



DefensePro X
Version 10.x

Training Lab Manual Analytics AMS

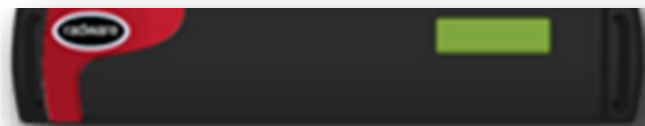


Table of Contents

OVERVIEW.....	3
SECURITY OPERATIONS REAL-TIME MONITORING DASHBOARD.....	3
DEFENSEPRO ANALYTICS DASHBOARD	10
DEFENSEPRO BEHAVIORAL PROTECTIONS DASHBOARD	11
FORENSICS	12
ALERTS.....	14
REPORTS.....	15

Overview

The Cyber Controller Analytics AMS dashboards display monitoring and reporting metrics. These metrics enable you to view and track real-time and historical information on selected AMS devices as well as security information on the traffic that the devices protect.

Exercises in this lab are viewed from the Analytics AMS perspectives.

Before you start make sure you have done the other labs generating attacks, so the database of the Analytics AMS is filled with data to show. Also you can run an attack like the TCP-RST Flood to see the system under attack.

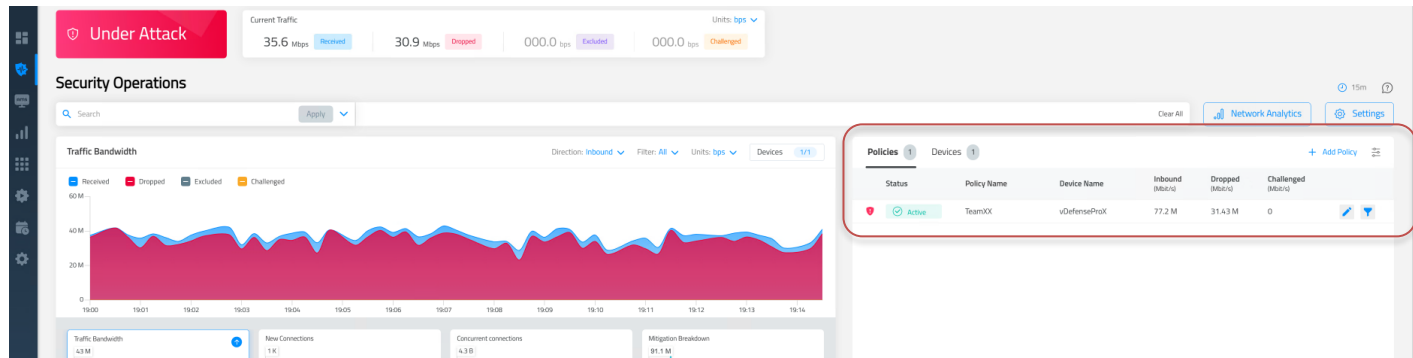
The screenshots are based on Cyber Controller version 10.7.0. For more details read the User guide for the version you are using, available on the Radware customer portal.

Security Operations Real-Time Monitoring Dashboard

1. In **Cyber Controller**, select **Security Operations** → **Real-Time Monitoring**



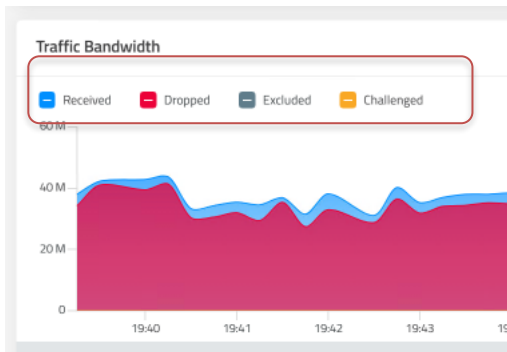
- By default you will see monitoring information from all DefensePro X policies and devices. Clicking on Policies or Devices, you can select a specific device and protection policy, in case you want to see only specific data. In our lab, we only have one device, so no need to do any specific selection.



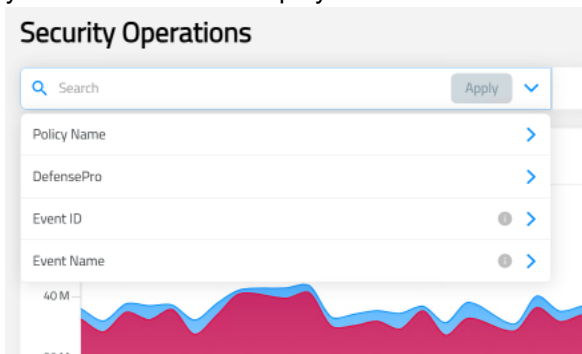
- In the Traffic Bandwidth graph you can select between bps/pps and inbound/outbound traffic information.



