SecurityScorecard

ISSUES REPORT FOR

Acme Inc.

This report was prepared on 12/20/2022 by SecurityScorecard.

SecurityScorecard's cutting-edge platform collects threat and vulnerability data, analyzes and processes it across 10 major, security categories using proprietary, non-invasive risk collection techniques.

If you have any questions about your report or want to get an updated report, please feel free to contact us at support@securityscorecard.io.

Learn more at securityscorecard.com

SCORECARD OVERVIEW

C

Acme Inc.

78% Security Score

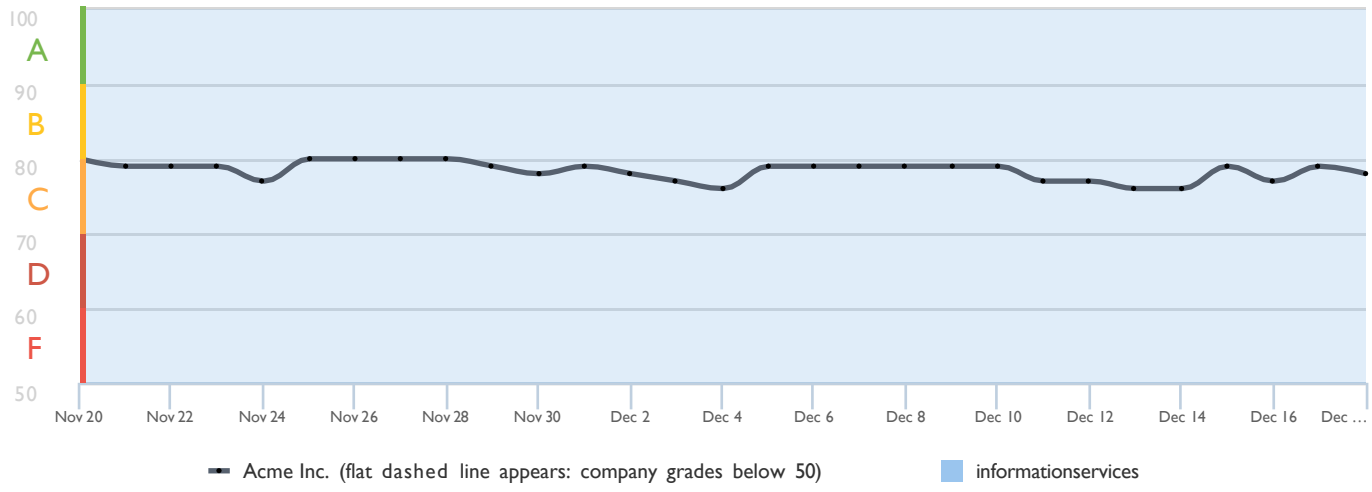
DOMAIN: AcmeInc.com

INDUSTRY: Information Services

A	93	NETWORK SECURITY	15 ISSUES		
D	65	DNS HEALTH	2 ISSUES		
F	56	PATCHING CADENCE	9 ISSUES		
A	100	ENDPOINT SECURITY	1 ISSUE		
A	94	IP REPUTATION	3 ISSUES		
F	56	APPLICATION SECURITY	31 ISSUES		
A	100	CUBIT SCORE	0 ISSUES		
A	100	HACKER CHATTER	0 ISSUES		
A	100	INFORMATION LEAK	3 ISSUES		
A	100	SOCIAL ENGINEERING	1 ISSUE		

30-DAY SCORE HISTORY

The chart below shows the evolution of the company's relative security ranking over time. The shaded area represents the range of values taken by companies in the information services industry.



Peaks in score performance represent improvements to overall security posture, remediation of open issues, and improved efforts to protect company infrastructure. Dips reflect introduction of system and application misconfigurations, prolonged malware activity.

ACTION ITEMS

FACTOR	SEVERITY	ISSUES DETECTED
Endpoint Security	i	Browser Average Age Indicates Older Versions. Our quantitative measurement of the adoption of latest browser versions indicates that out-of-date versions are in use at one or more of your IP addresses.
Information Leak	i	Email exposed. We observed that an email address for an account in this domain was listed in a data leak.
	i	IP address exposed. We observed that an IP address in this domain was listed in a data leak.
	i	Credentials at Risk (Historical). Credentials for accounts associated with employee emails were discovered.
Social Engineering	i	Exposed Personal Information (Historical). Personal information for individuals associated with employee emails were exposed.
IP Reputation	!!	Adware Installation. Communications indicative of adware installations were observed over the last 30 days.
	i	Adware Installation Trail. Communications indicative of adware installations were observed over the last 365 days.
	i	Malware Infection Trail. Communications indicative of malware infections were observed over the last 365 days.
Network Security	!!!	SSL/TLS Service Supports Weak Protocol. A TLS service was observed supporting weak protocols.
	!!	SSH Supports Weak Cipher. A weak cipher has been detected.
	!!	TLS Service Supports Weak Cipher Suite. A TLS service was observed supporting weak cipher suites.
	!!	Certificate Is Expired. Expired certificates prevent TLS clients from connecting to servers.
	!!	Certificate Is Self-Signed. Self-signed certificates prevent TLS clients from connecting to servers.
	!	FTP Service Observed. We observed FTP, a file-sharing service, publicly exposed.
	!	Certificate Without Revocation Control. A certificate was observed that did not contain either CRL or OCSP URLs.
	i	Cloud Provider Service Used. We discovered that you use a cloud provider service to host your web site or applications.
	i	DNS Server Accessible. We discovered a DNS server running on your network perimeter, accessible to the internet.
	i	HTTP Proxy Service Detected. We detected an HTTP proxy service exposed to the internet.
	i	IMAP Service Observed. We observed IMAP, an email retrieval service, publicly exposed.
	i	Networking Service Observed. We observed a networking service or device publicly exposed.
	i	POP3 Service Observed. We observed POP3, an email retrieval service, publicly exposed.

