SecurityScorecard

A Deep Dive in Scoring Methodology

By Bob Sohval, PhD
VP Data Science

Table of Contents

SecurityScorecard evaluates organizations' security profiles non-intrusively, using an 'outside-in' methodology.

This approach enables SecurityScorecard to operate at scale, measuring and updating cybersecurity ratings daily on more than one million organizations globally.

Cybersecurity Ratings

The rise of the internet and its global role in e-commerce, business operations, communications, and social media, has created both opportunities and risks. While it can fuel economic growth and speed up the dissemination of news and ideas, the existence of vulnerabilities in commonly used software products and services, and poor adherence to recommended security practices can expose organizations to significant financial and reputational harm at the hands of malicious actors — including both individuals and nation states.

Cybersecurity ratings provide a means for objectively monitoring the security hygiene of organizations and gauging whether their security posture is improving or deteriorating over time. The ratings are valuable for vendor risk management programs, determining risk premiums for cyber insurance, credit underwriting and financial trading decisions, M&A due diligence information, executive-level reporting, and for self-monitoring. Cybersecurity ratings, and the extensive information on which they are based, are also helpful for assessing compliance with cybersecurity risk standards.

What do Scores Mean?

SecurityScorecard conveys detailed analysis of organizations' security postures with Total Score, an easy-to-understand letter grade—A (90-100) to F (< 60), Total Score directly reflects all the security issues that we discover on an organization's internet-facing assets using issue type weights.

Cybersecurity ratings can be compared to financial credit ratings. Just as a poor credit rating is associated with a greater probability of default, a poor cybersecurity rating is associated with a higher probability of sustaining a data breach or other adverse cyber event.

Validation of SecurityScorecard scores using statistical analysis demonstrates that companies with an F rating have a 13.8x greater likelihood of incurring a data breach compared to companies with an A.

Factor Scores

SecurityScorecard calculates and provides detailed reports on 10 different factor scores. The factor scores group and describe different aspects of cyber risk along multiple axes. They allow security teams to identify vulnerable areas and focus their remediation efforts where they will have the greatest impact.

Score factors have numeric scores of 0-100. Issue types are weighted based on relative breach risk. Issue type weights are the only weights that impact the total score. This makes the scoring calculation process clear and simple to understand.

Individual Factor Scores are calculated based on the severity and quantity of security issues or findings associated with the factor.

Factor Score of 100 indicates that no cybersecurity issues were detected for that factor.

Grade	Score
A	≥90
B	80-89
C	70-79
D	60-69
F	<60

SECURITYSCORECARD'S 10 RISK FACTOR GROUPS

1 Application Security

2 Cubit Score

3 DNS Health

4 Endpoint Security

5 Hacker Chatter

6 Informational Leak

7 IP Reputation

8 Network Security

9 Patching Cadence

10 Social Engineering

Cybersecurity Signals

SecurityScorecard monitors hundreds of different cybersecurity signals and calculates a score based on a defined subset of issues. Each issue is associated with one of the ten risk factor groups and is assigned a weight reflecting its severity based on how closely correlated it is to breach likelihood. Informational and Positive issues (reflecting good security practice) are captured and presented to users for improved awareness, but do not contribute to score.

The security issues measured by SecurityScorecard, along with the assigned factor, severity-based weight, update cadence and age out window, are presented in the following table.

Notes:

- Severity levels are subject to change as we continue to improve and refine our scoring algorithm. These changes will occur as part of our quarterly scoring recalibrations, and the version number will be updated accordingly.
- Detailed descriptions, risks, and recommendations for each issue type can be found in the SecurityScorecard platform.

Issue Type	Factor	Severity	Recommendation	Frequency	Age Out
Active CVE Exploitation Attempted	IP Reputation	LOW	Investigate the IP listed in the Findings table below. Then perform an incident response management process.	Varies*	15
Adware Installation	IP Reputation	LOW	Investigate the devices associated with the IP addresses listed, checking for evidence of adware installations.	Varies*	30
Adware Installation Trail	IP Reputation	LOW	Investigate the devices associated with the IP addresses listed, checking for evidence of adware installations.	Varies*	365
Age exposed	Information Leak	INFO	Reset the password for the compromised account. If the username is no longer active, ensure that no other services link to the affected email address, such as cloud-based applications that your organization uses.	Varies*	15
Alleged Breach Incident	Hacker Chatter	MEDIUM	Investigate the alleged activity to determine if it can be substantiated and remediate as necessary.	Varies*	30
Apache Cassandra Service Observed	Network Security	MEDIUM	Exposing database services to the Internet is not recommended. Consider placing the service behind a VPN, preventing public access. If making the service private is not possible, restrict the service by allowlisting the IP addresses that require access.	Weekly	45
Apache CouchDB Service Observed	Network Security	MEDIUM	Exposing database services to the Internet is not recommended. Consider placing the service behind a VPN, preventing public access. If making the service private is not possible, restrict the service by allowlisting the IP addresses that require access.	Weekly	45
API key exposed	Information Leak	INFO	Reset the password for the compromised account. If the username is no longer active, ensure that no other services link to the affected email address, such as cloud-based applications that your organization uses.	Varies*	15
Apple AirPort Device Detected	Network Security	LOW	Place the wireless administrative portal behind a firewall.	Weekly	45
Attack Detected	IP Reputation	LOW	Investigate the devices associated with the IP addresses listed, checking for evidence of malware infections.	Varies*	30
Attempted Information Leak	Information Leak	LOW	Investigate the IP listed in the Findings table below. Then perform an incident response management process.	Varies*	15
Birthday exposed	Information Leak	INFO	Reset the password. Subscribe to an identity-monitoring service to ensure no unauthorized accounts were made in the user's name.	Varies*	15
Bitcoin Server Exposed	Network Security	INFO	Assess the business need for exposing a Bitcoin server to the internet, and consider placing it behind a firewall.	Weekly	45
Browser Average Age Indicates Older Versions	Endpoint Security	LOW	Update the web browsers in question to the latest major release versions. Enable automatic updates if available from your web browser vendor and permitted in your environment.	Varies*	None
Browser logs contain debug messages	Application Security	LOW	Follow best practices to keep sensitive information out of browser logs.	Weekly	15
CDN Used	Network Security	LOW	Identification of a CDN could be useful information to your customers and partners, and there is no recommended action.	Weekly	45
Certificate Is Expired	Network Security	LOW	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.	Weekly	45
Certificate Is Revoked	Network Security	HIGH	If the service is not in use, decommission it. Otherwise, contact the CA and arrange issuance of a new certificate.	Weekly	45
Certificate Is Self-Signed	Network Security	LOW	If the service is not in use, decommission it. Otherwise, contact the CA and arrange issuance of a new certificate.	Weekly	45
Certificate key is smaller than recommended size	Application Security	LOW	Migrate to larger keys.	Weekly	15
Certificate Lifetime Is Longer Than Best Practices	Network Security	LOW	If the service is not in use, decommission it. Otherwise, contact the CA and arrange issuance of a new certificate.	Weekly	45

Issue Type	Factor	Severity	Recommendation	Frequency	Age Out
Certificate Signed With Weak Algorithm	Network Security	LOW	If the service is not in use, decommission it. Otherwise, contact the CA and arrange issuance of a new certificate.	Weekly	45
Certificate Without Revocation Control	Network Security	LOW	If the service is not in use, decommission it. Otherwise, contact the CA and arrange issuance of a new certificate.	Weekly	45
Cleartext password exposed	Information Leak	MEDIUM	Reset the password for the compromised account. If the username is no longer active, ensure that no other services link to the affected email address, such as cloud-based applications that your organization uses.	Varies*	15
Cloud Provider Service Used	Network Security	INFO	Identification of a cloud provider service could be useful information to your customers and partners, and there is no recommended action.	Weekly	45
Cobalt Strike C2 Detected	IP Reputation	INFO	When a Cobalt Strike C2 service is detected on a server on which it has no legitimate reason or authorization to be deployed, it is likely that a breach has occurred. Investigate the server logs to determine what methods the attacker used to gain access, such as brute force, stolen credentials, exploited vulnerabilities, or random code execution (RCE). Quarantine the server as soon as possible. Remove the Cobalt Strike C2 installation from the server. Change the passwords on any accounts associated with the server. If possible, place the server behind the firewall. Block the IP address from which the attacker originated.	Varies*	15
Cobalt Strike C2 server detected	Network Security	MEDIUM	Investigate the logs on the server on which the Cobalt Strike C2 was installed to determine how the attacker was able to access your domain. Remove the Cobalt Strike C2 installation from the breached server. Change the passwords on any accounts associated with the server. If possible, place the server behind the firewall. Block the IP address from which the attacker originated.	Weekly	45
Content Security Policy (CSP) Missing	Application Security	LOW	Enable CSP headers via your web server configuration.	Weekly	45
Content Security Policy Contains 'unsafe-*' Directive	Application Security	LOW	• Remove the unsafe directives from the content security policy. For trusted resources that must be used inline with HTML, you can use nonces or hashes in your content security policy's source list to mark the resources as trusted. • Nonces are randomly generated numbers placed with inline content that you trust. By including the nonce in both the content and the header, the browser knows to trust the script. • Example inline script with a nonce: <script nonce=aBFef03nceIOfn39hr3r satsdfa>alert('Hello, world.');</script> • Example policy that allows the inline script to be run without unsafe directives: • Content-Security-Policy: script-src 'nonce-aBFef03nceIOfn39hr3rsatsdfa' • Warning: For nonces to be effective, they must be randomly regenerated every time the page is loaded. If an attacker can guess the nonce value, the protection is useless. • Hashes work similarly to nonces, but only need to be generated once. By taking the hash of a script and including it in the header, it will mark the script as trusted. If the attacker tries to change the script, the hash will change and it will no longer be trusted. • Example inline script to be hashed:x <script>alert('Hello, world.');</script> • Example policy that allows the inline script to be run without unsafe directives: • Content-Security-Policy: script-src 'sha256-qznLcsROx4GACP2dm0UCK CzCG-HiZ1guq6ZZDob_Tng='	Weekly	45
Content Security Policy Contains Broad Directives	Application Security	LOW	Explicitly specify trusted sources for your script-src and object-src policies. Ideally you can use the 'self' directive to limit scripts and objects to only those on your own domain, or you can explicitly specify domains that you trust and rely upon for your site to function.	Weekly	45
Credentials at Risk (Historical)	Information Leak	LOW	Ensure employees are not using the affected credentials for any corporate or third-party logins. Ensure that all passwords have been changed since the indication of breach. In the case of corporate passwords, check logs for repeated failed login attempts or repeated password reset attempts from suspicious IP addresses.	Varies*	None