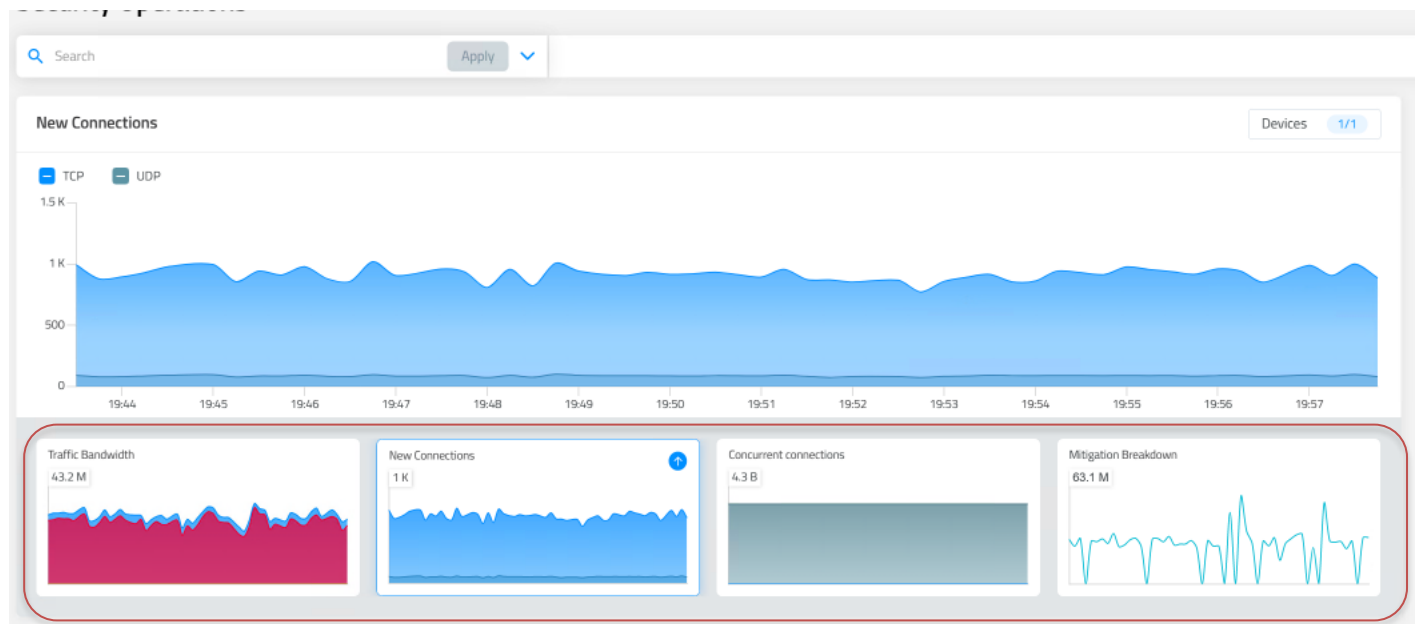
- You can click on the Received, Dropped, Excluded, or Challenged to filter out traffic you don't want to see.

