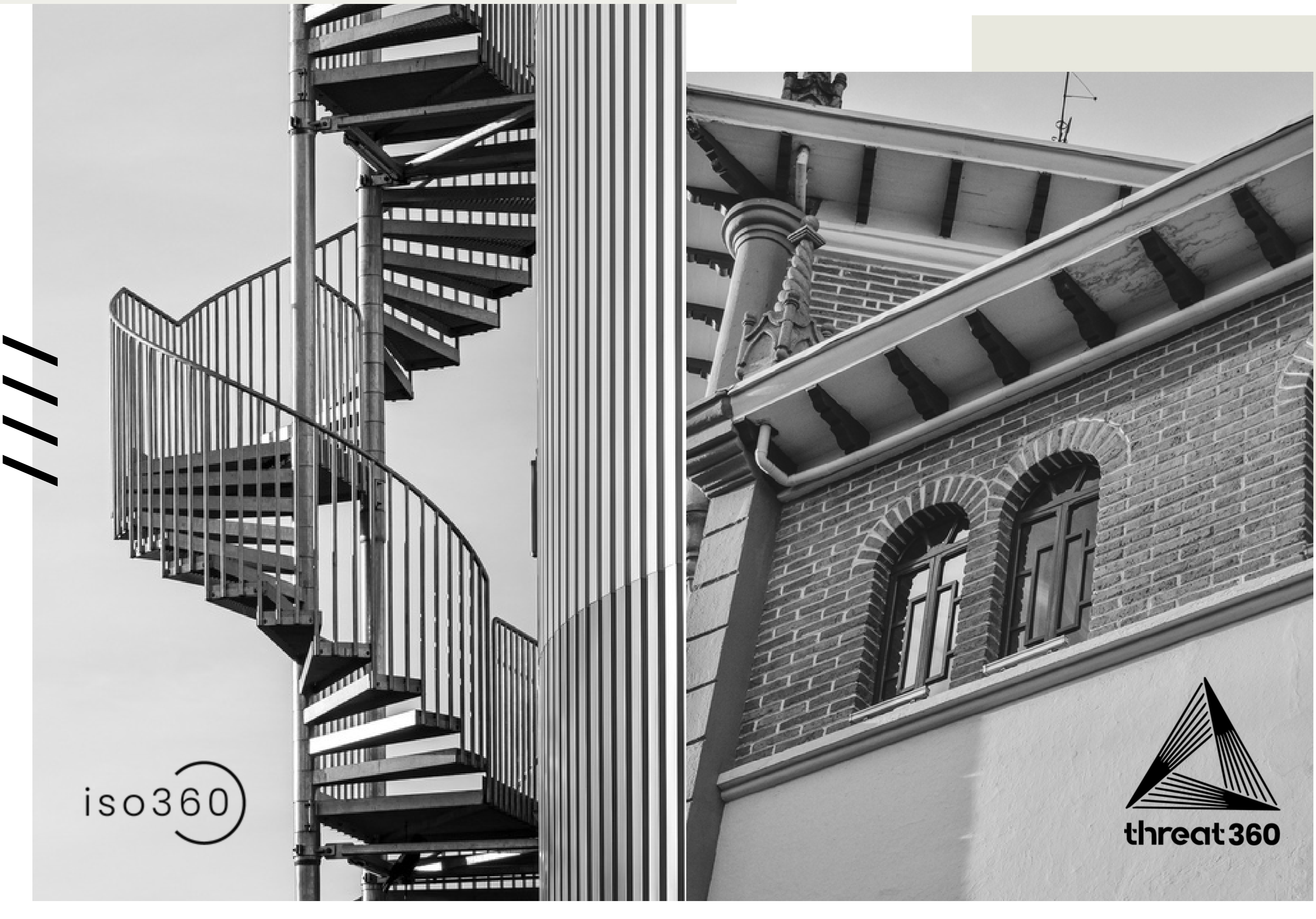
INTELLIGENCE REPORT

THREAT360



iso360

threat360

DETAILED REPORT

Scorecard for Company x

Generated **September 19, 2024**
by iso360.io, Threat Scorecard

About this report
This report is a point-in-time capture of this Scorecard as of x:xx:xx PM UTC, Date xx.xx.xxxx

