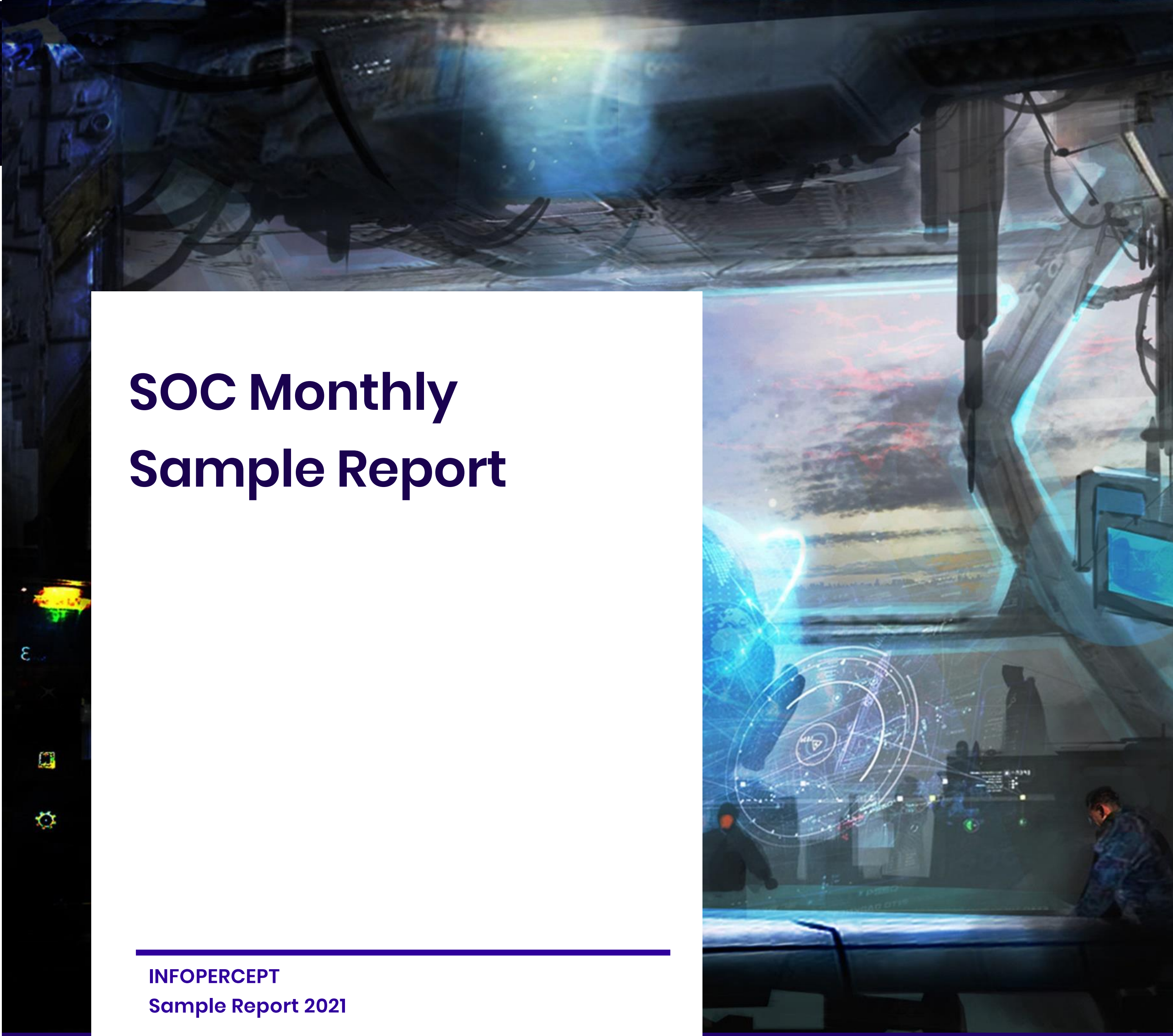


SOC Monthly Sample Report

INFOPERCEPT
Sample Report 2021

Infopercept

YOUR DATE HERE

COMPANY NAME
Authored by: Your Name

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.

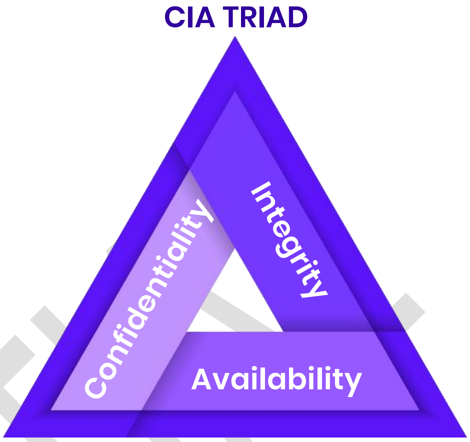
Table of Contents

Copyright

Disclaimer

By accessing and using this report you agree to the following terms and conditions and all applicable laws, without limitation or qualification, unless otherwise stated, the contents of this document including, but not limited to, the text and images contained herein and their arrangement are the property of Infopercept Consulting Pvt Ltd (Infopercept). Nothing contained in this document shall be construed as conferring by implication, estoppel, or otherwise, any license or right to any copyright, patent, trademark or other proprietary interest of Infopercept or any third party. This document and its contents including, but not limited to, graphic images and documentation may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, without the prior written consent of Infopercept. Any use you make of the information provided, is at your own risk and liability. Infopercept makes no representation about the suitability, reliability, availability, timeliness, and accuracy of the information, products, services, and related graphics contained in this document. All such information products, services, related graphics and other contents are provided 'as is' without warranty of any kind. The relationship between you and Infopercept shall be governed by the laws of the Republic of India without regard to its conflict of law provisions. You and Infopercept agree to submit to the personal and exclusive jurisdiction of the courts located at Mumbai, India. You are responsible for complying with the laws of the jurisdiction and agree that you will not access or use the information in this report, in violation of such laws. You represent that you have the lawful right to submit such information and agree that you will not submit any information unless you are legally entitled to do so.

Infopercept



Client Name	ABC Corporation
Name of report recipient	CISO
Report Created for:	ABC Corporation
Report issue date	30 October 2020
Report Version	1.0
Author Name	Infopercept SOC Team
Classification	Client Confidential

CYBER SECURITY IS OUR SHARED RESPONSIBILITY

Project Description

PROJECT OVERVIEW

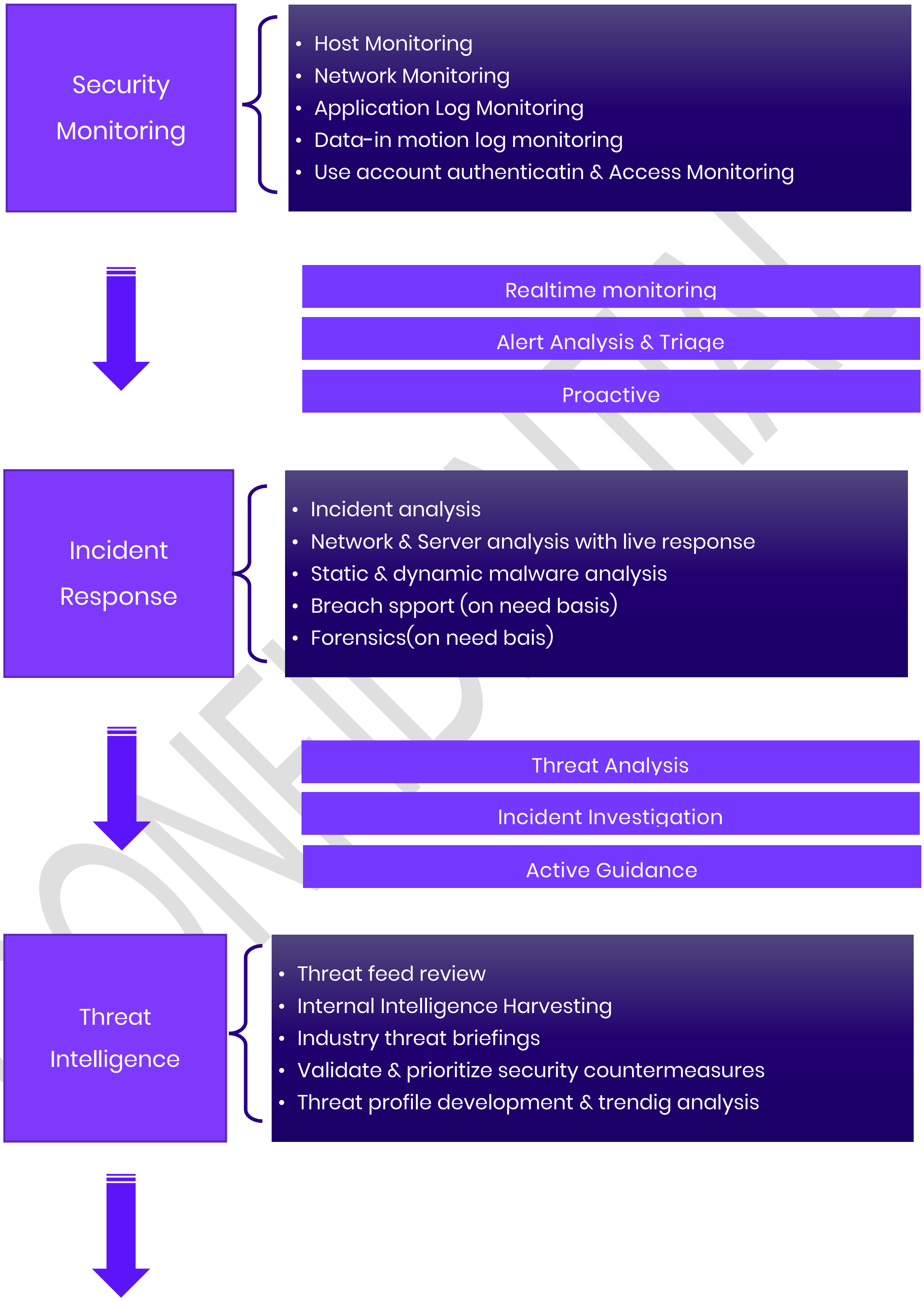
ABC Corporation is the first Intelligent, Innovative and Automated finance platform that connects various Fund seekers, Fund provider and service providers. The web portal provides fund processing quickly.
Current technical security assessment focuses on security assessment covering the hosting of application over AWS environment and controls applied over the operating system, database, application server & logical access controls implemented over the ABC portal.

PROJECT OBJECTIVE

Periodic blue team exercise by Infopercept team is typically recommended to actively strengthen an organization's security posture. This approach facilitates the provision of clear and specific "Early Warning System" about the applications, systems and network. In other words, the weaknesses in the infrastructure are identified by Infopercept team before they can be exploited by intruders and malicious insiders.

PROJECT OBJECTIVE POINT

1. Identify and prioritize the organization's risks.
2. Minimize the likelihood of data breaches.
3. Help to safeguard sensitive data and intellectual property
4. Improve compliance with industry and regulatory requirements (e.g. PCI-DSS, ISO27001, GDPR).
5. Improve the reputation and goodwill of the organization.
6. Inspire customers' confidence.



Security Monitoring

- Host Monitoring
- Network Monitoring
- Application Log Monitoring
- Data-in motion log monitoring
- Use account authenticatin & Access Monitoring

Realtime monitoring

Alert Analysis & Triage

Proactive

Incident Response

- Incident analysis
- Network & Server analysis with live response
- Static & dynamic malware analysis
- Breach spport (on need basis)
- Forensics(on need bais)

Threat Analysis

Incident Investigation

Active Guidance

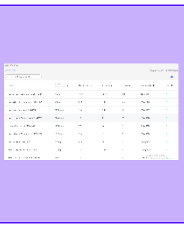
Threat Intelligence

- Threat feed review
- Internal Intelligence Harvesting
- Industry threat briefings
- Validate & prioritize security countermeasures
- Threat profile development & trendig analysis

1. Annexure A

Particulars	Activities	Status	Page
1. Security Operations Center	• Remote Monitoring Services for Client on 24x7 basis (355 days) • Daily, weekly and monthly reporting to Client management	Completed	
2. Certification support	• Responsible for maintenance of ISO 27001:2013 standard certification at client end. • Responsible for managing Bank ORA (onsite risk assessments) & annual vendor risk assessments. • Implementing ISO 22301 requirement and guiding ABC toward ISO 22301 certification & continuous management. • Responsible for managing ORA / site reviews by agency (xyz-xxy-xxz-yyz-zzx-xxz and other banks on case to case basis as would be required) wrt Information Security Responsible for action tracker for closing observations / issues raised in audit within reasonable timeframe as agreed with Client Management • Managing relationships with auditors & external agencies wrt to audit & representing as Virtual CISO & BCM at client end	ISO 27000 Completed on July 2020	N/A
3. Vulnerability Assessment & Penetration Testing	• Monthly VAPT for entire infrastructure • VAPT in case of critical incident detection. • VAPT on every new product / module release (Client would not release code to production without Service Provider consent) • Detailed report to be furnished to Client management on every VAPT • Security Testing for each release	**Completed** Detailed reports shared via email and through mentioned tickets.	
4. Red Teaming Exercise	• Advanced Phishing attack simulation • Advanced malware attack simulation • API Security Attack Simulation • Database Security Simulation • Advanced Wireless Security Testing • Targeted User attack simulation	CWIS-775 CWIS-774 CWIS-782 CWIS-776 CWIS-758 CWIS-760	
5. ISMS Training & Awareness	• Launching monthly awareness campaign; measuring & communicating training feedback to management • Helping in creating knowledge repository & training records for Client • In person training sessions on bi-annual basis for all employees along with Quiz.	Completed	

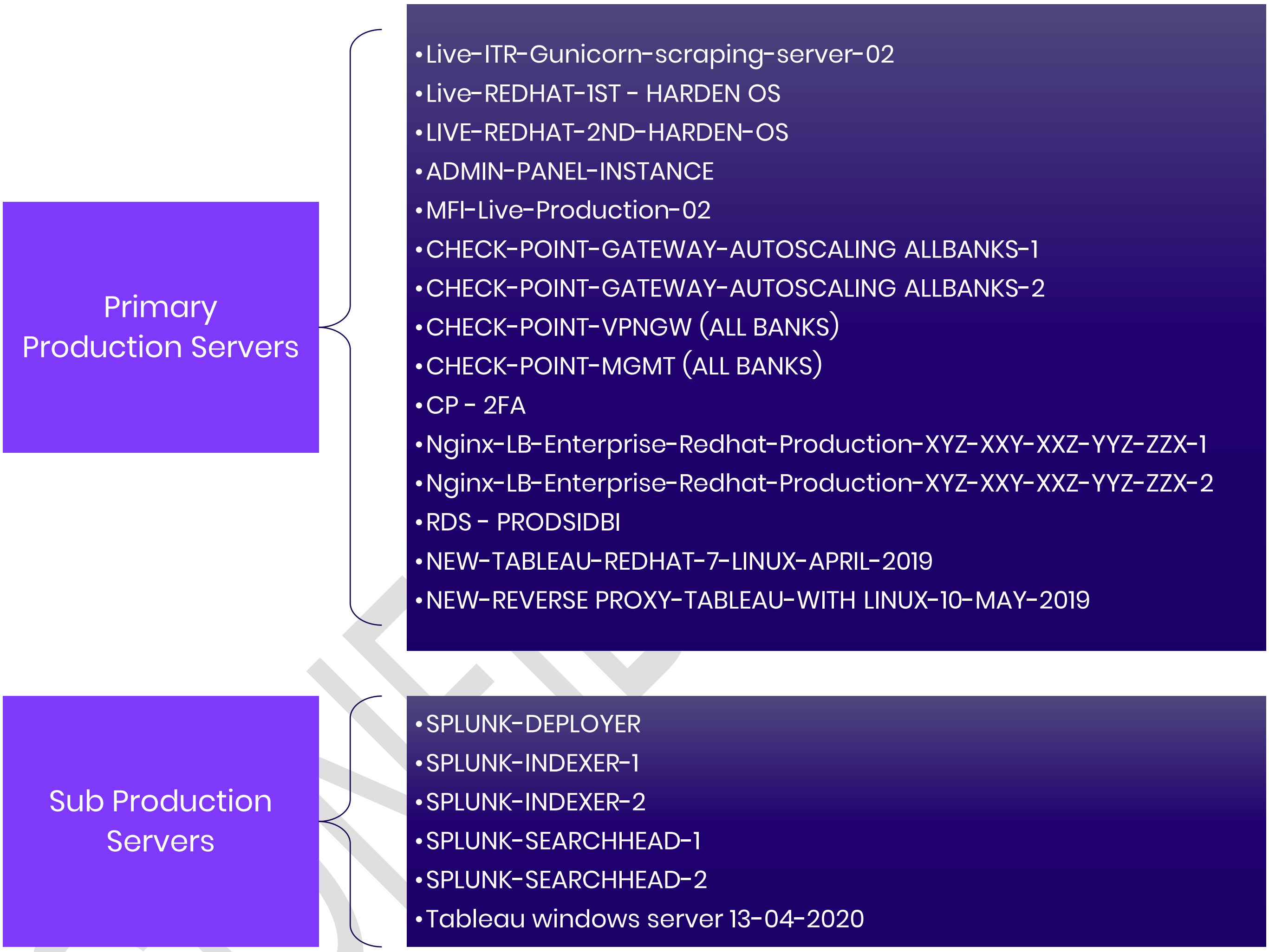
Particulars	Activities	Status	Page
6. Policy & Procedure Management	• Maintaining ISMS policies and procedures, hardening guidelines, mandated by ISO 27001, banks, agencies, regulatory authorities • Ensuring proper communication of Client's policies & procedure to employees at regular intervals; • Ensuring adherence to ISMS review procedure & enhancing the policies and procedures at annual interval. • Ensuring required policy / procedures for Privacy management & BCM	Task Completed	
7. Data Security & Information Risk Management	• Keeping risk register updated with risk treatment plan • Conducting periodical risk assessment in line with ISMS procedure • Recommending actions required at various risk levels • Updating management on monthly basis for high /critical risk & Status report for various risk identified. • Auditing end point security & related technologies • Auditing email technologies and sharing information on emails & recommendations for enforcement of end point security.	Completed	ABC Risk Register.pptx
8. Infrastructure Management	• AWS infrastructure security reviews • Guiding adherence on Change management cycle requirement & building up the process • Active directory design, setup & group policy suggestions on implementing along with hardening • Antivirus policy management & guidance on incident management against critical threats • Backup policy & framework creation for CCTV footage, access management • Recommendations on Email security implementations – AD sync, rights management, IP binding, group management, • Infrastructure architecture and vendor co-ordination on setup.	Completed	Access_Control_Matrix.xlsx CIS_Amazon_Web_Services_Three Tier.word

Particulars	Activities	Status	Page
9. Firewall Security	• Firewall Configuration review on biannual basis • Vulnerability assessment of firewall security covering port scanning, • Creation of content filtering policies for various teams • Critical incident review • SonicWALL Access rule hardening in process. Completed issue points are defined in SonicWALL access rule	Completed	CFS Report V2.xlsx
10. Hardening Reviews	• Hardening reviews & implementation support for AWS, OS, DB, Firewall, • Reviewing timely closure of issues identified during hardening review and updating management at quarterly intervals.	We have completed hardening of ABC (Ahmedabad) Office.	
11. Secure SDLC	• Strategizing & building up mobile platform of Client with security requirements • Interaction with stakeholders on freezing the Secure SDLC process • Interaction with vendors (if required) to clearly lay out security guidelines (Completed) • Suggesting process improvements to make development cycle secure. • Note: This requires investment of tool and people following the process suggested.	CWIS-440 CWIS-448 CWIS-458 We will not provide Sonarqube report this month due to work load of developers.	PDF ABC(Android)Mobile_Static_VAPT PDF ABC(Android)Mobile_Static_VAPT
12. Business Continuity	• Guiding out to have biannual BCP drills & setting up communication plan for the drills • Drafting up BCP test results and management review & suggestion to build up strong program • Building up disaster recovery plan (DRP), • DR Drill checklist creation and communication to team members • POC & Co-ordination for DR setup with Third party co-location service provider.	Imperva Enhancement of websites, Firewall enhancements done.	
13. ISMS implementation	• Implementation during scope enhancements as needed over period of time e.g. addition of product line in mobile or change in office	Imperva Enhancement of websites, Firewall enhancements done.	

