

ABC Corporation Daily SOC Report

INFOPERCEPT
Sample Report 2021

YOUR DATE HERE

COMPANY NAME
Authored by: Your Name



 **Infopercept**
Your Ally in Digital Warfare

This document is a highly confidential which contains all the information regarding the red team engagement that was done by Infopercept Team on ABC Company.

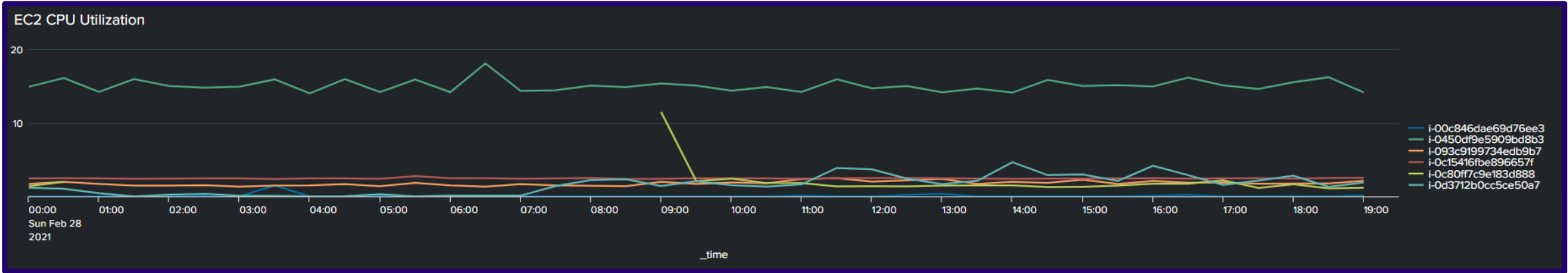
AWS Security Report@ABC Corporation



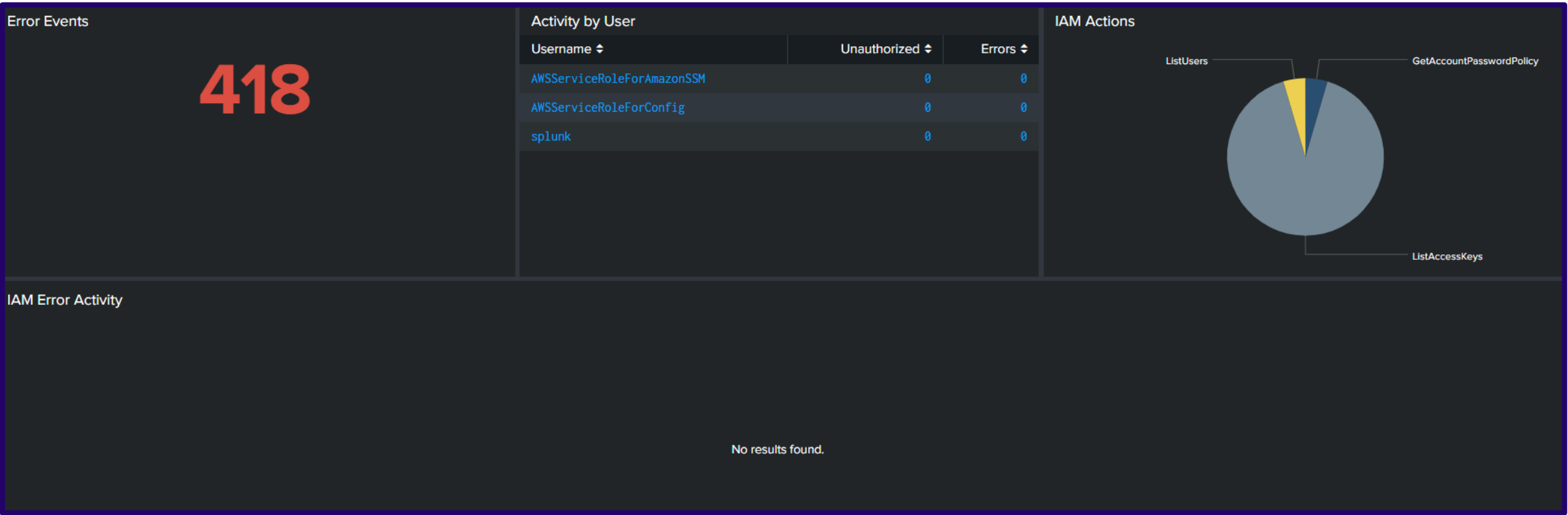
AWS Overview : Apps Servers

Running Instances	33 (9:00AM to 9:00PM)
Stopped Instances	33
Production Instances	21

PRIVATE_IP_ADDRESS	KEY_NAME	ID	INSTANCE_TYPE
10.0.1.1	Adm	i-0450df9e5909bd8b3	r5a.2xlarge
10.0.2.1	Pro	i-07bc6d596daa7a14a	r5.8xlarge
10.0.3.2	Pro	i-093c9199734edb9b7	r5.8xlarge
13.2.33.9	Lir Ta	i-0c15416fbe896657f	t2.medium
13.1.1-7-	Linux	i-0c80ff7c9e183d888	m5a.4xlarge
1.1	L s	i-0d3712b0cc5ce50a7	c5a.2xlarge
10.1	L s	i-0f6926fd1e5c1dc4c	c5a.2xlarge
1.1	N Red E	i-00c846dae69d76ee3	c5.large
1.1	N Red E	i-07ba56ebef8409f8f	c5.large



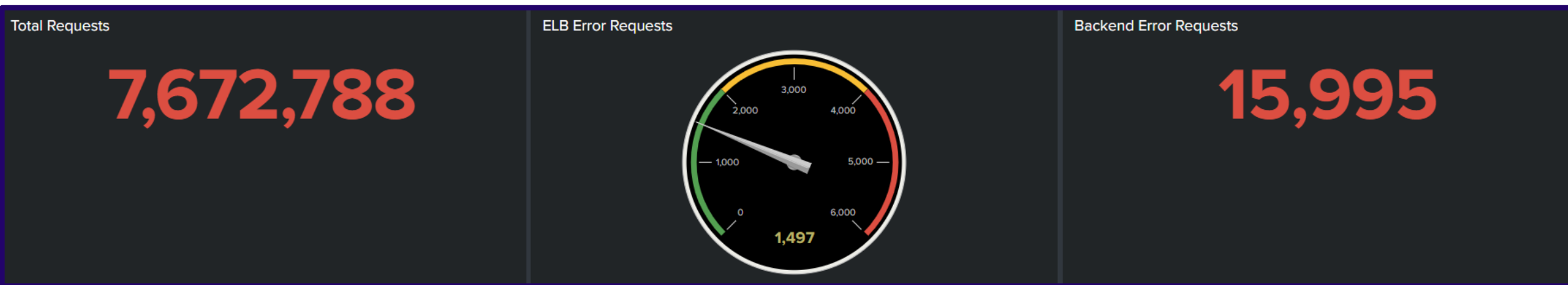
IAM User Activity – Normal Activity



IAM Error Activity

No results found.

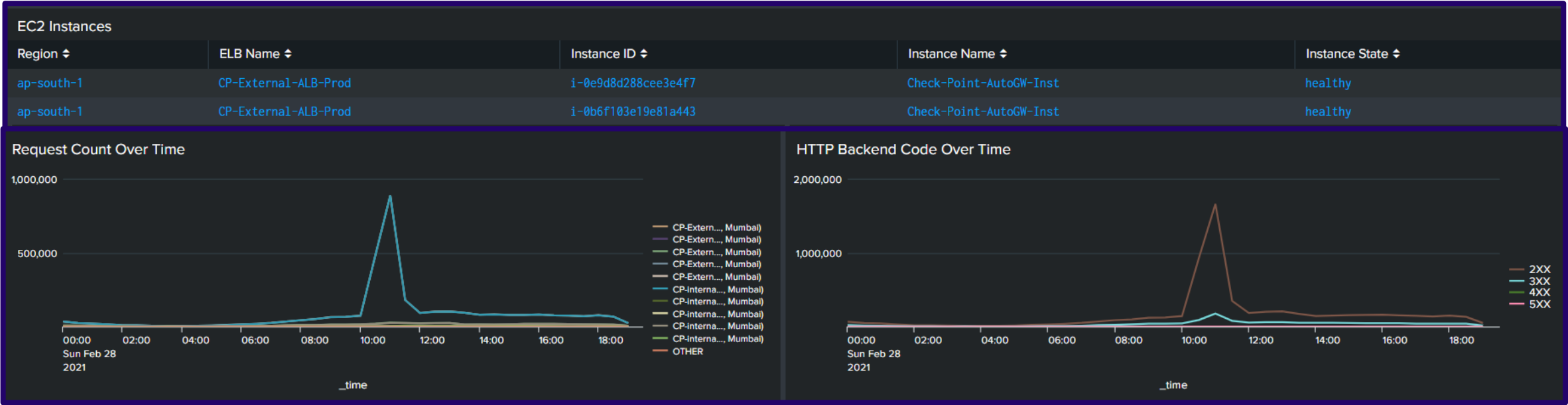
ELB Instances – CP-External ALB



ELB Instances – CP-External ALB

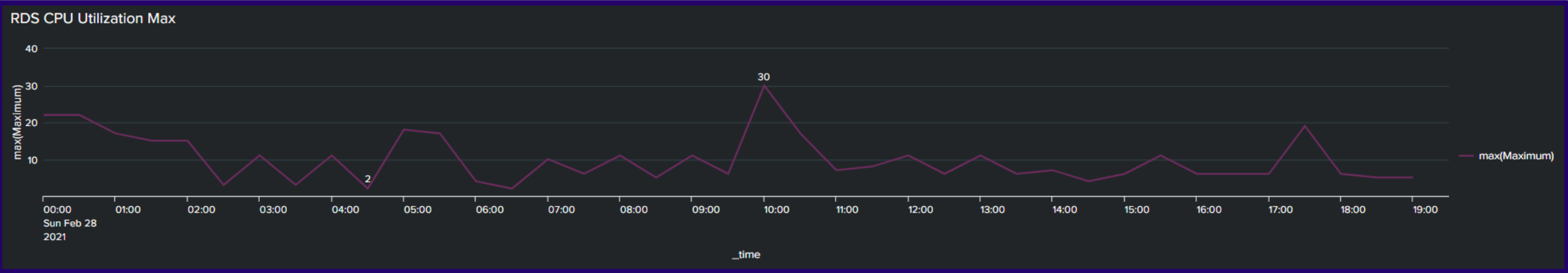
Backend Error Requests		
metric_name ↕	metric_dimensions ↕	count ↕
HTTPCode_Target_4XX_Count	LoadBalancer=[app/CP-External-ALB-B...c344ee]	95.0
HTTPCode_Target_4XX_Count	LoadBalancer=[app/CP-External-ALB-C...a634d]	14.0
HTTPCode_Target_4XX_Count	LoadBalancer=[app/CP-External-ALB-P...93ee24]	3661.0
HTTPCode_Target_4XX_Count	LoadBalancer=[app/CP-External-ALB-S...11c9c]	550.0
HTTPCode_Target_4XX_Count	LoadBalancer=[app/CP-External-ALB-p...6010839870]	1505.0
HTTPCode_Target_4XX_Count	LoadBalancer=[app/CP-internal-ALB-B...b0e8f]	1505.0
HTTPCode_Target_4XX_Count	LoadBalancer=[app/CP-internal-ALB-C...0b105]	14.0
HTTPCode_Target_4XX_Count	LoadBalancer=[app/CP-internal-ALB-r...d2053a81703]	95.0
HTTPCode_Target_4XX_Count	LoadBalancer=[app/CP-internal-ALB-r...74f02dd288a]	3549.0
HTTPCode_Target_4XX_Count	LoadBalancer=[app/CP-internal-ALB-r...8ef9716c336]	541.0
HTTPCode_Target_5XX_Count	LoadBalancer=[app/CP-External-ALB-B...c344ee]	37.0
HTTPCode_Target_5XX_Count	LoadBalancer=[app/CP-External-ALB-C...a634d]	9.0
HTTPCode_Target_5XX_Count	LoadBalancer=[app/CP-External-ALB-P...93ee24]	1619.0
HTTPCode_Target_5XX_Count	LoadBalancer=[app/CP-External-ALB-S...11c9c]	130.0
HTTPCode_Target_5XX_Count	LoadBalancer=[app/CP-External-ALB-p...6010839870]	748.0
HTTPCode_Target_5XX_Count	LoadBalancer=[app/CP-internal-ALB-B...b0e8f]	185.0
HTTPCode_Target_5XX_Count	LoadBalancer=[app/CP-internal-ALB-C...0b105]	9.0
HTTPCode_Target_5XX_Count	LoadBalancer=[app/CP-internal-ALB-r...d2053a81703]	37.0
HTTPCode_Target_5XX_Count	LoadBalancer=[app/CP-internal-ALB-r...74f02dd288a]	1560.0
HTTPCode_Target_5XX_Count	LoadBalancer=[app/CP-internal-ALB-r...8ef9716c336]	132.0

