

# ABC Corporation Daily SOC Report

---

INFOPERCEPT  
Sample Report 2021

YOUR DATE HERE

---

COMPANY NAME  
Authored by: Your Name



 **Infopercept**  
Your Ally in Digital Warfare

# AWS Security Report@ABC Corporation



# AWS Overview : Apps Servers

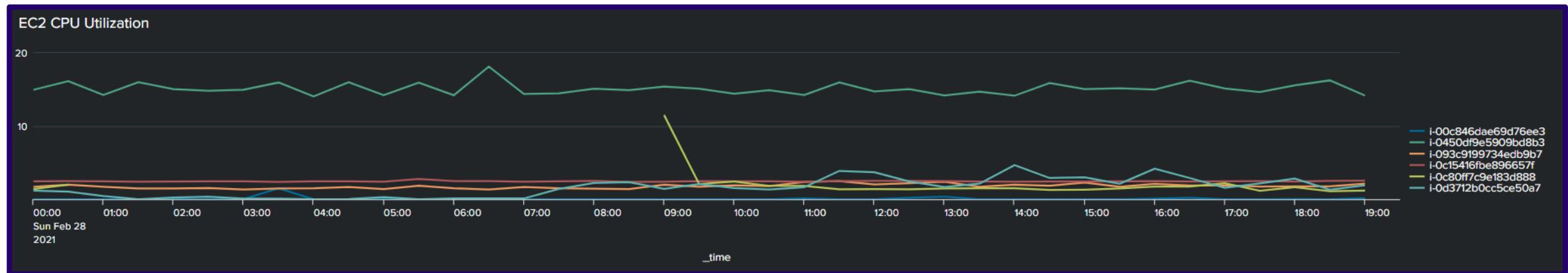
Running Instances	33 (9:00AM to 9:00PM)
Stopped Instances	33
Production Instances	21

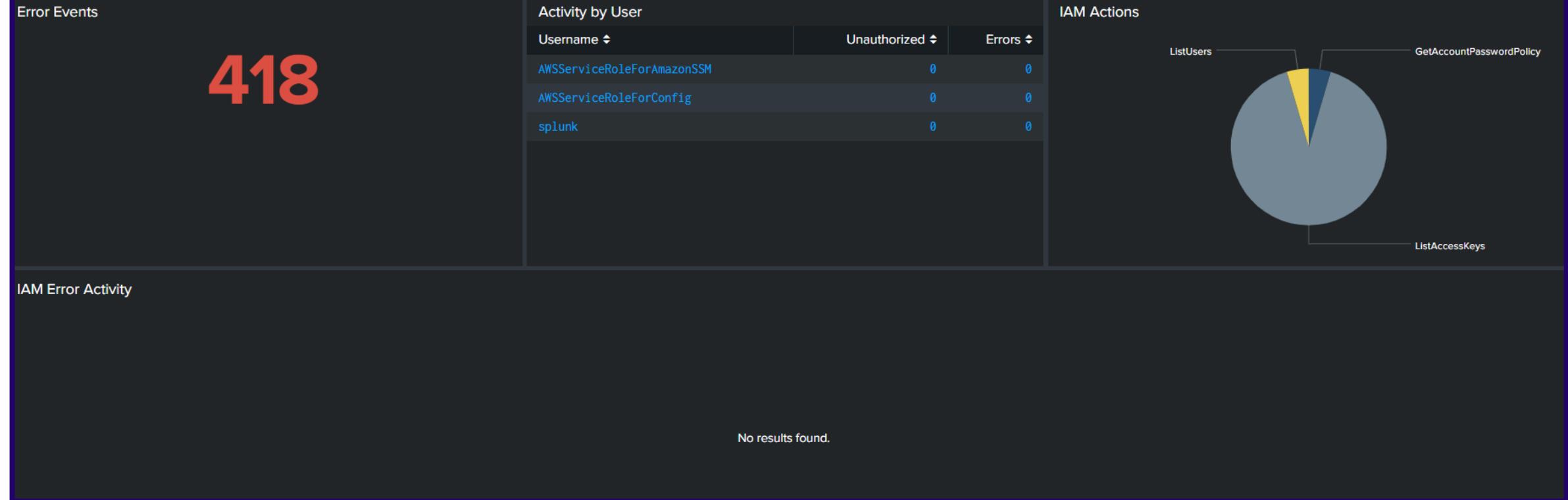
PRIVATE_IP_ADDRESS	KEY_NAME	ID	INSTANCE_TYPE
10.0.0.10	Adm	i-0450df9e5909bd8b3	r5a.2xlarge
10.0.0.10	Pro	i-07bc6d596daa7a14a	r5.8xlarge
10.0.0.10	Prc	i-093c9199734edb9b7	r5.8xlarge
13.233	Lin	i-0c15416fbe896657f	t2.medium
13.1	Ta	i-0c80ff7c9e183d888	m5a.4xlarge
1	Linu	i-0d3712b0cc5ce50a7	c5a.2xlarge
10.0.0.10	L	i-0f6926fd1e5c1dc4c	c5a.2xlarge
1	s	i-00c846dae69d76ee3	c5.large
1	N	i-07ba56ebef8409f8f	c5.large
1	Red		
1	E		
1	N		
1	Red		
1	E		

# AWS Overview : CPU Utilization

Infopercept

splunk>enterprise





Total Requests

**7,672,788**

ELB Error Requests



Backend Error Requests

**15,995**

# ELB Instances - CP-External ALB

Backend Error Requests		
metric_name	metric_dimensions	count
HTTPCode_Target_4XX_Count	LoadBalancer=[app/CP-External-ALB-B7f02dd288a]	95.0
HTTPCode_Target_4XX_Count	LoadBalancer=[app/CP-External-ALB-Cea634d]	14.0
HTTPCode_Target_4XX_Count	LoadBalancer=[app/CP-External-ALB-P793ee24]	3661.0
HTTPCode_Target_4XX_Count	LoadBalancer=[app/CP-External-ALB-S811c9c]	550.0
HTTPCode_Target_4XX_Count	LoadBalancer=[app/CP-External-ALB-p6010839870]	1505.0
HTTPCode_Target_4XX_Count	LoadBalancer=[app/CP-internal-ALB-Bab0e8f]	1505.0
HTTPCode_Target_4XX_Count	LoadBalancer=[app/CP-internal-ALB-C90b105]	14.0
HTTPCode_Target_4XX_Count	LoadBalancer=[app/CP-internal-ALB-n4d2053a81703]	95.0
HTTPCode_Target_4XX_Count	LoadBalancer=[app/CP-internal-ALB-n674f02dd288a]	3549.0
HTTPCode_Target_4XX_Count	LoadBalancer=[app/CP-internal-ALB-n68ef9716c336]	541.0
HTTPCode_Target_5XX_Count	LoadBalancer=[app/CP-External-ALB-B793ee24]	37.0
HTTPCode_Target_5XX_Count	LoadBalancer=[app/CP-External-ALB-Cea634d]	9.0
HTTPCode_Target_5XX_Count	LoadBalancer=[app/CP-External-ALB-P793ee24]	1619.0
HTTPCode_Target_5XX_Count	LoadBalancer=[app/CP-External-ALB-S811c9c]	130.0
HTTPCode_Target_5XX_Count	LoadBalancer=[app/CP-External-ALB-p6010839870]	748.0
HTTPCode_Target_5XX_Count	LoadBalancer=[app/CP-internal-ALB-Bab0e8f]	185.0
HTTPCode_Target_5XX_Count	LoadBalancer=[app/CP-internal-ALB-C90b105]	9.0
HTTPCode_Target_5XX_Count	LoadBalancer=[app/CP-internal-ALB-n4d2053a81703]	37.0
HTTPCode_Target_5XX_Count	LoadBalancer=[app/CP-internal-ALB-n674f02dd288a]	1560.0
HTTPCode_Target_5XX_Count	LoadBalancer=[app/CP-internal-ALB-n68ef9716c336]	132.0

## ELB Instances – CP-External ALB

EC2 Instances

Region	ELB Name	Instance ID	Instance Name	Instance State
ap-south-1	CP-External-ALB-Prod	i-0e9d8d288cee3e4f7	Check-Point-AutoGW-Inst	healthy
ap-south-1	CP-External-ALB-Prod	i-0b6f103e19e81a443	Check-Point-AutoGW-Inst	healthy

Request Count Over Time

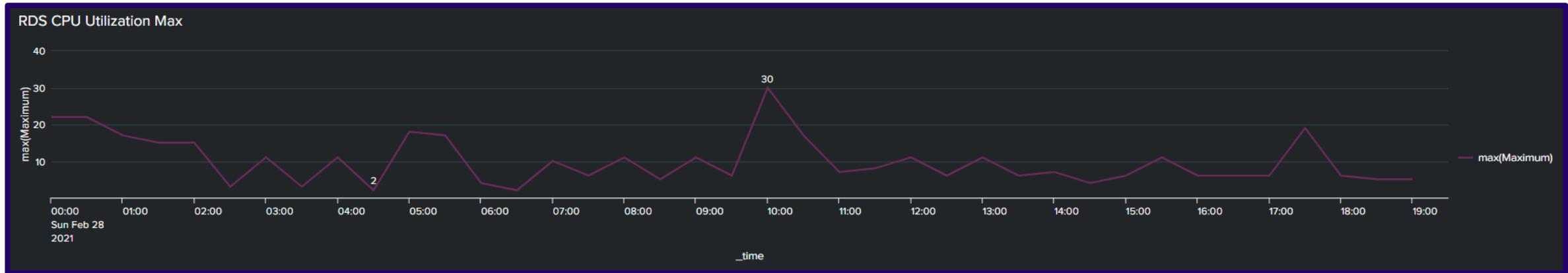
HTTP Backend Code Over Time

# RDS CPU & Memory Utilization: prod rds

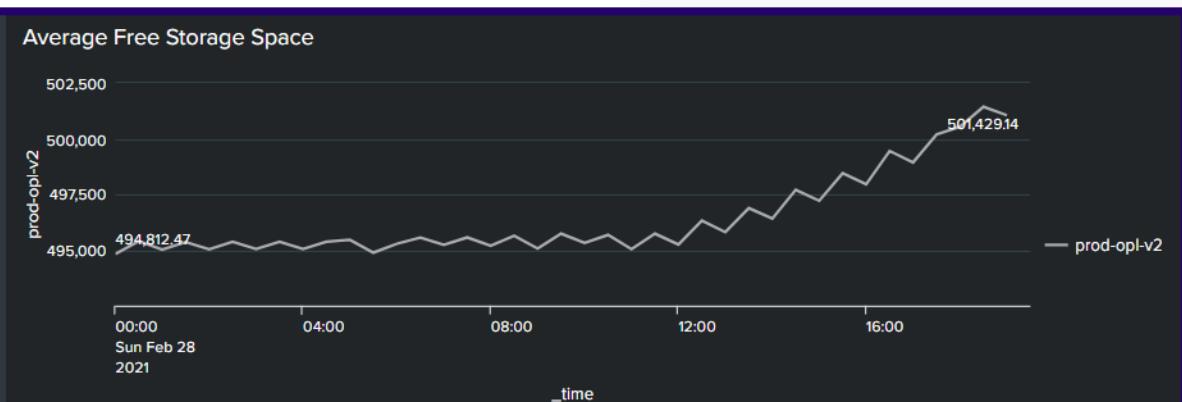
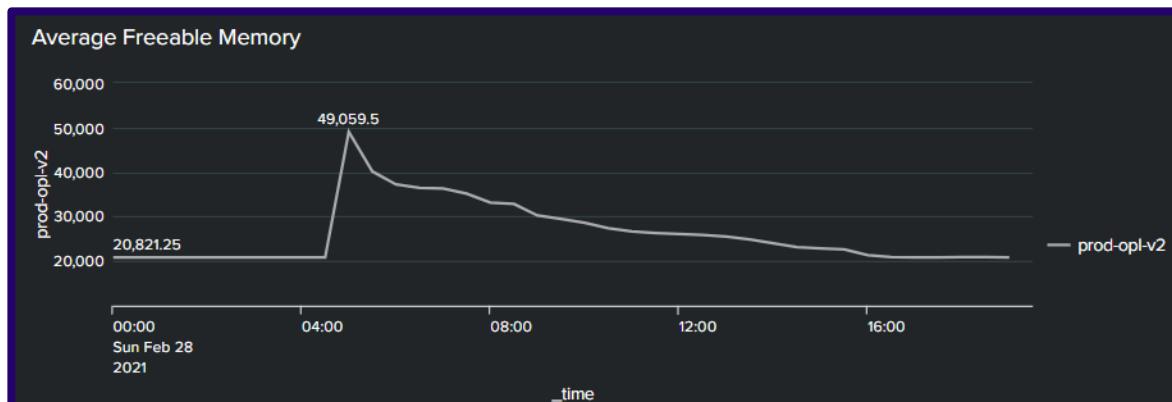
Infopercept

