

Acme Corporation marketing Cybersecurity Analysis Report

September 24, 2024

Introduction

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 multiple cybersecurity frameworks including the National Institute of Standards and Technology (NIST) Cybersecurity Framework, ISO 27001, the Center for Internet Security (CIS) controls, and SOC 2.

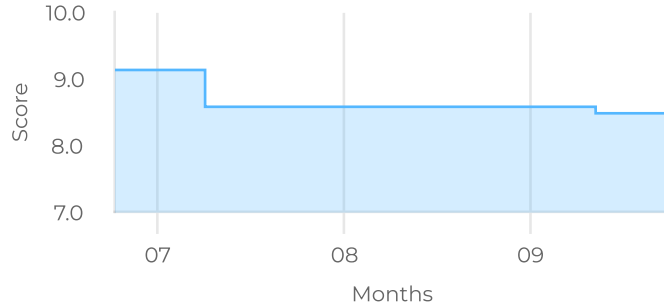
Please note, this report was prepared by Cynomi platform for the purpose of initial evaluation of your organization's cybersecurity posture. Cynomi does not take responsibility for or relating to the information included in this document or its accuracy and offers no warranty.

Powered by
cynomi

Posture score

8.5

Major efforts have been taken. While there is never a 100% guarantee of blocking attacks, the organization is well protected.



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.



Fraud

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



Ransomware

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



Website Defacement

An unauthorized and malicious modification of web page content.