ELB Instances – CP-External ALB

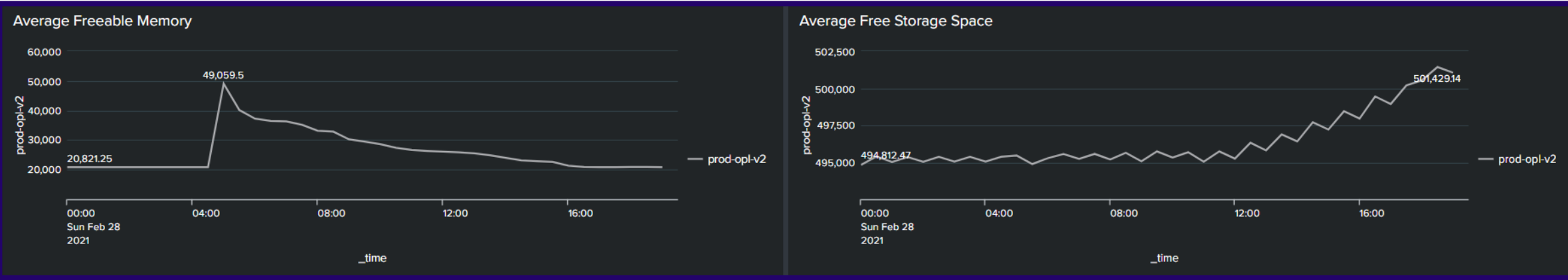


RDS CPU & Memory Utilization: prod rds

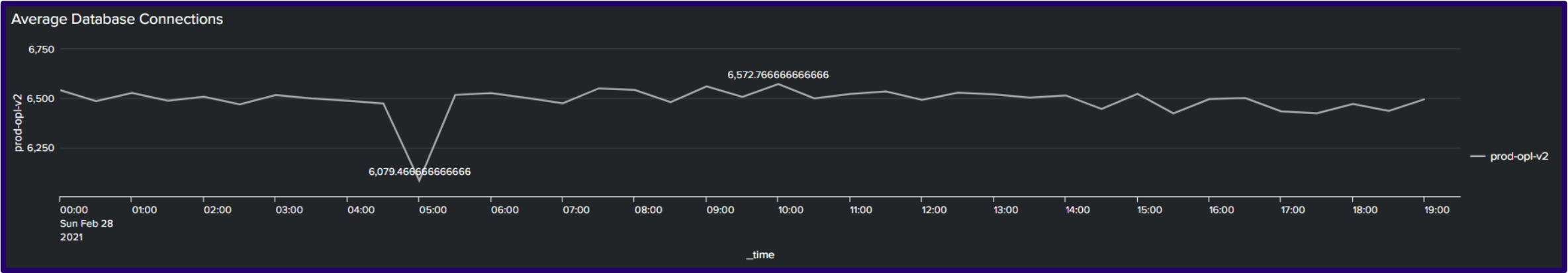
We Observed Normal CPU Utilization of Prod-



Average Freeable Memory of Prod- is 20 GB and Storage 501 GB



Average Database Connection of Prod was between from 6541 to 6495



Total Services Restarted (10.0.5.229)

0

Services Restarted over Time (10.0.5.229)

No results found.

Total Services Restarted (10.0.4.252)

0

Services Restarted over Time (10.0.4.252)

No results found.

Cloud Trail Alert: Instances: Run/Start Actions

eventTime ↕	awsRegion ↕	PreviousInstanceState ↕	CurrentInstanceState ↕	userIdentity.arn ↕	src ↕	instanceId ↕	count ↕
2021-02-27T19:00:20Z	ap-south-1	running	StopInstances	arn:aws:sts::652918353734:assumed-role/Lambda_ec2_execution/Dr-tableauec2server-stop	13.233.58.252	i-02e15052ddf663501	1
2021-02-27T19:00:44Z	ap-south-1	running	StopInstances	arn:aws:sts::652918353734:assumed-role/Lambda_ec2_execution/Linux-Tableau-RedHat-7-April-2019-Ec2-Stop	52.66.40.155	i-0c80ff7c9e183d888	1
2021-02-28T03:30:43Z	ap-south-1	stopped	StartInstances	arn:aws:sts::652918353734:assumed-role/Lambda_ec2_execution/Linux-Tableau-RedHat-7-April-2019-Ec2-Start	13.127.227.71	i-0c80ff7c9e183d888	1
2021-02-28T04:00:14Z	ap-south-1	stopped	StartInstances	arn:aws:sts::652918353734:assumed-role/Lambda_ec2_execution/Tableau-server-13-04-2020-Ec2-Start	13.235.215.39	i-04e456d77c2b305cf	1
2021-02-28T05:00:22Z	ap-south-1	running	StopInstances	arn:aws:sts::652918353734:assumed-role/Lambda_ec2_execution/Tableau-server-13-04-2020-Ec2-Stop	3.7.70.121	i-04e456d77c2b305cf	1

Linux Auditd : Production Server User Activity

_time ↕	host ↕	user ↕	cwd ↕	command ↕	action ↕
2021-02-28 11:56:41.484	ip-10-0-5-229		/apps/services/odop/service-connect-odop	nano config/application.properties	success

Operating System	Kernel	IP Address	Last Boot
Enterprise Linux 7	3.10.0-1062 (x86_64)	10.0.4.252	107 day/s ago

Operating System	Kernel	IP Address	Last Boot
Enterprise Linux 7	3.10.0-1062 (x86_64)	10.0.5.229	25 day/s ago

Top Users (last 7 days)	
user ↕	login_count ↕
	10
	8
	7
	6
	3
	1
	1
	1

RDS Backup and Restart Activity

Backup	
Automated backups Enabled (7 Days)	Latest restore time February 28, 2021, 1:30:00 PM UTC
Copy tags to snapshots Enabled	Backup window 18:23-18:53 UTC (GMT)

Snapshot: snap-034baf063cb9f8d1f (prod-ABC-v2-2)

Description

Permissions

Tags

Snapshot ID	snap-034baf063cb9f8d1f	Progress	100%
Status	completed	Capacity	425 GiB
Volume	vol-08c5981bca82edb4e	Encryption	Encrypted
Started	February 28, 2021 at 12:37:14 AM UTC+5:30	KMS Key ID	f07adcf6-b93c-4ab4-b69e-0f3ef74fef4b
Owner	652918353734	KMS Key Aliases	
Product codes	-	KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/f07adcf6-b93c-4ab4-b69e-0f3ef74fef4b
Description	Created for policy: policy-0fa874dcebb801043 schedule: Schedule 1	Fast Snapshot Restore	-
Outpost ARN	-		



Snapshot: snap-0ca8a5c1ea35294ab (MFI-Live-Production)

Description

Permissions

Tags

Snapshot ID	snap-0ca8a5c1ea35294ab
Status	completed
Volume	vol-0696130454ed50b5e
Started	February 28, 2021 at 12:30:37 AM UTC+5:30
Owner	652918353734
Product codes	-
Description	Created for policy: policy-09b83c29cda2204e6 schedule: Default Schedule
Outpost ARN	-

Progress	100%
Capacity	250 GiB
Encryption	Encrypted
KMS Key ID	f07adcf6-b93c-4ab4-b69e-0f3ef74fef4b
KMS Key Aliases	
KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/f07adcf6-b93c-4ab4-b69e-0f3ef74fef4b
Fast Snapshot Restore	-



Snapshot: snap-0bf451e848a214ed4 (Admin-panel-Instance)

Description

Permissions

Tags

Snapshot ID	snap-0bf451e848a214ed4	Progress	100%
Status	completed	Capacity	190 GiB
Volume	vol-0a227955afc2c55ed	Encryption	Encrypted
Started	February 28, 2021 at 12:18:24 AM UTC+5:30	KMS Key ID	f07adcf6-b93c-4ab4-b69e-0f3ef74fef4b
Owner	652918353734	KMS Key Aliases	
Product codes	-	KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/f07adcf6-b93c-4ab4-b69e-0f3ef74fef4b
Description	Created for policy: policy-040b7cb22a3c6b472 schedule: Schedule 1	Fast Snapshot Restore	-
Outpost ARN	-		

Tableau-RedHat-7-Linux-var-opt-partition Backup



Snapshot: snap-0bdecd51edc9bc66e (Tableau-RedHat-7-Linux-var-opt-partition)

Description

Permissions

Tags

Snapshot ID snap-0bdecd51edc9bc66e
Status completed
Volume [vol-029e055fb963cb779](#)
Started February 28, 2021 at 12:12:58 AM UTC+5:30
Owner 652918353734
Product codes -
Description Created for policy: policy-05113fe7c7804bf6b
schedule: Schedule 1
Outpost ARN -

Progress 100%
Capacity 100 GiB
Encryption Not Encrypted
KMS Key ID
KMS Key Aliases
KMS Key ARN
Fast Snapshot Restore -

Tableau-RedHat-7-Linux-opt-partition Backup



Snapshot: snap-00c965f40ba03c70c (Tableau-RedHat-7-Linux-opt-partition)

Description

Permissions

Tags

Snapshot ID

snap-00c965f40ba03c70c

Progress

100%

Status

completed

Capacity

100 GiB

Volume

vol-014a96999c7ef8464

Encryption

Not Encrypted

Started

February 28, 2021 at 12:12:06 AM UTC+5:30

KMS Key ID

Owner

652918353734

KMS Key Aliases

Product codes

-

KMS Key ARN

Description

Created for policy: policy-03e0c993a845c8943
schedule: Schedule 1

Fast Snapshot Restore

-

Outpost ARN

-

Snapshot: snap-024ebb7471b5168ec (Live-ITR-Gunicorn-scraping-server-01-100GB)

Description	Permissions	Tags
Snapshot ID	snap-024ebb7471b5168ec	
Status	completed	
Volume	vol-0e1afe3e49d12bcd4	
Started	February 28, 2021 at 12:10:46 AM UTC+5:30	
Owner	652918353734	
Product codes	-	
Progress	100%	
Capacity	100 GiB	
Encryption	Encrypted	
KMS Key ID	f07adcf6-b93c-4ab4-b69e-0f3ef74fef4b	
KMS Key Aliases		
KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/f07adcf6-b93c-4ab4-b69e-0f3ef74fef4b	
Fast Snapshot Restore	-	
Description	Created for policy: policy-04628df6e338466ea schedule: Schedule 1	
Outpost ARN	-	

Snapshot: snap-0fc9085ba3b58599f (Live-ITR-Gunicorn-scraping-server-02-100GB)

Description

Permissions

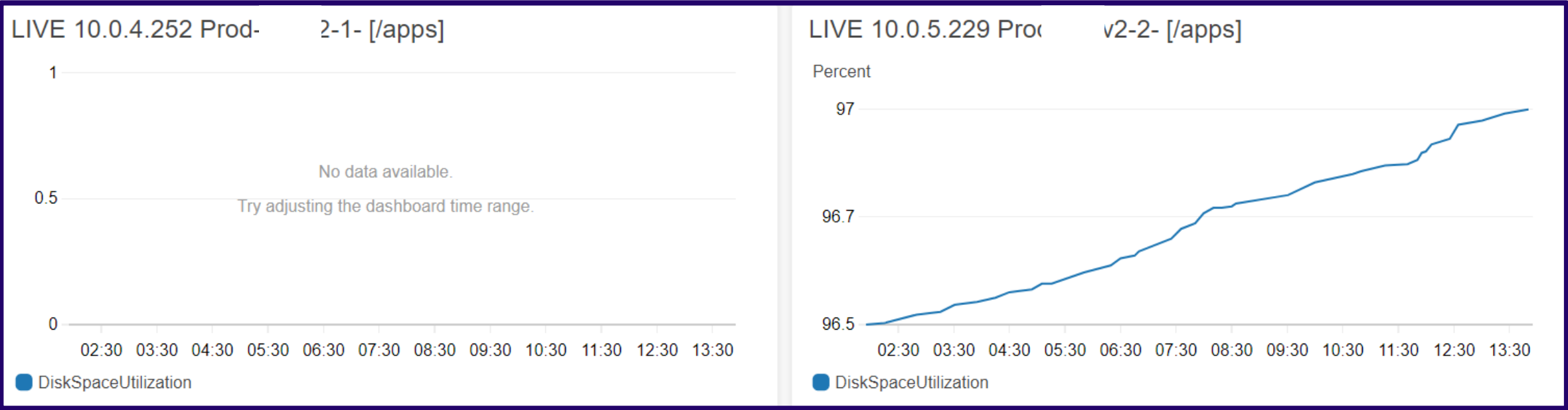
Tags

Snapshot ID	snap-0fc9085ba3b58599f
Status	completed
Volume	vol-0e623545a0c9afab5
Started	February 28, 2021 at 12:27:03 AM UTC+5:30
Owner	652918353734
Product codes	-
Description	Created for policy: policy-0d7dc7fbc33e92c41 schedule: Schedule 1
Outpost ARN	-

Progress	100%
Capacity	100 GiB
Encryption	Encrypted
KMS Key ID	f07adcf6-b93c-4ab4-b69e-0f3ef74fef4b
KMS Key Aliases	
KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/f07adcf6-b93c-4ab4-b69e-0f3ef74fef4b
Fast Snapshot Restore	-

Snapshot: snap-0de0347ababbdcbbb (Pre-Production-29-07-2020)

Description	Permissions	Tags
Snapshot ID	snap-0de0347ababbdcbbb	Progress100%
Status	completed	Capacity250 GiB
Volume	vol-09fe8781ea9c3fb07	EncryptionEncrypted
Started	February 28, 2021 at 12:12:46 AM UTC+5:30	KMS Key IDf07adcf6-b93c-4ab4-b69e-0f3ef74fef4b
Owner	652918353734	KMS Key Aliases
Product codes	-	KMS Key ARNarn:aws:kms:ap-south-1:652918353734:key/f07adcf6-b93c-4ab4-b69e-0f3ef74fef4b
Description	Created for policy: policy-0c772ae92c69a66d0 schedule: Schedule 1	Fast Snapshot Restore-
Outpost ARN	-	

