

1. Protect the GÉANT core network (AS 21320) and related infrastructure (*excluding backbone trunks*) from (D)DoS attacks.
2. Protect (*for subscribed customers*) NREN uplinks to the GÉANT network from being filled because of (D)DoS attacks targeted at the NREN and/or NREN institutions.

1.4 About this User Guide

This User Guide is for NRENs who currently use, or who are interested in using NeMo, as part of the GÉANT DDoS C&A service. It covers:

- GÉANT DDoS C&A service definition (Section 2).
- Gaining access to the NeMo web UI (Section 3).
- Email alerts from NeMo (Section 4).
- NeMo analysis using the web UI (Section 5).
- Mitigation (Section 6).
- Submitting bug notifications and feature requests (Section 7).

The latest version can be found on the Partner Portal, under the GÉANT DDoS C&A service section of the GÉANT Network Services Overview > Network Security Services page [[Partner Portal SvcsOverview](#)].

2 GÉANT DDoS C&A Service Definition

2.1 Overview

The aims of the GÉANT DDoS Cleansing and Alerting service are realised through:

- Deployment of NeMo detection nodes collecting and analysing flow data received from all relevant GÉANT routers.
- Configuration and tuning of these nodes to detect, and generate alerts on, common types of (D)DoS attacks. (This is an iterative and ongoing process requiring human intervention, adapting to the changing threat landscape.)
- Integration with multiple mitigation options:
 - a. A10 [\[A10\]](#).
 - b. NeMo's own mitigation nodes (planned post Nokia migration).
 - c. Firewall on Demand (FoD) / similar BGP FlowSpec router integration (under development as a future offering).

The components of the DDoS C&A solution work on layers 3 (Network) and 4 (Transport) of the OSI model to detect volumetric and protocol-based attacks such as SYN, ICMP and UDP floods as well as sudden increases in traffic volumes/patterns relative to baselines. Detection profiles are configured on a per-AS level and email alerts can be sent to customer-provided addresses. Once a customer has analysed an alert, the GÉANT Computer Emergency Response Team (CERT) can be requested to initiate manual mitigation if required (contact: cert@oc.geant.net).

DDoS C&A complements the attack mitigation options provided by RTBH and FoD (Firewall-on-Demand) whilst offering advanced detection and more fine-grained mitigation (scrubbing) to 'cleanse' traffic destined for NRENs and NREN customers. The goal of DDoS C&A is to filter as much malicious/attack traffic as possible without dropping legitimate traffic (within acceptable bounds).

This section describes the key features and functions of the service, namely:

- NREN Subscription/Configuration
- NREN User Configuration
- Service Delivery Model
- NeMo Alert Levels
- NeMo Sensitivity Categories
- NeMo Thresholds

2.2 NREN Subscription/Configuration

All **Peering (including GWS-subscribed) NRENs** are eligible for the DDoS C&A service (which is currently included in the base service package to members). **Note:** Currently only IAS traffic is included; R&E is under consideration for inclusion in the future.

NeMo detection mechanisms operate primarily on Autonomous Systems (AS numbers (ASNs)).

Monitored ‘objects’ are thus configured based on ASNs.

These AS objects are grouped together per NREN.

Each NREN (GÉANT customer) is therefore configured within NeMo as:

- One or more ‘lines’/ uplinks to the GÉANT network (for network modelling BUT NOT directly for DDoS detection).
- Usually one (but, in some cases, multiple) primary AS object(s).
- Optionally (resource permitting and within reason) NREN customer (e.g. university) public ASs.

Note: A10 mitigation is configured for rerouting **IAS traffic only**. R&E traffic rerouting (for scrubbing) *may* be considered in future as part of NeMo mitigation (if required).

2.3 NREN User Configuration

NeMo alerts for (potential) (D)DoS attacks can be sent to one or more NREN-specified email address (it is recommended that a team/group/alias/mailling list address is used rather than an individual’s email address).

Note: These addresses are utilised for the NREN AS group (including the NREN’s optionally configured institution ASNs).

Email alerts will contain basic information pertaining to the detected attack together with a link to the NeMo web UI which provides more detail and allows further analysis.

Access to the NeMo web UI currently requires a TLS client (authentication) certificate per user. These can be obtained via the Trusted Certificate Service (TCS, offered by GÉANT in association with Harica) or another CA of the NREN’s choice. Multiple users per NREN are supported (within reason).

2.4 Service Delivery Model

The GÉANT DDoS Cleansing and Alerting service is operated by the GÉANT Security Operations Centre (SOC) and supported by the GÉANT Security Products & Services and GN5 WP8 T3 DDoS teams.

Subscriptions are managed via the Partner Portal [[Partner Portal Subs](#)].

2.5 NeMo Alert Levels

NeMo is configured to provide alerts on DDoS attacks at three severity levels: INFO, WARNING and CRITICAL. INFO alerts are generated when the first traffic anomalies are observed. If the anomaly persists, the alert will be upgraded to WARNING. Alerts at this level should be investigated as indicators of a possible (D)DoS attack. An alert will be upgraded to CRITICAL if the traffic anomaly does not cease. At the discretion of the customer/NREN concerned, GÉANT recommends that both WARNING, but especially CRITICAL, alerts are analysed using the steps in Section 4.

NeMo produces emails from alerts containing the alert status and a summary of the alert profile, which are sent directly to the NREN (see Section 4). To avoid an excessive number of emails being sent to NRENs, the choice has been made to send emails only for alerts at WARNING and CRITICAL levels. A final email is sent when the alert closes (traffic anomaly ceases or normalises). How long an email takes to be generated will depend on the sensitivity category that an NREN is in, as this will affect how long an alert takes to reach WARNING level and generate an email. The sensitivity categories and associated trigger value conditions are summarised in the next section.

2.6 NeMo Sensitivity Categories

NeMo is designed to provide the best possible output for all subscribed NRENs. GÉANT has configured three sensitivity categories pertaining to the output of alerts. These three categories are default, low and high. Initially, all NRENs are placed in the middle category (sensitivity default) as a balanced option, allowing room to increase or decrease the sensitivity of alerts according to individual NREN requirements. The sensitivity categories include both a default threshold level and the number of times before alerts are generated at each criticality level.

From July 2023 onwards, these have been configured within the GÉANT NeMo instances as follows:

Alert Level (Sensitivity Category)	Trigger Value Conditions (point at which alerts are created)
INFO (Default)	1 event in 3 minutes
WARNING (Default)	5 events in 7 minutes
CRITICAL (Default)	8 events in 10 minutes
INFO (Low)	3 events in 6 minutes
WARNING (Low)	8 events in 10 minutes
CRITICAL (Low)	11 events in 15 minutes
INFO (High)	1 event in 3 minutes

Alert Level (Sensitivity Category)	Trigger Value Conditions (point at which alerts are created)
WARNING (High)	3 events in 5 minutes
CRITICAL (High)	5 events in 7 minutes

Table 2.1: NeMo alert levels, sensitivity categories and trigger value conditions

The output (in terms of volume of alerts) for each sensitivity group cannot be estimated as it will be subject to the NREN traffic profile, network size, and daily or weekly traffic.