Issue Type	Factor	Severity	Recommendation	Frequency	Age Out
Credentials at Risk for Up to 120 days	Information Leak	INFO	Ensure employees are not using the affected credentials for any corporate or third-party logins.	Varies	120
Credentials at Risk For Up to Two Years	Information Leak	INFO	Ensure employees are not using the affected credentials for any corporate or third-party logins.	Varies	730
Critical-Severity CVSS v3.0 Content Management System Vulnerability in Last Observation	Application Security	LOW	Regularly update CMS software, plugins, and themes to patch known vulnerabilities.	Varies	45
Critical-Severity CVSS v3.0 Service Vulnerability in Last Observation	Patching Cadence	LOW	Update or patch affected software and hardware. Enable automatic updates if available from your software vendor and permitted in your environment.	Varies	45
Critical-Severity CVSS v3.0 Vulnerability Patching Cadence	Patching Cadence	LOW	Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure.	Varies	150
Data Leak Detected	Hacker Chatter	INFO	Start by conducting a thorough forensic investigation to determine the scope and source of the breach. Enhance your cybersecurity measures by updating firewalls, employing advanced encryption, and ensuring all software is up-to-date with the latest security patches.	Varies	90
DNS Server Accessible	Network Security	MEDIUM	Perform a security audit of your DNS server configuration and apply any necessary controls, such as a firewall or DNS Security Extensions.	Weekly	45
Domain Advertised as Ransomware Victim	Hacker Chatter	HIGH	Perform a system audit to find how the attackers were able to gain entry. Then fix the issue. This may involve having to reset passwords or deploying other authentication methods. When you verify that no trace of the attacker remains, restore the data from most recent good backups if possible. Make sure to notify parties whose data may have been compromised.	Varies*	90
Domain Targeted By Threat Actor Group	Hacker Chatter	INFO	To mitigate the risks of being mentioned on the dark web, strengthen your cybersecurity posture. Conduct regular security audits to identify and patch vulnerabilities.	Varies	90
DOS Attack Attempt Detected	IP Reputation	LOW	Investigate the IP listed in the Findings table below. Then perform an incident response management process.	Varies*	15
Elasticsearch Service Observed	Network Security	MEDIUM	Remove the service from the Internet. Consider placing the service behind a VPN, preventing public access. If making the service private is not possible, restrict the service by allowlisting the IP addresses that require access.	Weekly	45
Email exposed	Information Leak	MEDIUM	Reset the password for the compromised account. If the username is no longer active, ensure that no other services link to the affected email address, such as cloud-based applications that your organization uses.	Varies*	15
Embedded IOT Web Server Exposed	Network Security	LOW	Place the IOT web server behind a firewall.	Weekly	45
Employer exposed	Information Leak	LOW	Reset the password for the compromised account. If the username is no longer active, ensure that no other services link to the affected email address, such as cloud-based applications that your organization uses.	Varies*	15
End-of-Life Product	Patching Cadence	MEDIUM	Ensure the affected product has an extended support contract that includes security patches. Review the vendor's statement of EOL guidelines for replacement products and upgrade to a new product line or manufacturer.	Weekly	45
End-of-Service Product	Patching Cadence	MEDIUM	Replace or upgrade the affected product. Review the vendor's statement of EOS guidelines for replacement products or contact the vendor. In some cases, it may be possible to negotiate a custom support plan for the EOS product.	Weekly	45

Issue Type	Factor	Severity	Recommendation	Frequency	Age Out
Exploit Attempt Detected	Information Leak	MEDIUM	Investigate the IP listed in the Findings table below. Then perform an incident response management process.	Varies*	15
Exposed Personal Information (Historical)	Social Engineering	LOW	It's not feasible to remove the information off the internet once exposed so mitigation against social engineering attacks are recommended. Ensure that:\n* employees have regular cyber security awareness training * protocols are established for handling sensitive information * periodic, unannounced, tests are performed.	Varies*	None
FTP Service Observed	Network Security	MEDIUM	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.	Weekly	45
Hashed password exposed	Information Leak	INFO	Reset the password for the compromised account. If the username is no longer active, ensure that no other services link to the affected email address, such as cloud-based applications that your organization uses.	Varies*	15
High-Severity CVSS v3.0 Content Management System Vulnerability in Last Observation	Application Security	LOW	Regularly update CMS software, plugins, and themes to patch known vulnerabilities.	Varies	45
High Severity Content Management System vulnerabilities identified	Application Security	MEDIUM	To resolve this issue, review the version of the CMS and plug-ins in use and ensure that they are updated. Put in place a system of constant CMS patching and reviews of new vulnerabilities from the security center of the CMS developer site.	Weekly	45
High Severity CVEs Patching Cadence	Patching Cadence	LOW	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 updating schedule for all soft- ware and hardware in use within your enterprise, ensuring that all the latest patches are implemented as they are released.	Weekly	120
High-Severity CVE patching analyzed	Patching Cadence	INFO	Monitor CVE lists and vulnerability repositories for exploit code that may affect the network infrastructure. Subscribe to the National Vulnerability Database (NVD) RSS or other feeds to learn of new exploits and vulnerabilities as they are released. Maintain a regular updating schedule for all your software and hardware, and apply all the latest patches as they are released. Also, correlate this analysis with individual CVE findings in your Scorecard to help you better understand the effectiveness of your patching practices.	Weekly	1
High-Severity CVSS v3.0 Service Vulnerability in Last Observation	Patching Cadence	LOW	Update or patch affected software and hardware. Enable automatic updates if available from your software vendor and permitted in your environment.	Varies	45
High-Severity CVSS v3.0 Vulnerability Patching Cadence	Patching Cadence	LOW	Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure.	Varies	120
High-Severity Vulnerability in Last Observation	Patching Cadence	MEDIUM	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.	Weekly	45
HTTP Proxy Service Detected	Network Security	MEDIUM	Verify whether the HTTP proxy service has a legitimate use. Otherwise, remove it from your network.	Weekly	45
IMAP Service Observed	Network Security	MEDIUM	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.	Weekly	45

Issue Type	Factor	Severity	Recommendation	Frequency	Age Out
Industrial Control System Device Accessible	Network Security	MEDIUM	Review the business necessity of exposing an ICS device, such as Modbus, DNP3, BACNET, or other critical infrastructure devices. Place such devices behind a VPN or firewall. If it is not possible to remove the service from the internet, consider restricting the service by adding dependent IPs to an allow list.	Weekly	45
Information Stealer Detected	IP Reputation	INMFO	In response to the detected information stealer, it is recommended to immediately isolate affected systems to prevent further data exfiltration. Initiate a thorough scan using updated antivirus and anti-malware tools to identify and remove the malicious software.	Varies	15
Insecure channel exposes sensitive information	Application Security	MEDIUM	Ensure that all pages in your site enforce use of SSL encryption and HTTPS protocol.	Weekly	15
Insecure HTTPS Redirect Pattern	Application Security	LOW	Any HTTP site should redirect the user to a secure (i.e. HTTPS) version of the same domain that was originally requested (or a higher-level/parent version of that same domain). For example, http://www.example.com should only redirect either to https://www.	Weekly	45
Instant messaging account exposed	Information Leak	INFO	Reset the password. For cases where the username is no longer used, ensure that no other services link to the affected email/user. Suggest to the affected user to not accept chat requests with unknown parties.	Varies*	15
IP address exposed	Information Leak	LOW	Have members of your organization use a virtual private network (VPN) to prevent threat actors from tracing their internet activity to the organization. Discourage use of the corporate network for personal use.	Varies*	15
IP Camera Accessible	Network Security	MEDIUM	Review the business necessity of exposing a public IP camera feed. Only keep it open when necessary, for example, for a purposely open feed. Even then, you could embed it in a website without exposing the underlying camera IP. If removal is not possible,	Weekly	45
IP on blacklist due to malicious activity	IP Reputation	MEDIUM	Regularly monitor IP reputation databases for any posted IP address that belongs to the organization. Investigate to rule out that the posting is a false positives or malicious. If not, remediate any issues on the IP address that are likely causing it to be on a blocklist. For example, scan for, and remove any malware on it. Ask the publisher of the blocklist to remove the IP address. Deploy email filtering and firewalls using the blocklists to deter inbound spam and malicious traffic.	Varies*	15
Java Debugger Detected	Network Security	INFO	Place the Java debugging service behind a firewall or otherwise block it from detection on the internet.	Weekly	45
Known compromised or Hostile Host	IP Reputation	MEDIUM	Investigate the IP listed in the Findings table below. Then perform an incident response management process.	Varies*	15
Language exposed	Information Leak	INFO	Reset the password for the compromised account. If the username is no longer active, ensure that no other services link to the affected email address, such as cloud-based applications that your organization uses.	Varies*	15
LDAP Server Accessible	Network Security	MEDIUM	Observe security best practices for your LDAP server and apply controls, such as using TLS to encrypt sessions.	Weekly	45
LDAP Server Allows Anonymous Binding	Network Security	MEDIUM	Disable anonymous binding on your LDAP server, which is easy to do.	Weekly	45
Link redirects to insecure website	Application Security	LOW	Ensure that all of your website's link or redirect destinations are secure, or provide visitors with explicit warnings when they are not.	Weekly	15
Low Severity Content Management System vulnerabilities identified	Application Security	MEDIUM	To resolve this issue, review the version of the CMS and plug-ins in use and ensure that they are updated. Put in place a system of constant CMS patching and reviews of new vulnerabilities from the security center of the CMS developer site.	Weekly	45
Low Severity CVEs Patching Cadence	Patching Cadence	LOW	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 updating schedule for all software and hardware in use within your enterprise, ensuring that all the latest patches are implemented as they are released.	Weekly	60

