

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: 08 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
			zulun	CHIKAFUY	INSERT	1
			oracle	BIPDR1_BIPLATFORM	UPDATE	7
			chulua	FCPREPROD	UPDATE	1
						9

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	<u>ICT Generator Fuel Gauge:</u> □ 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)	No of event alerts for humidity and faults per week ≤ 2		• No anomalies reported on Checklist.
	<u>Uninterruptible Power Supply:</u> System monitored and operating within the boundaries and limits imposed by controls.	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
	○ <i>Ups Runtime Power = 2 hours 3 minutes</i>	% of charging capacity = 100%		
	○ <i>Ups Runtime Power = 1 hour 30 minutes</i>	% of Utilization Capacity ≥ 50 %		Utilization Capacity should be above 50 % for full utilization of the UPS
	<u>Fire Safety systems</u>	Amber / Red flashing lights		No Amber / Red flashing lights
	Heating, Ventilation, Air Conditioning and Cooling systems	<ul style="list-style-type: none"> • Amber / Red flashing lights for critical, warning faults. • No of event alerts for faults per week ≤ 2. • No of reported Events in the event Log. Number of Alarm Alerts per week do not to 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

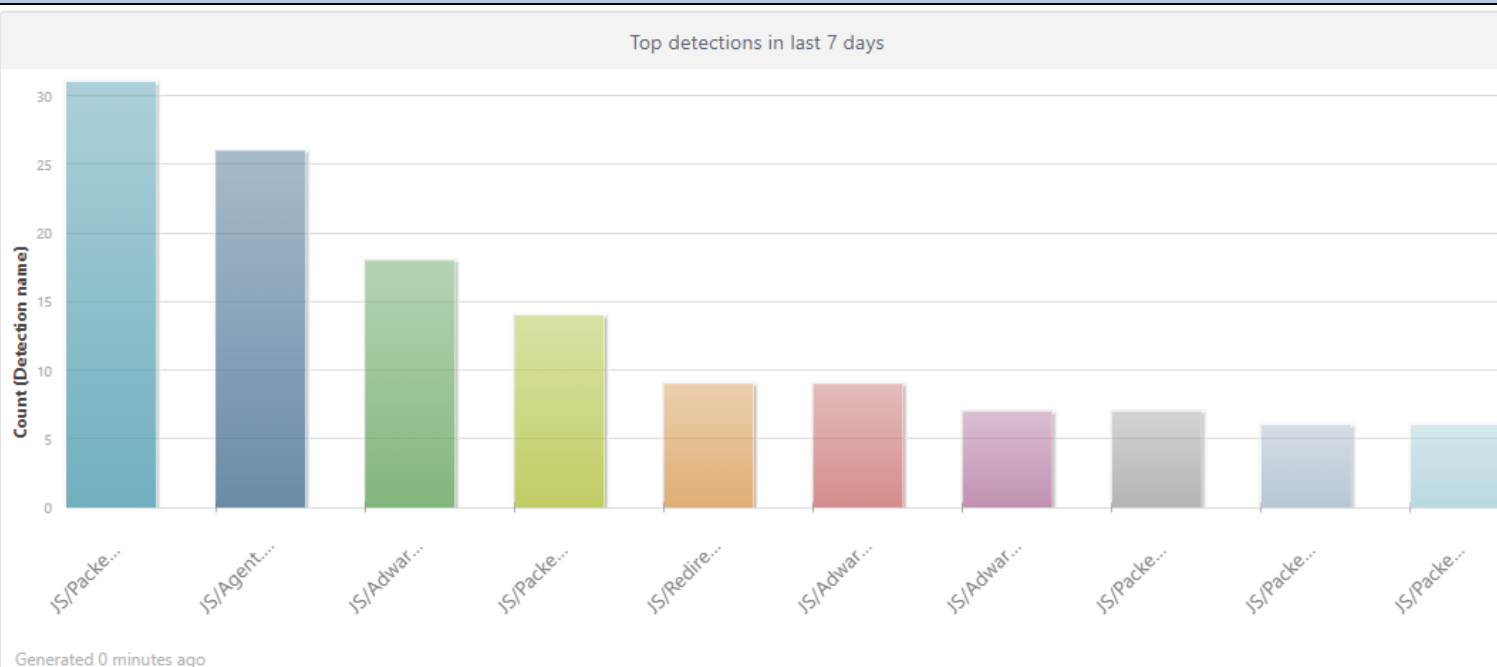
Access, Distribution and Modification of this document is prohibited unless you have been expressly authorized by FBC Executive Management or anyone with delegated authority.

Risk Indicators: Information Security Daily Checklist

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



Top detections in last 7 days

Group by (Detection name)	Count (Detection name)	Group by (Severity)	Group by (User)	Group by (IPv4 subnetwork)
JS/Packed.Agent.L	31	Warning	FBC\NdemeraT	194.0.7.0
JS/Agent.PHC	26	Warning	FBC\MuterereA	10.170.20.0
JS/Adware.Agent.CZ	18	Warning	FBC\dladlaa	10.170.20.0
JS/Packed.Agent.L	14	Warning	FBC\Adzikweyil	10.170.20.0
JS/Redirector.QKM	9	Warning	FBC\muromog	10.170.123.0
JS/Adware.Agent.CZ	9	Warning	FBC\mushongar	192.168.1.0
JS/Adware.TerraClicks.A	7	Warning	FBC\makonie	10.170.20.0
JS/Packed.Agent.L	7	Warning	FBC\moyosibs	10.170.20.0
JS/Packed.Agent.L	6	Warning	FBC\BodzoK	10.170.20.0
JS/Packed.Agent.L	6	Warning	FBC\mushongar	192.168.1.0

Findings	31 JS/Packed.Agent.L 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	JS/Packed.Agent.L are JavaScript files that have been obfuscated or packed in a way that make it difficult for traditional antivirus programs to analyze its contents. This type of detection may indicate the presence of malicious code or behavior within the JavaScript file.
---------	--

b. Overview of Antivirus Update Status													
	Monday		Tuesday		Wednesday		Thursday		Friday		Saturday		
AD TOTAL DEVICES				1623		1642							
Workstations				1405		1425							
MacBook				25		25							
Servers				193		192							
ESET Devices				1408		1406							
Workstations				1226		1225							
MacBooks				19		18							
Servers				163		163							
DLP DEVICES						1240							
workstations						1219							
Macbook						21							
	January	February	March	April	May	June	July	August					
AD Clean-up (Deleted Machines)	59	32	81										
ESET Version		Workstations		Servers		MacBook's							
Latest version		1116		93		4							
Lower version		109		70		14							
Total		1225		163		18							