FACTOR	SEVERITY	ISSUES DETECTED
Network Security		Website Uses GoDaddy TLS Certificates. A data breach of GoDaddy exposed account information for users of their TLS certificates. This exposure puts your organization at potential risk of future compromises, such as phishing campaigns.
		TLS Certificate Status Request ("OCSP Stapling") Detected. The organization has taken additional steps to include revocation information with their TLS Certificate response.
DNS Health		SPF Record Missing. A missing SPF record has been detected for a domain.
		SPF Record Contains a Softfail without DMARC. Softfail attributes in SPF without DMARC makes spoofing and phishing email possible.
Application Security		Site does not enforce HTTPS. Site does not enforce the use of HTTPS encryption, leaving the user vulnerable to man-in-the-middle attackers (who can falsify data and inject malicious code).
		Content Security Policy (CSP) Missing. A Content Security Policy (CSP) directive tells a web browser what locations it can load resources from when rendering a webpage. This helps prevent mistaken or malicious resources from being injected into a webpage (and then executed by a user's browser).
		Website Does Not Implement HSTS Best Practices. Even if a website is protected with HTTPS, most browsers will still try first to connect to the HTTP version of the website unless explicitly specified. At that moment, visitors to the website are vulnerable to a man-in-the-middle attacker that can prevent them from reaching the HTTPS version of the website they intended to visit and instead divert them to a malicious website. The (expand) HSTS header ensures that, after a user's initial visit to the website, that they will not be susceptible to this man-in-the-middle attack because they will immediately connect to the HTTPS-protected website.
		Insecure HTTPS Redirect Pattern. Site redirects to a domain in a way that limits the security provided by HTTPS and HTTP Strict Transport Security (HSTS) headers; this leaves users vulnerable to being redirected to a spoofed/ malicious version of the site.
		Redirect Chain Contains HTTP. Site redirects through URLs that are not secured with HTTPS; this leaves users vulnerable to being redirected to a spoofed/ malicious version of the intended destination site.
		Session Cookie Missing 'HttpOnly' Attribute. Data may be exposed to unauthorized parties during cookie transmission and increases the risk of cross-site scripting (XSS) attacks.
		Session Cookie Missing 'Secure' Attribute. Data may be exposed to unauthorized parties during session cookie transmission, increasing the risk of session theft through man-in-the-middle (MITM) or traffic sniffing attacks.
		Content Security Policy Contains Broad Directives. A Content Security Policy (CSP) directive tells a web browser what locations it can load resources from when rendering a webpage. This helps prevent mistaken or malicious resources from being injected into a webpage (and then executed by a user's browser).
		Website does not implement X-Content-Type-Options Best Practices. Browsers will sometimes analyze the content themselves and handle it counter to the MIME type header; this can lead to security issues and execution of malicious code. For example, an attacker could hide malicious code with an image extension, where the browser does introspection and executes it as JavaScript.
		Website does not implement X-Frame-Options Best Practices. Not explicitly setting X-Frame-Options allows other, untrusted, websites to embed your site in a frame on their page. This can be used to make social engineering attacks appear more legitimate, or can even be used for clickjacking attacks.

	i	Server with Expired Certificate Contacted. We observed communication between your network and a website with an expired SSL certificate.
	i	Server certificate issued by country on denylist. The website uses server certificates issued by countries that have been singled out for illegal or suspicious activity by governments or trusted industry organizations. This could be damaging to the site's reputation for trustworthiness.
	i	Non-standard links detected: Contact information displayed. We detected links that include contact information which could be used for social engineering attacks.
	i	Content Security Policy Contains 'unsafe-*' Directive. A Content Security Policy (CSP) directive tells a web browser what locations it can load resources from when rendering a webpage. This helps prevent mistaken or malicious resources from being injected into a webpage (and then executed by a user's browser).
	i	Site fails to load page components. The site failed to load one or more web page components, which could indicate that the site code is ut of date or poorly maintained, which entails potential security risks.
	i	Non-standard links detected: Unsafe File Transfer Protocol. This website contains a link to a server that uses file transfer protocol (FTP, which is not secure and is susceptible to a variety of attacks.

FACTOR	SEVERITY	ISSUES DETECTED
Application Security	i	Certificate key is smaller than recommended size. A certificate with an RSA key length smaller than 2048 bits is more susceptible to attacks and certificates with longer keys.
	i	Non-standard links detected: Unsafe Telnet protocol. This website contains a link to a server that uses Telnet protocol, which is not secure and is susceptible to attacks.
	i	Site links to insecure websites. This site provides links to websites that use HTTP, which could be dangerous for users.
	i	Website communicates with payment provider. Direct communication with a payment provider can make the website a more desirable attack target.
	i	Link redirects to insecure website. A website link redirects visitors to a separate site where communication is not encrypted. If visitors are not aware that the site is insecure, they may divulge information that can be captured by malicious parties.
	i	Website References Object Storage. Objects (files) stored in object storage buckets (storage partitions) can be downloaded, referenced, and used by websites.
	i	Server error detected. Server errors on the website could indicate gaps in server maintenance with potential security implications.
	i	Site emits visible browser logs. Emitting browser logs to the developers console can expose sensitive information to anyone on the internet.
	i	Site requests data over insecure channel. Pages in the web site are requesting or delivering some content without SSL, putting visitors at risk of attacks.
	i	Unsafe Implementation Of Subresource Integrity. Subresource integrity (SRI) is a security feature that enables browsers to verify that files they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing website elements to provide a cryptographic hash that a fetched file must match.
	i	Website Copyright is Not Current. We observed copyright on a public-facing website in your network that is not current.
	i	Site receives data over Websockets. Use of WebSockets warrants continuous inspection of the data provided by third parties over that protocol.
	i	Site may use WebSockets to send user data. Using WebSockets to send user data can expose the site to a number of risks, such as data theft or denial of service.
	i	Website does not implement X-XSS-Protection Best Practices. Not explicitly setting X-XSS-Protection means that clients viewing a website could be at risk of reflected Cross-site Scripting (XSS) attacks.
	✓	Website copyright is current. A current copyright is indicative of good maintenance and security practices for this site.
Patching Cadence	!!!	High Severity CVEs Patching Cadence. High severity vulnerability seen on network more than 45 days after CVE was published.
	!!!	High-Severity Vulnerability in Last Observation. We observed a high-severity vulnerability during our last scan, which may still be publicly exposed.
	!!	Medium Severity CVEs Patching Cadence. Medium severity vulnerability seen on network more than 90 days after CVE was published.
	!!	Medium-Severity Vulnerability in Last Observation. We observed a medium-severity vulnerability during our last scan, which may still be publicly exposed.