Cybersecurity readiness level

34

Total Domains

21

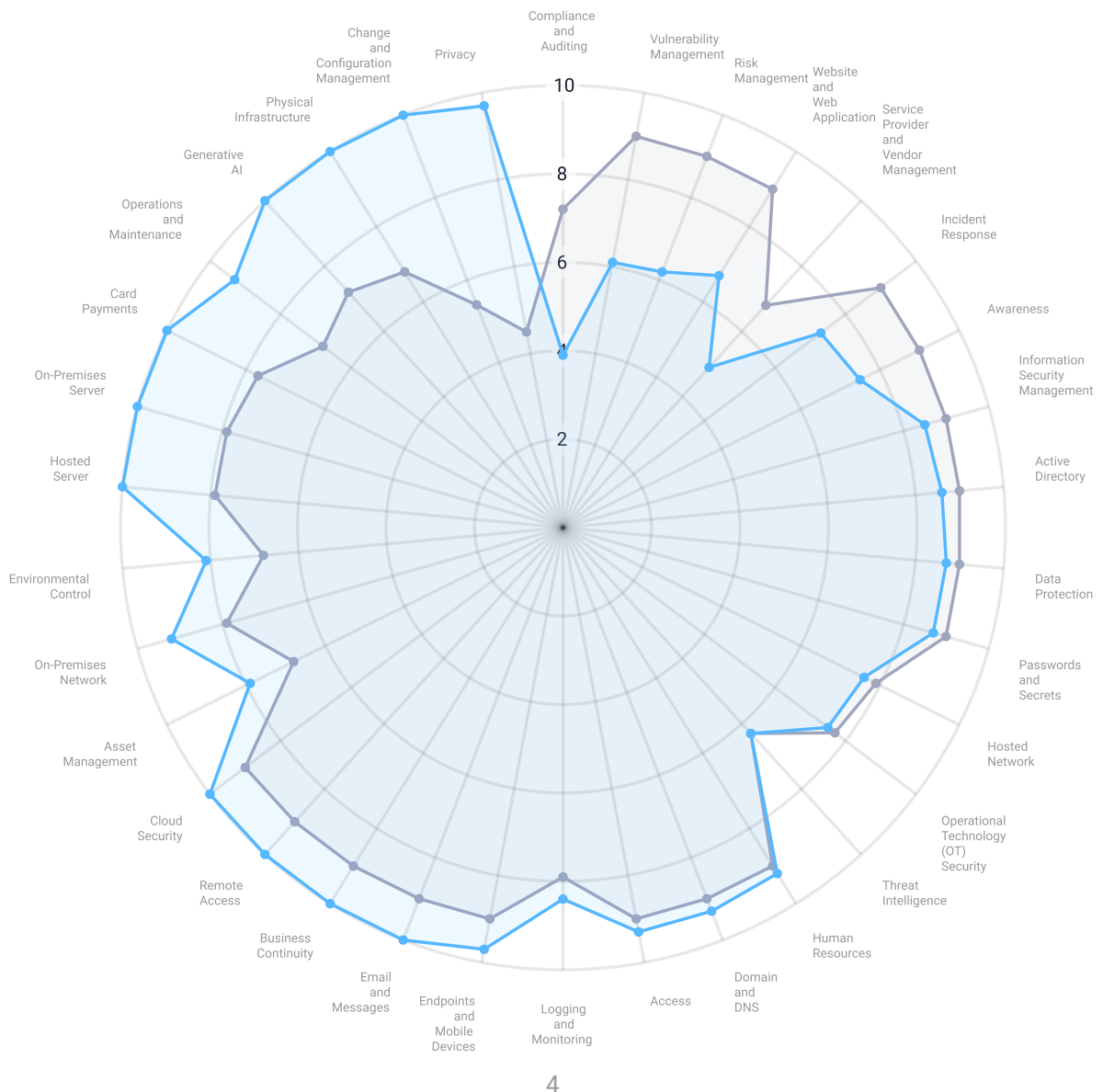
Meet target score

13

Under target score

A mapping process of your organization shows that 34 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	9.3
Active Directory	8.6
Asset Management	7.9
Awareness	7.5
Business Continuity	10
Card Payments	10
Change and Configuration Management	10
Cloud Security	10
Compliance and Auditing	3.9
Data Protection	8.7
Domain and DNS	9.3
Email and Messages	10
Endpoints and Mobile Devices	9.7
Environmental Control	8.1
Generative AI	10
Hosted Network	7.6
Hosted Server	10
Human Resources	9.2
Incident Response	7.3
Information Security Management	8.5
Logging and Monitoring	8.4
On-Premises Network	9.2
On-Premises Server	10
Operational Technology (OT) Security	7.5
Operations and Maintenance	9.3
Passwords and Secrets	8.7

Company readiness by security domain

DOMAIN	SCORE
Physical Infrastructure	10
Privacy	9.7
Remote Access	10
Risk Management	6.2
Service Provider and Vendor Management	4.9
Threat Intelligence	6.3
Vulnerability Management	6.1
Website and Web Application	6.7