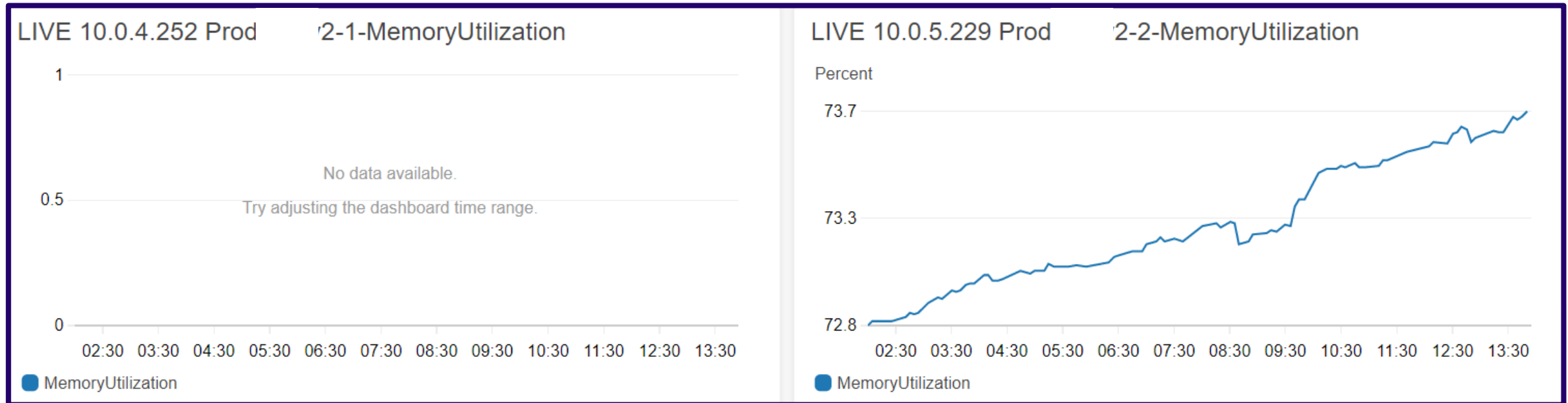


Prod-ABC-v2-1 –

Server is not running

Prod-ABC-v2-2 – 97.00%

Host Monitoring - /Memory Utilization

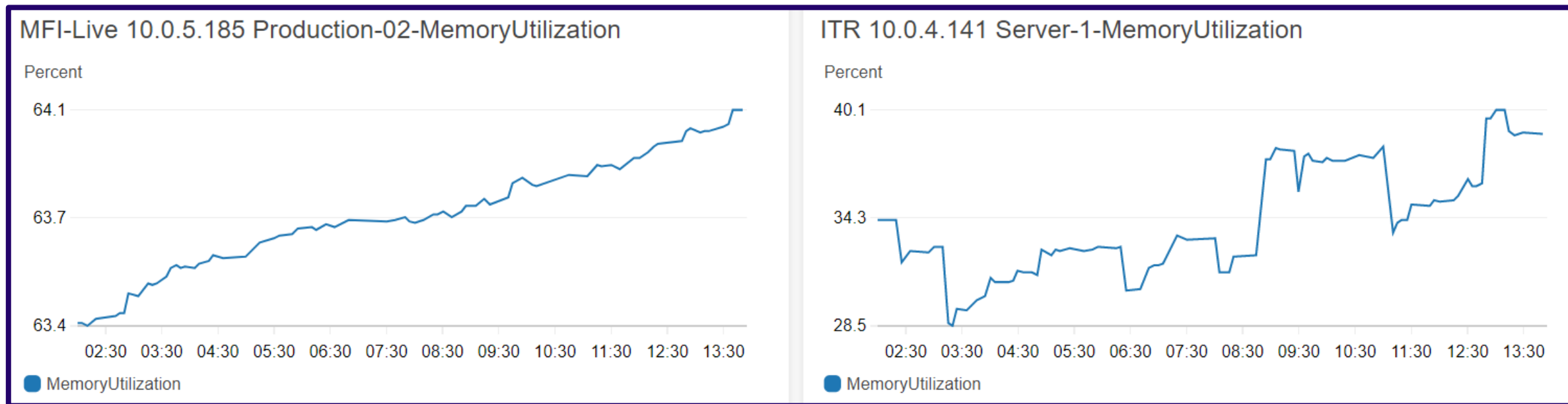


Prod-ABC-v2-1

Server is not running

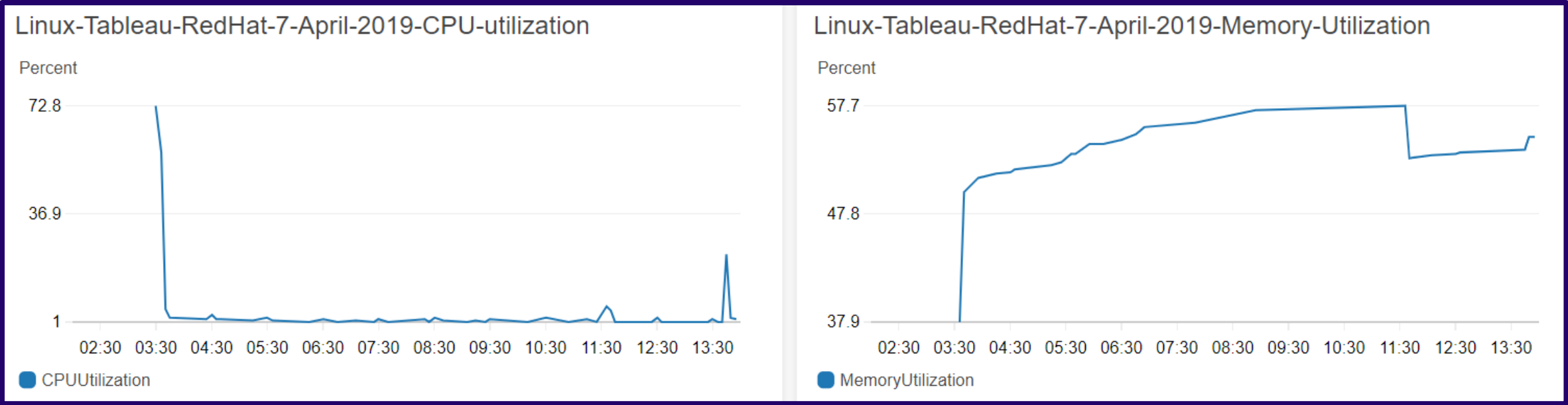
Prod-ABC-v2-2 – 73.71%

Host Monitoring - /Memory Utilization



MFI-Live 10.0.5.185 Production-02 – 64.05%

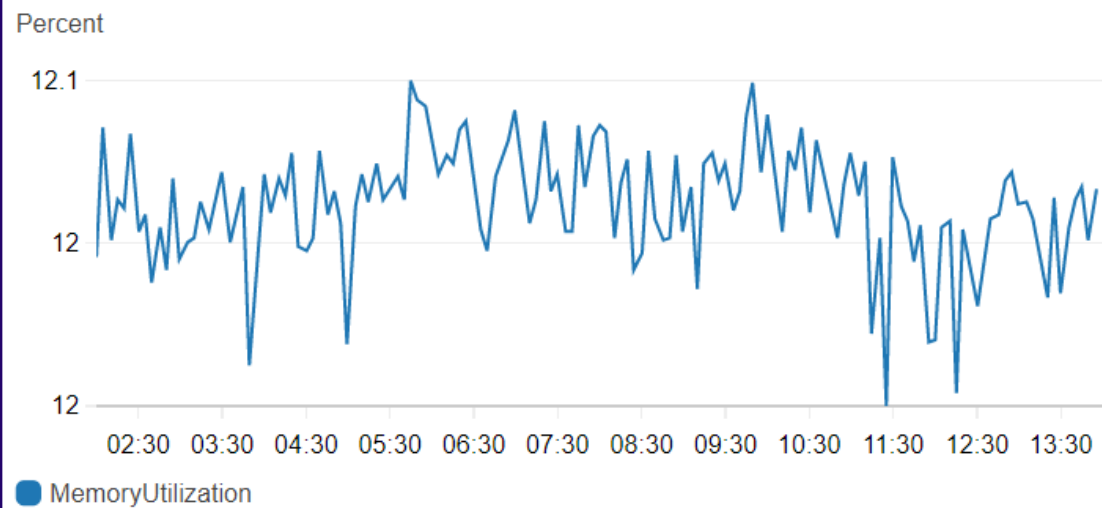
ITR 10.0.4.141 Server-1 – 38.81%



Linux-Tableau-RedHat-7-April-2019 CPU-Utilization – 1.8%

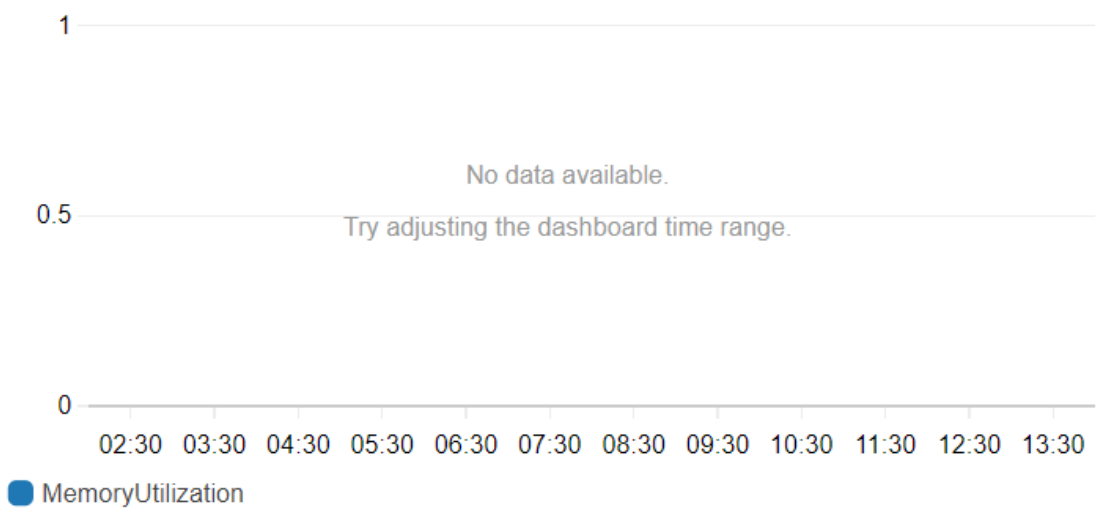
Linux-Tableau-RedHat-7-April-2019 Memory-Utilization – 54.81%

Nginx-LB-Enterprise-Redhat-Production-

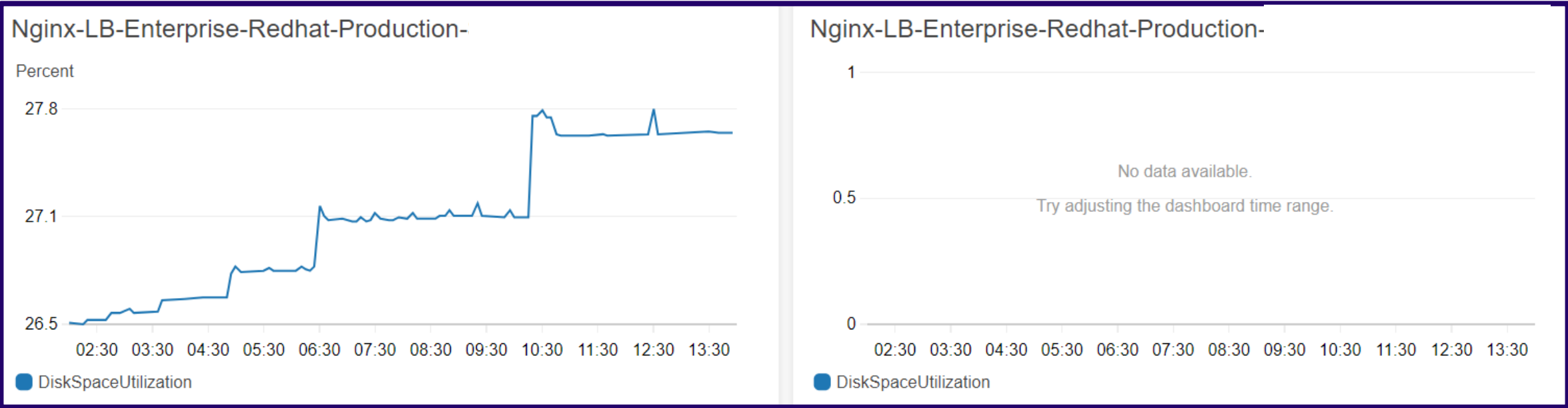


Nginx-LB-Enterprise-Redhat-Production-
MEMORY-Utilization – 12.04%

Nginx-LB-Enterprise-Redhat-Production-



Nginx-LB-Enterprise-Redhat-Production-
-BackupServer
MEMORY-Utilization –
Server is not running



Nginx-LB-Enterprise-Redhat-Production-
Disk-Utilization – 27.66%


Nginx-LB-Enterprise-Redhat-Production-
BackupServer
Disk-Utilization –

Server is not running


Site Lock & Trust Guard Report @ABC Corporation




Security Summary										
Domain		Malware	Spam	Vulnerability	SSL	Risk Score	SMART	PatchMan	SMART DB	WAF Plan
		Good	Good	Good	Good	Low	Upgrade	Upgrade	Upgrade	Upgrade
		Good	Good	Good	Good	Low	Pending	Pending	Upgrade	Upgrade
		Good	Good	Good	Good	Low	Upgrade	Upgrade	Upgrade	Upgrade
		Good	Good	Good	Good	Low	Good	Good	Pending	Upgrade
		Good	Good	Good	Good	Low	Pending	Pending	Upgrade	Upgrade




MALWARE SCAN
Last Good Scan: 2/28/2021
Last Scan: 2/28/2021




RISK SCORE
Last Scan: 2/28/2021



SPAM SCAN
Last Good Scan: 2/28/2021
Last Scan: 2/28/2021



SSL SCAN
Last Good Scan: 6/30/2020
Last Scan: 2/27/2021



VULNERABILITY SCAN
Last Good Scan: 2/28/2021
Last Scan: 2/28/2021

Site Status

Website Details

Blacklist Status

Blacklist Status

✓ Domain clean by Google Safe Browsing:

✓ Domain clean by Norton Safe Web:

✓ Domain clean on PhishTank:

✓ Domain clean on the Opera browser:

✓ Domain clean by SiteAdvisor:

✓ Domain clean by the Sucuri Malware Labs:

✓ Domain clean on SpamHaus DBL:


✓ Domain clean on Yandex (via Sophos):

✓ Domain clean by ESET:

Site Status

Website Details

Blacklist Status




Website:

Site Status:

Blacklist Status:

OK


OK



Malware Scan Status

PASSED

2021-02-23 04:15:50



Latest Scan Status

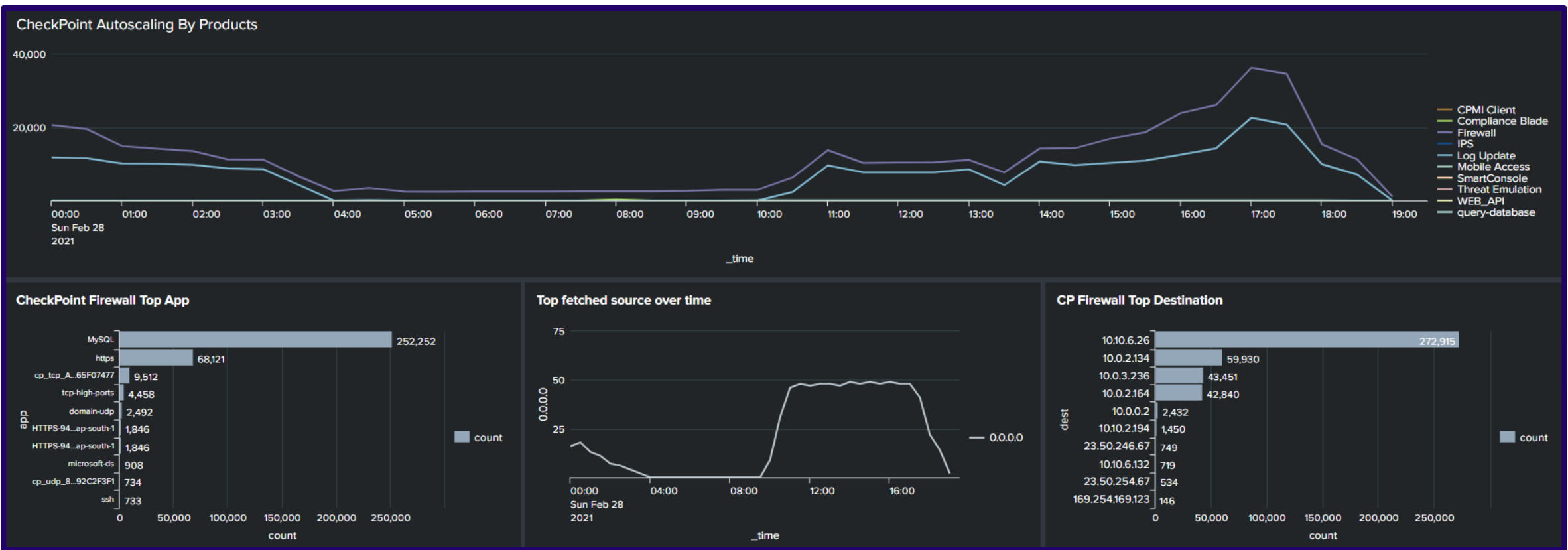
PASSED

2021-02-25 07:54:26

View Reports

Check Point Report @ABC Corporation





Threat Emulation Top 10 Source count

No results found.

Threat Emulation Top 10 Destination count

No results found.

Check Point – Application and URL Filtering

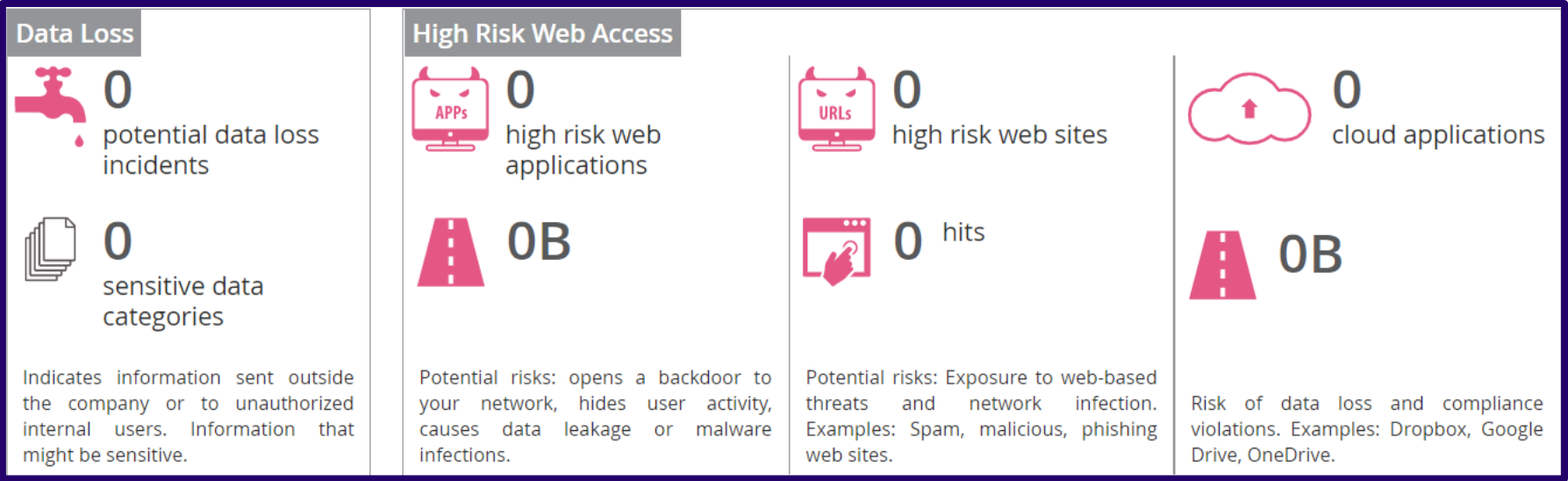
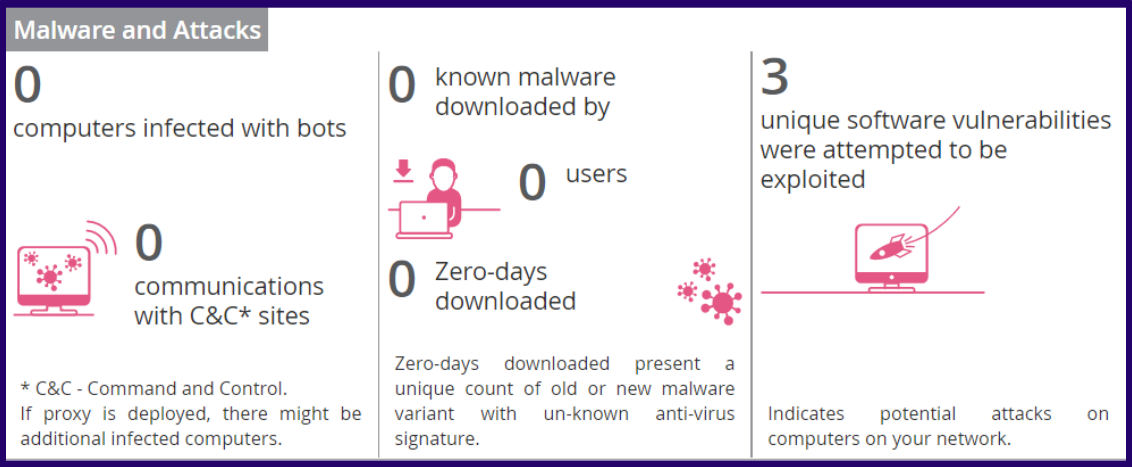
General Activity

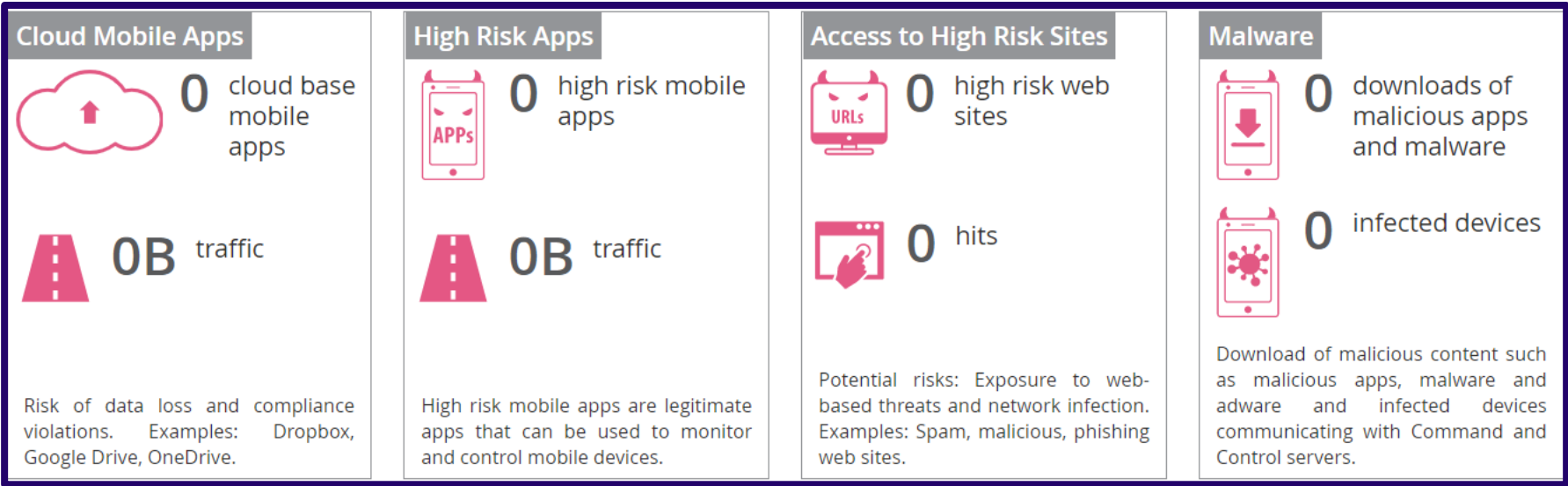
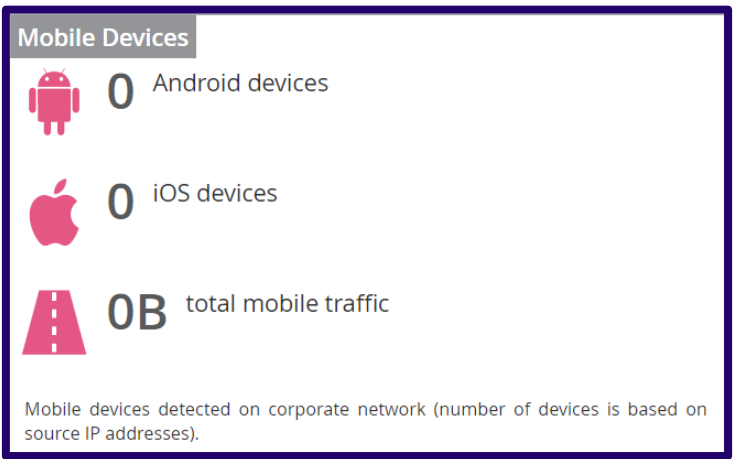
Note: Migration is going on for ABC testing.

High Bandwidth Applications

Note: Migration is going on for ABC testing.

