Risk Indicators: Information Security Daily Checklist

SUMMARY

Purpose: Overview /Security health check on key systems and devices

Scope/Domain: Information Security

Report Recipients: I. T Audit, I.T Risk, IT & MIS, PMO, Information Security Steering Committee Checklist

Prepared by: Patrick T. Siziba

Report Preparation Date: 22 May 2024

REVIEWED ITEMS

	1. **Group IT & MIS Daily Risk Indicators**: Sectional Checklists
Description	TechSupport Checklist: - A summarized daily health check for the IT Infrastructure IS Support Checklist: - A summarized daily health check for IT databases and applications domain. Digital Channels Checklist: - A summarized daily health check for EFT & Networks infrastructure. Data Team Checklist: - A summarized daily health and security check for database infrastructure
Control Objective	- To check for the presence of high and potential risk security issues in the system reports provided by IT&MIS daily

Name of Checklist	**Potential Indicators of Risk**	**Metric**		**Comment**
Digital Channels Checklist	≥80 % indicates over utilization of resources which may compromise the integrity and availability of service.	% of Disk usage ≤ 95 % % of CPU usage ≤ 80% % Memory usage ≤ 80 %		Within threshold
Data Team Checklist	≥80 % indicates over utilization of resources which may compromise the integrity and availability of service	% of Disk usage ≤ 95 % % of CPU usage ≤ 80% % Memory usage ≤ 80 %		Within threshold
	Program Changes in line with change management process.	Program Changes on Oracle DB No changes.		

USER	DB USERNAME	Action	Count
oracle	BIPDR1_BIPLATFORM	UPDATE	7
oracle	BIPDR1_BIPLATFORM	DELETE	2
root	FCPREPROD	INSERT	2

Access, Distribution and Modification of this document is prohibited unless you have been expressly authorized by FBC Executive Management or anyone with delegated authority.

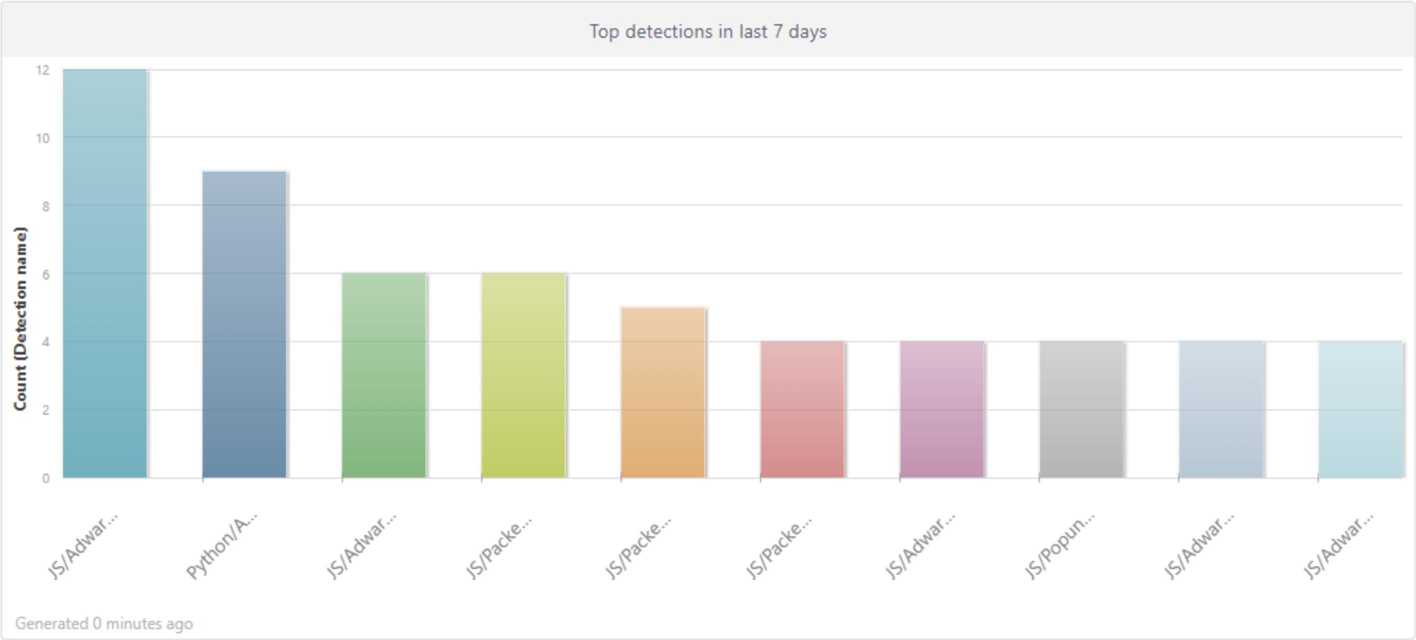
Risk Indicators: Information Security Daily Checklist

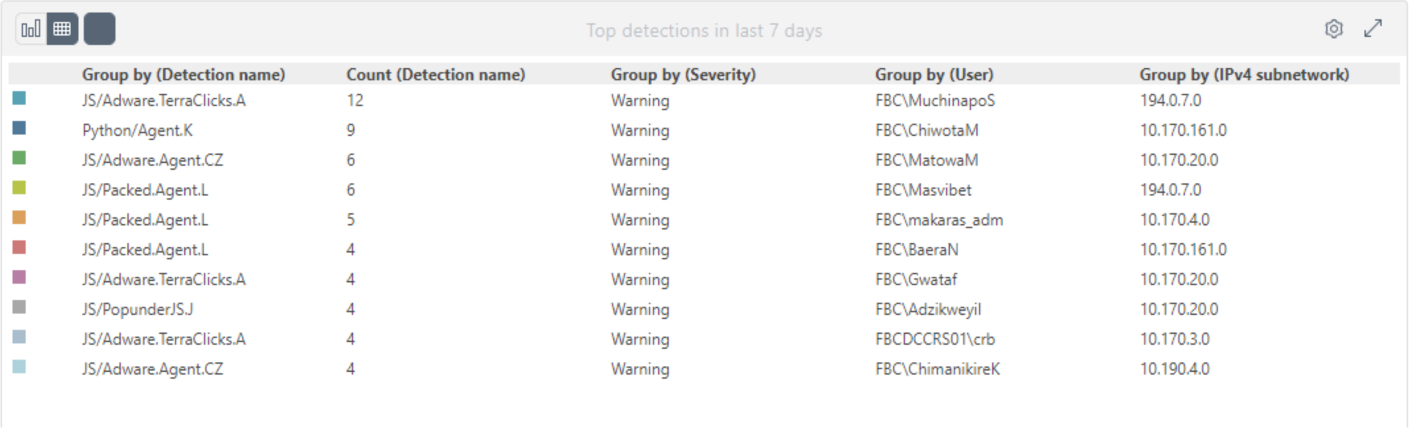
IS Support Checklist	≥80 % indicates over utilization of resources which may compromise the integrity and availability of service	% of Disk usage ≤ 95 % % of CPU usage ≤ 80% % of Memory usage ≤ 80 %		
Technical Support Checklist	ICT Generator Fuel Gauge: Generator Fuel below 50 %	% level of generator fuel ≥ 50 % Generator Temperature≤50°C		Within threshold
	• Temperature should not exceed 50 °C. No of event alerts per week should not exceed 2 (Events for high humidity and faults)	N0 of event alerts for humidity and faults per week≤ 2		• No anomalies reported on Checklist.
	Uninterruptible Power Supply: System monitored and operating within the boundaries and limits imposed by controls. ○ *Ups Runtime Power = 2hours 3 minutes* ○ *Ups Runtime Power = 1 hour 30 minutes* Fire Safety systems	Runtime ≥15 minutes for UPS 2 max runtime of 30 minutes		Charging capacity should be 100 % all the time indicating the general health of the UPS batteries
		% of charging capacity =100%		
		% of Utilization Capacity ≥ 50 %		Utilization Capacity should be above 50 % for full utilization of the UPS
		Amber / Red flashing lights		No Amber / Red flashing lights
	Heating, Ventilation, Air Conditioning and Cooling systems	• Amber / Red flashing lights for critical, warning faults. • N0 of event alerts for faults per week≤ 2. • No of reported Events in the event Log. Number of Alarm Alerts per week do not exceed 2		No anomalies reported on Checklist.
	≥80 % indicates over utilization of resources which may compromise the integrity and availability of service	% of Disk usage ≤ 95 % % of CPU usage ≤ 80% • % Memory usage ≤ 80 %	i.	ii. Within threshold

Risk Indicators: Information Security Daily Checklist

2. Antivirus Server	
Description	- Application used to prevent, detect, and remove malicious software
Control Objective	- To check for the effectiveness of the antivirus security solution and identify any anomalies/exceptions that may need to be addressed manually and further investigate/interrogate persistent and recurring threats.

a. Top viral Threats in the last 7 days





	Group by (Detection name)	Count (Detection name)	Group by (Severity)	Group by (User)	Group by (IPv4 subnetwork)
■	JS/Adware.TerraClicks.A	12	Warning	FBC\MuchinapoS	194.0.7.0
■	Python/Agent.K	9	Warning	FBC\ChiwotaM	10.170.161.0
■	JS/Adware.Agent.CZ	6	Warning	FBC\MatowaM	10.170.20.0
■	JS/Packed.Agent.L	6	Warning	FBC\Masvibet	194.0.7.0
■	JS/Packed.Agent.L	5	Warning	FBC\makaras_adm	10.170.4.0
■	JS/Packed.Agent.L	4	Warning	FBC\BaeraN	10.170.161.0
■	JS/Adware.TerraClicks.A	4	Warning	FBC\Gwataf	10.170.20.0
■	JS/PopunderJS.J	4	Warning	FBC\Adzikweyil	10.170.20.0
■	JS/Adware.TerraClicks.A	4	Warning	FBCDCCRS01\crb	10.170.3.0
■	JS/Adware.Agent.CZ	4	Warning	FBC\ChimanikireK	10.190.4.0

Findings	**12 JS/Adware.TerrClicks.A** malware detections were recorded by ESET. This malware type recorded the highest viral threat count of all categories in the past 7 days.

Risk Indicators: Information Security Daily Checklist

Comment	Web shells are malicious scripts that enable threat actors to compromise web servers and launch additional attacks. Threat actors first penetrate a system or network and then install a web shell. From this point onwards, they use it as a permanent backdoor into the targeted web applications and any connected systems.

b. Overview of Antivirus Update Status

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
AD TOTAL DEVICES	**1604**		**1700**			
Workstations	1384		1390			
MacBook	25		25			
Servers	195		195			
ESET Devices	**1419**	**1420**	**1424**			
Workstations	1242	1242	1244			
MacBooks	13	14	14			
Servers	164	164	166			
DLP DEVICES	**1240**		**1126**			
workstations	1219		1109			
Macbook	21		17			

	January	February	March	April	May	June	July	August
AD Clean-up (Deleted Machines)	59	32	81	60				

ESET Version	**Workstations**	**Servers**	**MacBook's**
Latest version	1170	105	5
Lower version	74	61	9