Issue Type	Factor	Severity	Recommendation	Frequency	Age Out
Low-Severity CVE patching analyzed	Patching Cadence	INFO	Monitor CVE lists and vulnerability repositories for exploit code that may affect the network infrastructure. Subscribe to the National Vulnerability Database (NVD) RSS or other feeds to learn of new exploits and vulnerabilities as they are released. Maintain a regular updating schedule for all your software and hardware, and apply all the latest patches as they are released. Also, correlate this analysis with individual CVE findings in your Scorecard to help you better understand the effectiveness of your patching practices.	Weekly	1
Low-Severity CVSS v3.0 Content Management System Vulnerability in Last Observation	Application Security	LOW	Regularly update CMS software, plugins, and themes to patch known vulnerabilities.	Varies	45
Low-Severity CVSS v3.0 Service Vulnerability in Last Observation	Patching Cadence	LOW	Update or patch affected software and hardware. Enable automatic updates if available from your software vendor and permitted in your environment.	Varies	45
Low-Severity CVSS v3.0 Vulnerability Patching Cadence	Patching Cadence	LOW	Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure.	Varies	60
Low-Severity Vulnerability in Last Observation	Patching Cadence	MEDIUM	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.	Weekly	45
Malformed SPF Record	DNS Health	MEDIUM	A malformed SPF record can occur as the result of different conditions including: creating multiple SPF records per domain, invalid modifiers, and reaching maximum number of modifiers. The SPF standard can be found at https:// tools.ietf.org/html/rfc7208. Additionally, there are tools available at the SPF Project, http:// www.open-spf.org/Tools.	Weekly	15
Malicious botnet C2 server detected	IP Reputation	HIGH	Investigate the IP listed in the Findings table below. Then perform an incident response management process.	Varies*	15
Malicious Scan Detected	IP Reputation	HIGH	Investigate the IP listed in the Findings table below. Then perform an incident response management process.	Varies*	15
Malicious TOR Exit Node Detected	IP Reputation	HIGH	Avoid using Tor for business purposes whenever possible and use a virtual private network (VPN) to encrypt internet traffic.	Varies*	15
Malicious TOR Relay/Router Node Detected	IP Reputation	LOW	Avoid using Tor for business purposes whenever possible and use a virtual private network (VPN) to encrypt internet traffic.	Varies*	15
Malicious User Agent Detected	IP Reputation	LOW	Create rules to normalize user-agent strings to enable monitoring of endpoints for out-of-date applications and unauthorized software. Remove this computer from the network and reinstall its operating system. Disable unnecessary ports, protocols, or services. Restrict or discontinue any use of FTP and Telnet services, non-approved VPN services, or remote network administration tools. Change all account passwords and enforce a strong password policy. Train employees to anticipate and prevent social engineering attacks.	Varies*	15
Malware Controller Observed	IP Reputation	LOW	Investigate the devices associated with the IP addresses listed, checking for evidence of malware infections.	Varies*	30
Malware Detected	IP Reputation	HIGH	Disconnect the device from your network, back up important files, run a malware scan, and reinstall the operating system. Then restore backed-up files. For long-term protection, maintain a schedule of recurring malware scans and train the organization to anticipate, and prevent, social engineering campaigns.	Varies*	15
Malware Infection	IP Reputation	LOW	Investigate the devices associated with the IP addresses listed, checking for evidence of malware infections.	Varies*	30

Issue Type	Factor	Severity	Recommendation	Frequency	Age Out
Malware Infection Trail	IP Reputation	LOW	Investigate the devices associated with the IP addresses listed, checking for evidence of malware infections.	Varies*	365
Medium Severity Content Management System vulnerabilities identified	Application Security	MEDIUM	To resolve this issue, review the version of the CMS and plug-ins in use and ensure that they are updated. Put in place a system of constant CMS patching and reviews of new vulnerabilities from the security center of the CMS developer site.	Weekly	45
Medium Severity CVEs Patching Cadence	Patching Cadence	LOW	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 updating schedule for all software and hardware in use within your enterprise, ensuring that all the latest patches are implemented as they are released.	Weekly	90
Medium-severity CVE patching analyzed	Patching Cadence	INFO	Monitor CVE lists and vulnerability repositories for exploit code that may affect the net- work infrastructure. Subscribe to the National Vulnerability Database (NVD) RSS or other feeds to learn of new exploits and vulnerabilities as they are released. Maintain a regular updating schedule for all your software and hardware, and apply all the latest patches as they are released. Also, correlate this analysis with individual CVE findings in your Scorecard to help you better understand the effectiveness of your patching practices.	Weekly	1
Medium-Severity CVSS v3.0 Service Vulnerability in Last Observation	Patching Cadence	LOW	Update or patch affected software and hardware. Enable automatic updates if available from your software vendor and permitted in your environment	Varies	45
Medium-Severity CVSS v3.0 Vulnerability Patching Cadence	Patching Cadence	LOW	Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure.	Varies	90
Medium-Severity Vulnerability in Last Observation	Patching Cadence	MEDIUM	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.	Weekly	45
Microsoft SQL Server Service Observed	Network Security	MEDIUM	Exposing database services to the Internet is not recommended. Consider placing the service behind a VPN, preventing public access. If making the service private is not possible, restrict the service by allowlisting the IP addresses that require access.	Weekly	45
Minecraft Server Accessible	Network Security	MEDIUM	Unless you are an ISP or hosting provider, there is no need to run an externally exposed Minecraft server on your network. If you do, add people approved for access to an allow list on a firewall.	Weekly	45
Mirai Botnet Traffic Detected	IP Reputation	MEDIUM	Follow Center for Internet Security (CIS) benchmarks for best practices to secure targets or potential targets. Ensure that all IoT devices are on a separate network from systems critical for daily operations. Keep IoT device versions and operating systems up to date. Run regular malware scans. Change all account passwords and enforce a strong password policy. Train employees to anticipate and prevent social engineering attacks.	Varies*	15
Mobile Printing Service Detected	Network Security	LOW	Determine whether exposing a mobile printing service to the internet is necessary. If not, place it behind a firewall and restrict its access to trusted users.	Weekly	45
MongoDB Service Observed	Network Security	MEDIUM	Exposing database services to the Internet is not recommended. Consider placing the service behind a VPN, preventing public access. If making the service private is not possible, restrict the service by allowlisting the IP addresses that require access.	Weekly	45
MOVEit Service in Use (CVE-2023-34362)	Application Security	INFO	Promptly identify if you have any MOVEit servers. If you do, immediately close Ports 80/443, plus any additional ports facing the public internet that the services may be running on.	Varies	45

Issue Type	Factor	Severity	Recommendation	Frequency	Age Out
MySQL Server Running with Empty Password	Network Security	LOW	Require a password challenge for your internet-exposed MySQL server, or place it behind a firewall.	Weekly	45
MySQL Service Observed	Network Security	MEDIUM	Exposing database services to the Internet is not recommended. Consider placing the service behind a VPN, preventing public access. If making the service private is not possible, restrict the service by allowlisting the IP addresses that require access.	Weekly	45
Name exposed	Information Leak	INFO	Reset the password for the compromised account. If the username is no longer active, ensure that no other services link to the affected email address, such as cloud-based applications that your organization uses.	Varies*	15
Neo4j Database Accessible	Network Security	INFO	Move the Neo4J database onto a VPN, or behind a firewall.	Weekly	45
NetBus Remote Access Service Detected	Network Security	INFO	Restrict NetBus service to known, essential users.	Weekly	45
Network Attached Storage Device Exposed	Network Security	HIGH	Assess the business need for exposing a NAS device to the internet, and consider placing it behind a firewall.	Weekly	45
Networking Service Observed	Network Security	MEDIUM	This issue type concerns a networking service or device, such as a router or service that is associated with routers like BGP, a firewall, or tunneling service. No change or update to your internet-facing assets is necessary.	Weekly	45
Non-social media access token exposed	Information Leak	INFO	Reset the password for the compromised account. If the username is no longer active, ensure that no other services link to the affected email address, such as cloud-based applications that your organization uses.	Varies*	15
Non-standard links detected: Contact information displayed	Application Security	LOW	Review the need to expose personal contact information and remove any unnecessary instances. Train your staff to heighten their awareness of signs of social engineering attacks.	Weekly	15
Non-standard links detected: Local file path exposed	Application Security	LOW	Follow security best practices for creating URLs and impose restrictions on file URLs if possible.	Weekly	15
Non-standard links detected: Unsafe File Transfer Protocol	Application Security	MEDIUM	Use secure, encrypted protocols for transferring data.	Weekly	15
Non-standard links detected: Unsafe Telnet protocol	Application Security	INFO	Use secure, encrypted protocols for accessing computers remotely.	Weekly	15
November 2022 OpenSSL 3.X vulnerability detected	Application Security	HIGH	Note the SSL versions in the Findings table below. Update vulnerable versions to the 3.0.7 patch.	Weekly	45
Occupation exposed	Information Leak	INFO	Reset the password for the compromised account. If the username is no longer active, ensure that no other services link to the affected email address, such as cloud-based applications that your organization uses.	Varies*	15
Open Port Discovered	Network Security	INFO	Disable or restrict access to open RDP and SSH ports if they are not required for remote administration. This reduces the attack surface and minimizes the potential for unauthorized access.	Varies	45
OpenVPN Device Accessible	Network Security	MEDIUM	This issue type concerns a router, server, or networking device that is running OpenVPN on your network. No change or update to your internet-facing assets is necessary, but examining such devices for evidence of compromise is recommended.	Weekly	45
Oracle Database Server Accessible	Network Security	MEDIUM	Move the Oracle database onto a VPN or behind a firewall, and only allow dependent applications to access it.	Weekly	45
Oracle Service Registry Detected	Network Security	INFO	Place the Oracle Service Registry behind a firewall.	Weekly	45