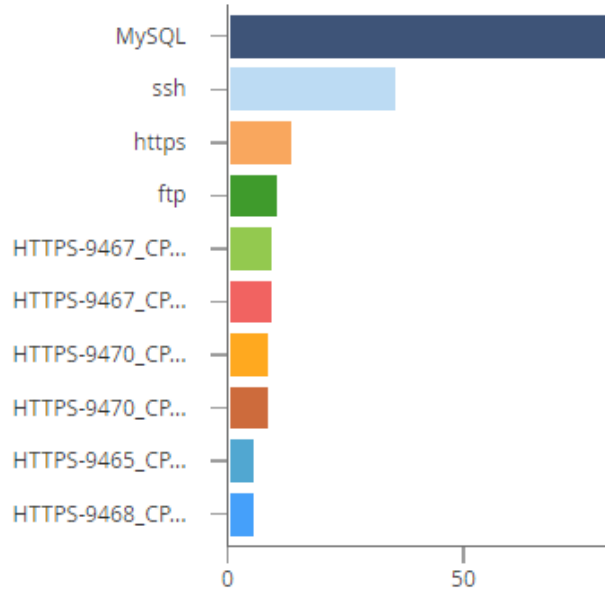
Executive Summary of Security Checkup



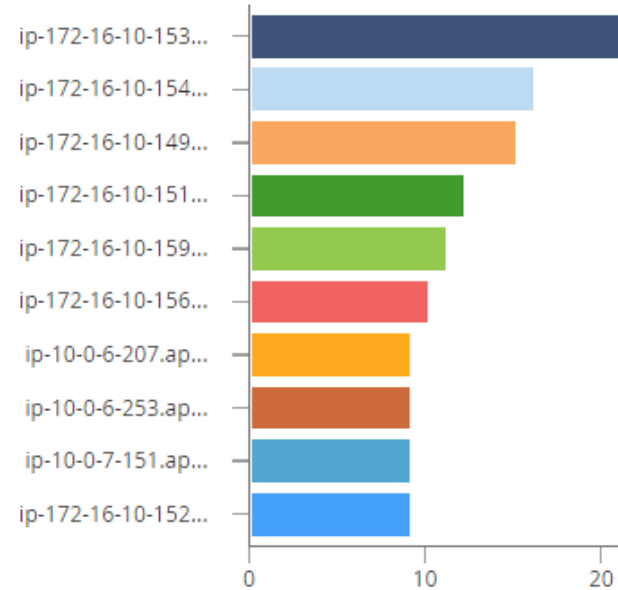


Network Traffic Analysis

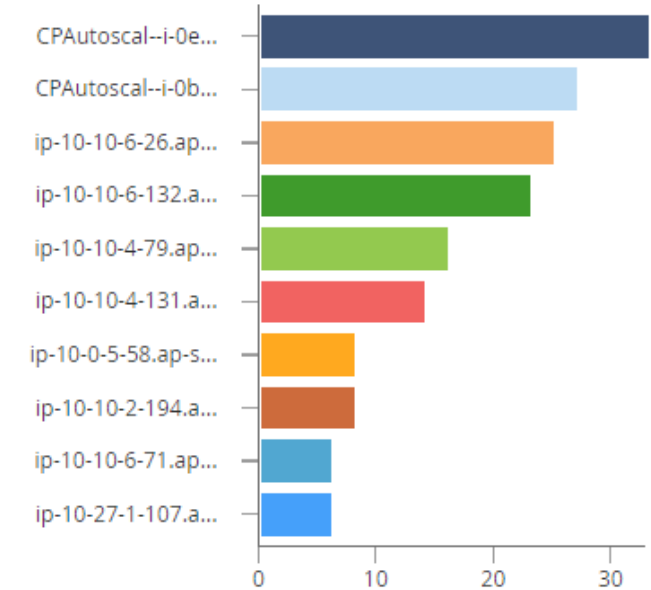
Top Services



Top Sources

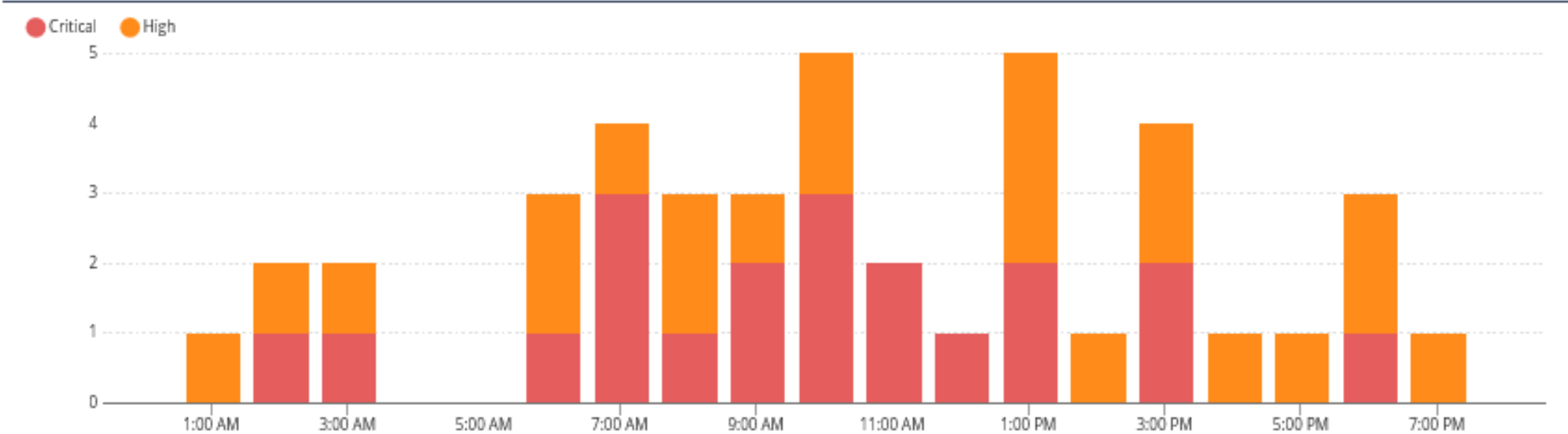


Top Destinations



Overview

Protections By Severity Timeline

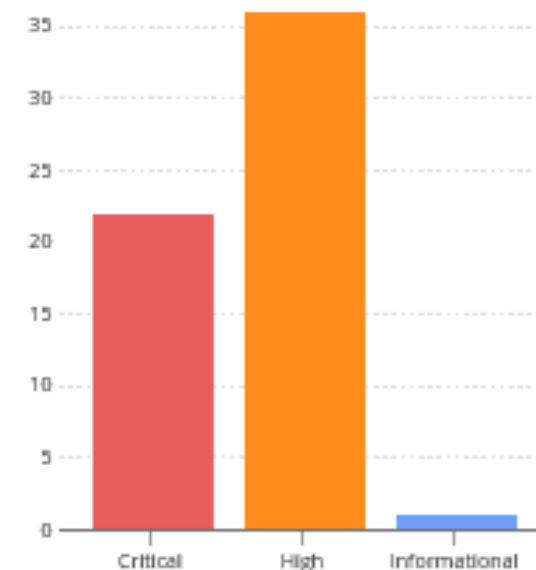


Intrusion Prevention System

Top Attacks

Logs	Protection Name	Severity	Action	Origin
20	ZMap Security Scanner over HTTP	High	Prevent	3 Origins
11	NoneCMS ThinkPHP Remote Code Execution (CVE-2018-20062)	Critical	Prevent	3 Origins
7	Zend Technologies Zend Framework Zend_XmlRpc Information Disclosure	High	Prevent	3 Origins
5	WordPress HTTP Brute Force Login Attempt	High	Prevent	2 Origins
4	Web Server Exposed Git Repository Information Disclosure	Critical	Prevent	2 Origins
4	Masscan Port Scanner	High	Prevent	3 Origins
2	Dasan GPON Router Authentication Bypass	Critical	Prevent	2 Origins
1	Apache Tomcat PUT Method Arbitrary File Upload Remote Code Execution (CVE-2017-12615)	Critical	Prevent	1 Origin
1	PHP Web Shell Generic Backdoor	Critical	Prevent	1 Origin
1	Draytek Vigor Command Injection (CVE-2020-8515)	Critical	Prevent	1 Origin
1	MVPower DVR Remote Code Execution	Critical	Prevent	1 Origin
1	Apache Struts2 Content-Type Remote Code Execution	Critical	Prevent	1 Origin

Attacks by Severity



Intrusion Prevention System

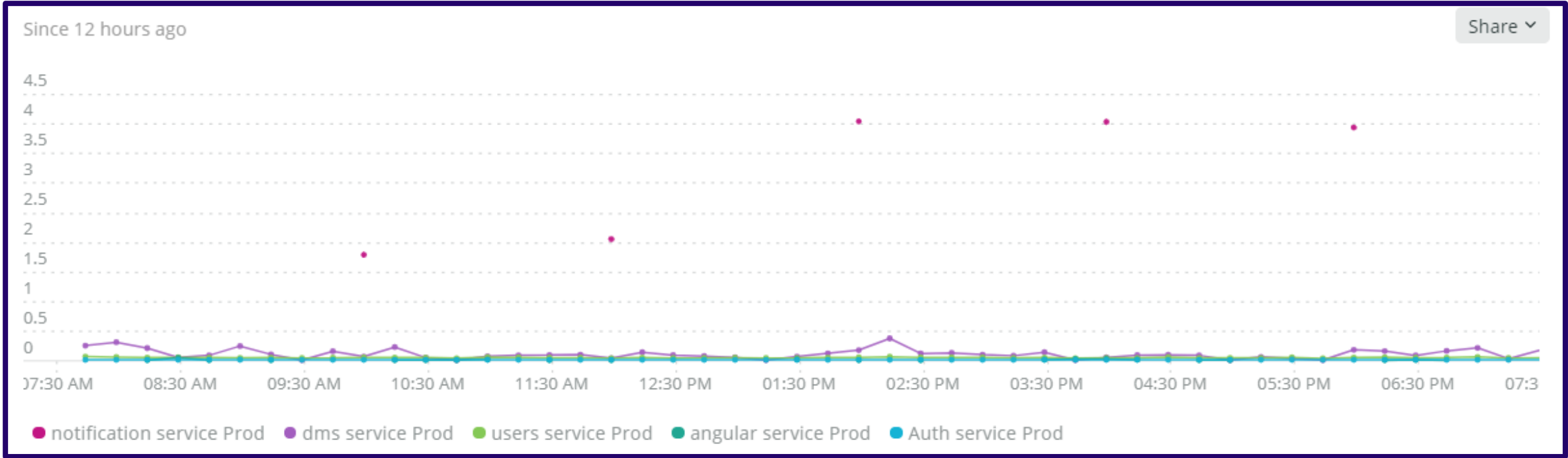
Top Origins And Top Protections

Origin	Protection	Severity	Action	Logs
CPAutoSG-- i-081b5b8723bedb12e-- ap-south-1	ZMap Security Scanner over HTTP	High	Prevent	9
	NoneCMS ThinkPHP Remote Code Execution (CVE-2018-20062)	Critical	Prevent	5
	WordPress HTTP Brute Force Login Attempt	High	Prevent	4
	Zend Technologies Zend Framework Zend_XmlRpc Information Disclosure	High	Prevent	4
	Apache Tomcat PUT Method Arbitrary File Upload Remote Code Execution (CVE-2017-12615)	Critical	Prevent	1
	Total: 9 Protections	Critical	1 Action	27
CPAutoSG-- i-059356f476614a81f-- ap-south-1	ZMap Security Scanner over HTTP	High	Prevent	10
	NoneCMS ThinkPHP Remote Code Execution (CVE-2018-20062)	Critical	Prevent	5
	Web Server Exposed Git Repository Information Disclosure	Critical	Prevent	3
	Masscan Port Scanner	High	Prevent	2
	Zend Technologies Zend Framework Zend_XmlRpc Information Disclosure	High	Prevent	2
	Total: 7 Protections	Critical	1 Action	24
CP-VPNGW	Web Server Exposed Git Repository Information Disclosure	Critical	Prevent	1
	PHP Web Shell Generic Backdoor	Critical	Prevent	1
	Masscan Port Scanner	High	Prevent	1
	Zend Technologies Zend Framework Zend_XmlRpc Information Disclosure	High	Prevent	1
	Dasan GPON Router Authentication Bypass	Critical	Prevent	1
	Total: 7 Protections	Critical	1 Action	7
Total: 3 Origins	12 Protections	Critical	1 Action	58

New Relic APM Report @ABC Corporation

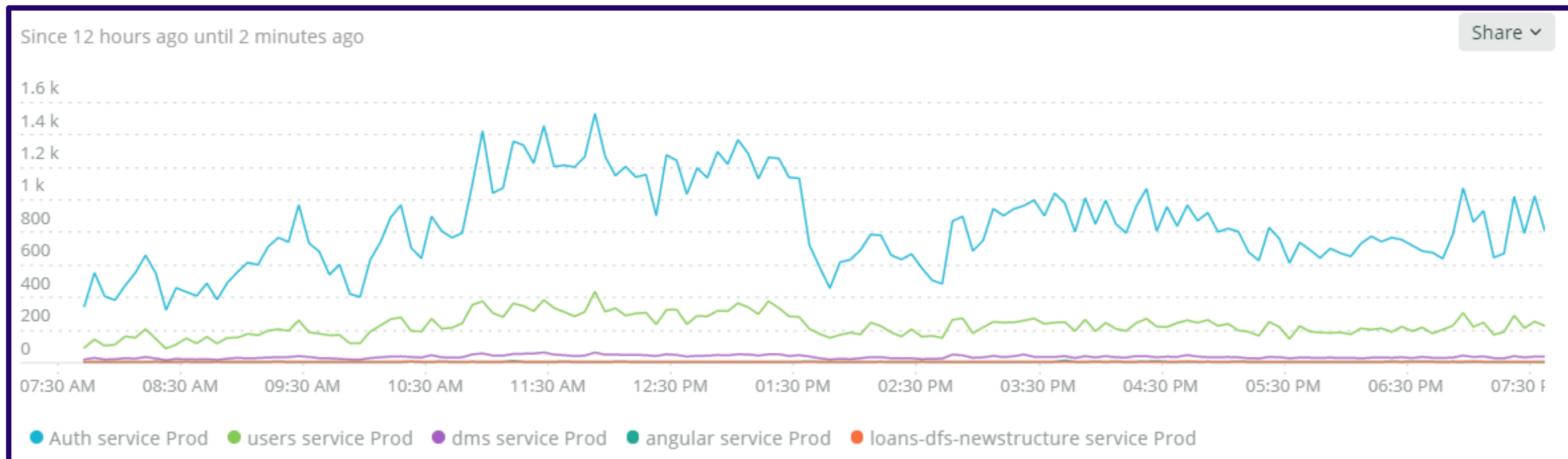


Top 5 application services response time



notification service Prod had highest response rate.