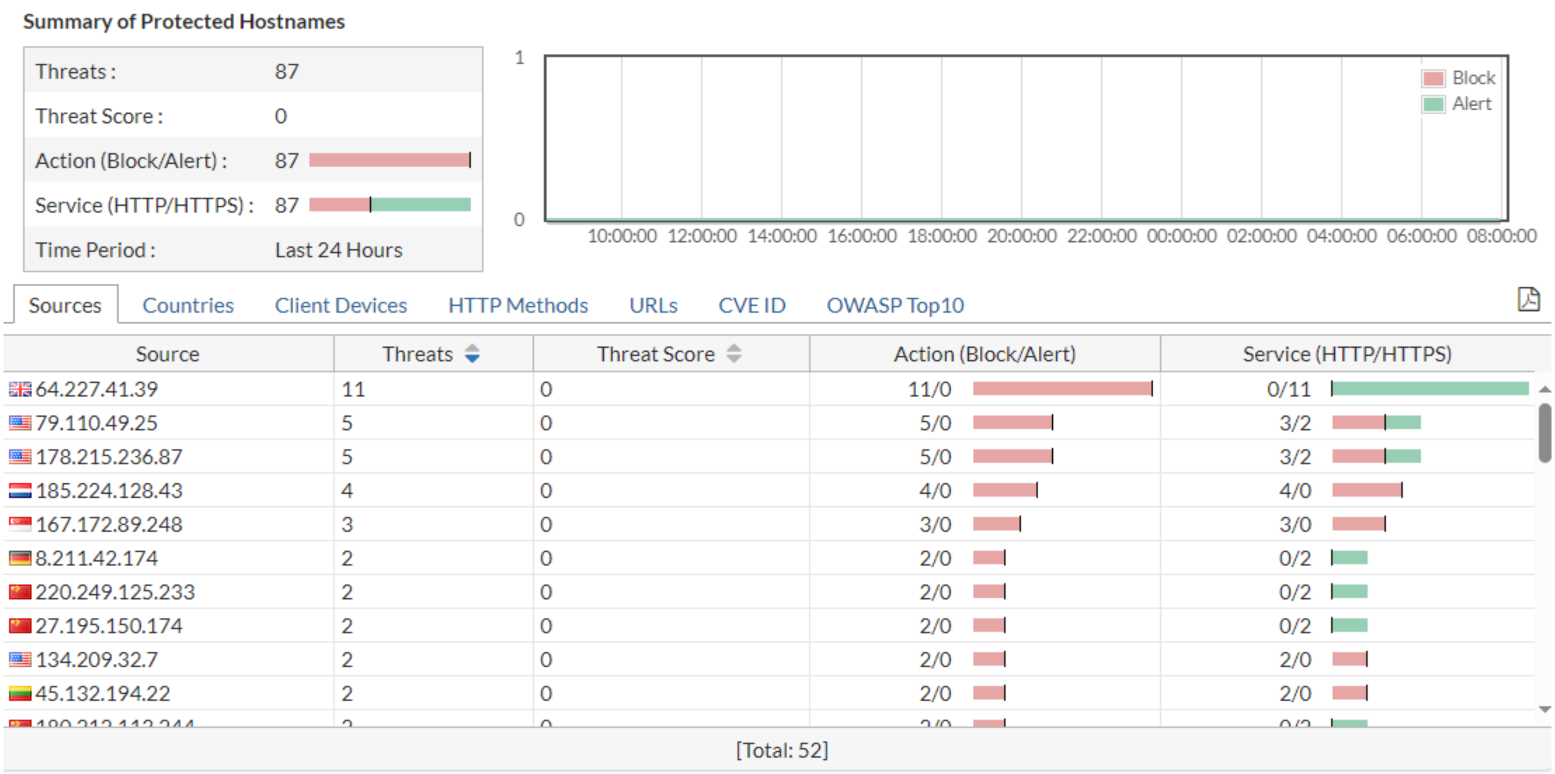
Risk Indicators: Information Security Daily Checklist

Total	**1244**	**166**	**14**

Findings	**1424 devices** or licenses have been recorded on ESET. **1244 workstations** recorded. • **1170** are running **ESET** version **11** whilst **74** are on **lower** versions. **166** servers recorded. ESET updates pending restart to upgrade version. • **105** are running **ESET** version **11** whilst **61 servers** are running lower/outdated **ESET** version. **14** MacBook(s) recorded. • **5** MacBook device is running the latest **ESET** version **7 and** whilst **9** devices are running **lower** versions i.e. 6. **1239 devices** have Data Leakage Protection (DLP) • 1218 workstations have DLP. • 21 MacBooks have DLP installed.
Comments	Problems of machines detected to be at security risk and those requiring attention are but not limited to: • Device requires restart. • Email client protection is paused. • Module update failed. • Real time system protection is paused or non-functional. • Recent update attempts failed. • Security product out of date or not activated

Risk Indicators: Information Security Daily Checklist

3. Web Application Firewall	
Description	- The Web Application Firewall examines traffic emanating from internal web application for suspicious activity and automatically filters out illegitimate traffic based on the defined firewall policy.
Control Objective	- To check for the effectiveness of the security solution and identify any anomalies/exceptions that may need to be addressed manually and further investigate/interrogate persistent and recurring threats.
a. Daily Intrusions Detected	



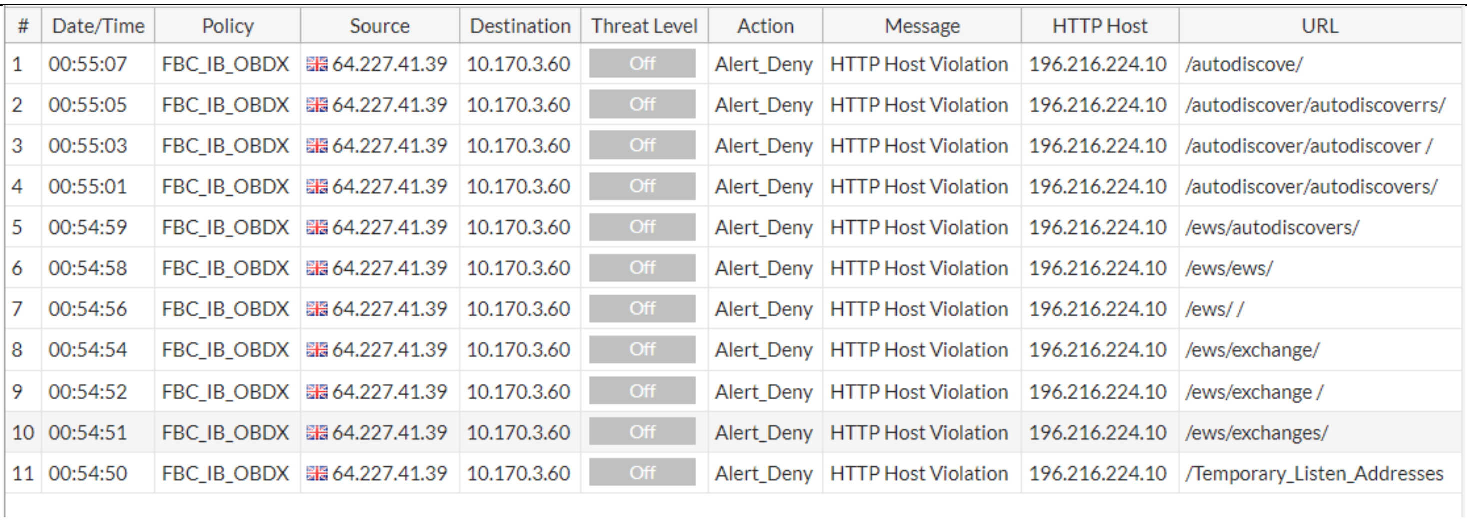
Summary of Protected Hostnames

Threats :	87
Threat Score :	0
Action (Block/Alert) :	87
Service (HTTP/HTTPS) :	87
Time Period :	Last 24 Hours

Source	Threats	Threat Score	Action (Block/Alert)	Service (HTTP/HTTPS)
64.227.41.39	11	0	11/0	0/11
79.110.49.25	5	0	5/0	3/2
178.215.236.87	5	0	5/0	3/2
185.224.128.43	4	0	4/0	4/0
167.172.89.248	3	0	3/0	3/0
8.211.42.174	2	0	2/0	0/2
220.249.125.233	2	0	2/0	0/2
27.195.150.174	2	0	2/0	0/2
134.209.32.7	2	0	2/0	2/0
45.132.194.22	2	0	2/0	2/0
180.213.112.244	2	0	2/0	0/2

[Total: 52]

Risk Indicators: Information Security Daily Checklist



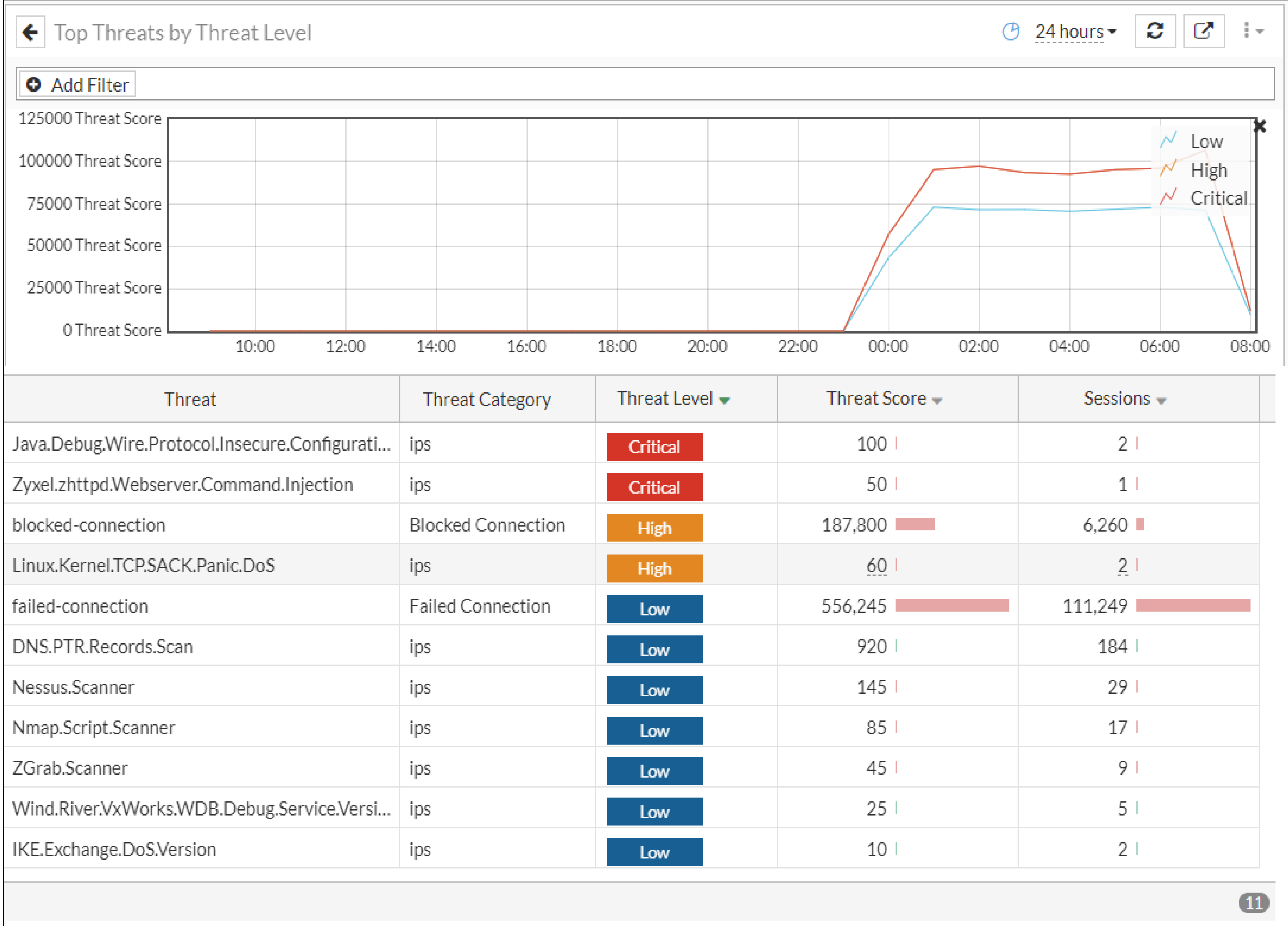
#	Date/Time	Policy	Source	Destination	Threat Level	Action	Message	HTTP Host	URL
1	00:55:07	FBC_IB_OBDX	64.227.41.39	10.170.3.60	Off	Alert_Deny	HTTP Host Violation	196.216.224.10	/autodiscove/
2	00:55:05	FBC_IB_OBDX	64.227.41.39	10.170.3.60	Off	Alert_Deny	HTTP Host Violation	196.216.224.10	/autodiscover/autodiscoverrs/
3	00:55:03	FBC_IB_OBDX	64.227.41.39	10.170.3.60	Off	Alert_Deny	HTTP Host Violation	196.216.224.10	/autodiscover/autodiscover /
4	00:55:01	FBC_IB_OBDX	64.227.41.39	10.170.3.60	Off	Alert_Deny	HTTP Host Violation	196.216.224.10	/autodiscover/autodiscovers/
5	00:54:59	FBC_IB_OBDX	64.227.41.39	10.170.3.60	Off	Alert_Deny	HTTP Host Violation	196.216.224.10	/ews/autodiscovers/
6	00:54:58	FBC_IB_OBDX	64.227.41.39	10.170.3.60	Off	Alert_Deny	HTTP Host Violation	196.216.224.10	/ews/ews/
7	00:54:56	FBC_IB_OBDX	64.227.41.39	10.170.3.60	Off	Alert_Deny	HTTP Host Violation	196.216.224.10	/ews/ /
8	00:54:54	FBC_IB_OBDX	64.227.41.39	10.170.3.60	Off	Alert_Deny	HTTP Host Violation	196.216.224.10	/ews/exchange/
9	00:54:52	FBC_IB_OBDX	64.227.41.39	10.170.3.60	Off	Alert_Deny	HTTP Host Violation	196.216.224.10	/ews/exchange /
10	00:54:51	FBC_IB_OBDX	64.227.41.39	10.170.3.60	Off	Alert_Deny	HTTP Host Violation	196.216.224.10	/ews/exchanges/
11	00:54:50	FBC_IB_OBDX	64.227.41.39	10.170.3.60	Off	Alert_Deny	HTTP Host Violation	196.216.224.10	/Temporary_Listen_Addresses

Findings	**11 threats** from external source **IP 64.227.41.39** recorded the highest threat count. A total of **87** threats from **52** different external IP addresses were detected and dropped.
Comment	URLs attached above were detected as malicious payloads. The firewall managed to drop or block all the threats in the past **24 hrs**.