Next Steps: Stay at an A

This company has an A as of September 19, 2024

A

→

Set a plan to maintain your A

✓

SECURITY SUMMARY REPORT

Scorecard for Company x

Generated **September 19, 2024**
by iso360.io Threat Scorecard

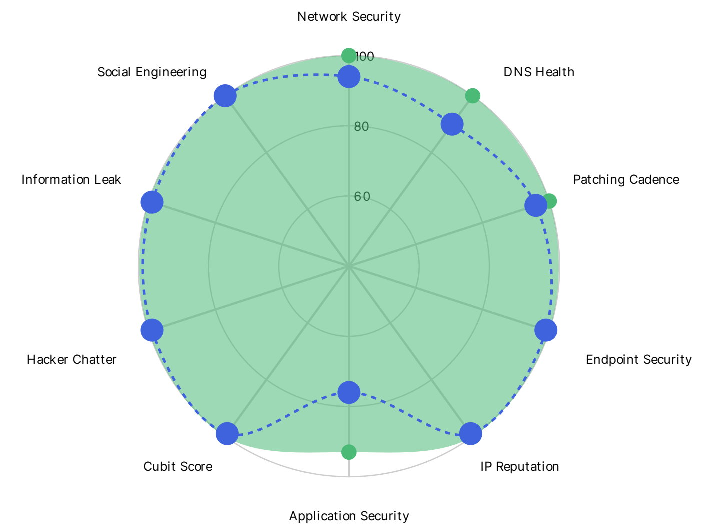
A 97

Threat Indicators

A	100	**NETWORK SECURITY** Detecting insecure network settings
A	100	**DNS HEALTH** Detecting DNS insecure configurations and vulnerabilities
A	100	**PATCHING CADENCE** Out of date company assets which may contain vulnerabilities or risks
A	100	**ENDPOINT SECURITY** Detecting unprotected endpoints or entry points of user tools, such as desktops, laptops, mobile devices, and virtual desktops
A	100	**IP REPUTATION** Detecting suspicious activity, such as malware or spam, within your company network
A	93	**APPLICATION SECURITY** Detecting common website application vulnerabilities
A	100	**CUBIT SCORE** Proprietary algorithms checking for implementation of common security best practices
A	100	**HACKER CHATTER** Monitoring hacker sites for chatter about your company
A	100	**INFORMATION LEAK** Potentially confidential company information which may have been inadvertently leaked
A	100	**SOCIAL ENGINEERING** Measuring company awareness to a social engineering or phishing attack

Industry Comparison:
Unknown

● Comapny x
● industry average



VULNERABILITIES	MEASURE
Findings on Open Ports	0
Site Vulnerabilities	2
Malware Discovered	0
Leaked Information	0