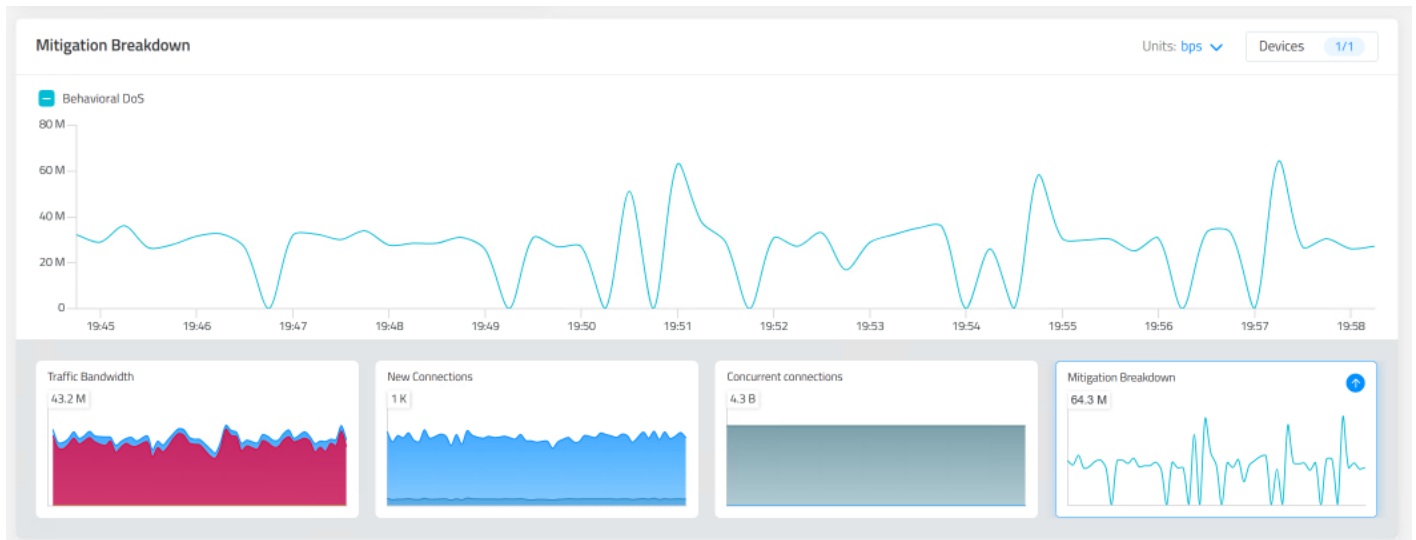


- You can click on the drop down in Search window to select which Policies, Devices, Event IDs, or Event Names you want to filter for display.



- If you click on New Connections, Concurrent Connections, or Mitigation Breakdown you see different views.





7. If you click on the pencil/edit icon, you can edit the policy.

Policies 1 Devices 1 [+ Add Policy](#)

Status	Policy Name	Device Name	Inbound (Mbit/s)	Dropped (Mbit/s)	Challenged (Mbit/s)	
Active	TeamXX	vDefenseProX	71.88 M	32.76 M	0	