Risk Indicators: Information Security Daily Checklist

4. **Core Banking Firewall**	
Description	- The Core Banking Firewall examines internal traffic for suspicious activity and protects the whole environment
Control Objective	- To check for the effectiveness of the security solution and identify any anomalies/exceptions that may need to be addressed manually and further investigate/interrogate persistent and recurring threats.

a. Daily Intrusions Detected



Threat	Threat Category	Threat Level	Threat Score	Sessions
Java.Debug.Wire.Protocol.Insecure.Configurati...	ips	Critical	100	2
Zyxel.zhttpd.Webserver.Command.Injection	ips	Critical	50	1
blocked-connection	Blocked Connection	High	187,800	6,260
Linux.Kernel.TCP.SACK.Panic.DoS	ips	High	60	2
failed-connection	Failed Connection	Low	556,245	111,249
DNS.PTR.Records.Scan	ips	Low	920	184
Nessus.Scanner	ips	Low	145	29
Nmap.Script.Scanner	ips	Low	85	17
ZGrab.Scanner	ips	Low	45	9
Wind.River.VxWorks.WDB.Debug.Service.Versi...	ips	Low	25	5
IKE.Exchange.DoS.Version	ips	Low	10	2

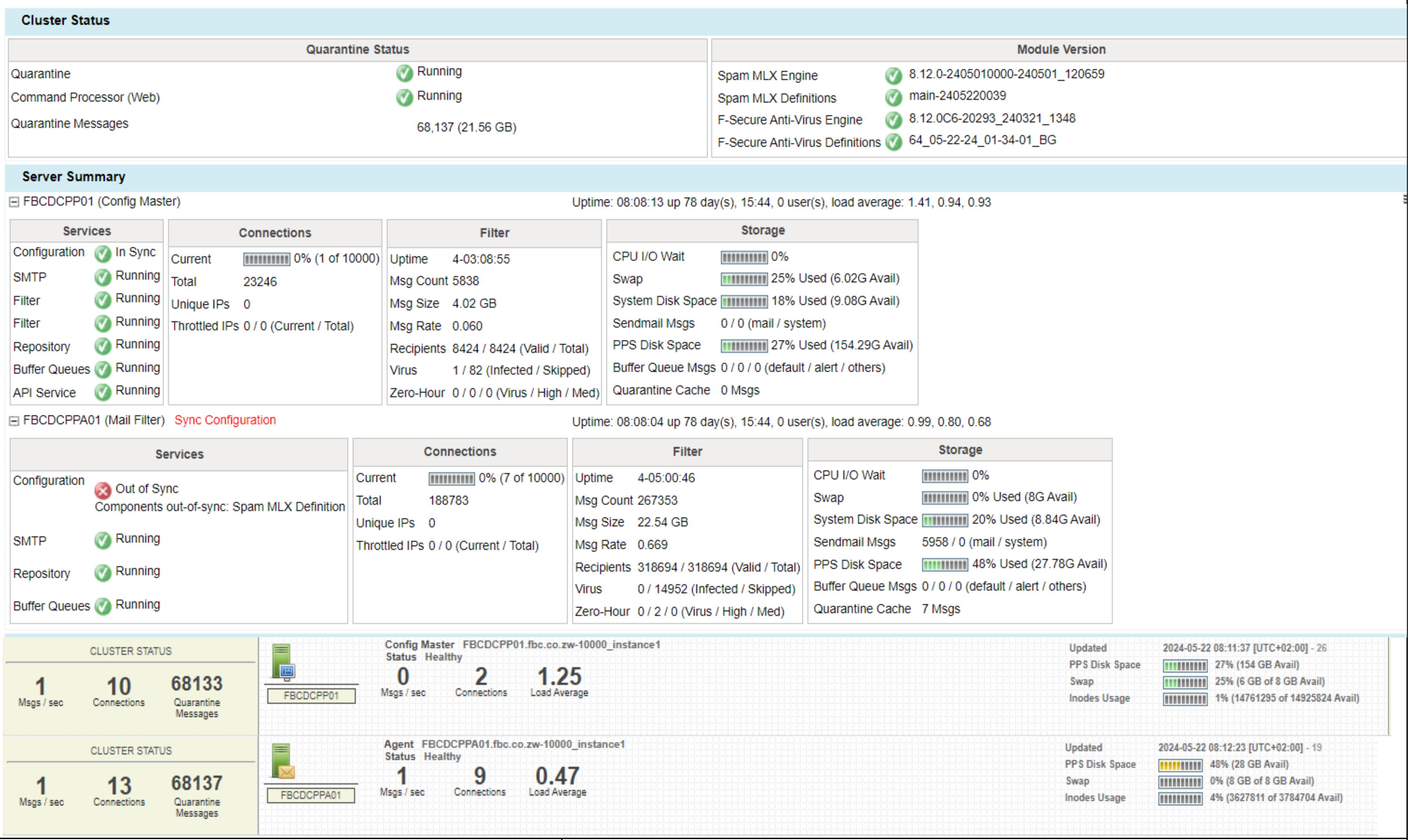
11

Findings	**2 critical** level threat, **2 high** level threat, and **7 low** level threats were detected by the firewall in the past **24hrs**.
Comment	All threats were successfully detected and blocked or dropped by the firewall.

Risk Indicators: Information Security Daily Checklist

5. Proofpoint Email Security	
Description	- This is an E-mail security system that blocks spam, phishing, and viruses from reaching the users` inbox.
Control Objective	- To check for the effectiveness of the security solution and identify any anomalies/exceptions that may need to be addressed manually and further investigate/interrogate 3persistent and recurring threats.

a. Proofpoint Services



Cluster Status

Quarantine Status	
Quarantine	✓ Running
Command Processor (Web)	✓ Running
Quarantine Messages	68,137 (21.56 GB)

Module Version	
Spam MLX Engine	✓ 8.12.0-2405010000-240501_120659
Spam MLX Definitions	✓ main-2405220039
F-Secure Anti-Virus Engine	✓ 8.12.0C6-20293_240321_1348
F-Secure Anti-Virus Definitions	✓ 64_05-22-24_01-34-01_BG

Server Summary

⊟ FBCDCPP01 (Config Master) Uptime: 08:08:13 up 78 day(s), 15:44, 0 user(s), load average: 1.41, 0.94, 0.93

Services	
Configuration	✓ In Sync
SMTP	✓ Running
Filter	✓ Running
Filter	✓ Running
Repository	✓ Running
Buffer Queues	✓ Running
API Service	✓ Running

Connections	
Current	0% (1 of 10000)
Total	23246
Unique IPs	0
Throttled IPs	0 / 0 (Current / Total)

Filter	
Uptime	4-03:08:55
Msg Count	5838
Msg Size	4.02 GB
Msg Rate	0.060
Recipients	8424 / 8424 (Valid / Total)
Virus	1 / 82 (Infected / Skipped)
Zero-Hour	0 / 0 / 0 (Virus / High / Med)

Storage	
CPU I/O Wait	0%
Swap	25% Used (6.02G Avail)
System Disk Space	18% Used (9.08G Avail)
Sendmail Msgs	0 / 0 (mail / system)
PPS Disk Space	27% Used (154.29G Avail)
Buffer Queue Msgs	0 / 0 / 0 (default / alert / others)
Quarantine Cache	0 Msgs

⊟ FBCDCPPA01 (Mail Filter) Sync Configuration Uptime: 08:08:04 up 78 day(s), 15:44, 0 user(s), load average: 0.99, 0.80, 0.68

Services	
Configuration	✗ Out of Sync Components out-of-sync: Spam MLX Definition
SMTP	✓ Running
Repository	✓ Running
Buffer Queues	✓ Running

Connections	
Current	0% (7 of 10000)
Total	188783
Unique IPs	0
Throttled IPs	0 / 0 (Current / Total)

Filter	
Uptime	4-05:00:46
Msg Count	267353
Msg Size	22.54 GB
Msg Rate	0.669
Recipients	318694 / 318694 (Valid / Total)
Virus	0 / 14952 (Infected / Skipped)
Zero-Hour	0 / 2 / 0 (Virus / High / Med)

Storage	
CPU I/O Wait	0%
Swap	0% Used (8G Avail)
System Disk Space	20% Used (8.84G Avail)
Sendmail Msgs	5958 / 0 (mail / system)
PPS Disk Space	48% Used (27.78G Avail)
Buffer Queue Msgs	0 / 0 / 0 (default / alert / others)
Quarantine Cache	7 Msgs

CLUSTER STATUS

Msgs / sec	Connections	Quarantine Messages
1	10	68133

FBCDCPP01

Config Master FBCDCPP01.fbc.co.zw-10000_instance1
Status Healthy

Msgs / sec	Connections	Load Average
0	2	1.25

Updated	2024-05-22 08:11:37 [UTC+02:00] - 26
PPS Disk Space	27% (154 GB Avail)
Swap	25% (6 GB of 8 GB Avail)
Inodes Usage	1% (14761295 of 14925824 Avail)

CLUSTER STATUS

Msgs / sec	Connections	Quarantine Messages
1	13	68137

FBCDCPPA01

Agent FBCDCPPA01.fbc.co.zw-10000_instance1
Status Healthy

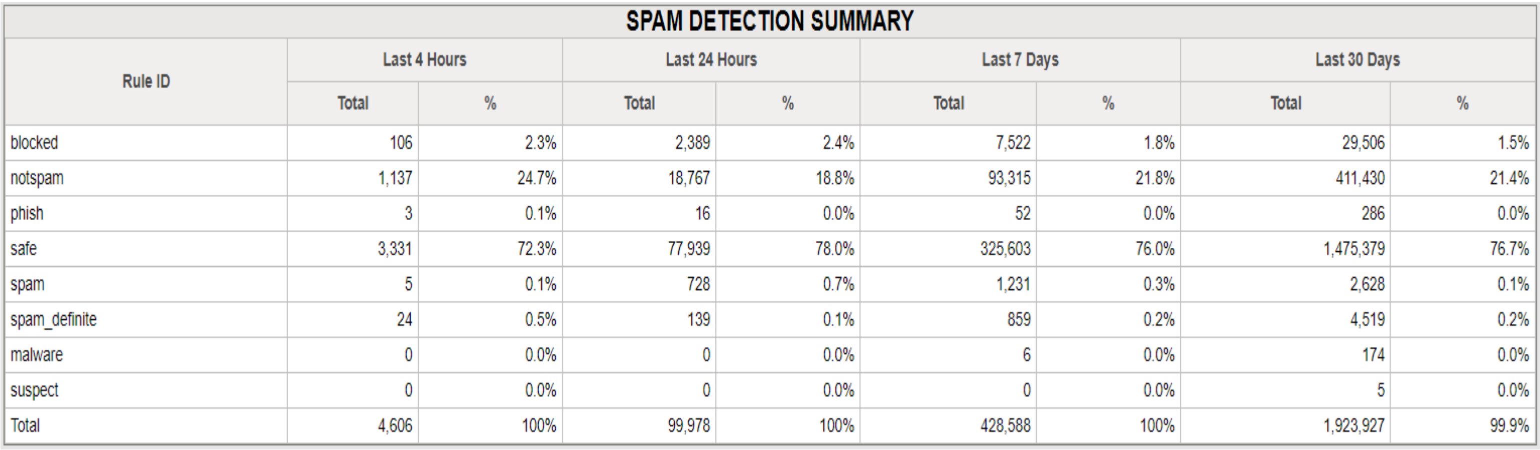
Msgs / sec	Connections	Load Average
1	9	0.47

Updated	2024-05-22 08:12:23 [UTC+02:00] - 19
PPS Disk Space	48% (28 GB Avail)
Swap	0% (8 GB of 8 GB Avail)
Inodes Usage	4% (3627811 of 3784704 Avail)

Findings	Proofpoint services are running.
Comment	**Services, Connections,** and **Storage** services for the **configuration master server** are running at optimum.