!	Low Severity CVEs Patching Cadence. Low severity vulnerability seen network more than 120 days after CVE was published.

FACTOR	SEVERITY	ISSUES DETECTED
Patching Cadence	!	Low-Severity Vulnerability in Last Observation. We observed a low-severity vulnerability during our last scan, which may still be publicly exposed.
	i	High-severity CVE patching analyzed. This analysis reflects the number of high-severity CVEs detected in the network, the percentage that were resolved in the past 180 days, and how quickly you apply patches.
	i	Low-severity CVE patching analyzed. This analysis reflects the number of low-severity CVEs detected in the network, the percentage that were resolved in the past 180 days, and how quickly you apply patches.
	i	Medium-severity CVE patching analyzed. This analysis reflects the number of medium-severity CVEs detected in the network, the percentage that were resolved in the past 180 days, and how quickly you apply patches.

A 93 NETWORK SECURITY

ABOUT THIS FACTOR

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

SSL/TLS Service Supports Weak Protocol	10
Certificate Is Revoked	0
Elasticsearch Service Observed	0
Industrial Control System Device Accessible	0
MongoDB Service Observed	0
Neo4j Database Accessible	0
Oracle Database Server Accessible	0
SSH Software Supports Vulnerable Protocol	0

MEDIUM SEVERITY

TLS Service Supports Weak Cipher Suite	4
SSH Supports Weak Cipher	8
Certificate Is Self-Signed	4
Certificate Is Expired	3
Apache Cassandra Service Observed	0
Apache CouchDB Service Observed	0
Certificate Signed With Weak Algorithm	0
LDAP Server Accessible	0
Microsoft SQL Server Service Observed	0
MySQL Service Observed	0
PPTP Service Accessible	0
PostgreSQL Service Observed	0
RDP Service Observed	0
Redis Service Observed	0
Remote Access Service Observed	0
SMB Service Observed	0
SSH Supports Weak MAC	0
VNC Service Observed	0
rsync Service Observed	0

LOW SEVERITY

FTP Service Observed	1
Certificate Without Revocation Control	4
Certificate Lifetime Is Longer Than Best Practices	0
IP Camera Accessible	0
LDAP Server Allows Anonymous Binding	0
Telnet Service Observed	0

POSITIVE SIGNALS

TLS Certificate Status Request ("OCSP Stapling") Detected	1335

INFORMATIONAL

Website Uses GoDaddy TLS Certificates	1
POP3 Service Observed	1
Networking Service Observed	1
IMAP Service Observed	1
HTTP Proxy Service Detected	5
DNS Server Accessible	84
Cloud Provider Service Used	7
Apple AirPort Device Detected	0
Bitcoin Server Exposed	0
CDN Used	0
Cobalt Strike C2 server detected	0
Embedded IOT Web Server Exposed	0
Java Debugger Detected	0
Minecraft Server Accessible	0
Mobile Printing Service Detected	0
MySQL Server Running with Empty Password	0
NetBus Remote Access Service Detected	0
Network Attached Storage Device Exposed	0
OpenVPN Device Accessible	0
Oracle Service Registry Detected	0
Printer Detected	0
Product Potentially Impacted by CVE-2022-41040 & CVE-2022-41082	0
Product Potentially Impacted by PowerShell Remoting RCE	0
Product Running Vulnerable Log4j Version	0
Pulse Connect Secure VPN Product Observed	0
SOAP Server Accessible	0
SOCKS Proxy Service Detected	0
TOR Server Detected	0

Telephony/VoIP Device Accessible	0
UPnP Accessible	0
iSCSI Device Exposed	0

NETWORK SECURITY > ISSUE DETAIL

SSH Supports Weak Cipher

A weak cipher has been detected.

To learn more regarding this issue, please visit *https://support.securityscorecard.com*

RECOMMENDATION

Configure the SSH server to disable Arcfour and CBC ciphers.

ABOUT THIS ISSUE

The SSH server is configured to support either Arcfour or Cipher Block Chaining (CBC) mode cipher algorithms. SSH can be configured to use Counter (CTR) mode encryption instead of CBC. The use of Arcfour algorithms should be disabled.

NETWORK SECURITY > ISSUE DETAIL

IMAP Service Observed

We observed IMAP, an email retrieval service, publicly exposed.

To learn more regarding this issue, please visit *https://support.securityscorecard.com*

RECOMMENDATION

Review the business necessity of hosting a public IMAP server, and remove it from the Internet if possible. If not possible, consider restricting the service by allowlisting the IP addresses that require access.