splunk>enterprise

We Observed Normal CPU Utilization of Prod-

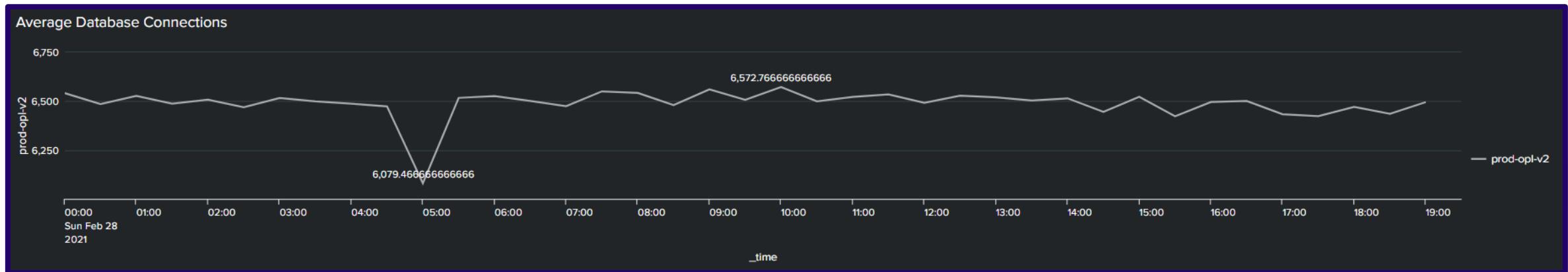


Average Freeable Memory of Prod is 20 GB and Storage 501 GB



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

Infopercept

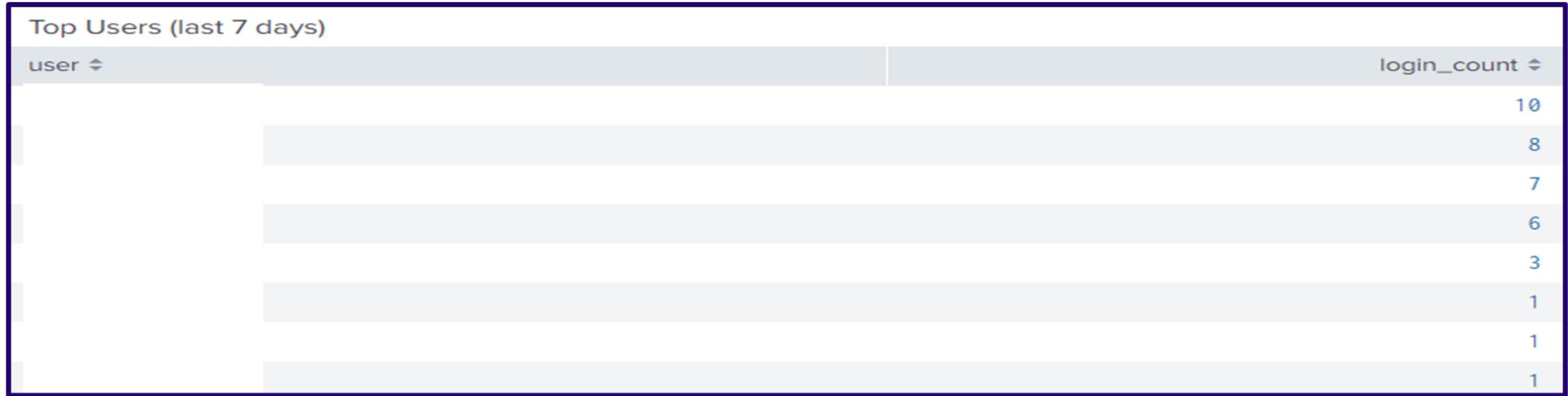
splunk>enterprise

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-tableauc2server-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

_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)	<b>10.0.4.252</b>	<b>107 day/s ago</b>

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



# RDS Backup and Restart Activity

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

# Admin-panel-Instance Backup

Snapshot: snap-0bf451e848a214ed4 (Admin-panel-Instance)		
Description	Permissions	Tags
Snapshot ID	snap-0bf451e848a214ed4	Progress 100%
Status	completed	Capacity 190 GiB
Volume	<a href="#">vol-0a227955afc2c55ed</a>	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
Snapshot ID	snap-0bdecd51edc9bc66e
Status	completed
Volume	<a href="#">vol-029e055fb963cb779</a>
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

Infopercept



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	-		

# Live-ITR-Gunicorn-scraping-server-01 Backup



Snapshot: snap-024ebb7471b5168ec (Live-ITR-Gunicorn-scraping-server-01-100GB)		
Description	Permissions	Tags
Snapshot ID	snap-024ebb7471b5168ec	Progress 100%
Status	completed	Capacity 100 GiB
Volume	<a href="#">vol-0e1afe3e49d12bcd4</a>	Encryption Encrypted
Started	February 28, 2021 at 12:10:46 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-04628df6e338466ea schedule: Schedule 1	Fast Snapshot Restore -
Outpost ARN	-	

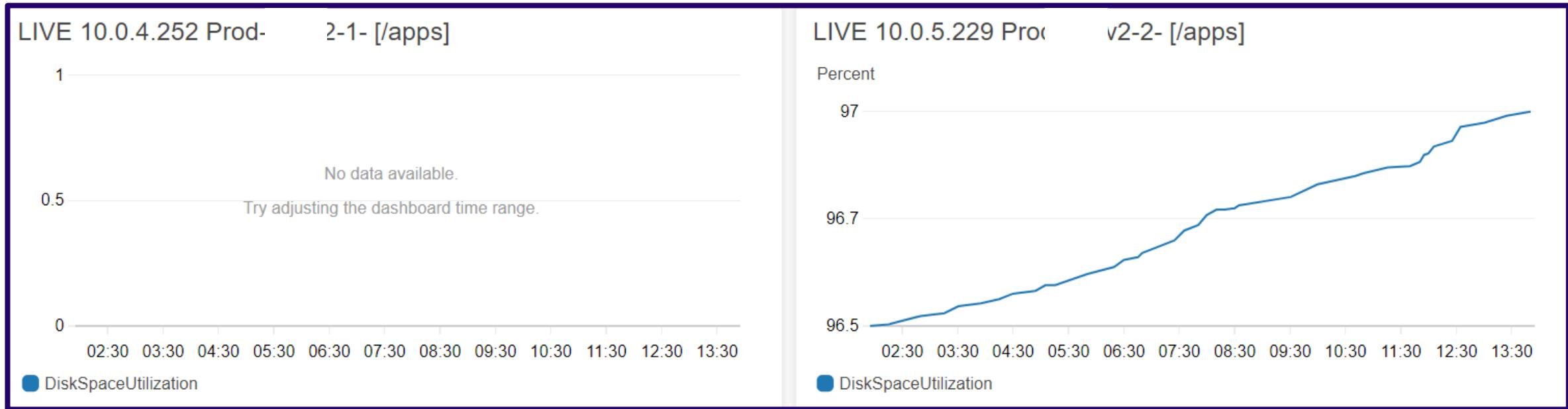
# Live-ITR-Gunicorn-scraping-server-02 Backup

Snapshot: snap-0fc9085ba3b58599f (Live-ITR-Gunicorn-scraping-server-02-100GB)			
Description	Permissions	Tags	
Snapshot ID	snap-0fc9085ba3b58599f	Progress	100%
Status	completed	Capacity	100 GiB
Volume	<a href="#">vol-0e623545a0c9afab5</a>	Encryption	Encrypted
Started	February 28, 2021 at 12:27:03 AM UTC+5:30	KMS Key ID	f07adcf6-b93c-4ab4-b69e-0f3ef74fef4b
Owner	652918353734	KMS Key Aliases	
Product codes	-	KMS Key ARN	<a href="#">arn:aws:kms:ap-south-1:652918353734:key/f07adcf6-b93c-4ab4-b69e-0f3ef74fef4b</a>
Description	Created for policy: policy-0d7dc7fbc33e92c41 schedule: Schedule 1	Fast Snapshot Restore	-
Outpost ARN	-		

# Pre-Production-29-07-2020 Backup

Snapshot: snap-0de0347ababbdcbbb (Pre-Production-29-07-2020)				
Description	Permissions	Tags		
Snapshot ID	snap-0de0347ababbdcbbb		Progress	100%
Status	completed		Capacity	250 GiB
Volume	<a href="#">vol-09fe8781ea9c3fb07</a>		Encryption	Encrypted
Started	February 28, 2021 at 12:12:46 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-0c772ae92c69a66d0 schedule: Schedule 1		Fast Snapshot Restore	-
Outpost ARN	-			