Scan Findings

Severity

1014

Findings detected

61

Critical

2

Low

321

High

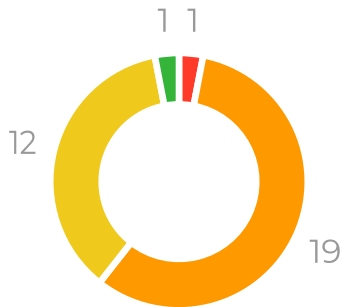
12

Info

618

Medium

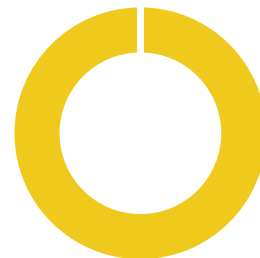
Internal Cynomi scan



7 targets scanned

Total: 33

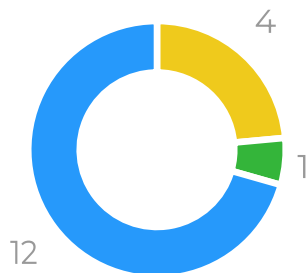
Microsoft Secure Score



1 targets scanned

Total: 6

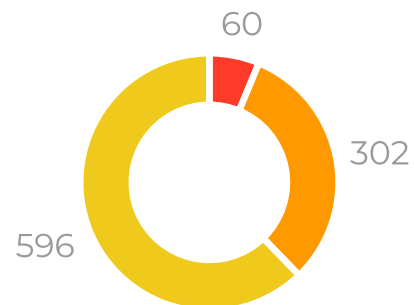
External Cynomi scan



2 targets scanned

Total: 17

External Nessus scan



87 targets scanned

Total: 958

Risk mitigation plan

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

90

Open tasks

9

Critical

26

High

31

Medium

24

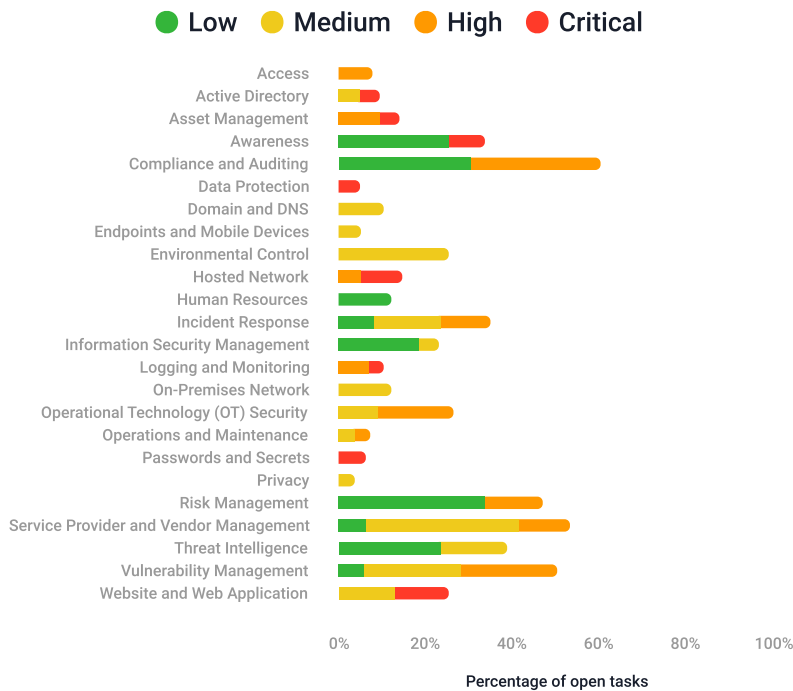
Low

86% tasks completed

90 Open tasks



Open tasks



Task status

89

Not started

1











In progress

Appendix A

Top 10 open tasks

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

 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
 Passwords and secrets are not managed by a password management tool.	Deploy a password management tool.	CYT-00000233135
 Inconsistent and unsecure domain controller configurations may lead to security vulnerabilities, an increased attack surface and a compromised Active Directory.	Standardize and update domain controller configuration settings, operating systems and protocols.	CYT-86899049432
 Sensitive and private data is not encrypted in transit.	Encrypt all sensitive data in transit.	CYT-00000757544
 The company does not have a mechanism for setting thresholds for incident alerts, which may result in overlooking potential attacks or significant security events.	Apply alert thresholds and identify potential attacks	CYT-00000959963
 No verification relating to the security best practices of your website's or web app's hosting provider.	Maintain security best practices for third party hosted web servers.	CYT-00000593957
 There are no cybersecurity exercises for employees.	Conduct attack simulations for all employees.	CYT-00000555493
 The organization cannot plan the adequate protection levels for assets that store, process, and transmit sensitive information.	Categorize hardware and system assets according to their level of sensitivity as defined in the data protection policy.	CYT-00000395293
 Company networks are not properly segmented.	Separate information flows by segmenting company networks.	CYT-00000924331
 Company network computers can directly access the internet.	Enforce the channeling of internet access from company networks through a web security solution.	CYT-00000105315
 No vulnerability management plan in place.	Establish and use a vulnerability management policy and plan.	CYT-00000933946

Appendix B

Open tasks by domain - Access

 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
<p> Failing to implement controls that trigger automated notices for changes in user access permissions may result in unauthorized access and lack of transparency in access management.</p>	<p>Automate notices to appropriate personnel for changes to user access permissions.</p>	<p>CYT-72084815841</p>
<p> Failure to implement controls that prevent unauthorized access to cryptographic keys can result in the compromise of critical security assets and encryption keys.</p>	<p>Implement controls that prevent unauthorized access to cryptographic keys.</p>	<p>CYT-87994462010</p>