Particulars	Activities	Status	Page
14. Technology evaluation	• Recommendation, comparison and analysis for all the procurement impacting IT infra, IT Policy & IT security policyTechnology evaluation	Morphisec, Sophos AV, Microsoft Intunes	PDF POC for Android_Intune PDF Morphisec_POC v2
15. Gameplan - Security Dashboard for Boardroom	• Product will help ABC to populate Risk, Dashboards required by Management and we don't need to run Presentation for the same	Need 2 server for game plan. Base configuration would be 4 core process and 16GB ram. By June the implementation will start.	N/A
16. Security Automation	• Integration with Amazon Alexa for Splunk • Creation of Bot for L1 areas agreed between ABC & Infopercept	Integration of Alexa and Splunk has been completed successfully. Chabot has been created for communicating alarm over telegram.	BMP Bitmap Images

2. Server Inventory

Total Servers - 21



Primary Production Servers

- Live-ITR-Gunicorn-scraping-server-02
- Live-REDHAT-1ST - HARDEN OS
- LIVE-REDHAT-2ND-HARDEN-OS
- ADMIN-PANEL-INSTANCE
- MFI-Live-Production-02
- CHECK-POINT-GATEWAY-AUTOSCALING ALLBANKS-1
- CHECK-POINT-GATEWAY-AUTOSCALING ALLBANKS-2
- CHECK-POINT-VPNGW (ALL BANKS)
- CHECK-POINT-MGMT (ALL BANKS)
- CP - 2FA
- Nginx-LB-Enterprise-Redhat-Production-XYZ-XXY-XXZ-YYZ-ZZX-1
- Nginx-LB-Enterprise-Redhat-Production-XYZ-XXY-XXZ-YYZ-ZZX-2
- RDS - PRODSIDBI
- NEW-TABLEAU-REDHAT-7-LINUX-APRIL-2019
- NEW-REVERSE PROXY-TABLEAU-WITH LINUX-10-MAY-2019

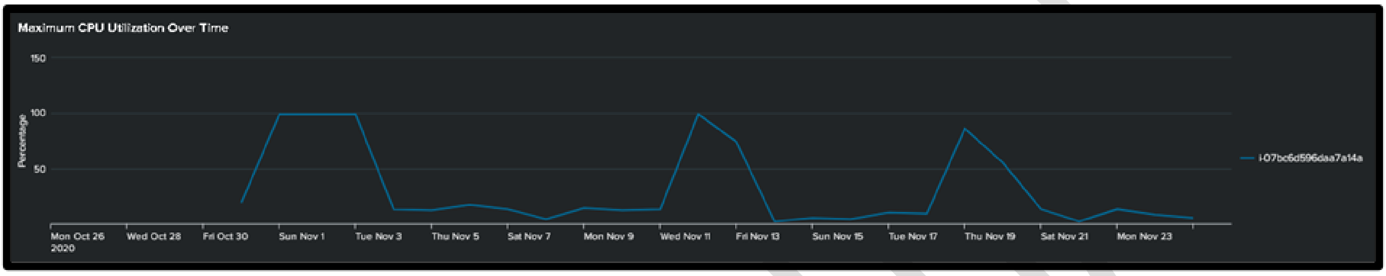
Sub Production Servers

- SPLUNK-DEPLOYER
- SPLUNK-INDEXER-1
- SPLUNK-INDEXER-2
- SPLUNK-SEARCHHEAD-1
- SPLUNK-SEARCHHEAD-2
- Tableau windows server 13-04-2020

3. Host Monitoring: Primary Production Servers

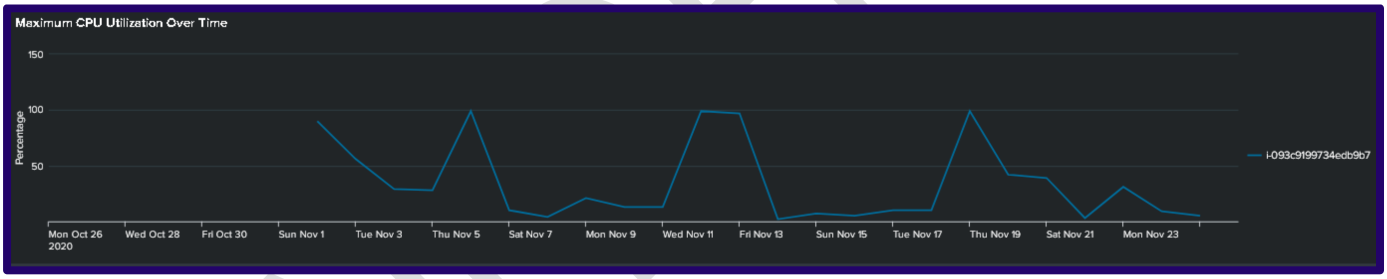
3.1. Prod-ABC-V2-Server-1

Instance Under monitoring	IP Address	CPU Utilization
Prod-ABC-V2-Server-1	10.0.4.252	19% to 5%



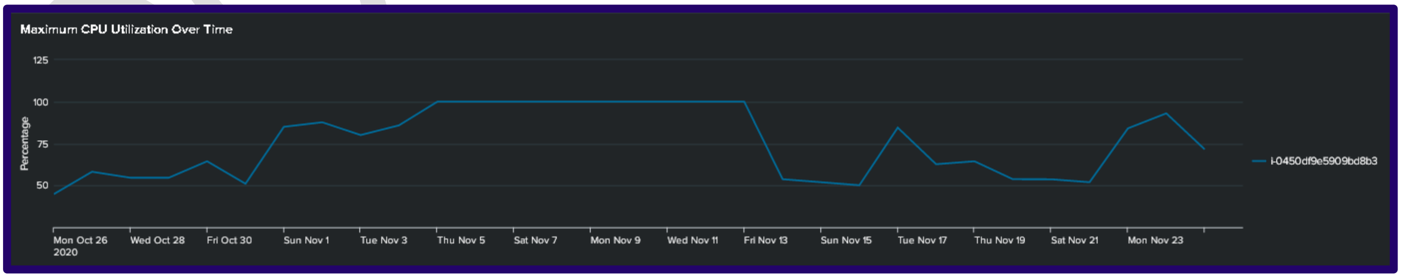
3.2 Prod-ABC-V2-Server-2

Instance Under monitoring	IP Address	CPU Utilization
Prod-ABC-V2-Server-2	10.0.5.229	90% to 5%



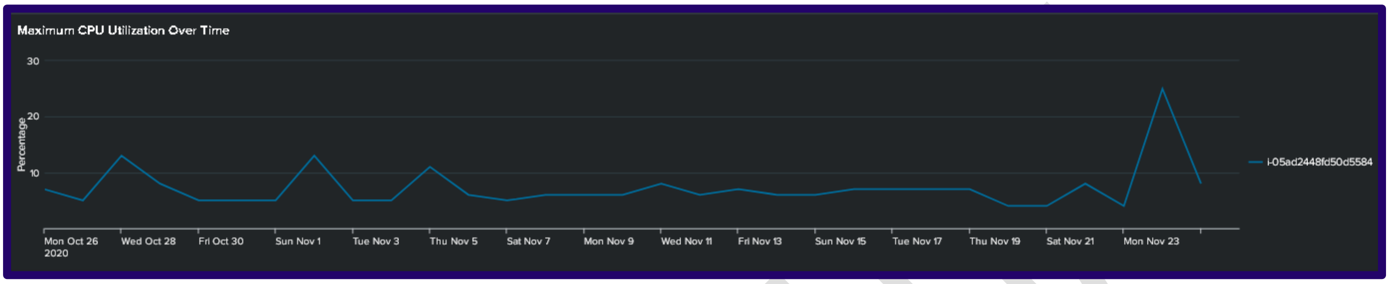
3.3 Admin-panel-instance

Instance Under monitoring	IP Address	CPU Utilization
Admin-panel-instance	10.0.5.174	99% to 42%



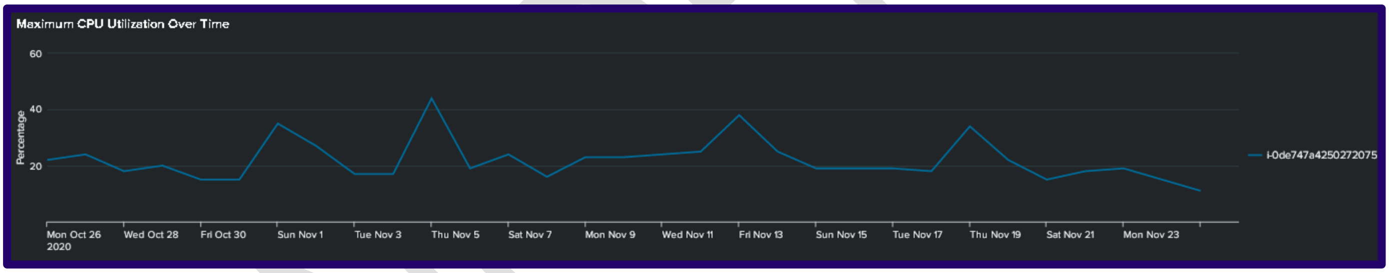
3.4 MFI-production-02

Instance Under monitoring	IP Address	CPU Utilization
MFI-production-02	10.0.5.185	7% to 8%



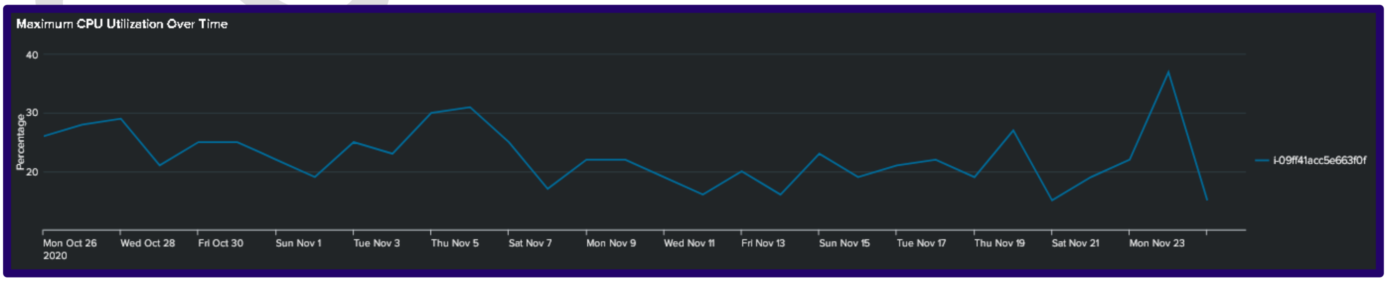
3.5 Check-Point-Gateway-Auto Scaling -ALL Branch

Instance Under monitoring	IP Address	CPU Utilization
Check-Point-Gateway-AutoScaling-ALL Branch	13.233.156.6	22% to 11%



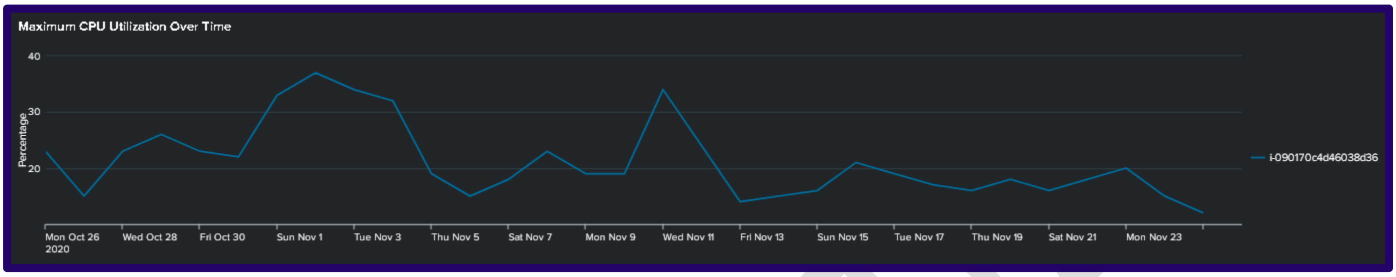
3.6 Check-Point-Gateway-Auto Scaling- ALL Branch

Instance Under monitoring	IP Address	CPU Utilization
Check-Point-Gateway-AutoScaling- ALL Branch	13.127.214.112	1% to 20%



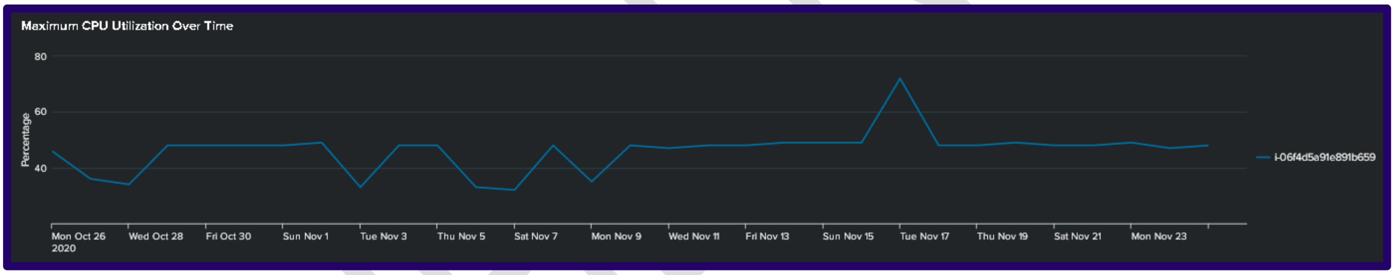
3.7 Check-Point-GATEWAY-VPN – ALL Branch

Instance Under monitoring	IP Address	CPU Utilization
Check-Point-Gateway-AutoScaling- ALL Branch	15.207.186.133	23 % to 12 %



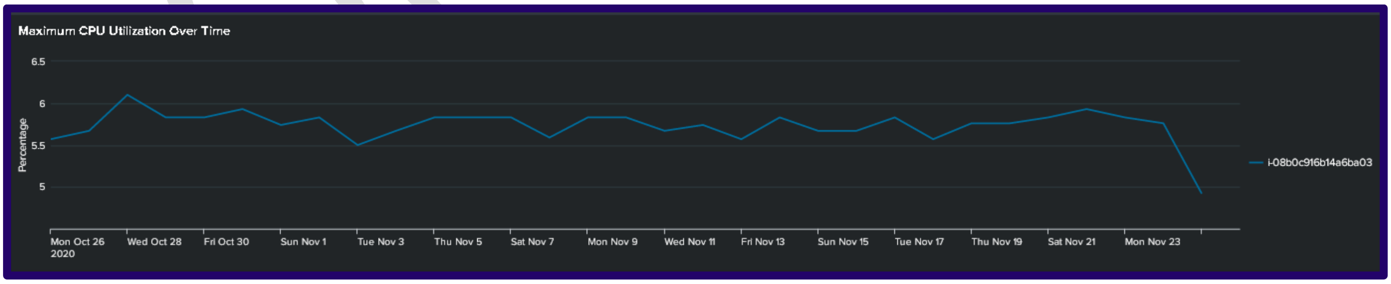
3.8 Check-point- MGMT-ALL Branch

Instance Under monitoring	IP Address	CPU Utilization
Check-Point-MGMT-ALL Branch	15.207.227.95	46 % to 48%



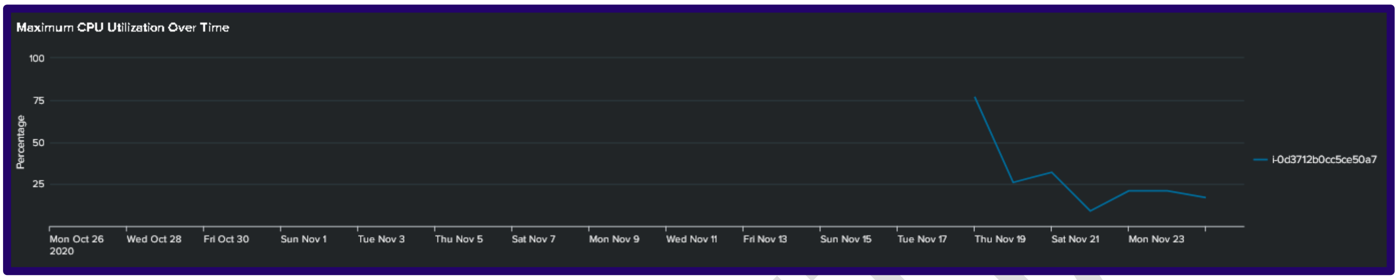
3.9 Check-point- MFA- 2FA

Instance Under monitoring	IP Address	CPU Utilization
Check-Point-MFA-2FA-Infopercept	10.0.12.251	5% to 4%



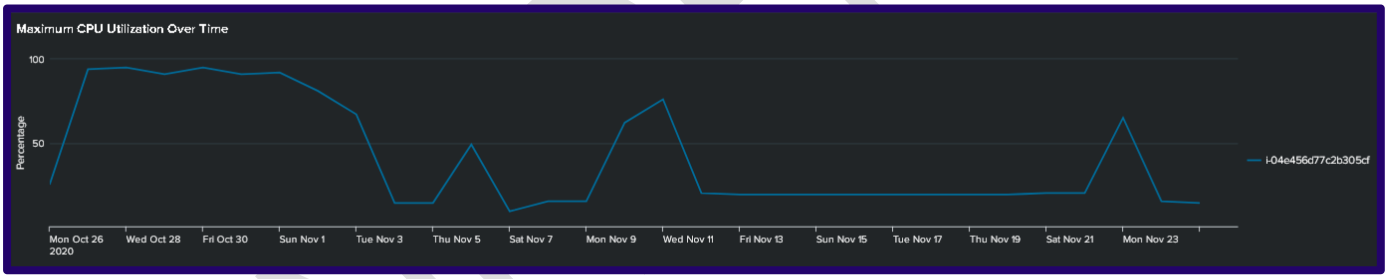
3.10 Live-ITR-Gunicorn-scraping-server-01