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

Findings	<p>1406 devices or licenses have been recorded on ESET.</p> <p>1225 workstations recorded.</p> <ul style="list-style-type: none"> • 1116 are running ESET version 11 whilst 109 are on lower versions. <p>163 servers recorded. ESET updates pending restart to upgrade version.</p> <ul style="list-style-type: none"> • 93 are running ESET version 11 whilst 70 servers are running lower/outdated ESET version. <p>18 MacBook(s) recorded.</p> <ul style="list-style-type: none"> • 4 MacBook device is running the latest ESET version 7 and whilst 14 devices are running lower versions i.e. 6. <p>1240 devices have Data Leakage Protection (DLP)</p> <ul style="list-style-type: none"> • 1219 workstations have DLP. • 21 MacBooks have DLP installed.
Comments	<p>AD devices in need of cleanup initiated IT team. Problems of machines detected to be at security risk and those requiring attention are but not limited to:</p> <ul style="list-style-type: none"> • 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 : 56

Threat Score : 0

Action (Block/Alert) : 56

Service (HTTP/HTTPS) : 56

Time Period : Last 24 Hours

08:00:0010:00:0012:00:0014:00:0016:00:0018:00:0020:00:0022:00:0000:00:0002:00:0004:00:0006:00:00

BlockAlert

Sources

Countries

Client Devices

HTTP Methods

URLs






CVE ID

OWASP Top10

Source	Threats	Threat Score	Action (Block/Alert)	Service (HTTP/HTTPS)
87.121.105.25	5	0	5/0	3/2
185.224.128.43	5	0	5/0	5/0
152.32.247.130	4	0	4/0	4/0
184.105.247.195	3	0	3/0	3/0
146.19.24.28	3	0	3/0	3/0
64.62.156.49	3	0	3/0	3/0
183.200.61.155	2	0	2/0	0/2
123.152.208.108	2	0	2/0	0/2
71.6.134.235	2	0	2/0	2/0
165.227.108.239	2	0	2/0	2/0
25.205.205.150	1	0	1/0	0/1
[Total: 35]				

#	Date/Time	Policy	Source	Destination	Threat Level	Action	Message	HTTP Host	URL
1	05-07 17:50	FBC_IB_OBDX	87.121.105.25	10.170.3.60	Off	Alert_Deny	HTTP Host Violation	196.216.224.10	/vendor/phpunit/phpunit/src/Util/F
2	05-07 17:50	FBC_IB_OBDX	87.121.105.25	10.170.3.60	Off	Alert_Deny	HTTP Host Violation	196.216.224.10	/
3	05-07 17:50	FBC_IB_OBDX	87.121.105.25	10.170.3.60	Off	Alert_Deny	HTTP Host Violation	196.216.224.10	/.env
4	05-07 17:50	FBC_IB_OBDX	87.121.105.25	10.170.3.60	Off	Alert_Deny	HTTP Host Violation	196.216.224.10	/
5	05-07 17:50	FBC_IB_OBDX	87.121.105.25	10.170.3.60	Off	Alert_Deny	HTTP Host Violation	196.216.224.10	/.env

Risk Indicators: Information Security Daily Checklist

#	Date/Time	Policy	Source	Destination	Threat Level	Action	Message	HTTP Host	URL
1	05:13:17	FBC_IB_OBDX	 185.224.128.43	10.170.3.60	Off	Alert_Deny	HTTP Host Violation	196.216.224.10	/
2	00:23:30	FBC_IB_OBDX	 185.224.128.43	10.170.3.60	Off	Alert_Deny	HTTP Host Violation	196.216.224.10	/
3	05-07 18:15	FBC_IB_OBDX	 185.224.128.43	10.170.3.60	Off	Alert_Deny	HTTP Host Violation	196.216.224.10	/
4	05-07 13:50	FBC_IB_OBDX	 185.224.128.43	10.170.3.60	Off	Alert_Deny	HTTP Host Violation	196.216.224.10	/
5	05-07 08:03	FBC_IB_OBDX	 185.224.128.43	10.170.3.60	Off	Alert_Deny	HTTP Host Violation	196.216.224.10	/
Findings				5 threats from external source IP 87.121.105.25 and 185.224.128.43 recorded the highest threat count. A total of 56 threats from 35 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					
<div><div><div>← Top Threats by Threat Level</div><div><div>🕒 24 hours</div><div>🔄</div><div>🔗</div><div>⋮</div></div></div><div><div>➕ Add Filter</div><div><div>150000 Threat Score</div><div>125000 Threat Score</div><div>100000 Threat Score</div><div>75000 Threat Score</div><div>50000 Threat Score</div><div>25000 Threat Score</div><div>0 Threat Score</div></div><div><div>08:00</div><div>10:00</div><div>12:00</div><div>14:00</div><div>16:00</div><div>18:00</div><div>20:00</div><div>22:00</div><div>00:00</div><div>02:00</div><div>04:00</div><div>06:00</div></div><div><div><div></div>Low</div><div><div></div>High</div><div><div></div>Critical</div></div></div></div>					
Threat		Threat Category	Threat Level	Threat Score	Sessions
Realtek.SDK.UDP.Server.Command.Execution		ips	Critical	1,100	22
blocked-connection		Blocked Connection	High	305,550	10,185
failed-connection		Failed Connection	Low	742,795	148,559
Nessus.Scanner		ips	Low	215	43
Nmap.Script.Scanner		ips	Low	175	35
Wind.River.VxWorks.WDB.Debug.Service.Versi...		ips	Low	65	13
Port.Scanning		ips	Low	30	6
Findings		1 critical level threat, 1 high level threat, and 5 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		Module Version	
Quarantine	✔ Running	Spam MLX Engine	✔ 8.12.0-2405010000-240501_120659
Command Processor (Web)	✔ Running	Spam MLX Definitions	✔ main-2405080041
Quarantine Messages	57,705 (16.78 GB)	F-Secure Anti-Virus Engine	✔ 8.12.0C6-20293_240321_1348
		F-Secure Anti-Virus Definitions	✔ 64_05-08-24_04-55-01_BG