# Host Monitoring - /appspartition

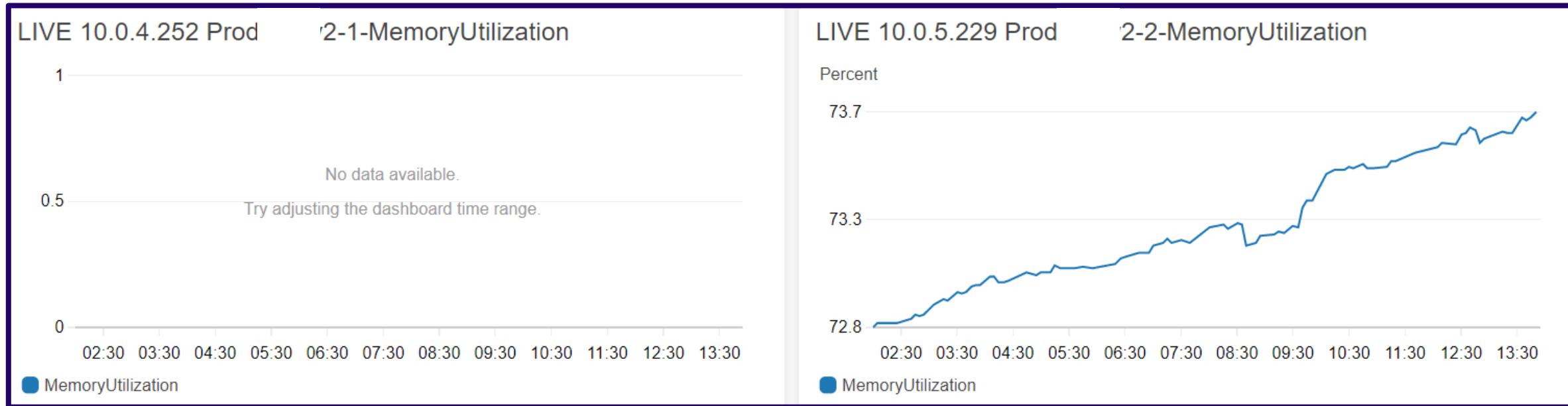


Prod-ABC-v2-1 -

**Server is not running**

Prod-ABC-v2-2 - **97.00%**

# Host Monitoring - /Memory Utilization

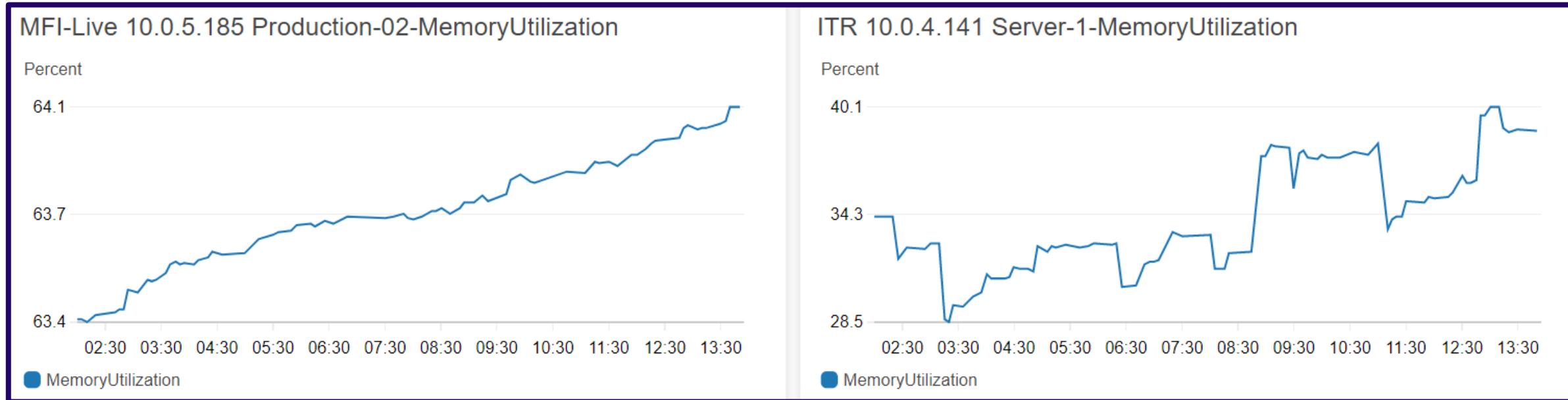


Prod-ABC-v2-1

**Server is not running**

Prod-ABC-v2-2 – **73.71%**

# Host Monitoring - /Memory Utilization

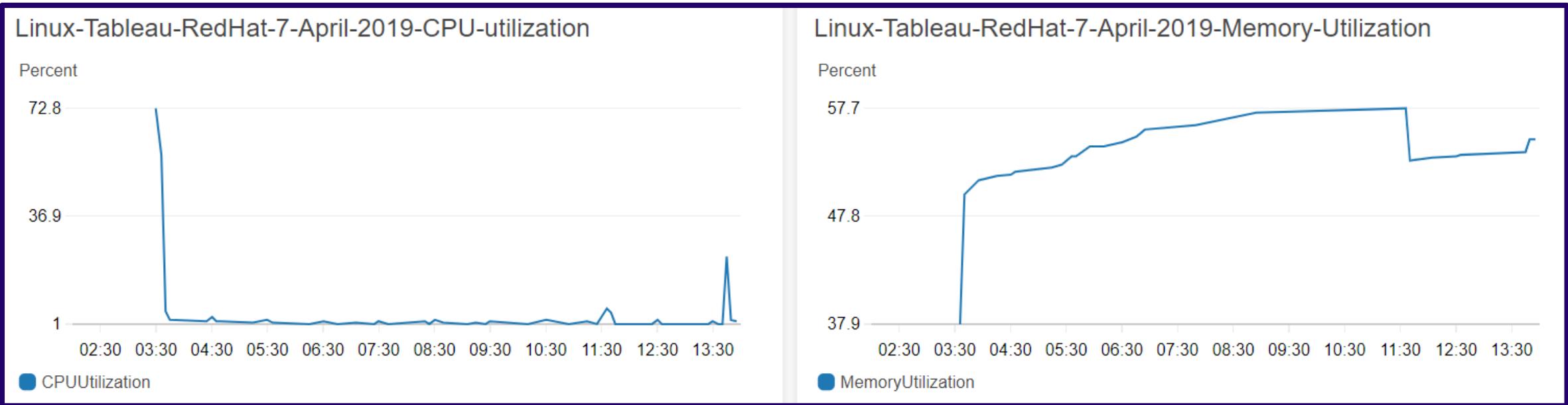


**MFI-Live 10.0.5.185 Production-02 – 64.05%**

**ITR 10.0.4.141 Server-1 – 38.81%**

# Host Monitoring - /CPU & Memory Utilization

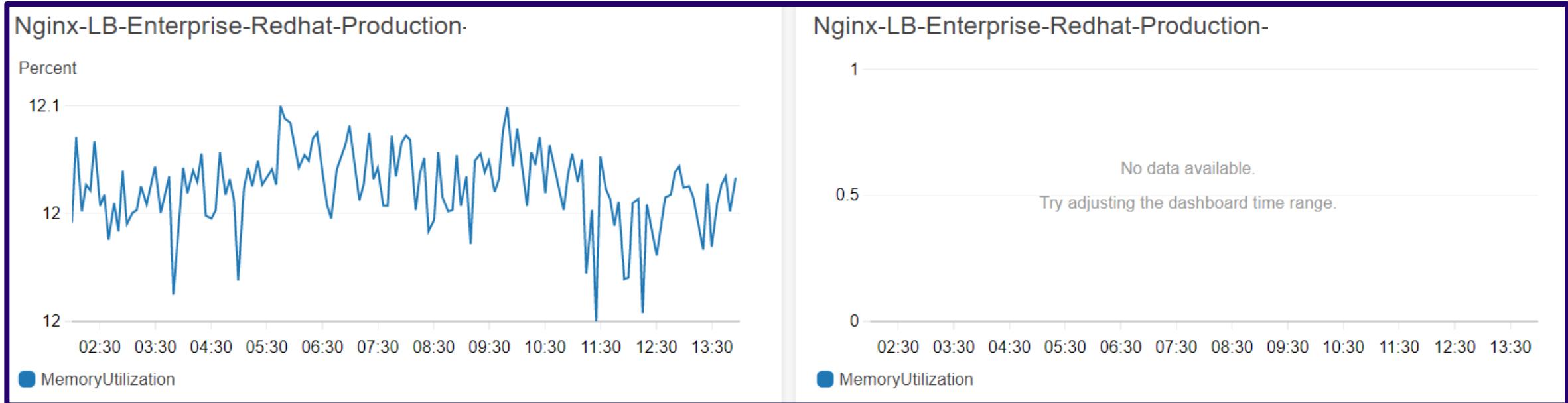
Infopercept



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

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

# Host Monitoring - /Memory Utilization



Nginx-LB-Enterprise-Redhat-Production-

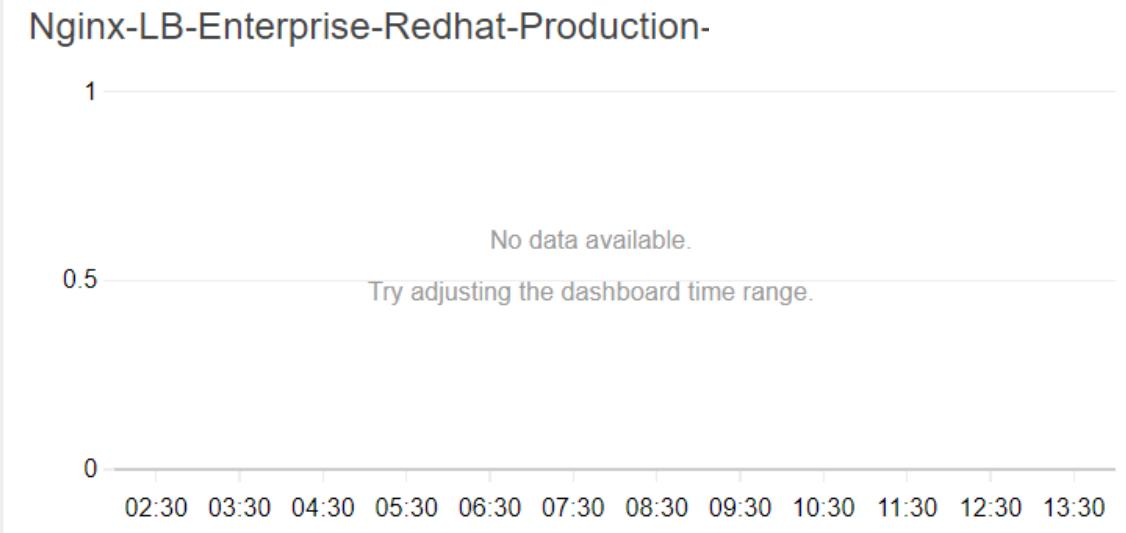
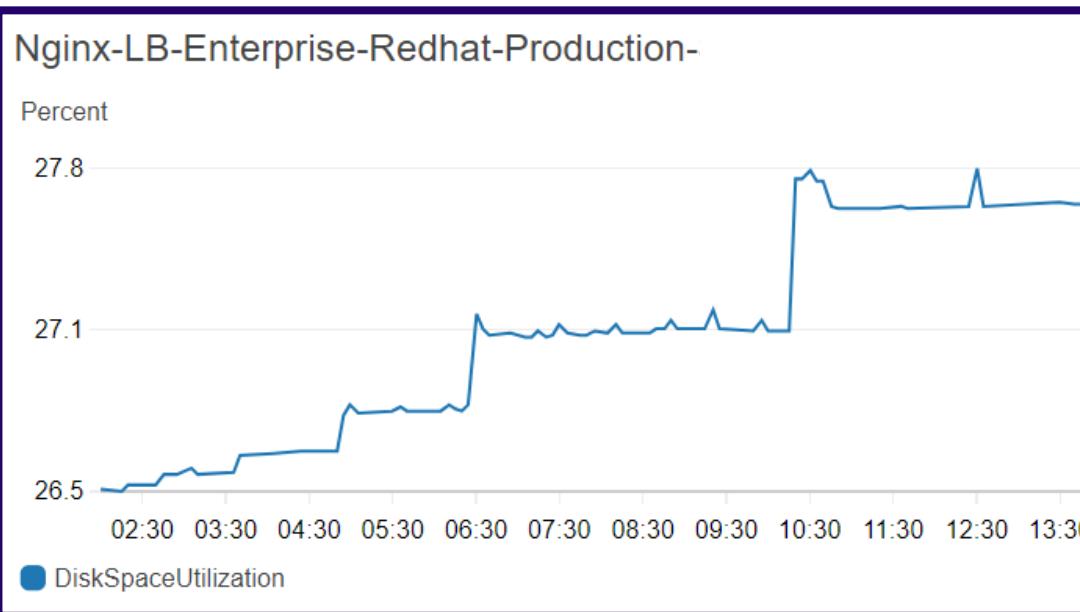
**MEMORY-Utilization – 12.04%**

Nginx-LB-Enterprise-Redhat-Production-  
-BackupServer

**MEMORY-Utilization –**

**Server is not running**

# Host Monitoring - /Disk Utilization



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

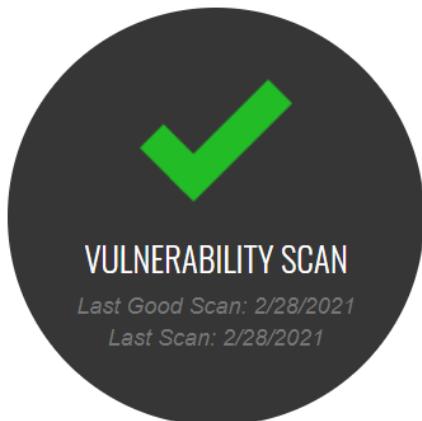
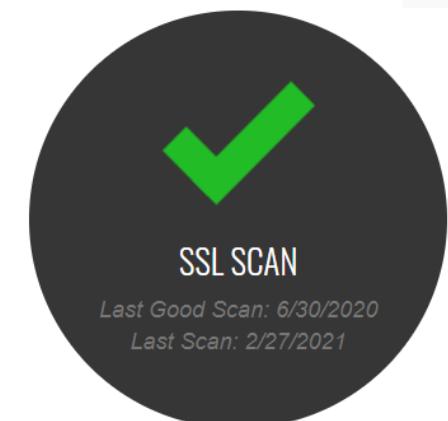
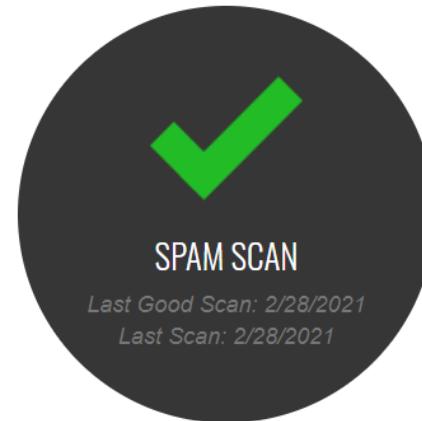


# Site Lock – Daily Scan Reports

Infocept

 SiteLock

Domain	Malware	Spam	Vulnerability	SSL	Risk Score	SMART	PatchMan	SMART DB	WAF Plan
www.infopercept.com	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



# TrustGuard – Daily Scan Reports

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:		

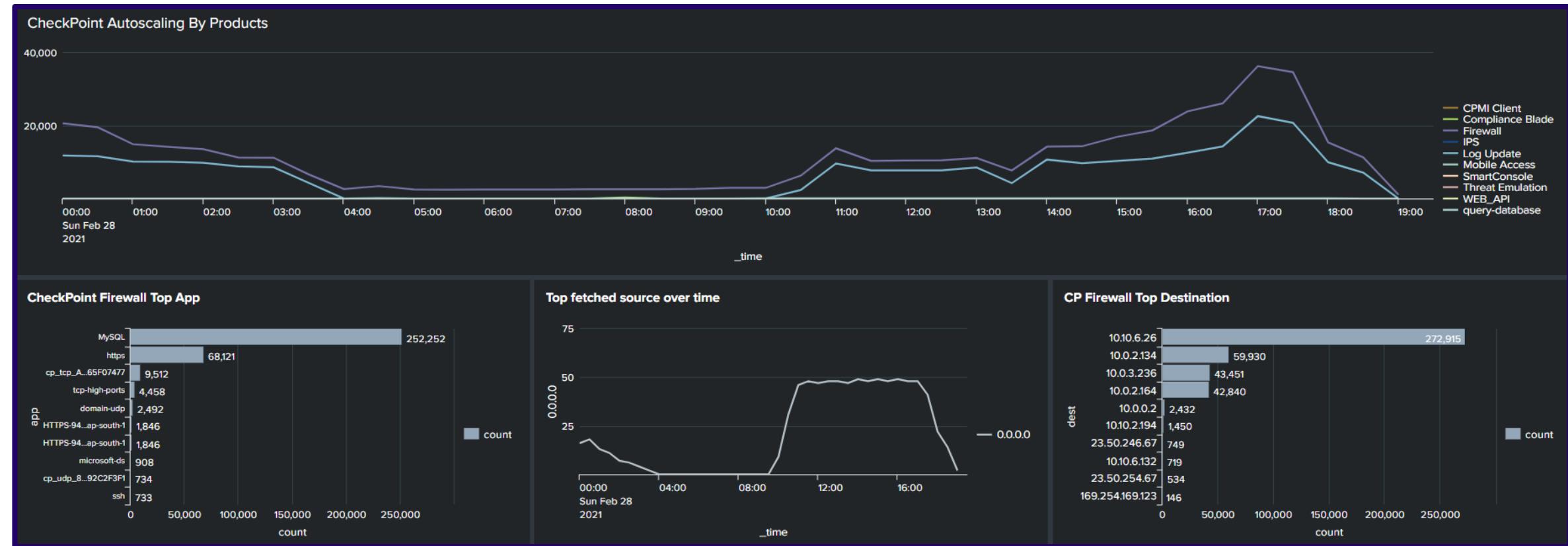
Site Status	Website Details	Blacklist Status
	Website: <input type="text"/>	
	Site Status: <span style="color: green;">OK</span>	
	Blacklist Status: <span style="color: green;">OK</span>	
Malware Scan Status		
	PASSED	2021-02-23 04:15:50
Latest Scan Status		
	PASSED	2021-02-25 07:54:26
		<a href="#">View Reports</a>

# Check Point Report @ABC Corporation



# Checkpoint VPN GW Products

Infopercept



## Threat Emulation Top 10 Source count

No results found.