ABOUT THIS ISSUE

The IMAP protocol offers access to messages stored on email servers. IMAP servers frequently contain all messages ever sent or received by an email account, not just recent messages. We observed an IMAP service on the Internet, accessible by the public. Email retrieval services are attractive targets to attackers due to the data they may contain. An attacker that gains access to an email account's messages may use them for blackmail, impersonating the owner of the email account, or employ the information when launching further attacks. An attacker with access to an email account's messages may gain access to many online accounts associated with that email address by using the password reset functions available on most websites. Attackers may target the service with authentication bypass attacks (e.g., brute-forcing, buffer overflows, blank passwords) in an attempt to gain control of the host or access the messages within. Attackers may launch denial-of-service (DoS) attacks against the service, rendering it unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

NETWORK SECURITY > ISSUE DETAIL

Certificate Is Expired

Expired certificates prevent TLS clients from connecting to servers.

To learn more regarding this issue, please visit *https://support.securityscorecard.com*

RECOMMENDATION

Services presenting expired certificates should cause noticeable failures, so confirm the service is still in use. If the service is not in use, decommission it. Otherwise, contact the CA and arrange issuance of a new certificate. Evaluate the organization's certificate management policy to ensure that certificates are renewed or decommissioned prior to their expiration date.

ABOUT THIS ISSUE

When a Certificate Authority (CA) issues a certificate, they embed two dates: the date at which the certificate starts being valid, and the date at which the certificate stops being valid. If a TLS client (e.g., web browser) connects to a TLS server (e.g., website) and receives a certificate that is expired, then the TLS client will refuse to connect. Certificates are digital assets that require renewal or decommissioning on a schedule.

NETWORK SECURITY > ISSUE DETAIL

Certificate Is Self-Signed

Self-signed certificates prevent TLS clients from connecting to servers.

To learn more regarding this issue, please visit *https://support.securityscorecard.com*

RECOMMENDATION

If the service is not in use, decommission it. Otherwise, contact the CA and arrange issuance of a new certificate.

ABOUT THIS ISSUE

When a certificate is issued, it is signed by a private key. Publicly-accessible services should have certificates signed by keys associated with public certificate authorities (CA). The credentials of certificate authorities are stored in a table called the trust store which is baked into modern web browsers and operating systems. Certificates signed by keys not in the trust store prevent TLS clients from connecting to servers. Off-the-shelf software and hardware frequently runs services that use self-signed certificates by default. If these services are publicly-accessible then they should be configured to use certificates issued by known certificate authorities. Failure to do so exposes users of the service to man-in-the-middle attacks on the open Internet. Self-signed certificates have narrow, but legitimate use cases, such as protecting services whose clients are configured to use public key pinning.

NETWORK SECURITY > ISSUE DETAIL

TLS Service Supports Weak Cipher Suite

A TLS service was observed supporting weak cipher suites.

To learn more regarding this issue, please visit *https://support.securityscorecard.com*

RECOMMENDATION

Disable the cipher suites listed in the evidence column of the measurement.

ABOUT THIS ISSUE

Transport Layer Security (TLS), the successor to Secure Socket Layer (SSL), is a network protocol that encrypt communications between TLS servers (e.g., websites) and TLS clients (e.g., web browsers). Every communication is secured by a cipher suite: a combination of several algorithms working in concert. Cryptographic algorithms do not have a defined lifetime, but academics, researchers, and nation states are constantly evaluating them for weaknesses. Consensus on which algorithms are untrustworthy evolves over time, and if a communication is protected with a weak cipher suite then that communication can be altered or decrypted.

NETWORK SECURITY > ISSUE DETAIL

FTP Service Observed

We observed FTP, a file-sharing service, publicly exposed.

To learn more regarding this issue, please visit *https://support.securityscorecard.com*

RECOMMENDATION

Review the business necessity of hosting a public FTP server, and remove it from the Internet if possible. If not possible, consider restricting the service by allowlisting the IP addresses that require access.

ABOUT THIS ISSUE

The FTP protocol offers access to files stored on servers, giving users the ability to upload, download, and delete files. Many FTP servers are used by automated processes, and are neglected or poorly-configured. Modern protocols, such as SFTP, provide better security than FTP. We observed an FTP service on the Internet, accessible by the public. File-sharing services are attractive targets to attackers due to the data they may contain. An attacker that gains access to the files on an FTP server may sell the files within, use them for blackmail, or employ the information when launching further attacks. A breached FTP server may result in legal proceedings, have public notification requirements, negatively impact public image, and have insurance implications. Attackers may target the service with authentication bypass attacks (e.g., brute-forcing, buffer overflows, blank passwords) in an attempt to gain control of the host or exfiltrate its databases. Attackers may launch denial-of-service (DoS) attacks against the service, rendering it unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

NETWORK SECURITY > ISSUE DETAIL

Certificate Without Revocation Control

A certificate was observed that did not contain either CRL or OCSP URLs.

To learn more regarding this issue, please visit *https://support.securityscorecard.com*

RECOMMENDATION

If the service is not in use, decommission it. Otherwise, contact the CA and arrange issuance of a new certificate.

ABOUT THIS ISSUE

When a Certificate Authority (CA) issues a certificate, they embed URLs that can be used to check if a certificate has been revoked. Certificates that are revoked are no longer valid, and TLS clients (e.g., web browsers) will refuse to connect to servers presenting revoked certificates. Certificates are revoked for a variety of reasons: the decommissioning of a server, the retirement of a product or business name, the early renewal of a replacement certificate, or the belief that an attacker may have acquired the certificate's corresponding private key. If a certificate does not include revocation controls, it cannot be revoked. Issuing irrevocable credentials is a violation of best practices.

NETWORK SECURITY > ISSUE DETAIL

POP3 Service Observed

We observed POP3, an email retrieval service, publicly exposed.