iso360.io
threat intelligence

Scorecard Overview

A

Company x

97 Security Score

DOMAIN: companyx.com

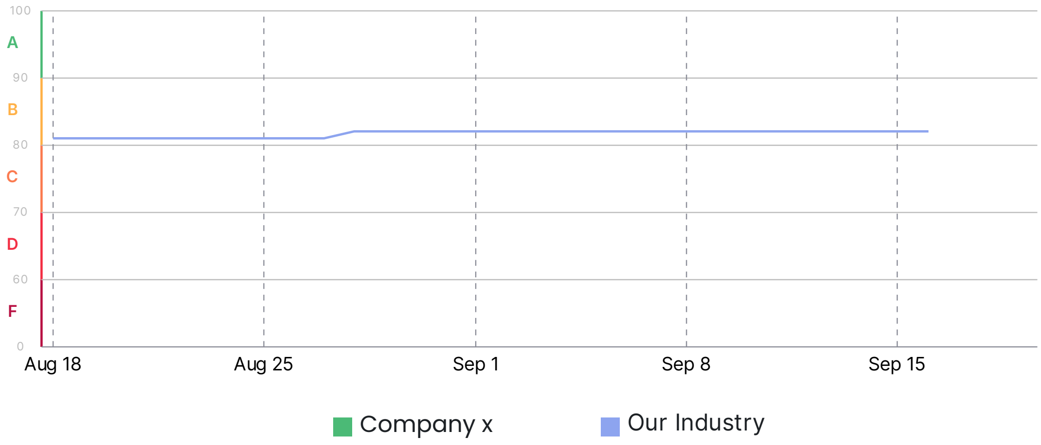
INDUSTRY: Unknown

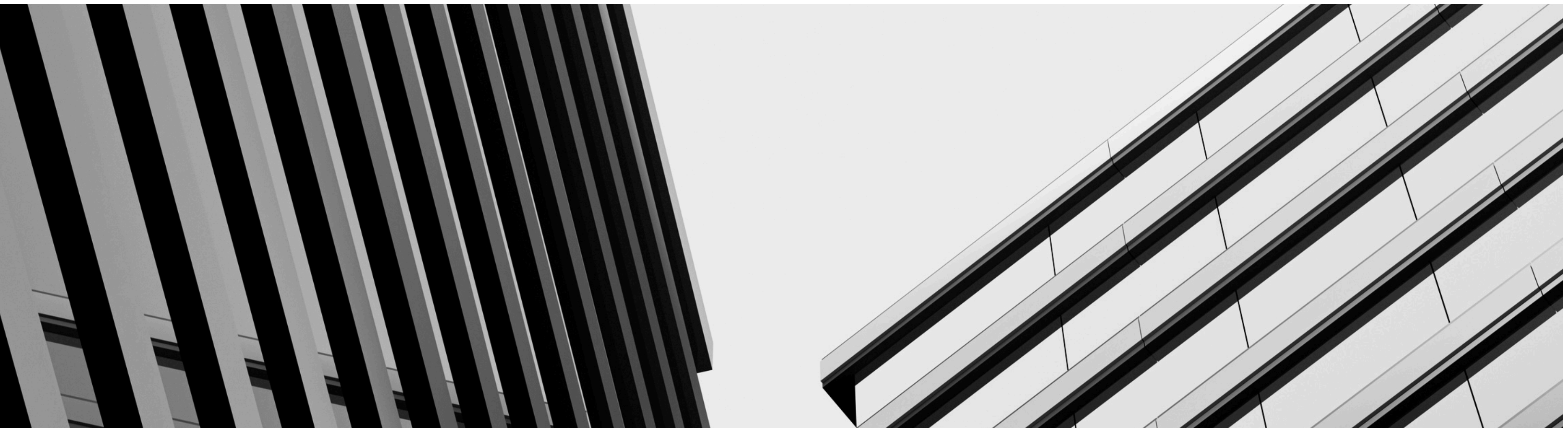
Factors

A	100	SOCIAL ENGINEERING	0 ISSUES
A	100	INFORMATION LEAK	0 ISSUES
A	100	ENDPOINT SECURITY	0 ISSUES
A	100	HACKER CHATTER	0 ISSUES
A	100	IP REPUTATION	0 ISSUES
A	100	DNS HEALTH	0 ISSUES
A	93	APPLICATION SECURITY	2 ISSUES
A	100	CUBIT SCORE	0 ISSUES
A	100	PATCHING CADENCE	0 ISSUES
A	100	NETWORK SECURITY	0 ISSUES