Appendix B

Open tasks by domain - Active Directory

 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
<p> Inconsistent and unsecure domain controller configurations may lead to security vulnerabilities, an increased attack surface and a compromised Active Directory.</p>	<p>Standardize and update domain controller configuration settings, operating systems and protocols.</p>	<p>CYT-86899049432</p>
<p> Weak algorithms and the existence of backward compatibility when not required increases the possibility of unauthorized access, presents known vulnerabilities for malicious actors to exploit and reduces overall network security.</p>	<p>Ensure protocols use strong encryption algorithms and disable backward compatibility across domain controllers.</p>	<p>CYT-20359254748</p>

Appendix B

Open tasks by domain - Asset Management




 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
 The organization cannot plan the adequate protection levels for assets that store, process, and transmit sensitive information.	Categorize hardware and system assets according to their level of sensitivity as defined in the data protection policy.	CYT-00000395293
 The organization does not know what systems need to be protected.	Identify all assets and establish an asset inventory.	CYT-00000304608
 Failing to conduct regular reviews of critical systems supported by legacy technologies may result in unidentified vulnerabilities and security gaps, increasing the risk of cyberattacks.	Review critical systems supported by legacy technologies to identify potential vulnerabilities, upgrade opportunities, or new defense layers.	CYT-14756261722

Appendix B

Open tasks by domain - Awareness

 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
<p> There are no cybersecurity exercises for employees.</p>	<p>Conduct attack simulations for all employees.</p>	<p>CYT-00000555493</p>
<p> Not providing basic cybersecurity awareness materials to customers may result in customers falling victim to phishing attacks impersonating the company, potentially leading to reputational damage and financial losses.</p>	<p>Ensure customer awareness materials are readily available.</p>	<p>CYT-27473034528</p>
<p> Failing to provide security awareness training to customers annually may result in customers being less vigilant about cybersecurity threats and more susceptible to cyberattacks.</p>	<p>Provide retail customers and commercial clients with cybersecurity awareness training information, at least annually.</p>	<p>CYT-28855738172</p>
<p> Using generic, company-wide security awareness training may result in employees not fully understanding the specific risks associated with their business unit, leading to inadequate protection against targeted threats.</p>	<p>Provide business units with cybersecurity training relevant to their particular department's risks.</p>	<p>CYT-60480630535</p>

Appendix B

Open tasks by domain - Compliance and Auditing


 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
● Not all company compliance requirements have been identified.	Identify all regulatory requirements and standards which apply to the company.	CYT-00000016508
● Cybersecurity controls may need to be updated to ensure effectiveness.	Conduct cybersecurity control functional reviews.	CYT-00000969080
● There is no compliance and governance plan.	Establish a compliance and governance plan.	CYT-00000002079
● Failing to ensure that threat intelligence aligns with the organization's risk posture and size may result in ineffective threat assessments and misalignment with the company's risk management strategy.	Ensure the internal audit validates that the threat intelligence received matches the organization's risk posture and size.	CYT-38720857610
● Not updating the processes and procedures for internal audit evaluations in line with changes to the company's risk profile may result in misalignment between audit activities and risk management strategy.	Implement a process to update the internal audit function based on risk profile changes to the company.	CYT-11984182620
● Failure to regularly review the organization's cybersecurity risk appetite statement may result in outdated risk tolerance guidelines and ineffective alignment with the company's risk management strategy.	Ensure the internal audit regularly reviews the cyber risk appetite statement.	CYT-45480328816

Appendix B

Open tasks by domain - Data Protection


 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
 Sensitive and private data is not encrypted in transit.	Encrypt all sensitive data in transit.	CYT-00000757544

Appendix B

Open tasks by domain - Domain and DNS

 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
 DNS is not fault tolerant	Enable the use of both a primary and secondary DNS server.	CYT-87543968984

Appendix B

Open tasks by domain - Endpoints and Mobile Devices

 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
<p> Failing to validate software versions and patches on mobile devices used for remote access may result in security gaps and non-compliance with security standards.</p>	<p>Validate software versions and patches for any mobile devices connecting to the corporate network for storing and accessing company information.</p>	CYT-43536648264