Top 5 application services throughput



Auth service Prod had highest throughput rate

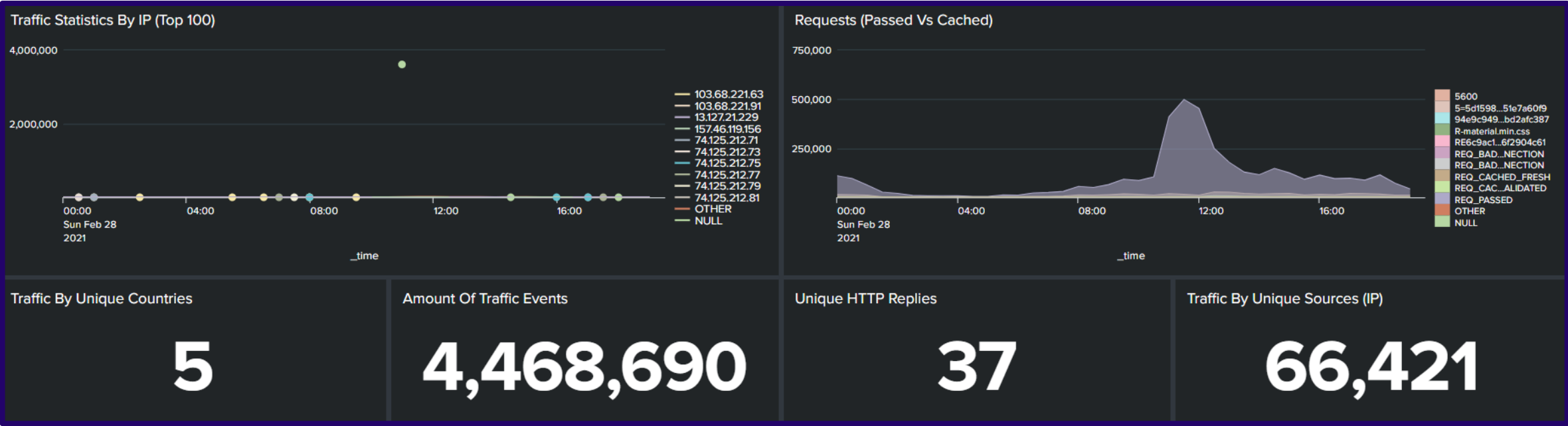
Imperva Report @ABC Corporation



Incapsula Main View Attack Logs

Number Of Attacking Countries	Number Of Attacks	Number Of Attack Types	Number Of Attackers
12	415	9	33

Attack Types	Count	Percentage
IncapRules(Anti Scrapper Policy)	304	68.315%
IncapRules(Clients with more than 2 UA)	51	11.461%
Bot Access Control	40	8.989%
Illegal Resource Access	32	7.191%
IncapRules(Blocking Attacks)	10	2.247%
IncapRules(Block Anonymous Proxy and TOR)	3	0.674%
IncapRules(Blocking Web Attacks)	3	0.674%
No:csf4d:csfref:rec:ver:j82b81306e79d3Browser:cs6Lab:request=dll.banutm_source=AExternalId=52851jld9bdc8c385522e4a42cd214641a4d1itude:cs8=77.5855&cai\=206796_78049&px\=1:pt=63760 src=157.45.218.65	1	0.225%
SIEMintegration	1	0.225%



AV Security Report @ AWS & CW Office



Virus Scan

Report Summary

Date – 28th February 2021
Group Name: All Groups
Endpoint Name: All
User Name: All
Records Found: 01

Row Labels	Count of Source
Ransomware	1
Grand Total	1

Device Control

Report Summary

Date – 28th February 2021
Group Name: All Groups
Endpoint Name: All
User Name: All
Records Found: 00

Report Summary

Date: 28th February 2021

Group Name: All Groups

Endpoint Name: All

User Name: All

Records Found: 00

IDS / IPS – Port Scanning

Report Summary

Date: 28th February 2021

Group Name: All Groups

Endpoint Name: All

User Name: All

Records Found: 00 (All Events are blocked)

Report Summary

Date: 28th February 2021

Group Name: All Groups

Endpoint Name: All

User Name: All

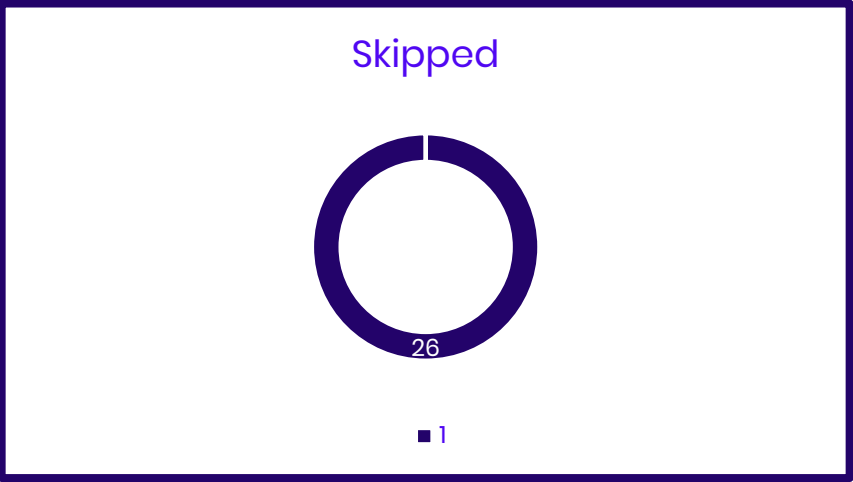
Records Found: 13

Date & Time	Category	Message
28 Feb 2021 (20:42:01)	Information	Infopercept logged in from 192.168.1.215.
28 Feb 2021 (13:00:43)	Information	Scheduled Virus Scan notification sent for group 'QA_Team_New'.
28 Feb 2021 (13:00:41)	Information	Scheduled Virus Scan notification sent for group 'Reseach_youtube_allow'.
28 Feb 2021 (13:00:41)	Information	Scheduled Virus Scan notification sent for group 'Research_Analyst_Team_Youtube_allow'.
28 Feb 2021 (13:00:41)	Information	Scheduled Virus Scan notification sent for group 'IT_Team_Youtube_allow'.
28 Feb 2021 (13:00:41)	Information	Scheduled Virus Scan notification sent for group 'RnD_Team_New'.
28 Feb 2021 (13:00:40)	Information	Scheduled Virus Scan notification sent for group 'Research_Team_New'.
28 Feb 2021 (13:00:40)	Information	Scheduled Virus Scan notification sent for group 'HR_Team_New'.
28 Feb 2021 (13:00:39)	Information	Scheduled Virus Scan notification sent for group 'Administration_Team_New'.
28 Feb 2021 (13:00:39)	Information	Scheduled Virus Scan notification sent for group 'IT_Team_New'.
28 Feb 2021 (13:00:21)	Information	Scheduled Virus Scan notification sent for group 'Default_New'.
28 Feb 2021 (08:00:04)	Information	License information has been updated.
28 Feb 2021 (05:27:50)	Information	Infopercept logged in from 192.168.1.215.

Report Summary

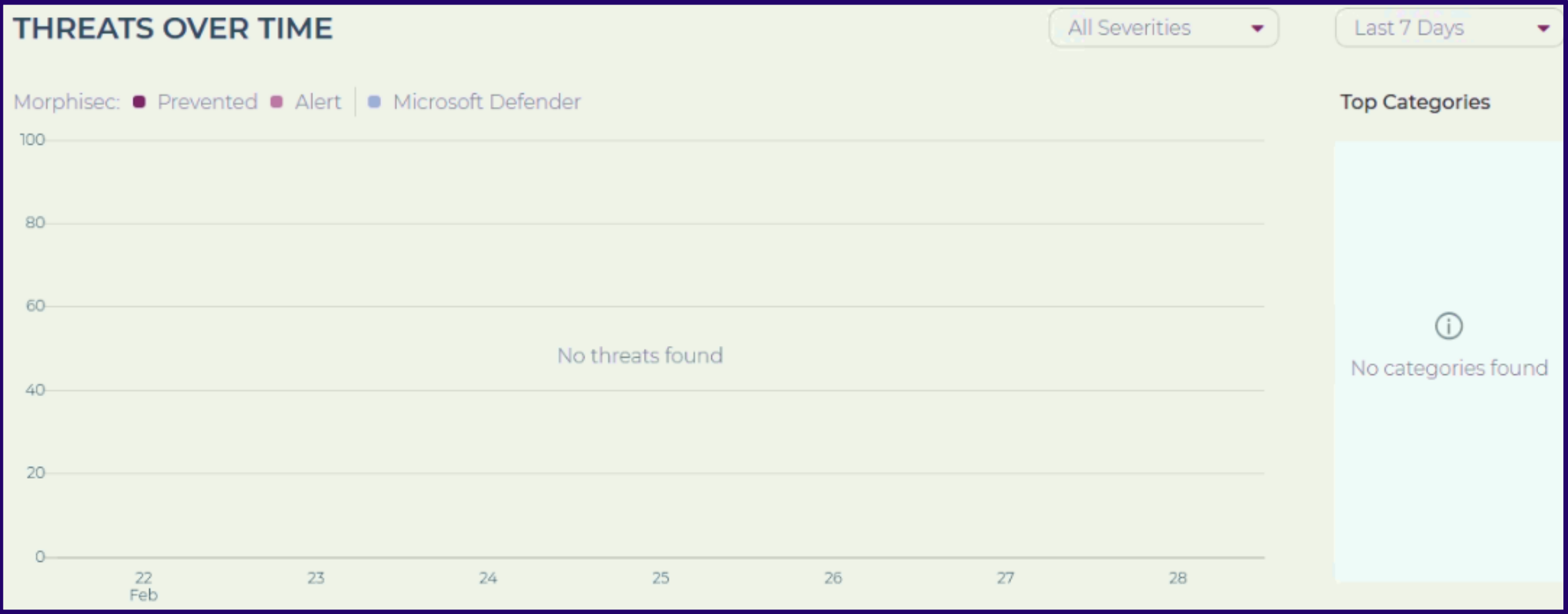
Date: 28th February 2021
Group Name: All Groups
Endpoint Name: All
User Name: All
Records Found: 26

Row Labels	Count of Source
Skipped	26
Slack	26
Grand Total	26



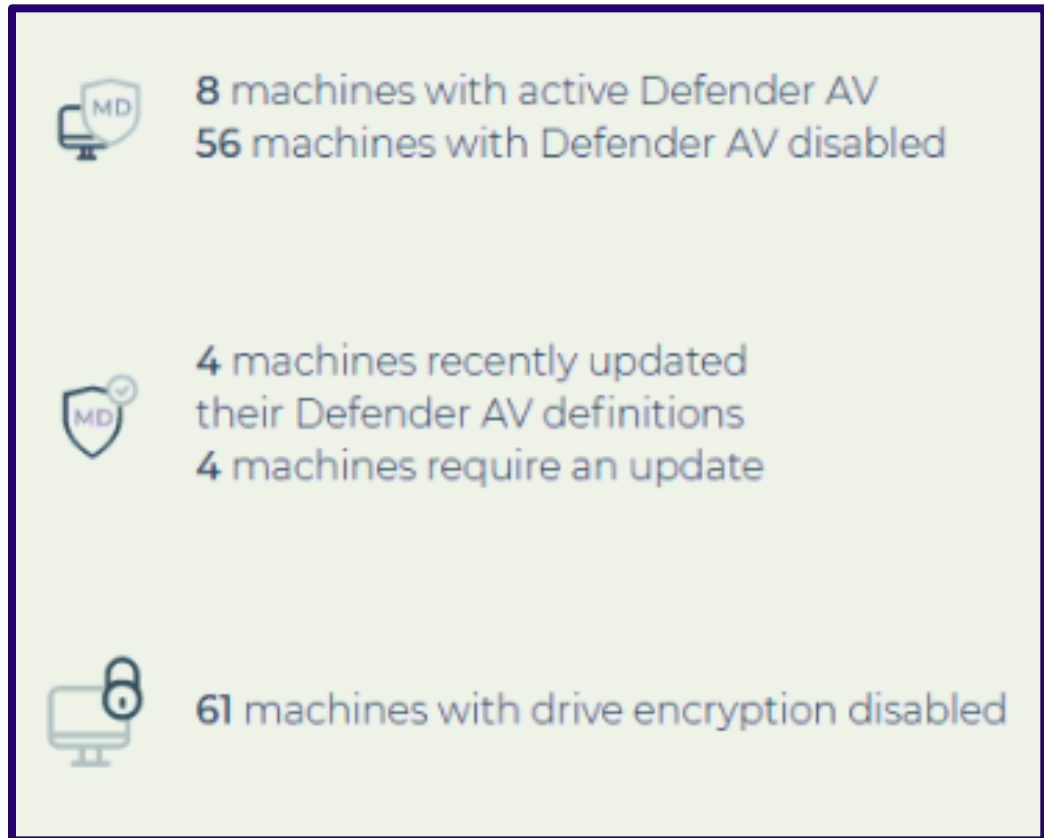
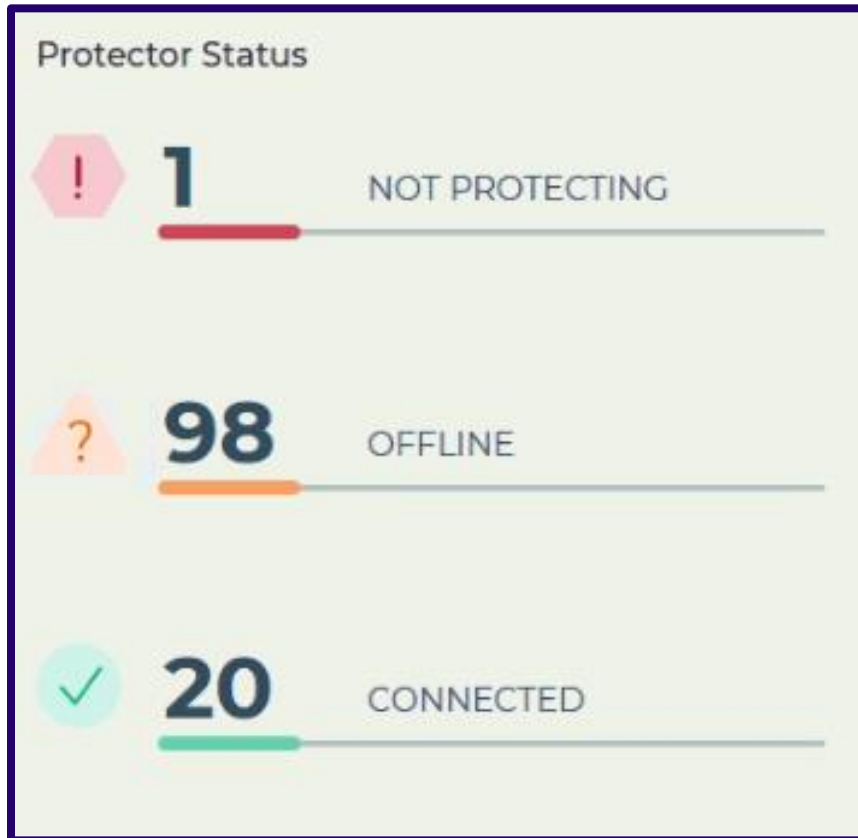
Row Labels	Count of Source
Skipped	26
Grand Total	26