Server Summary

FBCDCPP01 (Config Master)
 Uptime: 07:52:52 up 64 day(s), 15:28, 0 user(s), load average: 1.02, 0.86, 0.94

☰

Services	Connections	Filter	Storage
Configuration ✔ In Sync	Current <div style="width: 100%; height: 10px; background: linear-gradient(to right, #007bff, #007bff);"></div> 0% (0 of 10000)	Uptime 11:10:49	CPU I/O Wait <div style="width: 100%; height: 10px; background: linear-gradient(to right, #007bff, #007bff);"></div> 0%
SMTP ✔ Running	Total 2186	Msg Count 491	Swap <div style="width: 100%; height: 10px; background: linear-gradient(to right, #007bff, #007bff);"></div> 26% Used (5.91G Avail)
Filter ✔ Running	Unique IPs 0	Msg Size 29.88 MB	System Disk Space <div style="width: 100%; height: 10px; background: linear-gradient(to right, #007bff, #007bff);"></div> 18% Used (9.08G Avail)
Filter ✔ Running	Throttled IPs 0 / 0 (Current / Total)	Msg Rate 0.054	Sendmail Msgs 0 / 0 (mail / system)
Repository ✔ Running		Recipients 531 / 531 (Valid / Total)	PPS Disk Space <div style="width: 100%; height: 10px; background: linear-gradient(to right, #007bff, #007bff);"></div> 25% Used (158.67G Avail)
Buffer Queues ✔ Running		Virus 0 / 0 (Infected / Skipped)	Buffer Queue Msgs 0 / 0 / 0 (default / alert / others)
API Service ✔ Running		Zero-Hour 0 / 0 / 0 (Virus / High / Med)	Quarantine Cache 0 Msgs

FBCDCPPA01 (Mail Filter) Sync Configuration
 Uptime: 07:52:44 up 64 day(s), 15:29, 0 user(s), load average: 0.91, 0.57, 0.48

☰

Services	Connections	Filter	Storage
Configuration ✘ Out of Sync Component out-of-sync: Spam MLX Definition, Virus Definitions	Current <div style="width: 100%; height: 10px; background: linear-gradient(to right, #007bff, #007bff);"></div> 0% (0 of 10000)	Uptime 10:59:10	CPU I/O Wait <div style="width: 100%; height: 10px; background: linear-gradient(to right, #007bff, #007bff);"></div> 0%
SMTP ✔ Running	Total 7873	Msg Count 7339	Swap <div style="width: 100%; height: 10px; background: linear-gradient(to right, #007bff, #007bff);"></div> 0% Used (8G Avail)
Filter ✔ Running	Unique IPs 0	Msg Size 792.91 MB	System Disk Space <div style="width: 100%; height: 10px; background: linear-gradient(to right, #007bff, #007bff);"></div> 20% Used (8.89G Avail)
Repository ✔ Running	Throttled IPs 0 / 0 (Current / Total)	Msg Rate 0.317	Sendmail Msgs 5569 / 0 (mail / system)
Buffer Queues ✔ Running		Recipients 9066 / 9066 (Valid / Total)	PPS Disk Space <div style="width: 100%; height: 10px; background: linear-gradient(to right, #007bff, #007bff);"></div> 48% Used (28.2G Avail)
		Virus 0 / 504 (Infected / Skipped)	Buffer Queue Msgs 0 / 0 / 0 (default / alert / others)
		Zero-Hour 0 / 1 / 0 (Virus / High / Med)	Quarantine Cache 1 Msgs

CLUSTER STATUS				Config Master FBCDCPP01.fbc.co.zw-10000_instance1				Updated 2024-05-08 07:58:20 [UTC+02:00] - 10					
0	0	57711		0	0	1.27		PPS Disk Space	<div style="width: 100%; height: 10px; background: linear-gradient(to right, #007bff, #007bff);"></div> 25% (159 GB Avail)	Swap	<div style="width: 100%; height: 10px; background: linear-gradient(to right, #007bff, #007bff);"></div> 26% (6 GB of 8 GB Avail)	Inodes Usage	<div style="width: 100%; height: 10px; background: linear-gradient(to right, #007bff, #007bff);"></div> 1% (14761392 of 14925824 Avail)
Msgs / sec	Connections	Quarantine Messages	FBCDCPP01	Msgs / sec	Connections	Load Average							

CLUSTER STATUS				Agent FBCDCPPA01.fbc.co.zw-10000_instance1				Updated 2024-05-08 07:58:37 [UTC+02:00] - 22					
0	1	57711		0	1	0.35		PPS Disk Space	<div style="width: 100%; height: 10px; background: linear-gradient(to right, #007bff, #007bff);"></div> 48% (28 GB Avail)	Swap	<div style="width: 100%; height: 10px; background: linear-gradient(to right, #007bff, #007bff);"></div> 0% (8 GB of 8 GB Avail)	Inodes Usage	<div style="width: 100%; height: 10px; background: linear-gradient(to right, #007bff, #007bff);"></div> 4% (3628955 of 3784704 Avail)
Msgs / sec	Connections	Quarantine Messages	FBCDCPPA01	Msgs / sec	Connections	Load Average							

Risk Indicators: Information Security Daily Checklist

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

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	0	0.0%	1,305	1.8%	4,038	1.0%	31,632	1.9%
malware	0	0.0%	5	0.0%	147	0.0%	165	0.0%
notspam	737	37.1%	15,139	20.8%	82,580	21.2%	349,337	21.1%
phish	0	0.0%	7	0.0%	52	0.0%	293	0.0%
safe	1,220	61.4%	56,085	77.1%	301,681	77.4%	1,264,083	76.5%
spam	2	0.1%	65	0.1%	298	0.1%	1,735	0.1%
spam_definite	29	1.5%	139	0.2%	776	0.2%	4,812	0.3%
suspect	0	0.0%	1	0.0%	1	0.0%	11	0.0%
Total	1,988	100%	72,746	100%	389,573	99.9%	1,652,068	99.9%

Findings (SPAM)

For the past 7 days:

147 email(s) were identified as malware.