Edit Policy

General and Networks

Enable

Policy Name *

TeamXX

Device *

vDefenseProX

Description

DefenseProX Level 1 Class

Network Table

+ Add New

Classification *	Type *	Network Address *	Prefix *	
Destination	IPv4	27.1.0.0	16	

Security Policy

Priority *

10

Copy from Template *

Basic-Global-10.0.0.0

Protection Sections

Expand All

Collapse All

General Parameters

Anti-Scan

BDoS Protection

Connection Limit

Connection PPS

DNS Flood Protection

EAAF

HTTPS Protection

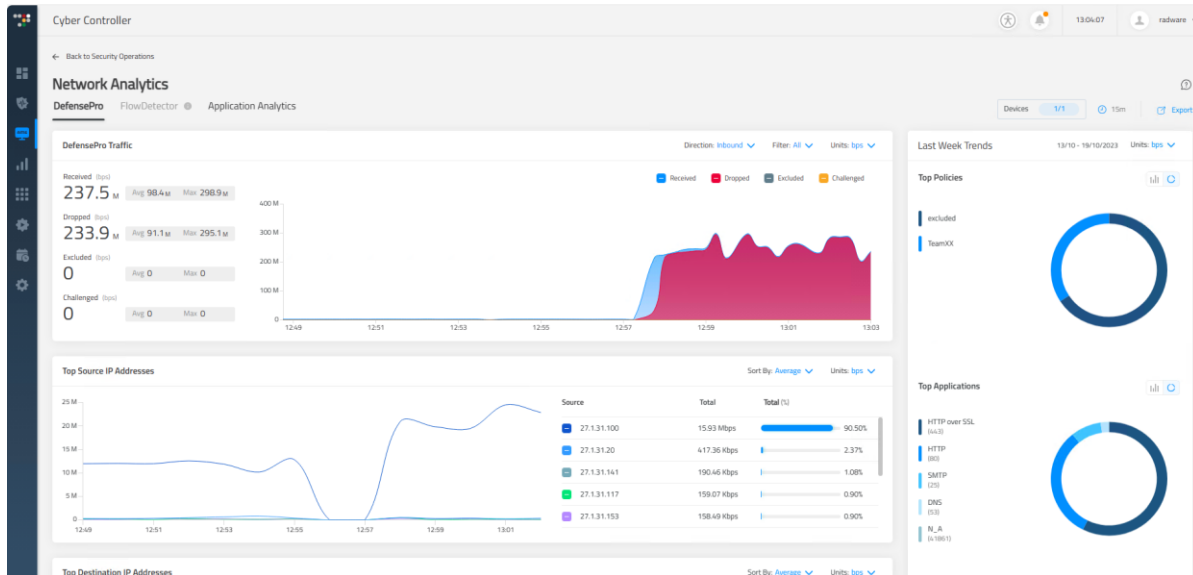
Cancel

Submit

DefensePro X Level 1 – Analytics AMS

7

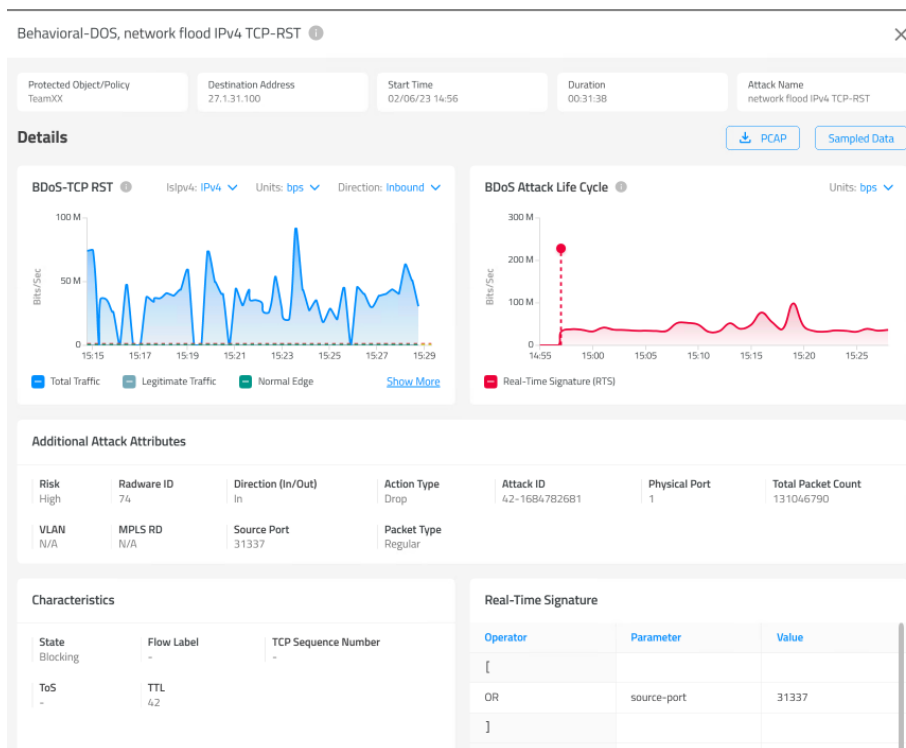
8. If you click on the Network Analytics you can see the DefensePro **Network Analytics** Dashboard, which gives you information on the current status of the DefensePro.



9. In Security Operations view you can see Detection Events.

Detection Events 1									
Action	Status	Category	Event Name	Event Destination	Updated Time	Duration	Policy Name	DP Name	Info
Drop	Ongoing	Behavioral-DOS	network flood IPv4 TCP...	27.1.31.100	06/02/2023 15:30:40	00:34:04	TeamXX	vDefenseProX	

10. If you click on event info (magnifying glass) you will see it's details.
 11. If event is protected by Behavioral DoS you will see BDoS Attack Life Cycle graph.



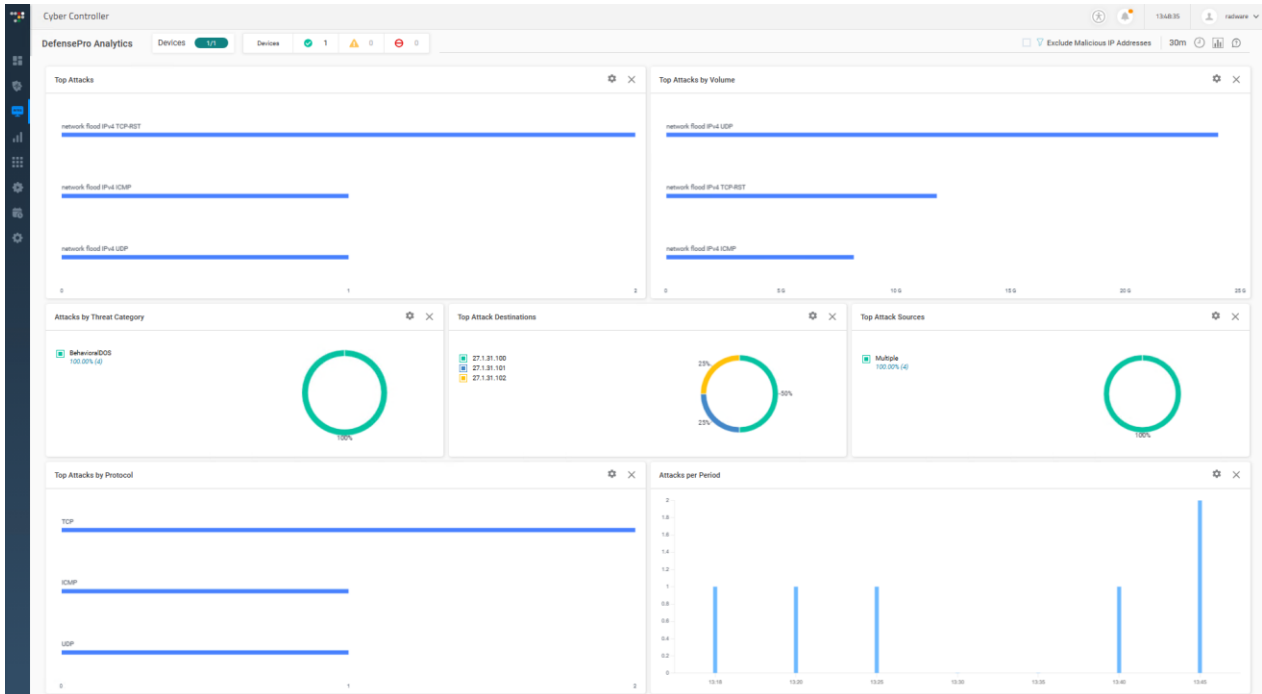
12. If you click on red dot you can see Real-Time Signature.