Instance Under monitoring	IP Address	CPU Utilization
Live-ITR-Gunicorn-Scraping-server-01	10.0.4.213	77% to 19%



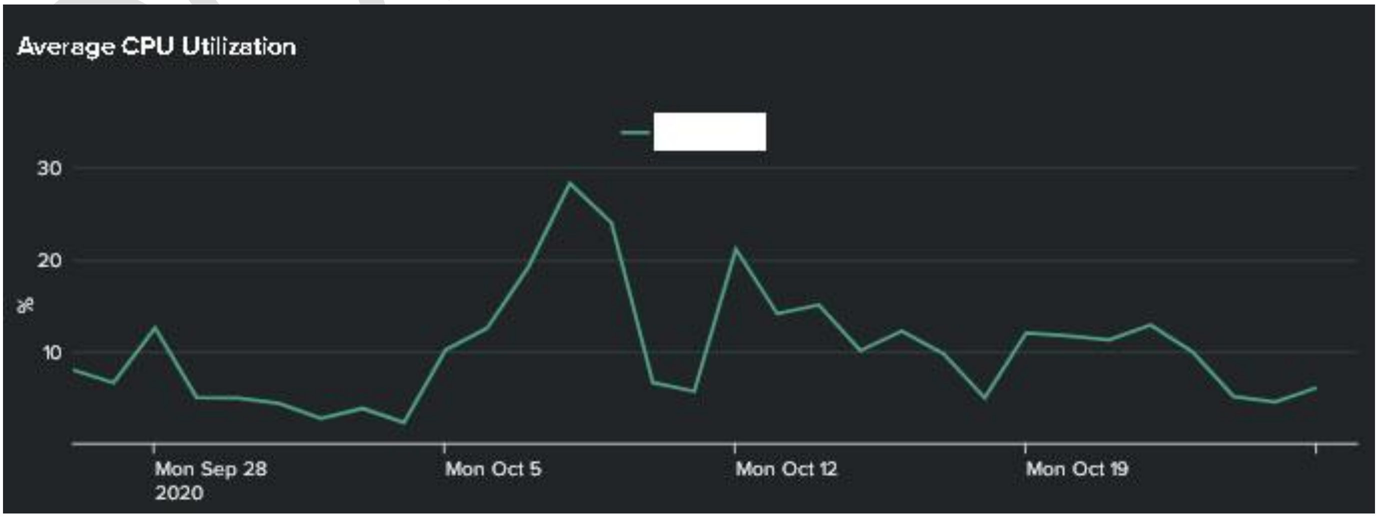
3.11 Tableau windows server 13-04-2020

Instance Under monitoring	IP Address	CPU Utilization
Tableau windows server 13-04-2020	13.232.88.24	25% to 14%

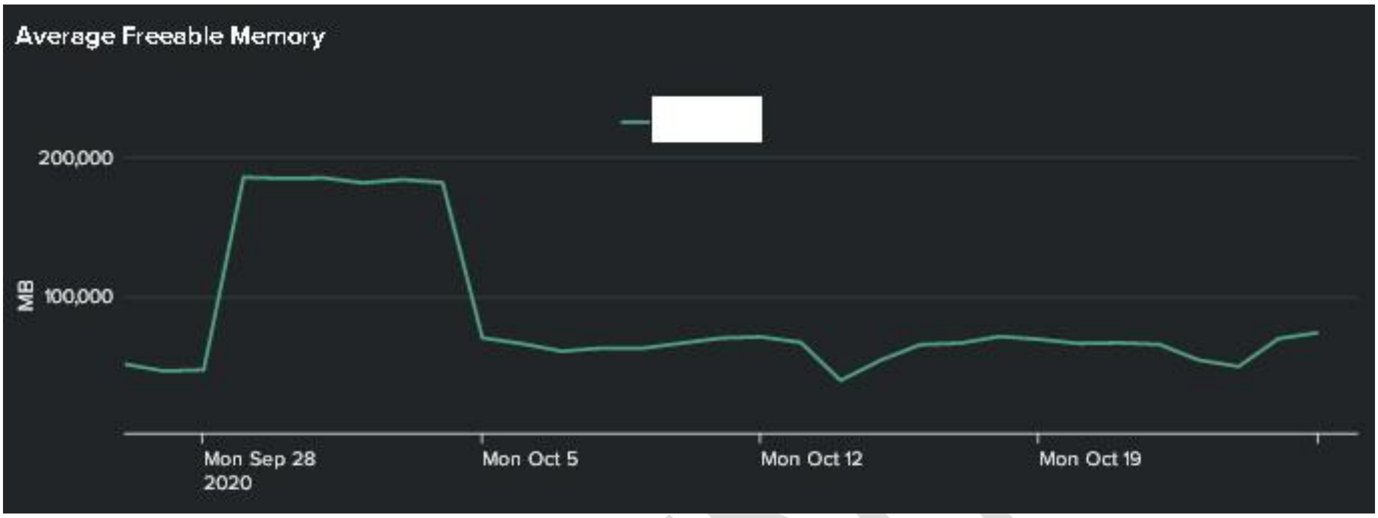


3.12 PROD-xyz-RDS

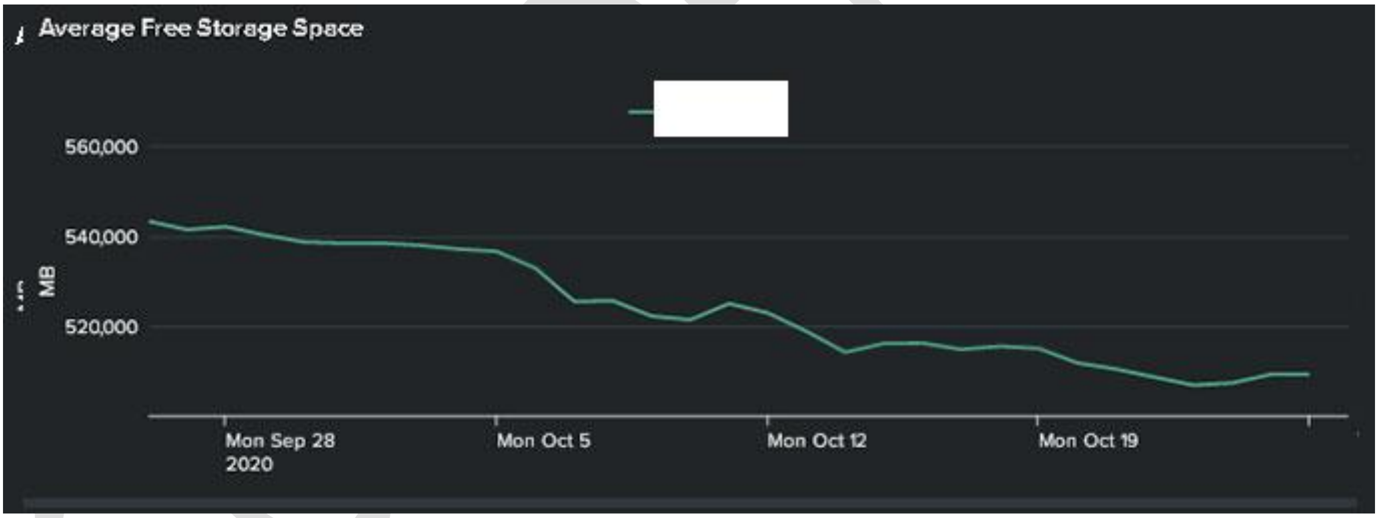
Instance Under monitoring	CPU Utilization
PROD-xyz-RDS	7% to 6%



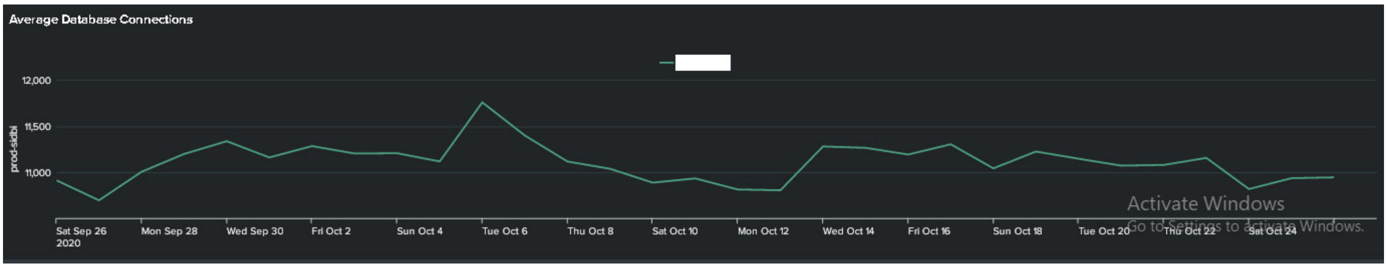
Instance Under monitoring	Memory Utilization
xxy-xyz-xxz	50 GB to 72 GB



Instance Under monitoring	Free Storage
xxy-xyz-xxz	543 GB to 509 GB

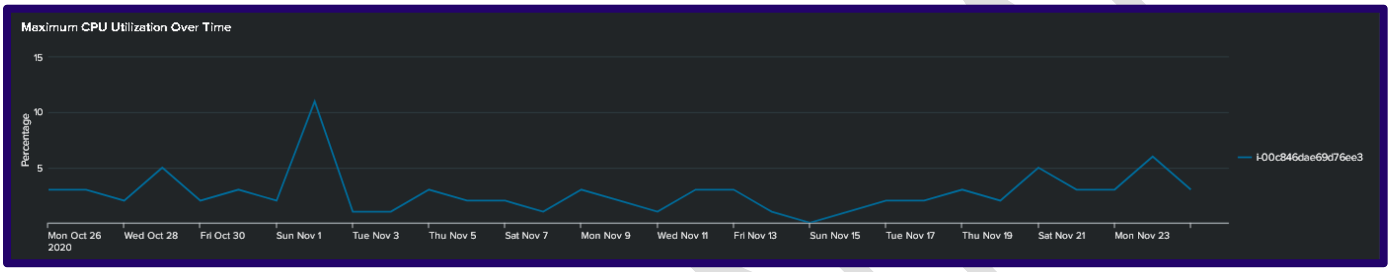


Instance Under monitoring	Database Connections
xxy-xyz-xxz	10912 to 10944



3.13 Nginx-LB-Enterprise-Redhat-Production-xyz-xxy-xxz-yyz-zzx-xxz-1

Instance Under monitoring	IP Address	CPU Utilization
Nginx-LB-Enterprise-Redhat-Production-xyz-xxy-xxz-yyz-zzx-xxz-1	10.0.4.26	3% to 3%



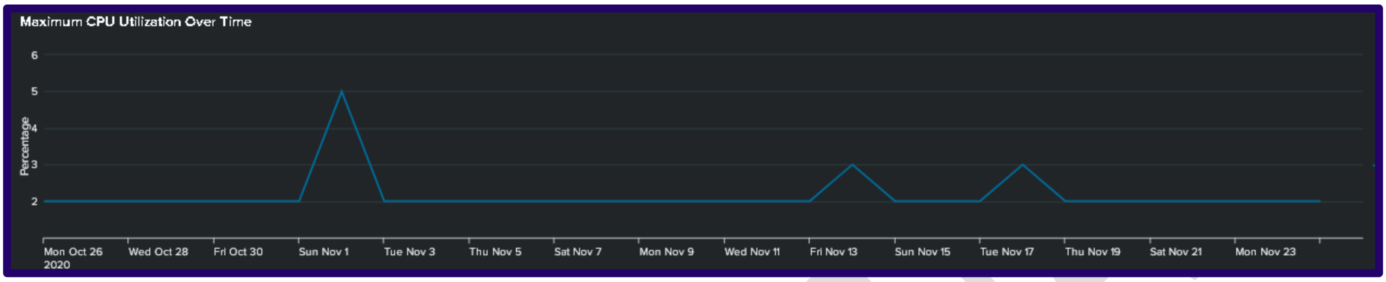
3.14 Nginx-LB-Enterprise-Redhat-Production-xyz-xxy-xxz-yyz-zzx-xxz-2

Instance Under monitoring	IP Address	CPU Utilization
Nginx-LB-Enterprise-Redhat-Production-xyz-xxy-xxz-yyz-zzx-xxz-2	10.0.5.92	2% to 2%

4. Host Monitoring: Sub Production Servers

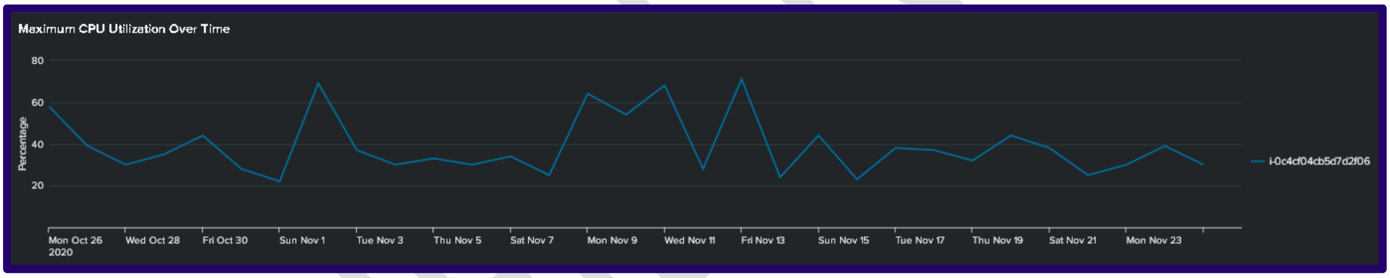
4.1 Splunk deployer

Instance Under monitoring	IP Address	CPU Utilization
Splunk Deployer	10.0.11.67	2% to 2%



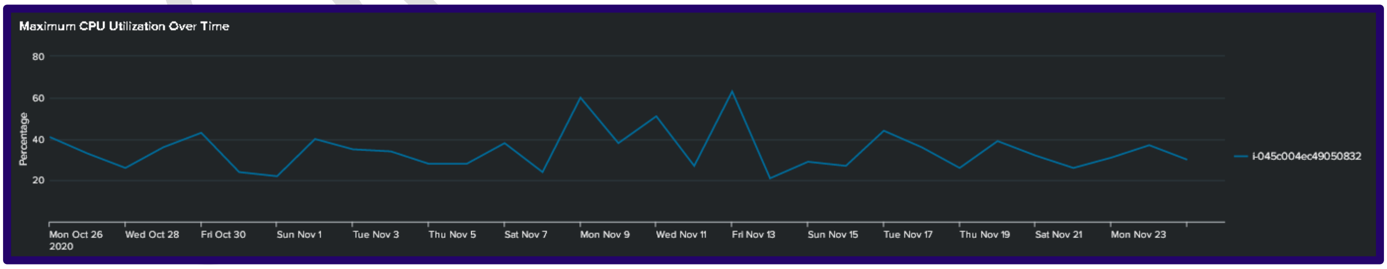
4.2 Splunk Indexer 1

Instance Under monitoring	IP Address	CPU Utilization
Splunk Indexer 1	10.0.9.5	58% to 30%



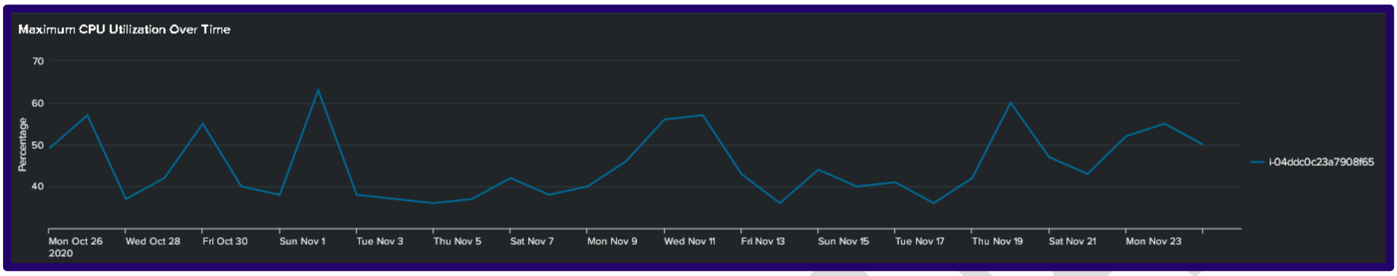
4.3 Splunk Indexer 2

Instance Under monitoring	IP Address	CPU Utilization
Splunk Indexer 1	10.0.11.106	41% to 30%



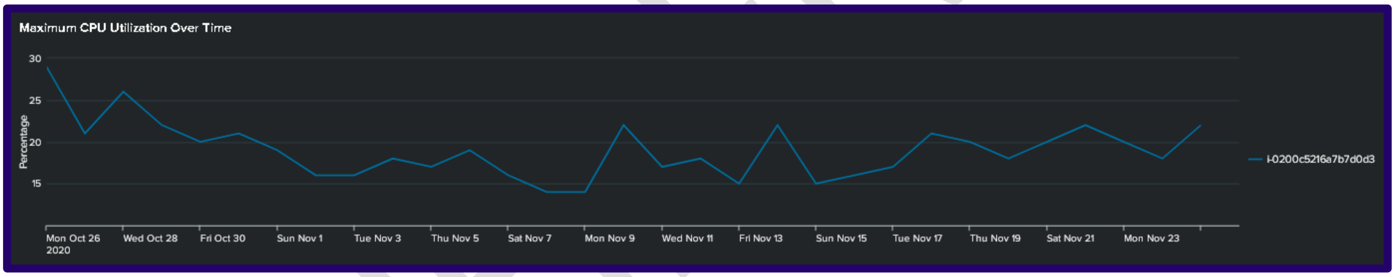
4.4 Splunk Search head 1

Instance Under monitoring	IP Address	CPU Utilization
Splunk SearchHead 1	10.0.9.131	49% to 50%



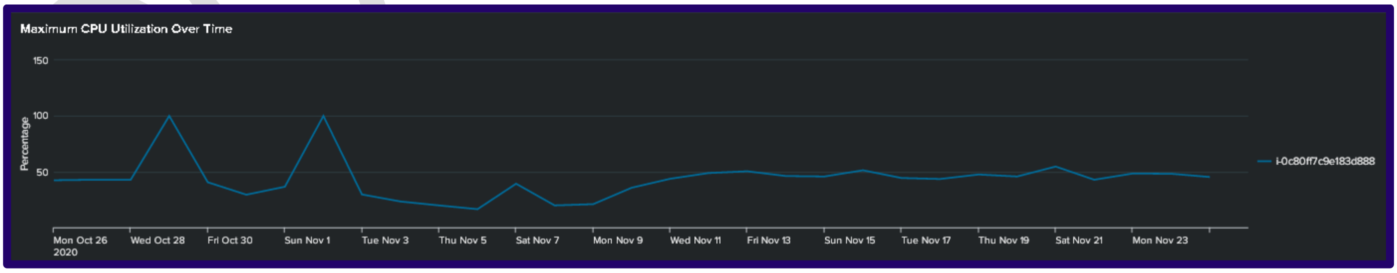
4.5 Splunk Search head 2

Instance Under monitoring	IP Address	CPU Utilization
Splunk SearchHead-2	10.0.11.97	30% to 24%



