

Sample Cybersecurity Analysis Report

April 19, 2023

Introduction

“The key to success is a well-constructed cybersecurity strategy with clear priorities. Spending must be balanced between people and technology with careful consideration for which risks should be addressed in which order. Decision-makers must be mindful of how their choices map against the NIST Cybersecurity framework to deliver a rounded set of defenses.” WSJ Cybersecurity

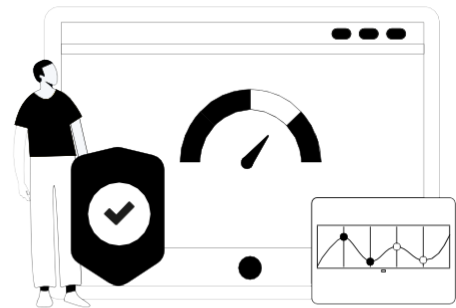
This report details your organization's cybersecurity posture. It provides a high-level cyber risk assessment to indicate your organization's effectiveness at addressing cyber risks. It also provides a prioritized list of recommendations to improve your posture and mitigate those risks. The information in the report is compiled from publicly available information about your organization as well as information provided by you about your organization's environment. Recommendations in this report, adhere to the National Institute of Standards and Technology (NIST) Cybersecurity framework which is internationally recognized as the global 'gold standard' for an assessment of this kind.

Please note, this report was prepared by CyblQs platform for the purpose of initial evaluation of your organization's cybersecurity posture. CyblQs does not take responsibility for or relating to the information included in this document or its accuracy and offers no warranty.

Posture score

6.6

Moderate protection measures have been taken. While there is more to be done, the organization obtains reasonable protection.



Attack vector score

Current cybersecurity threat readiness of four cyber attack categories.

Data Leak

An overlooked exposure in a data storage which might lead to data breach.



Website Defacement

An unauthorized and malicious modification of web page content.



Ransomware

A threat by a malicious software to either publish or block access to data by encryption, unless a ransom is paid.



Fraud

A crime in which someone gains inappropriate access to financial or sensitive business information, used to commit fraudulent crimes.