Real-Time Signature

Operator	Parameter	Value/s
[
OR	source-port	31337
]		
AND		
[
AND	packet-size	54
AND	destination-port	25
AND	destination-ip	27.1.31.100
AND	ttd	42
]		

DefensePro Analytics Dashboard

1. In **Cyber Controller**, select **AMS Analytics** → **DefensePro Analytics**
2. Select the relevant time frame, to make sure you see events.

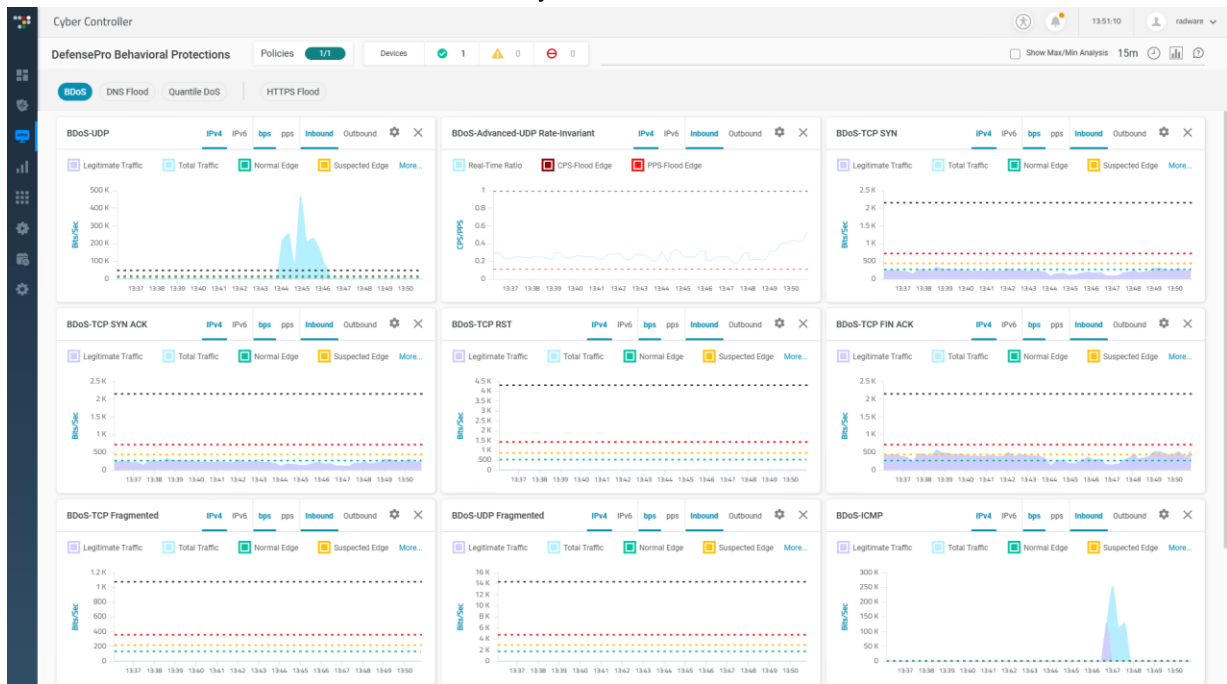


3. This dashboard can be customized, by using the widgets icon 
4. Each widget can be changed to show only data from a specific device or/and policy using the gear symbol. So you can add the same widget twice and show content from different devices/policies.

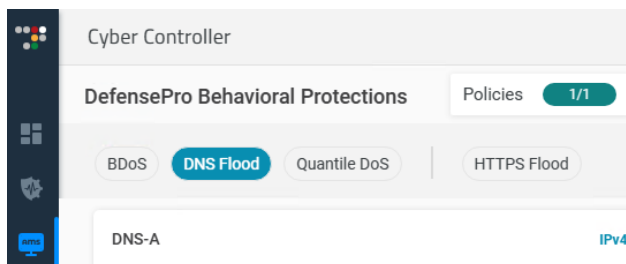
DefensePro Behavioral Protections Dashboard

This dashboard is used to see the BDoS and DNS protection learning information for a specific policy on a specific device.