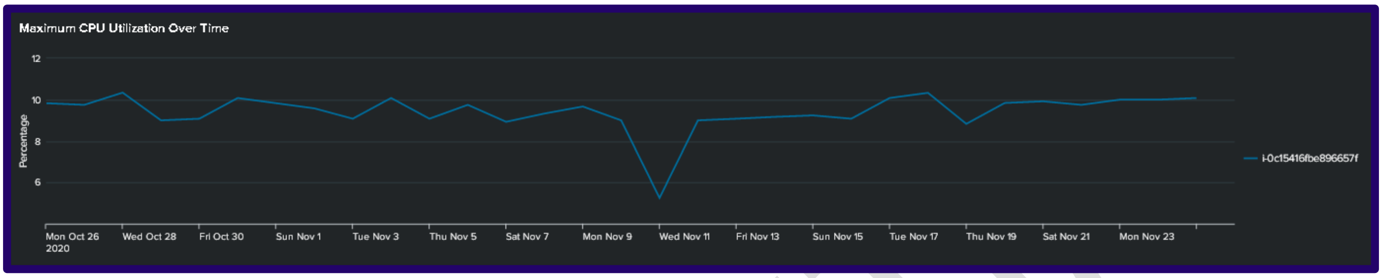
4.6 Linux-Tableau-Redhat-7-April-2019

Instance Under monitoring	IP Address	CPU Utilization
Linux-Tableau-Redhat-7-April-2019	13.233.8.41	42% to 45%



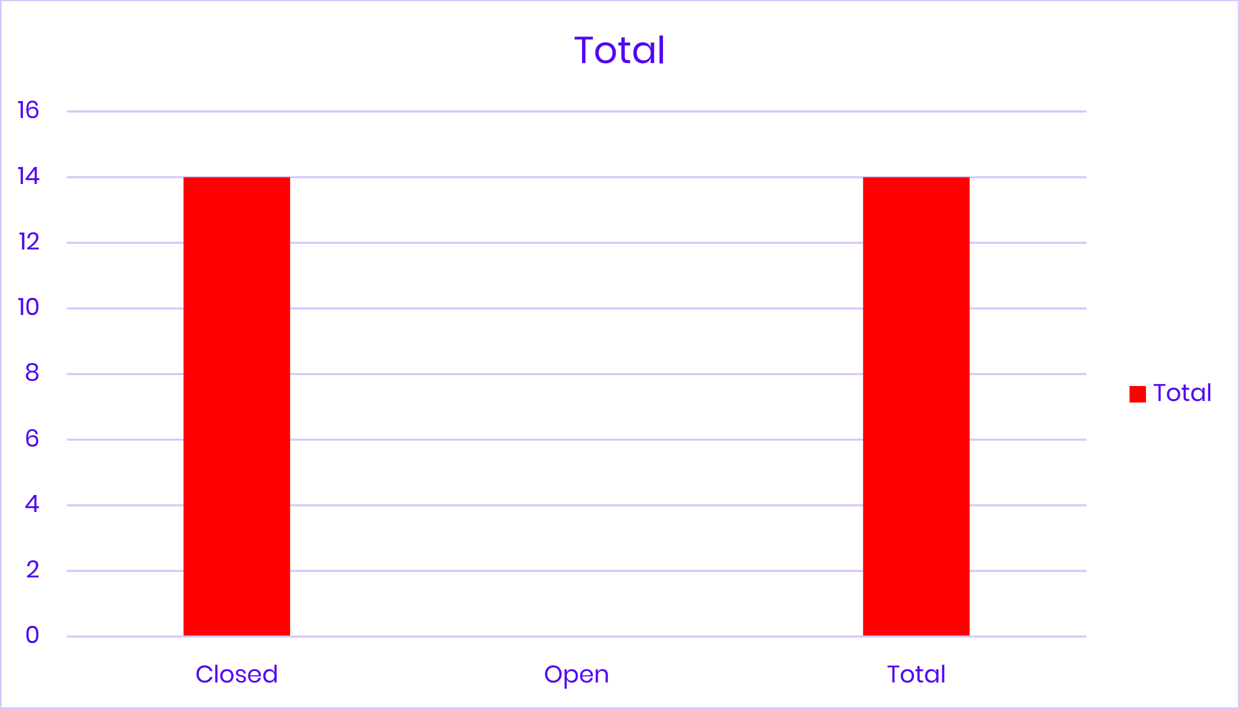
4.7 Linux-Reverse Proxy-Tableau-10-May-2019

Instance Under monitoring	IP Address	CPU Utilization
Linux-Reverse Proxy-Tableau-10-May-2019	10.0.6.242	9% to 10%



5. Incident Summary

Incident Status	Incidents Counts
Closed	14
Open	0



5.1 High-severity alert: Users targeted by phish campaigns (30-10-2020)

Incident reported on (Date):	2nd November 2020
Incident reported Number: (You Track)	CWIS-822
Ticket Summary:	High-severity alert: Users targeted by phish campaigns (30-10-2020)
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	As per analysis we have blocked 2 domains so we are closing these tickets.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	-

5.2 Change Group in Seqrite

Incident reported on (Date):	2nd November 2020
Incident reported Number: (You Track)	CWIS-826
Ticket Summary:	Change Group in Seqrite
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	As requested by Sumit we have moved CWDT044 to IT Team Policy in Seqrite..
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	-

5.3 Splunk Data Sources On-boarding

Incident reported on (Date):	2nd November 2020
Incident reported Number: (You Track)	CWIS-827
Ticket Summary:	Splunk Data Sources On-boarding
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	As per the request we have on-boarded both Nginx Server Logs (10.0.5.92,10.0.4.26) & New Production Server logs (10.0.4.252, 10.0.5.229).Also we have started fetching general/audit/error/slow-query logs from the new RDS (prod-ABC-v2).
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	-

5.4 Netextender Issue

Incident reported on (Date):	4th November 2020
Incident reported Number: (You Track)	CWIS-833
Ticket Summary:	Netextender Issue
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	As per the mail of Sumit we came to know that Ma'am and Sir password expire. so we have changed the password from SonicwaLL fIrewall.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	-

5.5 Email Address Whitelisting over Office365

Incident reported on (Date):	5th November 2020
Incident reported Number: (You Track)	CWIS-836
Ticket Summary:	Email Address Whitelisting over Office365
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	As per request from Sir we have released mail from Quarantine and allowed the user "Email" as it is Vendor of UPS.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	-

5.6 Systems not protected in morphisec

Incident reported on (Date):	10th November 2020
Incident reported Number: (You Track)	CWIS-841
Ticket Summary:	Systems not protected in morphisec
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	Today we have identified all systems are protected so we are closing these tickets.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	-

5.7 Systems not protected in morphisec

Incident reported on (Date):	12th November 2020
Incident reported Number: (You Track)	CWIS-842
Ticket Summary:	Systems not protected in morphisec
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	Today we have identified all systems are protected so we are closing these ticket.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	-

5.8 High-severity alert: Users targeted by phish campaigns (11-11-2020)

Incident reported on (Date):	12th November 2020
Incident reported Number: (You Track)	CWIS-844
Ticket Summary:	High-severity alert: Users targeted by phish campaigns (11-11-2020)
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	We have identified 4 malicious domains that were detected in Users targeted by phish campaigns of 11th November 2020 alert. Kindly block the 4 malicious domain which is as follow. weekly@uxarchive.com amadiploma@amaindia.org info@cassixcom.com vivek@eb5brics.com Activity for blocking email ID's over Office365 is been completed.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	-

5.9 Systems not protected in morphisec

Incident reported on (Date):	13th November 2020
Incident reported Number: (You Track)	CWIS-845
Ticket Summary:	Systems not protected in morphisec
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	Today we have identified all systems are protected so we are closing these ticket.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	-

5.10 Quarantine mail released

Incident reported on (Date):	13th November 2020
Incident reported Number: (You Track)	CWIS-846
Ticket Summary:	Quarantine mail released
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	We have released mail from O365: Sender address: hr@abc.com Received: 11/11/20 6:14 PM Subject: File Recipient(s): ithelpdesk@abc.com
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	-

5.11 Systems not protected in morphisec

Incident reported on (Date):	16th November 2020
Incident reported Number: (You Track)	CWIS-848
Ticket Summary:	Systems not protected in morphisec
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	Today we have identified all systems are protected so we are closing these ticket.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	-

5.12 Systems not protected in morphisec

Incident reported on (Date):	18th November 2020
Incident reported Number: (You Track)	CWIS-850
Ticket Summary:	Systems not protected in morphisec
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	Today we have identified all systems are protected so we are closing these ticket.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	-

5.13 Systems not protected in morphisec

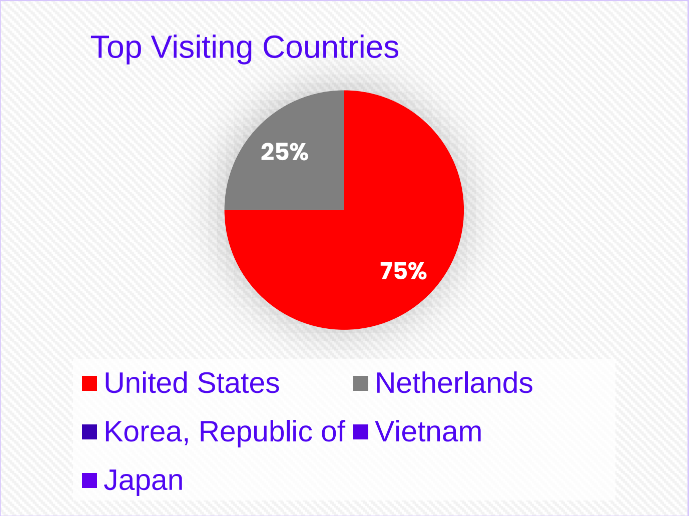
Incident reported on (Date):	20th November 2020
Incident reported Number: (You Track)	CWIS-854
Ticket Summary:	Systems not protected in morphisec
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	The same system is been not protected by morphisec its been raised in another ticket no 856. so closing this ticket.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	-

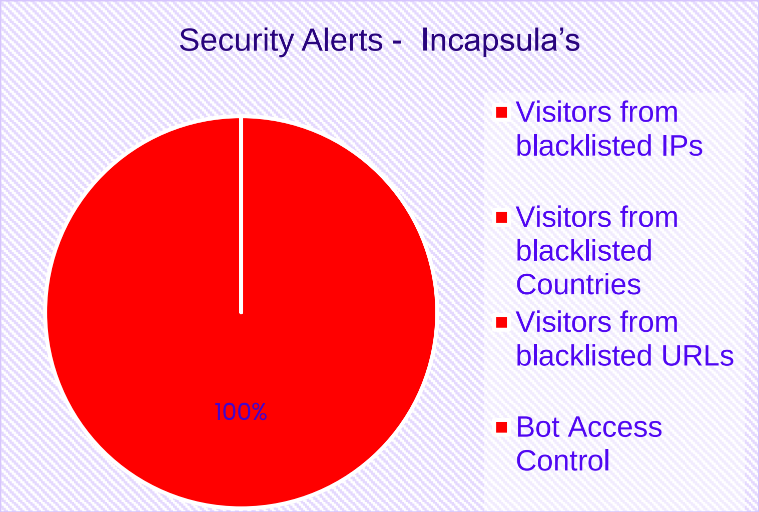
5.14 Systems not protected in morphisec

Incident reported on (Date):	23rd November 2020
Incident reported Number: (You Track)	CWIS-856
Ticket Summary:	Systems not protected in morphisec
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	Today we have identified all systems are protected so we are closing these ticket.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	-

6. Network Monitoring

6.1 Top Visiting Countries & Security Alerts





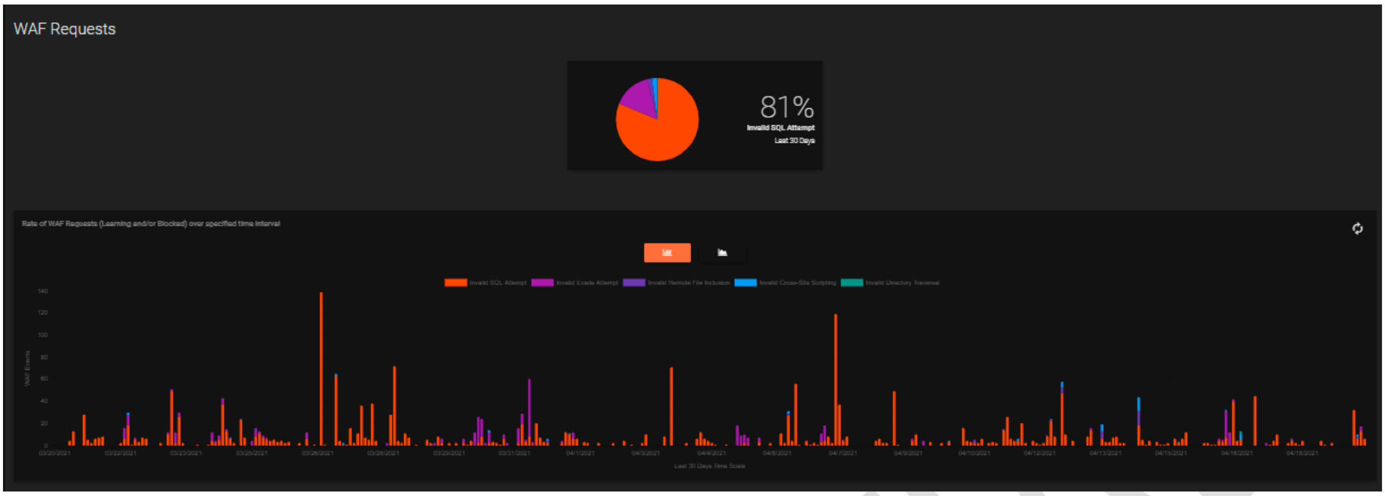
6.2. LOCAL INFRA – ABC & XYZ Office – SonicWALL

No.	Location	Firewall Issues	Completed	Pending
1	ABC Office	22	22	0
2	Mumbai Office	16	0	16

6.3 Filter Rule List Does Not End with Drop All and Log

Risk	Filter Rule List Does Not End With Drop All And Log
Location	Mumbai only
Date	28/09/2020
Severity	Informational
Issue Description	It is common for an attacker to perform network reconnaissance in order to identify potential target hosts and services. An attacker's reconnaissance phase can vary greatly in intensity and covertness, but any network scans which do not match the configured filter rules will not be logged.
Recommendations	Infopercept Consulting Private Limited recommends that a drop all and log filter rule should be configured as the final rule in a filter rule list.
ABC Comments	
ABC Stakeholder / POC	SOC Team
Target timeline for closure	
You Track Ticket Details	
Status	Pending
Remarks	

6.4 Total WAF Request Overview

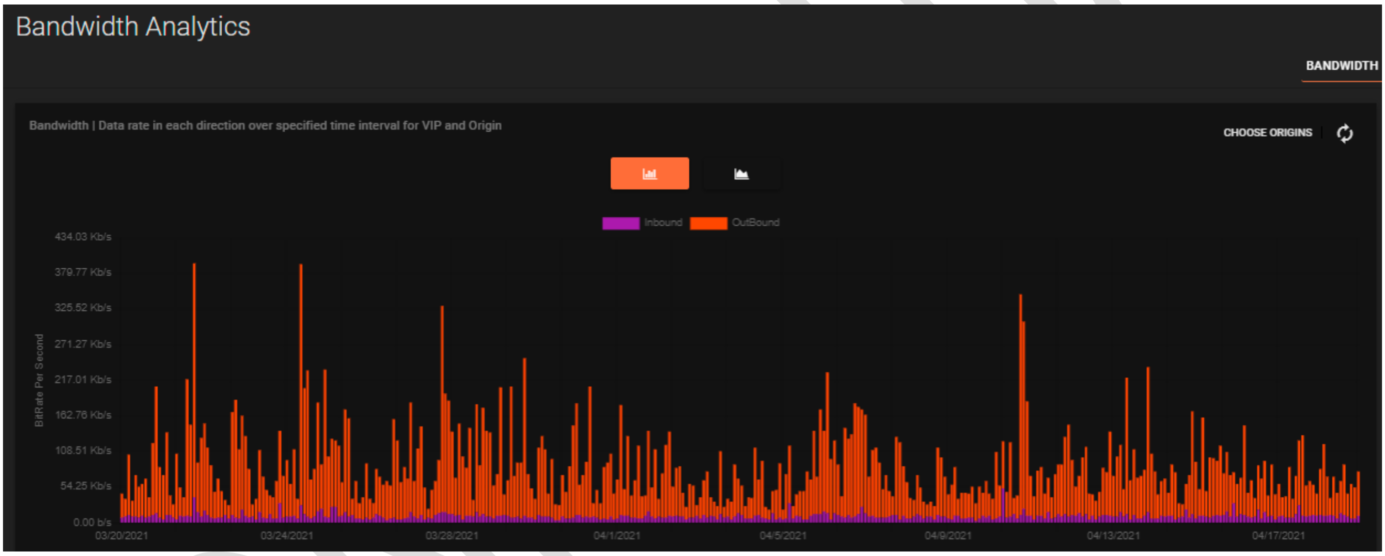


WAF Requests

81%
Invalid SQL Attempt
Last 30 Days

Rate of WAF Requests (Learning and/or Blocked) over specified time interval

6.5 WAF Bandwidth Analytics Overview



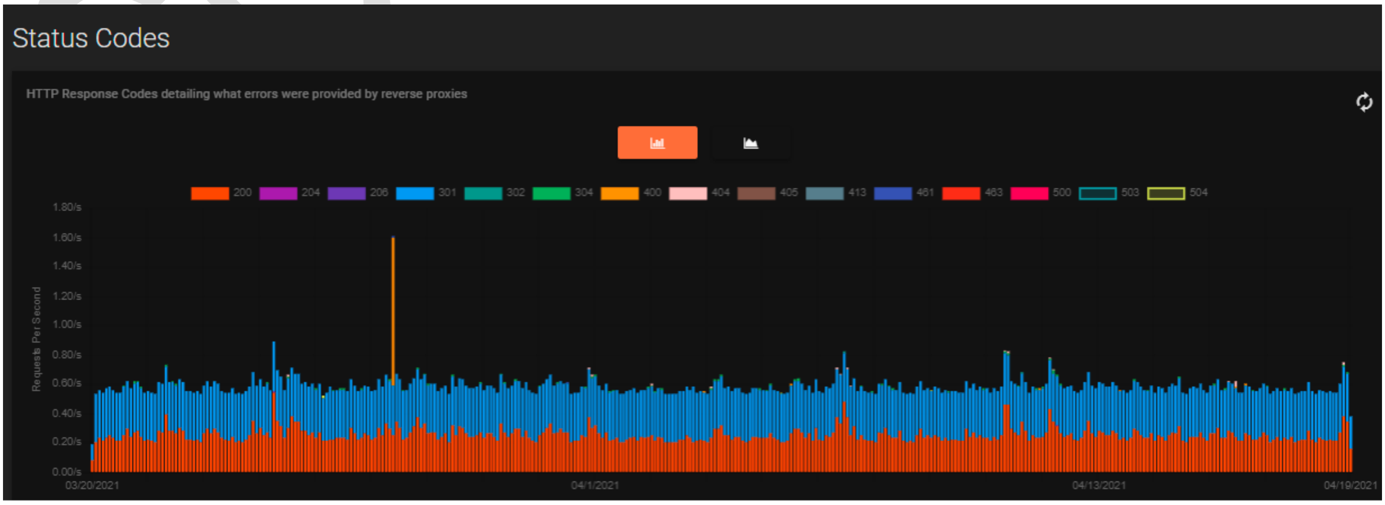
Bandwidth Analytics

BANDWIDTH

Bandwidth | Data rate in each direction over specified time interval for VIP and Origin