THREATS OVER TIME

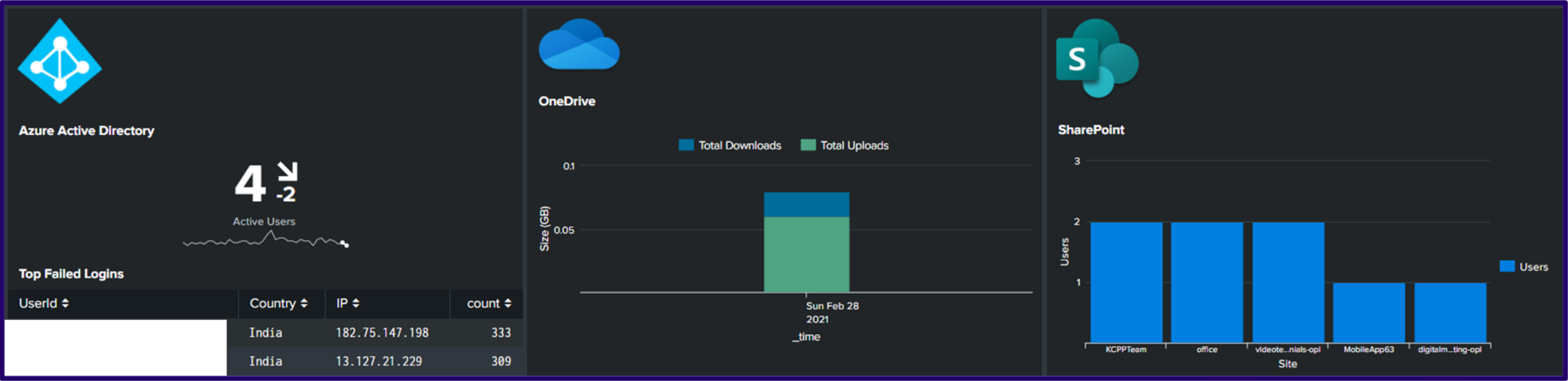


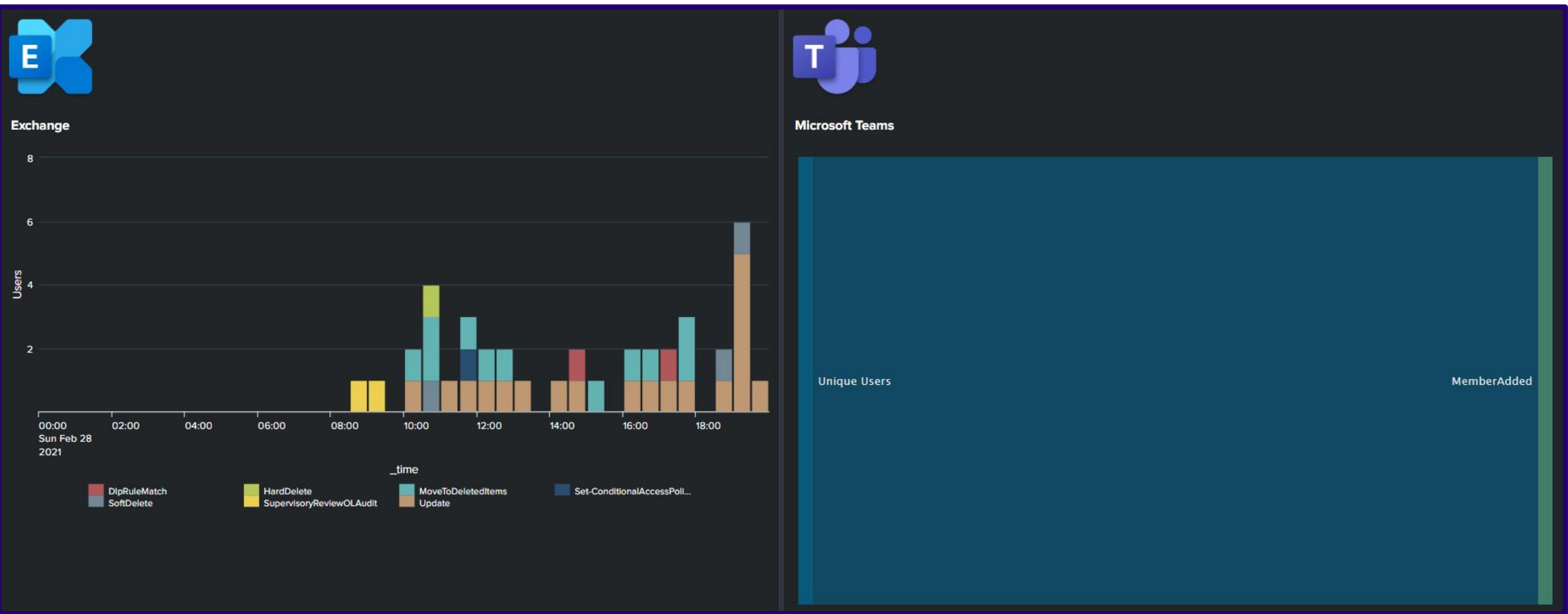
Auth service Prod had highest throughput rate

PROTECTOR STATUS

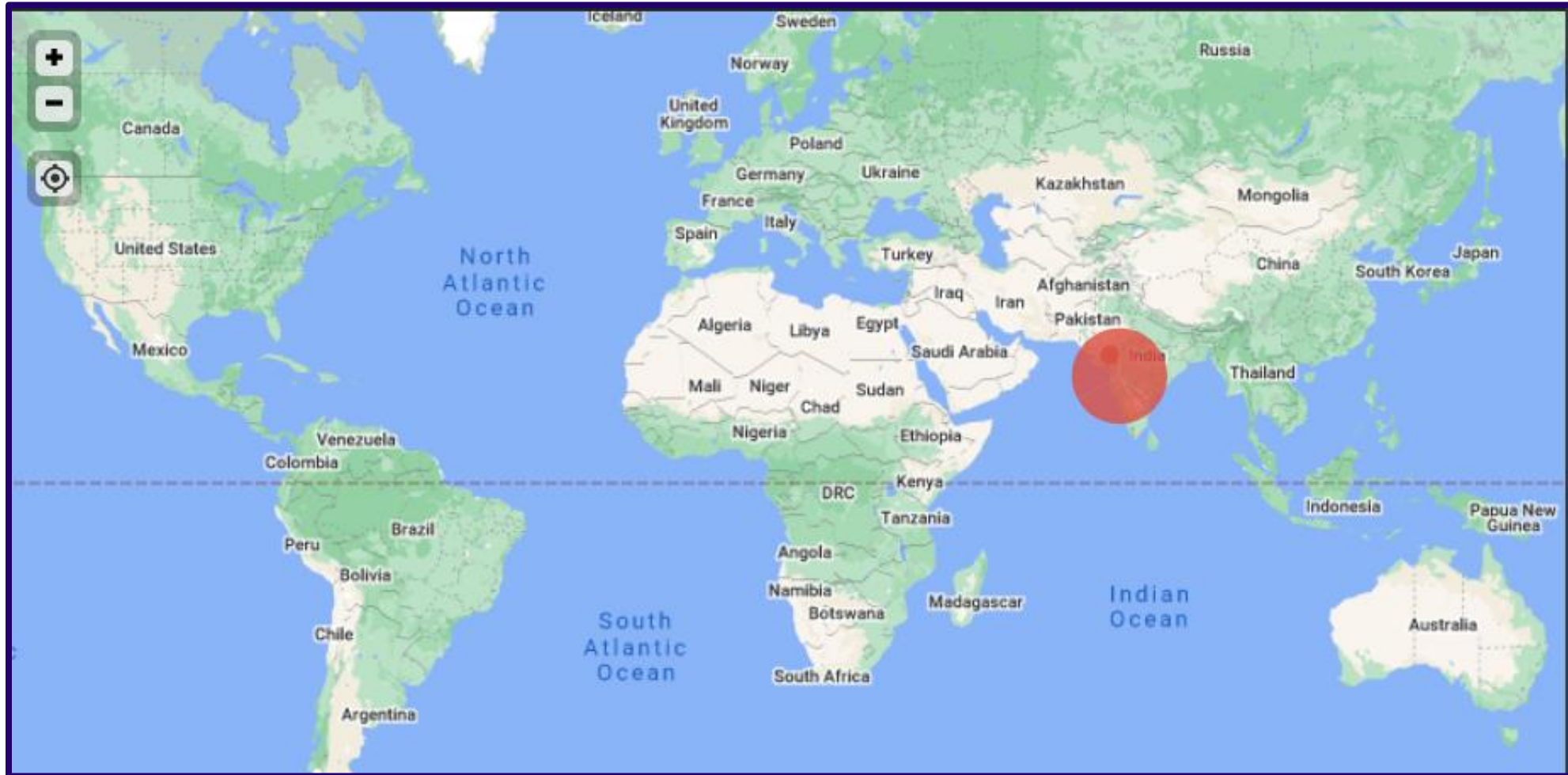




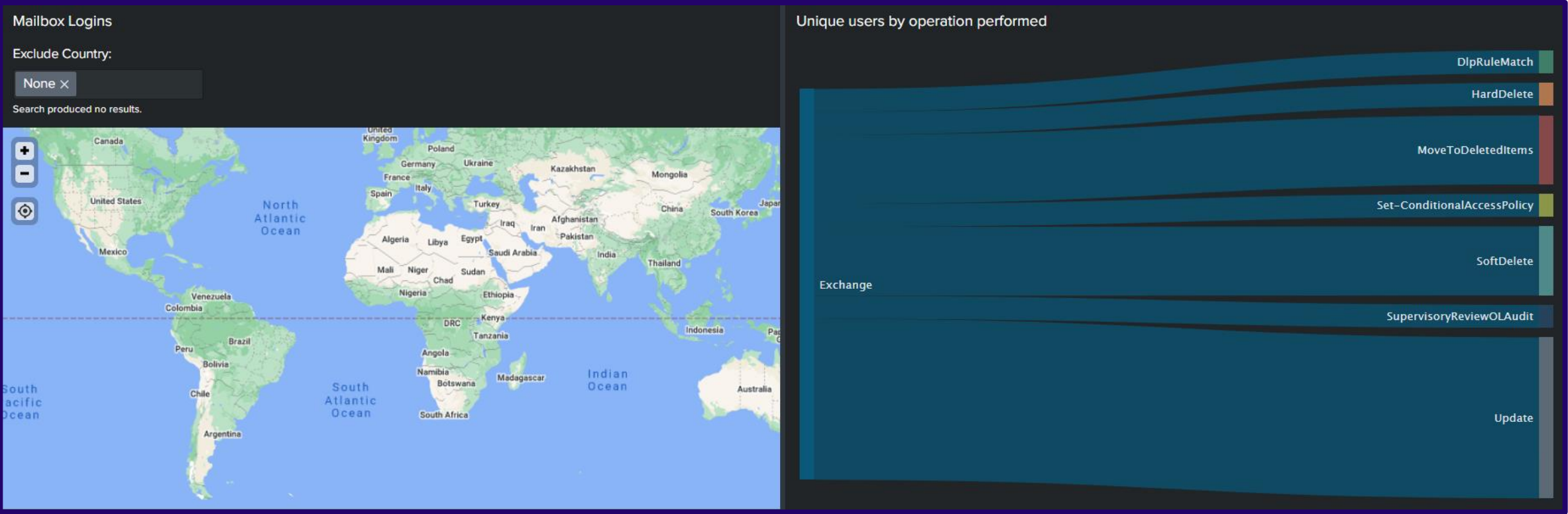




Office 365 Azure AD Login Activity



Azure AD Failed Login Attempts				
User ↕	LogonError ↕	Client IP ↕	Country ↕	count ↕
2d19b417-ce18-402c-ac0a-27b908797ce7	InvalidUserNameOrPassword	13.127.21.229	India	231
387dd2a9-f12a-4cd9-b966-76cc17c73f6e	UserStrongAuthClientAuthNRequiredInterrupt	182.75.147.198	India	4
501bce39-7124-4f35-b1a6-1f4ec4120e19	UserStrongAuthClientAuthNRequired	182.75.147.198	India	46
71c01291-7c2d-458d-9b1f-51d0c0d48747	InvalidPasswordExpiredPassword	14.99.96.186	India	18
d328e27f-f6db-45c3-a677-7dd7927139e7	InvalidUserNameOrPassword	182.75.147.198	India	333
d328e27f-f6db-45c3-a677-7dd7927139e7	InvalidUserNameOrPassword	203.88.128.170	India	4
e0a1f450-532e-4fcc-b426-34d81bac6614	InvalidPasswordExpiredPassword	13.127.21.229	India	309



Above Dashboard gives brief of the Operations performed by End Users in Exchange today

Failed logins because of MFA errors

Failed logins because of MFA errors			
User ↕	ClientIP ↕	LogonError ↕	count ↕
		UserStrongAuthClientAuthNRequired	46
		UserStrongAuthClientAuthNRequiredInterrupt	4


Password Resets






Note: No password resets recorded today.