## Threat Emulation Top 10 Destination count

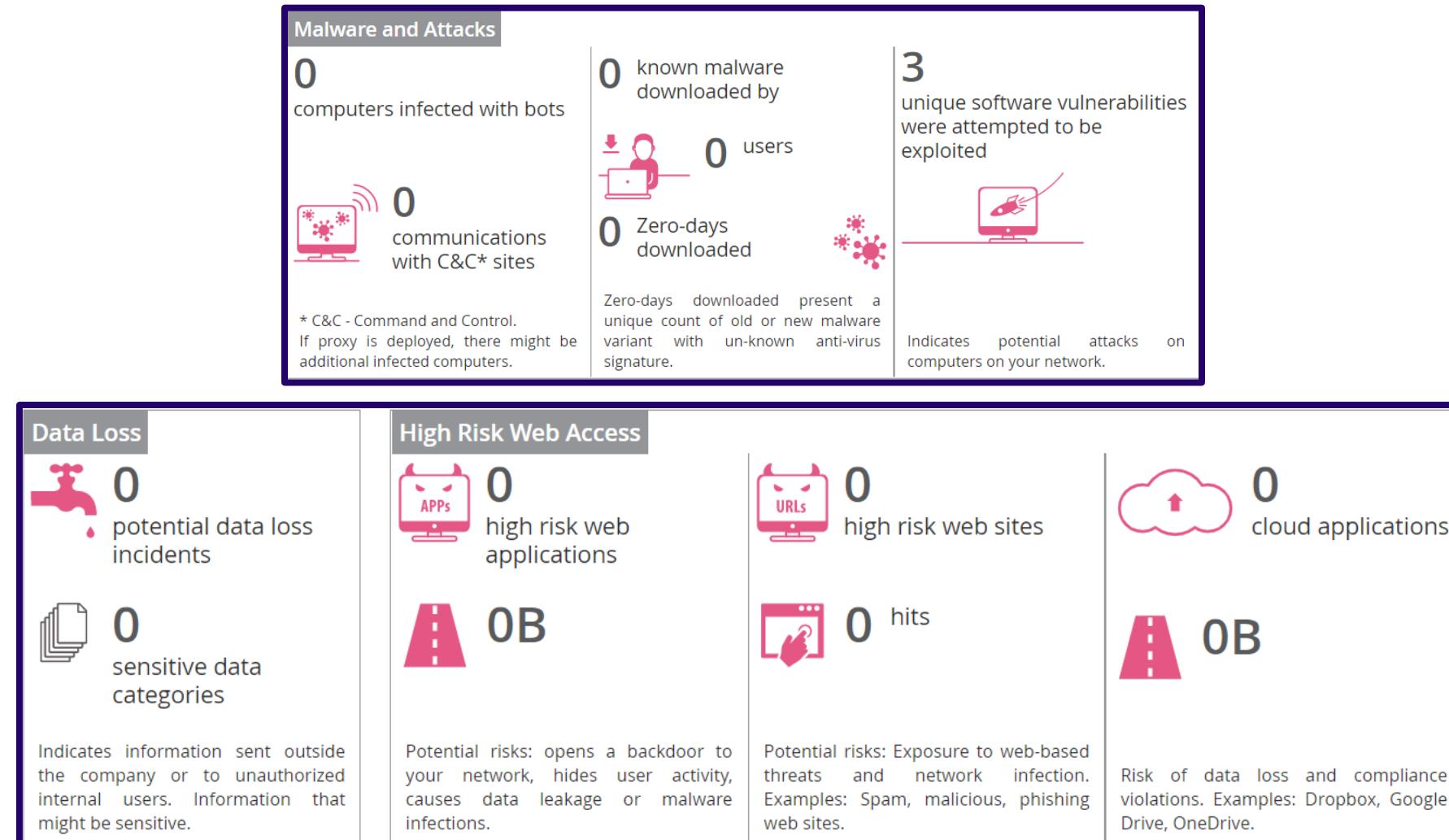
No results found.

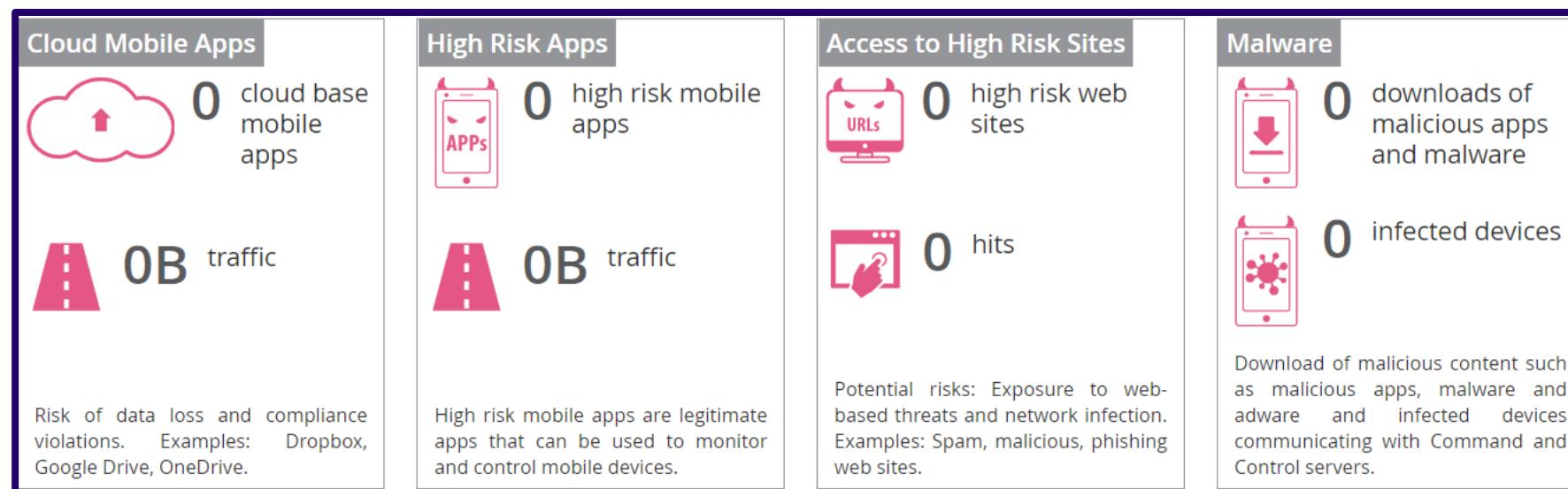
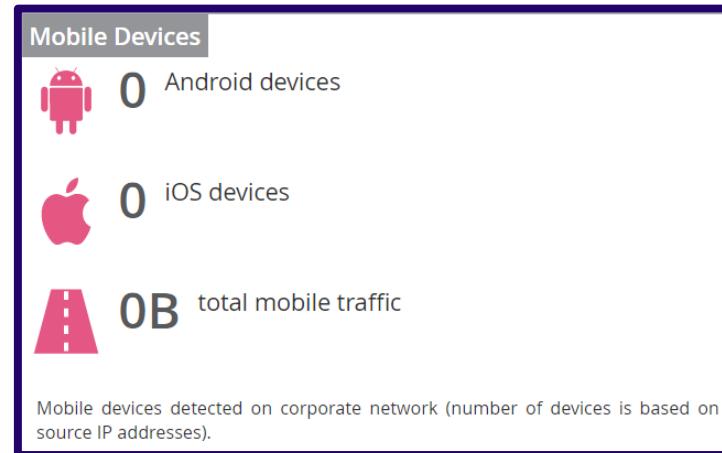
## General Activity

Note: Migration is going on for ABC testing.

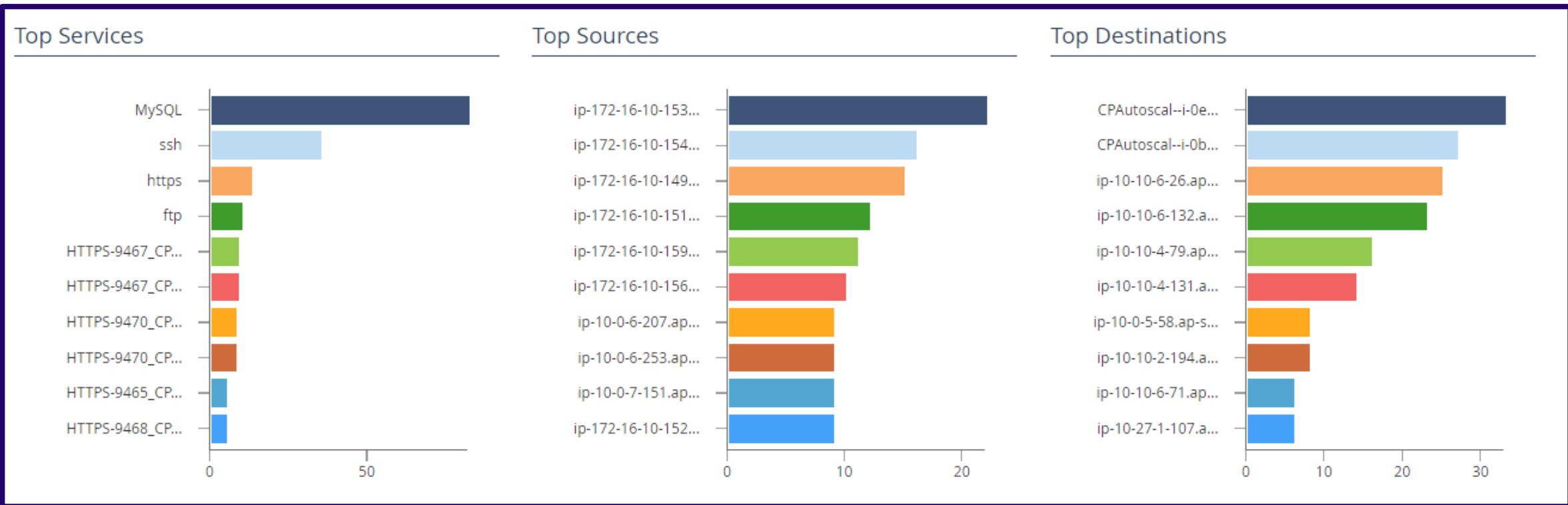
Note: Migration is going on for ABC testing.