52 emails were identified as phishing emails, this indicates an increase from yesterday's records.

298 mails were identified as spam emails, this indicates a slight decrease from yesterday's records.

301 681 emails were recorded as safe.

c. Virus Protection Summary

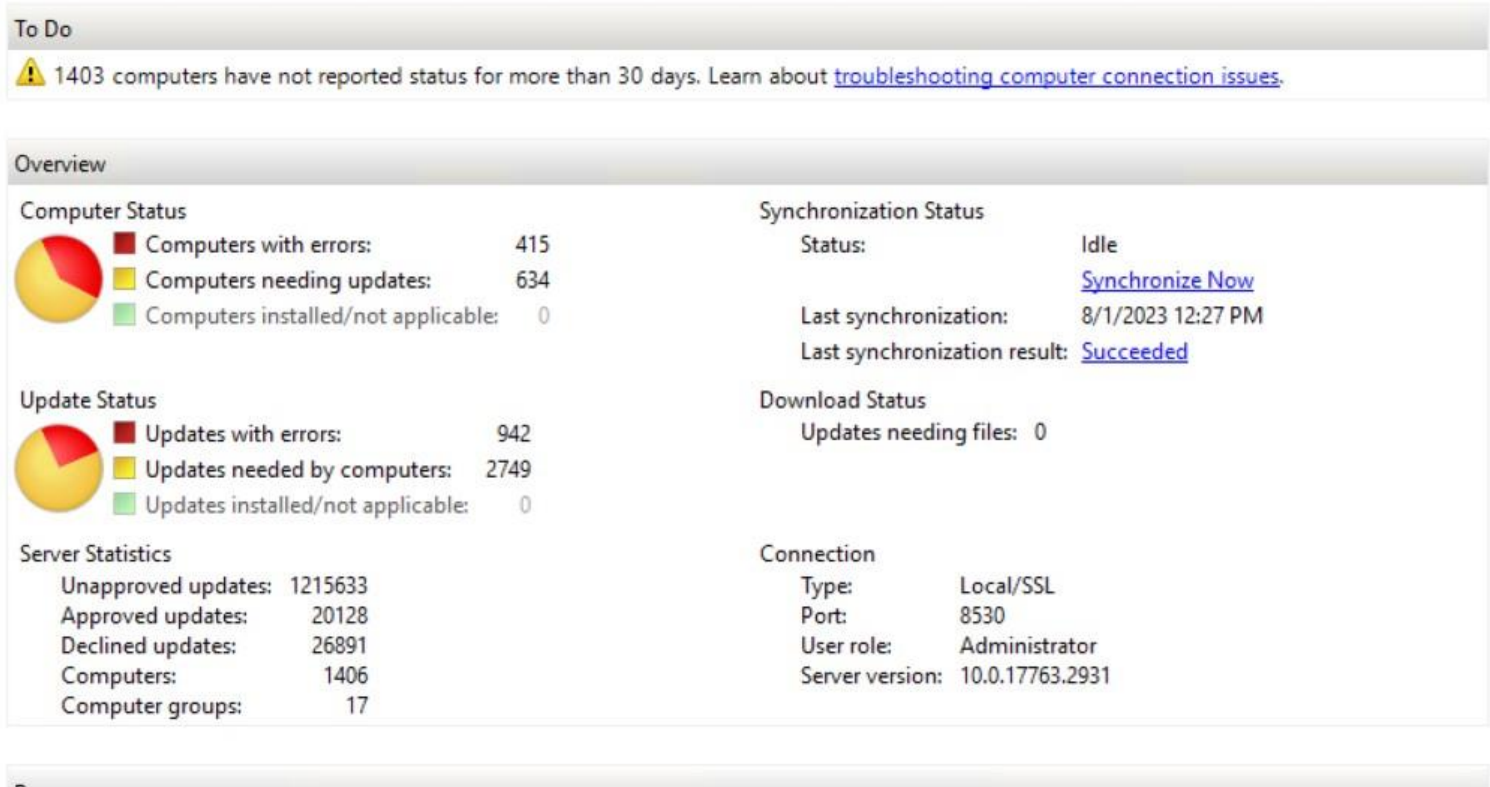
Risk Indicators: Information Security Daily Checklist

VIRUS PROTECTION SUMMARY					
Rule ID		Last 4 Hours	Last 24 Hours	Last 7 Days	Last 30 Days
Viruses Detected		318	1,667	9,167	25,019
Rank	Top Viruses			Last 7 Days	
1	protected			10,105	
2	malware.html/infected.webpage.ge			7	
3	trojan.tr/avi.agenttesla.lyfha			5	
4	trojan.tr/avi.agenttesla.uazdb			1	

Findings (VIRUS)	The Proofpoint solution managed to detect and block a total of 10 105 viruses in the last 7 days .
Comments	All the viruses were detected and cleaned by Proof point.

d. Reported Phishing Emails		
Date	Count	
Sunday	1	
Monday	0	
Tuesday	0	
Wednesday	0	
Thursday	0	
Friday	0	
Saturday	0	
Total	1	
Findings		1 spam/phishing email(s) was reported as at 08/05/24 .
Comment		The total weekly count of reported phishing emails is 1 . 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	
 <p>The screenshot displays the WSUS Dashboard with the following information:</p> <ul style="list-style-type: none"> To Do: 1403 computers have not reported status for more than 30 days. Learn about troubleshooting computer connection issues. Overview: <ul style="list-style-type: none"> Computer Status: <ul style="list-style-type: none"> Computers with errors: 415 Computers needing updates: 634 Computers installed/not applicable: 0 Update Status: <ul style="list-style-type: none"> Updates with errors: 942 Updates needed by computers: 2749 Updates installed/not applicable: 0 Server Statistics: <ul style="list-style-type: none"> Unapproved updates: 1215633 Approved updates: 20128 Declined updates: 26891 Computers: 1406 Computer groups: 17 Synchronization Status: <ul style="list-style-type: none"> Status: Idle Last synchronization: 8/1/2023 12:27 PM Last synchronization result: Succeeded Download Status: <ul style="list-style-type: none"> Updates needing files: 0 Connection: <ul style="list-style-type: none"> 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




Risk Indicators: Information Security Daily Checklist

Model	Priority	Last Breach	Unacknowledged Breaches	Acknowledged Breaches	Mean Score	Standard Deviation	Devices
Anomalous Connection / Unusual Internal Remote Desktop	1	Wed May 8 2024, 06:57:05	8	0	48.00%	1.67%	7
Anomalous File / Zip or Gzip from Rare External Location	1	Wed May 8 2024, 06:26:07	1	0	46.50%	0.00%	1
System / New Subnet Detected	0	Wed May 8 2024, 00:18:24	2	0	30.00%	0.00%	1

Findings

The AI Analyst summarizes possible attacks or threats from devices connected on the FBC network. **1121 breaches** were discovered, which translates to **58 incidents** with **14 critical incidents**.