Failed login attempts from multiple IP-Addresses		
User ↕	UniqueIP ↕	SourceIP ↕
<div></div>	2	182.75.147.198
		203.88.128.170

Device Status

Intune enrolled devices

Device compliance status	
Status	Devices
Compliant	57
In grace period	0
Not evaluated	36
Not compliant	8 
Total	101

Intune enrolled devices	
LAST UPDATED 2/27/2021, 8:29:21 PM	
Platform	Devices
Windows	 82
Android	 18
iOS/iPadOS	 2
macOS	 0
Windows Mobile	 0
Total	102

Tenant Status / Resource alerts


Tenant status


Account status
Active


Service health
Healthy


Connector status
Healthy

Resource alerts

 **Device compliance**
8 devices not in compliance

 **Device configuration**
2 devices have profile errors


 **Device enrollment**
5 devices have enrollment failures




 **Client apps**
1 installation failure

Top Applications		View by: Sessions	
Application Name	Percentage of Applications		
Service ALL Port for R&D	43.63%		
General HTTPS	22.72%		
General DNS	15.86%		
General HTTP	7.63%		
Service Tivo TCP Data	3.27%		
General UDP	1.46%		
Service Suresh	1.00%		
Service SMB	0.92%		
Service RPC Services	0.69%		
General NETBIOS	0.43%		


Top Users		View by: Sessions	
User Name	Percentage of Users		
UNKNOWN	99.46%		
amitp	0.14%		
divyesh	0.12%		
SmitM	0.10%		
socteam	0.09%		
helpdesk	0.06%		
SOCTEAM2	0.02%		
aneri	0.01%		
SOCTEAM	0.01%		
ITHelpdesk	0.00%		








Top Virus

View by: Sessions 

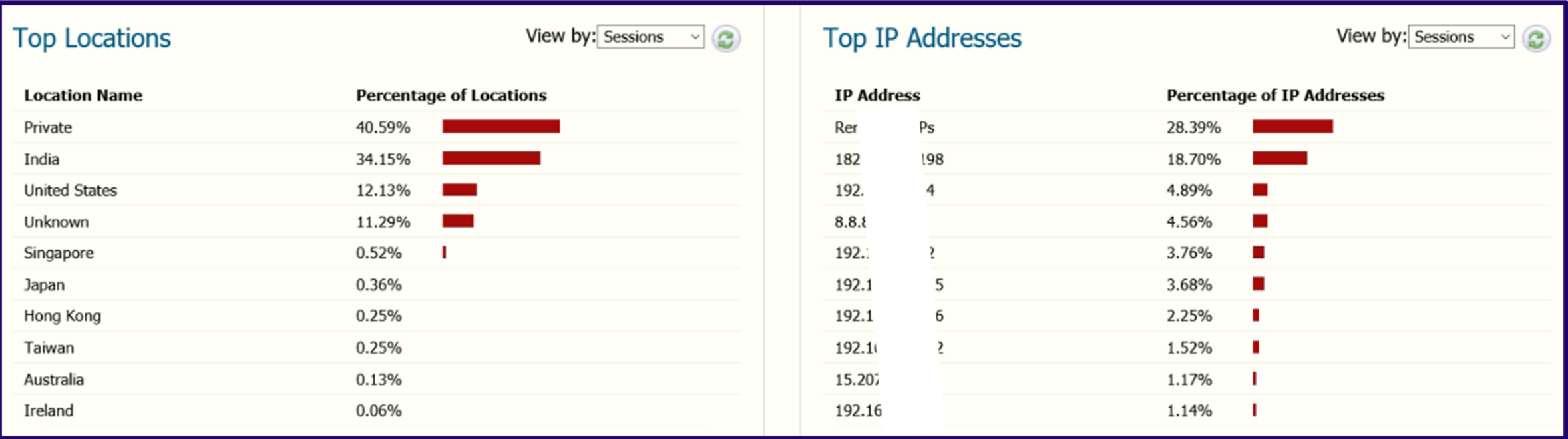
Virus Name	Percentage of Virus
Nanspy.AE (Trojan)	40.00% 
ARMADILLO packed executable_2 file (...)	40.00% 
UPX_Packed_Executable_0 (Trojan)	20.00% 

Top Intrusions

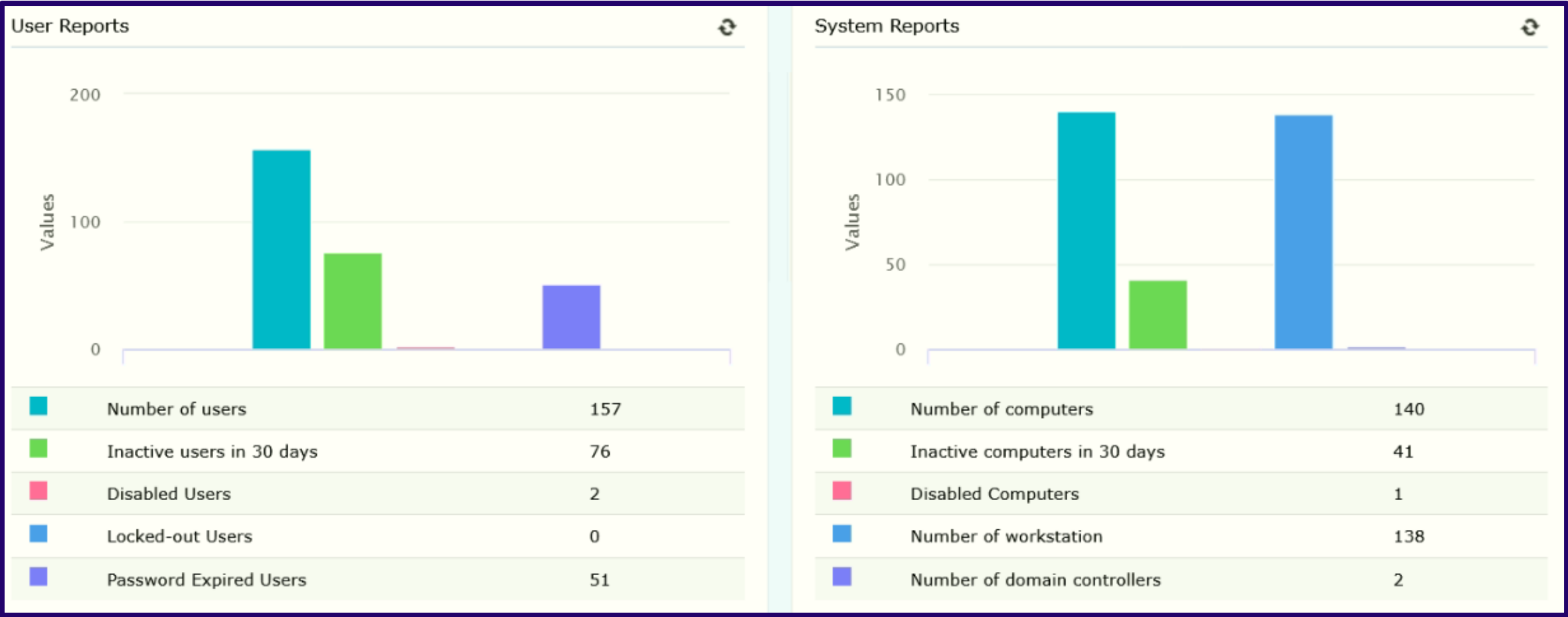
View by: Sessions 

Intrusion Name	Percentage of Intrusions
Time-To-Live Exceeded in Transit	44.80% 
Echo Reply	25.56% 
PING	20.28% 
NetBIOS Name Request Probe	4.41% 
Suspicious Executable File Download 10	0.78% 
PING with Null Payload	0.77% 
Web Application Directory Traversal ...	0.62% 
/etc/passwd Access 2	0.40%
SSLv2.0 Client Hello 2	0.36%
Web Application Directory Traversal ...	0.24%

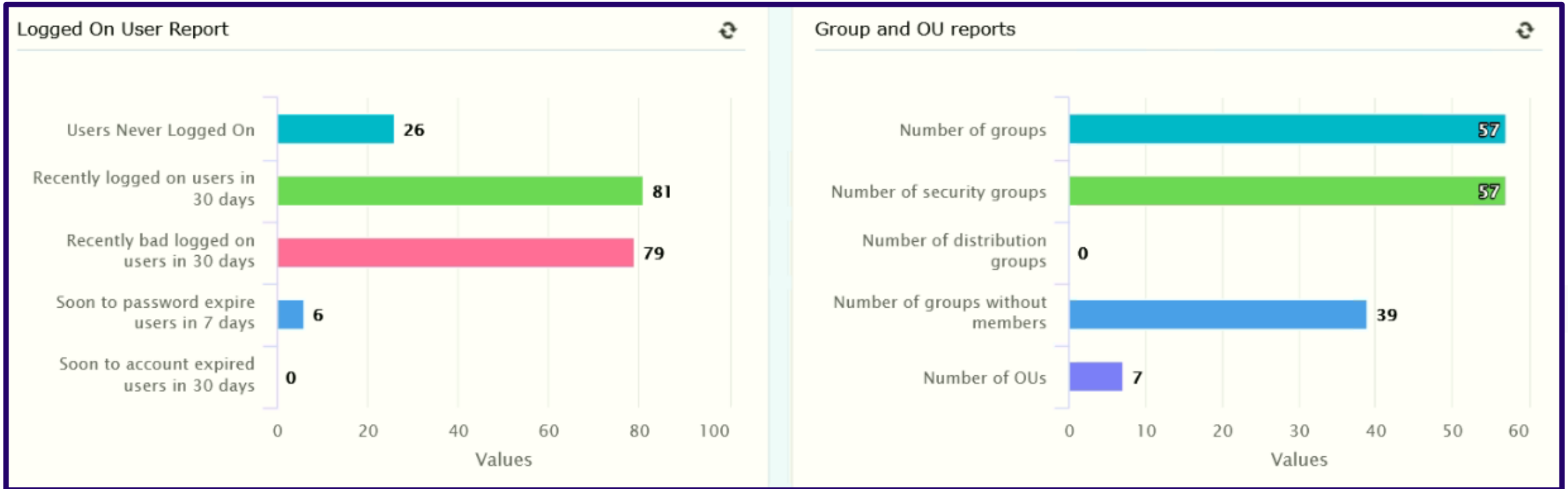




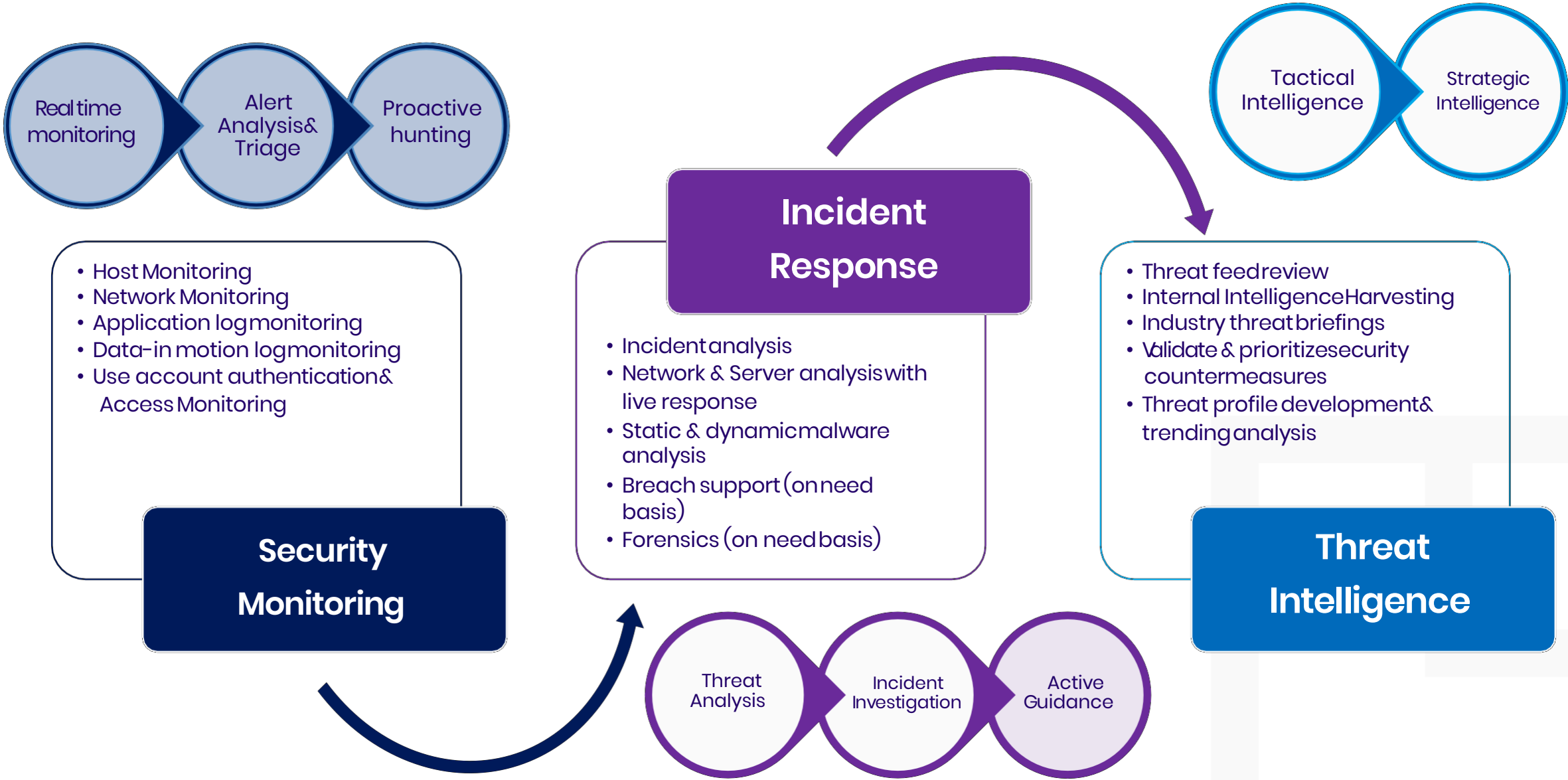
User And System Reports:



Logged On User And Group and OU Reports:



ABC Corporation Security Operations Center Process



Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Our specialized core team comprises of experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, are abreast of the latest trends and security innovations; ensuring that you always get the best security approach & solutions for your specific business needs, exactly the way you want it to be.

Imprint

© Infopercept Consulting Pvt. Ltd. 2021

Publisher

H-1209, Titanium City Center,
Satellite Road,
Ahmedabad – 380 015,
Gujarat, India.

Contact Info

M: +91 9898857117

W: www.infopercept.com

E: sos@infopercept.com

By accessing/ proceeding further with usage of this platform / tool / site /application, you agree with the Infopercept Consulting Pvt. Ltd.'s (ICPL) privacy policy and standard terms and conditions along with providing your consent to/for the same. For detailed understanding and review of privacy policy and standard terms and conditions. kindly visit www.infopercept.com or refer our privacy policy and standard terms and conditions.

Global Offices

United State of America

+1 516 713 5040

United Kingdom

+44 2035002056

Sri Lanka

+94 702 958 909

Kuwait

+965 6099 1177

India

+91 9898857117