# Executive Summary of Security Checkup



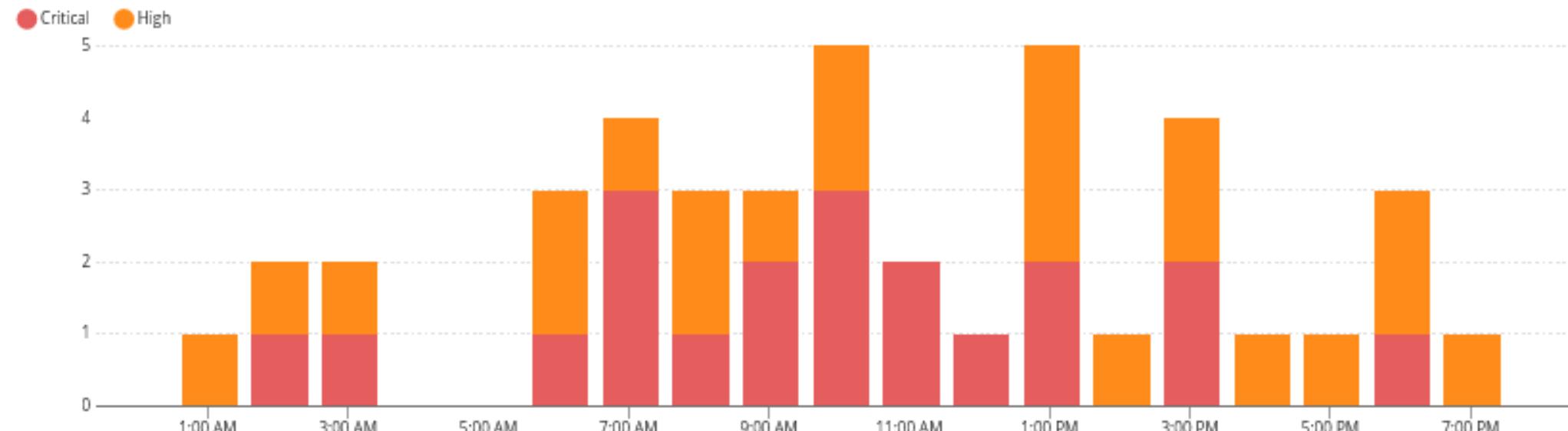


## Network Traffic Analysis



## Overview

Protections By Severity Timeline

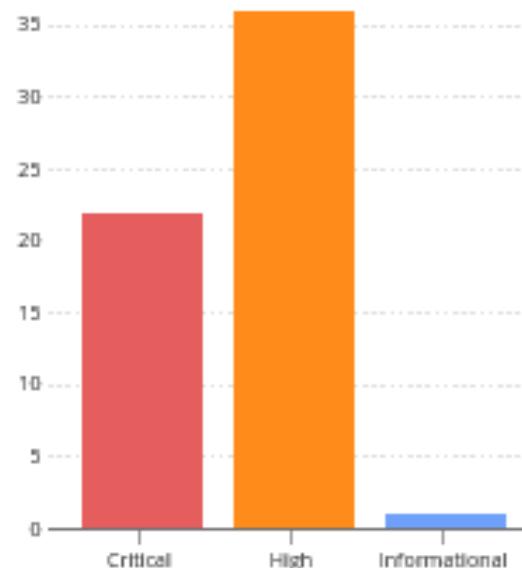


# Intrusion Prevention System

## Top Attacks

Logs	Protection Name	Severity	Action	Origin
20	ZMap Security Scanner over HTTP	<span style="background-color: orange; width: 10px; height: 10px; display: inline-block;"></span> High	Prevent	3 Origins
11	NoneCMS ThinkPHP Remote Code Execution (CVE-2018-20062)	<span style="background-color: red; width: 10px; height: 10px; display: inline-block;"></span> Critical	Prevent	3 Origins
7	Zend Technologies Zend Framework Zend_XmlRpc Information Disclosure	<span style="background-color: orange; width: 10px; height: 10px; display: inline-block;"></span> High	Prevent	3 Origins
5	WordPress HTTP Brute Force Login Attempt	<span style="background-color: orange; width: 10px; height: 10px; display: inline-block;"></span> High	Prevent	2 Origins
4	Web Server Exposed Git Repository Information Disclosure	<span style="background-color: red; width: 10px; height: 10px; display: inline-block;"></span> Critical	Prevent	2 Origins
4	Masscan Port Scanner	<span style="background-color: orange; width: 10px; height: 10px; display: inline-block;"></span> High	Prevent	3 Origins
2	Dasan GPON Router Authentication Bypass	<span style="background-color: red; width: 10px; height: 10px; display: inline-block;"></span> Critical	Prevent	2 Origins
1	Apache Tomcat PUT Method Arbitrary File Upload Remote Code Execution (CVE-2017-12615)	<span style="background-color: red; width: 10px; height: 10px; display: inline-block;"></span> Critical	Prevent	1 Origin
1	PHP Web Shell Generic Backdoor	<span style="background-color: red; width: 10px; height: 10px; display: inline-block;"></span> Critical	Prevent	1 Origin
1	Draytek Vigor Command Injection (CVE-2020-8515)	<span style="background-color: red; width: 10px; height: 10px; display: inline-block;"></span> Critical	Prevent	1 Origin
1	MVPower DVR Remote Code Execution	<span style="background-color: red; width: 10px; height: 10px; display: inline-block;"></span> Critical	Prevent	1 Origin
1	Apache Struts2 Content-Type Remote Code Execution	<span style="background-color: red; width: 10px; height: 10px; display: inline-block;"></span> Critical	Prevent	1 Origin

## Attacks by Severity



# Intrusion Prevention System

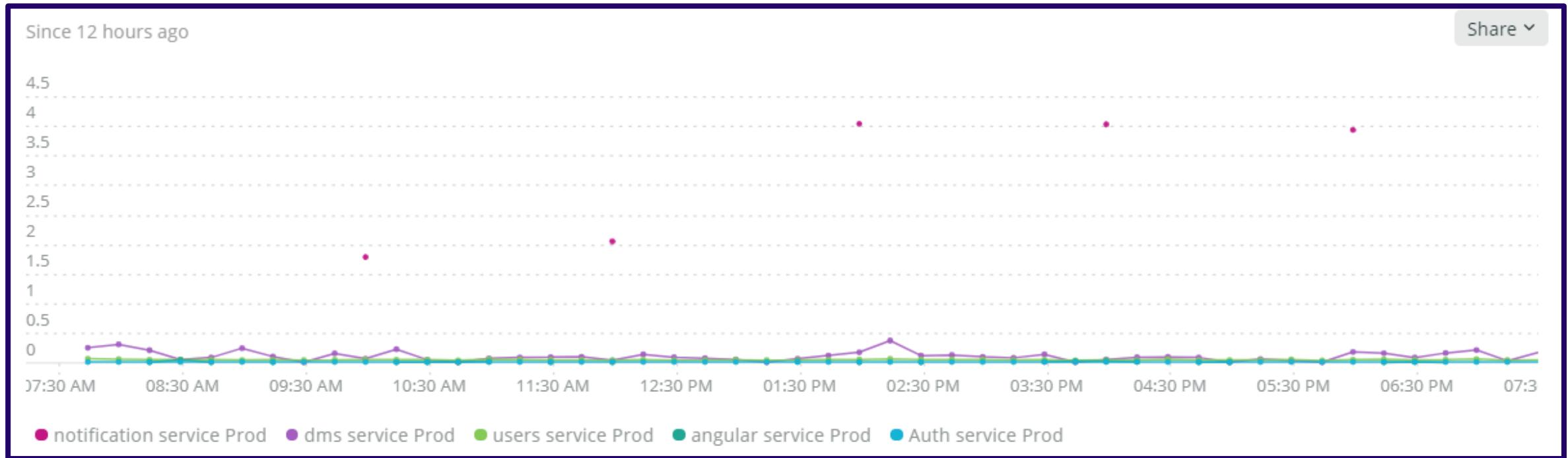
## Top Origins And Top Protections

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
	<b>Total: 9 Protections</b>	 Critical	<b>1 Action</b>	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
	<b>Total: 7 Protections</b>	 Critical	<b>1 Action</b>	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
	<b>Total: 7 Protections</b>	 Critical	<b>1 Action</b>	7
<b>Total: 3 Origins</b>	<b>12 Protections</b>	 Critical	<b>1 Action</b>	58

# New Relic APM Report @ABC Corporation



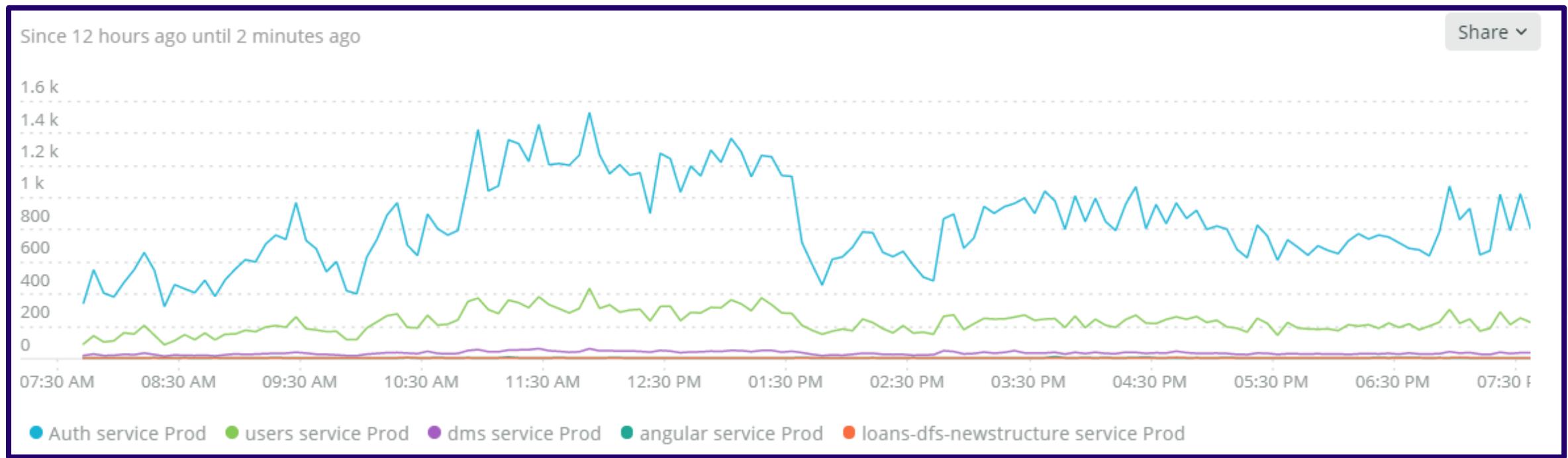
## Top 5 application services response time



notification service Prod had highest response rate.

# Host Monitoring – Application Throughput

## Top 5 application services throughput



Auth service Prod had highest throughput rate

# Imperva Report @ABC Corporation



# Incapsula Main View Attack Logs

Infopercept



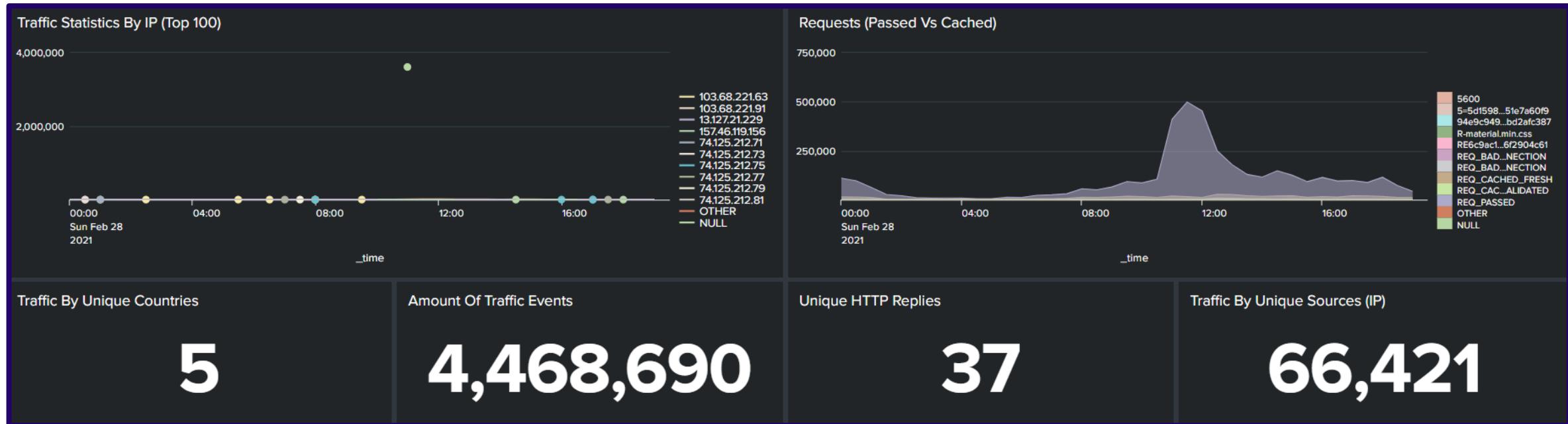
Number Of Attacking Countries	Number Of Attacks	Number Of Attack Types	Number Of Attackers
12	415	9	33

Attack Types	Count	Percentage
<a href="#">IncapRules(Anti Scrapper Policy)</a>	304	68.315%
<a href="#">IncapRules(Clients with more than 2 UA)</a>	51	11.461%
<a href="#">Bot Access Control</a>	40	8.989%
<a href="#">Illegal Resource Access</a>	32	7.191%
<a href="#">IncapRules(Blocking Attacks)</a>	10	2.247%
<a href="#">IncapRules(Block Anonymous Proxy and TOR)</a>	3	0.674%
<a href="#">IncapRules(Blocking Web Attacks)</a>	3	0.674%
No cst 4dr cst ref: rec ver  d82b81306e79d3 Browser cs6Lab: request=dil.ban/ utm_source\=A1 ExternalId=52851 1	d9bdc8c385522e4a42cd214641a4d1 itude.cs8=77.5855 &ccn\=206796_78049&px\=1 :pt=63760 src=l57.45.218.65	1 0.225%
<a href="#">SIEMintegration</a>	1	0.225%