Appendix B

Open tasks by domain - Environmental Control




 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
● Environmental hazards are not considered when selecting a facility location	Undertake facility location planning to minimize physical and environmental hazards.	CYT-09958734532
● Systems cannot be powered off in an emergency	Install emergency shutoff switches or devices for power in critical facilities.	CYT-85176276044

Appendix B

Open tasks by domain - Hosted Network

 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
 Company networks are not properly segmented.	Separate information flows by segmenting company networks.	CYT-00000924331
 Company network computers can directly access the internet.	Enforce the channeling of internet access from company networks through a web security solution.	CYT-00000105315
 There are no network traffic anomaly detection and prevention security controls.	Deploy network traffic anomaly detection and prevention security controls.	CYT-00000609986

Appendix B

Open tasks by domain - Human Resources

 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
<ul style="list-style-type: none">● Failing to have an ongoing HR program for recruiting, retaining, and developing cybersecurity staff may lead to a shortage of qualified personnel, compromising the effectiveness of the organization's security programs.	Implement a program for talent recruitment, retention, and succession planning for the cybersecurity and resilience staff.	CYT-95771075299
<ul style="list-style-type: none">● Failing to establish a cybersecurity-related mindset and culture may result in employees making decisions that do not prioritize cybersecurity, potentially leading to security vulnerabilities.	Promote a risk culture requiring formal consideration of cybersecurity risks in all business decisions.	CYT-39716472902

Appendix B

Open tasks by domain - Incident Response






 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
● No third-party Incident Response (IR) support.	Engage a third-party incident response vendor for fast response and post-incident reviews.	CYT-00000373508
● Implementing changes to systems or access rights for incident management without formal approval may introduce security risks and vulnerabilities.	Ensure that any changes pertaining to incident management are approved by management prior to implementation.	CYT-74194826294
● Having no plans to re-route or substitute critical functions and services affected by a successful attack on internet-facing systems may result in disruptions to operations and services.	Provide plans to re-route or substitute critical functions and services that may be affected by a successful cyber attack.	CYT-07524877459
● No use of automated incident response tools.	Implement an automated incident response tool, such as an Endpoint Detection and Response (EDR), to be able to respond to an attack and contain it.	CYT-00000175316
● Failing to conduct resilience testing aligned with realistic and emerging threats may leave the institution unprepared to respond effectively to actual cyber incidents.	Perform resilience testing based on analysis and identification of realistic and highly likely threats.	CYT-09489481954
● Failing to reconfigure and thoroughly test restored assets before putting them back into operation may result in security weaknesses and vulnerabilities.	Establish processes that ensure restored assets are appropriately reconfigured and thoroughly tested prior to operating.	CYT-50676351900
● Not quarantining, removing, disposing of, or replacing assets affected by a security incident may result in ongoing security vulnerabilities and potential re-infections.	Implement processes for assets affected by a security incidents.	CYT-96324412294
● Not preparing an annual report of security incidents may result in a lack of transparency and awareness of security issues among the board and relevant stakeholders.	Produce an annual board report consisting of security incidents or violations.	CYT-28771812576
● Not actively participating in sector-specific cyber exercises or scenarios may result in insufficient incident response capabilities and preparedness.	Ensure the company engages in sector-specific cyber exercises or scenarios.	CYT-68368038235

Appendix B

Open tasks by domain - Information Security Management

 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
 Security planning is not included in organizational plans and budgets	Establish a discrete line item for information security and privacy in budget.	CYT-74448617961
 Failing to assess the risks posed by external critical infrastructure could leave the company unprepared for disruptions, potentially leading to operational failures.	Ensure any critical infrastructure risks that could affect the institution are considered.	CYT-82672974730
 Without an annual report, the board may lack crucial insight into the state of information security and business continuity programs, potentially leading to uninformed decision-making.	Provide a management report to the board detailing the overall status of information security and business continuity programs.	CYT-20983795950
 The absence of threat intelligence and security posture metrics from a board meeting may result in the board lacking critical insights into emerging cyber threats and the company's security readiness.	Address threat intelligence trends and the organization's security posture, in order to enhance the board meeting package.	CYT-19661001886
 Without a board approved cyber risk appetite statement, the company may lack a clear framework for managing cyber risks, potentially leading to inconsistent risk management practices.	Produce a cyber risk appetite statement for the organization and gain board approval.	CYT-56064130724