Issue Type	Factor	Severity	Recommendation	Frequency	Age Out
Outdated Operating System Observed	Endpoint Security	HIGH	Update affected device's operating system. Enable automatic updates if available from your software vendor and permitted in your environment. 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.	Weekly	30
Outdated Web Browser Observed	Endpoint Security	HIGH	Update the web browsers in question. Enable automatic updates if available from your web browser vendor and permitted in your environment.	Varies*	30
Parent's name exposed	Information Leak	INFO	Reset the password. Subscribe to an identity-monitoring service to ensure no unauthorized accounts were made in the user's name.	Varies*	15
Password exposed	Information Leak	INFO	Reset the password for the compromised account. If the username is no longer active, ensure that no other services link to the affected email address, such as cloud-based applications that your organization uses.	Varies*	15
Password hint exposed	Information Leak	MEDIUM	Reset the password for the compromised account. If the username is no longer active, ensure that no other services link to the affected email address, such as cloud-based applications that your organization uses.	Varies*	15
Phishing Infrastructure	IP Reputation	INFO	Investigate the devices associated with the IP addresses listed, checking for evidence of malware infections.	Varies*	45
Phone number exposed	Information Leak	INFO	Reset the password for the compromised account. If the username is no longer active, ensure that no other services link to the affected email address, such as cloud-based applications that your organization uses.	Varies*	15
Physical address exposed	Information Leak	INFO	Reset the password for the compromised account. If the username is no longer active, ensure that no other services link to the affected email address, such as cloud-based applications that your organization uses.	Varies*	15
POP3 Service Observed	Network Security	MEDIUM	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.	Weekly	45
Possible Typosquat Domains Detected	Social Engineering	INFO	To deal with domain typosquatting, start by regularly monitoring domain registrations for variations of your brand name, and consider registering common misspellings. If you find typosquatting domains that infringe on your brand, consult with legal experts and report them to domain registrars.	Varies	90
PostgreSQL Service Observed	Network Security	MEDIUM	Exposing database services to the Internet is not recommended. Consider placing the service behind a VPN, preventing public access. If making the service private is not possible, restrict the service by allowlisting the IP addresses that require access.	Weekly	45
Potential Ninja Forms Vulnerability Detected	Application Security	INFO	Check the version of any Ninja Forms plugin at use in the domain and assure that all versions are patched to version 3.6.26.	Varies	45
Potential vulnerability detected	Application Security	INFO	Identify the version of the product running on the IP address listed in the Findings table below. Search for vulnerability advisories about that version published by the product provider or the CVE database, which you can link to in the References section of this page. Follow the remediation guidance of the provider or trusted industry experts.	Weekly	20
Potentially Exposed Cisco Web UI	Application Security	INFO	Check if the web UI feature is enabled on the Cisco IOS XE Software system. If either the ip http server or ip http secure-server command is present in the configuration, it indicates that the HTTP Server feature is enabled.	Varies	45
Potentially Vulnerable Application (PVA) Installation	IP Reputation	HIGH	Investigate the devices associated with the IP addresses listed, checking for evidence of PVA installations. Watch for potentially malicious interactions between expired domains and PVAs.	Varies*	30
Potentially Vulnerable Application Installation (PVA) Trail	IP Reputation	LOW	Investigate the devices associated with the IP addresses listed, checking for evidence of PVA installations. Watch for potentially malicious interactions between expired domains and PVAs.	Varies*	365

Issue Type	Factor	Severity	Recommendation	Frequency	Age Out
Potentially Vulnerable Cisco RV320/RV325 Router	Network Security	INFO	Because the vendor no longer provides support or patches for these devices, SecurityScorecard recommends that organizations replace them immediately.	Varies	45
Potentially Vulnerable Citrix NetScaler Service Detected	Application Security	INFO	Check the version numbers of NetScaler versions in this domain and immediately apply the latest patch to vulnerable versions.	Varies	45
Potentially Vulnerable Ivanti Connect Secure or Ivanti Policy Secure (CVE-2024-21887)	Application Security	INFO	Although Ivanti has not yet released a patch for CVE-2023-46805 or CVE-2024-21887, it has released a mitigation script to address the vulnerabilities. SecurityScorecard recommends that you execute this script as soon as possible.	Varies	45
Potentially Vulnerable Ivanti Connect Secure and Ivanti Policy Secure Gateways (CVE-2023-46805)	Application Security	INFO	Although Ivanti has not yet released a patch for CVE-2023-46805 or CVE-2024-21887, it has released a mitigation script to address the vulnerabilities. SecurityScorecard recommends that you execute this script as soon as possible.	Varies	45
Potentially Vulnerable Ivanti Sentry Device Detected	Application Security	INFO	Immediately apply the latest security patch for Ivanti Sentry, and use firewall rules to restrict administrative portal access to trusted IPs.	Varies	45
Potentially Vulnerable RocketMQ (CVE-2023-33246)	Application Security	INFO	To address this vulnerability, it is crucial for users of RocketMQ to update their installations to a secure version. The recommended versions are: For RocketMQ 5.x users: Upgrade to version 5.1.1 or above. For RocketMQ 4.x users: Upgrade to version 4.9.6 or above.	Varies	45
Potentially Vulnerable RocketMQ (CVE-2023-37582)	Application Security	INFO	To address this vulnerability, it is crucial for users of RocketMQ to update their installations to a secure version. The recommended versions are: For RocketMQ 5.x users: Upgrade to version 5.1.1 or above. For RocketMQ 4.x users: Upgrade to version 4.9.6 or above.	Varies	45
Potentially vulnerable to BIG-IP Configuration utility vulnerability (CVE-2023-46747)	Application Security	INFO	Make sure that the TMUI portal, also referred to as the BIG-IP Configuration utility, lives behind a firewall and is not accessible from the public internet.	Varies	45
PPTP Service Accessible	Network Security	MEDIUM	Review the business necessity of running a PPTP service on your network. PPTP is an obsolete and insecure method for implementing VPNs. Migrate the service to a more secure VPN implementation, such as OpenVPN.	Weekly	45
Printer Detected	Network Security	MEDIUM	Assess whether there is a business need to expose your printer to the internet. If so, prevent access by unknown parties by placing it behind a firewall or using an access control list (ACL).	Weekly	45
Product Potentially Impacted by CVE-2022-41040 & CVE-2022-41082	Network Security	LOW	No patch currently exists. However, monitor the Microsoft Security Response Center advisory in the references for this issue to keep abreast of relevant updates, including a patch release. Microsoft has posted several detection methods for exploitation of these CVEs using Microsoft Defender for the Endpoint and Microsoft Defender Antivirus related to webshell exploitation including the exister Chopper detections. If possible, remove the microsoft-exchange service from the public Internet and place it behind a firewall or VPN, so only internal users can access it. This will mitigate exploitation by non-organization entities, though this will not mitigate an insider threat or adversary already within the network looking to pivot off these vulnerabilities to gain higher level access to systems.	Weekly	45

Issue Type	Factor	Severity	Recommendation	Frequency	Age Out
Product Potentially Impacted by PowerShell Remoting RCE	Network Security	LOW	No patch currently exists; however, monitor the Microsoft Security Response Center advisory in the references for this issue to keep abreast of relevant updates, including a patch release. Microsoft has posted several detection methods for exploitation of these CVEs using Microsoft Defender for the Endpoint and Microsoft Defender Antivirus related to webshell exploitation including the exister Chopper detections. If possible, remove the microsoft httpapi or microsoft-httpapi service from the public Internet and place it behind a firewall or VPN, so only internal users can access it. This will mitigate exploitation by non-organization entities, though this will not mitigate an insider threat or adversary already within the network looking to pivot off these vulnerabilities to gain higher-level access to systems.	Weekly	45
Product Running Vulnerable Log4j Version	Network Security	HIGH	Update Log4j to 2.17.1 or a later version immediately. This version only runs on Java 8, so make sure to update Java if you are using an earlier version. If multiple Log4j installations are on an impacted machine, note each can contain a vulnerable version of Log4j, and you may need to remediate each independently.	Weekly	45
Products Susceptible To Ransomware Exploits Exposed	IP Reputation	LOW	Update your internet-facing products that are susceptible to ransomware attacks, evaluate the necessity of exposing them to the internet, and tightly limit their access based on business need, if possible.	Weekly	45
Pulse Connect Secure VPN Product Observed	Network Security	MEDIUM	This issue type concerns Pulse Connect Secure VPN running on routers, servers, or networking devices on your network. No change or update to your internet facing assets is immediately necessary, but examining devices that run the VPN is recommended.	Weekly	45
Race exposed	Information Leak	INFO	Reset the password for the compromised account. If the username is no longer active, ensure that no other services link to the affected email address, such as cloud-based applications that your organization uses.	Varies*	15
Ransomware Infection Detected	IP Reputation	HIGH	Look for evidence of ransomware infection in the assets associated with the IP addresses listed in the Findings table below.	Varies*	30
Ransomware Infection Trail Detected	IP Reputation	HIGH	Look for evidence of ransomware infection in the assets associated with the IP addresses listed in the Findings table below.	Varies*	365
Ransomware – Susceptible Remote Access Services Exposed	Cubit Score	HIGH	Determine the business need of exposing these services to the public internet. If possible, isolate them behind a secure, patched VPN service or firewall with appropriate allowlisting for approved users. If they must be exposed, keep the services patched and updated continuously. Keep them under constant observation with logging and security monitoring.	Varies*	1
RDP Service Observed	Network Security	MEDIUM	Exposing remote access services to the Internet is not recommended. Consider placing the service behind a VPN, preventing public access. If making the service private is not possible, restrict the service by allowlisting the IP addresses that require access ransomware_association	Weekly	45
Redirect Chain Contains HTTP	Application Security	HIGH	Any HTTP site should immediately redirect users to HTTPS-protected URLs and ensure that any further redirects do not occur over HTTP. Prefer the usage of HTTPS URLs over HTTP when available, avoiding an unnecessary redirect.	Weekly	45
Redis Service Observed	Network Security	MEDIUM	Exposing database services to the Internet is not recommended. Consider placing the service behind a VPN, preventing public access. If making the service private is not possible, restrict the service by allowlisting the IP addresses that require access.	Weekly	45
Remote Access Service Observed	Network Security	LOW	This issue type concerns a remote access service, such as a router providing a remote login service, or a Windows server providing a remote assistance service. Examine devices on a case-by-case basis, but no change or update to your internet-facing asset is immediately necessary.	Weekly	45
rsync Service Observed	Network Security	MEDIUM	Exposing rsync services to the Internet is not recommended. Consider placing the service behind a VPN, preventing public access. If making the service private is not possible, restrict the service by allowlisting the IP addresses that require access.	Weekly	45