# Incapsula Main View Traffic Logs

Infopercept

IMPERVA  
INCAPSULA



# AV Security Report @ AWS & CW Office



## 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
<b>Grand Total</b>	<b>1</b>

# 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

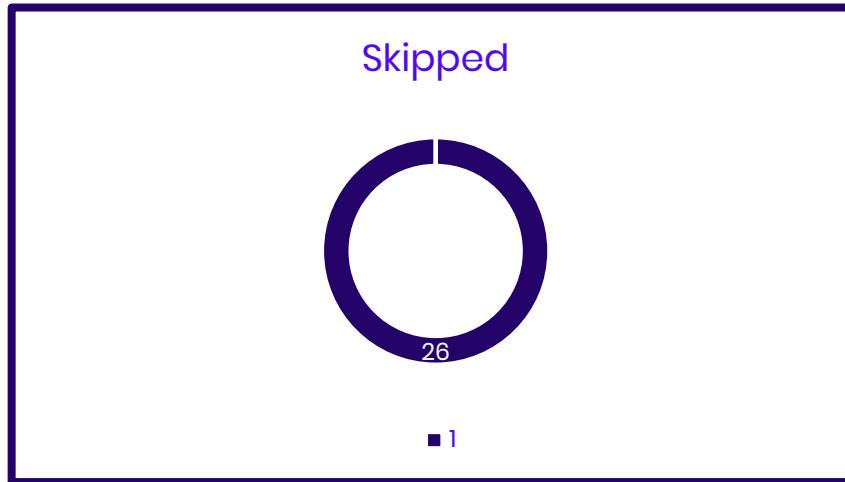
Group Name: All Groups

Endpoint Name: All

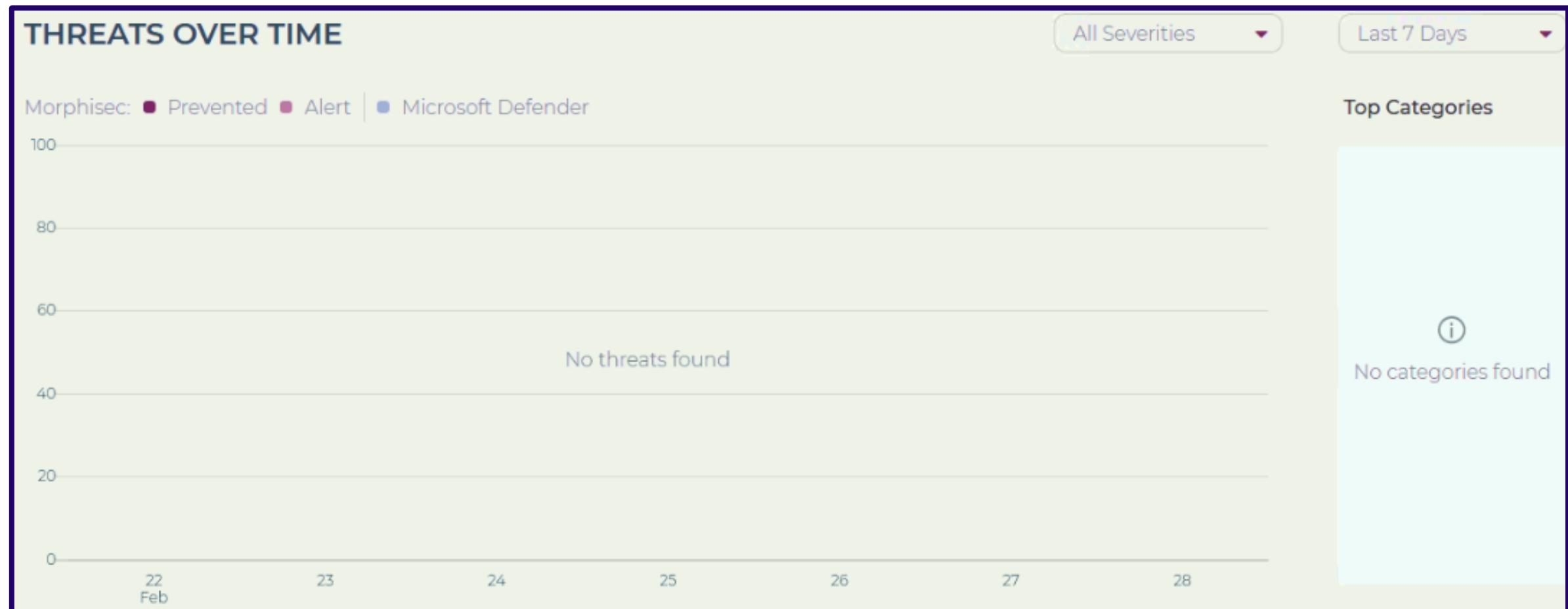
User Name: All

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

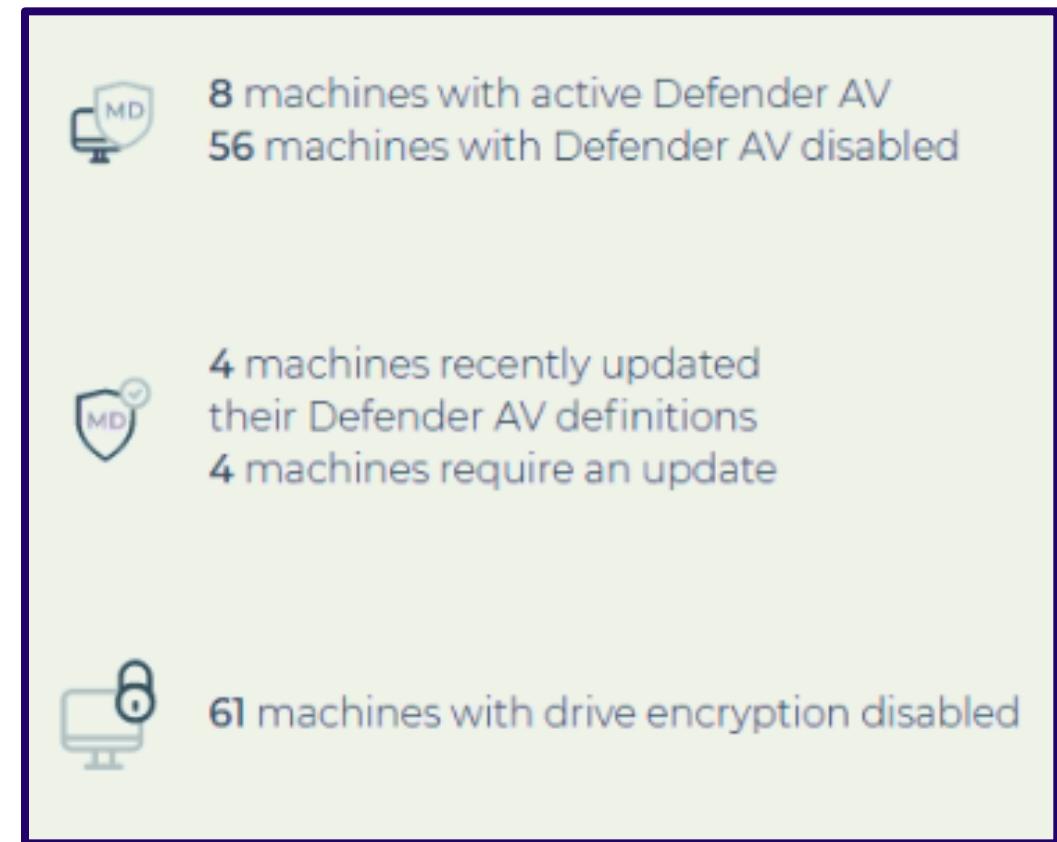
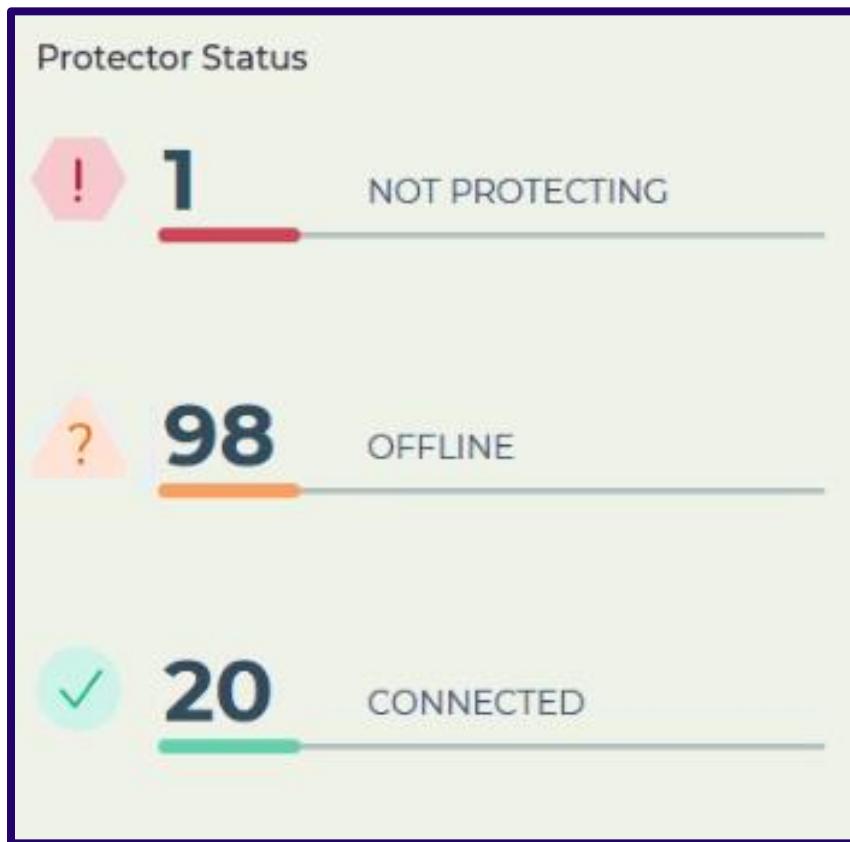