CHOOSE ORIGINS

6.6 HTTP Status Code Analysis



Status Codes

HTTP Response Codes detailing what errors were provided by reverse proxies

6. LOCAL INFRA – Bombay Office – SonicWALL

6.3.1 Filter Rules Allow Packets from Any Source to Network Destinations and Any Port

Risk	Filter Rules Allow Packets From Any Source To Network Destinations And Any Port
Date	28/09/2020
Severity	High
Issue Description	If network filtering rules are not configured to restrict access to network services from only those hosts that require the access then unauthorized access may be gained to those services covered in this issue finding. For a network edge device, this could lead to a remote attacker gaining access to network service. For an internal device this could lead a malicious user gaining unauthorized access to a service.
Recommendations	Infopercept Consulting Private Limited recommends that, where possible, all network filtering rules should be configured to restrict access to network services from only those hosts that require the access. However, it is worth noting that it may not be possible to achieve this in all circumstances, such as with a public web server where business requirements imply that any network address should be permitted to access the service.
ABC Comments	
ABC Stakeholder / POC	SOC Team
Target timeline for closure	
You Track Ticket Details	
Status	Pending
Remarks	

6.3.2 Filter Rule Allows Packets from Any Source

Risk	Filter Rule Allows Packets From Any Source
Date	28/09/2020
Severity	Low
Issue Description	If network filtering rules are not configured to restrict access to network services from only those hosts that require the access then unauthorized access may be gained to those services covered in this issue finding. For a network edge device, this could lead to a remote attacker gaining access to network service. For an internal device this could lead a malicious user gaining unauthorized access to a service.
Recommendations	Infopercept Consulting Private Limited recommends that, where possible, all network filtering rules should be configured to restrict access to network services from only those hosts that require the access. However, it is worth noting that it may not be possible to achieve this in all circumstances, such as with a public web server where business requirements imply that any network address should be permitted to access the service.
ABC Comments	
ABC Stakeholder / POC	SOC Team
Target timeline for closure	
You Track Ticket Details	
Status	Pending
Remarks	

6.4 LOCAL INFRA – Office 365 Email Policy Users

- Users mention in allowed list are portioned in following policies:
  - Can send email with attachment within the organization.
  - Can send email to outside organization without attachment.
  - Can send email with or without attachment to inside organization & outside the organization

6.4.1 Allowed users

Allowed	
Finance	xxx
Accounts	xxx
HR	
IT Helpdesk	

6.4.2 Not Allowed User

Not Allowed ○ Can send email with attachment within the organization. ○ Can send email to outside organization without attachment. ○ Cannot send email with attachment outside the organization (Only attachment 20 kb is allowed due to signature image).		
Finance	xxx	
Accounts	xxx	
HR		
IT Helpdesk		

6.4.3 LOCAL INFRA – Office 365 Incident Report

Security Incident- Detailed Analysis Report	
Incident reported on (Date):	15th October 2020
Reference	Service Health Status Incidents in Office365
Incident Reported via	Office365 Health Check Status
Incident reported Number:	(ID# INC-020151020)
Systems Affected:	Office365 Users
Severity: (High/Medium/Low)	High
Result upon Investigation	True positive
Damages due to incident:	Some users may be unable to send email messages
Action to be taken	If mails not getting sent inform SOC Team (securitymonitoring@abccorporation.com) or Ithelpdesk xxx
Issue Action to be taken end user:	If users not able to send mails than user would receive NDR (Non Delivery Report) so kindly forward mails to (securitymonitoring@abccorporation.com)
Root cause of incident:	A recent service update inadvertently caused an issue where sent emails are being miscounted, resulting in users being unable to send email messages.
Summary of Incident logs, alerts etc.... (Yes/No and details)	Yes
Recommended mitigation (Corrective action) steps:	Need to contact support agent for assistance, and they'll work to increase sending limits to resolve impact. Additionally, they are working to develop a fix for the issue. They will provide an update on its progress and deployment timeline when available.
Recommended Preventive activities to be carried out	Need to increase sending limits to resolve impact with help of Support Team

6.5 Local infra – active directory

6.5.1 Disabled Users

S.No	Display Name	SAM Account Name	When Created	Account Status	Account Expiry Time
1.	-	Xyz	2020/01/27 12:09	Disabled	Never Expires
2.	-	Xyz1234	2020/01/27 13:18	Disabled	Never Expires

6.5.2 Inactive Workstations (OS – Windows 10)

Due to work from home scenario many users are showing as inactive status.

S.No	Computer Name	DNS Name	Last Logon Time
1	CWDT001	CWDT001.corp.abc.com	21-3-20 18:55
2	CWDT002	CWDT002.corp. abc.com	15-9-20 18:59
3	CWDT0026	CWDT0026.corp. abc.com	15-9-20 18:01
4	CWDT012	CWDT012.corp. abc.com	10-9-20 14:15
5	CWDT014	CWDT014.corp. abc.com	15-7-20 16:33
6	CWDT017	CWDT017.corp. abc.com	21-3-20 14:40
7	CWDT019	CWDT019.corp. abc.com	20-3-20 20:48
8	CWDT024	CWDT024.corp. abc.com	5-9-20 18:52
9	CWDT027	CWDT027.corp. abc.com	27-8-20 11:11
10	CWDT028	CWDT028.corp. abc.com	20-3-20 18:10
11	CWDT031	CWDT031.corp. abc.com	21-8-20 14:00
12	CWDT034	CWDT034.corp. abc.com	11-9-20 19:42
13	CWDT038	CWDT038.corp. abc.com	23-3-20 22:19
14	CWDT040	CWDT040.corp. abc.com	23-3-20 09:38
15	CWDT045	CWDT045.corp. abc.com	23-3-20 09:18
16	CWDT055	CWDT055.corp. abc.com	27-8-20 19:36
17	CWDT063	CWDT063.corp. abc.com	23-3-20 10:37
18	CWDT084	CWDT084.corp. abc.com	20-3-20 16:10
19	CWDT085	CWDT085.corp. abc.com	20-3-20 16:29
20	CWDT090	CWDT090.corp. abc.com	23-3-20 10:24
21	CWDT092	CWDT092.corp. abc.com	23-3-20 10:04
22	CWDT104	CWDT104.corp. abc.com	21-3-20 19:05
23	CWDT105	CWDT105.corp. abc.com	20-3-20 15:36
24	CWDT106	CWDT106.corp. abc.com	23-3-20 10:49
25	CWDT107	CWDT107.corp. abc.com	11-2-20 20:00
26	CWDT111	CWDT111.corp. abc.com	20-3-20 16:22
27	CWDT112	CWDT112.corp. abc.com	22-9-20 23:06
28	CWDT113	CWDT113.corp. abc.com	22-5-20 23:19
29	CWDT114	CWDT114.corp. abc.com	20-3-20 15:40
30	CWDT115	CWDT115.corp. abc.com	23-3-20 12:05

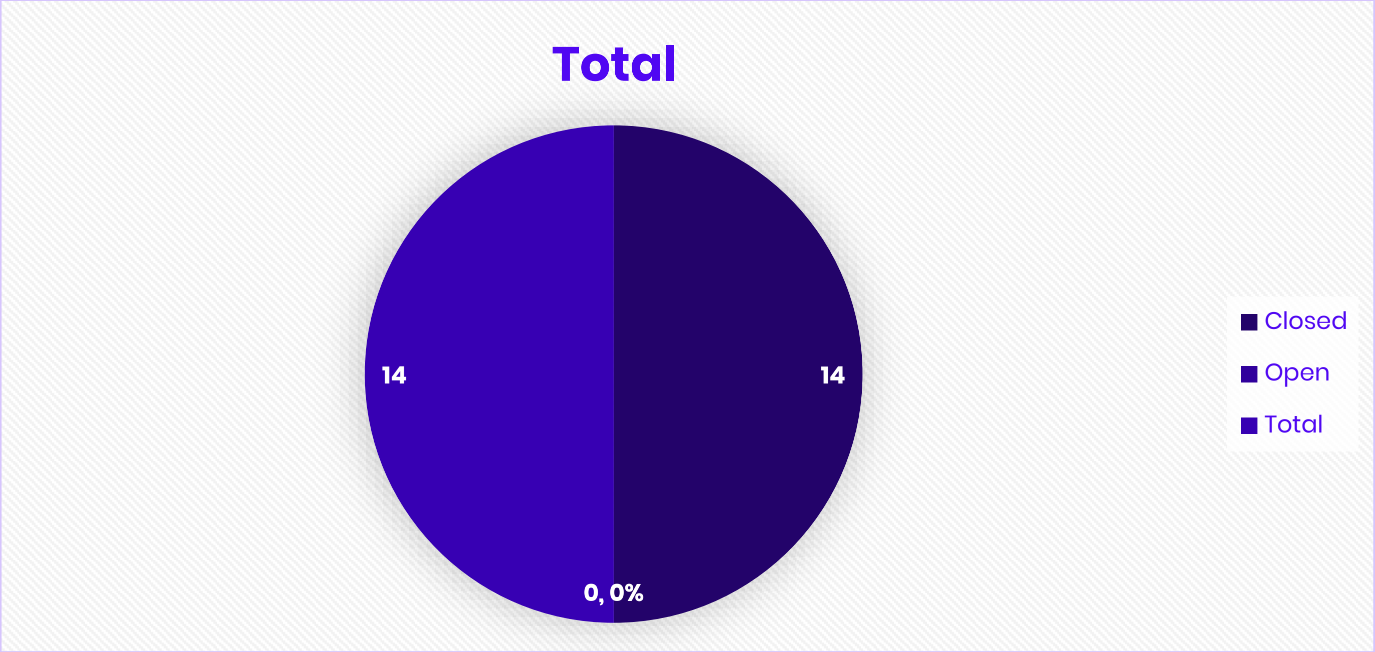
S.No	Computer Name	DNS Name	Last Logon Time
31	CWDT119	CWDT119.corp. abc.com	1-4-20 18:13
32	CWDT121	CWDT121.corp. abc.com	1-5-20 16:52
33	CWDT122	CWDT122.corp. abc.com	23-3-20 10:41
34	CWDT123	CWDT123.corp. abc.com	23-3-20 13:49
35	CWDT124	CWDT124.corp. abc.com	29-8-20 12:37
36	CWLT004	CWLT004.corp. abc.com	23-3-20 14:39
37	CWLT005	CWLT005.corp. abc.com	29-8-20 18:10
38	CWLT012	CWLT012.corp. abc.com	20-3-20 18:42
39	CWLT015	CWLT015.corp. abc.com	17-3-20 18:03
40	CWLT037	CWLT037.corp. abc.com	11-3-20 17:09
41	CWLT039	CWLT039.corp. abc.com	4-7-20 14:34
42	CWLT040	CWLT040.corp. abc.com	28-2-20 19:48
43	CWLT043	CWLT043.corp. abc.com	11-3-20 22:16
44	CWLT045	CWLT045.corp. abc.com	29-9-20 18:19
45	CWLT050	CWLT050.corp. abc.com	4-5-20 19:20
46	CWLT057	CWLT057.corp. abc.com	8-7-20 15:50
47	CWLT058	CWLT058.corp. abc.com	2-10-20 12:56
48	CWLT36	CWLT36.corp. abc.com	16-3-20 09:23
49	SERVER	SERVER.corp. abc.com	27-9-20 17:13

6.5.3 Soon to expire User Password Next 30 days

S.No	Display Name	SAM Account Name	Password Last Set	Password Expiry Date
1	-	krbtgt	27-1-20 00:13	9-3-20 00:13
2	John Doe	Abc	15-2-20 17:22	28-3-20 17:22
3	John Doe	Abc	20-3-20 15:42	1-5-20 15:42
4	John Doe	Abc	9-3-20 10:26	20-4-20 10:26
5	John Doe	Abc	8-7-20 10:55	19-8-20 10:55
6	John Doe	Abc	8-7-20 14:06	19-8-20 14:06
7	John Doe	Abc	21-8-20 13:05	2-10-20 13:05
8	John Doe	Abc	3-9-20 14:27	15-10-20 14:27
9	John Doe	Abc	27-1-20 00:13	9-3-20 00:13
10	John Doe	Abc	15-2-20 17:22	28-3-20 17:22
11	John Doe	Abc	28-2-20 17:38	10-4-20 17:38
12	John Doe	Abc	29-8-20 11:54	10-10-20 11:54
13	John Doe	Abc	27-1-20 09:15	9-3-20 09:15
14	John Doe	Abc	23-3-20 10:01	4-5-20 10:01
15	John Doe	Abc	20-3-20 17:32	1-5-20 17:32
16	John Doe	Abc	23-3-20 10:17	4-5-20 10:17
17	John Doe	Abc	1-8-20 11:01	12-9-20 11:01
18	John Doe	Abc	21-2-20 11:12	3-4-20 11:12
19	John Doe	Abc	23-3-20 10:08	4-5-20 10:08
20	John Doe	Abc	23-3-20 10:11	4-5-20 10:11

7. Change Management Observations

Incident Status	Incidents Counts
Closed	22
Open	2
Total	24



7.1 New Server and Services Onboarding for V2 Launch

Incident reported on (Date):	2nd November 2020
Incident reported Number: (You Track)	CWIS-825
Ticket Summary:	New Server and Services Onboarding for V2 Launch
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	We have on boarded new services over New Relic so we are closing these ticket.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	Signature:

7.2 Imperva Site Add

Incident reported on (Date):	2nd November 2020
Incident reported Number: (You Track)	CWIS-828
Ticket Summary:	Imperva Site Add
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	We have onboarded the abc.com URL again over Imperva and Security Rules has been applied accordingly
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	Signature:

7.3 Lifecycle Policy for New Server

Incident reported on (Date):	3rd November 2020
Incident reported Number: (You Track)	CWIS-830
Ticket Summary:	Lifecycle Policy for New Server
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	As per mail from Sir we have configure the lifecycle policy of new production server /apps parition.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	Signature:

7.4 Spoofing of XYZ Sir ID

Incident reported on (Date):	9th November 2020
Incident reported Number: (You Track)	CWIS-838
Ticket Summary:	Spoofing of XYZ Sir ID
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	An attacker performed a spoofing attack on and using ID: john@abc.com After the investigating Office365 Sign-in activities and analysis of email we found no indicators of account compromised and found the email was spoofed. The detailed Log Analysis and summary is sent to Sir on email. For security reason we have reset password of ID: john@abc.com in Office365 and new password shared to Sir on Email.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	Signature:

7.5 Seqrite Virus Detected (mbrowser1.log)

Incident reported on (Date):	12th November 2020
Incident reported Number: (You Track)	CWIS-843
Ticket Summary:	Seqrite Virus Detected (mbrowser1.log)
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	Detail log analysis has been done on the incident and the corresponding incident report and detailed log analysis report is also been attached with the ticket.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	Signature:

7.6 Error Observed in Cloudwatch Alarms

Incident reported on (Date):	13th November 2020
Incident reported Number: (You Track)	CWIS-847
Ticket Summary:	Error Observed in Cloudwatch Alarms
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	We have observed error on cloudwatch graph while alarm trigger. So we contacted AWS team and they are working on this. Task has been completed so we are closing this ticket.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	Signature:

7.7 Incident Report - INC18112020 (YYZ IP Getting Blocked)

Incident reported on (Date):	18th November 2020
Incident reported Number: (You Track)	CWIS-853
Ticket Summary:	Incident Report - INC18112020 (YYZ IP Getting Blocked)
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	We have found IP Address of YYZ Bank getting blocked over Anti-Scrapper Policy in Imperva. (Rule Definition: Number of Sessions >=40). As approved by sir we have whitelisted the IP Address (103.68.221.92) of YYZ over Anti-Scrapper Policy.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	Signature:

7.8 Open US Region over Imperva

Incident reported on (Date):	18th November 2020
Incident reported Number: (You Track)	CWIS-857
Ticket Summary:	Open US Region over Imperva
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	As requested by Sir we have Disabled the US Region over Imperva (abc.com).
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	Signature:

7.9 Live-ITR-Gunicorn-scraping-server-02 was not able to access

Incident reported on (Date):	20th November 2020
Incident reported Number: (You Track)	CWIS-860
Ticket Summary:	Live-ITR-Gunicorn-scraping-server-02 was not able to access
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	As of now error was resolved so we are closing these ticket.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	Signature:

7.10 MFA DIsable for Satyam.khatri and VPN Password reset

Incident reported on (Date):	20th November 2020
Incident reported Number: (You Track)	CWIS-861
Ticket Summary:	MFA DIsable for John and VPN Password reset
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	We have disable mfa for John and also setup new mfa for John and also reset password for vpn user john so we are closing these ticket.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	Signature:

7.11 Removed newrelic agent from ekyc service 10.0.4.90 BOB server

Incident reported on (Date):	**23rd November 2020**
Incident reported Number: (You Track)	CWIS-866
Ticket Summary:	System not protected in Morphisec
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	We have removed new relic agent from ekyc service in 10.0.4.90 BOB prod server.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	Signature:

7.12 RBI Advisory

Incident reported on (Date):	**24th November 2020**
Incident reported Number: (You Track)	CWIS-867
Ticket Summary:	RBI Advisory
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	We have blocked all the IP Addresses, URL's and Domains over Office365, Seqrite & Imperva.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	Signature:

7.13 Microsoft to do Application allow for intunes

Incident reported on (Date):	**24th November 2020**
Incident reported Number: (You Track)	CWIS-868
Ticket Summary:	Microsoft to do Application allow for intunes
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	We have allowed and assigned the Microsoft To-Do Application in Managed Play Store
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	Signature:

7.14 Morphisec Agent Installation

Incident reported on (Date):	24th November 2020
Incident reported Number: (You Track)	CWIS-869
Ticket Summary:	Morphisec Agent Installation
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	Till now we have installed 70 clients over morphisec server.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	Signature:

7.15 Sophos Anti-virus

Incident reported on (Date):	24th November 2020
Incident reported Number: (You Track)	CWIS-870
Ticket Summary:	Sophos Anti-virus
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	As there is a limitation over the product that anti-virus dont work together so we have working with the vendor resolve the same.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	Signature:

