THREATMATE™

YOUR NEXT MOVE

Generated on 9/2/2024

Cybersecurity Executive Report

Prepared for root

threatmate.com

Overall Risk Profile for root

ThreatMate continuously monitors the security across external, internal and cloud attack surfaces. The overall score includes into consideration all the attack surfaces and serves as an overall security metric.

The table below shows the categories that will improve the security score. The value of the category represents the category risk. If the issues in the category are addressed then the overall score will be improved by that much.

7.66	Internal Vulnerability Scan	Measures the vulnerability impact of internal services.
7.53	Endpoint OS Patch Management	Measures the vulnerability impact of unpatched operating systems.
0.64	Endpoint Application Patch Management	Measures the vulnerability impact of third party applications.
0.18	Internal TLS Scan	Measures the TLS security of internal services. This includes expired certificates and weak ciphers.
0.12	Endpoint Compliance	Measures the impact of non-compliant devices.
0.10	External TLS Scan	Measures the TLS security of services exposed to the Internet. This includes expired certificates and weak ciphers.
0.05	Internal Compliance Scan	Measures the compliance impact of internal services.
0.01	External Compliance Scan	Measures the compliance impact of services exposed to the Internet.

External Assets	Total Users	Internal Assets	Total Issues
26	19	76	186

External Security for root

ThreatMate continuously monitors company websites, subdomains, routers and firewalls for exposures. This comprises the external attack surface. ThreatMate also performs continuous automated penetration tests. External exposures bear the highest risk since anyone on the internet could find them and exploit them. The external score represents 50% of the overall security score.

The domain security checks the SPF and DMARC configuration for all subdomains that have an MX record. In summary, SPF establishes which IP addresses are allowed to send emails for a domain, while DMARC provides policies for handling emails that fail authentication, thus helping to prevent email fraud and improve email deliverability.

Domain Security (Top 5)

Name	SPF Status	DMARC Status
cybervault.app	OK	Missing
cybervault.app	OK	Missing

The table below shows the Top 5 most vulnerable external assets.

External Assets (Top 5)

Address	Hostname	Security Score	Exposures

The table below shows the Top 5 most vulnerable external hosts based on the last penetration test.

External Penetration Test (Top 5)

Address	Hostname	Total Exposures ↓	Low	Medium	High	Critical
demo.threatmate.com		1	1	0	0	0
staging.threatmate.com		1	1	0	0	0

Internal Security for root

ThreatMate continuously monitors the company internal assets for exposures. This includes company laptops, workstations, servers, Internet of Things devices such as printers, cameras and TVs and anything else connected to the internal company networks. ThreatMate also covers remote user devices running the ThreatMate endpoint agent.

The table below represents the Top 5 most vulnerable internal assets.

Internal Assets (Top 5)

Address	Hostname	Security Score	Exposures
172.20.0.3	172.20.0.3	9.75	107
172.20.0.19	172.20.0.19	9.75	177
172.20.0.35	172.20.0.35	9.75	126
172.20.0.49	172.20.0.49	9.53	14
172.20.0.62	172.20.0.62	8.74	1

The table below represents the Top 5 most vulnerable operating systems on company devices.

Outdated Operating Systems (Top 5)

Name	Security Score ↓	Affected Devices	Exposures
Update Microsoft Windows Server 2012 R2 Datacenter Evaluation	9.46	1	453
Update Microsoft Windows Server 2016 Datacenter Evaluation	9.46	1	399
Update Microsoft Windows Server 2019 Datacenter Evaluation	9.37	1	78
Update Microsoft Windows Server 2022 Datacenter Evaluation	9.37	1	142

ThreatMate performs weekly penetration tests against internal assets. Please refer to the apendix for a detailed overview of what the penetration test includes. The table below shows the Top 5 most vulnerable internal hosts based on the last penetration test.

Internal Penetration Test (Top 5)

Address	Hostname	Total Exposures ↓	Low	Medium	High	Critical
172.20.0.1		1	0	0	1	0
172.20.0.54		1	0	0	1	0
192.168.122.1		1	0	0	1	0
192.168.93.2		1	0	0	1	0
192.168.93.1		1	0	1	0	0

Cloud Security for root

The table bellows represents a summary of the cloud security analysis performed by ThreatMate.