To learn more regarding this issue, please visit *https://support.securityscorecard.com*

RECOMMENDATION

Review the business necessity of hosting a public POP3 server, and remove it from the Internet if possible. If not possible, consider restricting the service by allowlisting the IP addresses that require access.

ABOUT THIS ISSUE

The POP3 protocol offers access to messages stored on email servers. POP3 servers typically contain only the most recent messages received by an email account, deleting the messages from the server once they are downloaded by a user. The use of POP3 may complicate BCP/DR due to each individual user being responsible for the entirety of their email history. We observed a POP3 service on the Internet, accessible by the public. Email retrieval services are attractive targets to attackers due to the data they may contain. An attacker that gains access to an email account's messages may use them for blackmail, impersonating the owner of the email account, or employ the information when launching further attacks. An attacker with access to an email account's messages may gain access to many online accounts associated with that email address by using the password reset functions available on most websites. Attackers may target the service with authentication bypass attacks (e.g., brute-forcing, buffer overflows, blank passwords) in an attempt to gain control of the host or access the messages within. Attackers may launch denial-of-service (DoS) attacks against the service, rendering it unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

D 65 DNS HEALTH

ABOUT THIS FACTOR

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		POSITIVE SIGNALS
There are no High Risk Issues to detect for DNS Health		SPF Record Missing	101	SPF Record Contains a Softfail without DMARC	1	There are no Positive Risk Issues to detect for DNS Health
		Open DNS Resolver Detected	0	Malformed SPF Record	0	
				SPF Record Found Ineffective	0	

INFORMATIONAL

There are no Info Risk Issues to detect for DNS Health

DNS HEALTH > ISSUE DETAIL

SPF Record Missing

A missing SPF record has been detected for a domain.

To learn more regarding this issue, please visit *https://support.securityscorecard.com*

RECOMMENDATION

Create a valid Sender Policy Framework (SPF) record. Ensure the configuration of the SPF DNS record to verify syntax and MTA servers. Test the configuration to make sure its valid by checking the header of an incoming email looking for "spf=pass" Allow for DNS caching during testing; it may take up to 48 hours to fully propagate across the Internet. The nature of the SMTP protocol does not allow for complete prevention of spoofed emails, however the SPF header will reveal whether the email is authentic.

ABOUT THIS ISSUE

The Sender Policy Framework (SPF) is a simple but effective email-validation technique designed to detect the forgery of email (also called email spoofing). An SPF record is a mechanism that allows a receiving email server to validate that inbound email from a particular domain comes from a server that is authorized to send email on behalf of that particular domain. The list of authorized sending hosts for a domain is published as a Domain Name System (DNS) record for that domain in the form of a specially formatted TXT record. An SPF record is required for spoofed email prevention and anti-spam control.

DNS HEALTH > ISSUE DETAIL

SPF Record Contains a Softfail without DMARC

Softfail attributes in SPF without DMARC makes spoofing and phishing email possible.

To learn more regarding this issue, please visit *https://support.securityscorecard.com*

RECOMMENDATION

To resolve this issue, enumerate the list of email servers that are authorized to send email on behalf of the domain. Update the SPF and DMARC records with the proper anti-spoofing controls.

ABOUT THIS ISSUE

The Sender Policy Framework (SPF) is an email-validation technique designed to detect the forgery of email (also called email spoofing). An SPF record allows a receiving email server to validate that the inbound email comes from a server that is authorized to send email on behalf of that particular domain. The list of authorized sending hosts for a domain is published as a Domain Name System (DNS) record in the form of a TXT record. DMARC is an additional TXT record to further protect again email spoofing. An SPF record with soft fail has been detected without a sufficient DMARC record. The soft fail attribute without DMARC quarantine or reject enables spoofed email from the domain.

F 56 PATCHING CADENCE

ABOUT THIS FACTOR

The Patching Cadence module analyzes how quickly a company reacts to vulnerabilities to measure patching practices. We look at the rate at which it takes a company to remediate and apply patches compared to peers.

HIGH SEVERITY

High-Severity Vulnerability in Last Observation	149
High Severity CVEs Patching Cadence	157

MEDIUM SEVERITY

Medium-Severity Vulnerability in Last Observation	5952
Medium Severity CVEs Patching Cadence	5999
End-of-Life Product	0
End-of-Service Product	0

LOW SEVERITY

Low-Severity Vulnerability in Last Observation	927
Low Severity CVEs Patching Cadence	930

POSITIVE SIGNALS

There are no Positive Risk Issues to detect for Patching Cadence

INFORMATIONAL

Medium-severity CVE patching analyzed	1
Low-severity CVE patching analyzed	1
High-severity CVE patching analyzed	1
Vulnerabilities observed	0
Vulnerability observed in most recent scan	0

PATCHING CADENCE > ISSUE DETAIL

High-Severity Vulnerability in Last Observation

We observed a high-severity vulnerability during our last scan, which may still be publicly exposed.

To learn more regarding this issue, please visit *https://support.securityscorecard.com*

RECOMMENDATION

Update or patch affected software and hardware. Enable automatic updates if available from your software vendor and permitted in your environment. Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the Bugtraq mailing list to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular update schedule for all software and hardware in use within your organization, ensuring that all the latest patches are applied soon after they are released.

ABOUT THIS ISSUE

Common vulnerabilities and exposures (CVE) is a list of publicly-known vulnerabilities in software and hardware. Each CVE contains an ID, a description of the vulnerability, and the product names and versions which are affected by the vulnerability. Software and hardware frequently self-report their product name and version when hosts connect to them. By searching through the CVE list and cross-referencing the names and versions of products found on this company's network, we are able to infer the presence of vulnerabilities.