7.16 SonicWALL Mumbai Office Hardening Activity

Incident reported on (Date):	24th November 2020
Incident reported Number: (You Track)	CWIS-871
Ticket Summary:	SonicWALL Mumbai Office Hardening Activity
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	The firewall is accessible Now also we have taken the remote of the spare system from mumbai office as well.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	Signature:

7.17 Change group in Seqrite (CWLT016)

Incident reported on (Date):	**20th November 2020**
Incident reported Number: (You Track)	CWIS-862
Ticket Summary:	Change group in Seqrite (CWLT016)
Ticket Reporter:	SOC Team
Ticket Status:	Closed
Ticket Last Update:	As requested by johnand We have moved CWLT016 to IT TEAM Policy in Seqrite Antivirus.
Analysis done by:	-
Date:	Signature:
Report validated by:	-
Date:	Signature:

7.18 website unblock

Service Request on (Date):	**5th November 2020**
Service Request Number: (You Track)	CWIS-813
Service Requested By:	-
Service Request Summary:	link: https://www.streamlit.io/ https://www.hackerrank.com/
Service Request Status:	Closed
Service Request Remarks:	We have allowed the site from Seqrite.
Service Request Update By:	-

7.19 Unblock Url

Service Request on (Date):	**8th November 2020**
Service Request Number: (You Track)	CWIS-832
Service Requested By:	It helpdesk
Service Request Summary:	Please Unblock : https://app.giddh.com/magic.html?id=1604470208883qgwn7j4ko00nzor5h03z
Service Request Status:	Closed
Service Request Remarks:	We have allowed the site from Seqrite.
Service Request Update By:	-

7.20 Unable to access You Tube Links

Service Request on (Date):	**7th November 2020**
Service Request Number: (You Track)	CWIS-832
Service Requested By:	-
Service Request Summary:	I am not able to access following you tube links: https://youtu.be/S3FpCbTztrI https://youtu.be/Lledu_rTnIw These are the links for our client testimonials and I need to check for some language corrections for the website.
Service Request Status:	Closed
Service Request Remarks:	We have allowed the site from Seqrite.
Service Request Update By:	-

7.21 Website Access Required

Service Request on (Date):	**7th November 2020**
Service Request Number: (You Track)	CWIS-839
Service Requested By:	-
Service Request Summary:	https://digitalindiaawards.gov.in/ www.techcircle.in
Service Request Status:	Closed
Service Request Remarks:	We have allowed the site from Seqrite.
Service Request Update By:	-

7.22 Whitelisted URL from Seqrite

Service Request on (Date):	**9th November 2020**
Service Request Number: (You Track)	CWIS-840
Service Requested By:	SOC Team
Service Request Summary:	As per requested by Ma'am we have whitelisted below URL from Seqrite. https://freepik.cdnpk.net https://freepik
Service Request Status:	Closed
Service Request Remarks:	We have allowed the site from Seqrite.
Service Request Update By:	-

7.23 Allow to Open "https://projectlombok.org/" URL

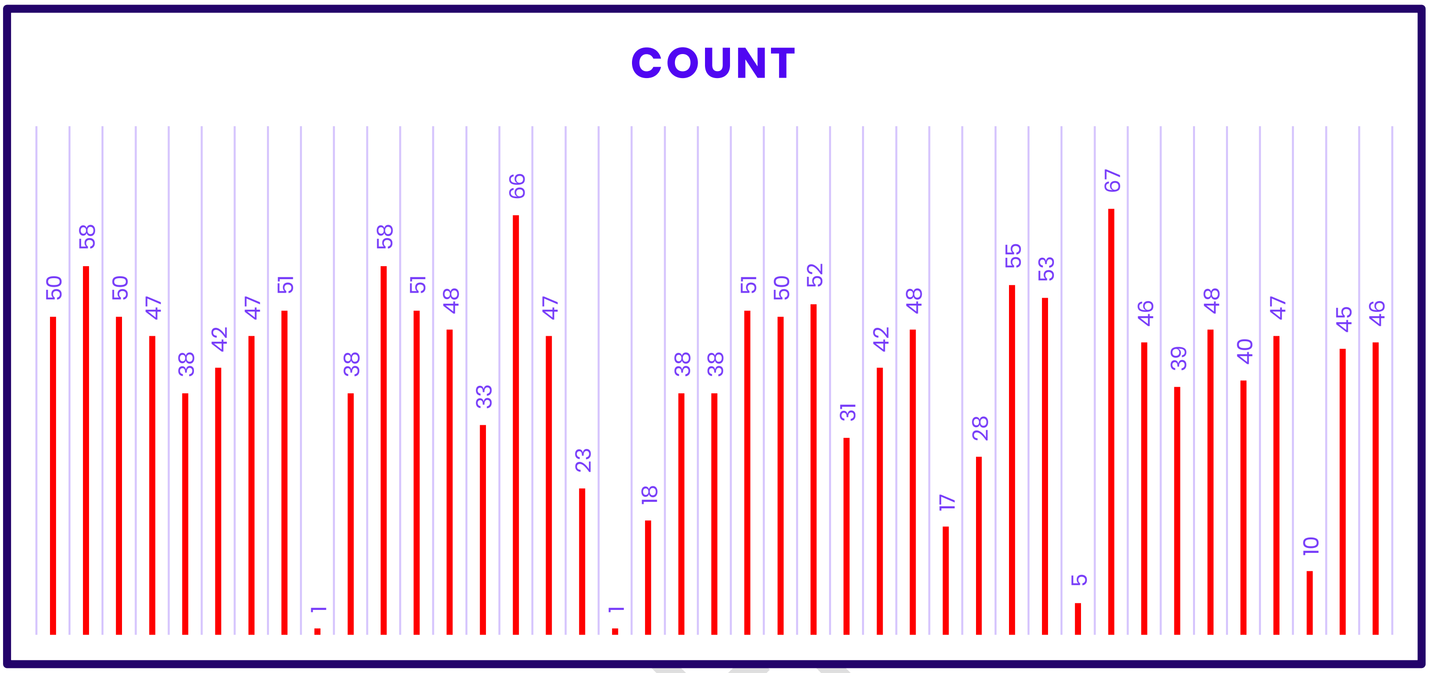
Service Request on (Date):	18th November 2020
Service Request Number: (You Track)	CWIS-851
Service Requested By:	-
Service Request Summary:	As per requested by John we have whitelisted below URL from Seqrite. https://projectlombok.org/
Service Request Status:	Closed
Service Request Remarks:	We have allowed the site from Seqrite.
Service Request Update By:	-

7.24 Access for skype for interview

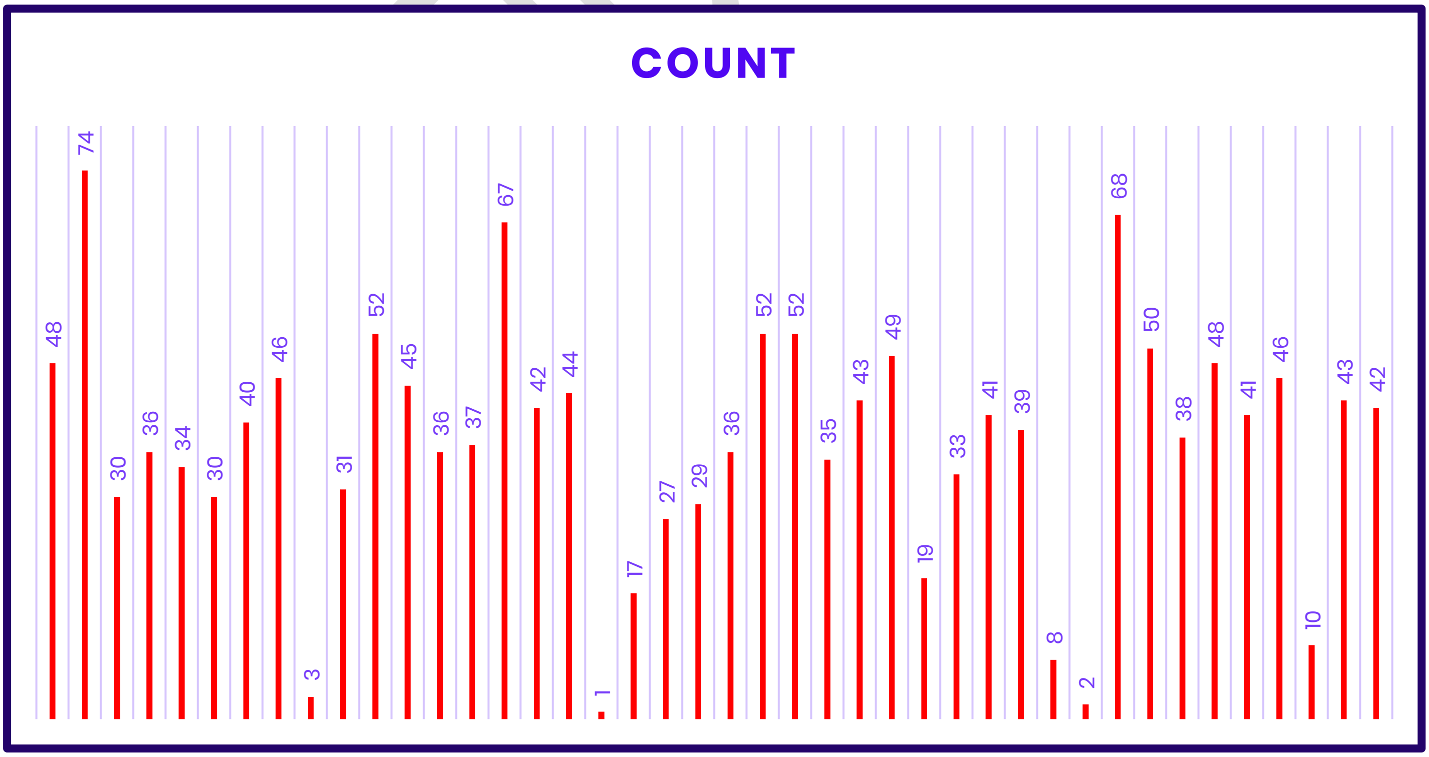
Service Request on (Date):	18th November 2020
Service Request Number: (You Track)	CWIS-852
Service Requested By:	-
Service Request Summary:	As per requested by John we have whitelisted Skype from Seqrite.
Service Request Status:	Closed
Service Request Remarks:	We have allowed the site from Seqrite.
Service Request Update By:	-

8. SIEM Splunk Dashboard

8.1 VPN User Login



8.2 Logged Out VPN Users

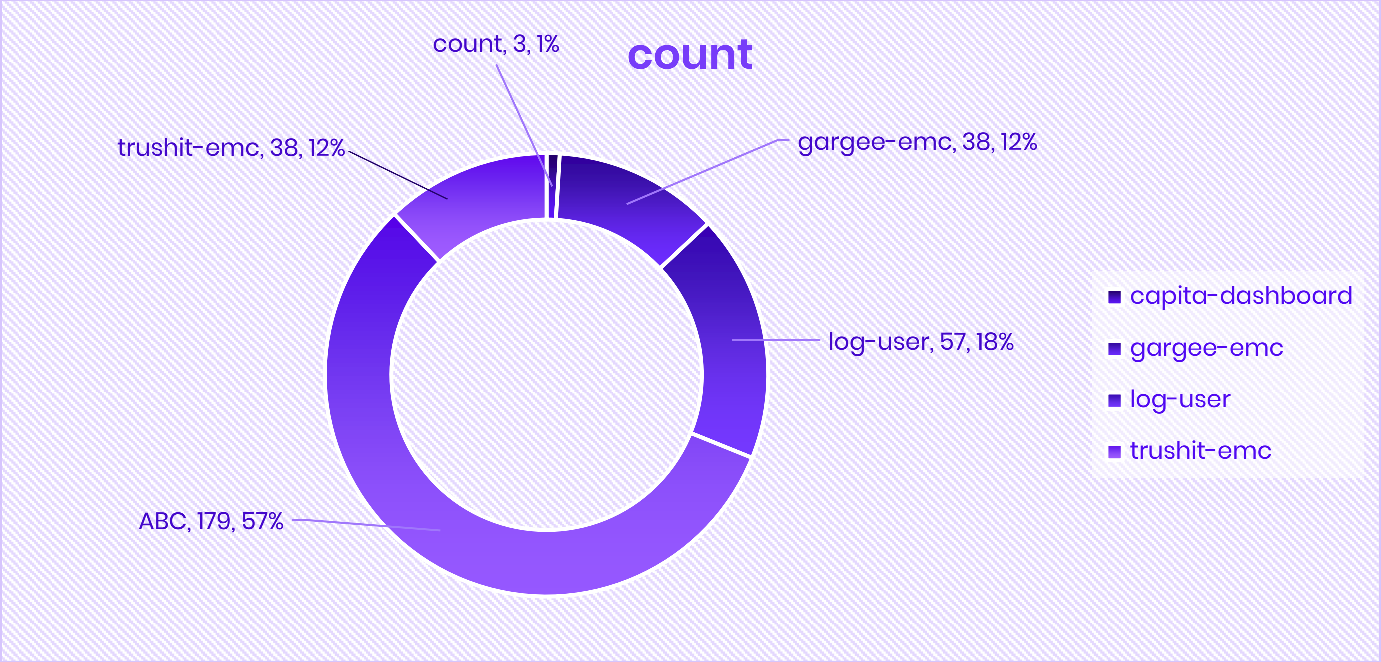


8.3 Unused Security Groups

There are security group which are unused so need to check and remove that

Account ID 0,	Region 0	ID :	VPC ID S	Insight	Severity S
652918353734	Asia Pacific (Mumbai)	sg-30le8a5b	vpc-21055349	Unused security group	⚠
652918353734	Asia Pacific (Mumbai)	sg-Ofbf78c053dOetb22	vpc-0083f5abd4f470c82	Unused security group	⚠
652918353734	Asia Pacific (Mumbai)	sg-Of9c90a86dacacb62	vpc-0083f5abd4f470c82	Unused security group	⚠
652918353734	Asia Pacific (Mumbai)	sg-0f781598abe6806f5	vpc-0c867a0fa671d39131	Unused security group	⚠
652918353734	Asia Pacific (Mumbai)	sg-016154ad050248ae	vpc-0083f5abd4f470c82	Unused security group	⚠
652918353734	Asia Pacific (Mumbai)	sg-0f35e588598b26d58	vpc-0c867a0fa671d39131	Unused security group	⚠
652918353734	Asia Pacific (Mumbai)	sg-Oefa9Idda0a8ef6ae	vpc-0083f5abd4f470c82	Unused security group	⚠
652918353734	Asia Pacific (Mumbai)	sg-0ec3430831847ce9a	vpc-0c867a0fa671d39131	Unused security group	⚠
652918353734	Asia Pacific (Mumbai)	sg-0e2fdaa8cfea6a362	vpc-0c867a0fa671d39b1	Unused security group	⚠
652918353734	Asia Pacific (Mumbai)	sg-0tl4e8eb639ea1466	vpc-0c867a0fa671d39b1	Unused security group	⚠
652918353734	Asia Pacific (Mumbai)	sg-Odcfd6081f74ac2d0	vpc-0083f5abd4f470c82	Unused security group	⚠
652918353734	Asia Pacific (Mumbai)	sg-Odbb0e5b4abb6Oleb	vpc-0083f5abd4f470c82	Unused security group	⚠
652918353734	Asia Pacific (Mumbai)	sg-0d6ca81b4c94e7341	vpc-0c867a0fa671d39b1	Unused security group	⚠
652918353734	Asia Pacific (Mumbai)	sg-Od514d9eeba869de3	vpc-0083f5abd4f470c82	Unused security group	⚠

8.4 AWS Console Login



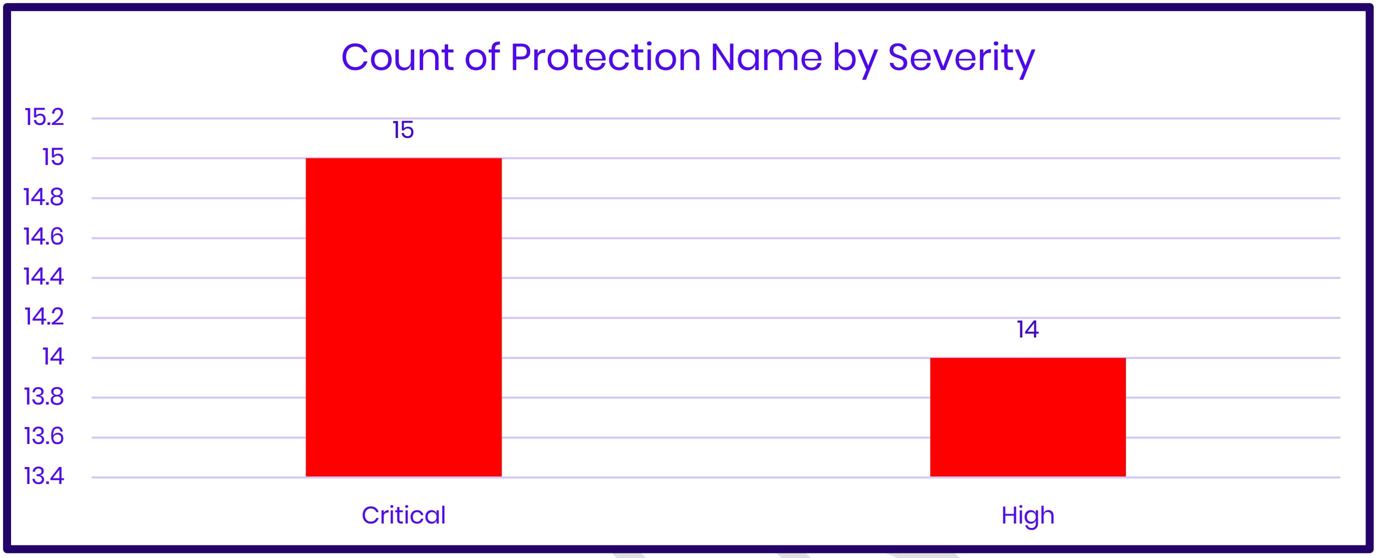
8.5 IAM User Insights

S.No.	Account ID	User Name	Insight	Severity
1	6.52918E+11	John Doe	IAM access key rotation	2
2	6.52918E+11	John Doe	IAM access key rotation	2
3	6.52918E+11	John Doe	IAM access key rotation	2
4	6.52918E+11	John Doe	IAM access key rotation	2
5	6.52918E+11	John Doe	IAM access key rotation	2
6	6.52918E+11	John Doe	IAM access key rotation	2
7	6.52918E+11	John Doe	IAM access key rotation	2
8	6.52918E+11	John Doe	User is unused for long time	2

