Sample Report*

HEALTHCARE TRIANGLE | cynomi

ACME Cybersecurity Risk Remediation Plan

September 3, 2023

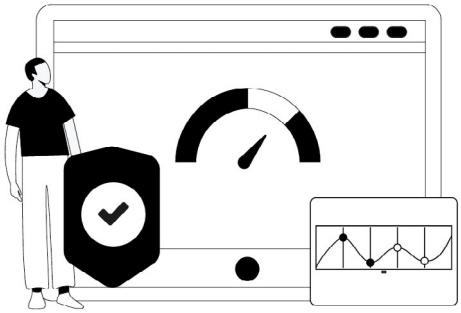
* This sample report is generated by the Cynomi virtual CISO platform and delivered to the client by the service provider. The process of running the assessment to generate the report takes an average of 2-4 hours. This printed report version represents only some of the information available in the full report.

Powered by cynomi

Posture score

6.3

Basic protection measures have been taken. Only the most basic attacks are blocked.



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.

Good

6.2

Website Defacement

An unauthorized and malicious modification of web page content.

Good

6.5

Ransomware

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

Good

6.4

Fraud

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

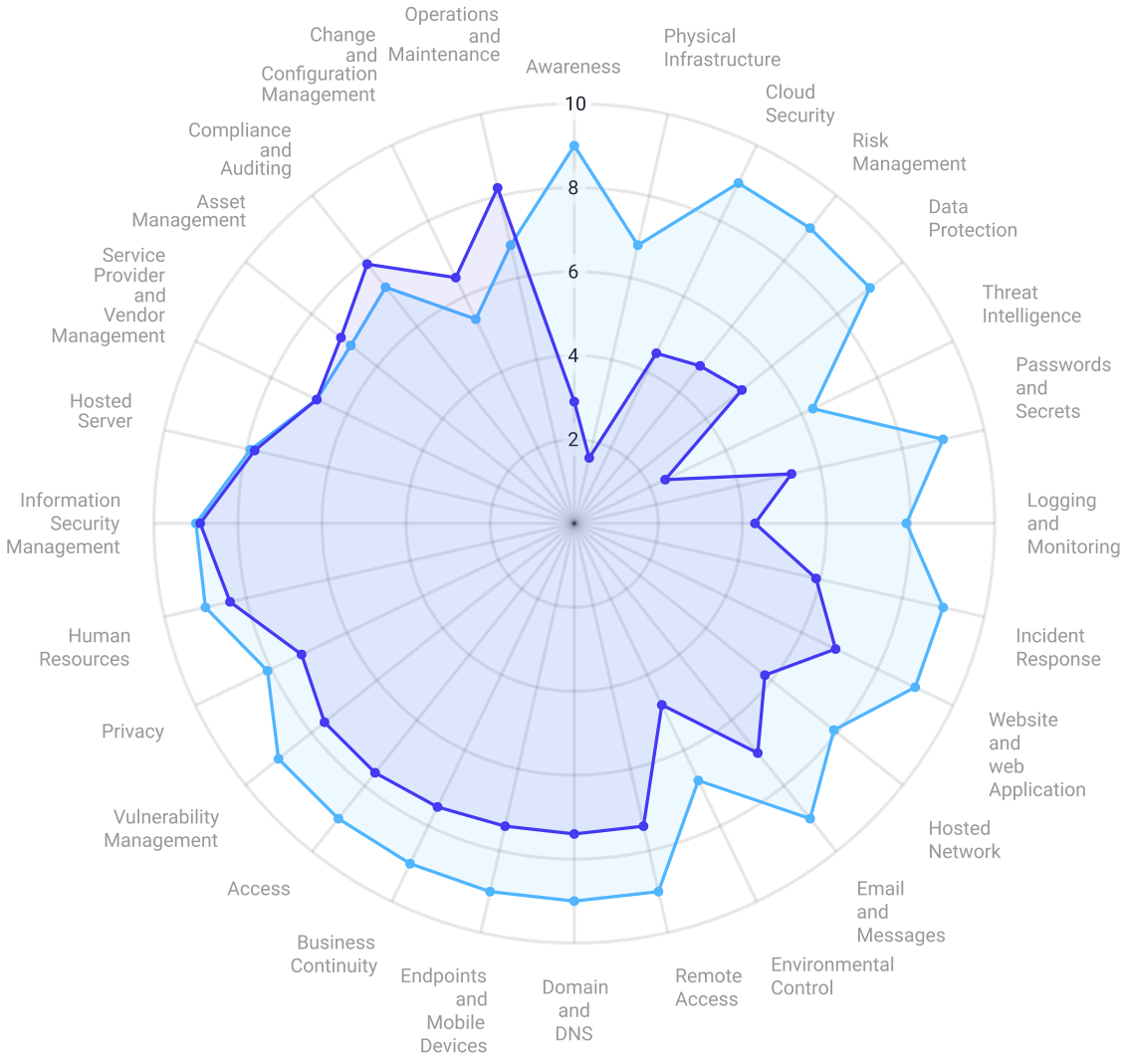
Good

6.2

Cybersecurity readiness level

28	5	23
Total Policies	Meet target score	Under target score

A mapping process of your organization shows that 28 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.

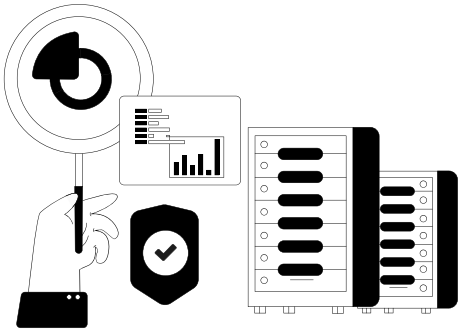


Company readiness by security domain

DOMAIN	SCORE
Access	7.6
Asset Management	7.1
Awareness	2.9
Business Continuity	7.5
Change and Configuration Management	6.5
Cloud Security	4.5
Compliance and Auditing	7.9
Data Protection	5.1
Domain and DNS	7.4
Email and Messages	7
Endpoints and Mobile Devices	7.4
Environmental Control	4.8
Hosted Network	5.8
Hosted Server	7.8
Human Resources	8.4