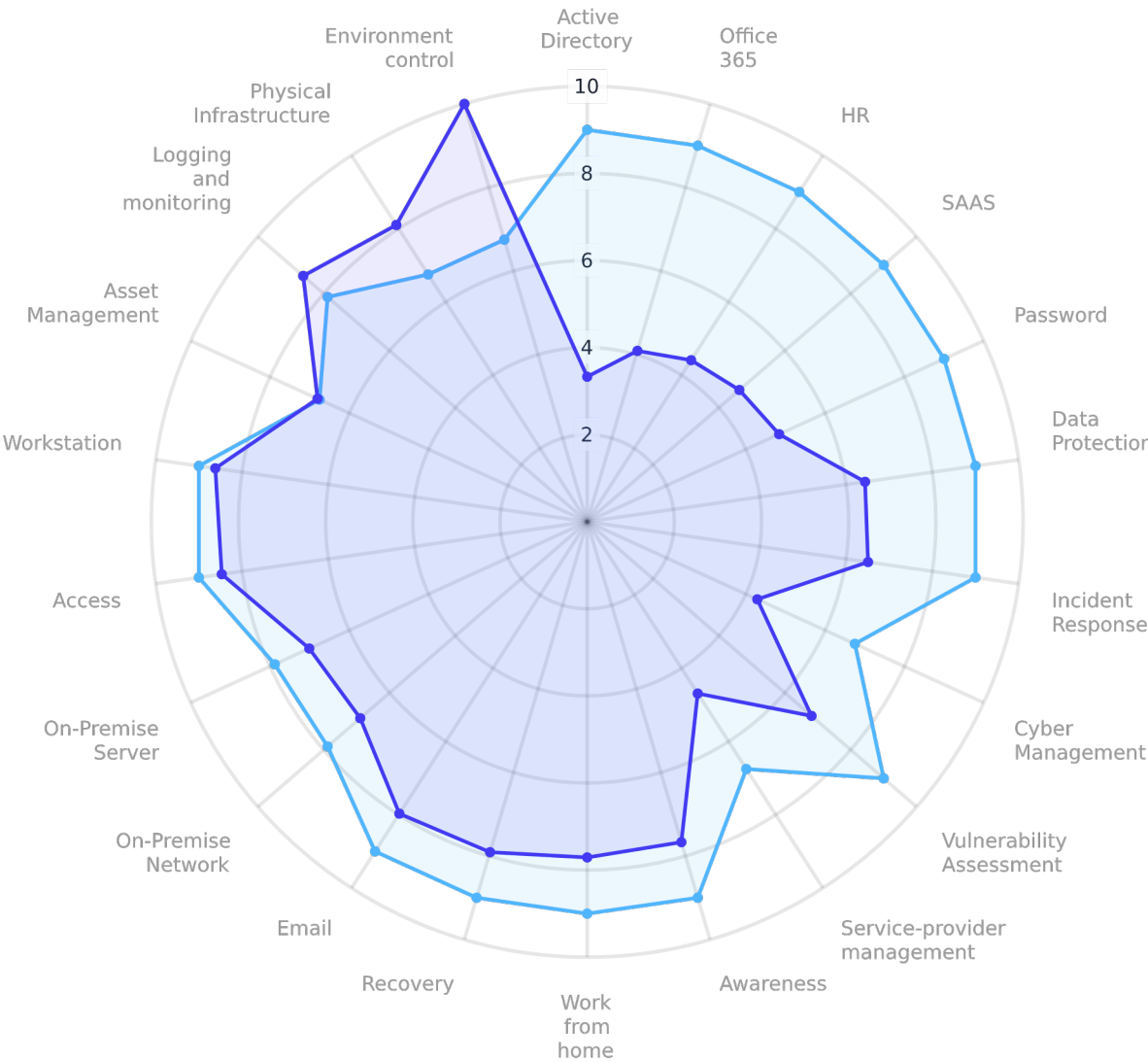


Cybersecurity readiness level

22 Total Policies	4 Meet target score	18 Under target score
----------------------	------------------------	--------------------------

A mapping process of your organization shows that 22 security domains must be secured to safeguard the organization from cyberattacks.

To increase the organization's cybersecurity readiness, follow the custom-made policies of each security domain. For a good cyber hygiene, address first security domains with large gaps between current and target score.

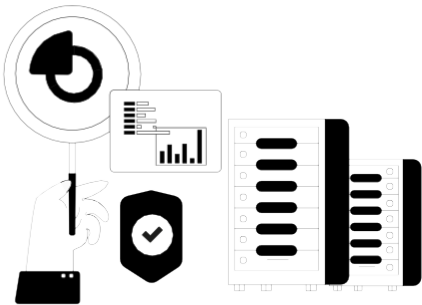


Company readiness by security domain

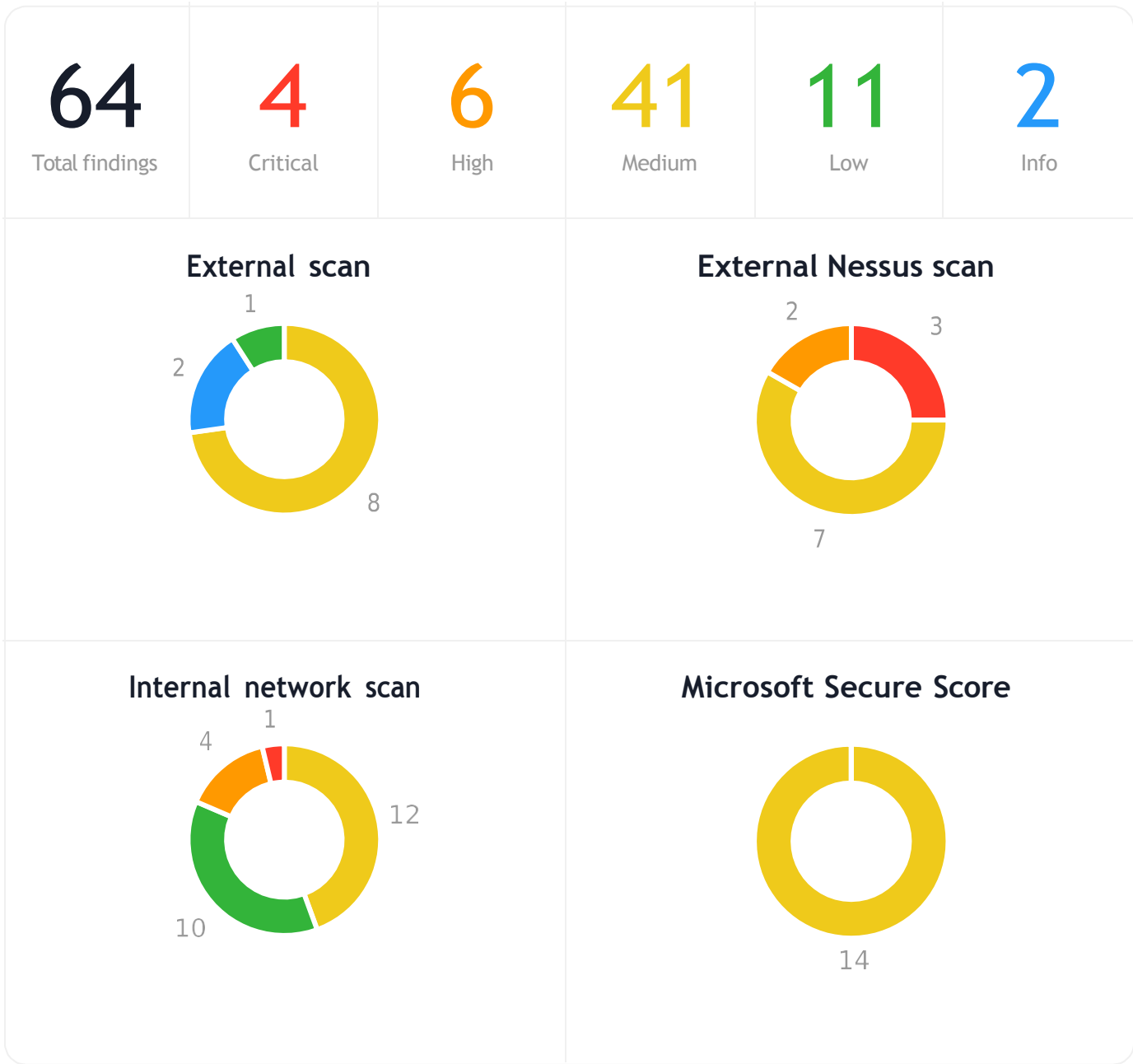
DOMAIN	SCORE
Access	8.5
Active Directory	3.3
Asset Management	6.8
Awareness	7.7
Cyber Management	4.3
Data Protection	6.4
Email	8
Environment control	10
HR	4.4
Incident Response	6.5
Logging and monitoring	8.6
Office 365	4.1
On-Premise Network	6.9
On-Premise Server	7
Password	4.8
Physical Infrastructure	8.1
Recovery	7.9
SAAS	4.6
Service-provider management	4.7
Vulnerability Assessment	6.8
Work from home	7.7
Workstation	8.6