PATCHING CADENCE > ISSUE DETAIL

High Severity CVEs Patching Cadence

High severity vulnerability seen on network more than 45 days after CVE was published.

To learn more regarding this issue, please visit *https://support.securityscorecard.com*

RECOMMENDATION

Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the National Vulnerability Database (NVD) RSS or other feeds to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular updating schedule for all software and hardware in use within your enterprise, ensuring that all the latest patches are implemented as they are released.

ABOUT THIS ISSUE

Based on scan data, the company had high severity CVE vulnerability that was open longer than 45 days after the CVE was published. High severity CVEs are those with a documented CVSS severity over 7.0. It is best practice in standards such as PCI DSS to mitigate or patch high severity vulnerabilities within 45 days. Details on each vulnerability are listed in the table below.

PATCHING CADENCE > ISSUE DETAIL

Medium-Severity Vulnerability in Last Observation

We observed a medium-severity vulnerability during our last scan, which may still be publicly exposed.

To learn more regarding this issue, please visit *https://support.securityscorecard.com*

RECOMMENDATION

Update or patch affected software and hardware. Enable automatic updates if available from your software vendor and permitted in your environment. Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the Bugtraq mailing list to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular update schedule for all software and hardware in use within your organization, ensuring that all the latest patches are applied soon after they are released.

ABOUT THIS ISSUE

Common vulnerabilities and exposures (CVE) is a list of publicly-known vulnerabilities in software and hardware. Each CVE contains an ID, a description of the vulnerability, and the product names and versions which are affected by the vulnerability. Software and hardware frequently self-report their product name and version when hosts connect to them. By searching through the CVE list and cross-referencing the names and versions of products found on this company's network, we are able to infer the presence of vulnerabilities.

PATCHING CADENCE > ISSUE DETAIL

Medium Severity CVEs Patching Cadence

Medium severity vulnerability seen on network more than 90 days after CVE was published.

To learn more regarding this issue, please visit *https://support.securityscorecard.com*

RECOMMENDATION

Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the National Vulnerability Database (NVD) RSS or other feeds to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular updating schedule for all software and hardware in use within your enterprise, ensuring that all the latest patches are implemented as they are released.

ABOUT THIS ISSUE

Based on scan data, the company had medium severity CVE vulnerability that was open longer than 90 days after the CVE was published. Medium severity CVEs are those with a documented CVSS severity between 4.0 and 6.9. It is best practice to mitigate or patch medium severity vulnerabilities within 90 days. Details on each vulnerability are listed in the table below.

PATCHING CADENCE > ISSUE DETAIL

Low-Severity Vulnerability in Last Observation

We observed a low-severity vulnerability during our last scan, which may still be publicly exposed.

To learn more regarding this issue, please visit *https://support.securityscorecard.com*

RECOMMENDATION

Update or patch affected software and hardware. Enable automatic updates if available from your software vendor and permitted in your environment. Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the Bugtraq mailing list to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular update schedule for all software and hardware in use within your organization, ensuring that all the latest patches are applied soon after they are released.

ABOUT THIS ISSUE

Common vulnerabilities and exposures (CVE) is a list of publicly-known vulnerabilities in software and hardware. Each CVE contains an ID, a description of the vulnerability, and the product names and versions which are affected by the vulnerability. Software and hardware frequently self-report their product name and version when hosts connect to them. By searching through the CVE list and cross-referencing the names and versions of products found on this company's network, we are able to infer the presence of vulnerabilities.

PATCHING CADENCE > ISSUE DETAIL

Low Severity CVEs Patching Cadence

Low severity vulnerability seen network more than 120 days after CVE was published.

To learn more regarding this issue, please visit *https://support.securityscorecard.com*

RECOMMENDATION

Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the National Vulnerability Database (NVD) RSS or other feeds to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular updating schedule for all software and hardware in use within your enterprise, ensuring that all the latest patches are implemented as they are released.

ABOUT THIS ISSUE

Based on scan data, the company had low severity CVE vulnerability that was open longer than 120 days after the CVE was published. Low severity CVEs are those with a documented CVSS severity under 4.0. It is best practice to mitigate or patch high severity vulnerabilities within 120 days. Details on each vulnerability are listed in the table below.

A 100 ENDPOINT SECURITY

ABOUT THIS FACTOR

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

Outdated Operating System Observed	0
Outdated Web Browser Observed	0

MEDIUM SEVERITY

There are no Medium Risk Issues to detect for Endpoint Security

LOW SEVERITY

There are no Low Risk Issues to detect for Endpoint Security

POSITIVE SIGNALS

There are no Positive Risk Issues to detect for Endpoint Security

INFORMATIONAL

Browser Average Age Indicates Older Versions	17

A 94 IP REPUTATION

ABOUT THIS FACTOR

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

Anonymous Open Proxy	0
Malware Controller Observed	0
Malware Infection	0
Phishing Infrastructure	0
Ransomware Infection Detected	0

MEDIUM SEVERITY

Adware Installation	2
Attack Detected	0
Products Susceptible To Ransomware Exploits Exposed	0
SMTP Server on Unusual Port	0

LOW SEVERITY

There are no Low Risk Issues to detect for IP Reputation

POSITIVE SIGNALS

There are no Positive Risk Issues to detect for IP Reputation

INFORMATIONAL

Malware Infection Trail	12
Adware Installation Trail	2
Active CVE Exploitation Attempted	0
Cobalt Strike C2 Detected	0
DOS Attack Attempt Detected	0
General Scan Detected	0
IP on blacklist due to malicious activity	0
Known compromised or Hostile Host	0
Malicious Scan Detected	0
Malicious TOR Exit Node Detected	0
Malicious TOR Relay/Router Node Detected	0
Malicious User Agent Detected	0
Malicious botnet C2 server detected	0
Malware Detected	0
Mirai Botnet Traffic Detected	0
Potentially Vulnerable Application (PVA) Installation	0
Potentially Vulnerable Application Installation (PVA) Trail	0
Ransomware Infection Trail Detected	0
Suspicious Traffic Observed	0
Threat actor infrastructure detected	0
Unsolicited Commercial Email	0

IP REPUTATION > ISSUE DETAIL

Adware Installation

Communications indicative of adware installations were observed over the last 30 days.