Incident Response	5.9
Information Security Management	8.9
Logging and Monitoring	4.3
Operations and Maintenance	8.2
Passwords and Secrets	5.3
Physical Infrastructure	1.6
Privacy	7.2
Remote Access	7.4
Risk Management	4.8
Service Provider and Vendor Management	6.8
Threat Intelligence	2.4
Vulnerability Management	7.6
Website and web Application	6.9

Scan findings

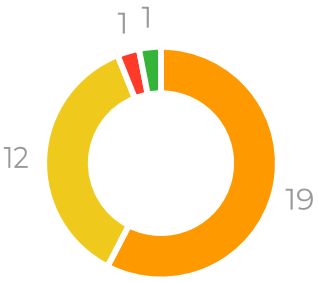
- Internal network scan
- External scan
- Microsoft Secure Score
- External Nessus scan



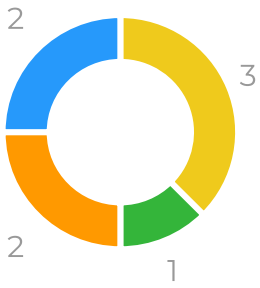
Scanning networks and applications exposes hidden infrastructure vulnerabilities. Addressing these vulnerabilities will reduce the chances of your organization being the subject of a cyberattack.

67	2	22	37	4	2
Total findings	Critical	High	Medium	Low	Info

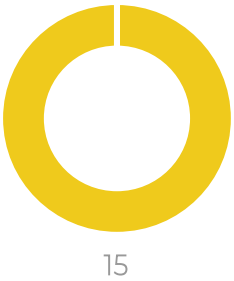
Internal network scan



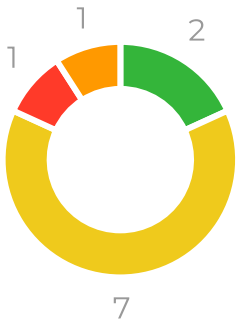
External scan



Microsoft Secure Score



External Nessus scan



Sample findings

Sample findings

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

SOURCE	SEVERITY	FINDING	ASSET
Internal network scan	Critical	On-premises workstation password in not required for computer users	192.16.0.11
External Nessus scan	Critical	SSL Version 2 and 3 Protocol Detection	127.7.4.123
Internal network scan	High	Not all domain controllers are set up with the same operating system	192.168.0.11
Internal network scan	High	On-premises workstation is missing security patches	192.16.0.11
Internal network scan	High	On-premises workstation antivirus is out of date	192.16.0.11