To request a change in your sensitivity category, please email soc@geant.org, with 'NeMo: Sensitivity' in the **Subject** field.

2.7 NeMo Thresholds

Thresholds in NeMo manifest as an 'ignore below' figure that can be configured per AS by a GÉANT engineer. This can and should be used if an NREN experiences consistent alerts that are not significant in size or data rate (generally regarded as 'noise'). If a threshold needs to be configured, soc@geant.org should be contacted with the number of packets per second that you would like to ignore as well as the name and number of the Autonomous System concerned.

The default thresholds (per sensitivity category) are as follows:

Sensitivity Category	Detector 'ignore below' parameter value (packets per minute)*	Equivalent packets per second value
Default	3000000 ppm	5000 pps
Low	6000000 ppm	10000 pps
High	600000 ppm	1000 pps

Table 2.2: NeMo default thresholds per sensitivity category

***Note:** The detector 'ignore below' parameter is configured per minute, but graphs and analysis tools work on per second. Simply multiply (or divide) by 60 to convert.

3 Gaining Access to the NeMo Web UI

NeMo alert emails only provide basic information about a potential attack. To see the details and perform further analysis, each user requires an account on the NeMo (web) client portal. For this, a TLS client authentication certificate is required.

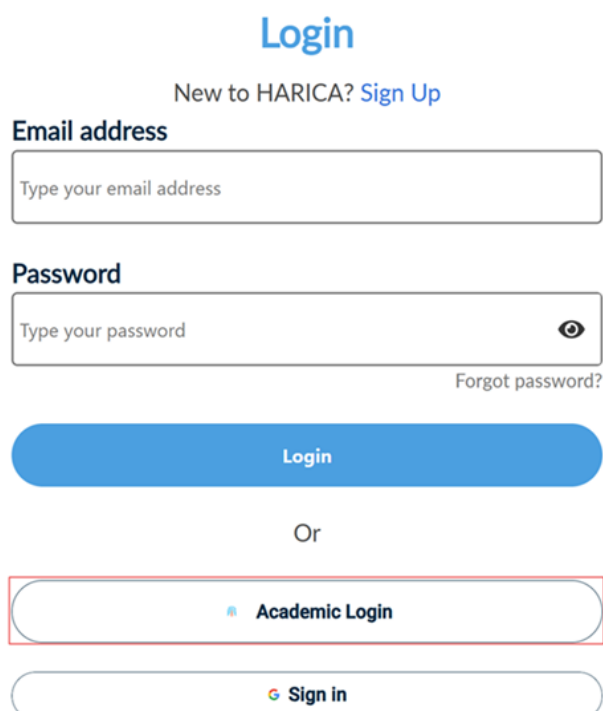
This section covers:

- Creating a Personal Client Certificate using TCS
- Importing your Certificate into your Browser.
- Completing NeMo Web Registration.

3.1 Creating a Personal Client Certificate Using TCS

Most client certificates from a commercial CA should work. For organisations making use of TCS, the steps to obtain a certificate are as follows:

1. Go to: <https://cm.harica.gr/>
2. Select Academic Login, search for your institution and login.



The screenshot shows the HARICA login interface. At the top, it says "Login" in blue. Below that, it asks "New to HARICA? Sign Up". There are two input fields: "Email address" with the placeholder text "Type your email address" and "Password" with the placeholder text "Type your password" and an eye icon for visibility. Below the password field is a link "Forgot password?". A blue "Login" button is centered below the fields. Below the button is the word "Or". There are two more buttons: "Academic Login" (highlighted with a red box) and "Sign in".


- From the menu on the top left, under Certificate Requests select "IGTF Client Auth".

Certificate Requests

 eSignatures

 eSeals

 Server

 Code Signing

 Email

 Client Auth

 IGTF Client Auth



- Select 'GÉANT Personal Authentication' as the Certificate Type and click Next.
- Review the application which should appear as follows (or similar).

Certificate Type	Service Duration
IGTF Personal	395 days
Subject Distinguished Name	
DC=org, DC=terena, DC=ica, C=NL, O=GÉANT Networking, CN=Muhammad Hussain Fazal Hussain.fazal@giant.org	

Check the box to agree with the Terms of Use (etc.) and click Submit Request.

- You should get a new entry in the dashboard under "Ready Certificates" – click the button "Enroll your Certificate".

7. Select your preferred algorithm, key size and set a passphrase. **Note:** the passphrase will be required to install the certificate! Check the box and “Enroll Certificate”.

Algorithm	Key size
ECDSA ▼	256 (default) ▼
Set a passphrase	
Type your passphrase 	
Confirm passphrase	
Retype your passphrase 	

8. Once your certificate enrolment is complete, it will be available for download.

3.2 Importing your Certificate into your Browser

If you are using Firefox, install your certificate by going to [about: preferences](#) > **Privacy & Security**. Scroll down to **Certificates** and click the **View Certificates...** button on the right-hand side. From the **Your Certificates** tab, click the **Import...** button at the bottom and select the downloaded certificate, providing the password as necessary (if/as configured when you made the certificate request). You should now see your certificate listed in the dialog.

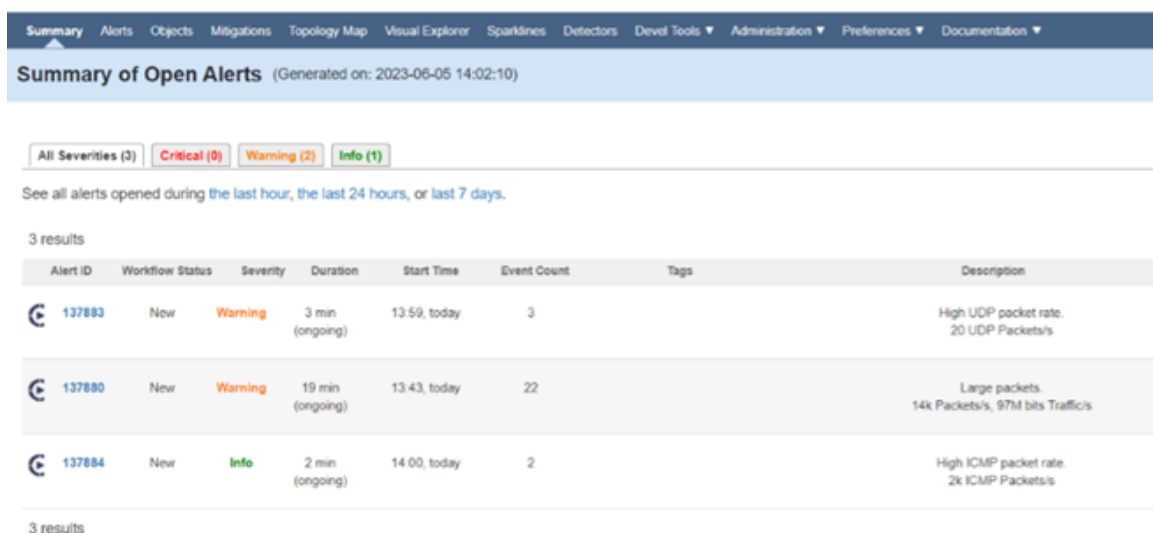
For Chrome, go to <chrome://settings> > **Privacy and security** > **Security** > **Manage certificates**. Click **Import** and follow the wizard prompts to import your certificate.