Scan findings

- ✓ External scan
- ✓ External Nessus scan
- ✓ Internal network scan
- ✓ Microsoft Secure Score



Scanning networks and applications exposes hidden infrastructure vulnerabilities. Addressing these vulnerabilities will reduce the chances of your organization being the subject of a cyberattack.



Scan findings

Sample findings

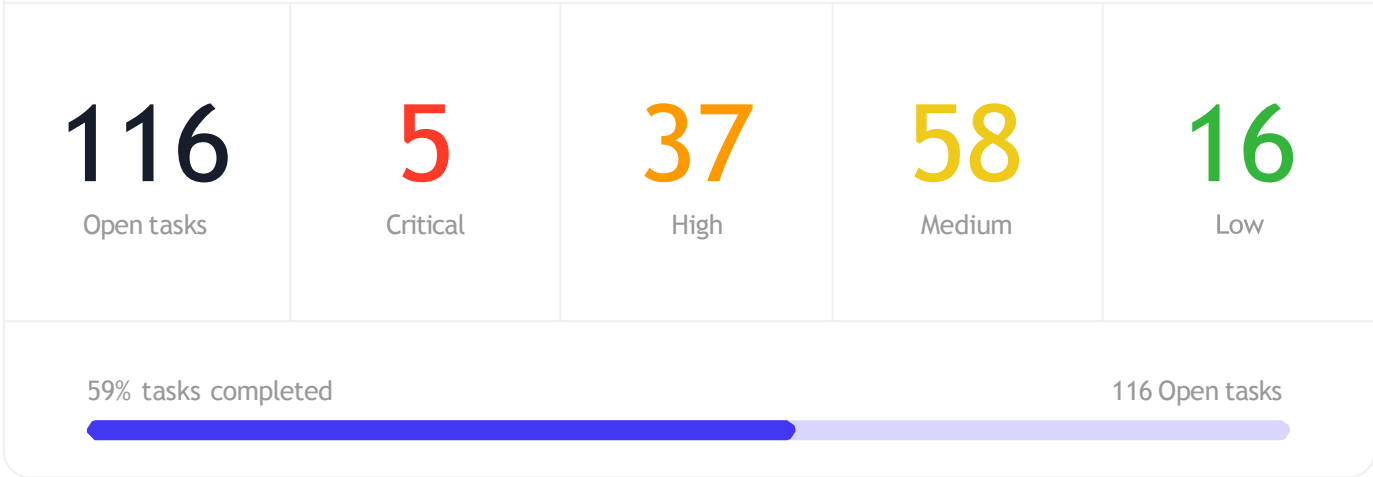
Each finding addresses a specific asset and details the specifics of its detected vulnerabilities. Using the CyblQs platform, you can review online or download the full list of findings.

SOURCE	SEVERITY	FINDING	ASSET
External Nessus scan	Critical	NFS Exported Share Information Disclosure	192.168.88.16
Internal network scan	Critical	Password length is not set to be at least 12 characters	192.168.0.10
External Nessus scan	High	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	192.168.88.16
External Nessus scan	High	ISC BIND Denial of Service	192.168.88.16
Internal network scan	High	Policies with domain controller security configurations are set to default	192.168.0.10