Auth service Prod had highest throughput rate

# PROTECTOR STATUS

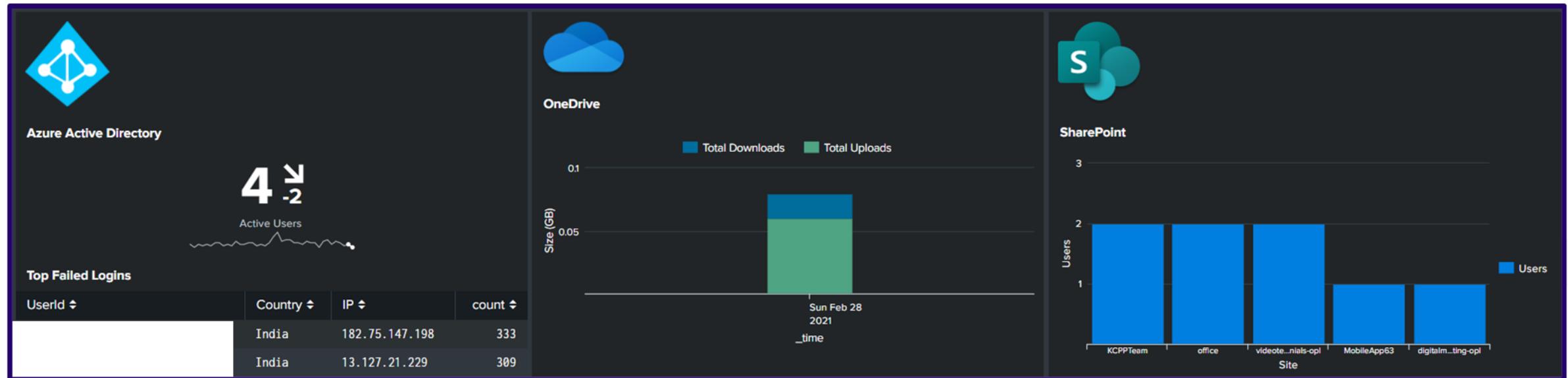
Infopercept

MORPHISEC  
Moving Target Defense

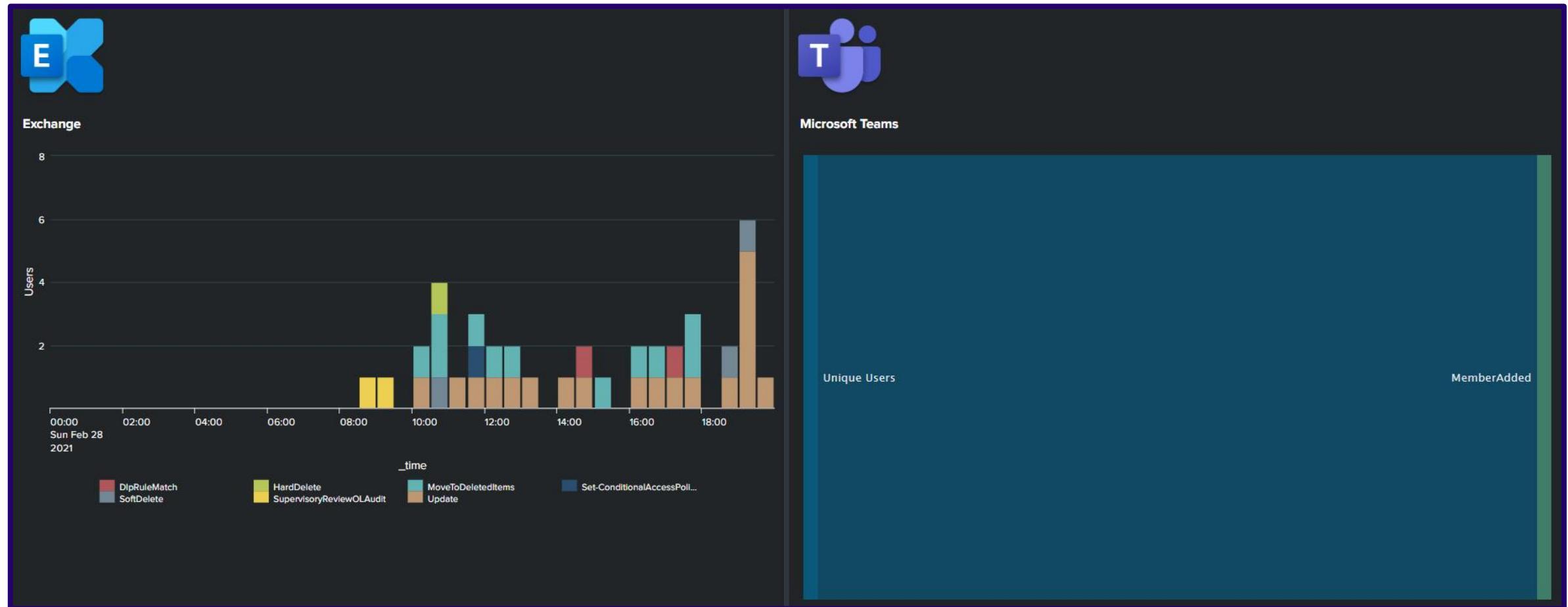




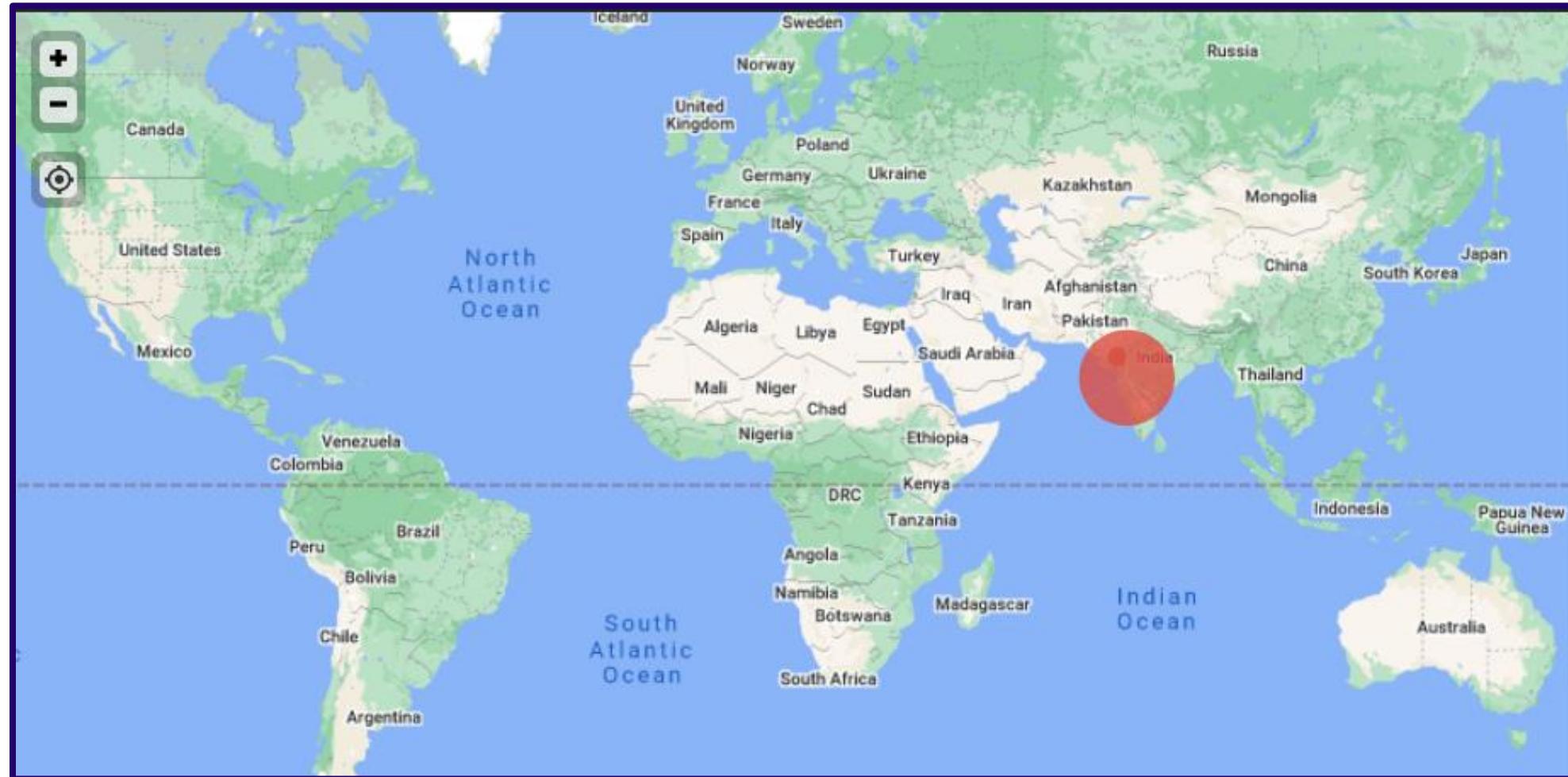
# Office 365 Overview



# Office 365 Overview

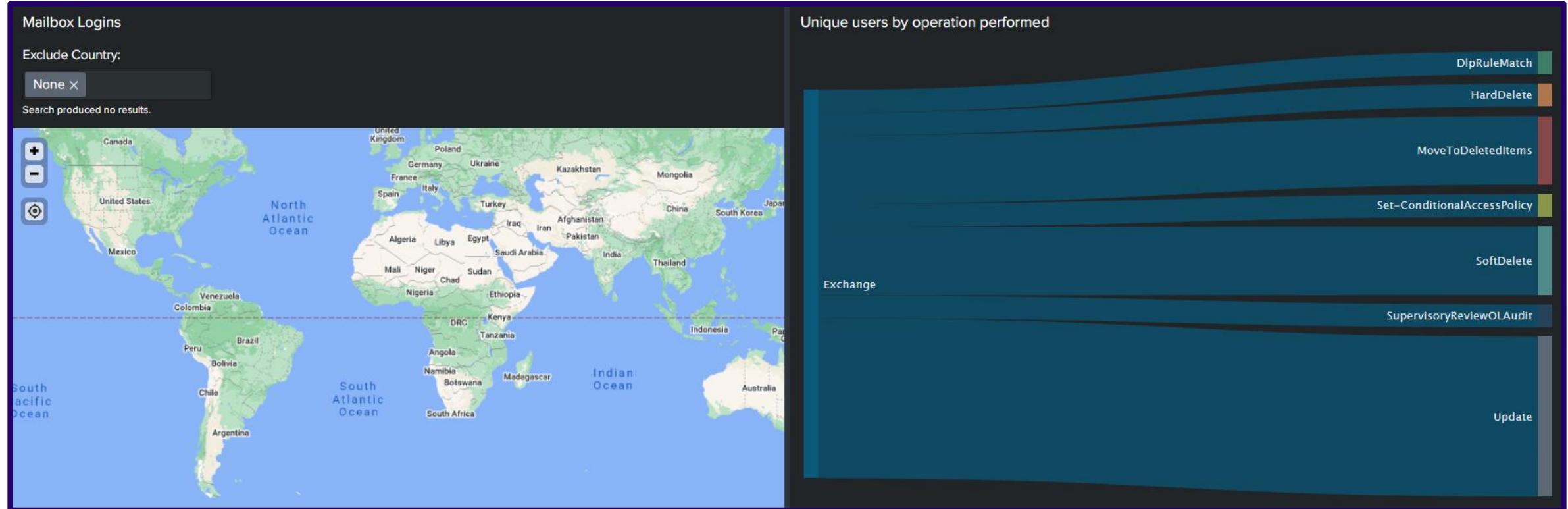


# Office 365 Azure AD Login Activity



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

# Office 365 Exchange Overview



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

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-Address

Failed login attempts from multiple IP-Addresses		
User	UniqueIP	SourceIP
[REDACTED]	2	182.75.147.198
		203.88.128.170

## Device compliance status

Status	Devices
Compliant	57
In grace period	0
Not evaluated	36
Not compliant	8 <span style="color:red;">!</span>
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**

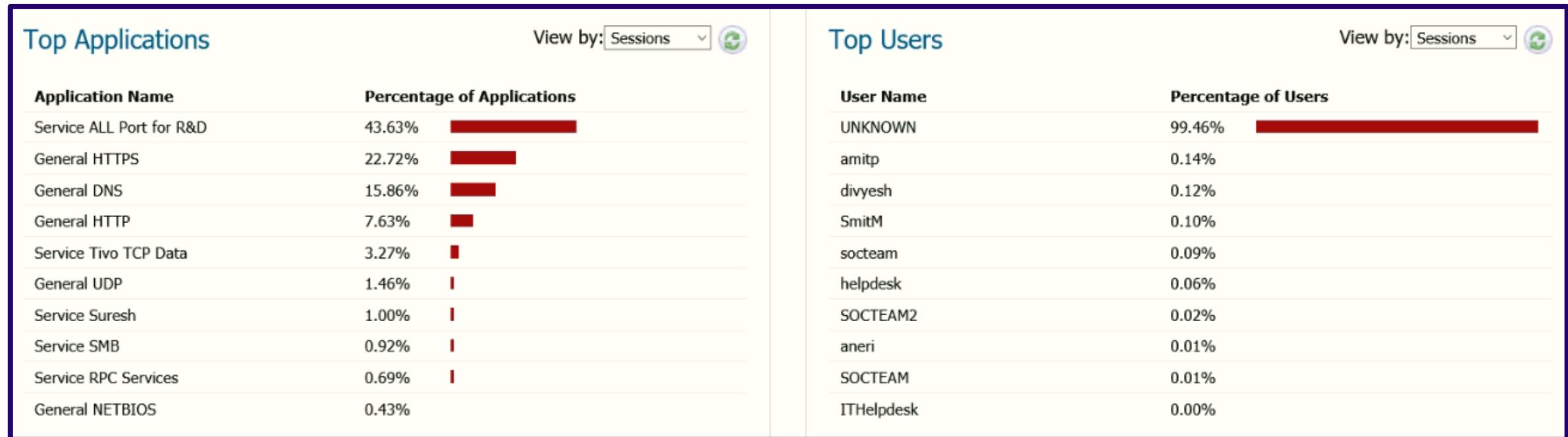
### Resource alerts

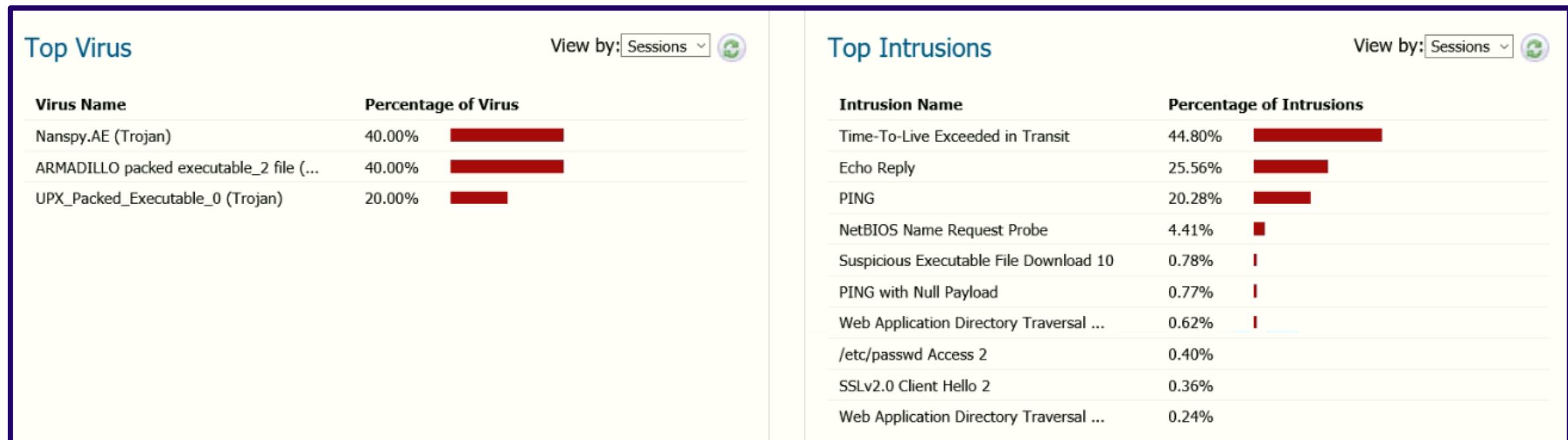
! Device compliance  
8 devices not in compliance