3.3 Completing NeMo Web Registration

1. Open your browser and navigate to: <https://primary.nemo.geant.org>.
2. Upon loading the page, you should receive an automatic prompt to use the downloaded certificate.
3. Select the imported certificate and click **OK**.
4. On the first attempt you will receive a page saying, ‘Access denied’.



5. Repeat the above steps on <https://secondary.nemo.geant.org>.
6. Email soc@geant.org to request account activation. Include your full name in the request. *Note that this process could take up to 2 business days, following which you should receive an email to verify that your account has been activated.*
7. Once confirmation has been received, navigate back to <https://primary.nemo.geant.org> and use your personal certificate to log in. You should be greeted by a screen like the one below.
8. Confirm that the Objects and Alerts are correct / matched to your NREN. If they are not, please contact the email address above for assistance.



Summary Alerts Objects Mitigations Topology Map Visual Explorer Sparklines Detectors Devel Tools Administration Preferences Documentation

Summary of Open Alerts (Generated on: 2023-06-05 14:02:10)

All Severities (3) Critical (0) Warning (2) Info (1)

See all alerts opened during the last hour, the last 24 hours, or last 7 days.

3 results

Alert ID	Workflow Status	Severity	Duration	Start Time	Event Count	Tags	Description
137883	New	Warning	3 min (ongoing)	13:59, today	3		High UDP packet rate. 20 UDP Packets/s
137880	New	Warning	19 min (ongoing)	13:43, today	22		Large packets. 14k Packets/s, 97M bits Traffic/s
137884	New	Info	2 min (ongoing)	14:00, today	2		High ICMP packet rate. 2k ICMP Packets/s


3 results

4 Email Alerts from NeMo

The information in this section will aid in the process recommended by GÉANT for receiving and understanding emails sent from NeMo so that you can best apply mitigation to the specified IP addresses found in the client portal.

1. Emails are sent from NeMo for both WARNING and CRITICAL alerts (with another email being generated on alert closure). Upon receiving an email from nemo-ddos@host.geant.org you can get basic information from the **Subject** field and open it to view the details, including the alert status.

[Geant NeMo] #143882 END WARN: 2001:798::/32 - "Normal UDP packet rate" [GEANT]

 nemo-ddos@geant.org
To: GÉANT SOC
ⓘ We removed extra line breaks from this message.

The UDP packet rate on
net 2001:798::/32
returned to normal values.

Alert closed.

Alert ID: 143882
Status: Closed
Severity: Warning

Start Time: 2023-06-15 08:27:09

2. The alert type will indicate the severity level and, together with the other information, help you decide whether to investigate (analyse further) or not.

The UDP packet rate on
net 2001:798::/32
returned to normal values.

Alert closed.

Alert ID: 143882
Status: Closed
Severity: Warning

Start Time: 2023-06-15 08:27:09

End Time: 2023-06-15 08:37:16

Start Time (Europe/Berlin): 2023-06-15 10:27:09 End Time (Europe/Berlin): 2023-06-15 10:37:16

3. Once alert type has been checked, you should check the attack type as shown below. This will give you a better idea of the attack profile of the alert.

[Geant NeMo] #143882 NEW WARN: 2001:798::/32 - "High UDP packet rate: 2k UDP Packets/s" [GEANT]

 nemo-ddos@geant.org
To: GÉANT SOC
ⓘ We removed extra line breaks from this message.

Observed high UDP packet rates of
2k UDP Packets/s
on
net 2001:798::/32.

Opened with severity Warning.

Alert ID: 143882
Status: Open
Severity: Warning

- The emails are broken up into easy-to-understand sections such as trigger type, first and last event seen, and full duration of the attack. If the email is warning of a suspected attack, use the link or the alert ID to navigate to the NeMo web UI for further analysis.

Alert ID: 143882
Status: Open
Severity: Warning

Start Time: 2023-06-15 08:27:09
End Time: ongoing
Start Time (Europe/Berlin): 2023-06-15 10:27:09 End Time (Europe/Berlin): ongoing
Duration: 0 min

First Event Seen: 2023-06-15 08:25:00
Last Event Seen: 2023-06-15 08:26:00
Event Count: 2

Trigger: High UDP Packet Rate (NET) (ID 21)

Alert Description:
High UDP packet rate.

Affected Objects:

Type	Name	Event Count
Net	2001:798::/32	2

Further Details:
<https://primary.nemo.geant.org/alerts/details/143882/>

- Upon clicking the link within the email, you will be redirected to the information page of the alert featured in the email. If so, follow the steps from Section 5.2. If you are locating the alert manually, use Section 5.1.

Warning Alert 143882 Dates/Tim

Alarm Begin/End today, 08:27 - 08:37 (11 min) 1 affected object, 2 events
Merge...
Mute

Alert Analyses

This alert has not been analyzed. [Analyze Alert >>](#)

Event Sources

2001.798./32 UDP Packets

Alert Details

Description High UDP packet rate.

Tags -

Event Count 2 [View all events...](#)

Trigger High UDP Packet Rate (NET) (ID 21)

Alert History / Comments

[+ Add Comment](#)

Date	User	Message
today, 08:37	System	The UDP packet rate on net 2001.798./32 returned to normal values. Alert closed.
today, 08:27	System	Observed high UDP packet rates of on net 2001.798./32. Opened with severity Warning.

2001.798./32 - UDP Packets (NET UDP)



Blue: Current value
Light blue: Same timeframe 1 week ago
Lighter blue: Same timeframe 4 weeks ago
Gray shaded area: Model corridor (if applicable)
Pink: Model prediction (if applicable)

5 NeMo Analysis Using the Web UI

This section provides an overview of the NeMo web UI, including accessing alerts, data analysis, navigation, and relevant explanations. For a full description of how to use the web UI / client portal, please use the DFN *NeMo User Manual*, which can be found at [\[NeMo\]](#) (or use the **Documentation** tab in the NeMo web UI).

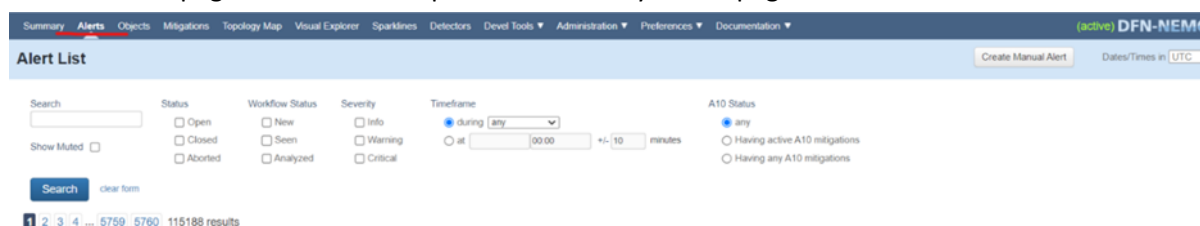
5.1 Accessing Alerts

You can access the alert information page by searching for the alert ID, or by locating it via its status, workflow status, severity, timeframe or A10 mitigation, as follows:

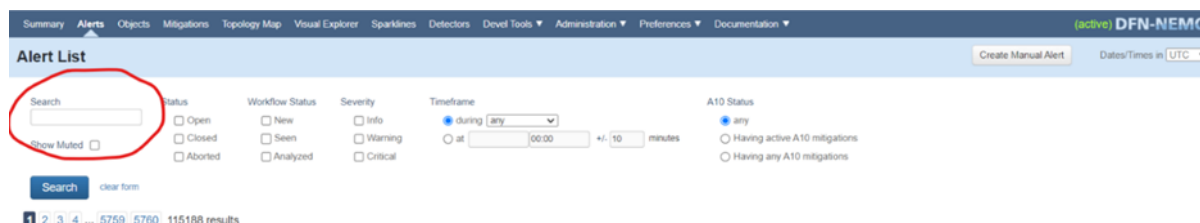
1. Provided you have not used the link in the email that takes you straight to the information page for the featured alert, upon opening NeMo you will be presented with the default page, like the one shown below.