Issue Type	Factor	Severity	Recommendation	Frequency	Age Out
Security question and answer exposed	Information Leak	MEDIUM	Reset the password for the compromised account. If the username is no longer active, ensure that no other services link to the affected email address, such as cloud-based applications that your organization uses.	Varies*	15
Server certificate issued by country on denylist	Application Security	LOW	Audit the site for any certificates issued by CAs in countries on denylists. Replace such certificates with those issued by CAs in reputable nations.	Weekly	15
Server error detected	Application Security	LOW	Inspect and address any operational problems on the server, especially those that could affect security. Keep a regular maintenance schedule for servers, applying patches whenever updates are available.	Weekly	15
Server with Expired Certificate Contacted	Application Security	LOW	Avoid using a service on a website with an expired certificate. If possible, ask the website owner to renew the expired certificate, especially if it is critical to your business.	Weekly	15
Session Cookie Missing 'HttpOnly' Attribute	Application Security	HIGH	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.	Weekly	15
Session Cookie Missing 'Secure' Attribute	Application Security	HIGH	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.	Weekly	15
Site does not enforce HTTPS	Application Security	LOW	Any site served to a user (possibly at the end of a redirect chain) should be served over HTTPS.	Weekly	15
Site Does Not Use Best Practices Against Embedding of Malicious Content	Application Security	LOW	Add one of the following headers, using the 'DENY' or 'ALLOW-FROM' directive, to responses from this website: X-Frame-Options: DENY' X-Frame-Options: ALLOW-FROM https://example.com/'	Weekly	45
Site emits visible browser logs	Application Security	LOW	Prevent emission of browser logs in the developers console.	Weekly	15
Site fails to load page components	Application Security	LOW	Maintain a regular audit cycle for website code, replace bad code, and enforce secure coding standards.	Weekly	15
Site links to insecure websites	Application Security	LOW	Avoid providing links to insecure websites whenever possible.	Weekly	15
Site may use WebSockets to send user data	Application Security	LOW	Avoid using WebSockets to send user data. If there is a business requirement to use that protocol, add security measures such as: having WebSocket servers validate the "Origin" header against the expected origins during connection establishment and using tokens or similar methods to authenticate the WebSocket connection when sensitive data is being transferred over the WebSocket	Weekly	15
Site receives data over Websockets	Application Security	LOW	Monitor the data the website is receiving from third-party sources in real time, in case malicious or undesirable content is being sent directly to visiting browsers. Also, audit the content for sensitive data.	Weekly	15
Site requests data over insecure channel	Application Security	LOW	Ensure that all web pages and all content they contain is delivered over a SSL channel with HTTPS protocol.	Weekly	15
SMB Service Observed	Network Security	MEDIUM	Exposing SMB to the Internet is not recommended. Consider placing the service behind a VPN, preventing public access. If making the service private is not possible, restrict the service by allowlisting the IP addresses that require access.	Weekly	45
SMTP Server on Unusual Port	IP Reputation	MEDIUM	Determine whether your organization intended for the identified SMTP server to be running on an unusual port. If not, investigate why and remediate accordingly.	Weekly	45
SOAP Server Accessible	Network Security	MEDIUM	This issue type concerns a device running an exposed SOAP service on your network, which could be serving web application traffic, device traffic, or other control services.	Weekly	45
Social media account exposed	Information Leak	INFO	Reset the password. For cases where the username is no longer used, ensure that no other services link to the affected email/user. Have the affected user set privacy controls to their social media accounts.	Varies*	15

Issue Type	Factor	Severity	Recommendation	Frequency	Age Out
Social media token exposed	Information Leak	INFO	Reset the password for the compromised account. If the username is no longer active, ensure that no other services link to the affected email address, such as cloud-based applications that your organization uses. Suggest to the affected user to check their social media account and delete unknown apps from their account.	Varies*	15
Social Security number exposed	Information Leak	MEDIUM	Reset the password for the compromised account. Subscribe to an identity-monitoring service to prevent creation of unauthorized accounts in the compromised name.	Varies*	15
SOCKS Proxy Service Detected	Network Security	MEDIUM	Assess whether your use of a SOCKS proxy has a legitimate business purpose. If not, consider making it inaccessible to the internet.	Weekly	45
SPF Record Contains a Softfail without DMARC	DNS Health	MEDIUM	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.	Weekly	15
SPF Record Found Ineffective	DNS Health	MEDIUM	To resolve this issue, enumerate the list of email servers that are authorized to send email on behalf of the domain. Update the SPF record with the correct email authorization list. See the reference link for conventions to ensure that your records provide maximum protection against spoofing.	Weekly	15
SPF Record Missing	DNS Health	MEDIUM	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.	Weekly	15
SQL Payload Using Tor proxy Detected	Network Security	INFO	To mitigate SQL injection vulnerabilities and enhance cybersecurity, adopt a comprehensive approach that includes input validation, parameterized queries, web application firewall deployment, least privilege access controls, regular updates, security testing, code reviews, adherence to secure coding guidelines, ongoing training, vigilant monitoring, a well-defined incident response plan, and data encryption.	Varies	90
SSH Software Supports Vulnerable Protocol	Network Security	MEDIUM	Configure the SSH service to support only SSH protocol version 2 or higher. Upgrade the SSH service software to the latest version of software.	Weekly	55
SSH Supports Weak Cipher	Network Security	MEDIUM	Configure the SSH server to disable Arc four and CBC ciphers.	Weekly	55
SSH Supports Weak MAC	Network Security	MEDIUM	Configure the SSH server to disable the use of MD5.	Weekly	55
SSL/TLS Service Supports Weak Protocol	Network Security	HIGH	Disable the protocols listed in the evidence column of the measurement.	Weekly	45
Suspicious Traffic Observed	IP Reputation	INFO	Investigate the devices associated with the IP addresses listed, checking for evidence of malware infections or other types of compromise.	Varies*	30
Telephony/VoIP Device Accessible	Network Security	INFO	This issue type is an internet-facing telephony service or device, such as a VoIP product or service associated with SIP, a SIP proxy, or similar protocols. No change is necessary, as there is no inherent risk.	Weekly	45
Telnet Service Observed	Network Security	MEDIUM	Telnet is an inherently unsafe protocol. Remove the service from the Internet. If a remote access service is necessary, replace Telnet with SSH if possible. If not possible, often the case with older networked hardware, ensure the service is only accessible by VPN.	Weekly	45
Threat actor infrastructure detected	IP Reputation	INFO	Perform a complete Digital Forensics and Incident Response (DFIR), starting with the flagged asset and expanding to any assets that communicate with it. Refer to the Findings table below for the implicated IP address and port numbers, the protocol used to host the threat actor infrastructure, and the SHA256 hash value of the malware detected in your asset's communications. After removing the threat actor's software, contact any organization who blocked your affected IPs, and provide evidence to have the block removed.	Varies*	30

Issue Type	Factor	Severity	Recommendation	Frequency	Age Out
TLS Certificate Status Request ("OCSP Stapling") Detected	Network Security	INFO	There are no drawbacks to implementing OCSP stapling and servers should adopt this practice wherever possible. In addition to providing clear security benefits, implementation of OCSP stapling removes the need for maintenance of CRLs and can vastly reduce the traffic on organization-owned OCSP servers, which also provides operational benefits.	Weekly	45
TLS Service Supports Weak Cipher Suite	Network Security	LOW	Disable the cipher suites listed in the evidence column of the measurement.	Weekly	45
TOR Server Detected	Network Security	HIGH	Unless there is a specific, legitimate business reason for running it, remove the TOR server from your network.	Weekly	45
Tor Traffic Detected	Network Security	INFO	Begin by identifying the device or user responsible for the TOR connection and assess whether it aligns with legitimate business or personal needs. If there are no valid reasons for its use, consider blocking or restricting TOR access within your network to mitigate potential security risks.	Varies	90
Unsafe Implementation Of Subresource Integrity	Application Security	LOW	Please ensure that all website elements (i.e. <script> and <link>) loading JavaScript and CSS stylesheets hosted with external organizations contain the 'integrity' directive with a valid checksum.	Weekly	45
UPnP Accessible	Network Security	HIGH	Review the business need of exposing UPnP-enabled devices. Hide them behind a firewall, or make them accessible only on an intranet.	Weekly	45
User-agent string exposed	Information Leak	INFO	Reset the password for the compromised account. If the username is no longer active, ensure that no other services link to the affected email address, such as cloud-based applications that your organization uses.	Varies*	15
Username exposed	Information Leak	INFO	Reset the password for the compromised account. If the username is no longer active, ensure that no other services link to the affected email address, such as cloud-based applications that your organization uses.	Varies*	15
VNC Service Observed	Network Security	MEDIUM	Exposing remote access services to the Internet is not recommended. Consider placing the service behind a VPN, preventing public access. If making the service private is not possible, restrict the service by allowlisting the IP addresses that require access.	Weekly	45
Vulnerable VMWare ESXi Server Detected	Application Security	HIGH	Apply VMWare's update to any unpatched servers as soon as possible. Otherwise, deactivate OpenSLP services or limit access to a list of trusted IP addresses. Maintain up-to-date backups of data that threat actors may target for encryption. Only expose services to the wider internet when necessary. Consistently monitor network traffic for any unexpected behavior.	Weekly	45
Web Application Firewall (WAF) Detected	Application Security	POSITIVE	Companies should consider implementing a web application firewall that can protect against common web vulnerabilities, such as SQL Injection and cross-site scripting (XSS). Many hosting providers offer WAF capabilities as well.	Weekly	45
Web application potentially vulnerable to Spring4Shell	Application Security	LOW	Upgrade Spring Core to versions 5.3.18 or 5.2.20 and Spring Boot 2.6.6, depending on the variant. If not possible, apply appropriate configuration changes or follow downgrading instructions from Spring at https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement#suggested-workarounds.	Weekly	45
Website communicates with payment provider	Application Security	HIGH	Protect this website with common application security controls, such as a valid TLS certificate and secure cookies.	Weekly	15
Website copyright is current	Application Security	INFO	Continue updating the website's copyright each year.	Weekly	15
Website Copyright is Not Current	Application Security	INFO	Review all of your site content and code regularly to ensure that copyrights, code, and other content remain up to date.	Weekly	15