1. In **Cyber Controller**, select **AMS Analytics** → **DefensePro Behavioral Protections**
2. Click on **Policies** to select a specific protection policy on a device to see its details. Make sure you have a BDoS or/and a DNS protection profile in the selected policy.
3. Select the relevant time frame, to make sure you see events Dashboard



4. You can also select **DNS Flood**, **Quantile DoS**, and **HTTPS Flood** behavioral protection tabs in this section.



Forensics

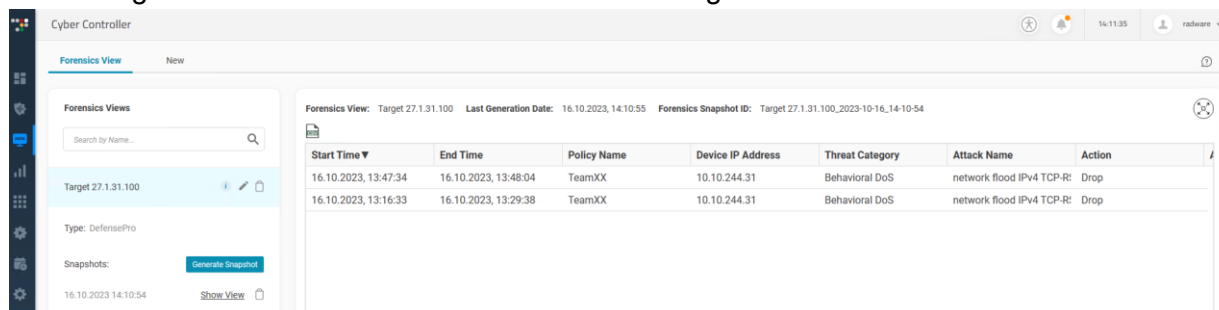
Use the **Forensics** module to analyze and discover the source of security attacks, attack methods and trends, or other problem incidents.

When the Forensics module generates an iteration of a forensics-view, it is referred to as a forensicsview *snapshot*. Each forensics-view snapshot can contain a maximum of 10,000 entries.

1. In **Cyber Controller**, select **AMS Analytics → Forensics**
2. Click on the **New** tab to create a new view
3. Use the following information for the new Forensics View:


Parameter	Value
Forensics Name	Target 27_1_31_100
Product	DefensePro
Policies	Select device and policy you created
Time	Today
Criteria	Destination IP Equals IPv4 27.1.31.100 - click Add Condition to use the criteria
Criteria > Apply To	Any Condition (OR)
Output	Select all fields
Format	HTML
Schedule	Run Report / Once

4. Click **Submit**
5. Select the **Forensic View** and click on **Generate Snapshot**
6. After it is generated click on the **Show View** that was generated.



7. Click on an event to see it's details

Attack Details



Refine View

Sampled Data

Close

Action	Drop	Protocol	TCP
Attack ID	37-1697192953	Radware ID	74
Threat Category	Behavioral DoS	Risk	High
Destination IP Address	27.1.31.100	Policy Name	TeamXX
Destination Port	25	Source IP Address	171.95.204.243
Device IP Address	10.10.244.31	Source Port	31337
Direction	In	Start Time	2023/10/16 13:16:33
Duration	785	Status	Terminated
End Time	2023/10/16 13:29:38	VLAN Tag	N/A
Attack Name	network flood IPv4 TCP-RST	Packet Type	Regular
Total Mbits Dropped	11504.98	Average Burst Rate	0 Kbps
Total Packets Dropped	27271119	State	Real-Time Signature Blocking
Attack Packet Rate (pps)	34784	Current Burst Number	0
Physical Port	1	Max. Burst Rate	0 Kbps

Real-Time Signature

Operator	Parameter	Value/s
[
OR	source-port	31337
]		
AND		
[
AND	packet-size	54
AND	destination-port	25

8. Use can use the icon to enlarge the view.

Alerts

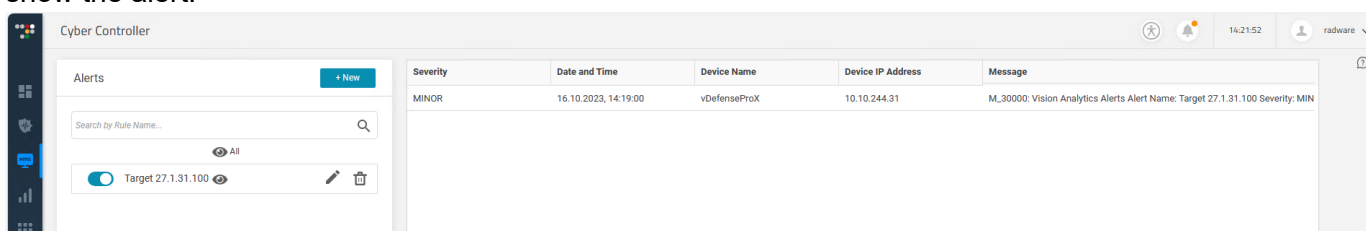
Use the Alerts module to create rules for alerts that Analytics generates. The Alerts screen displays the alert rules. You can turn alert rules on and off, as you require.