Risk Indicators: Information Security Daily Checklist

b. SPAM Detection Summary

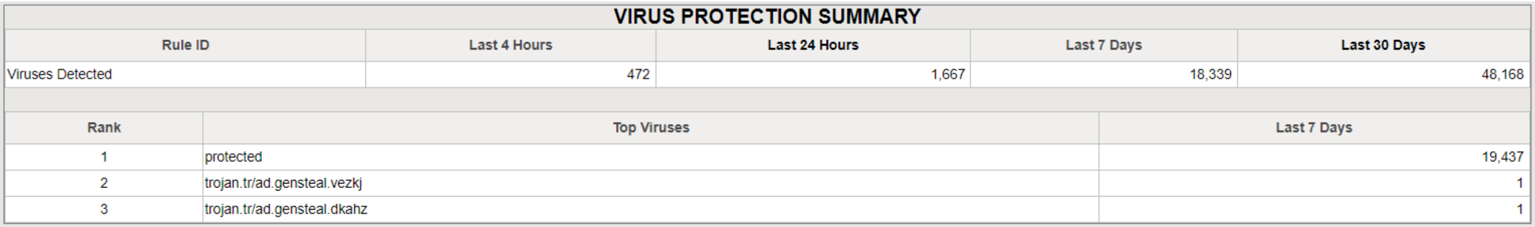


SPAM DETECTION SUMMARY

Rule ID	Last 4 Hours		Last 24 Hours		Last 7 Days		Last 30 Days	
	Total	%	Total	%	Total	%	Total	%
blocked	106	2.3%	2,389	2.4%	7,522	1.8%	29,506	1.5%
notspam	1,137	24.7%	18,767	18.8%	93,315	21.8%	411,430	21.4%
phish	3	0.1%	16	0.0%	52	0.0%	286	0.0%
safe	3,331	72.3%	77,939	78.0%	325,603	76.0%	1,475,379	76.7%
spam	5	0.1%	728	0.7%	1,231	0.3%	2,628	0.1%
spam_definite	24	0.5%	139	0.1%	859	0.2%	4,519	0.2%
malware	0	0.0%	0	0.0%	6	0.0%	174	0.0%
suspect	0	0.0%	0	0.0%	0	0.0%	5	0.0%
Total	4,606	100%	99,978	100%	428,588	100%	1,923,927	99.9%

Findings (SPAM)	For the past 7 days: **6** email(s) were identified as malware. **52 emails** were identified as phishing emails, this indicates an decrease from yesterday's records. **1231 mails** were identified as spam emails, indicating an increase from yesterday's records. **325 603** emails were recorded as safe.

c. Virus Protection Summary



VIRUS PROTECTION SUMMARY

Rule ID	Last 4 Hours	Last 24 Hours	Last 7 Days	Last 30 Days
Viruses Detected	472	1,667	18,339	48,168

Rank	Top Viruses	Last 7 Days
1	protected	19,437
2	trojan.tr/ad.gensteal.vezkj	1
3	trojan.tr/ad.gensteal.dkahz	1

Findings (VIRUS)	The Proofpoint solution managed to detect and block a total of **19,437** viruses in the last **7 days.**
Comments	All the viruses were detected and cleaned by Proof point.

Risk Indicators: Information Security Daily Checklist

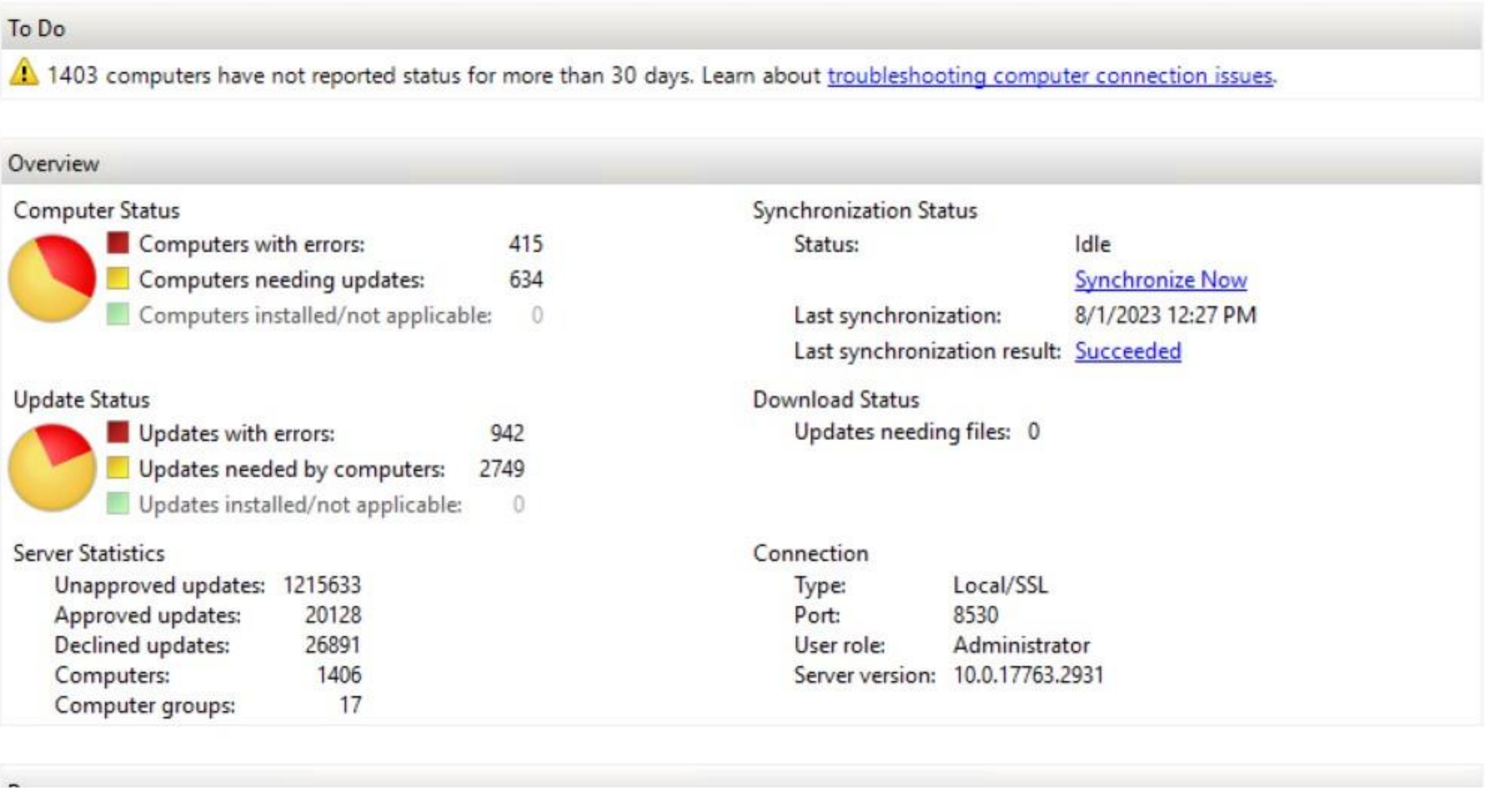
d. Reported Phishing Emails

Date	**Count**
Sunday	**0**
Monday	**0**
Tuesday	**0**
Wednesday	**0**
Thursday	
Friday	
Saturday	
Total	**0**

Findings	**0** spam/phishing email(s) was reported as at **22/05/24.**
Comment	The total weekly count of reported phishing emails is **0**. All the reported phishing/spam emails were manually blocked on the email gateway at the time of reporting.

Risk Indicators: Information Security Daily Checklist

6. **Windows Server Update Services (WSUS)**	
Description	
Control Objective	- To check for the effectiveness of the enterprise windows security updates and to identify any anomalies/exceptions that may need to be addressed manually and further investigate/interrogate persistent and recurring threats.
a. WSUS Dashboard	



To Do

⚠ 1403 computers have not reported status for more than 30 days. Learn about troubleshooting computer connection issues.

Overview

Computer Status

🟥 Computers with errors:	415
🟨 Computers needing updates:	634
🟩 Computers installed/not applicable:	0

Synchronization Status

Status:	Idle Synchronize Now
Last synchronization:	8/1/2023 12:27 PM
Last synchronization result:	Succeeded

Update Status

🟥 Updates with errors:	942
🟨 Updates needed by computers:	2749
🟩 Updates installed/not applicable:	0

Download Status

Updates needing files:	0

Server Statistics

Unapproved updates:	1215633
Approved updates:	20128
Declined updates:	26891
Computers:	1406
Computer groups:	17

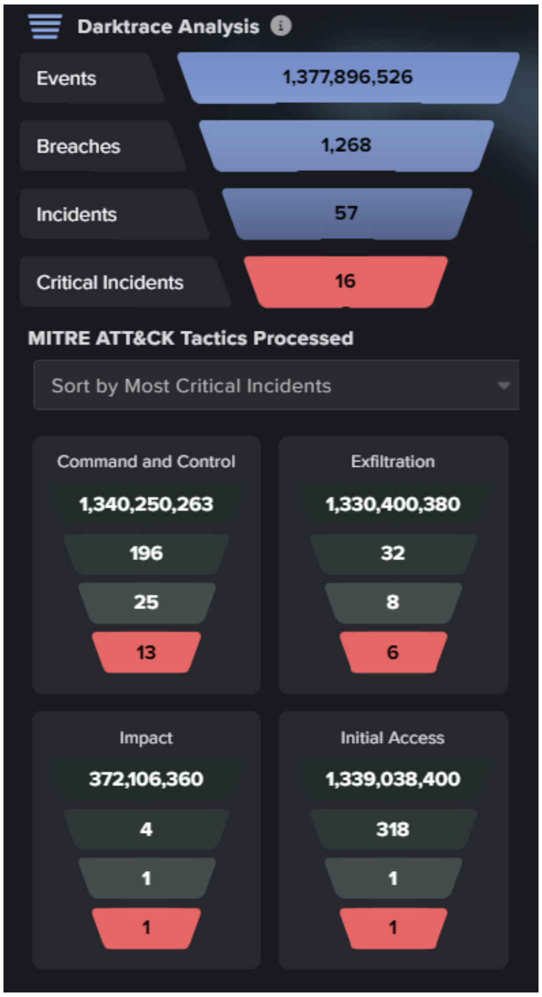
Connection

Type:	Local/SSL
Port:	8530
User role:	Administrator
Server version:	10.0.17763.2931

Findings	There are **415** machines with Windows update errors in total. **634** machines require updates. The total number of updates that must be installed on the machines **are 2749**
Comment	Server currently out of service and planned for decommissioning in favour of M365 Intune patch-management.