30-Day Score History

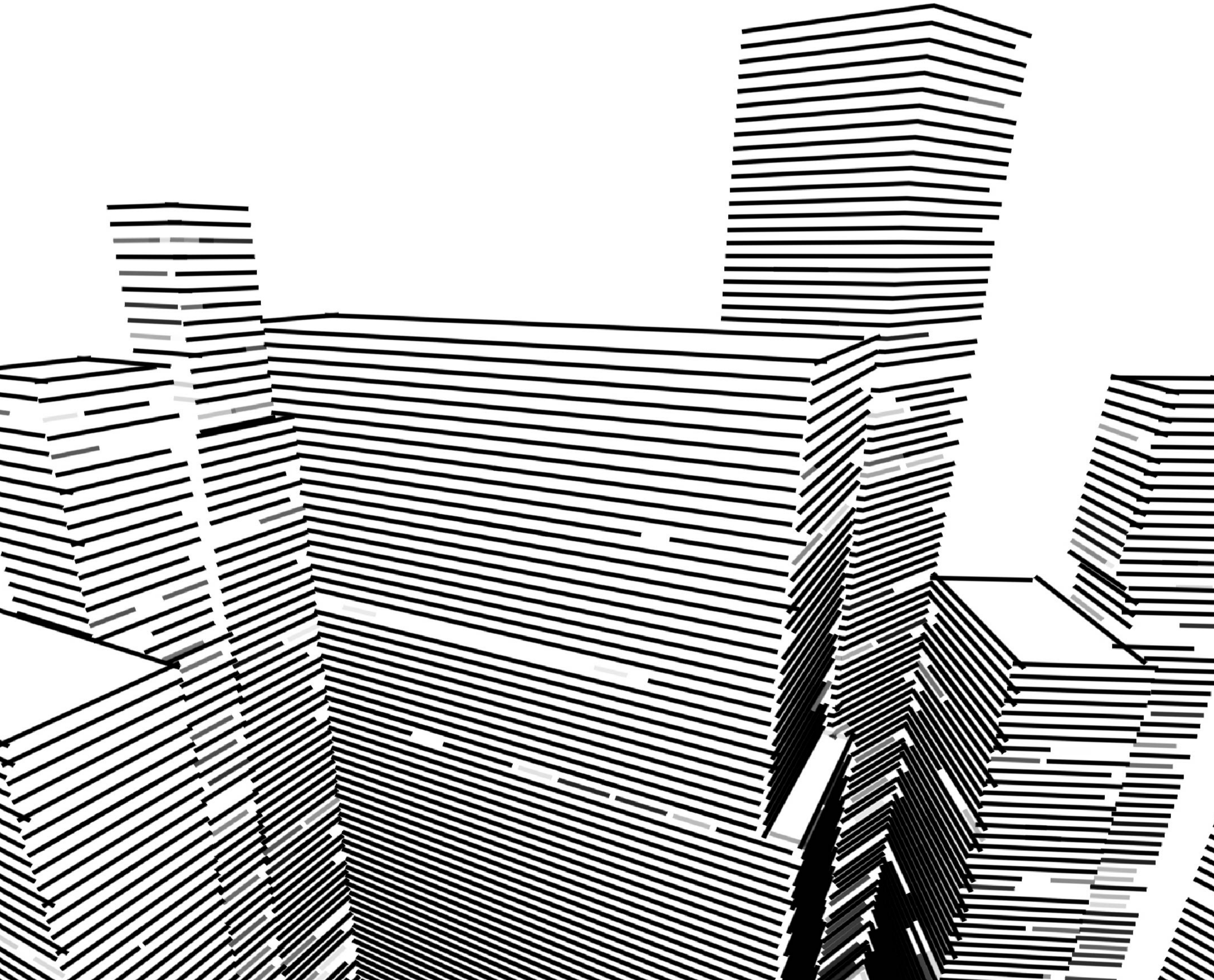
The chart below shows the evolution of the company's relative security ranking over time. Peaks in score performance represent improvements to overall security, remediation of open isues, and improved efforts to protect company infrastructure. Dips reflect introduction of system and application misconfigurations, prolonged malware activity.





Action Items

FACTOR	SEVERITY	SCORE IMPACT	ISSUES DETECTED
Application Security	▮▯▯	-1.1	Site Does Not Use Best Practices Against Embedding of Malicious Content. Not using X-Frame-Options means greater vulnerability to clickjacking attacks. Without this security header, web pages are susceptible to being embedded within iframes on other domains without explicit permission. Clickjacking involves maliciously presenting a framed web page to deceive users into interacting with altered content. This can lead to various security threats, including unauthorized access, data theft, or unintended user actions on legitimate websites.
	▮▯▯	-1.5	Unsafe Implementation Of Subresource Integrity. Without SRI, externally loaded resources, like scripts and stylesheets, lack integrity verification. This makes them susceptible to tampering. This creates a potential avenue for attackers to inject malicious scripts, which leads to Cross-Site Scripting (XSS) vulnerabilities, unauthorized data access, and other security threats.



A 100 SOCIAL ENGINEERING

The SecurityScorecard Social Engineering Module is used to determine the potential susceptibility of an organization to a targeted social engineering attack. The Social Engineering module ingests data from social networks and public data breaches, and blends proprietary analysis methods. The Social Engineering Score is an informational indicator calculated based on the quantity of indicators that appear in SecurityScorecard collection sensors.

HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
There are no High Severity Issues for Social Engineering	There are no Medium Severity Issues for Social Engineering	There are no Low Severity Issues for Social Engineering

No issues found

A 100 INFORMATION LEAK

This Information Leak module makes use of chatter monitoring and deep web monitoring capabilities to identify compromised credentials being circulated by hackers. These come in the form of bulk data breaches announced publicly as well as smaller breaches, and smaller exchanges between hackers

HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
There are no High Severity Issues for Information Leak	There are no Medium Severity Issues for Information Leak	There are no Low Severity Issues for Information Leak

No issues found

A 100 ENDPOINT SECURITY

The Endpoint Security Module tracks identification points that are extracted from metadata related to the operating system, web browser, and related active plugins. The information gathered allows companies to identify outdated versions of these data points which can lead to client-side exploitation attacks.

HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
There are no High Severity Issues for Endpoint Security	There are no Medium Severity Issues for Endpoint Security	There are no Low Severity Issues for Endpoint Security

No issues found

threat360

INTELLIGENCE REPORT

A 100 HACKER CHATTER

The SecurityScorecard Hacker Chatter module is an automated collection and aggregation system for the analysis of multiple streams of underground hacker chatter. Forums, IRC, social networks, and other public repositories of hacker community discussions are continuously monitored, collected and aggregated in order to locate mentions of business names and websites. The Hacker Chatter score is an informational indicator ranking that is ranked based on the quantity of indicators that appear within the collection sensors.

HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
There are no High Severity Issues for Hacker Chatter	There are no Medium Severity Issues for Hacker Chatter	There are no Low Severity Issues for Hacker Chatter

No issues found

A 100 IP REPUTATION

The IP Reputation and Malware Exposure module makes use of the SecurityScorecard sinkhole infrastructure as well as a blend of OSINT malware feeds, and third party threat intelligence data sharing partnerships. The SecurityScorecard sinkhole system ingests millions of malware signals from commandeered Command and Control (C2) infrastructures globally from all over the world. The incoming data is processed and attributed to corporate enterprises. The quantity and duration of malware infections are used as the determining factor for calculating is module the Malware Exposure Key Threat Indicator.

HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
There are no High Severity Issues for IP Reputation	There are no Medium Severity Issues for IP Reputation	There are no Low Severity Issues for IP Reputation

No issues found

A 100 DNS HEALTH

This module measures the health and configuration of a company's DNS settings. It validates that no malicious events occurred in the passive DNS history of the company's network. It also helps validate that mail servers have proper protection in place to avoid spoofing. It also helps verify that DNS servers are configured correctly.

HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
There are no High Severity Issues for DNS Health	There are no Medium Severity Issues for DNS Health	There are no Low Severity Issues for DNS Health

No issues found

A 93

APPLICATION SECURITY

The Web Application Vulnerability module uses incoming threat intelligence from known exploitable conditions identified via: whitehat CVE databases, blackhat exploit databases, and sensitive findings indexed by major search engines. The module ingests data from multiple public data sets, third party feeds, and an internal proprietary indexing and aggregation engine.
The score determines the likelihood of an upcoming web application breach, and checks for any existing defacement code. Presence of vulnerable applications, outdated versions, and active defacements are used to calculate the overall grade.

HIGH SEVERITY

There are no High Severity Issues for Application Security

MEDIUM SEVERITY

There are no Medium Severity Issues for Application Security

LOW SEVERITY

Site Does Not Use Best Practices Against Embedding of Malicious Content	1
Unsafe Implementation Of Subresource Integrity	1

Site Does Not Use Best Practices Against Embedding of Malicious Content

-1.1 SCORE IMPACT

Not using X-Frame-Options means greater vulnerability to clickjacking attacks. Without this security header, web pages are susceptible to being embedded within iframes on other domains without explicit permission. Clickjacking involves maliciously presenting a framed web page to deceive users into interacting with altered content. This can lead to various security threats, including unauthorized access, data theft, or unintended user actions on legitimate websites.

Description

The X-Frame-Options is an HTTP header that controls whether a web page can be displayed within an iframe. It prevents clickjacking attacks by allowing webmasters to specify if their site can be embedded in frames on other domains. This header helps protect against unauthorized framing of a website's content, enhancing the overall security of web applications.

Recommendation

- Implement X-Frame-Options with the 'SAMEORIGIN' directive to allow framing only from the same origin.
- Include the Content Security Policy (CSP) directive frame-ancestors "self" to allow framing from the same origin.
- Consider using frame-ancestors "none" to disallow all framing.