The right side of the Alerts screen can show the alerts from the alert rules. Alerts from alert rules that are turned go to the Cyber Controller Alerts Table pane. You can also configure alert rules to send alerts via email.

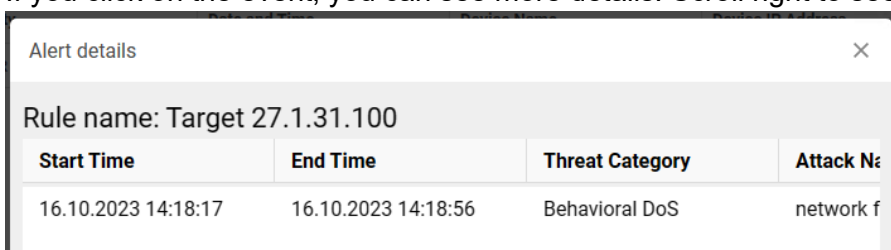
1. In **Cyber Controller**, select **AMS Analytics → Alerts**
2. Click on the **+New** button to create a new alert
3. Use the following information for the new Alerts View:

Parameter	Value
Alert Name	Target 27.1.31.100
Select Product	DefensePro
Scope	Select the device or the policy you configured
Criteria	Destination IP Equals IPv4 27.1.31.100 - click Add New Condition to use the criteria
Criteria → Apply To	Any Condition
Threshold → Run Alert	Send an alert any time the criteria match

4. Click **Submit**
5. Run a new attack against the target server to trigger the alert
6. When the alert gets triggered, you can see it. You might need to click on the “Shown/Hidden” eye icon to show the alert.



7. If you click on the event, you can see more details. Scroll right to see more details.

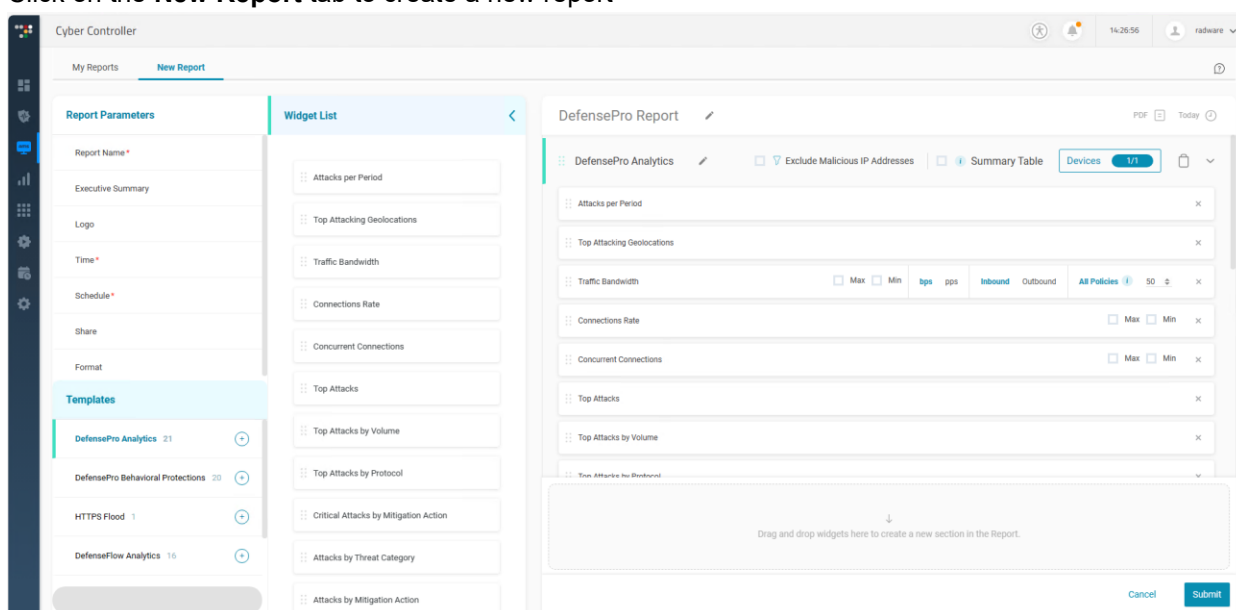



Reports

We will return to this section at the end of the training so the report will show enough activities.