Risk Indicators: Information Security Daily Checklist

7. Darktrace	
Description	This is a Cyber AI Incident Analyst that has self-learning technology to detect and autonomously responds to cyber-attacks in real time.
Control Objective	Darktrace AI interrupts in-progress cyber-attacks in seconds, including ransomware, email phishing, and threats to cloud environments and critical infrastructure



Darktrace Analysis

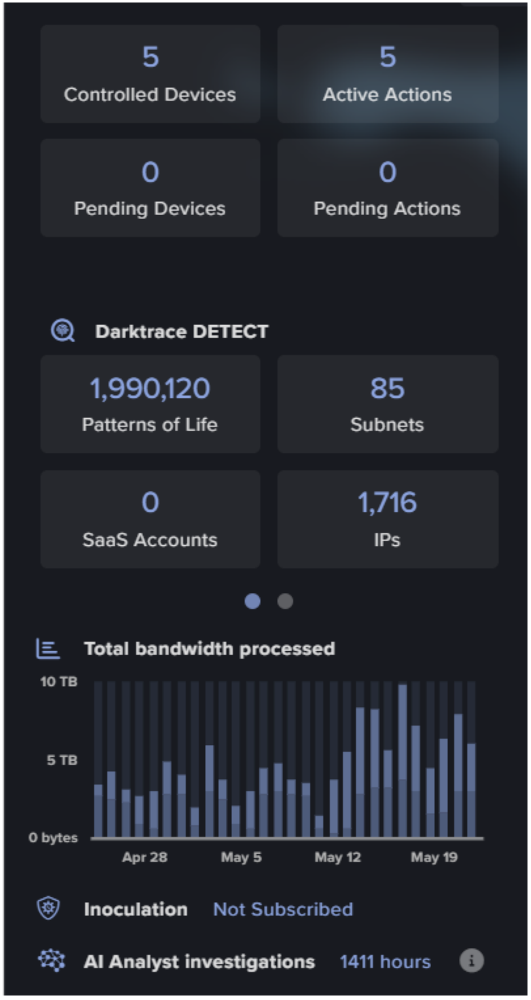
Events	1,377,896,526
Breaches	1,268
Incidents	57
Critical Incidents	16

MITRE ATT&CK Tactics Processed

Sort by Most Critical Incidents

Command and Control	Exfiltration
1,340,250,263	1,330,400,380
196	32
25	8
13	6

Impact	Initial Access
372,106,360	1,339,038,400
4	318
1	1
1	1



5 Controlled Devices	5 Active Actions
0 Pending Devices	0 Pending Actions

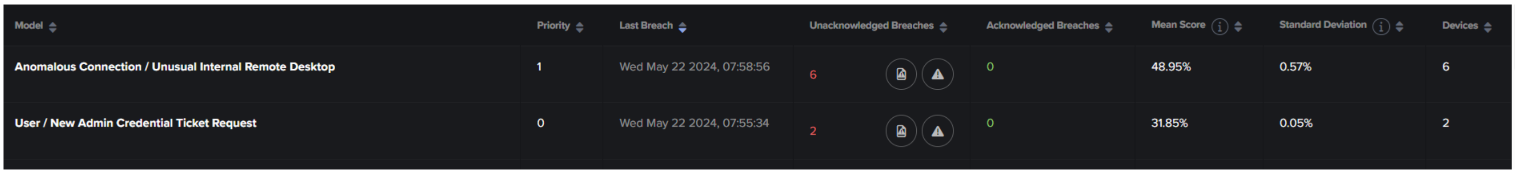
Darktrace DETECT

1,990,120 Patterns of Life	85 Subnets
0 SaaS Accounts	1,716 IPs

Total bandwidth processed

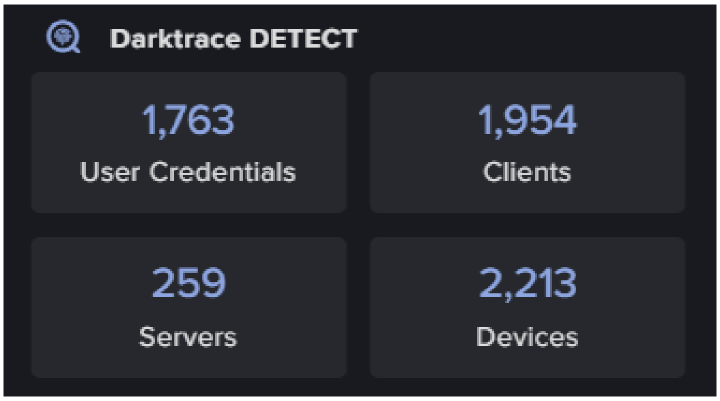
Inoculation Not Subscribed

AI Analyst investigations 1411 hours



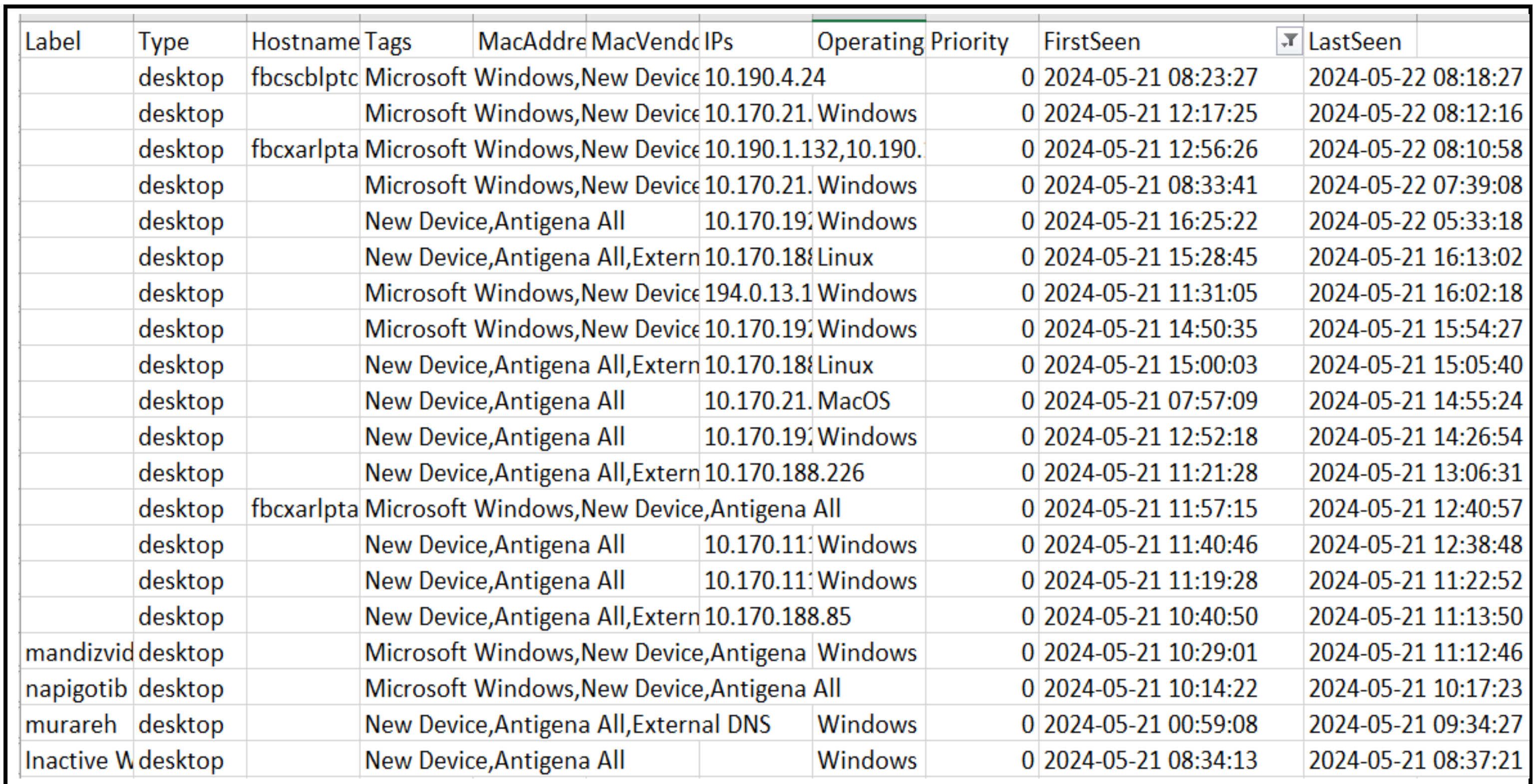
Model	Priority	Last Breach	Unacknowledged Breaches	Acknowledged Breaches	Mean Score	Standard Deviation	Devices
Anomalous Connection / Unusual Internal Remote Desktop	1	Wed May 22 2024, 07:58:56	6	0	48.95%	0.57%	6
User / New Admin Credential Ticket Request	0	Wed May 22 2024, 07:55:34	2	0	31.85%	0.05%	2

Risk Indicators: Information Security Daily Checklist

Findings	The AI Analyst summarizes possible attacks or threats from devices connected on the FBC network. **1268 breaches** were discovered, which translates to **57 incidents** with **16 critical incidents.** Darktrace DETECT 1,763 User Credentials 1,954 Clients 259 Servers 2,213 Devices **2213 client machines** are connected and are being monitored on Darktrace as at **22/05/2024 .** **259 servers** are connected and are being monitored on Darktrace as at **22/05/2024.**
Comment	Antigena is blocking or quarantining machines discovered to have possible breaches.

8. Darktrace New devices on the network.	
Description	Device admin lists all "devices" actively observed and modelled for pattern of life by Darktrace DETECT in the last six months. Devices in this context include network devices observed through network monitoring (both on premise and cloud), entities created by a Darktrace integration such as the TSA, device monitored a Darktrace/Endpoint cSensor agent, and users created by a Darktrace/Apps, Cloud or Zero trust module.
Control Objective	To check for new devices connected on FBC Network Infrastructure.