1734 client machines are connected and are being monitored on Darktrace as at **08/05/2024 as at 0825 AM**.

283 servers are connected and are being monitored on Darktrace as at **08/04/2024**.

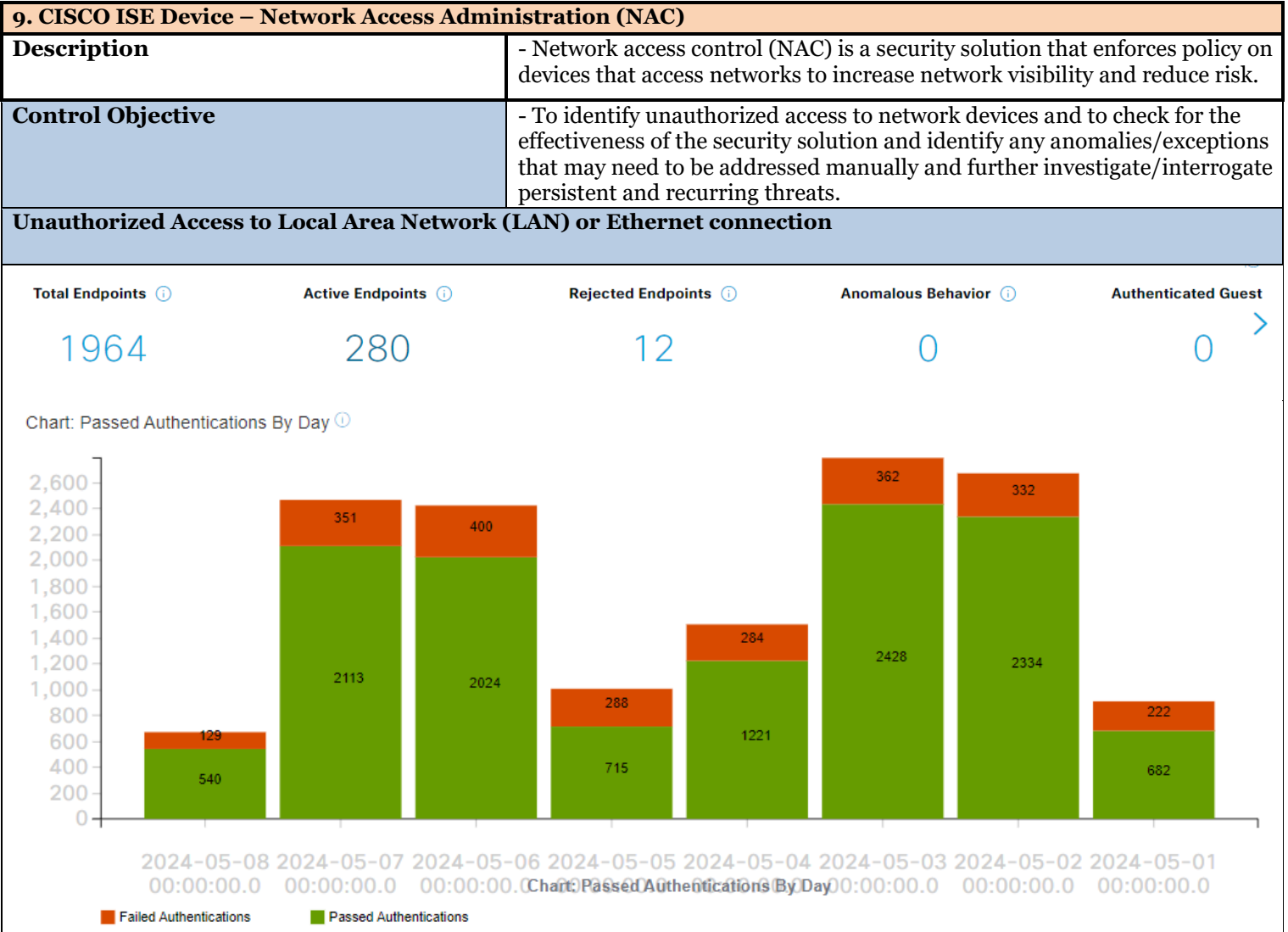
Comment

Antigena is blocking or quarantining machines discovered to have possible breaches.

Risk Indicators: Information Security Daily Checklist

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.							
Label	Type	Hostname	Tags	MacA	MacVend	IPs	Operating	Priority	FirstSeen	LastSeen	
	desktop		New Device,Antigena All			10.170.22.	Linux	0	2024-05-07 07:34:27	2024-05-08 07:34:01	
	desktop		New Device,Antigena All			10.170.22.177		0	2024-05-07 07:38:42	2024-05-07 13:17:04	
Inactive Window	desktop		Microsoft Windows,New Device,Antigena All				Windows	0	2024-05-07 07:53:13	2024-05-07 07:56:23	
kandat	desktop		Microsoft Windows,New Device,Antigena All				Windows	0	2024-05-07 06:52:44	2024-05-07 07:36:08	
Findings				Darktrace identified 4 new device(s) on the network as of the 7 th of 7 May 2024 as at 0837hrs .							
Comment				The recently discovered devices have valid IP address.							