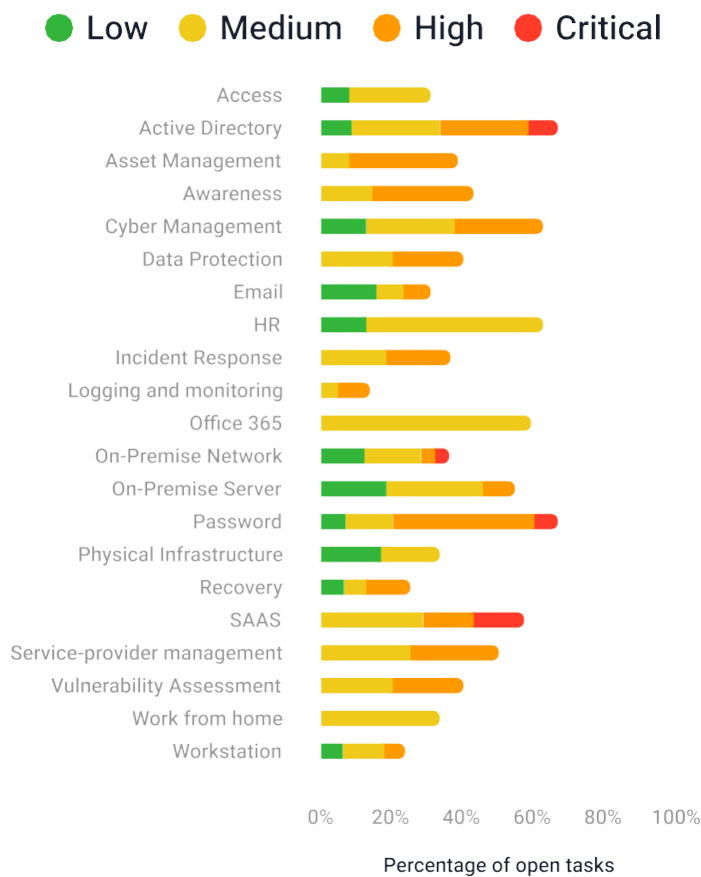
Source	Finding	Asset	Product	Version	Severity	CVE-ID
Internal network scan	Password length is not set to be at least 12 characters	10.10.0.10	Active Directory	-	Critical	
Internal network scan	The Server Message Block version 1 (SMBv1) protocol is supported	10.10.0.10	Active Directory	-	Critical	
Internal network scan	New Technology LAN Manager (NTLM) authentication protocol is used	10.10.0.10	Active Directory	-	High	
Internal network scan	Not all user passwords are set with an expiration date	10.10.0.10	Active Directory	-	High	
Internal network scan	Policies with domain controller security configurations are set to default	10.10.0.10	Active Directory	-	High	
Internal network scan	Reversible encryption for password storage is not disabled	10.10.0.10	Active Directory	-	High	
Internal network scan	Inactive user accounts have been found in the system	10.10.0.10	Active Directory	-	High	
Internal network scan	Maximum password history is lower than 24	10.10.0.10	Active Directory	-	High	
Internal network scan	Not all domain controllers are set up with the same operating system	10.10.0.10	Active Directory	-	High	
External scan	CVE-2017-8923 php 7.4.20	https://lite1067.ca/	Php	7.4.20	High	CVE-2017-8923
External scan	CVE-2017-8923 php 7.4.20	https://cfmb.ca/	Php	7.4.20	High	CVE-2017-8923
External scan	CVE-2017-8923 php 7.4.20	https://lite92.ca/	Php	7.4.20	High	CVE-2017-8923
External scan	CVE-2017-9120 php 7.4.20	https://lite1067.ca/	Php	7.4.20	High	CVE-2017-9120
External scan	CVE-2017-9120 php 7.4.20	https://cfmb.ca/	Php	7.4.20	High	CVE-2017-9120
External scan	CVE-2017-9120 php 7.4.20	https://lite92.ca/	Php	7.4.20	High	CVE-2017-9120
External scan	CVE-2019-9517 apache 2.4.29	https://lite1067.ca/	Apache	2.4.29	High	CVE-2019-9517
External scan	CVE-2019-9517 apache 2.4.29	https://cfmb.ca/	Apache	2.4.29	High	CVE-2019-9517
External scan	CVE-2019-9517 apache 2.4.29	https://lite92.ca/	Apache	2.4.29	High	CVE-2019-9517
External scan	The weak Transport Layer Security (TLSv1.1) protocol is supported by your web server	https://hotcountry925.ca/	-	-	High	
External scan	The weak Transport Layer Security (TLSv1) protocol is supported by your web server	https://hotcountry925.ca/	-	-	High	
External scan	Open port 21 TCP protocol	162.211.10.166	Microsoft Ftpd	-	High	
External scan	Open port 443 TCP Protocol	54.84.131.112	Apache Httpd	2.4.29	High	CVE-2019-0211
External scan	Open port 443 TCP Protocol	54.84.131.112	Apache Httpd	2.4.29	High	CVE-2022-31813
External scan	Open port 443 TCP Protocol	54.84.131.112	Apache Httpd	2.4.29	High	CVE-2022-23943
External scan	Open port 443 TCP Protocol	54.84.131.112	Apache Httpd	2.4.29	High	CVE-2022-22720
External scan	Open port 443 TCP Protocol	54.84.131.112	Apache Httpd	2.4.29	High	CVE-2021-44790
External scan	Open port 443 TCP Protocol	54.84.131.112	Apache Httpd	2.4.29	High	CVE-2021-26691
External scan	Open port 443 TCP Protocol	54.84.131.112	Apache Httpd	2.4.29	High	CVE-2019-9517
External scan	Open port 443 TCP Protocol	54.84.131.112	Apache Httpd	2.4.29	High	CVE-2021-39275
External scan	CVE-2021-39275 apache 2.4.29	https://lite1067.ca/	Apache	2.4.29	High	CVE-2021-39275
External scan	CVE-2021-39275 apache 2.4.29	https://cfmb.ca/	Apache	2.4.29	High	CVE-2021-39275
External scan	CVE-2021-39275 apache 2.4.29	https://lite92.ca/	Apache	2.4.29	High	CVE-2021-39275
External scan	CVE-2021-44790 apache 2.4.29	https://lite1067.ca/	Apache	2.4.29	High	CVE-2021-44790
External scan	CVE-2021-44790 apache 2.4.29	https://cfmb.ca/	Apache	2.4.29	High	CVE-2021-44790
External scan	CVE-2021-44790 apache 2.4.29	https://lite92.ca/	Apache	2.4.29	High	CVE-2021-44790
External scan	CVE-2022-22720 apache 2.4.29	https://lite1067.ca/	Apache	2.4.29	High	CVE-2022-22720
External scan	CVE-2022-22720 apache 2.4.29	https://cfmb.ca/	Apache	2.4.29	High	CVE-2022-22720
External scan	CVE-2022-22720 apache 2.4.29	https://lite92.ca/	Apache	2.4.29	High	CVE-2022-22720
External scan	CVE-2022-23943 apache 2.4.29	https://lite1067.ca/	Apache	2.4.29	High	CVE-2022-23943
External scan	CVE-2022-23943 apache 2.4.29	https://cfmb.ca/	Apache	2.4.29	High	CVE-2022-23943
External scan	CVE-2022-23943 apache 2.4.29	https://lite92.ca/	Apache	2.4.29	High	CVE-2022-23943