0 findings

ANALYSIS	DOMAIN	SCHEME	OBSERVATIONS	FINAL URL	LAST OBSERVED

Unsafe Implementation Of Subresource Integrity

-1.5 SCORE IMPACT

Without SRI, externally loaded resources, like scripts and stylesheets, lack integrity verification. This makes them susceptible to tampering. This creates a potential avenue for attackers to inject malicious scripts, which leads to Cross-Site Scripting (XSS) vulnerabilities, unauthorized data access, and other security threats.

Description

Subresource Integrity (SRI) is a security feature in web development designed to ensure the integrity of externally loaded resources on a webpage. These include scripts, stylesheets, and fonts. With SRI, developers include a cryptographic hash of the expected resource content in the HTML. When a user visits the webpage, the browser checks this hash against the actual content

Recommendation

- Ensure accurate cryptographic hashes are specified for all externally loaded resources using SRI attributes in the HTML.
- Routinely review and update cryptographic hashes to align with changes in resource content.
- Implement robust input validation and sanitization practices to prevent injection attacks.
- Use CSP to restrict resource sources. This adds an extra

fetched from the external source. If the hashes match, that means the resource hasn't been tampered with or compromised.

layer of control over content execution.
- Conduct regular security audits and penetration testing to promptly identify and address vulnerabilities.

0 findings

DOMAIN	SCHEME	OBSERVATIONS	LAST OBSERVED

A 100 CUBIT SCORE

This proprietary module measures a variety of security issues that a company might have. For example, we check public threat intelligence databases for IP addresses that have been flagged. These misconfigurations may have high exploitability and could cause significant harm to the privacy of your data and infrastructure

HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
There are no High Severity Issues for Cubit Score	There are no Medium Severity Issues for Cubit Score	There are no Low Severity Issues for Cubit Score

No issues found

A 100 NETWORK SECURITY

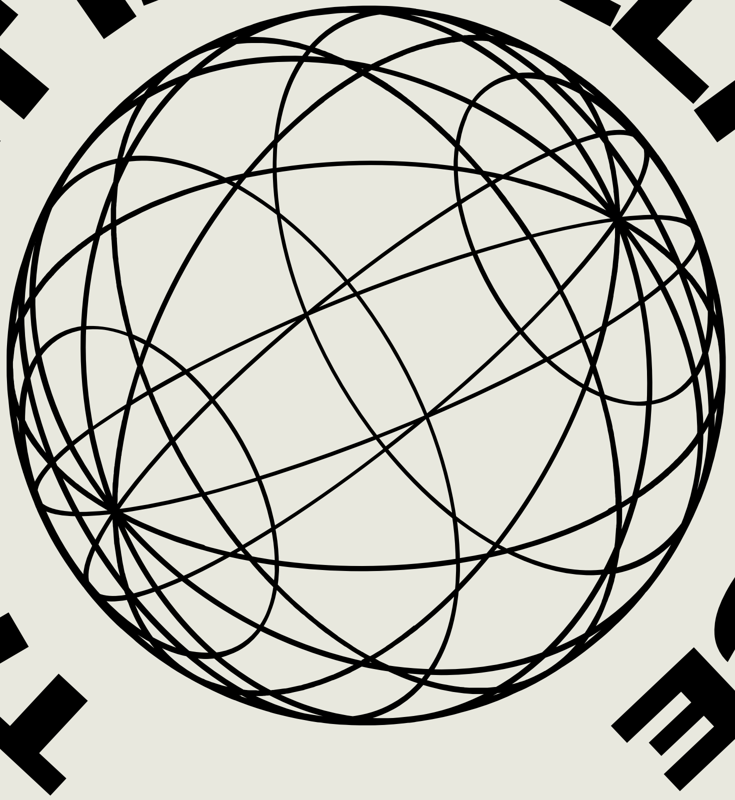
The Network Security module checks public datasets for evidence of high risk or insecure open ports within the company network. Insecure ports can often be exploited to allow an attacker to circumvent the login process or obtain elevated access to the system. If misconfigured, the open port can act as the entry point between a hacker's workstation and your internal network

HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
There are no High Severity Issues for Network Security	There are no Medium Severity Issues for Network Security	There are no Low Severity Issues for Network Security

No issues found

threat360

THREAT INTELLIGENCE



ANALYSIS REPORT

THREAT360.IO

iso360