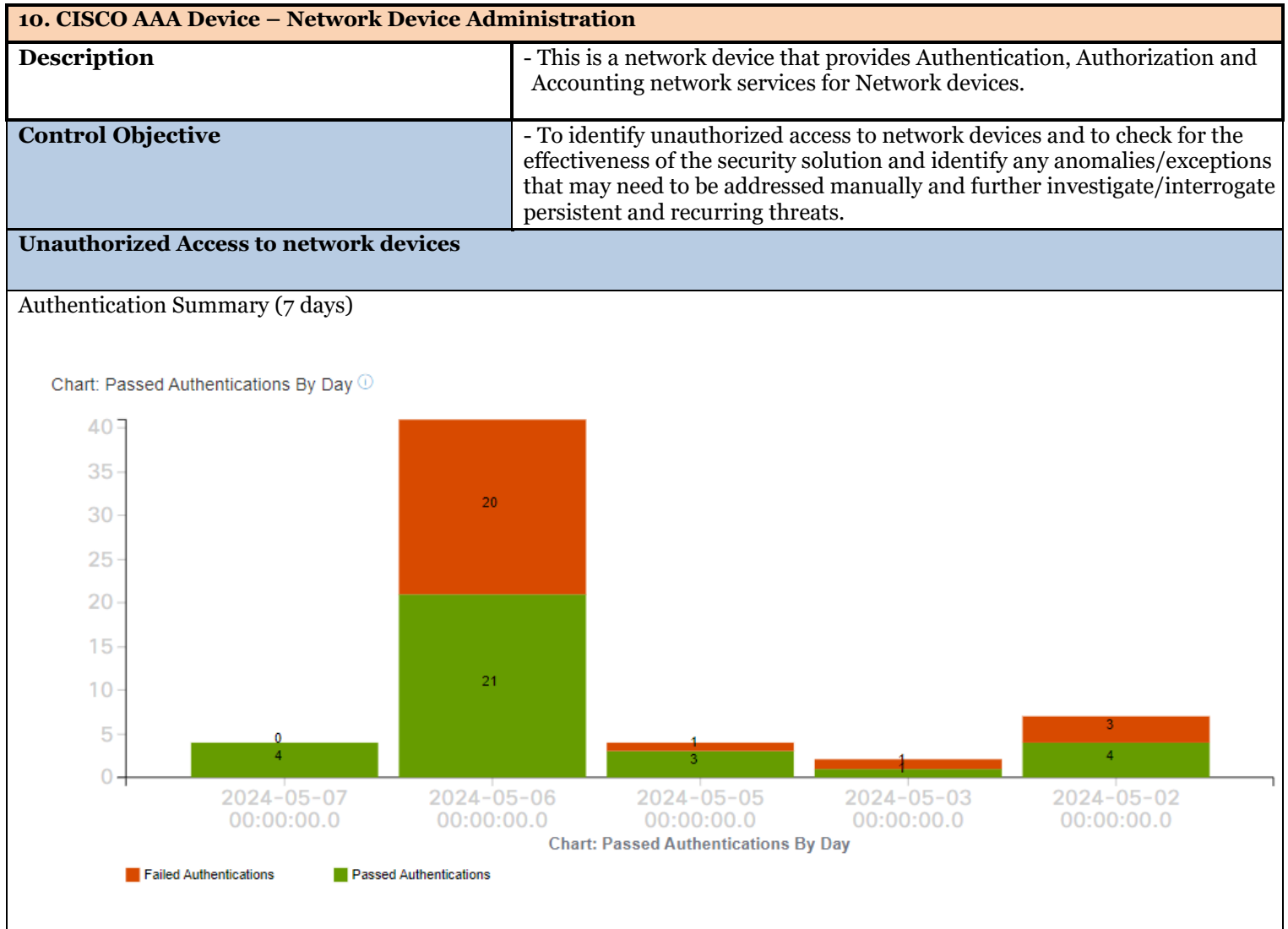
Risk Indicators: Information Security Daily Checklist



Risk Indicators: Information Security Daily Checklist

Day	Pass...	Failed	Total	Failed (%)	Avg Response Time (ms)	Pea
2024-05-08 00:00:00.0	540	129	669	19.28	29.17	6002
2024-05-07 00:00:00.0	2113	351	2464	14.25	20.1	3465
2024-05-06 00:00:00.0	2024	400	2424	16.5	63.57	2570
2024-05-05 00:00:00.0	715	288	1003	28.71	57.08	2004
2024-05-04 00:00:00.0	1221	284	1505	18.87	36.61	2103
2024-05-03 00:00:00.0	2428	362	2790	12.97	33.73	4880
2024-05-02 00:00:00.0	2334	332	2666	12.45	29.52	1850
2024-05-01 00:00:00.0	682	222	904	24.56	26.06	805
<div><div></div></div>						
Findings			540 successful and 129 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.			

Risk Indicators: Information Security Daily Checklist



Risk Indicators: Information Security Daily Checklist

Day	Passed	Failed	Total	Failed (%)
2024-05-07 00:00:00.0	4	0	4	0
2024-05-06 00:00:00.0	21	20	41	48.78
2024-05-05 00:00:00.0	3	1	4	25
2024-05-03 00:00:00.0	1	1	2	50
2024-05-02 00:00:00.0	4	3	7	42.86

Findings	4 Successful and 0 failed authentication attempts to network devices recorded in the past 48 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.

