

VISTA NIDS - THREAT SUMMARY

21

High Alerts

12

Medium Alerts

71

Low Level Alerts

50

Information Log

Timeline Alert Chart



Recent Alerts

High Alert

User report_operator Tried to access unauthorised page. - 2025-04-26 02:57:33
User report_operator Tried to access unauthorised page. - 2025-04-25 10:36:40
User report_operator Tried to access unauthorised page. - 2025-04-23 14:19:53
User report_operator Tried to access unauthorised page. - 2025-04-23 14:19:46
Login blocke for user report operator due to multiple faille attempts.

Medium Alert

Admin report_admin created new user: delete_user. - 2025-04-28 02:26:22
Admin report_admin deleted user stha-aysh. - 2025-04-25 11:11:47
Admin e

Admin aayush deleted user test user. - 2025-04-20 16:40:00
Admin aayush deleted user cp4a. - 2025-04-20 16:39:12

Low Alert

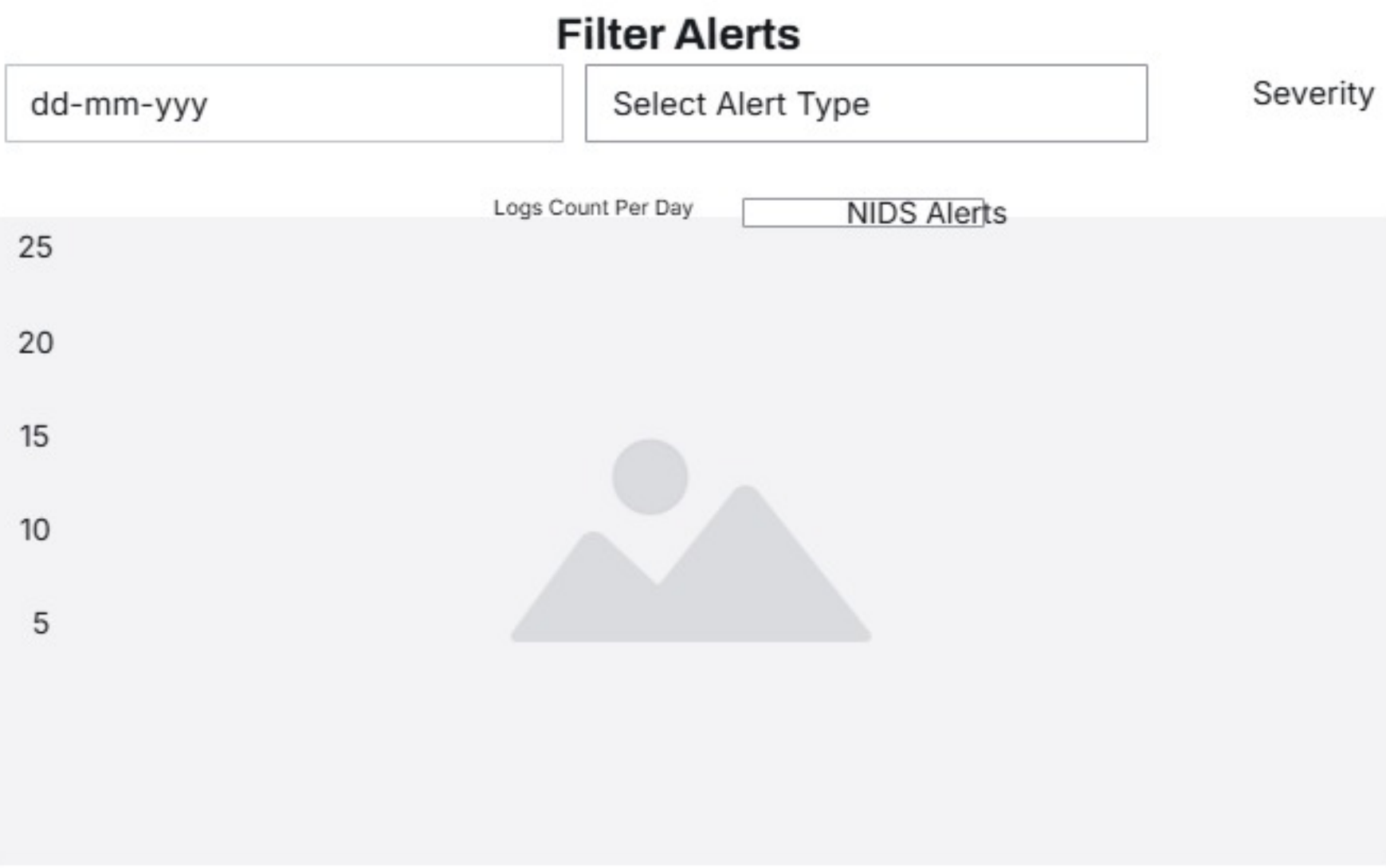
Failed login atempt for user repor_admin. Attempt number: 1 - 2025-04-28
Failed login attempt for user delete_user.Attempt number 1 - 2025-04-28
Failed login attempt for user operator_ user. Atempt number 1- 2025-04-26