Risk mitigation plan

Completing critical and high severity tasks will impact organization cybersecurity the most, and increase posture score.



Open tasks













Task status



Appendix A





Top 10 open tasks

The top 10 open tasks which impact your security posture the most.

ISSUE	RECOMMENDATION	ID
 Administrators may use the same password for their "normal" activities and admin tasks which require a higher set of privileges.	Require administrators to have different passwords and accounts for their admin user tasks.	CYT-845259
 Not all domain controllers run a supported operating system.	Set all domain controllers to run a supported and updated Operating System (OS).	CYT-095911
 Domain controller traffic is not secured.	Disable Server Message Block version 1 (SMBv1) protocol on all domain controllers.	CYT-438206
 Your SaaS service providers may not be meeting the required data security regulations and standards.	Verify that all SaaS applications holding company sensitive data comply with the relevant data protection regulation.	CYT-929692
 Your company's network can be remotely accessed without a VPN.	Allow remote access to on-premises company networks only by using a Virtual Private Network (VPN).	CYT-504061
 No third party Incident Response (IR) support.	Engage a third-party IR vendor for fast response and post-incidents reviews.	CYT-373508
 Critical information gathering is missing from your IR preparation phase.	Maintain an updated company asset inventory, including network topology and sensitive data locations.	CYT-791067
 Undiscovered and unknown web application vulnerabilities.	Test business-critical web applications periodically for penetration by external actors and mitigate	CYT-788907
 There is no security-system penetration testing program for identifying vulnerabilities of external assets.	Test systems periodically for penetration by external actors and mitigate.	CYT-313367
 Users may be using the same password for numerous accounts and services.	Do not use the same password for different user accounts.	CYT-678163

Appendix B

Open tasks by domain - Access

ISSUE	RECOMMENDATION	ID
 There is no defined process for removing unauthorized access rights and privileges to assets and systems.	Establish a periodical audit of users' access rights and privileges.	CYT-584712
 There is no defined process for removing unauthorized access rights and privileges to assets and systems.	Provide Single Sign-On capability to access company systems containing sensitive data.	CYT-688505
 There is no defined process for updating employee access rights and privileges upon role change.	Adjust users' access rights and privileges upon role changes.	CYT-632658
 Inactive user accounts are not automatically flagged and removed.	Remove inactive user accounts, preferably automatically.	CYT-952139



Appendix B

Open tasks by domain - Active Directory

ISSUE	RECOMMENDATION	ID
● Not all domain controllers run a supported operating system.	Set all domain controllers to run a supported and updated Operating System (OS).	CYT-095911
● Domain controller traffic is not secured.	Disable Server Message Block version 1 (SMBv1) protocol on all domain controllers.	CYT-438206
● Unverified domains might be trusted.	Carefully check external domains for compliance with company Active Directory policy before configuring as trusted.	CYT-678223
● There are obsolete accounts that need to be deleted.	Delete disabled user accounts after a defined time period.	CYT-668032
● Some domain controller permissions and privileges are not restricted.	Prohibit default domain controller policy insecure configurations.	CYT-005337
● High-privilege administrative groups are not secured.	Limit the number of accounts in high-privilege administrative groups.	CYT-675864
● Standard users are granted high-privilege permissions.	Configure standard users to have only standard access permissions.	CYT-373978
● Unauthorized users might have domain controller object permissions.	Configure all domain controller objects to be owned by domain admin group.	CYT-289730
● GPOs use weak password exchange protocol.	Prevent GPOs from using Network LAN Manager (NTLM)	CYT-047309
● Local administrator accounts are not secured.	Rename all local administrator account default names.	CYT-283637
● Unauthorized users are granted the access rights and permissions of authorized users.	Deny anonymous user access to system information.	CYT-492591
● Non-administrative accounts might be able to set passwords via Group Policy.	Do not allow any Extensible Markup Language (XML) file with cpassword in System Volume (Sysvol).	CYT-841136
● There is no software update verification policy for DNS zones.	Use only secure updates from certified known sources in DNS zones.	CYT-226266
● Some domain controllers support old system versions.	Disable domain controller backward compatibility if not necessary.	CYT-538658