Risk mitigation plan

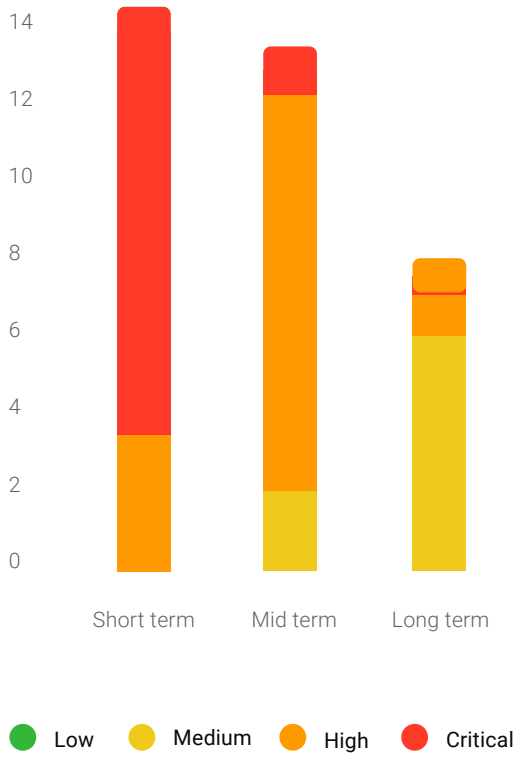
The risk assessment of your company revealed 409 tasks to address. 34 tasks have been added to your risk mitigation plan.

34	12	14	8	0
Total findings	Critical	High	Medium	Low

29% tasks completed

24 Open tasks

Plan breakdown



Task status

10	12
Completed*	Not started
9	3
In progress	Deferred

0

Deferred

* Includes tasks in status done or fulfilled

Appendix A - Work Plan

Short term

NAME	POLICY	STATUS	DUE DATE	ID
Setting password length and structure	Passwords and Secrets	Fulfilled	Oct 3, 2023	CYT-00000999533
Enforcing password complexity rules	Passwords and Secrets	Fulfilled	Oct 31, 2023	CYT-00000784598
Implementing Multi-Factor Authentication for external-access assets and services	Access	Done	Sep 29, 2023	CYT-00000617212
Training employees in general cybersecurity awareness	Awareness	Done	Oct 25, 2023	CYT-00000720276
Setting alert thresholds and identifying potential attacks	Logging and Monitoring	In progress	Sep 27, 2023	CYT-00000959963
Securing web internet access	Hosted Network	In progress	Oct 4, 2023	CYT-00000105315
Training company management in cybersecurity awareness	Awareness	In progress	Oct 12, 2023	CYT-00000097378
Preparing for power outage	Environmental Control	In progress	Oct 25, 2023	CYT-00000771169
Conducting cybersecurity simulation exercises	Awareness	In progress	Oct 27, 2023	CYT-00000555493
Controlling communication and computing area access	Physical Infrastructure	In progress	None	CYT-00000996872
Enforcing Multi-Factor Authentication for remote access	Hosted Network	In progress	Oct 26, 2023	CYT-00000642532
Training Physical Security Personnel in Cybersecurity Awareness	Awareness	In progress	Oct 26, 2023	CYT-69955260505
Creating strong passwords using best practices	Passwords and Secrets	In progress	Oct 31, 2023	CYT-00000106274
Backing up network device data and configuration	Business Continuity	Review	Sep 29, 2023	CYT-00000649110