2. Locating an alert using an alert ID provided within a NeMo-generated email can be done on the **Alerts** page found on the top menu bar of any NeMo page.

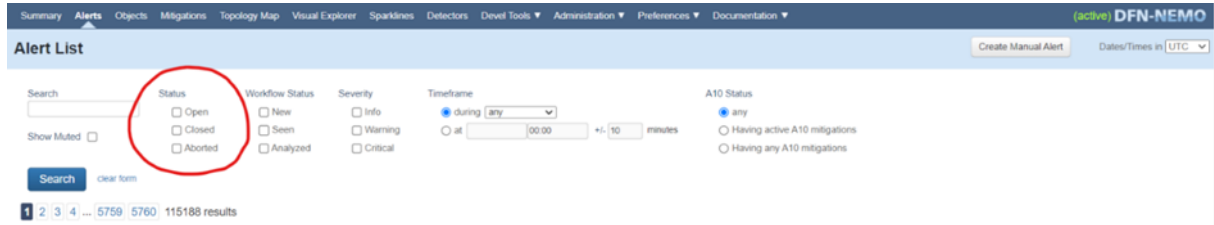


3. From the resulting **Alert List** page you can search for the ID using the search bar located on the left-hand side of the window.

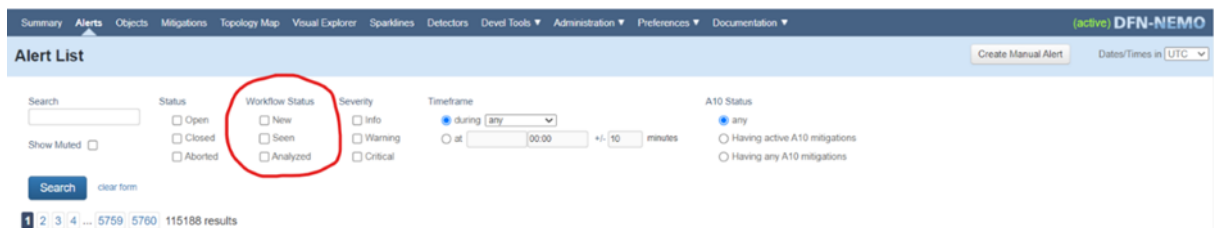


4. If you do not have an alert ID, or are just searching for types, or for the times that alerts were created, you can use the following:

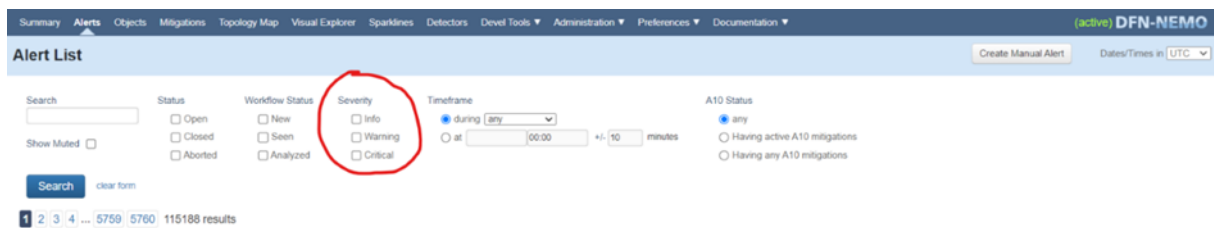
Located beside the search bar is a **Status** selection group containing three boxes. These boxes can be used to filter between open (ongoing) alerts, closed (finished) alerts and aborted (stopped manually) alerts.



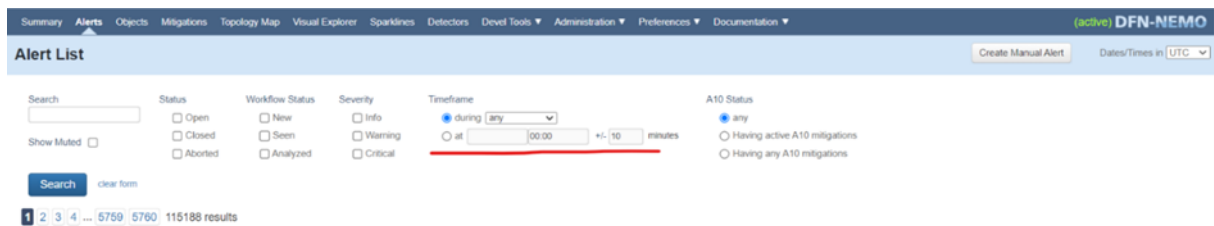
5. The **Workflow Status** selection group lets you filter by whether alerts are completely new, have been seen, or have been analysed.



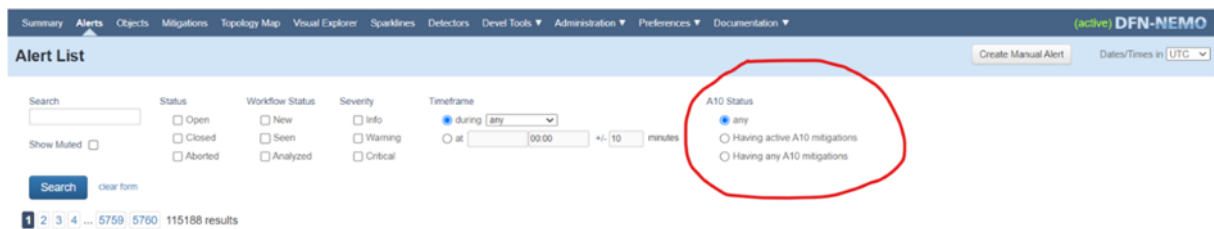
6. The **Severity** selection group lets you pick between the three severity levels: info, warning and critical.