Appendix B

Open tasks by domain - Logging and Monitoring

 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
● The company does not have a mechanism for setting thresholds for incident alerts, which may result in overlooking potential attacks or significant security events.	Apply alert thresholds and identify potential attacks	CYT-00000959963
● Failing to implement tools to detect unauthorized data mining may result in insider threats and data breaches.	Implement the use of tools to detect unauthorized data mining.	CYT-53354755912
● Unreliable event detection processes may result in missed security events and delayed responses to incidents.	Ensure that event detection processes are proven reliable.	CYT-84895482286

Appendix B

Open tasks by domain - On-Premises Network

 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
● Failing to configure perimeter firewalls for wireless network environments to restrict unauthorized traffic may result in unauthorized access to wireless networks and potential security breaches.	Implement and configure any wireless network environments with perimeter firewalls to restrict unauthorized traffic.	CYT-35444853947
● Failing to extend monitoring controls to cover all internal network-to-network connections may result in undetected unauthorized activities and potential security breaches within the company's internal network.	Establish monitoring controls for the coverage of all internal, network-to-network connections.	CYT-47442597480
● The absence of posture checking tools to automatically block access from unpatched devices may result in security vulnerabilities and potential breaches.	Use tools to automatically block attempted access from unpatched employee and third-party devices.	CYT-79701691554
● Allowing the broadcast range of wireless network(s) to extend beyond company-controlled boundaries may expose the network to unauthorized access from outside secure areas, increasing the risk of security breaches.	Confine broadcast range of the wireless network(s) to company-controlled boundaries.	CYT-60843423896

Appendix B

Open tasks by domain - Operational Technology (OT) Security



 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
<p>● The lack of robust protective measures and prompt alert mechanisms leaves the organization exposed to risks such as operational interruptions and potential breaches, necessitating regular enhancements and reviews of these measures to effectively mitigate and manage such risks.</p>	<p>Implement alert mechanisms for unauthorized operations on OT components</p>	<p>CYT-26122942724</p>
<p>● The absence of correctly implemented and maintained secure and restricted remote access protocols exposes OT components to unauthorized access and exploitation, posing a significant risk to the organization's security posture.</p>	<p>Implement secure and restricted remote access to OT components.</p>	<p>CYT-89085502729</p>
<p>● Improper integration or suboptimal configuration of IDS/IPS solutions can compromise the security of OT networks, leading to potential operational failures due to undetected threats or false positives disrupting critical processes.</p>	<p>Implement intrusion detection and prevention systems (IDS/IPS) in OT networks.</p>	<p>CYT-94892600043</p>
<p>● If the organization lacks stringent network segregation between controllers and workstations, it remains vulnerable to potential security breaches, emphasizing the need for regular assessment and enhancement of network configurations and firewall rules.</p>	<p>Establish network separation between controllers and workstations.</p>	<p>CYT-63379574665</p>
<p>● If controls limiting the capabilities of privileged users in OT components aren't in place, the organization remains vulnerable to both inadvertent mistakes and intentional malicious actions from inside or outside.</p>	<p>Limit privileged user capabilities in OT components.</p>	<p>CYT-14054168223</p>
<p>● A lack of well-defined, enforced, and regularly updated network filtering rules for ports and protocols leaves the organization vulnerable to security incidents, emphasizing the necessity for rigorous and ongoing measures to restrict communication within the OT network.</p>	<p>Establish OT network filtering and communication restrictions.</p>	<p>CYT-72766182800</p>

Appendix B

Open tasks by domain - Operations and Maintenance


 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
 Sensitive systems are not physically and logically partitioned	Implement the separation of systems both physically and logically	CYT-07589354170
 Systems are not covered under maintenance contracts	Ensure timely maintenance during a failure.	CYT-26701877524