Appendix A - Work Plan

Mid term

42 tasks

NAME	POLICY	STATUS	DUE DATE	ID
Deploying password management tool	Passwords and Secrets	Fulfilled	None	CYT-00000233135
Enforcing password change on first login	Passwords and Secrets	Fulfilled	None	CYT-00000173037
Enforcing physical access control and audit log management for facility entry and exit points	Physical Infrastructure	Fulfilled	None	CYT-00000010800
Training cybersecurity personnel and IT administrators in cybersecurity awareness	Awareness	Review	None	CYT-00000801509
Collecting and storing all awareness training data	Awareness	Not started	None	CYT-00000906502
Creating a management process and policy for passwords and secret authentication information	Passwords and Secrets	Not started	None	CYT-69380916206
Setting password history limit	Passwords and Secrets	Not started	None	CYT-00000694130
Prohibiting storing clear text passwords in local files	Passwords and Secrets	Not started	None	CYT-00000618272
Prohibiting using the same password for different accounts and services	Passwords and Secrets	Not started	None	CYT-00000678163
Managing site access authorization	Physical Infrastructure	Not started	None	CYT-00000971513
Protecting sensitive and removable assets	Physical Infrastructure	Review	None	CYT-00000905568
Implementing physical security for sites and equipment	Physical Infrastructure	Not started	None	CYT-86108571158

NIST-CSF Compliance Report

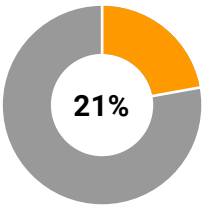
Company coverage

Total controls

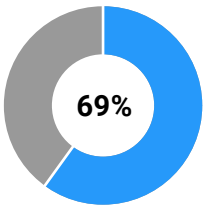
NIST-CSF

59% completed

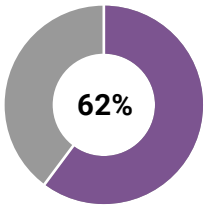
Function



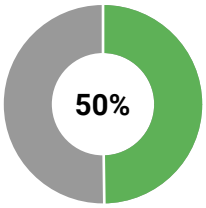
Detect (DE)



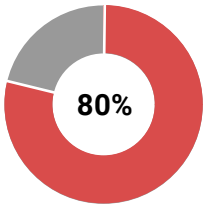
Identify (ID)



Protect (PR)



Recover (RC)



Respond (RS)

NIST-CSF Compliance Report

CONTROL	NAME	CONTROL STATUS
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	Partially
DE.AE-2	Detected events are analyzed to understand attack targets and methods	Not Implemented
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	Not Implemented
DE.AE-4	Impact of events is determined	Not Implemented
DE.AE-5	Incident alert thresholds are established	Not Implemented
DE.CM-1	The network is monitored to detect potential cybersecurity events	Partially
DE.CM-2	The physical environment is monitored to detect potential cybersecurity events	Partially
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	Not Implemented
DE.CM-4	Malicious code is detected	Implemented
DE.CM-5	Unauthorized mobile code is detected	Partially
DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events	Not Implemented
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	Not Implemented
DE.CM-8	Vulnerability scans are performed	Not Implemented
DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability	Partially
DE.DP-2	Detection activities comply with all applicable requirements	Not Implemented
DE.DP-3	Detection processes are tested	Partially
DE.DP-4	Event detection information is communicated	Not Implemented
DE.DP-5	Detection processes are continuously improved	Not Implemented

About Healthcare Triangle

Healthcare Triangle, Inc.TM (HCTI), based in Pleasanton, Calif., reinforces healthcare progress through breakthrough technology. HCTI achieves HITRUST Certification for Cloud and Data Platform (CaDP) to manage risks.

We support healthcare and life sciences organizations improve health outcomes by enabling the adoption of new technologies, data enlightenment, business agility, and accelerating the value of their IT investments. HC/LS turn to HCTI for expertise in cloud transformation, security and compliance, data lifecycle management, and clinical/business performance optimization.

For more information, please visit www.healthcaretriangle.com

Get in Touch 888.706.0310 | info@healthcaretriangle.com

About Cynomi

MSPs, MSSPs and consulting firms leverage Cynomi's AI-powered, automated vCISO platform to provide vCISO services at scale - without scaling their existing resources.

Cynomi's multitenant platform automatically generates everything a vCISO needs: risk and compliance assessments, tailored security policies, actionable remediation plans with prioritized tasks, task management tools & customer-facing reports.

Scale Revenues | Increase Upsell | Minimize Churn | Increase Sales Pipeline

www.cynomi.com