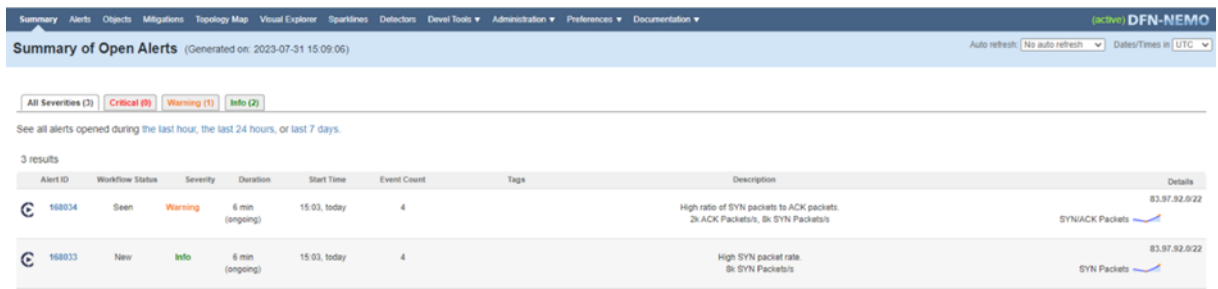
7. The **Timeframe** selection point lets you pick a time and look for alerts within a specified time range both before and after the time you have suggested, set by the +/- box.



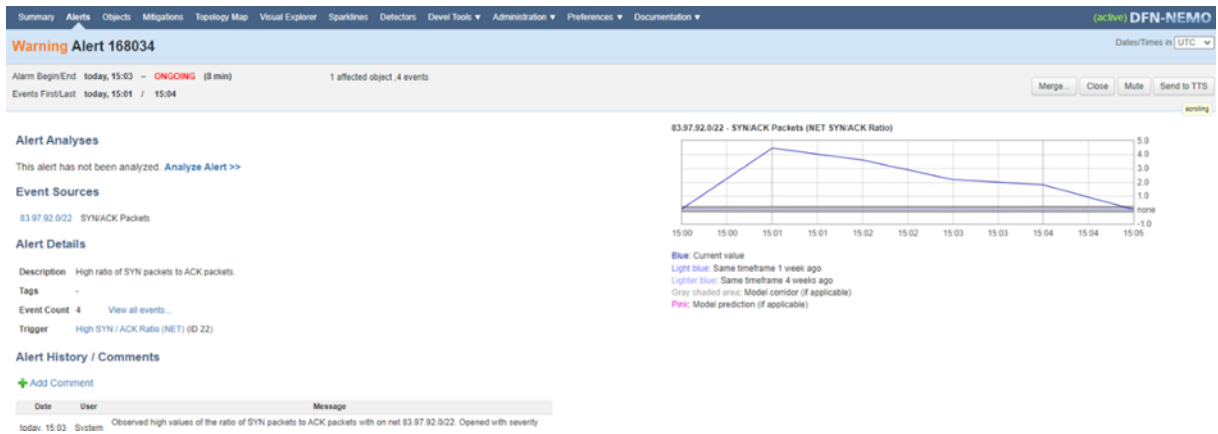
8. You can also filter alerts according to whether they are undergoing or have undergone A10 mitigation.



9. Once you have located the alert you are looking for, select it from the alert list.



10. Finally, click the alert to view the alert information page. Here you can see event information, alert type, trigger type and time. To view the alert information and obtain the IP addresses needed for mitigation, click the **Analyze Alert >>** link.



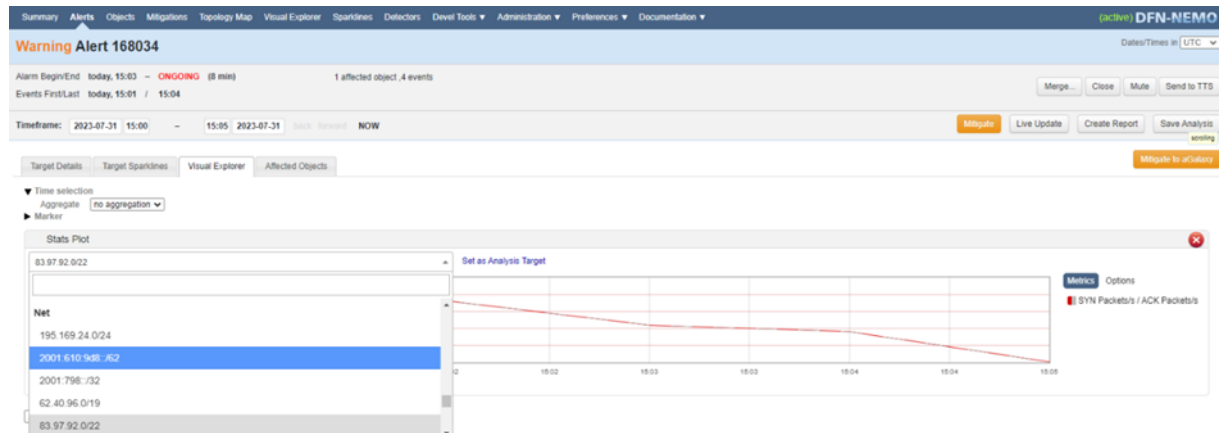
5.2 Analysing Graphical Data with Visual Explorer

After clicking the **Analyze Alert >>** link you can begin to analyse the alert. Visual Explorer is the best way to analyse graphical data. This section describes how to access the Visual Explorer page, the graph types available, and how to add, remove and manipulate them.

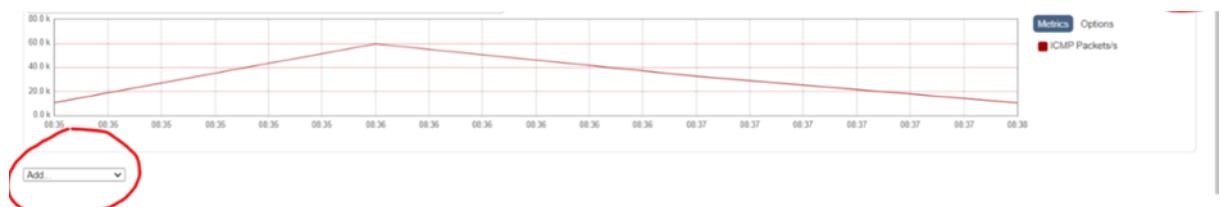
1. The Visual Explorer page can be found using two methods. One is by opening the alert as described in Section 5.1 and then selecting the **Visual Explorer** tab in the centre left of the analysis page. This will give you graphical information on the alert you are viewing. The other is by selecting the **Visual Explorer** tab on the menu bar located at the top of any NeMo page. However, the second method should be used for non-alert-based analysis.



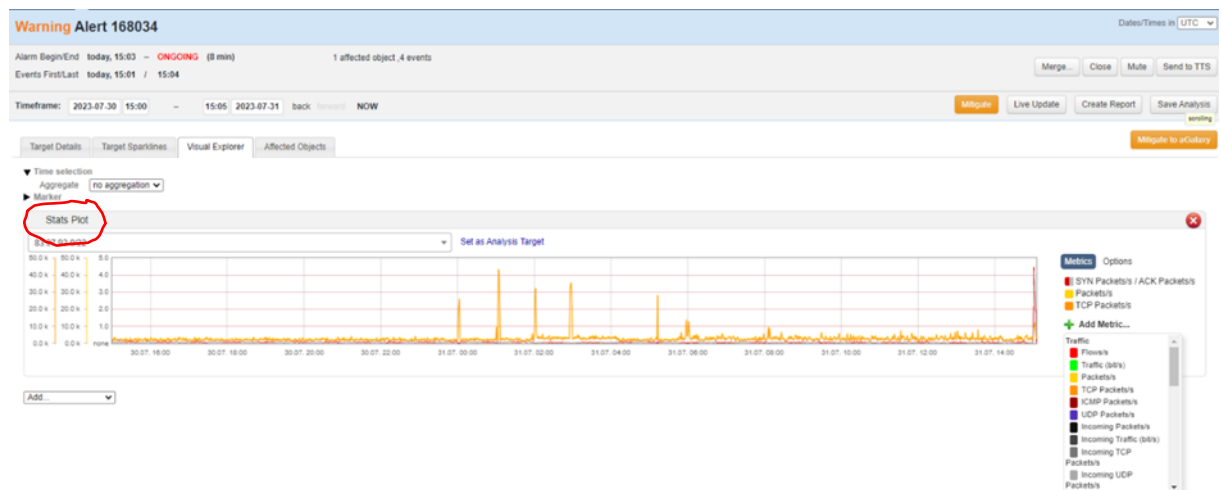
- Once the **Visual Explorer** tab has been selected, you will see a single graph populate the window. Use the box on the left of the window to select either your entire AS or lines configured for NeMo.