Risk Indicators: Information Security Daily Checklist

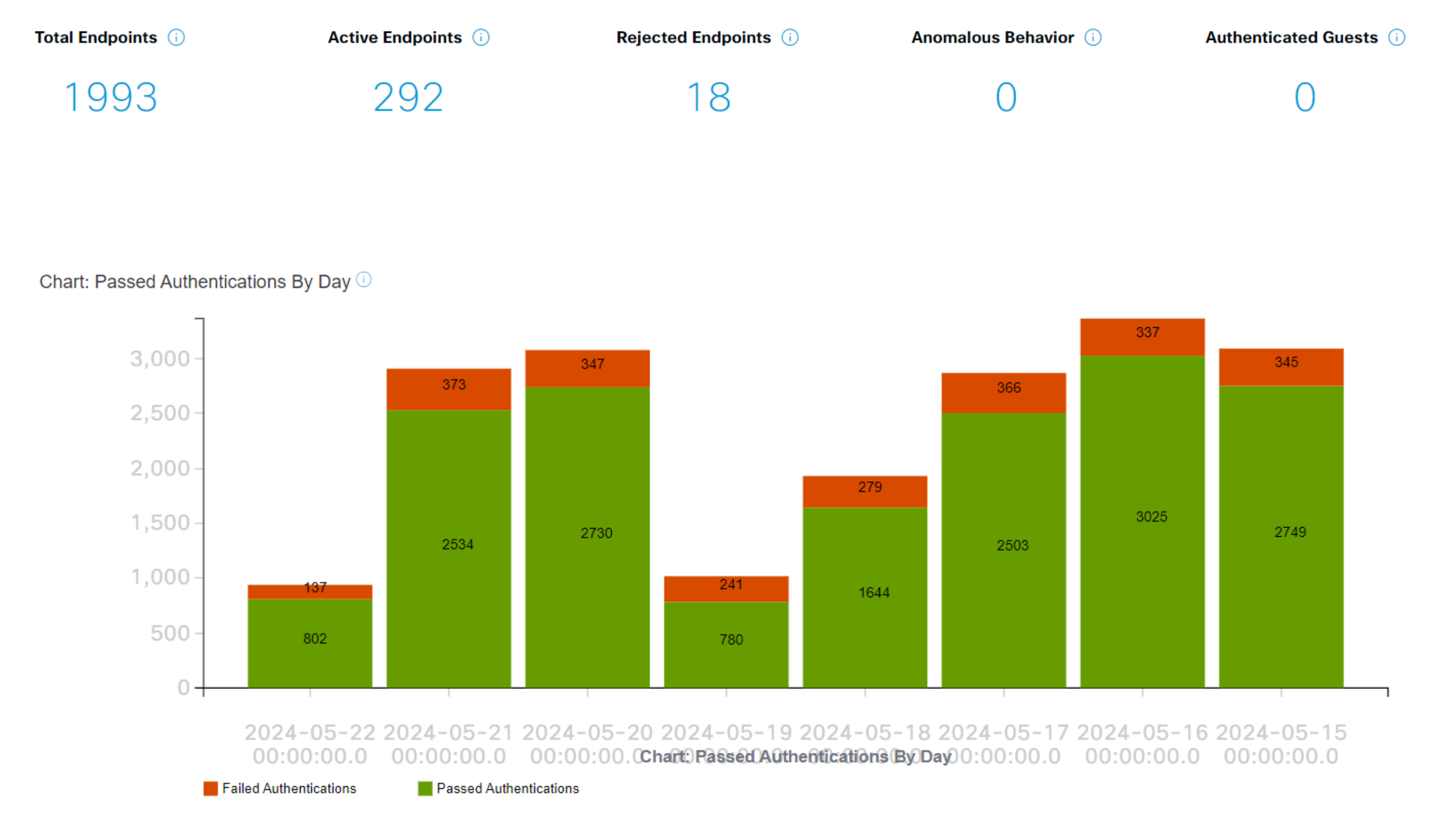


Label	Type	Hostname	Tags	MacAddre	MacVendc	IPs	Operating	Priority	FirstSeen	LastSeen
	desktop	fbcscblptc	Microsoft Windows,New Device			10.190.4.24		0	2024-05-21 08:23:27	2024-05-22 08:18:27
	desktop		Microsoft Windows,New Device			10.170.21.	Windows	0	2024-05-21 12:17:25	2024-05-22 08:12:16
	desktop	fbcxarlpta	Microsoft Windows,New Device			10.190.1.132,10.190.		0	2024-05-21 12:56:26	2024-05-22 08:10:58
	desktop		Microsoft Windows,New Device			10.170.21.	Windows	0	2024-05-21 08:33:41	2024-05-22 07:39:08
	desktop		New Device,Antigena All			10.170.19	Windows	0	2024-05-21 16:25:22	2024-05-22 05:33:18
	desktop		New Device,Antigena All,Extern			10.170.18	Linux	0	2024-05-21 15:28:45	2024-05-21 16:13:02
	desktop		Microsoft Windows,New Device			194.0.13.1	Windows	0	2024-05-21 11:31:05	2024-05-21 16:02:18
	desktop		Microsoft Windows,New Device			10.170.19	Windows	0	2024-05-21 14:50:35	2024-05-21 15:54:27
	desktop		New Device,Antigena All,Extern			10.170.18	Linux	0	2024-05-21 15:00:03	2024-05-21 15:05:40
	desktop		New Device,Antigena All			10.170.21.	MacOS	0	2024-05-21 07:57:09	2024-05-21 14:55:24
	desktop		New Device,Antigena All			10.170.19	Windows	0	2024-05-21 12:52:18	2024-05-21 14:26:54
	desktop		New Device,Antigena All,Extern			10.170.188.226		0	2024-05-21 11:21:28	2024-05-21 13:06:31
	desktop	fbcxarlpta	Microsoft Windows,New Device,Antigena All					0	2024-05-21 11:57:15	2024-05-21 12:40:57
	desktop		New Device,Antigena All			10.170.11	Windows	0	2024-05-21 11:40:46	2024-05-21 12:38:48
	desktop		New Device,Antigena All			10.170.11	Windows	0	2024-05-21 11:19:28	2024-05-21 11:22:52
	desktop		New Device,Antigena All,Extern			10.170.188.85		0	2024-05-21 10:40:50	2024-05-21 11:13:50
mandizvid	desktop		Microsoft Windows,New Device,Antigena				Windows	0	2024-05-21 10:29:01	2024-05-21 11:12:46
napigotib	desktop		Microsoft Windows,New Device,Antigena All					0	2024-05-21 10:14:22	2024-05-21 10:17:23
murareh	desktop		New Device,Antigena All,External DNS				Windows	0	2024-05-21 00:59:08	2024-05-21 09:34:27
Inactive W	desktop		New Device,Antigena All				Windows	0	2024-05-21 08:34:13	2024-05-21 08:37:21

Findings	Darktrace identified **20** new device(s) on the network as of **22 May 2024**.
Comment	The recently discovered devices have valid IP address.

Risk Indicators: Information Security Daily Checklist

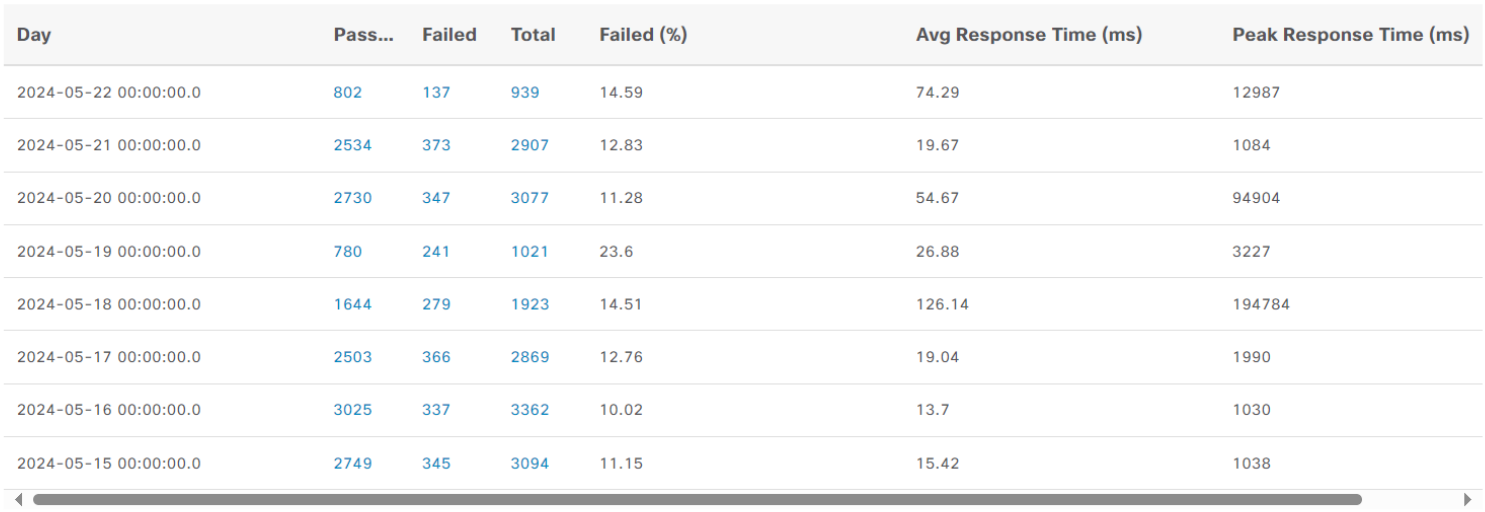
9. CISCO ISE Device – Network Access Administration (NAC)	
Description	- Network access control (NAC) is a security solution that enforces policy on devices that access networks to increase network visibility and reduce risk.
Control Objective	- To identify unauthorized access to network devices and to check for the effectiveness of the security solution and identify any anomalies/exceptions that may need to be addressed manually and further investigate/interrogate persistent and recurring threats.
Unauthorized Access to Local Area Network (LAN) or Ethernet connection	



Total Endpoints	Active Endpoints	Rejected Endpoints	Anomalous Behavior	Authenticated Guests
1993	292	18	0	0

Chart: Passed Authentications By Day

Risk Indicators: Information Security Daily Checklist



Day	Pass...	Failed	Total	Failed (%)	Avg Response Time (ms)	Peak Response Time (ms)
2024-05-22 00:00:00.0	802	137	939	14.59	74.29	12987
2024-05-21 00:00:00.0	2534	373	2907	12.83	19.67	1084
2024-05-20 00:00:00.0	2730	347	3077	11.28	54.67	94904
2024-05-19 00:00:00.0	780	241	1021	23.6	26.88	3227
2024-05-18 00:00:00.0	1644	279	1923	14.51	126.14	194784
2024-05-17 00:00:00.0	2503	366	2869	12.76	19.04	1990
2024-05-16 00:00:00.0	3025	337	3362	10.02	13.7	1030
2024-05-15 00:00:00.0	2749	345	3094	11.15	15.42	1038

Findings	**802** successful and **137** failed network authentication sessions from client machines were recorded for the past **24 hours.**
Comment	All failed network authentication sessions from different client machines were due to expired user passwords, locked user account profiles, expired user profiles on the domain and network timeout.

10. CISCO AAA Device – Network Device Administration	
Description	- This is a network device that provides Authentication, Authorization and Accounting network services for Network devices.
Control Objective	- To identify unauthorized access to network devices and to check for the effectiveness of the security solution and identify any anomalies/exceptions that may need to be addressed manually and further investigate/interrogate persistent and recurring threats.
Unauthorized Access to network devices	

Risk Indicators: Information Security Daily Checklist

Authentication Summary (7 days)

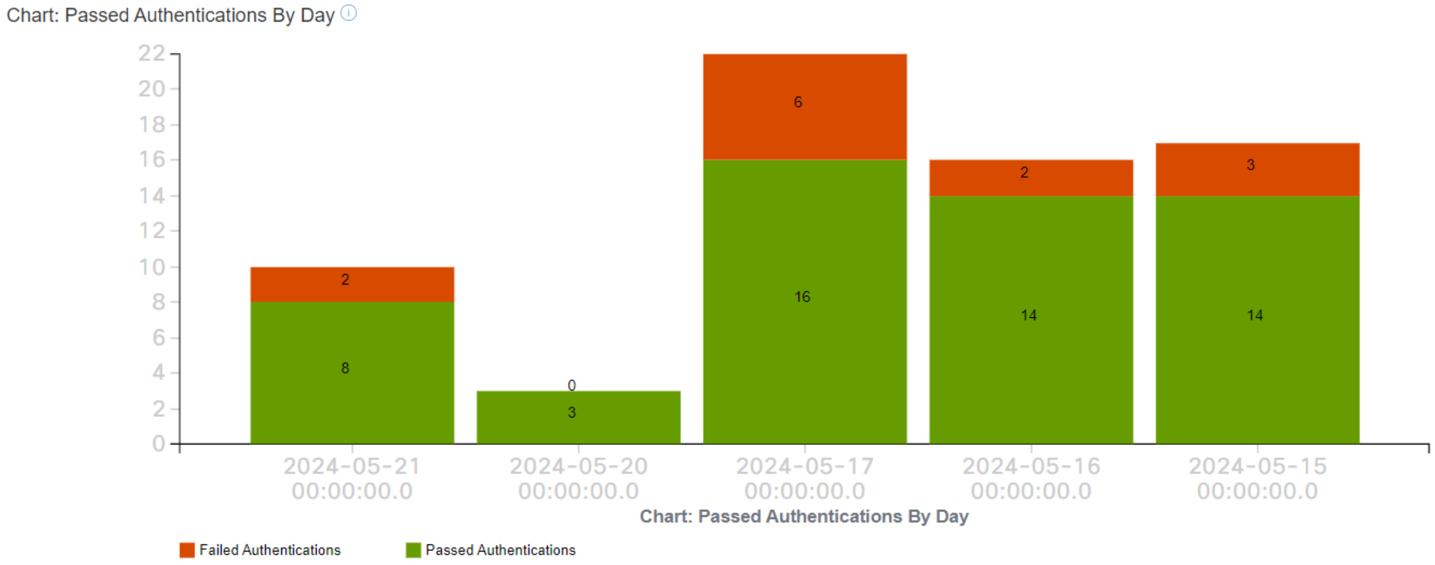
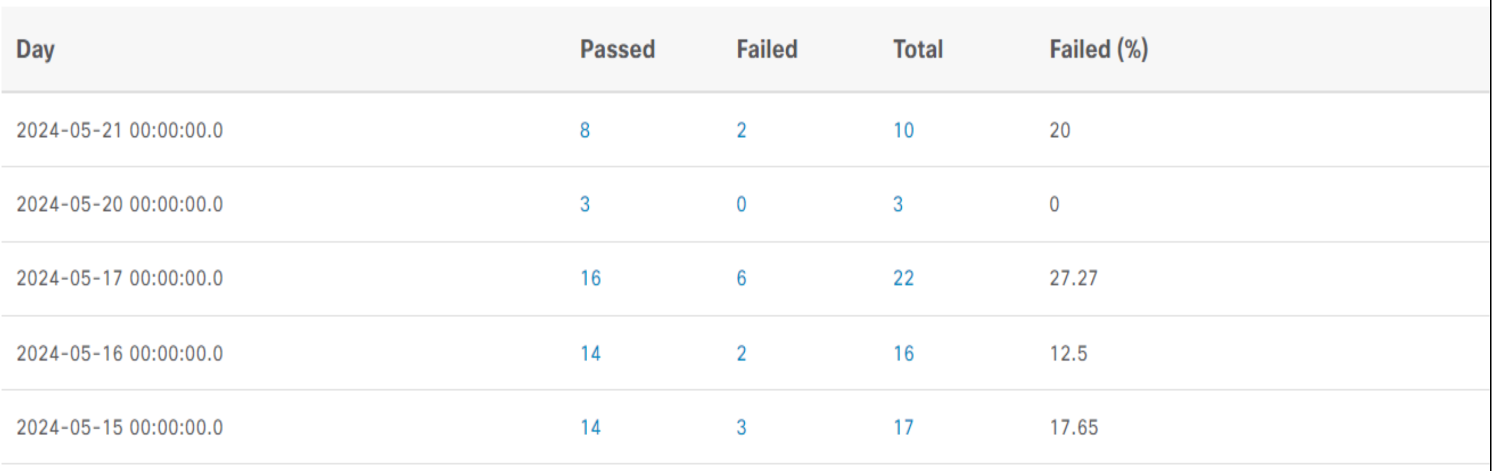