Failed login attempt for user admin_user. Attempt number: 1 - 2025-04-26 09:33:41

Failed login attempt for user operator_user. Attempt number: 1 - 2025-04-26 09:33:21

Informations

User report_admin logged in successfully. - 2025-04-29 13:40:33
User report_admin logged in successfully. - 2025-04-29 07:22:21
User report_admin logged in successfully. - 2025-04-28 19:20:46
User report_admin logged in successfully. - 2025-04-28 07:21:18
User report_admin updated profile details. - 2025-04-28 01:46:00





Manage Users

[+ Create User](#)









Filter by Role

▼

Email Verification

▼

Sort by Date

	Profile	Username	Email	Phone	Role	Email Verified	Last Login	Date Joined	Actions
		report_operator	report.operator@test.com	+9779800000000	OPERATOR	Not Verified	Apr 24, 2025, 00:09	Apr 22, 2025	Edit Delete
		report_admin	np05cp4a220010@iic.edu.np	+977 1234500000	ADMIN	Verified	Apr 28, 2025, 07:21	Apr 22, 2025	Show Profile
		asmin-stha	asminshrestha248@gmail.com	23123231	OPERATOR	Not Verified	N/A	Mar 16, 2025	Edit Delete
		operator-wanem	NP05CP4A22001@iic.edu.np	+977 9891200000	OPERATOR	Not Verified	Mar 12, 2025, 15:48	Dec 29, 2024	Edit Delete
		aayush	ayushhaang09@gmail.com	None	ADMIN	Verified	Apr 22, 2025,02:28	Dec 29, 2024	Edit Delete



Upload PCAP File

Select PCAP File:

Choose File

No file chosen

Upload

Uploaded PCAP Files

Filename	Upload Date	Uploaded By	Size	Report
smallFlows.pcap	2025-03-09 04:31:20	username : aayush role : ADMIN	9444731 bytes	<div>View Report</div>



User Profile

View and manage user details



Not Verified

Send Verification

First name

documentation

Last name

operator

Username

report_operator

Email

report.operator@test.com

Phone Number

+9779800000000

Role

Operator

← Back to Users



Save Changes



Delete User



User Profile

Edit Profile

Delete Acco



documentation administrator

Role:Admin

Username: report_admin

Email: np05cp4a220010@iic.edu.np

Phone Number: +977 1234500000

Email Verified: Verified

Date Joined: April 22, 2025

Last Login: April 28, 2025, 7:21 a.m.