Issue Type	Factor	Severity	Recommendation	Frequency	Age Out
Website defaced	Application Security	INFO	Investigate how threat actors were able to access the web server. Based on your findings, install controls to prevent similar events in the future. Be especially cautious about file uploads to your site or prevent them altogether.	Weekly	15
Website Does Not Implement HSTS Best Practices	Application Security	LOW	Every web application (and any URLs traversed to arrive at the website via redirects) should set the HSTS header to remain in effect for at least 12 months (31536000 seconds). It is also recommended to set the 'includeSubDomains' directive so that request	Weekly	45
Website does not implement X-Content-Type-Options Best Practices	Application Security	LOW	Add the following header to responses from this website: 'X-Content-Type-Options: nosniff'	Weekly	45
Website does not implement X-XSS-Protection Best Practices	Application Security	INFO	Add the following header to responses from this website: 'X-XSS-Protection: 1; mode=block'	Weekly	45
Website Hosted by GoDaddy's Wordpress	Application Security	INFO	Consult with GoDaddy to find out if your website has been impacted by the breach. Have users in your organization change their website login credentials. Train your organization to recognize and report phishing emails.	Weekly	15
Website Hosted on Object Storage	Application Security	LOW	Ensure that the usage of external services, such as Amazon S3, conforms to company policies.	Weekly	45
Website References Object Storage	Application Security	HIGH	Ensure that the usage of external services, such as Amazon S3, conforms to company policies.	Weekly	45
Website Uses GoDaddy TLS Certificates	Network Security	INFO	Consult with GoDaddy to find out if your website has been impacted by the breach. Have users in your organization change their website administration login credentials. Train your organization to recognize and report phishing emails.	Weekly	45
Websocket requests contain sensitive fields or PII	Application Security	HIGH	Remove sensitive information from websocket requests.	Weekly	15

***There is no regular scanning frequency for this issue type. We collect data from multiple sources when it is available.**

Signal Processing Workflow

Generating meaningful cybersecurity ratings consists of four distinct processing stages:

Signal Collection, Attribution Engine, Cyber Analytics, and Scoring Engine.

Signal Collection

- IPv4 Scans
- Malware Sinkholes
- DNS data
- External data feeds

Attribution Engine

- RIR, DNS, SSL data
- Domain discovery
- Subdomains
- IP-domain pairing

Cyber Analytics

- Study emerging threats
- CVEs
- Machine Learning

Score Engine

- Digital Footprint
- Size normalization
- Factor scores
- Total score

Signal Collection

SecurityScorecard scans the entire IPv4 webspace at a regular cadence to identify vulnerable digital assets. Additionally, SecurityScorecard monitors signals across the internet, relying on a global network of sensors that spans the Americas, Asia, and Europe. We operate one of the world's largest networks of sinkholes and honeypots to capture malware signals and further enrich our data set by leveraging commercial and open-source intelligence sources. SecurityScorecard supplements its data collection with external feeds from approximately 40 third-party public and commercial data sources. SecurityScorecard ingests approximately 1.5 Terabytes of data daily aspart of our signal collections program

Attribution Engine

Most of the signals collected are associated with an IP or related domain, which must then be matched with an organization, based on its digital footprint.

Attribution of IPs is a challenging process due to the dynamic nature of the internet. Netblocks of IPs can be assigned dynamically by Internet Service Providers (ISP), Cloud Service Providers (CSP), and Content Delivery Networks (CDN). These can change by the day or even by the hour. Furthermore, due to the distributed nature of the internet, DNS updates can take time to propagate across the web.

Fundamentally, attribution is a stochastic or probabilistic process, rather than a deterministic one. This means that on a practical basis, attribution can never be 100% accurate. However, with good quality data sources and advanced algorithms, the error rate can be held to a reasonably low level.

SecurityScorecard performs attribution using automated processes operating at internet scale, incorporating machine learning algorithms to optimize accuracy.

SecurityScorecard attributes IPs to domains using RIR, DNS, SSL and other means as well as using third party data feeds. As each data source has its own confidence level, the data sources are aggregated for each candidate domain-IP pair and the domain-IP pair is accepted if the overall confidence level is satisfactory. The IP digital footprints are updated daily.

In addition to IP attribution, SecurityScorecard operates a domain discovery process to find related domains and subdomains that are controlled by each scored organization.

For each scorecard, SecurityScorecard utilizes the Domain WHOIS service as well as passive DNS sources to generate a list of related domains. The list is then processed using statistical techniques and substring matching to retain only high confidence related domains.

Based on pentesting by independent experts, the False Positive Rate for incorrectly attributing a domain to an organization is typically less than 5%.

We perform subdomain discovery using in-house systems which use data from CommonCrawl, SSL certifications, as well as several commercially available data feeds. Since subdomains are resolved to DNS A records and are owned by the parent domain, the effective False Positive rate is very low.

Based on an independent assessment by security firm, the False Positive Rate for domain attribution was less than 1%.

Cyber Analytics

SecurityScorecard deploys a suite of analytics developed by its Threat Intel researchers, Data Scientists, and Software Engineers to extract and derive key insights from the raw input signals. Examples of key analytics, engineering and data processing include:

- Reverse engineering of malware families to enable identification of different malware strains and characterization of their behavior and threat level.
- Identification of CVEs and other vulnerabilities based on examination of digital assets returned from banner grabs as well as analysis of website code base, communication protocols, and SSL certifications.
- Application of machine learning algorithms to improve the quality and accuracy of security findings and provide ke insights on security posture.

Scoring Engine

Scoring is a deterministic process based on an organization's digital footprint and observed risk signals. SecurityScorecard's scoring engine publishes and updates scores daily on more than 12 million organizations around the world. Our scoring methodology is described here.

Scoring Methodology

A unique challenge in providing fair and accurate ratings for organizational cybersecurity is properly accounting for the wide range of organizational sizes. Smaller entities, such as "MomAndPop.com" bearing a small digital footprint with just a single or a few IPs, will inevitably have fewer findings and correspondingly fewer security flaws compared to large enterprises operating over as many as hundreds of millions of IPs.

Conversely, larger entities will nearly always have more security defects than smaller entities and would receive worse security scores if no correction were made for the size of the digital footprint.

Size Normalization

To eliminate bias due to size, SecurityScorecard developed a principled scoring methodology based on a robust, statistical framework that ensures fair scores regardless of organization size.

Many types of security issues scale with the size of the organization. Larger organizations typically have a larger "attack surface" compared to smaller entities. More employees mean more devices to be protected and more servers mean more chances for an exposed port which should properly sit behind a firewall. Some issue types scale with the number of IPs. Others might scale with the number of related domains or number of employees.

As noted above, the digital footprint of different organizations can vary from a single IP to hundreds of millions of IPs. This range spans more than eight orders of magnitude, or more than eight multiples of ten. The best way to make meaningful measurements over such a large dynamic range is to use a logarithmic scale, where each increment corresponds to a multiple of 10.

Other common examples where a logarithmic scale is used to compare measurements spanning a wide dynamic range include the following:

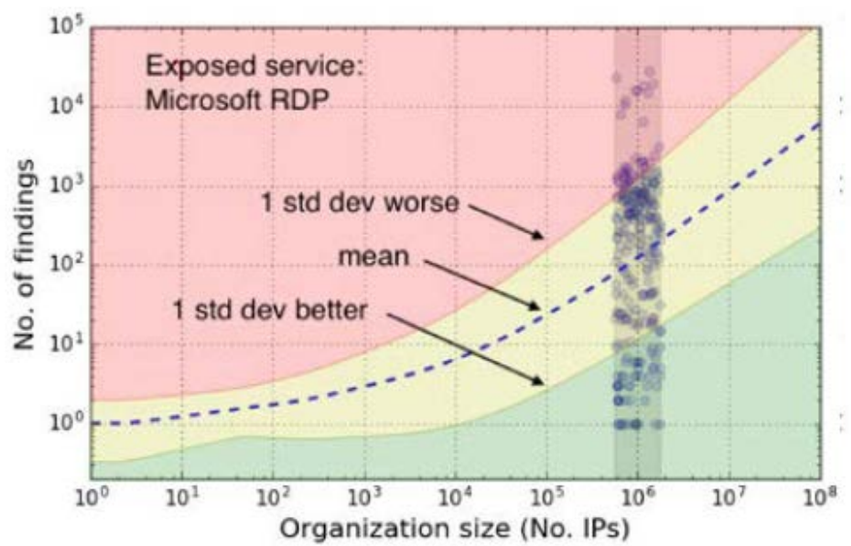
- Richter scale for measuring earthquakes over more than 9 order of magnitude.
- Decibel scale for measuring sound amplitude over 12 orders of magnitude.
- pH scale for measuring chemical acidity over 14 orders of magnitude.