Chart: Passed Authentications By Day ⓘ

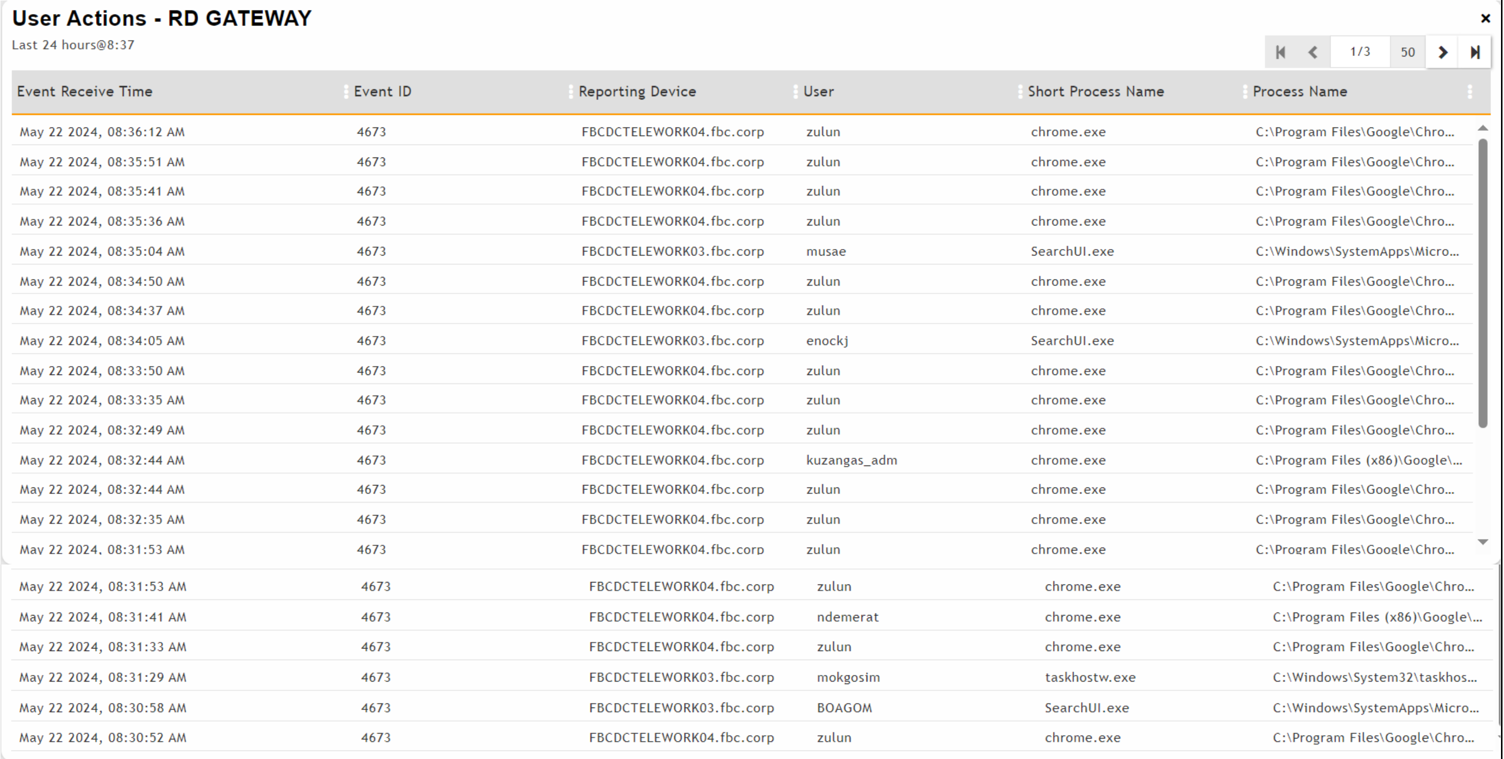


Day	Passed	Failed	Total	Failed (%)
2024-05-21 00:00:00.0	8	2	10	20
2024-05-20 00:00:00.0	3	0	3	0
2024-05-17 00:00:00.0	16	6	22	27.27
2024-05-16 00:00:00.0	14	2	16	12.5
2024-05-15 00:00:00.0	14	3	17	17.65

Findings	**8 Successful** and **2 failed** authentication attempts to network devices recorded in the past **24 hours.**
Comment	All failed attempts are due to domain or Active Directory non-existent user object or credentials being used to login to network devices.

Risk Indicators: Information Security Daily Checklist

11. RD Gateway Monitoring	
Description	- This is monitoring of remote users connecting via the gateway to access services remotely from home
Control Objective	- To verify if there are no unauthorized users connecting to FBC network.
User Activities.	