- You can remove graphs with the red X on the right of the graph and add new ones using the **Add** field on the left.

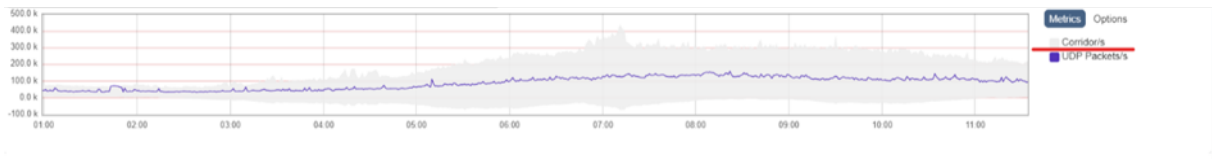


- NeMo contains two types of graphs, as shown below. These graphs give a visual representation of the flow data perceived within the alert. The first graph type is the **Stats Plot**, indicated in the title at the top of the graph. This graph can show multiple datatypes on one object at the same time. Statistics such as packet rate and packets per second can be seen on the left of the graph. This graph can be used to analyse deviations and spikes but cannot be used to compare the datatype with the corridor responsible for creating the alerts. All corridor analysis must be done from the second type of graph.



- The second type of graph is named **Detector Model Plot**. This graph is only capable of presenting one datatype at a time but can compare this datatype to the corridor when it is added using the **Metrics** fields on the right of the graph. The corridor is responsible for

generating the alert once it has been breached. This graph is better for checking breaches, reviewing alert triggers, and reviewing your entire Autonomous System.



- Once you have picked your graph you can manipulate and edit it to best suit your needs. The **Add Metric...** field can be used to add datatypes on the appropriate graph. By navigating to the **Options** tab to the right of **Metrics** you can change the plot height, toggle multiple axes and set the graph to no longer use a true zero point (better for analysis).

Metrics Options

- Flows/s
- Traffic (bit/s)
- UDP Packets/s
- + Add Metric...

Metrics **Options**

Plot height

Multiple axes yes no

Y-Axis scale true zero-point

5.3 Manipulating Time Parameters within Analysis Window

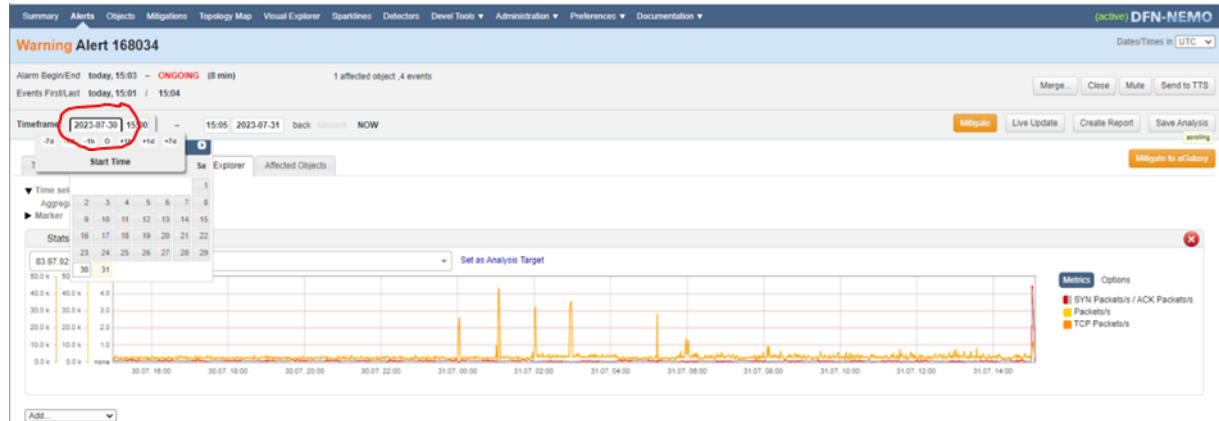
Once the analysis page is viewed as described in Section 5.1, by default you will be looking at the **Target Details** page with a single graph populating the centre screen. The graph will be showing the time of the first event (sometimes with up to a minute’s delay) and the last event. This section describes how to check information and change the date and time of the attack you are viewing.

- It is good practice to check the alert ID and times against the emails you have received. This information can be viewed in the top left-hand corner of the window next to **Alarm Begin/End** and **Events First/Last**. The graph in the centre of the window will be populated by these times.

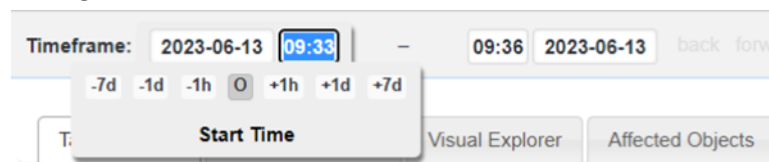
- You can use the **Timeframe:** fields in the top left-hand corner of the window to change the date and time of the attack you are viewing on the graph. The two boxes on the left indicate

the start date and time of the attack; the second pair of boxes indicate the end time and date of the attack.

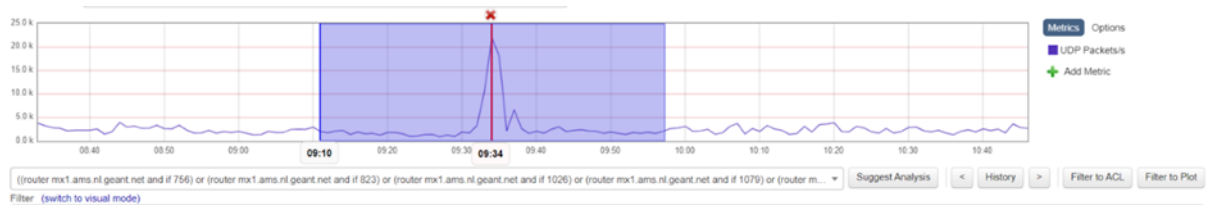
- To change the date/time, you can do one of two things. Either use the calendar field to pick both the start and end dates by clicking the box shown below.



- You can also choose to use the small **Start Time** and **End Time** fields to quickly navigate hours and days by hovering over the field.