Cloud Security Issues

Name	Value	Description
Licensed Users	19	Number of licensed users. This is the number of users you're paying for.
Super Admin Users	8	Number of super admin users. This should be more than 1 but keep the number small. Each super admin user has complete access to the Microsoft 365 tenant.
Super Admin Users with no multi-factor authentication	1	Number of super admin users without MFA. This value should be 0 as super admin accounts are a high risk to the company due to their high privilege access.
Total Users with no multi-factor authentication	1	The total number of licensed users without MFA. This value should be 0 as users without MFA represent a higher risk to the company.
Stale Users	0	The number of users that have an active account but haven't logged in for a year. These users probably left the company and their account should be deleted. Otherwise users that left the company could still login with their old account.
Users With an Old Password	1	The number of users that haven't changed their password in a year. This shows how many users have old passwords in the company.
Dark Web Breached Users	2	The number of users that have their account leaked on the Dark Web.

The table bellows shows the Top 5 most leakded users on the Dark Web.

Dark Web Users (Top 5)

Email	Number of Breaches ↓	Last Breach Date
stan@gmail.com	95	7/17/2024, 8:00:00 PM
admin@example.com	55	7/17/2024, 8:00:00 PM

Appendix

What is a ThreatMate Penetration Test

ThreatMate performs weekly penetration tests against external assets. The tests include thorough analysis of websites and external servers. Here are the general categories of exposures that are tested:

Misconfigurations

Tests for common misconfigurations in web servers, applications, and cloud services that could expose sensitive information or weaken security controls.

Security Headers

Checks for the presence and correct configuration of security headers (e.g., Content Security Policy, Strict-Transport-Security) that help protect against various types of attacks such as cross-site scripting (XSS), clickjacking, and man-in-the-middle (MITM).

Vulnerabilities

Scans for known vulnerabilities in web applications, frameworks, and server software that could be exploited by attackers to gain unauthorized access or disrupt services.

Sensitive Information Exposure

Identifies instances where sensitive information (e.g., credentials, API keys, sensitive files) may be inadvertently exposed through misconfigured web applications or services.

Outdated Software

ThreatMate checks for outdated software versions (e.g., CMS, plugins, libraries) that may contain known vulnerabilities or weaknesses that could be exploited.

Injection Flaws

Tests for injection vulnerabilities such as SQL injection, XML injection, and command injection that could allow attackers to manipulate or extract data from the application's backend systems.

Cross-Site Scripting (XSS)

Looks for vulnerabilities that could enable attackers to inject malicious scripts into web pages viewed by other users, potentially compromising their accounts or stealing sensitive information.

Directory Traversal and File Inclusion

Examines whether the application is vulnerable to directory traversal attacks or file inclusion vulnerabilities that could allow unauthorized access to files or directories.

Authentication and Session Management

Assesses the strength and effectiveness of authentication mechanisms, session management controls, and access controls implemented by the application.

What is a Domain Security Report

Sender Policy Framework (SPF)

SPF is a security measure that helps prevent email spoofing by verifying that incoming mail from a domain is sent from an authorized mail server. It works by publishing DNS records that specify which mail servers are allowed to send emails on behalf of the domain. By implementing SPF, organizations can reduce the risk of phishing attacks and unauthorized use of their domain name for malicious purposes. It enhances email deliverability and strengthens email authentication.

Domain-based Message Authentication, Reporting & Conformance (DMARC)

DMARC builds upon SPF and DKIM (DomainKeys Identified Mail) to provide additional protection against email spoofing and phishing. It allows domain owners to specify policies for how emails that fail SPF and DKIM checks should be handled. DMARC enables domain owners to receive reports on email authentication results, helping them monitor and improve email security. It enhances the effectiveness of SPF and DKIM by providing a standardized way for email receivers to verify the authenticity of emails claiming to come from their domains.

Benefits

- Enhanced Email Security: SPF and DMARC work together to authenticate emails and prevent unauthorized use of domain names.
- Reduced Phishing Risk: Implementation reduces the likelihood of phishing attacks that exploit trust in legitimate domain names.
- Improved Deliverability: Properly configured SPF and DMARC policies can improve email deliverability by reducing the likelihood of emails being marked as spam or rejected by email filters.
- Compliance Readiness: Helps organizations meet regulatory requirements and industry standards related to email security.

Recommendation

It is recommended to implement SPF and DMARC policies for all domains to strengthen email authentication and protect against email spoofing and phishing attacks. Regular monitoring and adjustment of policies based on DMARC reports are crucial to maintaining effective email security posture.