First Name:documentation

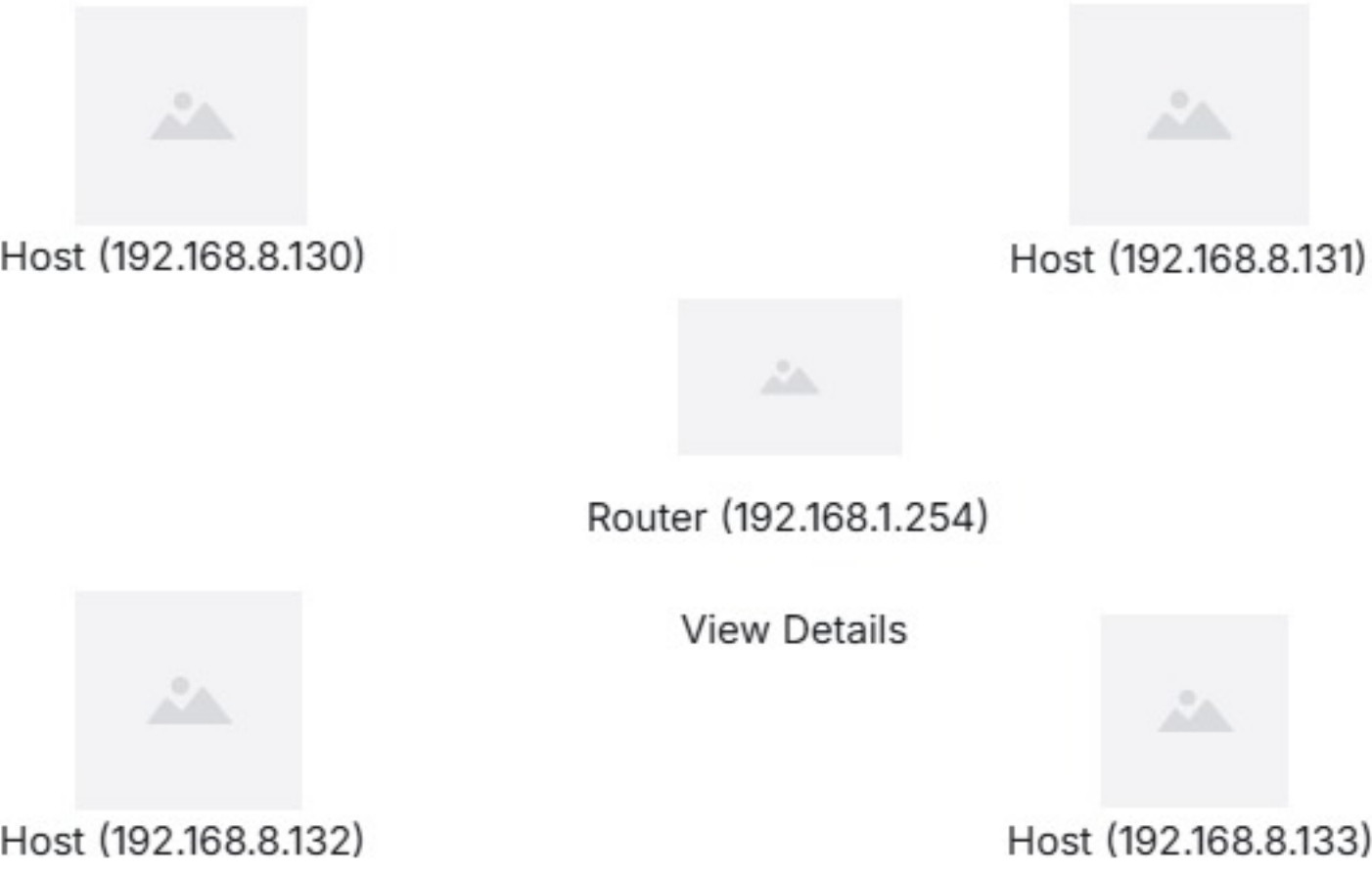
Last Name:administrator



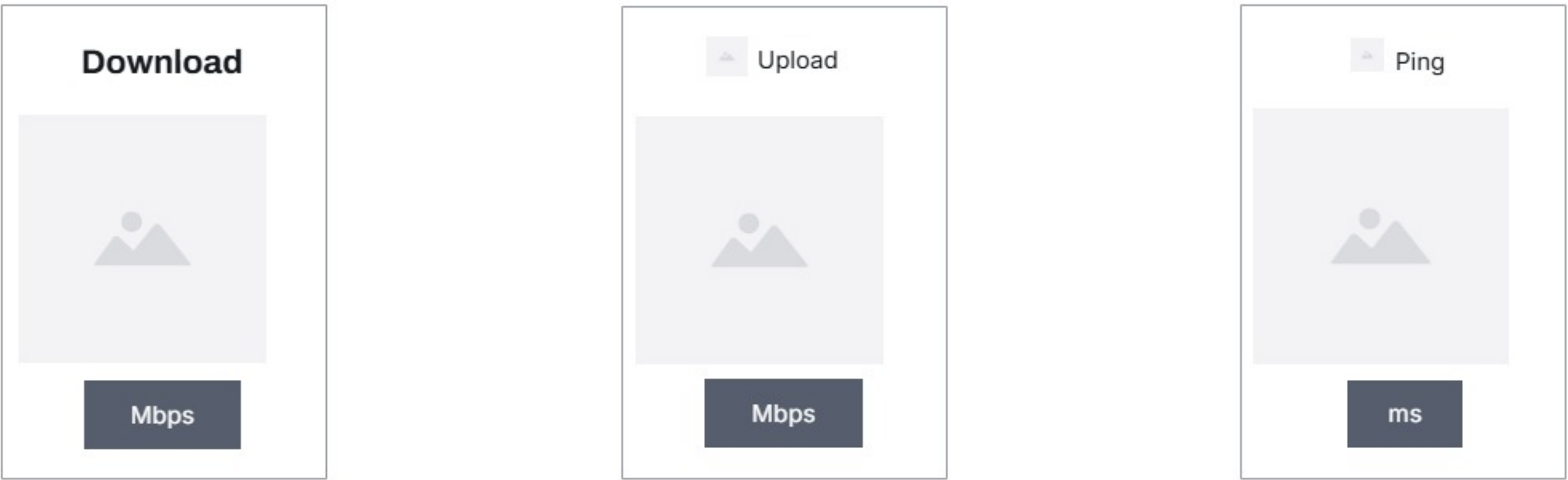
Network Information

Router IP.	192.168.1.254
Network Subnet	192.168.0.0/20
Online Devices	<div>3832</div>
Host IP	192.168.1.66
Total Available Hosts	4094

III Network Map



Network Performance





Admin Options

Manage Rules

Download Rules

Create a New Rule.

SID

Destination IP

Protocol

Destination Port

Action

Message

Source IP

Content

Source Port

Reference

Create Rule

Snort Rules

alert any any any → any any (sid:1000001; rev:1;)



Manage Rules

Go Back

ID	Action	Protocol	Source IP	Source Port	Destination IP	Destination Port	Payload	Message	Reference	Options
100001	alert	tcp	\$EXTERNAL_NET	any	192.168.1.254	3000	"Incorrect Credentials"	Failed login attempt detected on API, Someone tried to login to the router	aayush	dit ID
SID00007	alert	tcp	\$EXTERNAL_NET	any	any	any	uid=0(root)	Potential Command Injection Detected: uid=0(root)	report_admin	ditID
SID001	alert	tcp	172.20.10.4	any	172.20.10.4	any	admin'	sqli injection payload detected	aayush	ditTD
SIDO0124	alert	tcp	\$EXTERNAL_NET	any	\$HOME_NET	any	Incorrect Credentials	Login Failure - Incorrect Credentials Detected	aayush	dit D
SID004	alert	tcp	\$EXTERNAL_NET	any	\$HOME_NET	443	union select	sqli injection payload detected	aayush	dit D
SID007	alert	tcp	any	any	192.168.1.254	22		attempt to connect to the router using ssh	aayush	dit ID

[Home](#)[NIDS](#)[Network Map](#)[Pcap Analyzer](#)[Manage Rules](#)[Manage User](#)[Settings](#)[? Logout](#)

Edit Rule (SID: 100001)

Action

alert

Protocol

tcp

Source IP

\$EXTERNAL_NET

Source Port

any

Destination IP