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 Actions - RD GATEWAY						
Last 24 hours@8:37						<div> <div></div> <div></div> <div>1/3</div> <div>50</div> <div></div> <div></div> </div>
Event Receive Time	Event ID	Reporting Device	User	Short Process Name	Process Name	
May 08 2024, 08:36:15 AM	4673	FBCDCTELEWORK04.fbc.co...	zulun	chrome.exe	C:\Program Files\Google\C...	
May 08 2024, 08:35:55 AM	4673	FBCDCTELEWORK04.fbc.co...	zulun	chrome.exe	C:\Program Files\Google\C...	
May 08 2024, 08:35:39 AM	4673	FBCDCTELEWORK04.fbc.co...	muzunzet	chrome.exe	C:\Program Files (x86)\Go...	
May 08 2024, 08:35:30 AM	4673	FBCDCTELEWORK04.fbc.co...	muzunzet	chrome.exe	C:\Program Files (x86)\Go...	
May 08 2024, 08:35:27 AM	4673	FBCDCTELEWORK04.fbc.co...	zulun	chrome.exe	C:\Program Files\Google\C...	
May 08 2024, 08:35:22 AM	4673	FBCDCTELEWORK04.fbc.co...	zulun	chrome.exe	C:\Program Files\Google\C...	
May 08 2024, 08:35:15 AM	4648	FBCDCTELEWORK04.fbc.co...	zulun	lsass.exe	C:\Windows\System32\lsas...	
May 08 2024, 08:35:15 AM	4673	FBCDCTELEWORK04.fbc.co...	ndemerat	chrome.exe	C:\Program Files (x86)\Go...	
May 08 2024, 08:35:15 AM	4673	FBCDCTELEWORK04.fbc.co...	zulun	chrome.exe	C:\Program Files\Google\C...	
May 08 2024, 08:35:09 AM	4624	FBCDCTELEWORK04.fbc.co...	ZuluN	NtLmSsp	NtLmSsp	
May 08 2024, 08:35:05 AM	4624	FBCDCTELEWORK04.fbc.co...	ZuluN	NtLmSsp	NtLmSsp	
May 08 2024, 08:34:29 AM	4673	FBCDCTELEWORK04.fbc.co...	zulun	chrome.exe	C:\Program Files\Google\C...	
May 08 2024, 08:34:29 AM	4673	FBCDCTELEWORK04.fbc.co...	zulun	chrome.exe	C:\Program Files\Google\C...	
May 08 2024, 08:34:19 AM	4673	FBCDCTELEWORK04.fbc.co...	zulun	chrome.exe	C:\Program Files\Google\C...	
May 08 2024, 08:34:14 AM	4673	FBCDCTELEWORK04.fbc.co...	ndemerat	chrome.exe	C:\Program Files (x86)\Go...	
May 08 2024, 08:34:14 AM	4673	FBCDCTELEWORK04.fbc.co...	zulun	chrome.exe	C:\Program Files\Google\C...	
May 08 2024, 08:33:29 AM	4673	FBCDCTELEWORK04.fbc.co...	zulun	chrome.exe	C:\Program Files\Google\C...	
May 08 2024, 08:33:23 AM	4673	FBCDCTELEWORK04.fbc.co...	ndemerat	chrome.exe	C:\Program Files (x86)\Go...	
May 08 2024, 08:33:16 AM	4673	FBCDCTELEWORK04.fbc.co...	ndemerat	chrome.exe	C:\Program Files (x86)\Go...	
May 08 2024, 08:33:16 AM	4673	FBCDCTELEWORK04.fbc.co...	zulun	chrome.exe	C:\Program Files\Google\C...	

Findings	3 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																																								
<div>VPN Logon: Top VPN Users Ranked By Failed VPN Logon</div> <div>Last 24 hours@8:35</div> <table><thead><tr><th>Reporting IP</th><th>User</th><th>COUNT(Matched Events)</th></tr></thead><tbody><tr><td>10.170.10.9</td><td>GuduP</td><td>4</td></tr><tr><td>10.170.10.9</td><td>BeharA</td><td>1</td></tr><tr><td>10.170.10.9</td><td>Chirongomaf</td><td>1</td></tr><tr><td>10.170.10.9</td><td>KatekweK</td><td>1</td></tr><tr><td>10.170.10.9</td><td>OthataM</td><td>1</td></tr><tr><td>10.170.10.9</td><td>Saungwemel</td><td>1</td></tr><tr><td>10.170.10.9</td><td>Viruk</td><td>1</td></tr><tr><td>10.170.10.9</td><td>machengetee</td><td>1</td></tr><tr><td>10.170.10.9</td><td>marquess</td><td>1</td></tr><tr><td>10.170.10.9</td><td>matareg</td><td>1</td></tr><tr><td>10.170.10.9</td><td>mharakurwam</td><td>1</td></tr><tr><td>10.170.10.9</td><td>ndlovumt</td><td>1</td></tr></tbody></table>		Reporting IP	User	COUNT(Matched Events)	10.170.10.9	GuduP	4	10.170.10.9	BeharA	1	10.170.10.9	Chirongomaf	1	10.170.10.9	KatekweK	1	10.170.10.9	OthataM	1	10.170.10.9	Saungwemel	1	10.170.10.9	Viruk	1	10.170.10.9	machengetee	1	10.170.10.9	marquess	1	10.170.10.9	matareg	1	10.170.10.9	mharakurwam	1	10.170.10.9	ndlovumt	1
Reporting IP	User	COUNT(Matched Events)																																						
10.170.10.9	GuduP	4																																						
10.170.10.9	BeharA	1																																						
10.170.10.9	Chirongomaf	1																																						
10.170.10.9	KatekweK	1																																						
10.170.10.9	OthataM	1																																						
10.170.10.9	Saungwemel	1																																						
10.170.10.9	Viruk	1																																						
10.170.10.9	machengetee	1																																						
10.170.10.9	marquess	1																																						
10.170.10.9	matareg	1																																						
10.170.10.9	mharakurwam	1																																						
10.170.10.9	ndlovumt	1																																						
Findings	A total of 15 failed VPN logon attempts were recorded on SIEM, a decrease from yesterday’s recordings. 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.		