Appendix B

Open tasks by domain - Passwords and Secrets

 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
 Passwords and secrets are not managed by a password management tool.	Deploy a password management tool.	CYT-00000233135

Appendix B

Open tasks by domain - Privacy

 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
<ul style="list-style-type: none">● Service providers do not properly handle the company's consumer personal data.	Implement a process for the handling of personal data by service providers.	CYT-45186167661

Appendix B

Open tasks by domain - Risk Management

 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
<p> Failing to identify and enhance authentication controls for internet-based systems and high-risk transactions may result in increased vulnerability to cyberattacks targeting critical assets.</p>	<p>Ensure the risk assessment identifies internet-based systems and high-risk transactions that require additional authentication controls.</p>	<p>CYT-80251144685</p>
<p> There is no qualified individual accountable and responsible for risk management</p>	<p>Ensure that management assigns a qualified individual to be accountable for and ensure organization-wide risk management.</p>	<p>CYT-81276287416</p>
<p> Neglecting to address non-technological risks (e.g.: financial, strategic, regulatory, and compliance risks) in the risk management program may lead to unanticipated consequences and losses.</p>	<p>Include non-technological cyber risks in the company's risk management program.</p>	<p>CYT-44502389556</p>
<p> Failing to calculate and understand the impact of cybersecurity incident losses per business unit or department may result in misallocation of resources and an inadequate response to incidents.</p>	<p>Implement a process to analyze and assign potential losses and expenses related to cybersecurity incidents, per business unit.</p>	<p>CYT-86567805363</p>
<p> Neglecting to adjust the risk assessment process to consider widely known risks and best practices may lead to inadequate risk management and failure to address known threats effectively.</p>	<p>Adjust the risk assessment for widely known risks or common risk management practices.</p>	<p>CYT-44451984968</p>
<p> Not monitoring and remediating high residual risks from risk assessments may result in unaddressed vulnerabilities and potential security incidents.</p>	<p>Monitor moderate and high residual risk issues from the cybersecurity risk assessment until items are addressed.</p>	<p>CYT-23838603045</p>
<p> Not presenting and discussing cybersecurity at independent risk management meetings may result in a lack of focus on cyber risks and inadequate risk management.</p>	<p>Present and discuss cyber risk reports at independent risk management meetings.</p>	<p>CYT-45992244421</p>

Appendix B

Open tasks by domain - Service Provider and Vendor Management






 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
● Failing to establish procedures for monitoring and testing third-party connections may result in unmanaged security risks and vulnerabilities in external connections.	Monitor and test controls for primary and backup third-party connections on a regular basis.	CYT-80481403917
● Counterfeit or tampered assets can come into the organization through the supply chain	Use techniques to secure the procurement process.	CYT-38482053330
● Failing to review due diligence results and management's recommendations regarding third-parties may result in insufficient oversight of external partners and potential risks.	Ensure the board, board committee or appointed professional reviews a summary of due diligence results including management's recommendations regarding the use of third-parties.	CYT-08119651130
● Not conducting pre-contract physical site visits of high-risk vendors may lead to the inadequate assessment of vendor security and reliability.	Arrange physical, pre-contract site visits of high-risk vendors by the company or a qualified third-party.	CYT-89925731888
● Failing to implement automated reminders for third-party information collection may result in outdated or incomplete information, hindering effective risk management.	Implement automated reminders to identify when required third-party information needs to be obtained or analyzed.	CYT-87709970352
● Failing to design and verify security controls for detecting and preventing intrusions from third-party connections may expose the company's systems to unauthorized access and security breaches.	Ensure security controls are designed and verified to detect and prevent intrusions from third-party connections.	CYT-10205531696
● Not scaling the monitoring of third-parties based on risk may result in misallocation of resources and attention, leaving high-risk third-parties inadequately monitored.	Align the monitoring of third-parties in accordance with the associated risk they pose.	CYT-67261660292
● The absence of monitoring controls covering all external connections may result in limited visibility into potential threats and security incidents involving third-party service providers, business partners, and customers.	Establish the use of monitoring controls to cover all external connections (e.g.: third-party service providers, business partners, customers).	CYT-28368252719
● Failing to implement a process to identify new third-party relationships, including those established without formal approval, may result in a lack of visibility into potential security risks.	Establish a process to identify new third-party relationships, including those that were established without formal approval.	CYT-93026290521