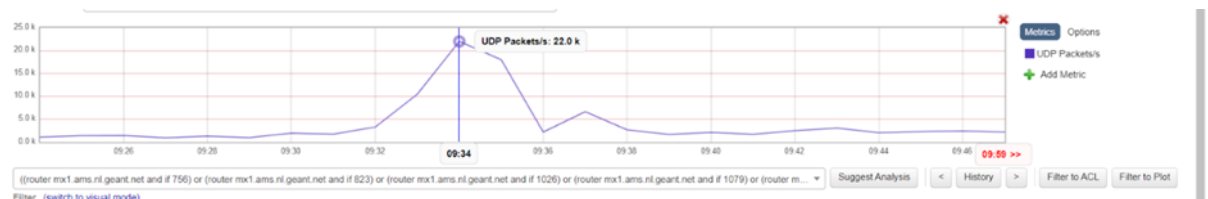
- You can also use your cursor to select a time within the graph window by clicking the mouse and dragging it over the time you wish to view.



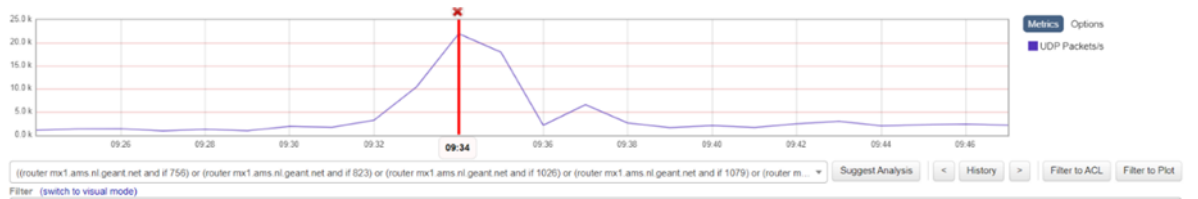
5.4 Analysing IP Addresses of an Alert

To display more information and refine your analysis, including details such as the source IP, destination IP and percentage of traffic by any given IP, take the following steps:

- To check the time of a particular spike, hover your cursor over the graph. The cursor will also show the packet amount at that time. The cursor can be used to pinpoint a specific part of your analysis, such as a spike or a dip.



- By double-clicking on an area that you wish to analyse further, you will populate the area selected with a bold vertical line. This line indicates the area you are analysing.



- The line is used by the system to populate a range of tabs, such as **Top-N**, **Possible Targets** and **Parallel Coordinates**, which are described below. However, you *must* hit the **Search** button shown below before analysing or the new data will not be written into the tabs. This action must be repeated each time you wish to look at a new data group by moving the vertical red line.

- The **Top-N** tab is one of the most useful tools within NeMo analysis and contains information such as source IP, destination IP, percentage of traffic by any given IP, and packet rate. Once the **Search** button has been clicked, all this information will populate in the page. This process can be repeated for all other pages.

- Adjacent to **Top-N** is the **Possible Targets** tab. This tab will provide you with some extremely basic suggested analysis. Note, however, that using this as the basis for mitigation could cause issues as the suggested analysis only populates the top 3 IP addresses. Check that the suggested analysis has not missed any IP addresses before sending them to be mitigated. (Mitigation is discussed in Section 6.)

Src IP	Src Port	Dst IP	Dst Port	Sampled Count
		193.108.160.152		3079800
84.17.49.44				2205000
84.17.49.44	4500			1896000
84.17.49.44			4500	1896000
	4500	193.108.160.152		1896000
		193.108.160.152	4500	1896000
	443	193.108.160.152		850200
31.13.84.4	443			532500
31.13.84.4				532500
31.13.84.4			55568	426600

- If at any point you would like to see the area on the graph that you are viewing in the **Top-N** tab (or in any other tab), you can hover the cursor over the **Results for:** text under the **Search** fields and you will see a red box showing the time you are viewing.

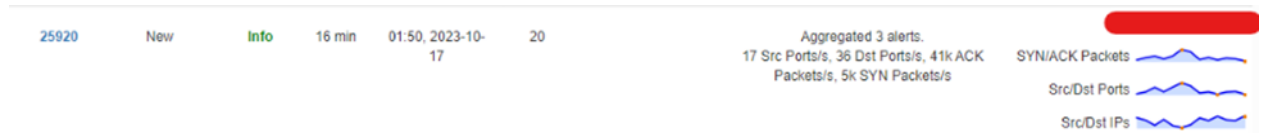
5.5 NeMo Alert Aggregation

NeMo differentiates between ‘simple’ alerts and ‘meta’ alerts. As stated in the DFN *NeMo User Manual* (which can be found at [\[NeMo\]](#) or in the **Documentation** tab on the NeMo web UI), simple alerts are non-aggregated alerts that summarise observations on a single network object within NeMo.

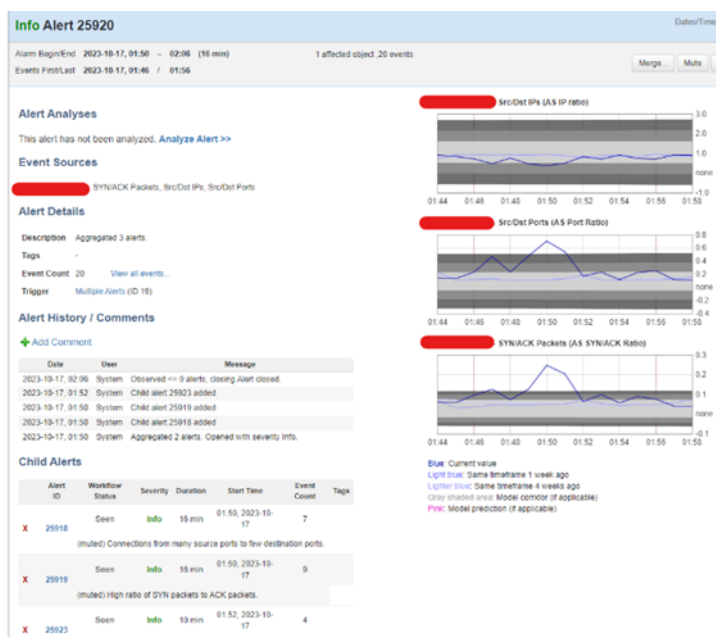
Meta alerts are different in that they aggregate together multiple simple alerts and the objects they are summarising into one alert, for ease of analysis. For example, a simple alert contains one object and one detector shown in one accompanying graph. However, meta-alerts can aggregate multiple alerts and their accompanying information, resulting in the ability to view multiple detectors and objects at once from a single alert.

When a simple alert is assigned to a meta-alert, all notifications for the simple alert are suppressed. From then on, NeMo emails will only be generated if the meta-alert to which it has been assigned is upgraded or closed. The simple alert will still be monitored by NeMo and escalated through its respective criticality levels accordingly. The simple alert can be added to multiple meta-alerts if NeMo categorises it as relevant.