Size normalization begins with scatter plots to capture how the number of occurrences of a given issue varies with organization size.

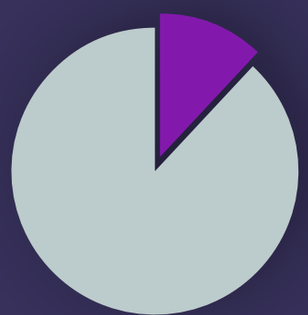
For each organization and each security issue, the number of occurrences of the issue type is captured. The **example shown** is open port 3389, which corresponds to Microsoft's Remote Desktop Protocol. A scatter plot is generated in which every scored entity represents a point on a log-log plot of the logarithm of the number of issue counts (y-axis) vs. the logarithm of the number of IPs (x-axis). A typical scatter plot will contain millions of data points, providing a large statistical "mass" for better accuracy and stability.

The large quantity of organizations scored by SecurityScorecard — currently more than 12 million — helps ensure an accurate characterization of the distribution of the number of occurrences of each issue type with organization size, resulting in more accurate scoring.

The size normalization process enables SecurityScorecard to provide score context for its users. In the example shown on the following page, the company has 3 instances of DNS Open Resolver, a misconfiguration of DNS services that can be exploited by malicious actors to launch a DDoS attack, potentially causing business interruption and reputational harm. Based on SecurityScorecard's analysis of 12 million organizations, only 12% of entities of comparable size have this security flaw. Furthermore, among those similarly sized companies that do have the same flaw, the average number of such findings is 2, while this company has 3 findings, which is worse than average.



Comparison to similar companies



- 12% have this issue, just like this company
- 88% do not have this issue
- 2 findings on average
- 3 findings for this company

Calibration Process

SecurityScorecard generates a scatter plot similar to the example on the previous page for every scored issue type. A locally-weighted, nonparametric fitting algorithm is then applied to characterize both the mean (blue dashed curve) and the standard deviation of the number of expected issue counts as functions of organization size.

It is noteworthy that the dependence of issue counts on organization size is non-linear (the dashed blue line is curved). Simply assuming that the number of issue counts scales linearly with size would introduce serious errors, resulting in systematically distorted and incorrect cybersecurity scores.

This calibration process is carried out for every scored issue type, using data collected over a 2-month time interval to smooth out statistical fluctuations.

This process enables fair performance comparisons of organizations to others of similar size. In the example scatter plot, an organization in the red zone is at least 1 standard deviation worse than the mean, while an organization in the green zone is at least 1 standard deviation better than the mean. This approach ensures that comparisons are always made relative to other organizations of similar size.

Calculating Factor Scores

The calibration process described above enables a reliable and stable statistical estimate to be calculated for a given organization and security issue, corresponding to how many standard deviations above or below the mean that organization is situated for the particular security issue. In statistical parlance, this is known as a “z-score”.

SecurityScorecard uses a “modified z-score”, where $z = 0$ if no findings are present, while $z = 1$ when the number of findings equals the mean for entities with the same size digital footprint. In this framework, $0 \leq z < 1$ corresponds to better than average, while $z > 1$ corresponds to worse than average.

Calculating Raw Total Score

$$RTS_d = \sum_{i \in f} w_i \times z_{di}$$

In version 3.0 of our scoring methodology, we no longer use a factor score to calculate the total score. We calculate the raw total score (RTS) by adding up all the z-scores associated with issue findings multiplied by their weights, or severity levels (low, medium, high, critical).

We use machine learning to calculate weights based on their correlation to likelihood of breach: the greater the correlation, the greater the severity level.

Calculating Total Score

$$TS_d = MAX - \frac{MAX - TS_0}{\mu(x_d)} \times RTS_d$$

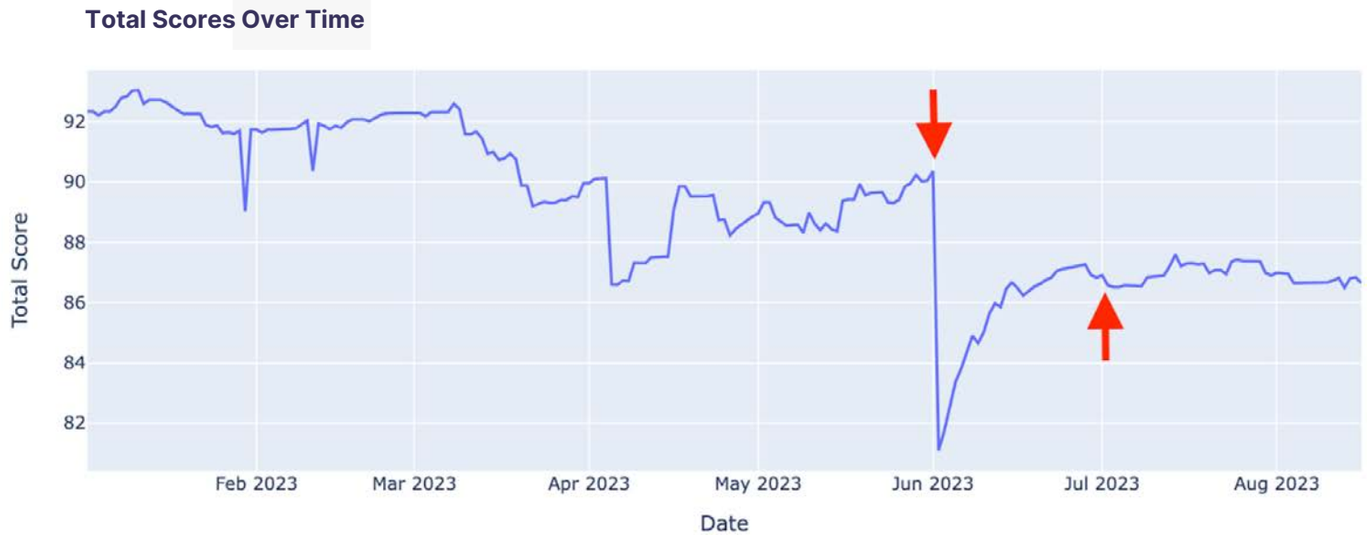
After calculating the raw total score, we scale it based on the expected value of issue finding counts. We want to fairly score an organization by comparing it to others with similar Digital Footprint sizes.

Informational and positive issues do not contribute to the score.

Breach Penalty

A data breach at an organization is external evidence that a security intrusion has occurred, reflecting increased risk. To reflect this risk, its score is reduced by 10% upon disclosure of a breach. The negative score impact of the penalty gradually diminishes to zero over a 30-day period.

The score history at right illustrates the impact of a data breach that occurred in early June. The breach penalty reduced the score by 10 percent from 90 to 81. The penalty's impact on the score diminished over the next 30 days and then no longer affected the score in early July.



Keeping the Scoring Framework Current

SecurityScorecard makes every effort to create and maintain cybersecurity ratings that are meaningful, accurate, and relevant.

Since cyber threats are constantly evolving with the emergence of new threats and development of new countermeasures and best practices — much like an arms race — SecurityScorecard continuously monitors the threat landscape and evaluates new data sources and new analytics to better reflect cybersecurity risk.

Calibration Cadence

As part of this effort, SecurityScorecard recalibrates its scoring algorithm on a regular monthly cadence. Similarly, credit rating agencies, including FICO, S&P, and Moody's also recalibrate their scoring algorithms periodically, albeit less frequently owing to the relative stability of financial risk ratings criteria compared to cybersecurity risk ratings.

Maintaining a regular scoring update cadence enables SecurityScorecard to preserve fair cybersecurity risk ratings in a dynamic threat environment and also to introduce new issue types reflecting new risk metrics, as needed, to keep users and their ecosystems better informed.

Industry Comparisons

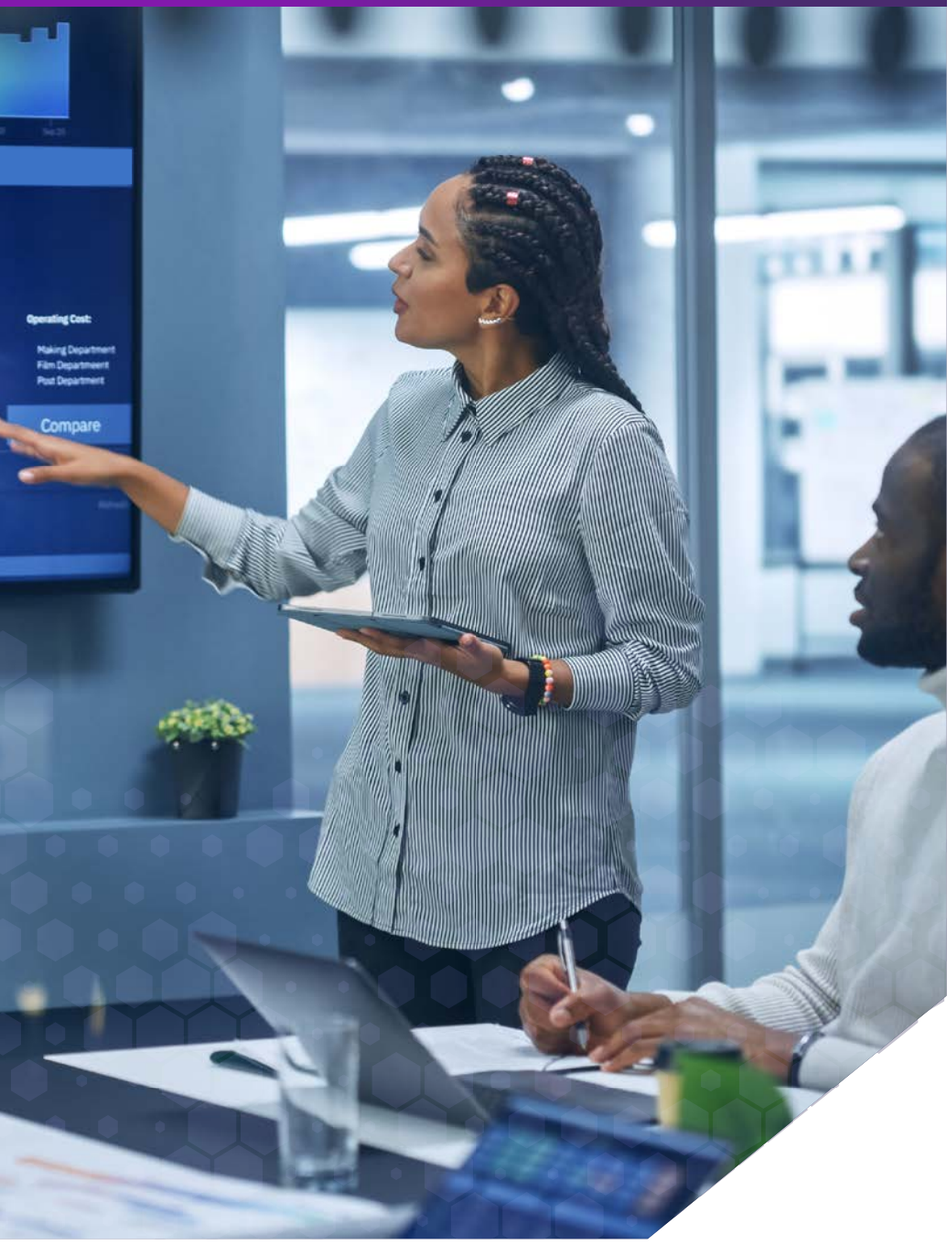
The calibration and scoring processes described above are applied globally to all organizations on the platform. This approach ensures a large statistical "mass" for reliably measuring and benchmarking the security posture of more than 12 million organizations.