Appendix B

Open tasks by domain - Threat Intelligence

 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
<p> Failing to maintain threat intelligence in a read-only repository may lead to the unintentional modification of indicators, potentially resulting in inaccurate threat data when referenced.</p>	<p>Store and maintain a read-only, central repository of cyber threat intelligence.</p>	<p>CYT-13307166974</p>
<p> Failing to establish and maintain an efficient SOC or equivalent may result in delayed or inadequate responses to security incidents, increasing the company's exposure to cyber risks.</p>	<p>Establish and maintain a Security Operations Center (SOC) or equivalent, for centralized and coordinated security processes and technology.</p>	<p>CYT-94394584660</p>
<p> Not establishing information-sharing agreements may hinder the company's ability to collaborate with other organizations and share threat information, reducing collective cybersecurity efforts.</p>	<p>Use information-sharing agreements to facilitate sharing threat information with other financial sector organizations or third-parties.</p>	<p>CYT-44412597262</p>
<p> Failing to proactively share threat information with industry peers, law enforcement, regulators and information-sharing forums may result in a lack of collective awareness and cooperation in addressing cyber threats.</p>	<p>Share threat information proactively with the industry, law enforcement, regulators, and information-sharing forums.</p>	<p>CYT-96028906492</p>
<p> Not communicating and collaborating with the public sector regarding cyber threats may limit the company's access to government resources and support during cybersecurity incidents.</p>	<p>Communicate and collaborate with the public sector regarding cyber threats.</p>	<p>CYT-89570424490</p>

Appendix B

Open tasks by domain - Vulnerability Management

 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
● No vulnerability management plan in place.	Establish and use a vulnerability management policy and plan.	CYT-00000933946
● Penetration testing is not conducted for externally exposed assets.	Conduct penetration testing for externally exposed assets.	CYT-00000313367
● Found vulnerabilities are not remediated.	Remediate vulnerabilities found during vulnerability assessment and penetration testing.	CYT-00000072154
● Failing to test and apply patches for high-risk vulnerabilities promptly may expose the company's systems to exploitation by cyber adversaries, leading to security breaches and data compromise.	Ensure that patches are tested and applied upon release for high-risk vulnerabilities.	CYT-04263220318
● Penetration testing is not conducted for internal assets and network.	Conduct penetration testing for internal assets and networks.	CYT-00000553099
● There is no penetration testing program.	Establish and maintain a penetration testing program.	CYT-00000604116
● Not conducting thorough security investigations and forensic analysis of incidents may result in inadequate understanding of security breaches and their root causes.	Assign qualified staff or third-parties to perform security investigations, forensic analysis, and undertake remediation.	CYT-89792929071
● Failing to adhere to generally accepted forensic procedures may compromise the integrity of evidence, affecting the company's ability to support legal actions against cyber adversaries.	Use accepted and appropriate forensic procedures, including chain of custody, to gather and present evidence to support potential legal action.	CYT-20391475226
● The absence of thorough reviews of penetration testing activities may result in ineffective testing and missed vulnerabilities.	Review the penetration testing scope and results to help determine the need for rotating companies based on the quality of work.	CYT-64345490643

Appendix B

Open tasks by domain - Website and Web Application

 Repeat task  Repeat task - overdue

ISSUE	RECOMMENDATION	ID
● No verification relating to the security best practices of your website's or web app's hosting provider.	Maintain security best practices for third party hosted web servers.	CYT-00000593957
● A lack of proactive monitoring to detect and respond to anomalous behavior in real time may result in missed security incidents and increased risk.	Monitor online customer transactions for anomalous behavior.	CYT-24481639948