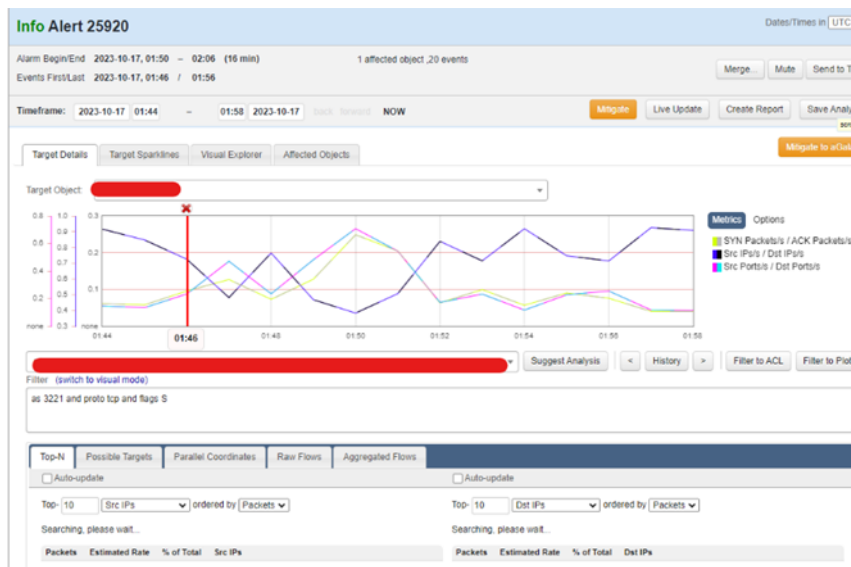
- The first difference you will notice will be on the **Alerts** page. **Alerts** will now show multiple detector types and graphs. You will notice that all related original simple alerts will now show as slightly grey as they have been suppressed.



- Once you open the summary page for the meta-alert you will be presented with all relevant objects, detector and graphical information from every simple alert that has been aggregated into the meta alert. This information will be presented together, for ease of analysis. Meta alert summary pages are structured in the same way the page for a simple alert would be presented.



- Upon clicking the **Analyze Alert >>** link you will see that the analysis page of a meta-alert will automatically populate the main graph with all the various metric types reported by the meta alert. These metric types correspond to the detector that generated the alert. This is once again for ease of analysis and can help to identify attack vector changes.



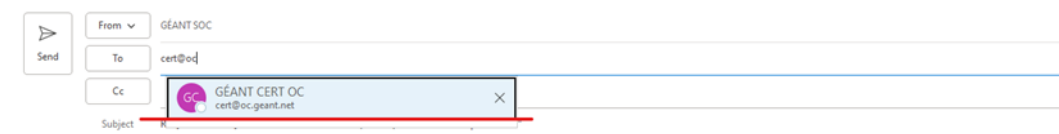
6 Mitigation

This section covers how to request mitigation, add IP addresses to the mitigation request and stop mitigation.

6.1 Requesting Mitigation

This section describes the process that needs to be followed for mitigation to be started manually by the GÉANT CERT. Note that any deviation from this process could result in mitigation not being enabled.

1. Once the IP addresses you would like included in the mitigation have been found (see Section 5), locate the email containing the alert information in its correct severity and click **Reply**. Check that the return email address has been set to cert@oc.geant.net.



2. Ensure that the IP addresses intended for mitigation are clearly stated in the email, as in the example below.

HI GEANT CERT,

Can you please mitigate following destination [IP's](#)

<IP1>

<IP2>

<IP3>

Kind Regards,
Ryan Richford
GÉANT Security Operations Centre

Networks • Services • People
<http://www.geant.org>

GÉANT Vereniging (Association) is registered with the Chamber of Commerce in Amsterdam with registration number 40535155 and operates in the UK Netherlands. UK branch address: City House, 126-130 Hills Road, Cambridge CB2 1PQ, UK.


-----Original Message-----

From: nemo-ddos@geant.org <nemo-ddos@geant.org>

Sent: Thursday, June 22, 2023 11:02 AM

To: GÉANT SOC <soc@geant.org>

3. Make sure you do not change the information in the **Subject** field before replying to / forwarding the alert email, as any change in the **Subject** line will result in the GÉANT ticketing system not propagating the alert to the required teams, potentially resulting in no mitigation.



4. Once the email has been received, the GÉANT service desk will reply to say the ticket has been picked up and handed over to an engineer.
5. Once the required mitigation has been activated, the on-call engineer will reply confirming this mitigation has been put in place.

6.2 Adding IP Addresses to the Mitigation

Once a given alert has started, it is possible to add/change IP addresses for mitigation. If you require this, please follow the following process.

1. To add/change IPs, first find the email that was sent to request the initial mitigation.
2. Reply to that email using **Reply All**, specifying the changes required, and send the email to cert@oc.geant.net, keeping the **Subject** information unchanged.
3. Once the email has been received by the GÉANT ticketing system, it will get relayed to a GÉANT engineer.
4. When the mitigation has been updated, a confirmation email will get sent to inform you that the mitigation has been enabled.

6.3 Stopping Mitigation

There are two methods by which mitigation can be stopped:

1. Mitigation stops automatically once a given alert has concluded.
2. To stop mitigation while the alert is still open in NeMo, use **Reply All** to reply to the email in which you requested the initial mitigation, asking for it to be stopped. This will be actioned by a GÉANT engineer and a confirmation email will be sent accordingly.

7 Submitting Bug Notifications and Feature Requests

This is the first time that NeMo has been deployed in GÉANT for the production DDoS C&A service. GÉANT is aware that there may be some bugs or missing features. If you would like to submit either a bug notification or a feature request, you can do so in an email to soc@geant.org with the subject line 'NeMo: Bug' or 'NeMo: Feature Request'. The email body should contain the point of contact, the institute name and a description of the related bug or feature request. Screenshots where applicable will aid in processing. Note that these notifications and requests will first be triaged and evaluated. Once validated and accepted, they will be actioned and/or forwarded to the development team as appropriate.

Enjoy NeMo!



References

- [A10] <https://www.a10networks.com/products/a10-defend-mitigator/>
- [NeMo] <https://security.geant.org/nemo-ddos-software/>
- [Partner_Portal_SvcsOverview] <https://geantprojects.sharepoint.com/sites/partner/NetworkServices/Lists/FeatureDescriptions/AllItems.aspx>
- [Partner_Portal_Sub] <https://geantprojects.sharepoint.com/sites/partner/Pages/DDoS-Cleansing-and-Alerting.aspx>

Glossary

AS	Autonomous System
ASN	Autonomous System Number
BGP	Border Gateway Protocol
C&A	Cleansing and Alerting
CA	Certificate Authority
CERT	Computer Emergency Response Team
DDoS	Distributed Denial of Service
FoD	Firewall on Demand
GWS	GÉANT World Service
IAS	Internet Access System
ICMP	Internet Control Message Protocol
IGTF	Interoperable Global Trust Federation
IP	Internet Protocol
NeMo	Network Monitoring
NREN	National Research and Education Network
OSI	Open Systems Interconnection
ppm	packets per minute
pps	packets per second
R&E	Research and Education
RTBH	Remotely Triggered Black Hole
SOC	Security Operations Centre
SYN	Synchronise
T	Task
TLS	Transport Layer Security
UDP	User Datagram Protocol

UI	User Interface
WP	Work Package
WP8	Work Package 8 Security
WP8 T3	WP8 Task 3 Security Products and Services