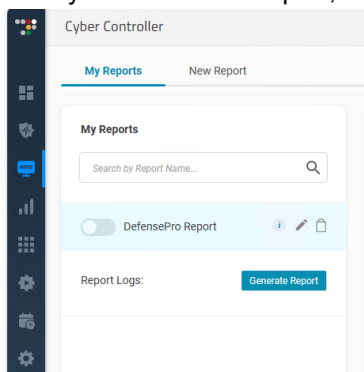
Use the Reports module to create and generate a report and view a single query on the fly. This is helpful when you want to quickly view data for a single query..

1. In **Cyber Controller**, select **AMS Analytics → Reports**
2. Click on the **New Report** tab to create a new report

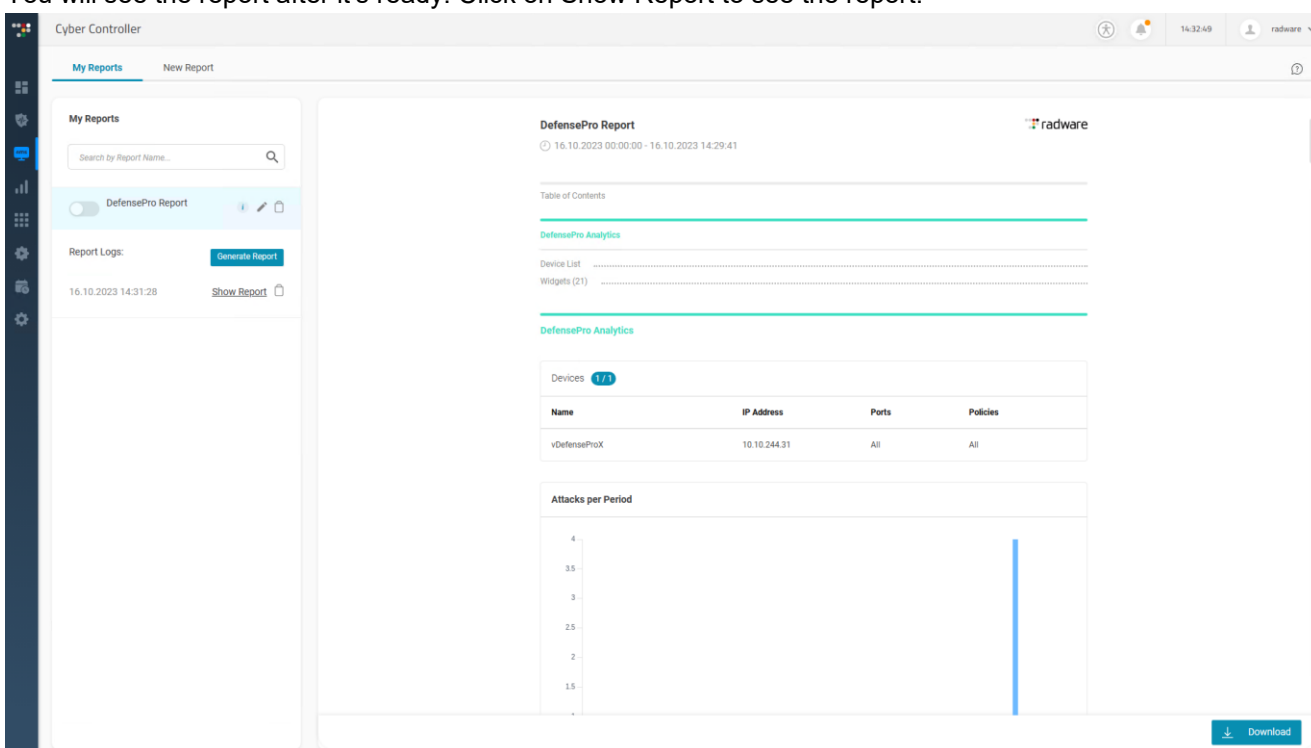


3. You can select between several different templates, create two reports one using the DefensePro Analytics and one using the DefensePro Behavioral Protections (use TeamXX policy) as template. Make sure you select a **time** range, there you have data to show (i.e. **This Week**). And select your device and policy for Behavioral template you need to select the device and the relevant protection policy.
4. Reports can be as well **Scheduled** and **Shared** via Email, so this would be useful, if you need to automatically generate a weekly/monthly report.
5. The **Format** of the report output can be PDF, HTML or CSV, depending on the purpose
6. At the Templates you can select what should be included. Use the  icon to add all widgets from a specific template

- After you created the report, we need to generate the report. Click on the Generate Report button.



- You will see the report after it's ready. Click on Show Report to see the report.



- Use the **Download File** button to export the report.



For questions, contact training@Radware.com

© 2019 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details, please see: <https://www.radware.com/LegalNotice/>. All other trademarks and names are property of their respective owners.