192.168.1.254

Destination Port

3000

Payload

"Incorrect Credentials"

Message

Failed login attempt detected on API, Someone tried to login to the router

Reference

Internal monitoring - login failure detection

Save Changes

Cancel



Download Rules

Filter by Protocol:

Show All

Add Rules

Download Rules

	Rule ID	Message	Action	Protocol
	100001	Failed login attempt detected on API, Someone tried to login to the router	alert	tcp
2	SID00007	Potential Command Injection Detected: uid=0(root)	alert	tcp
3	SID001	sqli injection payload detected	alert	tcp
4	SIDO0124	Login Failure - Incorrect Credentials Detected	alert	tcp
5	SIDO04	sqli injection payload detected	alert	tcp
	SID007	attempt to connect to the router using ssh	alert	tcp

: List of Outgoing IP Addresses

#	External IP	Count
<div><div></div><div></div><div></div><div></div><div></div></div>	52.54.161.49	2
	20.42.72.131	2
	69.173.158.64	59
	18.66.41.49	34
	20.189.173.1	61
<div><div></div><div></div><div></div><div></div><div></div></div>	20.42.65.84	5
<div><div></div><div></div><div></div><div></div><div></div></div>	18.66.41.56	34
<div><div></div><div></div><div></div><div></div><div></div></div>	185.53.177.51	22
<div><div></div><div></div><div></div><div></div><div></div></div>	52.168.117.171	
	204.79.197.203	16
	34.95.44.106	27
	188.166.199.38	14
	152.42.150.143	14
<div><div></div><div></div><div></div><div></div><div></div></div>	142.250.194.130	29
	104.108.236.221	153
	163.181.81.230	689
	47.246.136.160	208
	104.108.236.198	29
<div><div></div><div></div><div></div><div></div><div></div></div>	47.246.174.152	
<div><div></div><div></div><div></div><div></div><div></div></div>	124.41.244.35	42