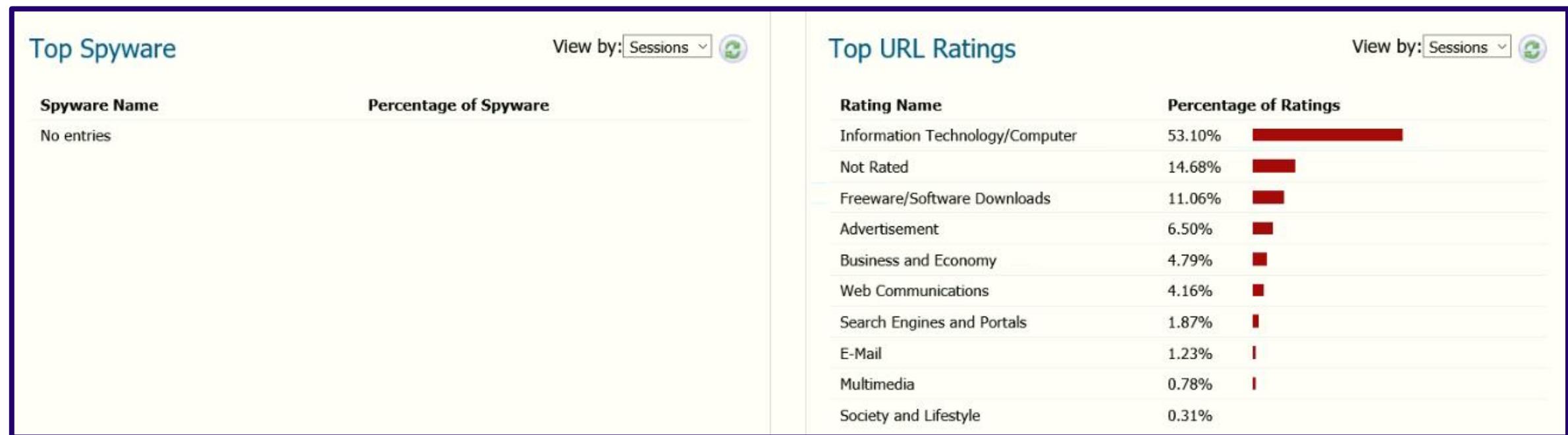
! Device configuration  
2 devices have profile errors

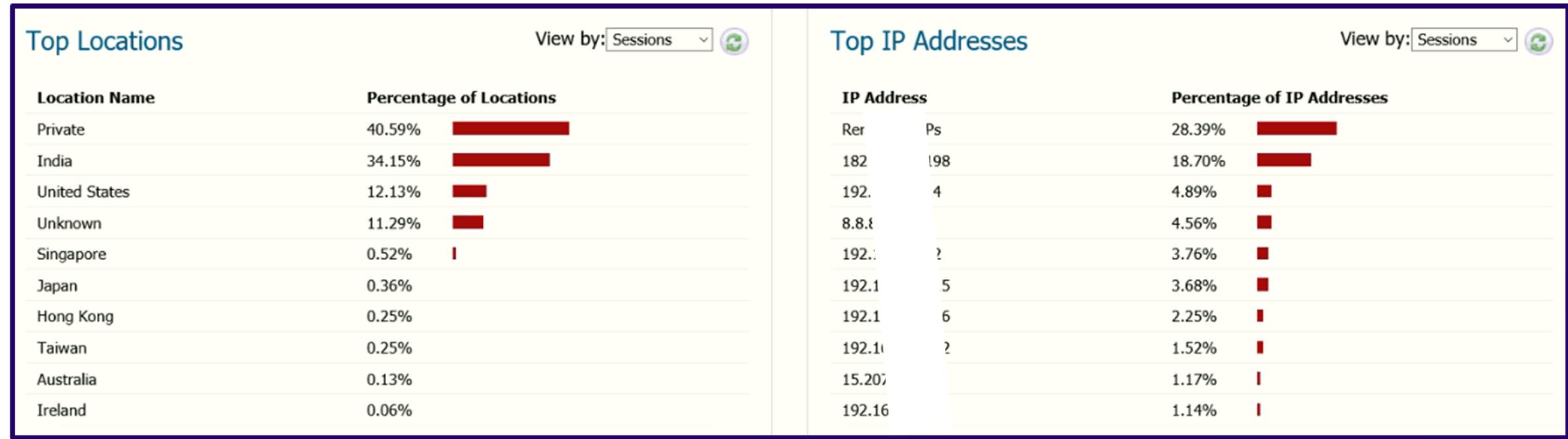
! Device enrollment  
5 devices have enrollment failures

! Client apps  
1 installation failure

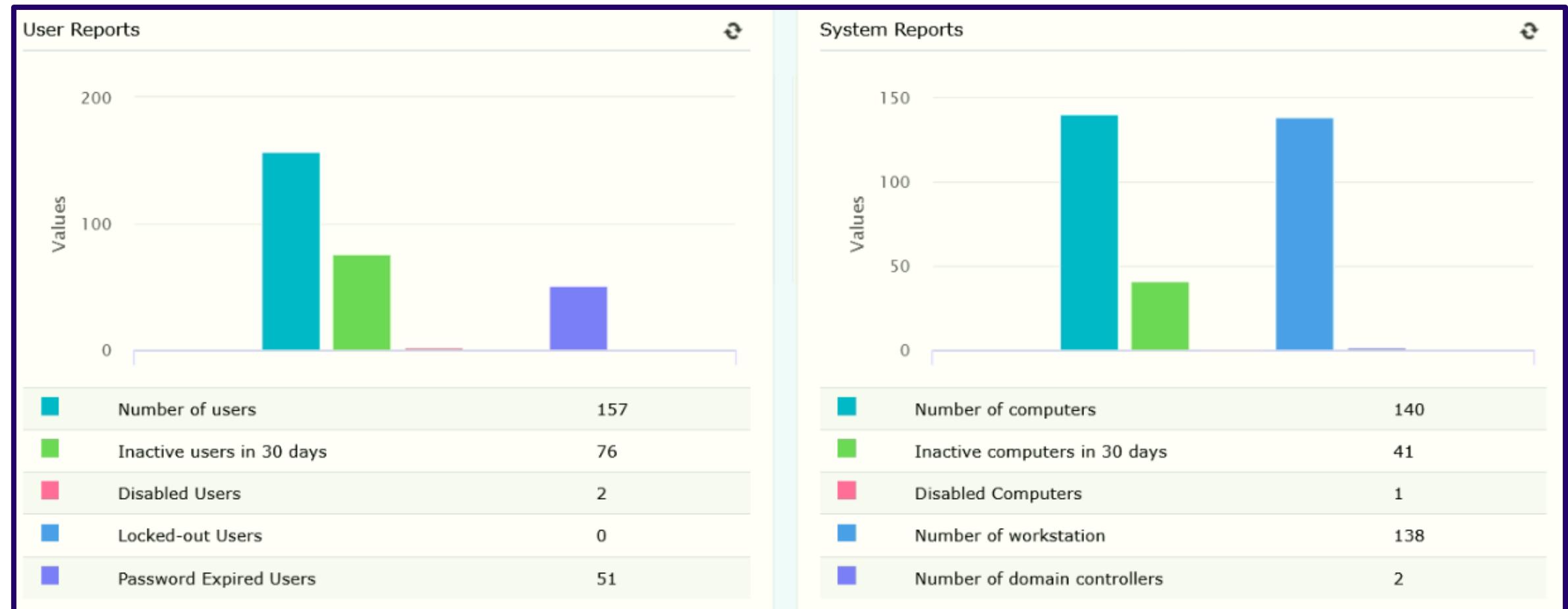




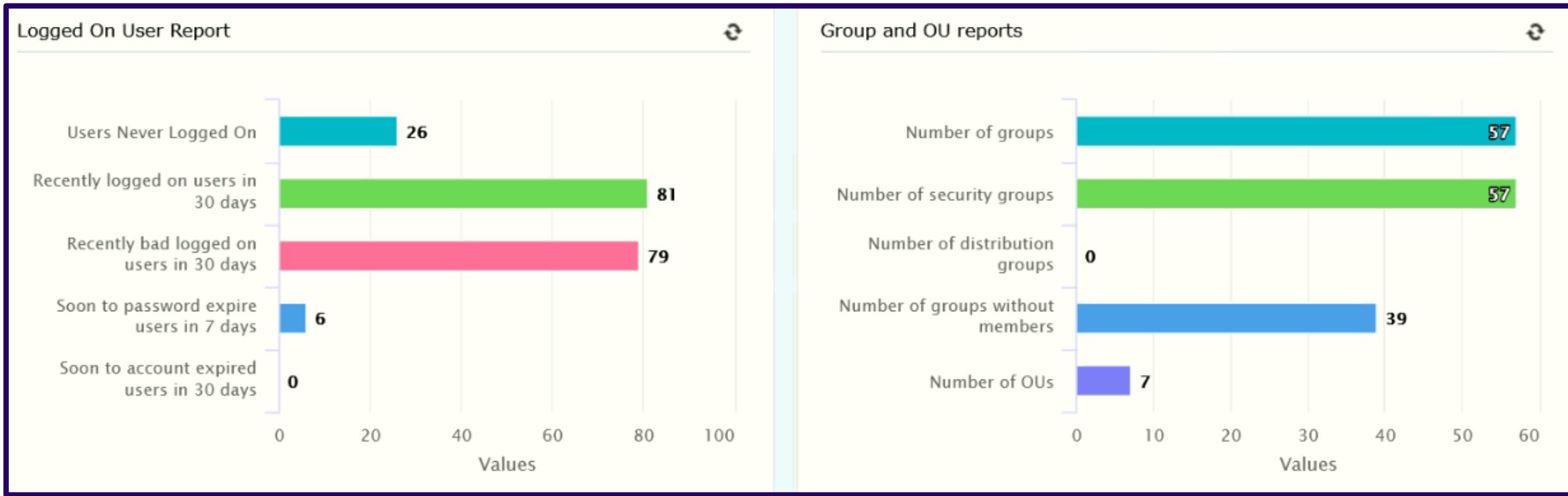




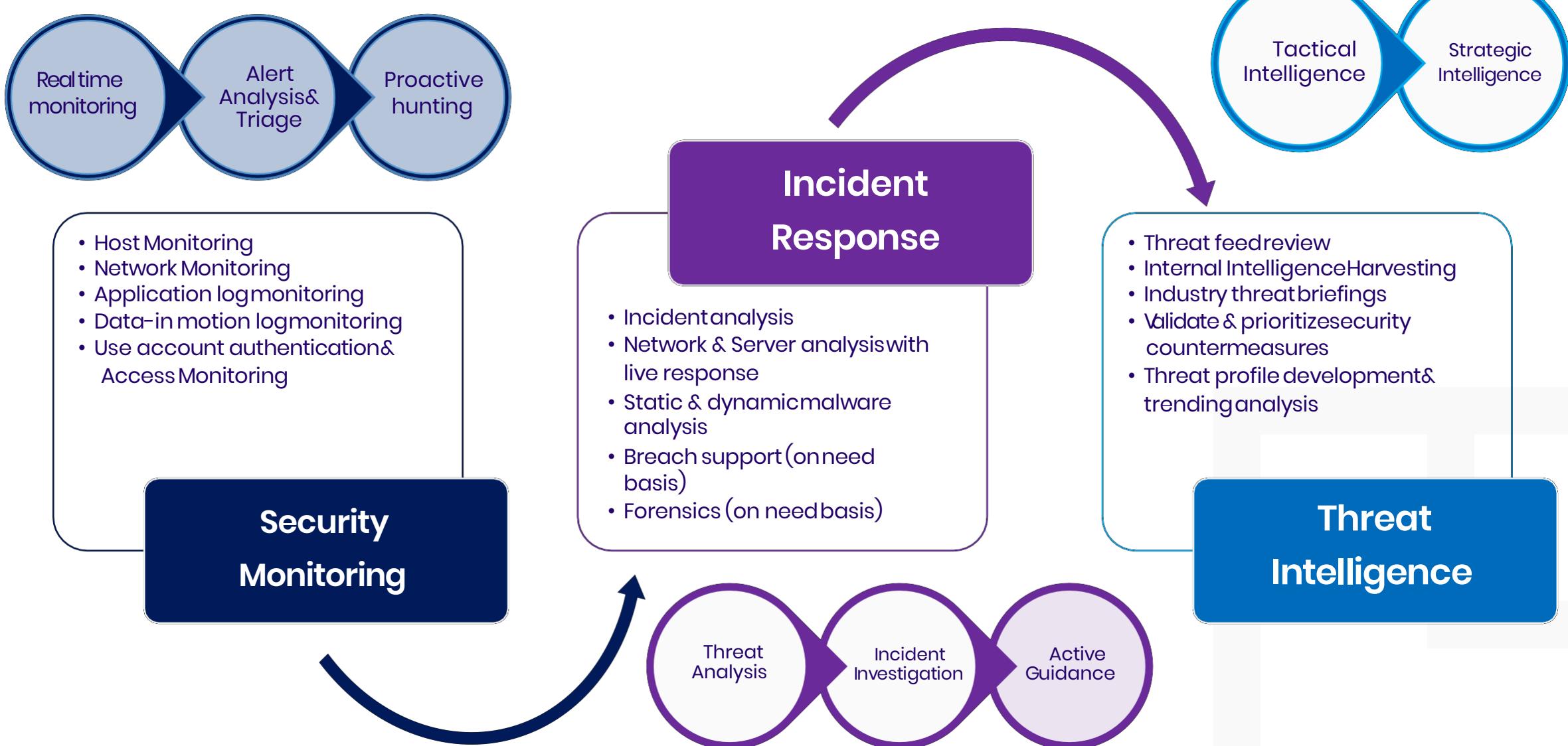
# User And System Reports:



# 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](http://www.infopercept.com)  
E: [sos@infopercept.com](mailto: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](http://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