Appendix B

Open tasks by domain - Active Directory

ISSUE	RECOMMENDATION	ID
 Unauthorized users might have administrator permissions and privileges.	Clear all default administrative groups with access privileges and leave empty.	CYT-232519
 Unauthorized users can add other unauthorized users and malicious machines to Active Directory.	Disable default capability of adding computer accounts by unprivileged users.	CYT-326103




Appendix B

Open tasks by domain - Asset Management

ISSUE	RECOMMENDATION	ID
 The network architecture and interconnectivity is not documented.	A network diagram exists which identifies high-risk environments.	CYT-311307
 Asset usage is not restricted to business use.	Organizational assets will not be used for any private purpose except as authorized.	CYT-112153
 The organization does not understand the types of sensitive data records that are stored, transmitted, or processed by their systems.	Data flow between assets that have statutory, regulatory, or contractual compliance impacts are documented.	CYT-183617
 Asset inventories are not kept up to date.	Update asset inventory when changes occur.	CYT-617887
 Sensitive data is not removed from end-of-life or recycled media.	Asset custodians are required to destroy media that cannot be sanitized.	CYT-939131






Appendix B

Open tasks by domain - Awareness

ISSUE	RECOMMENDATION	ID
 There is no process for ensuring employee commitment to company cybersecurity policy.	Ensure all employees are aware of and have signed company cybersecurity policy.	CYT-549414
 There is no improvement protocol for company security awareness programs.	Collect and store training data.	CYT-906502
 There is no employee security awareness program for detecting and reporting cyber incidents.	Conduct cybersecurity awareness training to employees about detecting and reporting potential signs of cyber incidents.	CYT-585743







Appendix B

Open tasks by domain - Cyber Management

ISSUE	RECOMMENDATION	ID
 The company does not have a full set of cybersecurity policies.	Create cybersecurity policies consistent with company assessed risks and relevant regulatory requirements.	CYT-635874
 An annual risk assessment is not carried out.	Perform routine risk assessments at planned intervals to continuously improve cybersecurity.	CYT-795670
 Company does not have cyber insurance.	Protect company assets from potential destructive effects of cybercrime by acquiring cybersecurity insurance.	CYT-115481
 Not all information security internal and external issues, which might affect company cybersecurity, are identified.	Identify all internal and external issues affecting company cybersecurity policy.	CYT-820950
 Not all information security persons of interest, who will be affected by company decisions and actions, are mapped, graded, or aware of cyber policies and procedures.	Understand who are the interested parties in company information security and what are their needs and expectations in terms of compliance obligations.	CYT-756954





Appendix B

Open tasks by domain - Data Protection

ISSUE	RECOMMENDATION	ID
 Incomplete mapping of sensitive or private data.	Discover all company data and classify according to sensitivity.	CYT-167544
 There is no process for disposing of data once it is no longer needed.	Enforce retention and deletion of regulated data according to law or business agreements.	CYT-612835
 There is no mapping of data according to the regulations or contractual agreements it needs to comply with.	Map all data types that are subject to regulations or contractual obligations and make sure they are protected according to the compliance requirements.	CYT-604160
 Logs containing sensitive data are not encrypted or do not have access limitations.	Protect logs containing sensitive data with access limitation and encryption.	CYT-527658
 There is no policy or procedure for properly and effectively using cryptography throughout company departments.	Develop and implement a key management policy.	CYT-056824
 There is no process for wiping data from company-owned end-user devices.	Enforce remote wipe capability on portable company-owned end-user devices	CYT-450493

Appendix B

Open tasks by domain - Email

ISSUE	RECOMMENDATION	ID
 Anti-Spam mechanisms to mitigate the reception of malicious mail are either missing or have not been configured.	Apply anti-spam tools.	CYT-632671
 There is no policy governing usage of company email accounts.	Issue an Email Usage Policy to be implemented by all company email account users.	CYT-428723
 A mechanism to prevent outgoing email spoofing is missing or has not been configured.	Apply anti-spoofing mechanisms.	CYT-073202
 Email forwarding rules are enabled.	Create and enforce email forwarding standards.	CYT-185743

Appendix B

Open tasks by domain - HR

ISSUE	RECOMMENDATION	ID
● Employment contract does not define unacceptable social behavior around the office and online.	Ensure that HR incorporates the rules for acceptable and unacceptable behavior for information and system usage, security, and privacy in employee and third-party contracts.	CYT-972818
● Company data is not protected against misuse by employees or third-party contractors.	Ensure that HR incorporate a Non-Disclosure Agreement (NDA) or a similar confidentiality agreement that reflect the demands for protecting data and operational details, for both employee and third-party contracts.	CYT-610545
● Company data is not protected against misuse by former employees or third-party contractors.	Ensure that all post-employment requirements for protecting sensitive company information are legally binding and incorporated into employee and third-party contracts.	CYT-067664
● Employment contract does not support legal investigation of suspected misconduct.	Verify that all employment contracts allow the company the ability to investigate employee misconduct when there is reasonable evidence of policy violation or any information security breach.	CYT-112516
● Employees and third-party contractors might not be aware of sanctions for violating company cyber policy.	Ensure that the company has an approved sanction process for cyber policy breaches.	CYT-687979