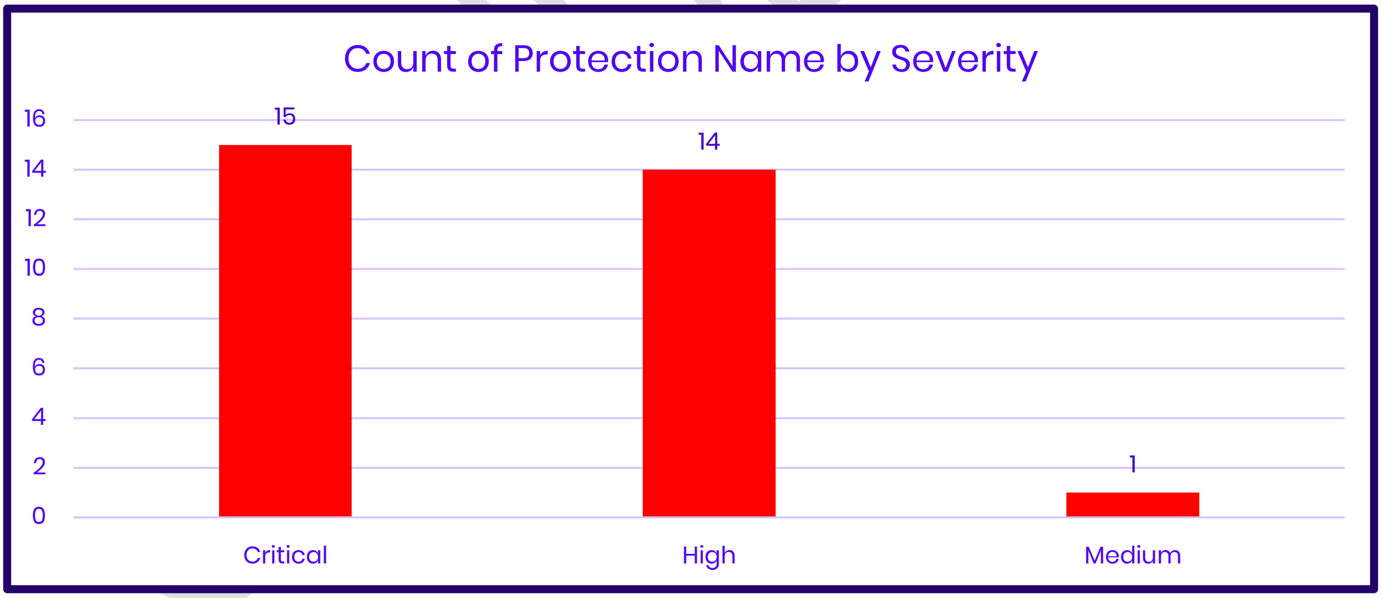
9. Check point smartview

9.1 CP-intrusion prevention system (IPS)

9.1.1 Most-Severity-Attacks

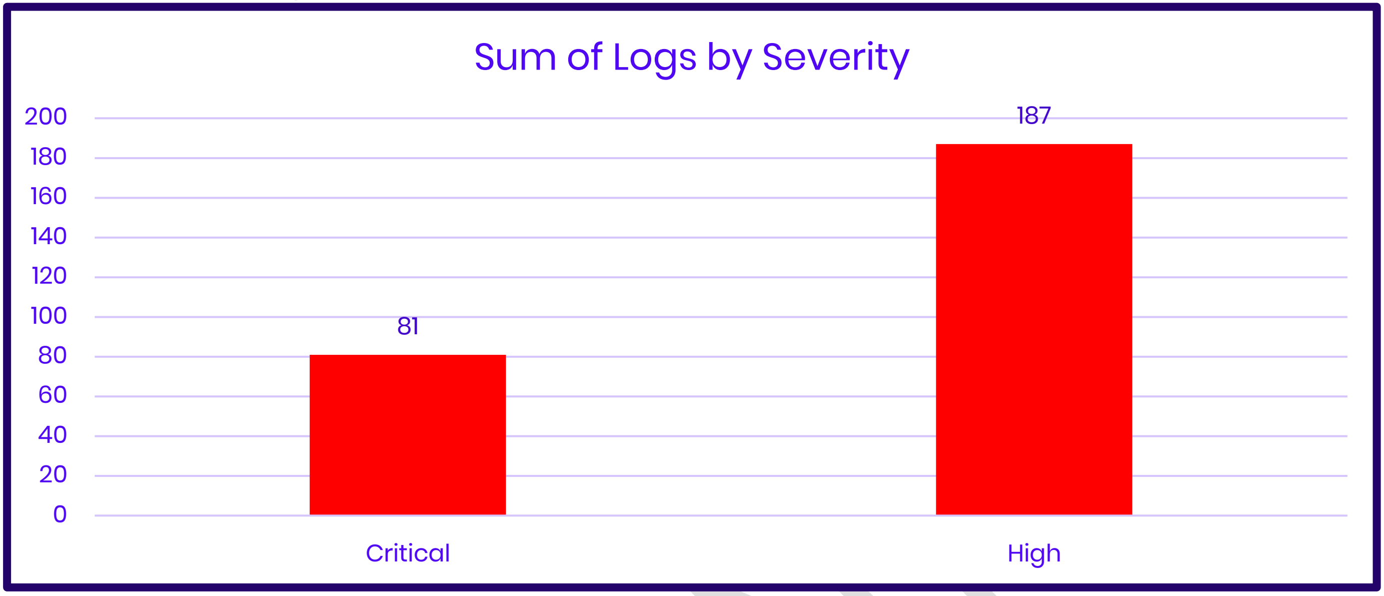


9.1.2 Top-Attacks

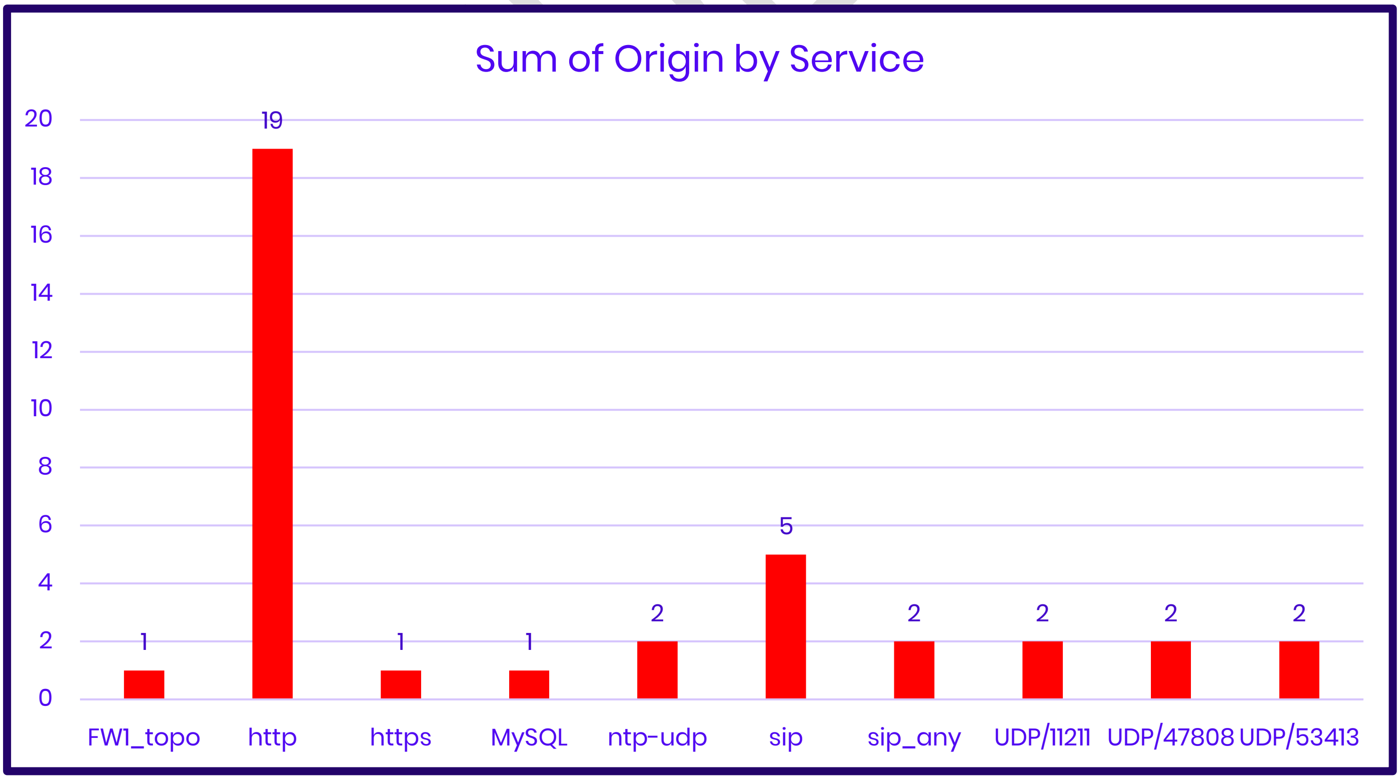


Note: Most of the attacks are occurred on Checkpoint VPN gateway or Checkpoint auto scaling gateways directly as auto scaling gateways are public also it includes IPS and threat emulation events.

9.1.3 Top-Origins and Top-Protections

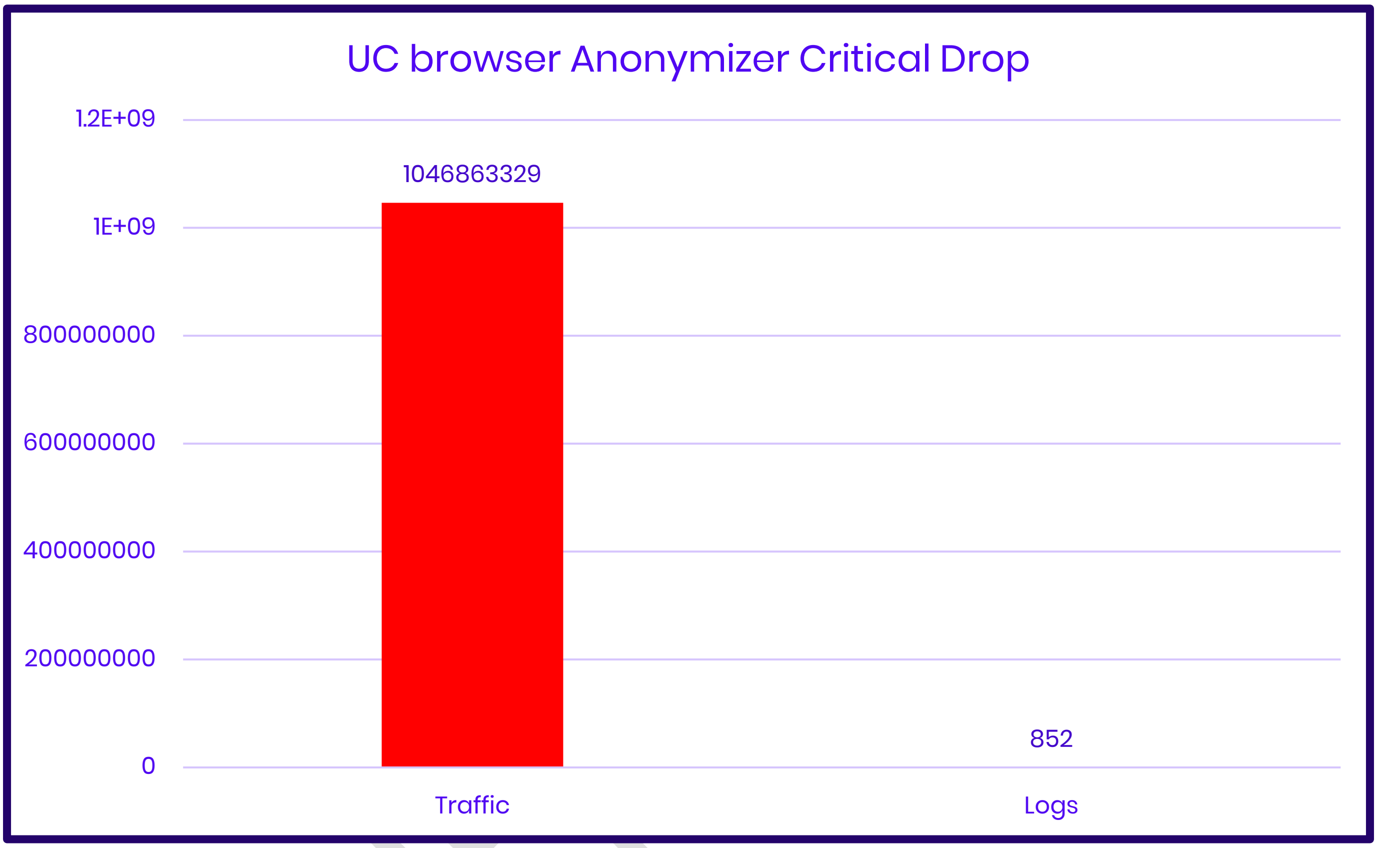


9.1.4 Top-Services and Top-Protections



9.2 Check Point Application and URL Filtering

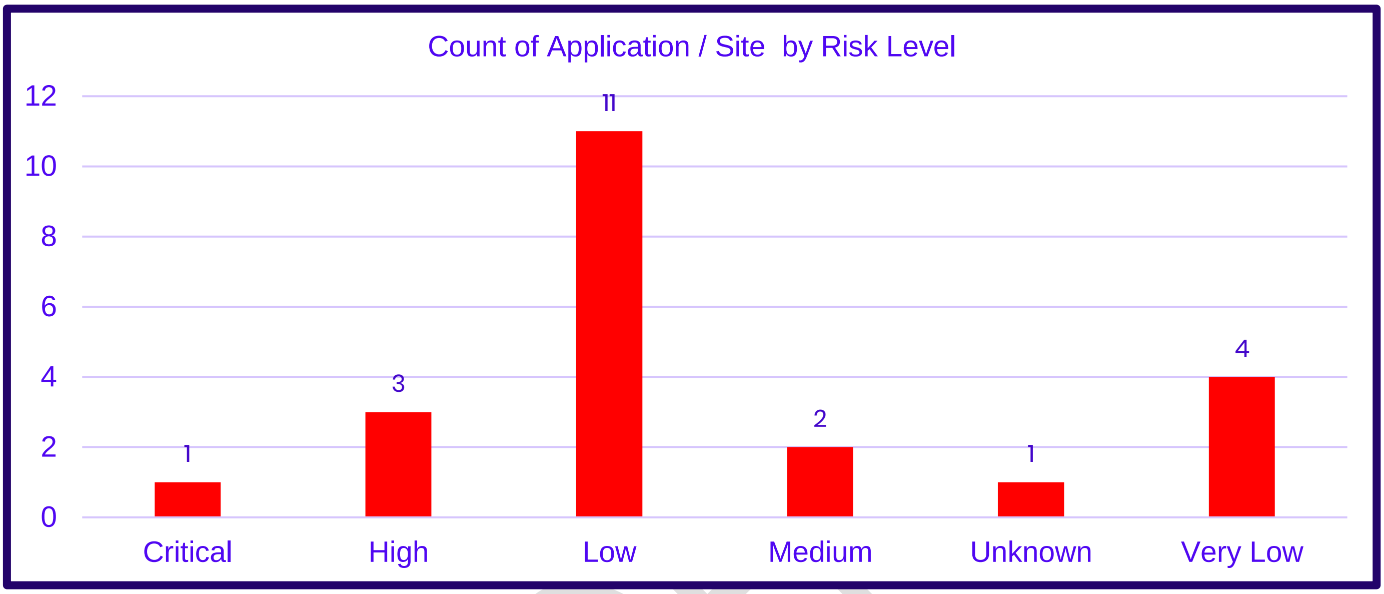
9.2.1 List of High-Risk Applications



An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable. It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet. It accesses the Internet on the user's behalf, protecting personal information by hiding the client computer's identifying information.

9.3 Executive Summary of Security Checkup

9.3.1 Top Applications Sites

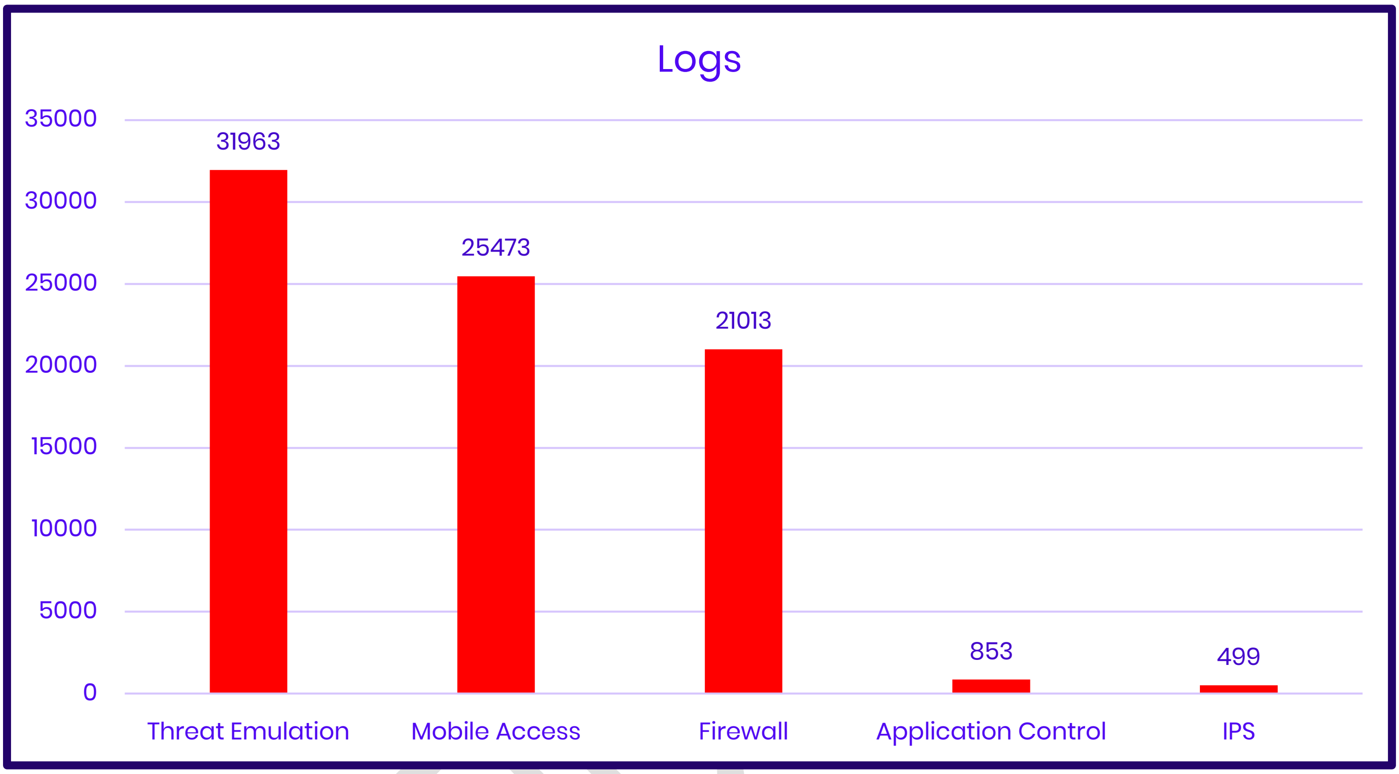


Application Name	Category	Risk
abc.com	Custom Application/Site	Medium
Google Data Saver	Browser Plugin	Medium
UC browser	Anonymizer	Critical
Googlebot	Web Spider	Very Low
AdsBot	Web Spider	Very Low
Yahoo Search	Search Engines / Portals	Low
Windows Media Player	Media Sharing	Low
Google News	Search Engines / Portals	Low
Postman	Computers / Internet	Low
Obot	Web Spider	Very Low
Microsoft Excel	Business / Economy	Low
Zabbix	Network Utilities	Low
Microsoft Word	Business / Economy	Low
abc.com	Custom Application/Site	Medium