User Actions - RD GATEWAY

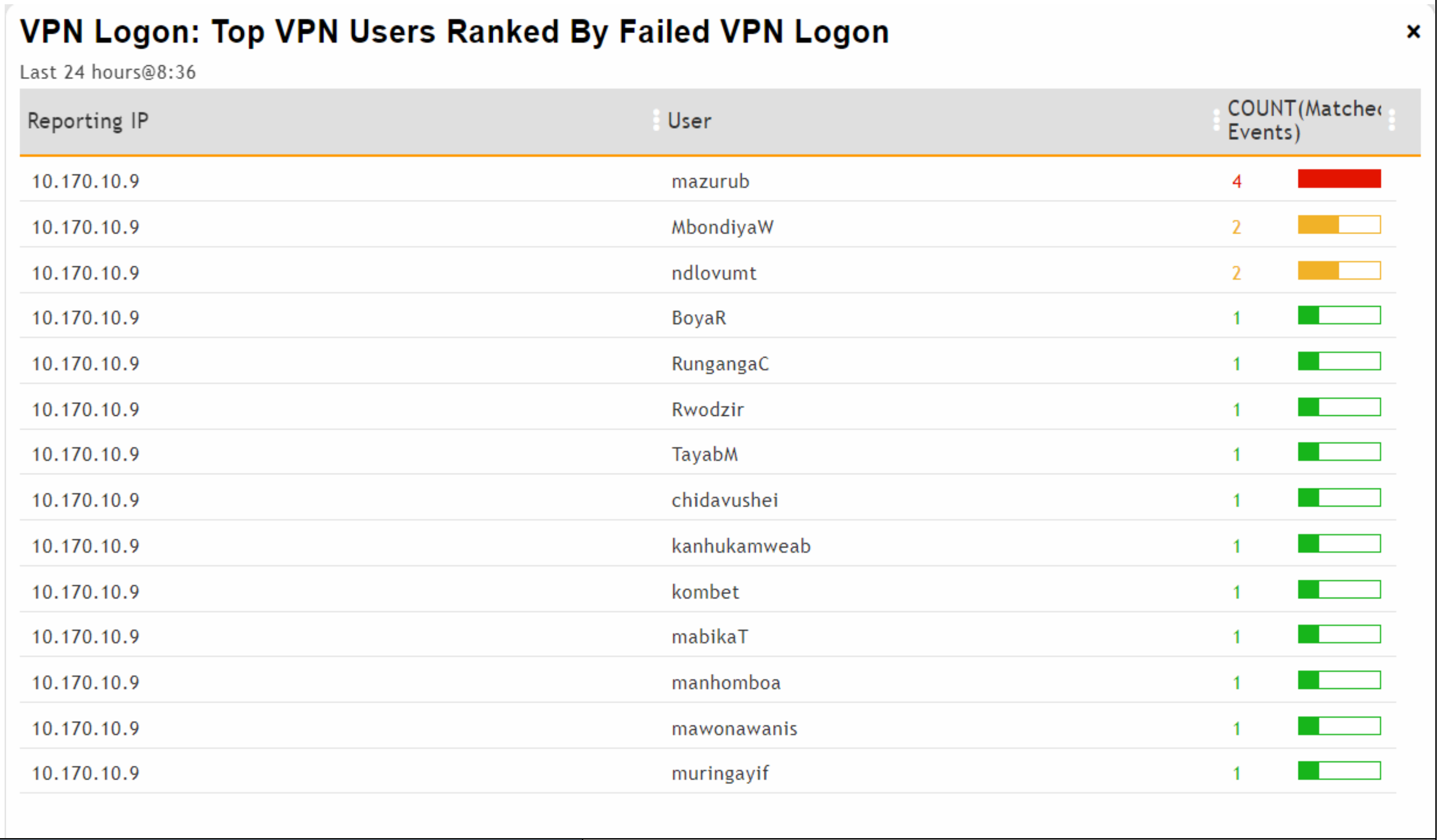
Last 24 hours@8:37

Event Receive Time	Event ID	Reporting Device	User	Short Process Name	Process Name
May 22 2024, 08:36:12 AM	4673	FBCDCTELEWORK04.fbc.corp	zulun	chrome.exe	C:\Program Files\Google\Chro...
May 22 2024, 08:35:51 AM	4673	FBCDCTELEWORK04.fbc.corp	zulun	chrome.exe	C:\Program Files\Google\Chro...
May 22 2024, 08:35:41 AM	4673	FBCDCTELEWORK04.fbc.corp	zulun	chrome.exe	C:\Program Files\Google\Chro...
May 22 2024, 08:35:36 AM	4673	FBCDCTELEWORK04.fbc.corp	zulun	chrome.exe	C:\Program Files\Google\Chro...
May 22 2024, 08:35:04 AM	4673	FBCDCTELEWORK03.fbc.corp	musae	SearchUI.exe	C:\Windows\SystemApps\Micro...
May 22 2024, 08:34:50 AM	4673	FBCDCTELEWORK04.fbc.corp	zulun	chrome.exe	C:\Program Files\Google\Chro...
May 22 2024, 08:34:37 AM	4673	FBCDCTELEWORK04.fbc.corp	zulun	chrome.exe	C:\Program Files\Google\Chro...
May 22 2024, 08:34:05 AM	4673	FBCDCTELEWORK03.fbc.corp	enockj	SearchUI.exe	C:\Windows\SystemApps\Micro...
May 22 2024, 08:33:50 AM	4673	FBCDCTELEWORK04.fbc.corp	zulun	chrome.exe	C:\Program Files\Google\Chro...
May 22 2024, 08:33:35 AM	4673	FBCDCTELEWORK04.fbc.corp	zulun	chrome.exe	C:\Program Files\Google\Chro...
May 22 2024, 08:32:49 AM	4673	FBCDCTELEWORK04.fbc.corp	zulun	chrome.exe	C:\Program Files\Google\Chro...
May 22 2024, 08:32:44 AM	4673	FBCDCTELEWORK04.fbc.corp	kuzangas_adm	chrome.exe	C:\Program Files (x86)\Google\...
May 22 2024, 08:32:44 AM	4673	FBCDCTELEWORK04.fbc.corp	zulun	chrome.exe	C:\Program Files\Google\Chro...
May 22 2024, 08:32:35 AM	4673	FBCDCTELEWORK04.fbc.corp	zulun	chrome.exe	C:\Program Files\Google\Chro...
May 22 2024, 08:31:53 AM	4673	FBCDCTELEWORK04.fbc.corp	zulun	chrome.exe	C:\Program Files\Google\Chro...
May 22 2024, 08:31:53 AM	4673	FBCDCTELEWORK04.fbc.corp	zulun	chrome.exe	C:\Program Files\Google\Chro...
May 22 2024, 08:31:41 AM	4673	FBCDCTELEWORK04.fbc.corp	ndemerat	chrome.exe	C:\Program Files (x86)\Google\...
May 22 2024, 08:31:33 AM	4673	FBCDCTELEWORK04.fbc.corp	zulun	chrome.exe	C:\Program Files\Google\Chro...
May 22 2024, 08:31:29 AM	4673	FBCDCTELEWORK03.fbc.corp	mokgosim	taskhostw.exe	C:\Windows\System32\taskhos...
May 22 2024, 08:30:58 AM	4673	FBCDCTELEWORK03.fbc.corp	BOAGOM	SearchUI.exe	C:\Windows\SystemApps\Micro...
May 22 2024, 08:30:52 AM	4673	FBCDCTELEWORK04.fbc.corp	zulun	chrome.exe	C:\Program Files\Google\Chro...

Findings	**6** privileged user accounts accessed RD gateway in the past **24 hrs**.
Comment	All user sessions are connecting successfully on the RD Gateway to access work resources.

Risk Indicators: Information Security Daily Checklist

12. VPN connections monitoring	
Description	- This is monitoring of remote users connecting via VPN to access services remotely from home
Control Objective	- To verify if there are no unauthorized users connecting to FBC network.
Login sessions	



VPN Logon: Top VPN Users Ranked By Failed VPN Logon

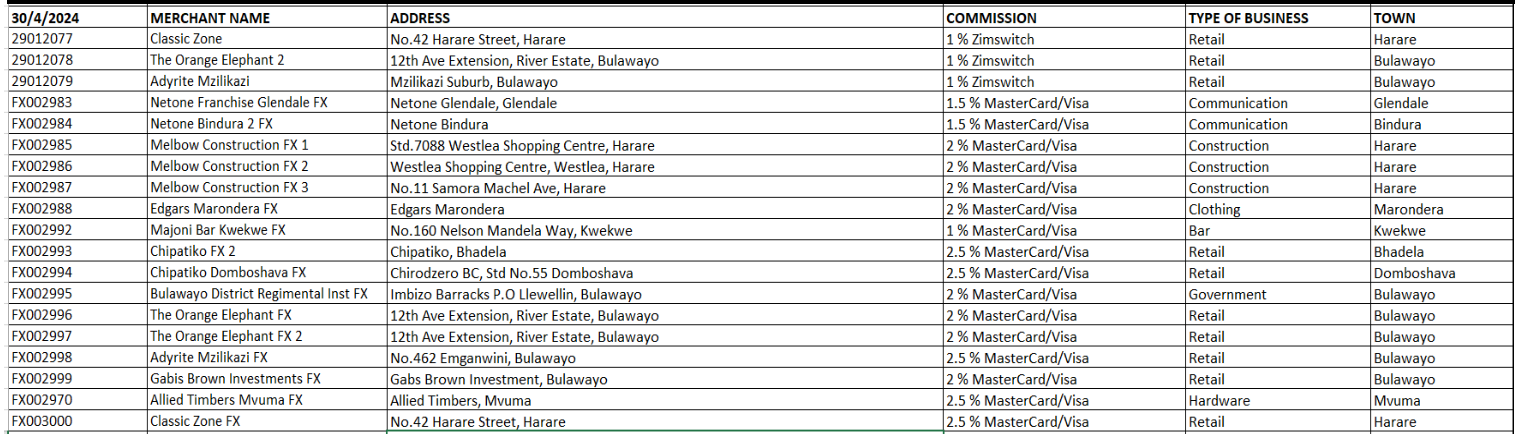
Last 24 hours@8:36

Reporting IP	User	COUNT(Matche Events)
10.170.10.9	mazurub	4
10.170.10.9	MbondiyaW	2
10.170.10.9	ndlovumt	2
10.170.10.9	BoyaR	1
10.170.10.9	RungangaC	1
10.170.10.9	Rwodzir	1
10.170.10.9	TayabM	1
10.170.10.9	chidavushei	1
10.170.10.9	kanhukamweab	1
10.170.10.9	kombet	1
10.170.10.9	mabikaT	1
10.170.10.9	manhomboa	1
10.170.10.9	mawonawanis	1
10.170.10.9	muringayif	1

Findings	A total of **19** failed VPN logon attempts were recorded on SIEM. The highest number of unsuccessful login attempts was **4.**
Comment	No unauthorized / unknown login attempts.

Risk Indicators: Information Security Daily Checklist

12. POS Terminal Configurations	
Description	- This is a process of checking maintenances for all newly created or re-assigned POS terminals (Merchant and Branch POS)
Control Objective	- To verify if there are any missing configurations that may lead to financial loss to the organization.



30/4/2024	MERCHANT NAME	ADDRESS	COMMISSION	TYPE OF BUSINESS	TOWN
29012077	Classic Zone	No.42 Harare Street, Harare	1 % Zimswitch	Retail	Harare
29012078	The Orange Elephant 2	12th Ave Extension, River Estate, Bulawayo	1 % Zimswitch	Retail	Bulawayo
29012079	Adyrite Mzilikazi	Mzilikazi Suburb, Bulawayo	1 % Zimswitch	Retail	Bulawayo
FX002983	Netone Franchise Glendale FX	Netone Glendale, Glendale	1.5 % MasterCard/Visa	Communication	Glendale
FX002984	Netone Bindura 2 FX	Netone Bindura	1.5 % MasterCard/Visa	Communication	Bindura
FX002985	Melbow Construction FX 1	Std.7088 Westlea Shopping Centre, Harare	2 % MasterCard/Visa	Construction	Harare
FX002986	Melbow Construction FX 2	Westlea Shopping Centre, Westlea, Harare	2 % MasterCard/Visa	Construction	Harare
FX002987	Melbow Construction FX 3	No.11 Samora Machel Ave, Harare	2 % MasterCard/Visa	Construction	Harare
FX002988	Edgars Marondera FX	Edgars Marondera	2 % MasterCard/Visa	Clothing	Marondera
FX002992	Majoni Bar Kwekwe FX	No.160 Nelson Mandela Way, Kwekwe	1 % MasterCard/Visa	Bar	Kwekwe
FX002993	Chipatiko FX 2	Chipatiko, Bhadela	2.5 % MasterCard/Visa	Retail	Bhadela
FX002994	Chipatiko Domboshava FX	Chirodzero BC, Std No.55 Domboshava	2.5 % MasterCard/Visa	Retail	Domboshava
FX002995	Bulawayo District Regimental Inst FX	Imbizo Barracks P.O Llewellin, Bulawayo	2 % MasterCard/Visa	Government	Bulawayo
FX002996	The Orange Elephant FX	12th Ave Extension, River Estate, Bulawayo	2 % MasterCard/Visa	Retail	Bulawayo
FX002997	The Orange Elephant FX 2	12th Ave Extension, River Estate, Bulawayo	2 % MasterCard/Visa	Retail	Bulawayo
FX002998	Adyrite Mzilikazi FX	No.462 Emganwini, Bulawayo	2.5 % MasterCard/Visa	Retail	Bulawayo
FX002999	Gabis Brown Investments FX	Gabs Brown Investment, Bulawayo	2 % MasterCard/Visa	Retail	Bulawayo
FX002970	Allied Timbers Mvuma FX	Allied Timbers, Mvuma	2.5 % MasterCard/Visa	Hardware	Mvuma
FX003000	Classic Zone FX	No.42 Harare Street, Harare	2.5 % MasterCard/Visa	Retail	Harare

Findings	POS machines deployed for the month of April.
Comment	The POS machines were last configured on **30/04/2024**. Verifications of accuracy of configuration on POS devices underway in liaison with the business.

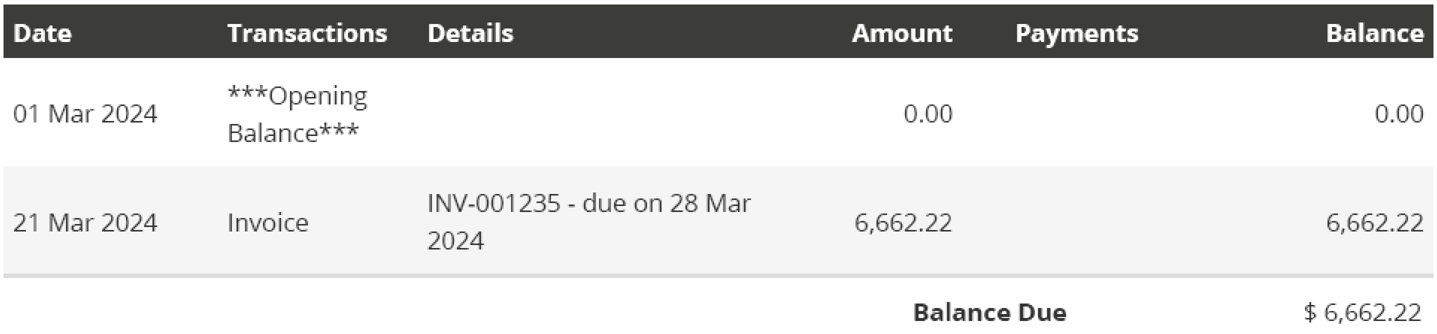
Risk Indicators: Information Security Daily Checklist

14. FBC SSL Certificate Balance	
Description	This is a process of checking the available balance which can be used for renewal of SSL certificates on Prima Secure.

	A POS Management Strategy is being developed to enable effective management of the POS infrastructure.

Risk Indicators: Information Security Daily Checklist

Control Objective	To track amount utilized on procurement of SSL certificates.
Prima Secure Remaining Balance	



Date	Transactions	Details	Amount	Payments	Balance
01 Mar 2024	***Opening Balance***		0.00		0.00
21 Mar 2024	Invoice	INV-001235 - due on 28 Mar 2024	6,662.22		6,662.22
				Balance Due	$ 6,662.22

'Findings	The current remaining balance to utilize for SSL certificates is at **$6,662.22** as at **18/04/2024 10:16hrs.**
Comment	Monthly tracking

15. Firewall Email Alerts

Description	This is a process of checking the number of firewall email alerts received each day
Control Objective	- To provide real-time analysis of security alerts generated by email

Risk Indicators: Information Security Daily Checklist

Email alerts

Day of the Week	Count
Sunday	209
Monday	210
Tuesday	133
Wednesday	72
Thursday	
Friday	
Saturday	
Total	**624**

Findings	**72** firewall email alerts were recorded on **22/05/2024.** The total weekly count of firewall alerts is **624.**
Comment	All threats were blocked by the firewall.

Created by: Patrick T. Siziba Date: 22/05/2024.... Signature: ....

Reviewed by: Nigel Baera Date: 22/05/2024.... Signature: ....