Appendix B

Open tasks by domain - Incident Response

ISSUE	RECOMMENDATION	ID
● No third party Incident Response (IR) support.	Engage a third-party IR vendor for fast response and post-incidents reviews.	CYT-373508
● Critical information gathering is missing from your IR preparation phase.	Maintain an updated company asset inventory, including network topology and sensitive data locations.	CYT-791067
● There is no process for communicating cybersecurity incidents to stakeholders, affected third-parties, or relevant employees.	Report information security events both internally and externally; for instance, third-party vendors, law enforcement, cyber insurance providers, and relevant government agencies.	CYT-143196
● There is no defined incident alert threshold that helps differentiating between events and incidents.	Establish a threshold for alerts when an incident is detected and classified.	CYT-024763

Appendix B

Open tasks by domain - Logging and monitoring

ISSUE	RECOMMENDATION	ID
● Endpoint device security-related events are not logged.	Define endpoint device security-related event logs as an event type.	CYT-001346
● Indicators of Compromise (IoCs) are not logged.	Define Indicators of Compromised (IoC) data as an event type.	CYT-987925
● There is no sensitive-role control record analysis.	Periodically review and analyze control records of users with sensitive roles or any account with access privileges.	CYT-405010










Appendix B

Open tasks by domain - Office 365

ISSUE	RECOMMENDATION	ID
● The policy for inbound phishing messages is not well defined.	For read or unread messages that are identified as phishing after delivery, assigned Anti-phishing inbound policy with both 'Enable zero-hour auto purge (ZAP).	CYT-225146
● Users can access your digital assets or services with only a username and password. Accounts can be easily breach.	Ensure all users can complete multifactor authentication for secure access.	CYT-297649
● Customer lockbox feature is turned off.	Turn on customer lockbox feature.	CYT-689126
● Suspicious login are not handle properly and protected with MFA.	Turn on sign-in risk policy.	CYT-037104
● Your organization can inadvertently share malicious files.	Turn on Microsoft Defender for Office 365 in SharePoint, OneDrive, and Microsoft Teams.	CYT-133258
● Weaker protocols and cipher such as TLS 1.0/1.1 and 3DES dependencies are used.	Remove TLS 1.0/1.1 and 3DES dependencies.	CYT-837198
● Users can grant access permissions for 3rd party apps that can be a malicious application.	Do not allow users to grant consent to unmanaged applications.	CYT-145731
● Missing MFA for administrative roles.	Require multifactor authentication for admin roles.	CYT-451131
● The policy for inbound spam messages is not well defined.	Create Zero-hour Auto Purge policies for spam messages.	CYT-526526
● Only one global administrator for the organization. In case this account is breached or corrupted , the administrator cannot fulfill the needs or obligations of your organization.	Designate more than one global admin	CYT-649177
● Users can edit thew Anti-spam list and add allowed domains.	Sender domains allowed for Anti-spam policies.	CYT-749546
● The common attachments filter for anti-malware isn't well configured.	Turn on the common attachment filter setting for Anti-malware policies.	CYT-679998
● Big number of Global Administrator where found in your active directory	Use limited administrative roles.	CYT-694286







Appendix B

Open tasks by domain - On-Premise Network

ISSUE	RECOMMENDATION	ID
 Your company's network can be remotely accessed without a VPN.	Allow remote access to on-premises company networks only by using a Virtual Private Network (VPN).	CYT-504061
 There are no network traffic anomaly detection and prevention security controls.	Deploy network traffic anomaly detection and prevention security controls.	CYT-101697
 The company's Wi-Fi router uses its default login and password.	Change Wi-Fi routers default login details and password and create new ones.	CYT-214199
 Your company's Wi-Fi routers' firmware is not regularly updated.	Regularly update Wi-Fi firmware.	CYT-635957
 The company's Wi-Fi router does not encrypt communications using WPA2/3.	Set Wi-Fi routers to use WPA2 or WPA3 communication encryption.	CYT-037925
 Your company's Wi-Fi routers' firewall is not activated.	Set Wi-Fi routers internal firewall to be activated.	CYT-496486
 The company's Wi-Fi routers are not located at a secure location.	Secure physical and environmental location of Wi-Fi routers.	CYT-685794
 Your company's Wi-Fi routers allow WPS and DHCP services.	Disable company routers Dynamic Host Configuration Protocol (DHCP) and Wi-Fi Protected Setup (WPS) services.	CYT-964786
 There are no dedicated computing resources for administrative management tasks.	Perform network administrative management tasks only by using dedicated computing resources.	CYT-565897











Appendix B

Open tasks by domain - On-Premise Server

ISSUE	RECOMMENDATION	ID
 Users are not locked out following several unsuccessful login accounts.	Following multiple unsuccessful attempts to sign in, enforce user logout.	CYT-327236
 There is no removable media anti-malware scan enforced.	For all removable media connected to company servers, configure anti-malware scan.	CYT-179618
 Unused and unnessecery services/ports are open and ready for communication	Uninstall or disable all unused or unnecessary services from company servers.	CYT-104481
 Server communication is not encrypted or secured.	Verify all communication flow from and to company servers is protected, encrypted, and monitored.	CYT-043215
 Autorun and autoplay are not automatically disabled when connecting removable media.	For all removable media connected to company servers, disable autorun and autoplay.	CYT-815208
 Not all company servers have a host-based firewall enabled.	On all company on-premises servers, implement a host-based firewall.	CYT-487742