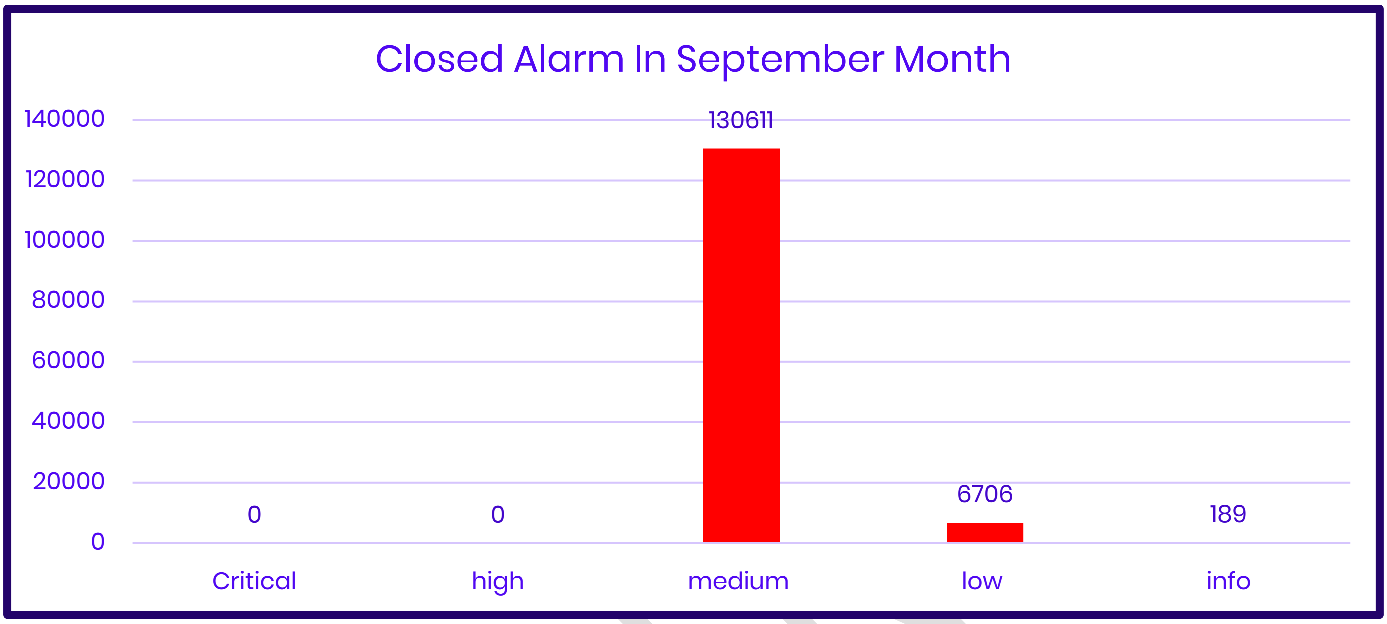
Summary of risk majorly reflects UC Browser being used by customers through their mobile phones in India. The same is kept on in line with previous discussions at ABC.

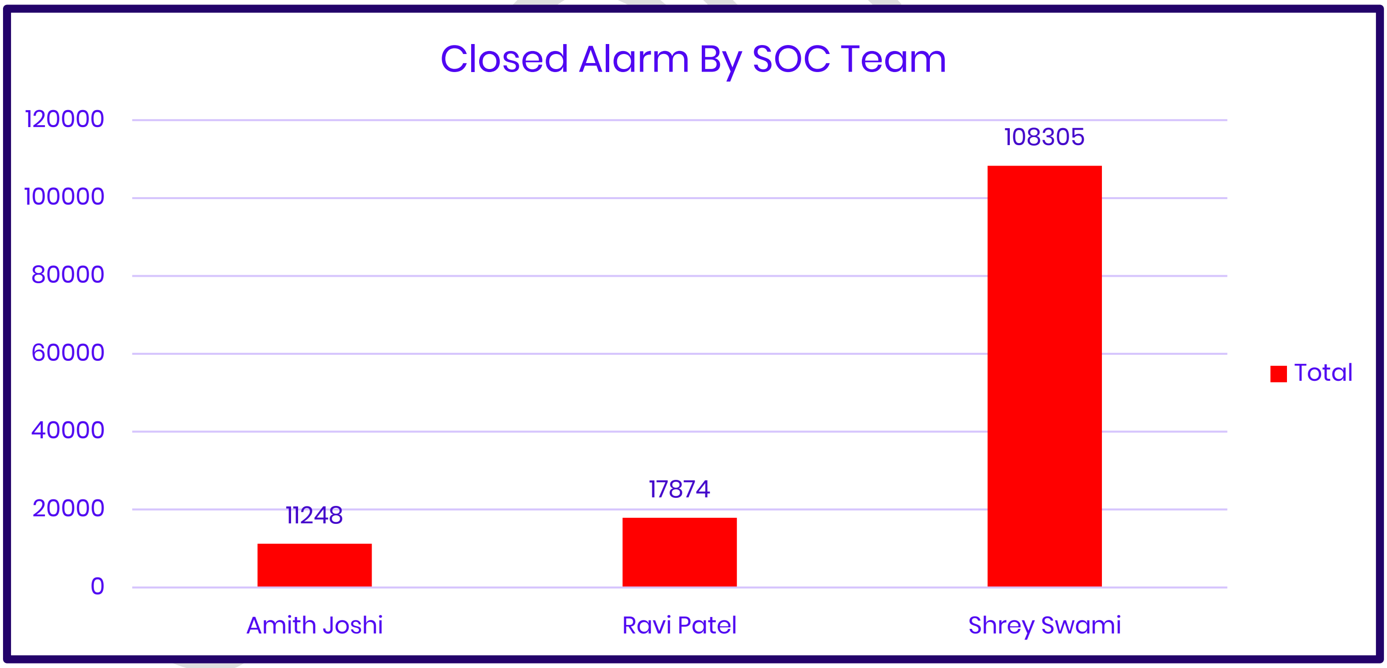
9.4 General Overview

9.4.1 Software Blades



10. Splunk Enterprise





11. Patch Management Observations

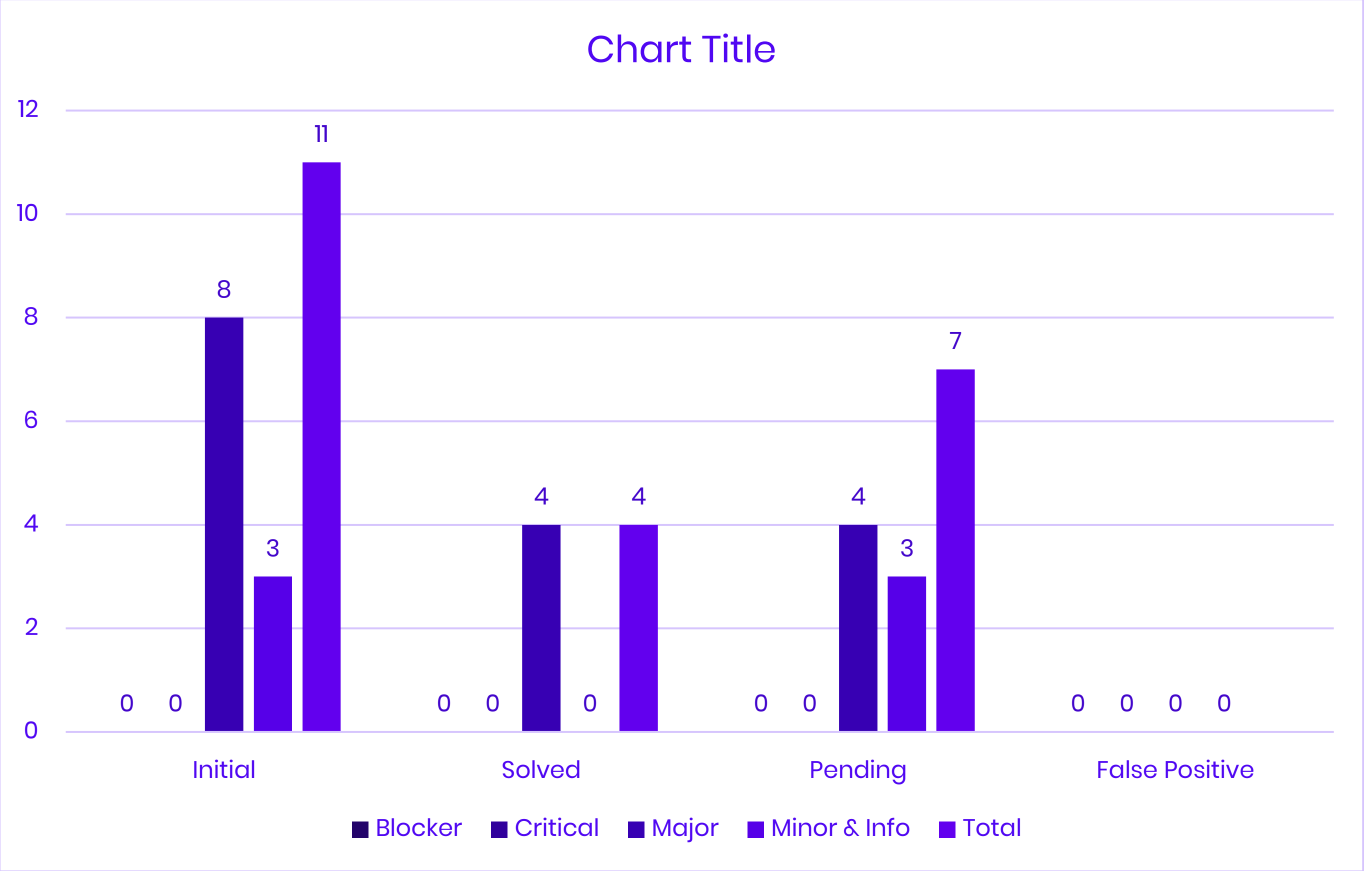
No	Requirement	Comment
1.	Any bug fix, security fix, updates or new versions released by the vendor or the internal software team will require for patch management	
2.	Patch Management is essential at the time of any new release from the vendor or the internal team for the system and applications used by ABC.	It has been informed to us that Patches are updated on request basis of user, these cases are not much, patch management need to be done according to policy set frequency
3.	OS (Windows) Patches	
4.	The "Install Automatic Updates" should be kept disabled.	On server (Which server) it is disabled but not on workstations and laptops
5.	How do you catagorize patches released from Microsoft?	Such categorization is not happening currently
6.	Patches released from Microsoft are to be categorized according to the Criticality and the systems affected (Example: Security updates are considered critical and updates for servers storing PHI data is critical)	It's a dependent clause that is not being followed
7.	Proper backup should be taken for the updated system in line with the Backup and Restoration policy.	Not happening
8.	The critical systems should be patched quarterly and other systems with comparatively low severity should be biannually.	There is WSUS server had been installed.
9.	For desktop computers, WSUS (Windows Server Update Server) should be used and only important updates should be rolled out.	Not happening
10.	The desktop computers should be updated biannually basis unless business-critical update is released by the vendor.	Not happening
11.	The updates should be first tested on UAT environment and QC should be performed on every application related to that server.	Not happening
12.	Once the QC is done in the UAT environment with positive report, the patch should be rolled out on the production environment after notifying all the stakeholders about the downtime.	Not happening
13.	On the other hand, the laptops should be updated biannually either physically or using remote access tools. WSUS should be configured	
14.	Operating System for which the vendor has stopped the support should not be used by ABC.	SonicWALL firmware had been updated.
15.	Network Devices Patches For Firewall, the vendor releases the latest firmware on the support page of their website and should be downloaded from there.	Till now CW is compiled as per policy set frequency but still CW sonic firewall is upgraded to the latest version

12. New Initiatives Taken

Sr. No	New Initiatives Taken
1	CWIS-825 New Server and Services Onboarding for V2 Launch - We have on boarded new services over New Relic so we are closing these ticket.
2	CWIS-827 Splunk Data Sources On-boarding - As per the request we have on-boarded both Nginx Server Logs (10.0.5.92,10.0.4.26) & New Production Server logs (10.0.4.252, 10.0.5.229). Also we have started fetching general/audit/error/slow-query logs from the new RDS (prod-ABC-v2).
3	CWIS-828 Imperva Site Add – We have on boarded the abc.com URL again over Imperva and Security Rules has been applied accordingly
4	CWIS-838 Spoofing of Sir ID - An attacker performed an spoofing attack on and using ID: john@abc.com After the investigating Office365 Sign-in activities and analysis of email we found no indicators of account compromised and found the email was spoofed. The detailed Log Analysis and summary is sent to Sir on email. For security reason we have reset password of ID: John@abc.com in Office365 and new password shared to Sir on Email.
5	CWIS-853 YYZ IP Getting Blocked - We have found IP Address of YYZ Bank getting blocked over Anti-Scrapper Policy in Imperva. (Rule Definition: Number of Sessions >=40). As approved by sir we have whitelisted the IP Address (103.68.221.92) of YYZ over Anti-Scrapper Policy.
6	CWIS-860 Live-ITR-Gunicorn-scraping-server-02 was not able to access – As of now error was resolved so we are closing these ticket.
7	CWIS-866 Removed newrelic agent from ekyc service 10.0.4.90 BOB server - We have removed new relic agent from ekyc service in 10.0.4.90 BOB prod server.
8	CWIS-867 RBI Advisory - We have blocked all the IP Addresses, URL's and Domains over Office365, Seqrite & Imperva.
9	CWIS-868 Microsoft to do Application allow for intunes - We have allowed and assigned the Microsoft To-Do Application in Managed Play Store.
10	CWIS-871 SonicWALL Mumbai Office Hardening Activity - The firewall is accessible Now also we have taken the remote of the spare system from mumbai office as well.

13. Static Code – Analysis Report

No	Initial	Solved	Pending	False Positive
Blocker	0	0	0	0
Critical	0	0	0	0
Major	8	4	4	0
Minor & Info	3	0	3	0
Total	11	4	7	



***If Any Query in Static Code report please contact to Development Team because we don't have Access of Sonarqube.**

14. Current Architecture (Updated)

Architecture is sanatized

15. Vulnerability Scan Report

- **ABC Corporation Mobile Application Dynamic Testing Report (Completed Patching)**

Particulars	Critical	High	Medium	Low	Date Of End
Vulnerability Identified	0	0	0	0	16th September 2020

- **ABC Corporation HRMS Web Application Vulnerability Assessment & Penetration Testing Report**

Particulars	Critical	High	Medium	Low	Date Of End
Vulnerability Identified	2	6	64	7	17th September 2020

- **ABC Corporation infra Vulnerability Assessment & Penetration Testing Report**

Particulars	Critical	High	Medium	Low	Date Of End
Vulnerability Identified	2	6	64	7	26th September 2020

- **ABC Corporation Production & Non-Production Vulnerability Assessment & Penetration Testing Report**

Particulars	Critical	High	Medium	Low	Date Of End
Vulnerability Identified	3	0	61	23	20th October 2020

- **ABC Corporation Web Application Vulnerability Assessment & Penetration Testing Report**

Particulars	Critical	High	Medium	Low	Date of End
Vulnerability Identified	0	1	4	5	31st October 2020

- **ABC Corporation BOB Web Application Vulnerability Assessment & Penetration Testing Report**

Particulars	Critical	High	Medium	Low	Date of End
Vulnerability Identified	0	3	0	3	25th September 2020

- **ABC Corporation UAT2 Portal(ODOP, MSME, Monitoring) Web Application Vulnerability Assessment & Penetration Testing Report**

Particulars	Critical	High	Medium	Low	Date of End
Vulnerability Identified	0	2	2	4	26th September 2020

- **ABC Corporation Retail Portals(HL, PL, Auto loan) Web Application Vulnerability Assessment & Penetration Testing Report**

Particulars	Critical	High	Medium	Low	Date of End
Vulnerability Identified	0	1	2	3	29th September 2020

Note: Required bank statements from April 2020 to September 2020 for UAT2.

Vulnerability open as per latest scan. Details reports shared separately mail.

Report Disclaimer

By accessing and using this report you agree to the following terms and conditions and all applicable laws, without limitation or qualification, unless otherwise stated, the contents of this document including, but not limited to, the text and images contained herein and their arrangement are the property of Infopercept Consulting Pvt. Ltd.
Nothing contained in this document shall be construed as conferring by implication, estoppels, or otherwise, any license or right to any copyright, patent, trademark or other proprietary interest of Infopercept Consulting Pvt. Ltd or any third party.

This document and its contents including, but not limited to, graphic images and documentation may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, without the prior written consent of Infopercept Consulting Pvt. Ltd.

Any use you make of the information provided, is at your own risk and liability. Infopercept Consulting Pvt. Ltd makes no representation about the suitability, reliability, availability, timeliness, and accuracy of the information, products, services, and related graphics contained in this document. All such information products, services, related graphics and other contents are provided 'as is' without warranty of any kind. The relationship between you and Infopercept Consulting Pvt. Ltd shall be governed by the laws of the Republic of India without regard to its conflict of law provisions. You and Infopercept Consulting Pvt. Ltd agree to submit to the personal and exclusive jurisdiction of the courts located at Ahmedabad. You are responsible for complying with the laws of the jurisdiction and agree that you will not access or use the information in this report, in violation of such laws.

You represent that you have the lawful right to submit such information and agree that you will not submit any information unless you are legally entitled to do so. This report is being supplied by us on the basis that it is for your benefit and information only and that, save as may be required by law or by a competent regulatory authority (in which case you shall inform us in advance), it shall not be copied, referred to or disclosed, in whole (save for your own internal purpose) or in part, without our prior written consent. The report is submitted on the basis that you shall not quote our name or reproduce our logo in any form or medium without prior written consent. You may disclose in whole this report to your legal and other professional advisers for the purpose of your seeking advice in relation to the report, provided that when doing so you inform them that:

- **Disclosure by them (save for their own internal purposes) is not permitted without our prior written consent, and**
- **To the fullest extent permitted by law we accept no responsibility or liability to them in connection with this report.**

Any advice, opinion, statement of expectation, forecast or recommendation supplied or expressed by us in this report is based on the information provided to us and we believe such advice, opinion, statement of expectation, forecast or recommendation to be true. However, such advice, opinion, statement of expectation, forecast or recommendation shall not amount to any form of guarantee that we have determined or predicted future events or circumstances but shall ensure accuracy, competency, correctness or completeness of the report based on the information provided to us.

About INFOPERCEPT

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

Global Offices

UNITED STATES OF AMERICA	+1 516 713 5040
UNITED KINGDOM	+44 2035002056
SRI LANKA	+94 702 958 909
KUWAIT	+965 6099 1177
INDIA	+91 9898857117

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.

Infopercept