To learn more regarding this issue, please visit *https://support.securityscorecard.com*

RECOMMENDATION

Investigate the devices associated with the IP addresses listed, checking for evidence of adware installations.

ABOUT THIS ISSUE

After adware has been installed on a device, it often communicates with a service on the Internet. This service allows the adware to register the device on which it is installed and receive the advertisements that will be displayed to the user.

IP REPUTATION > ISSUE DETAIL

Malware Infection Trail

Communications indicative of malware infections were observed over the last 365 days.

To learn more regarding this issue, please visit *https://support.securityscorecard.com*

RECOMMENDATION

Investigate the devices associated with the IP addresses listed, checking for evidence of malware infections.

ABOUT THIS ISSUE

After a device has been infected by malware, it often communicates with a command and control (C&C) service on the internet. This service allows the malware to register its infected device and receive instructions from the malware's authors. These instructions could cause the device to delete or encrypt its datastores, participate in distributed denial-of-service (DDoS) attacks, or perform any variety of malicious actions. Events in this unscored issue overlap with those in the Malware Infection issue, providing visibility into the last year of malware infections.

IP REPUTATION > ISSUE DETAIL

Adware Installation Trail

Communications indicative of adware installations were observed over the last 365 days.

To learn more regarding this issue, please visit *https://support.securityscorecard.com*

RECOMMENDATION

Investigate the devices associated with the IP addresses listed, checking for evidence of adware installations.

ABOUT THIS ISSUE

After adware has been installed on a device, it often communicates with a service on the Internet. This service allows the adware to register the device on which it is installed and receive the advertisements that will be displayed to the user. Events in this unscored issue overlap with those in the Adware Installation issue, providing visibility into the last year of adware installations.

F 56 APPLICATION SECURITY

ABOUT THIS FACTOR

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

Site does not enforce HTTPS	42
High Severity Content Management System vulnerabilities identified	0

MEDIUM SEVERITY

Website Does Not Implement HSTS Best Practices	6885
Redirect Chain Contains HTTP	32
Insecure HTTPS Redirect Pattern	22
Content Security Policy (CSP) Missing	3569
Medium Severity Content Management System vulnerabilities identified	0

LOW SEVERITY

Website does not implement X-Frame-Options Best Practices	3091
Website does not implement X-Content-Type-Options Best Practices	3402
Session Cookie Missing 'Secure' Attribute	3
Session Cookie Missing 'HttpOnly' Attribute	2
Content Security Policy Contains Broad Directives	15
Low Severity Content Management System vulnerabilities identified	0

POSITIVE SIGNALS

Website copyright is current	793
Domain Uses HSTS Preloading	0
Web Application Firewall (WAF) Detected	0

INFORMATIONAL

Website does not implement X-XSS-Protection Best Practices	3406
Website communicates with payment provider	17
Website References Object Storage	29
Website Copyright is Not Current	683
Unsafe Implementation Of Subresource Integrity	3551
Site requests data over insecure channel	2711
Site receives data over Websockets	42
Site may use WebSockets to send user data	46
Site links to insecure websites	70
Site fails to load page components	11965
Site emits visible browser logs	18894
Server with Expired Certificate Contacted	72
Server error detected	8460
Server certificate issued by country on denylist	1
Non-standard links detected: Unsafe Telnet protocol	1
Non-standard links detected: Unsafe File Transfer Protocol	14
Non-standard links detected: Contact information displayed	4684
Link redirects to insecure website	4875
Content Security Policy Contains 'unsafe-*' Directive	2
Certificate key is smaller than recommended size	3
Browser logs contain debug messages	0

Insecure channel exposes sensitive information	0
Non-standard links detected: Local file path exposed	0
November 2022 OpenSSL 3.X vulnerability detected	0
Potential vulnerability detected	0
Vulnerable Log4j version detected	0
Web application potentially vulnerable to Spring4Shell	0
Website Hosted by GoDaddy's Wordpress	0
Website Hosted on Object Storage	0
Website defaced	0
Websocket requests contain sensitive fields or PII	0

APPLICATION SECURITY > ISSUE DETAIL

Session Cookie Missing 'HttpOnly' Attribute

Data may be exposed to unauthorized parties during cookie transmission and increases the risk of cross-site scripting (XSS) attacks.

To learn more regarding this issue, please visit *https://support.securityscorecard.com*

RECOMMENDATION

Set session cookies with the 'HttpOnly' attribute to ensure they can not be accessed by any other means. A cookie marked with 'HttpOnly' will prevent any malicious injected scripts from being able to access it.

ABOUT THIS ISSUE

The cookie session ID is not set with the 'HttpOnly' attribute. The missing attribute could allow the session ID to be accessed by a client side script such as JavaScript. This exposes the cookies to potential theft via scripting attack vectors, such as XSS attacks.

APPLICATION SECURITY > ISSUE DETAIL

Session Cookie Missing 'Secure' Attribute

Data may be exposed to unauthorized parties during session cookie transmission, increasing the risk of session theft through man-in-the-middle (MITM) or traffic sniffing attacks.

To learn more regarding this issue, please visit *https://support.securityscorecard.com*

RECOMMENDATION

Change the default 'Secure' attribute from FALSE to TRUE to ensure session cookies are sent only with HTTPS. The 'Secure' attribute should be set on each cookie to prevent cookies from being observed by malicious actors. Implement the 'Secure' attribute when using the Set-Cookie parameter during authenticated sessions.

ABOUT THIS ISSUE

The session ID does not have the 'Secure' attribute, which prevents session cookies from being seen in plaintext. It may be possible for a malicious actor to steal session cookie data and perform session theft through man-in-the-middle (MITM) or traffic-sniffing attack. The exploitable condition causes unencrypted session cookies to be passed over the network if a user accesses the site through HTTP instead of HTTPS, or if a link to a resource, such as an image or .css file within the specified domain, uses the HTTP protocol.

A 100 CUBIT SCORE

ABOUT THIS FACTOR

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

Ransomware-Susceptible Remote Access Services Exposed 0

MEDIUM SEVERITY

There are no Medium Risk Issues to detect for Cubit Score

LOW SEVERITY

There are no Low Risk Issues to detect for Cubit Score

POSITIVE SIGNALS

There are no Positive Risk Issues to detect for Cubit Score

INFORMATIONAL

There are no Info Risk Issues to detect for Cubit Score

Subdomains were detected on target domain names that are accessible to the public Internet. There is a possibility that these subdomains may be portals to administrative functionalities for various enterprise applications.

No issues found.

A 100 HACKER CHATTER

ABOUT THIS FACTOR

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

Domain Advertised as Ransomware Victim 0

MEDIUM SEVERITY

There are no Medium Risk Issues to detect for Hacker Chatter

LOW SEVERITY

There are no Low Risk Issues to detect for Hacker Chatter

POSITIVE SIGNALS

There are no Positive Risk Issues to detect for Hacker Chatter

INFORMATIONAL

Alleged Breach Incident 0

No issues found.

A 100 INFORMATION LEAK

ABOUT THIS FACTOR

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

There are no High Risk Issues to detect for Information Leak

MEDIUM SEVERITY

There are no Medium Risk Issues to detect for Information Leak

LOW SEVERITY

Credentials at Risk	0

POSITIVE SIGNALS

There are no Positive Risk Issues to detect for Information Leak

INFORMATIONAL

IP address exposed	2
Email exposed	13
Credentials at Risk (Historical)	5
API key exposed	0
Age exposed	0
Attempted Information Leak	0
Birthday exposed	0
Cleartext password exposed	0
Employer exposed	0
Exploit Attempt Detected	0
Hashed password exposed	0
Instant messaging account exposed	0
Language exposed	0
Name exposed	0
Non-social media access token exposed	0
Occupation exposed	0
Parent's name exposed	0
Password exposed	0
Password hint exposed	0
Phone number exposed	0
Physical address exposed	0
Race exposed	0
Security question and answer exposed	0
Social Security number exposed	0
Social media account exposed	0
Social media token exposed	0
User-agent string exposed	0
Username exposed	0

A 100 SOCIAL ENGINEERING

ABOUT THIS FACTOR

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

There are no High Risk Issues to detect for Social Engineering

MEDIUM SEVERITY

There are no Medium Risk Issues to detect for Social Engineering

LOW SEVERITY

Exposed Personal Information	0

POSITIVE SIGNALS

There are no Positive Risk Issues to detect for Social Engineering

INFORMATIONAL

Exposed Personal Information (Historical)	602

No content (including ratings, data, reports, software or other application or output therefrom) or any part thereof (collectively, Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system without the prior written permission of SecurityScorecard, Inc. (SSC) The Content shall not be used for any unlawful or unauthorized purposes.

SSC and any third-parties, and their directors, officers, shareholders, employees, customers and agents (collectively SSC Parties) do not guarantee or warrant the accuracy, completeness, timeliness or availability of the Content. SSC Parties are not responsible for any errors or omissions (negligent or otherwise), regardless of the cause, or for the results obtained from the use of the Content. The Content is provided on an "as is" basis. SSC PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (I) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS,(3) FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall SSC Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

USERS OF THE CONTENT MUST USE ALL REASONABLE ENDEAVORS TO MITIGATE ANY LOSS OR DAMAGE WHATSOEVER (AND HOWSOEVER ARISING) AND NOTHING HEREIN SHALL BE DEEMED TO RELIEVE OR ABROGATE USERS OF ANY SUCH DUTY TO MITIGATE ANY LOSS OR DAMAGE.

IN ANY EVENT, TO THE EXTENT PERMITTED BY LAW, THE AGGREGATE LIABILITY OF THE SSC PARTIES FOR ANY REASON WHATSOEVER RELATED TO ACCESS TO OR USE OF CONTENT SHALL NOT EXCEED THE GREATER OF (A) THE TOTAL AMOUNT PAID TO SSC BY THE USER FOR SERVICES PROVIDED DURING THE 12 MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO LIABILITY, AND (B) U.S. $100.

Security-related analyses, including ratings and statements in the Content, are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SSC's opinions, analyses and ratings should not be relied on as a substitute for the skill, judgment and experience of the user and its management, employees, advisors andr clients when making business decisions. SSC assumes no obligation to update the Content following publication in any form or format. While SSC has obtained information from sources it believes to be reliable, SSC does not perform an audit and undertakes no duty of due diligence or independent verification of any information it receives. Users expressly agree that (a) the security ratings and other security opinions provided via the Content do not reflect, identify or detect every vulnerability or security issue or address any other risk; (b) the security ratings and other opinions provided do not take into account users' particular objectives, situations or needs; (c) each rating or other opinion will be weighed, if at all, solely as one factor in any decision made by or on behalf of any user; and (d) users will accordingly, with due care, make their own study and evaluation of the risks of doing business with any entity. If a user identifies any in the Content, we invite you to share that information with us by emailing us at support@securityscorecard.io.