Appendix B

Open tasks by domain - Password

ISSUE	RECOMMENDATION	ID
 Administrators may use the same password for their "normal" activities and admin tasks which require a higher set of privileges.	Require administrators to have different passwords and accounts for their admin user tasks.	CYT-845259
 Users may be using the same password for numerous accounts and services.	Do not use the same password for different user accounts.	CYT-678163
 Password history is not enforced or set to too-low a number.	Enforce a password history limit for all passwords.	CYT-694130
 Users may store passwords in locally saved, unencrypted files.	Prohibit storing passwords in clear text on local files.	CYT-618272
 Employees may share passwords between them.	Prohibit password sharing.	CYT-895649
 Passwords are delivered or shared in an unsecured manner.	Deliver or give over passwords to employees in a secure manner.	CYT-038083
 Some of your company's assets or devices may not comply with your company's password policy.	Enforce company password policy on all assets and devices.	CYT-769629
 Your password policy does not require password rotation.	Enforce password rotation for all passwords.	CYT-479013
 Users may write passwords on post-it notes.	Do not write passwords on any visible medium, such as Post-it Notes.	CYT-484886
 Password age has no minimum limit.	Enforce a password Minimum age for all passwords.	CYT-840846





Appendix B

Open tasks by domain - Physical Infrastructure

ISSUE	RECOMMENDATION	ID
 Removable media assets are not physically protected.	Physically protect removable storage devices, such as portable hard drives.	CYT-905568
 No physical controls are in place to protect devices with sensitive outputs.	Control physical access to output devices such as printers and copiers connected to systems containing sensitive information.	CYT-431987





Appendix B

Open tasks by domain - Recovery

ISSUE	RECOMMENDATION	ID
 Business-critical data is not mapped or backed-up.	Following mapping of critical processes and related assets, map and back up critical data.	CYT-162393
 There is no contingency plan for the case of company main office being unavailable.	Prepare a separate site for deploying contingency plans for data centers and employee workplaces.	CYT-644939
 There is no employee contingency plan training for the case of a disaster and the need for quick recovery.	Train employees for disaster recovery and emergency response.	CYT-556018
 There is no seperate admin account for backup tasks,	Create a dedicated admin account for backup and restore daily tasks.	CYT-199342


Appendix B

Open tasks by domain - SAAS

ISSUE	RECOMMENDATION	ID
 Your SaaS service providers may not be meeting the required data security regulations and standards.	Verify that all SaaS applications holding company sensitive data comply with the relevant data protection regulation.	CYT-929692
 No verification of security best practices and recommended controls are in place for your SaaS service providers.	Require security best practices for all SaaS services.	CYT-873052
 Users can access your SaaS applications without detection of risky or suspicious behavior.	Enforce Cloud Access Security Broker (CASB) for all user accounts with access to company SaaS applications.	CYT-529472
 Users log into company SaaS applications using different credentials with no central management.	Enforce a Single Sign-On (SSO) for all user accounts with access to company SaaS applications.	CYT-001328

Appendix B

Open tasks by domain - Service-provider management

ISSUE	RECOMMENDATION	ID
 There is no periodical service-provider security-assessment process.	Conduct periodical service-provider security assessments.	CYT-373569
 There is no requirement for service providers to notify of any security weakness.	Ensure service-provider contracts define security requirements and legally require notifying within a reasonable time of any security weakness which can influence the company.	CYT-482316

Appendix B

Open tasks by domain - Vulnerability Assessment

ISSUE	RECOMMENDATION	ID
● Undiscovered and unknown web application vulnerabilities.	Test business-critical web applications periodically for penetration by external actors and mitigate	CYT-788907
● There is no security-system penetration testing program for identifying vulnerabilities of external assets.	Test systems periodically for penetration by external actors and mitigate.	CYT-313367
● There is no security-system penetration testing program for identifying vulnerabilities of internal assets.	Test systems periodically for penetration by internal actors and mitigate.	CYT-553099
● There is no security-system penetration testing program for identifying system vulnerabilities.	Implement a penetration testing program for vulnerabilities in company security systems.	CYT-604116





Appendix B

Open tasks by domain - Work from home

ISSUE	RECOMMENDATION	ID
● Company users can use public Wi-Fi networks to access company assets.	Do not use public Wi-Fi except under exceptional circumstances and with the needed precaution and protection controls.	CYT-321483
● Data can not be remotely wiped from mobile devices.	Make sure that the company can remotely wipe or delete its proprietary data from stolen or lost devices or in cases of employee termination.	CYT-777915
● There is no defined termination time or process of remote access sessions after idle period.	Terminate idle remote access connection after a defined period of inactivity	CYT-135462

Appendix B

Open tasks by domain - Workstation

ISSUE	RECOMMENDATION	ID
 Company workstations are not hardened.	Disable connections to external media.	CYT-550972
 Not all unapproved services are disabled or uninstalled from company workstations.	Uninstall or disable unnecessary or unapproved services.	CYT-305127
 Unmanaged Personal workstation and devices can access company resources.	Restrict the connection of personal unmanaged workstations to company assets.	CYT-855803
 There are no restrictions on the number of local admins per workstation.	Use only a minimal amount of local admin accounts, and make sure they are securely managed.	CYT-136241