Each scored organization is assigned an industry tag to facilitate comparisons within and across industries. The total and factor scores of individual companies may be easily benchmarked against others within the same industry, either at a point in time or to examine trends over periods up to 12 months.

Global calibration and scoring also enables comparisons of overall security posture of different industry sectors, which is useful for cyber insurance underwriting and cyber risk assessment at sovereign and national levels.

Industry Categories

- Construction
- Education
- Energy
- Entertainment
- Financial Services
- Food
- Government
- Healthcare
- Hospitality
- Information
- Services
- Legal
- Manufacturing
- Non-profit
- Pharmaceutical
- Retail
- Technology
- Telecommunications
- Transportation

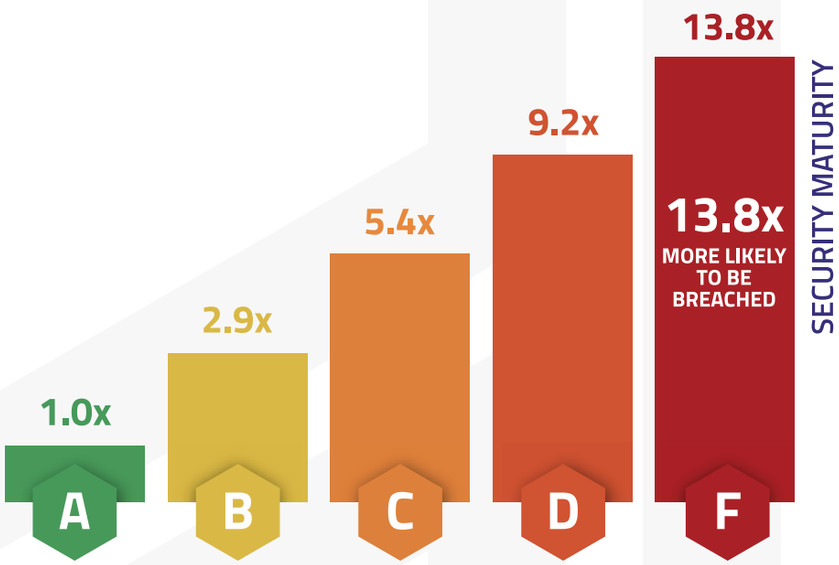


Collaboration with End Users

SecurityScorecard maintains a collaborative relationship with its users to improve awareness of cyber risk and to report accurate findings.

Users are provided with a Score Planner tool on the platform which enables them to interactively develop a remediation plan to improve their score. The tool proposes a path to better scores that users may customize according to their preferences.

In addition, users may dispute findings on their scorecard, due, for example, to compensating controls or attribution error, by submitting a refute online along with appropriate evidence. SecurityScorecard reviews each submitted refute and associated supporting evidence and, if warranted, corrects and updates the scorecard. A refute is accepted or denied within 48-hours on average. If accepted, the scorecard is updated between 48-72 hours.



Validation

SecurityScorecard's scoring algorithm has successfully passed rigorous internal verification and validation testing.

Verification testing is an engineering process to determine whether the algorithm's outputs conform to the inputs. The algorithm is subjected to a battery of statistical tests including edge cases to verify its accuracy and stability.

Validation testing determines whether the scoring algorithm satisfies its intended use as a cybersecurity risk assessment tool, i.e. do poor scores correlate with a higher likelihood of an adverse event.

In the credit rating sector, lower ratings correlate with a higher probability of default. For cybersecurity ratings, lower ratings (lower scores) should correlate with a higher likelihood of data breach.

SecurityScorecard analyzed the correlation between score and breach likelihood, based on available breach data. Statistical power is limited by the amount of breach data that is publicly available. The challenge is compounded by the fact that as many as 60-89% of breaches go unreported, since not all organizations are under regulatory obligation to disclose data breaches.

Validation testing demonstrated that companies with an F rating have a 13.8x greater likelihood of incurring a data breach compared to companies with an A.

Limitations

While SecurityScorecard's cyber risk ratings can provide substantial insights into the security postures of different organizations and their trends over time, there are some inherent limitations:

- SecurityScorecard employs an "outside-in" approach, which enables external assessment of the cybersecurity posture of organizations non-intrusively, and at scale. However, it is generally not possible to detect the presence of compensating controls internal to an organization's network. In such cases, SecurityScorecard will likely report a score that is too low. However, users may correct their own scores to reflect the presence of compensating controls by submitting a refute together with supporting evidence. A refute is accepted or denied within 48-hours on average. If accepted, the scorecard is updated between 48-72 hours.
- The dynamic nature of the internet also imposes limitations. Dynamic IPs can be reassigned daily or even hourly. Communication ports can be opened and closed at different times. Changes in domain and IP ownership can occur at any point, but take time to propagate across the internet. The dynamic nature of the internet imposes a fundamental limitation on the accuracy of any process seeking to characterize its current state. Results of such efforts are necessarily probabilistic rather than deterministic. For SecurityScorecard, this means that while scores and attribution are substantially correct, they will always be subject to some errors in the form of false positives and false negatives. SecurityScorecard has developed a suite of algorithms powered by machine learning to minimize these errors and is continuously enhancing our system architecture to improve update cadences to keep attribution and scoring as current as possible.

FAQ

Q: How often are scores updated?

A: Scores are updated and refreshed daily.

Q: How often do scoring algorithm changes occur?

A: Our scoring algorithm changes every three to four years.

Q: Why do scores fluctuate?

A: Scores fluctuate marginally from a regular scoring update cadence (once a month). This enables SecurityScorecard to preserve fair cybersecurity risk ratings in a dynamic threat environment and also to introduce new issue types reflecting new risk metrics, as needed, to keep users and their ecosystems better informed. Outside of scoring updates, scoring of an organization is a purely deterministic process. It is a function of the digital footprint and the number of security issues found. If these are unchanged, then the score will also be unchanged.

Q: Does SecurityScorecard normalize the score for organizational size?

A: Larger enterprises typically have a larger attack surface than smaller companies. SecurityScorecard levels the playing field to deliver fair scores for organizations of any size using a principled size normalization scheme.

Q: How often do scoring recalibrations occur and how do I know if they will impact my score?

A: Recalibrations occur once every quarter. If your score will be impacted by an upcoming recalibration, you will see a banner on the platform four weeks prior to the recalibration date to see the impact on the score changes along with a link to our knowledge base article for more detail.

Q: I see an IP on my digital footprint that is not mine. How can I trust your attribution?

A: SecurityScorecard performs IP attribution using automated processes operating at scale, using public RIR, DNS, and SSL data as well as third party data sources. Owing to the dynamic nature of the internet, in which IPs can be reassigned to different organizations by the day or even by the hour, IP attribution has a fundamentally probabilistic character and cannot be error-free. A team of independent pentest experts audited a random sample of SecurityScorecard scorecards to objectively determine the accuracy of SecurityScorecard IP and domain attribution. They found the attribution process to have an accuracy of 95%. Accuracy was 94% for positively attributing IP addresses, and 100% for DNS records.

Q: Are factor scores not used to calculate the overall score?

A: Factor scores represent the health of each of the factors based on the issue types tied to those factors. The overall score will be calculated by the issue types weights, since factors themselves will not have any weights.

Q: How are factor scores calculated?

A: Factor scores are calculated based on the issue types that are part of those factors. Each issue type has a weight, based on their severity, which contributes to the factor score.

Q: How much is the weight of each factor and how are factor weights determined?

A: There are no longer factor weights with the new scoring algorithm, overall scores are a direct representation of issue types. The factors will continue to have factor scores, but will not have factor weights.

About SecurityScorecard

Funded by world-class investors including Evolution Equity Partners, Silver Lake Waterman, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings with more than 12 million companies continuously rated.

Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 30,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight. SecurityScorecard is the first cybersecurity ratings company to offer digital forensics and incident response services, providing a 360-degree approach to security prevention and response for its worldwide customer and partner base.

SecurityScorecard continues to make the world a safer place by transforming the way companies understand, improve and communicate cybersecurity risk to their boards, employees and vendors. Every organization has the universal right to their trusted and transparent **Instant SecurityScorecard** rating. For more information, visit **securityscorecard.com** or connect with us on **LinkedIn**.

GET YOUR SCORE

Want to receive an email with your company's current score, please visit instant.securityscorecard.com.

Get Started

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.com