Secur-Serv CyberVue

Your Company Cybersecurity Analysis Report

Sample Report

Powered by cynomi

Introduction

View core results, security vulnerabilities, sample findings and security score examples from Secur-Serv CyberVue.

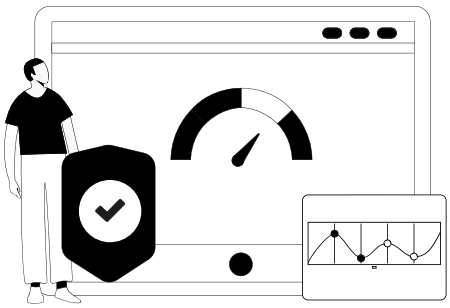
"The key to success is a well-constructed cybersecurity strategy with clear priorities. Spending must be balanced between people and technology with careful consideration for which risks should be addressed in which order. Decision-makers must be mindful of how their choices map against the NIST Cybersecurity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

Posture score

0.1

Protection measures have not been taken. The organization is exposed to cyber threats.



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.

0.1

Poor

Website Defacement

An unauthorized and malicious modification of web page content.

0.1

Poor

Ransomware

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

0.1

Poor

Fraud

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

0.1

Poor

Cybersecurity readiness level

29	0	29
Total Domains	Meet target score	Under target score

A mapping process of your organization shows that 29 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 good cyber hygiene, address the security domains with large gaps between the target score.

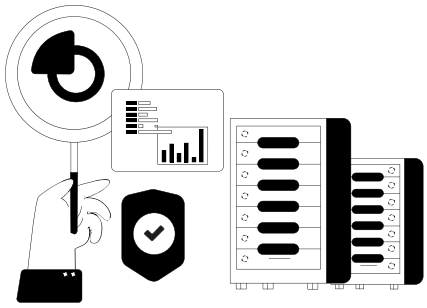
Company readiness by security domain

DOMAIN	SCORE
Access	0
Active Directory	0
Asset Management	0
Awareness	.5
Business Continuity	0
Change and Con guration Management	0
Compliance and Auditing	0
Data Protection	0
Domain and DNS	0
Email and Messages	0
Endpoints and Mobile Devices	0
Environmental Control	0
Human Resources	0
Incident Response	0
Information Security Management	0
Logging and Monitoring	0
Microsoft 365	0
On-Premises Network	0
On-Premises Server	0
Operational Technology (OT) Security	0
Operations and Maintenance	0
Passwords and Secrets	0
Physical Infrastructure	0
Remote Access	0
Risk Management	0
Service Provider and Vendor Management	0
Threat Intelligence	0
Vulnerability Management	0
Website and web Application	0

Results vary depending on IT environment. To learn more about your customized report, talk to a Secur-Serv representative.
Call 800.228.3628 or visit secur-serv.com

Scan Findings

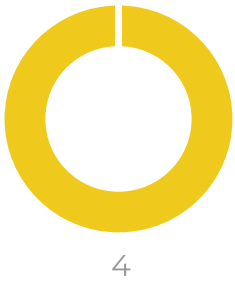
- Microsoft Secure Score
- External scan



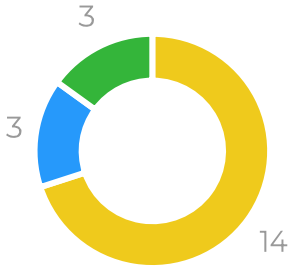
Scanning networks and applications exposes hidden infrastructure vulnerabilities. Addressing these vulnerabilities will reduce the chances of your organization being the subject of a cyberattack.

24	0	0	18	3	3
Total ndings	Critical	High	Me di um	Low	Info

Microsoft Secure Score



External scan



Scan 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
Microsoft Secure Score	Medium	Outgoing emails containing malware attachments are not blocked.	Microsoft 365 Cloud
Microsoft Secure Score	Medium	Teams meeting admission is not restricted to invited users.	Microsoft 365 Cloud
Microsoft Secure Score	Medium	Content sharing during Teams meetings is not restricted.	Microsoft 365 Cloud
Microsoft Secure Score	Medium	There is no restriction for joining Teams meetings.	Microsoft 365 Cloud
External scan	Medium	HTTP to HTTPS Redirect Not Enabled	https://yourcompany.com

Risk mitigation plan

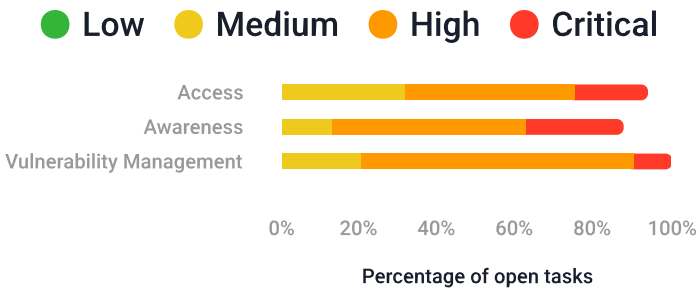
Completing critical and high severity tasks will impact organization cybersecurity the most, and increase posture score.

32	6	18	8	0
Open tasks	Critical	High	Medium	Low

6% tasks completed

32 Open tasks

Open tasks



Task status

32

Not started

Appendix A

Top 5 open tasks

The top 5 open tasks which impact your security posture the most.

	ISSUE	RECOMMENDATION	ID
🔴	New software vulnerabilities and security miscon gurations, which are inherent in any network or system, remain hidden and unmitigated.	Conduct external vulnerability assessments.	BFT-320107803
🔴	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.	BFT-0290021859
🔴	Some users lack unique identi cation.	Ensure that each user is assigned a unique identi er before being granted access to systems and services, avoiding the use of shared or generic accounts.	BFT-144276856
🟠	Unknown vulnerabilities in your company's web applications and APIs.	Conduct web application vulnerability assessments.	BFT-480061 00122
🟠	No vulnerability management plan in place.	Establish and use a vulnerability management policy and plan.	BFT-00333555095