28/3/2024	MERCHANT NAME	ADDRESS	COMMISSION	TYPE OF BUSINESS	TOWN
29012010	Terketh Investments	R.G Mugabe International Airport, Harare	1 % Zimswitch	Retail	Harare
29012011	Terketh Investments 2	R.G Mugabe International Airport, Harare	1 % Zimswitch	Retail	Harare
29012012	Dunexas Investments 9	Std.21158 Tilco Industrial Estate, Chitungwiza	1 % Zimswitch	Retail	Chitungwiza
29012013	Dunexas Investments 10	Std.21158 Tilco Industrial Estate, Chitungwiza	1 % Zimswitch	Retail	Chitungwiza
29012014	Dunexas Investments 11	Std.21158 Tilco Industrial Estate, Chitungwiza	1 % Zimswitch	Retail	Chitungwiza
29012015	Dunexas Investments 12	Std.21158 Tilco Industrial Estate, Chitungwiza	1 % Zimswitch	Retail	Chitungwiza
29012016	Dunexas Investments 13	Std.21158 Tilco Industrial Estate, Chitungwiza	1 % Zimswitch	Retail	Chitungwiza
29012017	Dunexas Investments 14	Std.21158 Tilco Industrial Estate, Chitungwiza	1 % Zimswitch	Retail	Chitungwiza
FX002705	Terketh Investments FX	R.G Mugabe International Airport, Harare	2.5 % MasterCard/Visa	Retail	Harare
FX002706	Terketh Investments FX 2	R.G Mugabe International Airport, Harare	2.5 % MasterCard/Visa	Retail	Harare
FX002707	Classic Team Catering FX	Std.2072 Ascot Infill, Gweru	2.5 % MasterCard/Visa	Catering	Gweru
FX002708	Tutorial Home FX	Tutorial Home, Harare	2.5 % MasterCard/Visa	Furniture	Harare
FX002709	Dunexas Investments FX	Std.21158 Tilco Industrial Estate, Chitungwiza	2.5 % MasterCard/Visa	Retail	Chitungwiza
FX002710	Dunexas Investments FX	Std.21158 Tilco Industrial Estate, Chitungwiza	2.5 % MasterCard/Visa	Retail	Chitungwiza
FX002711	Dunexas Investments FX	Std.21158 Tilco Industrial Estate, Chitungwiza	2.5 % MasterCard/Visa	Retail	Chitungwiza
FX002712	Dunexas Investments FX	Std.21158 Tilco Industrial Estate, Chitungwiza	2.5 % MasterCard/Visa	Retail	Chitungwiza
FX002713	Dunexas Investments FX	Std.21158 Tilco Industrial Estate, Chitungwiza	2.5 % MasterCard/Visa	Retail	Chitungwiza
FX002714	Dunexas Investments FX	Std.21158 Tilco Industrial Estate, Chitungwiza	2.5 % MasterCard/Visa	Retail	Chitungwiza
FX002715	Dunexas Investments FX	Std.21158 Tilco Industrial Estate, Chitungwiza	2.5 % MasterCard/Visa	Retail	Chitungwiza
FX002716	Dunexas Investments FX	Std.21158 Tilco Industrial Estate, Chitungwiza	2.5 % MasterCard/Visa	Retail	Chitungwiza
FX002717	Dunexas Investments FX	Std.21158 Tilco Industrial Estate, Chitungwiza	2.5 % MasterCard/Visa	Retail	Chitungwiza
FX002718	Dunexas Investments FX	Std.21158 Tilco Industrial Estate, Chitungwiza	2.5 % MasterCard/Visa	Retail	Chitungwiza
FX002719	Dunexas Investments FX	Std.21158 Tilco Industrial Estate, Chitungwiza	2.5 % MasterCard/Visa	Retail	Chitungwiza
FX002720	Dunexas Investments FX	Std.21158 Tilco Industrial Estate, Chitungwiza	2.5 % MasterCard/Visa	Retail	Chitungwiza
FX002721	Dunexas Investments FX	Std.21158 Tilco Industrial Estate, Chitungwiza	2.5 % MasterCard/Visa	Retail	Chitungwiza
FX002722	Dunexas Investments FX	Std.21158 Tilco Industrial Estate, Chitungwiza	2.5 % MasterCard/Visa	Retail	Chitungwiza
FX002723	Dunexas Investments FX	Std.21158 Tilco Industrial Estate, Chitungwiza	2.5 % MasterCard/Visa	Retail	Chitungwiza
FX002724	The Baby Place FX	Shp No.3 Cabs Centre, Cnr J Moyo and 2nd St, Harare	2.5 % MasterCard/Visa	Retail	Harare
FX002725	Senga Secondary School FX 2	Senga Secondary School, Gweru	2.5 % MasterCard/Visa	Education	Gweru
FX002726	Sanzhong Pvt Ltd FX	Std.1969 Westgate Area D, Harare	2.5 % MasterCard/Visa	Retail	Harare
29012018	Sanzhong Pvt Ltd	Std.1969 Westgate Area D, Harare	1 % Zimswitch	Retail	Harare

Findings	POS machines deployed for the month of February.
Comment	<p>The POS machines were last configured on 28/03/2024. Verifications of accuracy of configuration on POS devices underway in liaison with the business.</p> <p>A POS Management Strategy is being developed to enable effective management of the POS infrastructure.</p>

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.																																
Control Objective			To track amount utilized on procurement of SSL certificates.																																
Prima Secure Remaining Balance																																			
<table border="1" style="width: 100%; border-collapse: collapse; margin: 10px 0;"> <thead> <tr style="background-color: #333; color: white;"> <th style="text-align: left;">Date</th> <th style="text-align: left;">Transactions</th> <th style="text-align: left;">Details</th> <th style="text-align: right;">Amount</th> <th style="text-align: right;">Payments</th> <th style="text-align: right;">Balance</th> </tr> </thead> <tbody> <tr> <td>01 Mar 2024</td> <td>***Opening</td> <td></td> <td style="text-align: right;">0.00</td> <td></td> <td style="text-align: right;">0.00</td> </tr> <tr> <td></td> <td>Balance***</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr style="background-color: #f2f2f2;"> <td>21 Mar 2024</td> <td>Invoice</td> <td>INV-001235 - due on 28 Mar 2024</td> <td style="text-align: right;">6,662.22</td> <td></td> <td style="text-align: right;">6,662.22</td> </tr> <tr> <td colspan="5" style="text-align: right;">Balance Due</td> <td style="text-align: right;">\$ 6,662.22</td> </tr> </tbody> </table>						Date	Transactions	Details	Amount	Payments	Balance	01 Mar 2024	***Opening		0.00		0.00		Balance***					21 Mar 2024	Invoice	INV-001235 - due on 28 Mar 2024	6,662.22		6,662.22	Balance Due					\$ 6,662.22
Date	Transactions	Details	Amount	Payments	Balance																														
01 Mar 2024	***Opening		0.00		0.00																														
	Balance***																																		
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																																

Risk Indicators: Information Security Daily Checklist

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
Email alerts	
Day of the Week	Count
Sunday	0
Monday	250
Tuesday	210
Wednesday	89
Thursday	
Friday	
Saturday	
Total	549
Findings	89 firewall email alerts were recorded on 08/05/2024 . The total weekly count of firewall alerts is 549 .
Comment	All threats were blocked by the firewall.

Risk Indicators: Information Security Daily Checklist

Created by: Patrick T. Siziba Date: 08/05/2024.... Signature:

Reviewed by: Nigel Baera Date: 08/05/2024.... Signature: