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	Breach Risk	Threat Level	Recommendation	Frequency	Age Out
Active CVE Exploitation Attempted	IP Reputation	LOW	LOW	Investigate the IP listed in the Findings table below. Then perform an incident response management process.	Varies*	15
Adware Installation	IP Reputation	LOW	MEDIUM	Investigate the devices associated with the IP addresses listed, checking for evidence of adware installations.	Varies*	30
Adware Installation Trail	IP Reputation	LOW	INFO	Investigate the devices associated with the IP addresses listed, checking for evidence of adware installations.	Varies*	365
Age exposed	Information Leak	INFO	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	HIGH	Investigate the alleged activity to determine if it can be substantiated and remediate as necessary.	Varies*	30
Apache Cassandra Service Observed	Network Security	MEDIUM	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.	Daily**	45
Apache CouchDB Service Observed	Network Security	MEDIUM	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.	Daily**	45
Apple AirPort Device Detected	Network Security	LOW	INFO	Place the wireless administrative portal behind a firewall.	Daily**	45
Attack Detected	IP Reputation	LOW	MEDIUM	Investigate the devices associated with the IP addresses listed, checking for evidence of malware infections.	Varies*	30
Attempted Information Leak	Information Leak	LOW	INFO	Investigate the IP listed in the Findings table below. Then perform an incident response management process.	Varies*	15
Browser logs contain debug messages	Application Security	LOW	INFO	Follow best practices to keep sensitive information out of browser logs.	Varies*	15
CDN Used	Network Security	LOW	INFO	Identification of a CDN could be useful information to your customers and partners, and there is no recommended action.	Varies*	45
Certificate Is Expired	Network Security	LOW	MEDIUM	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.	Daily**	45
Certificate Is Revoked	Network Security	HIGH	HIGH	If the service is not in use, decommission it. Otherwise, contact the CA and arrange issuance of a new certificate.	Daily**	45
Certificate Is Self-Signed	Network Security	LOW	MEDIUM	If the service is not in use, decommission it. Otherwise, contact the CA and arrange issuance of a new certificate.	Daily**	45
Certificate key is smaller than recommended size	Application Security	LOW	INFO	Migrate to larger keys.	Varies*	15
Certificate Lifetime Is Longer Than Best Practices	Network Security	LOW	LOW	If the service is not in use, decommission it. Otherwise, contact the CA and arrange issuance of a new certificate.	Daily**	45
Certificate Signed With Weak Algorithm	Network Security	LOW	MEDIUM	If the service is not in use, decommission it. Otherwise, contact the CA and arrange issuance of a new certificate.	Varies*	45
Certificate Without Revocation Control	Network Security	LOW	LOW	If the service is not in use, decommission it. Otherwise, contact the CA and arrange issuance of a new certificate.	Daily**	45
Cloud Provider Service Used	Network Security	INFO	INFO	Identification of a cloud provider service could be useful information to your customers and partners, and there is no recommended action.	Daily**	45

Issue Type	Factor	Breach Risk	Threat Level	Recommendation	Frequency	Age Out
Cobalt Strike C2 Detected	IP Reputation	INFO	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	INFO	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.	Daily**	45
Content Security Policy (CSP) Missing	Application Security	LOW	MEDIUM	Enable CSP headers via your web server configuration.	Daily**	45
Content Security Policy Contains 'unsafe-*' Directive	Application Security	LOW	INFO	• 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='	Daily**	45
Content Security Policy Contains Broad Directives	Application Security	LOW	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.	Daily**	45
Credentials at Risk for Up to 120 days	Information Leak	INFO	INFO	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. See additional recommendations in the MITRE ATT&CK Mitigations site.	Varies*	120
Credentials at Risk For Up to Two Years	Information Leak	INFO	INFO	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. See additional recommendations in the MITRE ATT&CK Mitigations site.	Varies*	730
Critical-Severity CVSS v3.0 Content Management System Vulnerability in Last Observation	Application Security	LOW	HIGH	Regularly update CMS software, plugins, and themes to patch known vulnerabilities. Implement strong authentication methods such as multi-factor authentication. Configure strict access controls and permissions to limit user privileges. Regularly perform security audits and scans to identify and address potential vulnerabilities. Backup website data regularly to ensure quick recovery in case of a security incident.	Varies*	45

Issue Type	Factor	Breach Risk	Threat Level	Recommendation	Frequency	Age Out
Critical-Severity CVSS v3.0 Service Vulnerability in Last Observation	Patching Cadence	LOW	HIGH	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.	Daily**	45
Critical-Severity CVSS v3.0 Vulnerability Patching Cadence	Patching Cadence	LOW	HIGH	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.	Daily**	150
Data Leak Detected	Hacker Chatter	INFO	INFO	To resolve the potential data leak on the dark web, immediate and comprehensive action is essential. 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. Implement multi-factor authentication and strengthen access controls to minimize unauthorized access. Educate employees on cybersecurity best practices and the importance of vigilance against phishing attempts. Regularly monitor networks for unusual activity and engage a reputable cybersecurity firm for additional support. Swift, decisive action will help safeguard your company's sensitive information and restore security.	Varies*	90
DKIM Record Present	DNS Health	INFO	INFO	Continue to publish a DKIM record for your domain to authenticate outgoing emails. Move from a 'none' (monitoring) policy to 'quarantine' or 'reject' to improve security. Regularly review DMARC aggregate reports to ensure alignment of SPF and DKIM with DMARC. Train users to recognize phishing threats and handle suspicious emails cautiously. Continuously monitor and update your DKIM, SPF, and DMARC records to reflect any changes in your email infrastructure.	Varies*	15
DKIM Record Using Non-Secure Public Key Algorithm	DNS Health	INFO	INFO	Replace any DKIM public keys using algorithms other than RSA or Ed25519 with secure keys. Use RSA keys of at least 2048 bits or Ed25519 keys for enhanced security. Regularly review and rotate DKIM keys to maintain cryptographic strength. Align your DKIM configuration with your DMARC policy to maximize protection. Monitor DMARC aggregate reports to detect authentication issues. Educate users about phishing threats and promote secure email practices.	Varies*	15
DNS Server Accessible	Network Security	MEDIUM	INFO	Perform a security audit of your DNS server configuration and apply any necessary controls, such as a firewall or DNS Security Extensions.	Daily**	45
Domain Advertised as Ransomware Victim	Hacker Chatter	HIGH	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	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. Implement robust monitoring systems to detect and respond to suspicious activities promptly. Ensure all software and systems are up-to-date with the latest security patches. Educate employees on security best practices and phishing prevention. Use strong, unique passwords and enable multi-factor authentication (MFA) across all accounts. Engage with cybersecurity experts to stay informed about emerging threats and leverage threat intelligence services for proactive defense. Regularly back up critical data and develop a comprehensive incident response plan.	Varies*	90
DOS Attack Attempt Detected	IP Reputation	LOW	INFO	Investigate the IP listed in the Findings table below. Then perform an incident response management process.	Varies*	15

Issue Type	Factor	Breach Risk	Threat Level	Recommendation	Frequency	Age Out
Elasticsearch Service Observed	Network Security	MEDIUM	HIGH	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.	Daily**	45
Embedded IOT Web Server Exposed	Network Security	LOW	INFO	Place the IOT web server behind a firewall.	Daily**	45
Exploit Attempt Detected	Information Leak	MEDIUM	INFO	Investigate the IP listed in the Findings table below. Then perform an incident response management process.	Varies*	15
FTP Service Observed	Network Security	MEDIUM	LOW	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.	Daily**	45
High-Risk Application Security Vulnerabilities	Cubit Score	INFO	INFO	Secure Cookie Configuration: Configure cookies with the “secure” attribute to ensure they are transmitted only over HTTPS. Apply the “HTTP only” attribute to cookies to prevent client-side script access. Enforce HTTPS for Redirects: Update all redirect chains to use HTTPS exclusively, ensuring that data remains encrypted during transit. Harden Object Storage Security: Implement robust access controls and encryption for object storage to prevent unauthorized access and data exposure. Conduct Regular Security Reviews: Perform comprehensive security assessments and code reviews to identify and remediate vulnerabilities. Continuously monitor scorecards to quickly detect and respond to the presence of this synthetic signal. Vendor Risk Management: Use the synthetic signal to filter portfolios, enabling a focused review of vendors with high-risk application security vulnerabilities and prioritizing remediation efforts. By implementing these recommendations, organizations can mitigate the compounded risks associated with high-risk application security vulnerabilities and better protect their assets against potential exploitation.	Varies*	1
High-Severity Content Management System vulnerabilities identified	Application Security	MEDIUM	HIGH	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.	Varies*	45
High-Severity CVE Patching Analyzed	Patching Cadence	INFO	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.	Daily**	1
High-Severity CVEs Patching Cadence	Patching Cadence	LOW	HIGH	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.	Daily**	120
High-Severity CVSS v3.0 Content Management System Vulnerability in Last Observation	Application Security	LOW	HIGH	Regularly update CMS software, plugins, and themes to patch known vulnerabilities. Implement strong authentication methods such as multi-factor authentication. Configure strict access controls and permissions to limit user privileges. Regularly perform security audits and scans to identify and address potential vulnerabilities. Backup website data regularly to ensure quick recovery in case of a security incident.	Varies*	45
High-Severity CVSS v3.0 Service Vulnerability in Last Observation	Patching Cadence	LOW	HIGH	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.	Daily**	45

Issue Type	Factor	Breach Risk	Threat Level	Recommendation	Frequency	Age Out
High-Severity CVSS v3.0 Vulnerability Patching Cadence	Patching Cadence	LOW	HIGH	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.	Daily**	120
High-Severity Vulnerability in Last Observation	Patching Cadence	MEDIUM	HIGH	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.	Daily**	45
HTTP Proxy Service Detected	Network Security	MEDIUM	INFO	Verify whether the HTTP proxy service has a legitimate use. Otherwise, remove it from your network.	Daily**	45
IMAP Service Observed	Network Security	MEDIUM	INFO	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.	Daily**	45
Industrial Control System Device Accessible	Network Security	MEDIUM	HIGH	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.	Daily**	45
Infected by Targeted Attack	IP Reputation	INFO	INFO	Implement Endpoint Detection and Response (EDR): Deploy advanced security solutions that monitor system behavior, detect anomalies, and respond to suspicious activities in real time. Use Network Segmentation: Restrict lateral movement by isolating critical assets from less secure parts of the network. Enhance Email Security: Enable advanced filtering, sandboxing, and domain authentication protocols (SPF, DKIM, DMARC) to prevent phishing-based malware delivery. Regular Security Patching: Keep operating systems, applications, and security software updated to mitigate known vulnerabilities. Apply Least Privilege Principle: Restrict user and application permissions to minimize potential attack surfaces. Monitor for Indicators of Compromise (IoCs): Continuously analyze network traffic, system logs, and threat intelligence feeds to identify potential malware infections. Conduct Security Awareness Training: Educate users on identifying phishing emails, social engineering tactics, and suspicious links to reduce the risk of initial infection. Use Threat Intelligence Feeds: Leverage external intelligence sources to stay informed about emerging threats and targeted attack tactics.	Varies*	3
Information Stealer Detected	IP Reputation	INFO	INFO	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. Strengthen network defenses by updating firewall rules and enhancing intrusion detection systems. Conduct a comprehensive security audit to identify and rectify any vulnerabilities that were exploited. It's crucial to update all systems and software with the latest security patches. Additionally, consider implementing advanced threat detection solutions like Endpoint Detection and Response (EDR) for real-time monitoring and response.	Varies*	15
Insecure channel exposes sensitive information	Application Security	MEDIUM	INFO	Ensure that all pages in your site enforce use of SSL encryption and HTTPS protocol.	Varies*	15
Insecure HTTPS Redirect Pattern	Application Security	LOW	MEDIUM	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.	Daily**	45

Issue Type	Factor	Breach Risk	Threat Level	Recommendation	Frequency	Age Out
Insufficient DKIM Key Length	DNS Health	INFO	INFO	Upgrade your key length by generating a new DKIM key with a 2048-bit RSA key length and update the DNS record for your DKIM selector (e.g., default._domainkey). Regularly review DMARC aggregate reports to ensure alignment of SPF and DKIM with DMARC. Train users to recognize phishing threats and handle suspicious emails cautiously. Continuously monitor and update your DKIM, SPF, and DMARC records to reflect any changes in your email infrastructure.	Varies*	15
IP Camera Accessible	Network Security	MEDIUM	LOW	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,	Daily**	45
IP on blacklist due to malicious activity	IP Reputation	MEDIUM	INFO	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
Known compromised or Hostile Host	IP Reputation	MEDIUM	INFO	Investigate the IP listed in the Findings table below. Then perform an incident response management process.	Varies*	15
LDAP Server Accessible	Network Security	MEDIUM	MEDIUM	Observe security best practices for your LDAP server and apply controls, such as using TLS to encrypt sessions.	Daily**	45
LDAP Server Allows Anonymous Binding	Network Security	MEDIUM	LOW	Disable anonymous binding on your LDAP server, which is easy to do.	Daily**	45
Link redirects to insecure website	Application Security	LOW	INFO	Ensure that all of your website's link or redirect destinations are secure, or provide visitors with explicit warnings when they are not.	Varies*	15
Low-Severity Content Management System vulnerabilities identified	Application Security	MEDIUM	LOW	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.	Varies*	45
Low-Severity CVE Patching Analyzed	Patching Cadence	INFO	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.	Daily**	1
Low-Severity CVEs Patching Cadence	Patching Cadence	LOW	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.	Daily**	60
Low-Severity CVSS v3.0 Content Management System Vulnerability in Last Observation	Application Security	LOW	LOW	Regularly update CMS software, plugins, and themes to patch known vulnerabilities. Implement strong authentication methods such as multi-factor authentication. Configure strict access controls and permissions to limit user privileges. Regularly perform security audits and scans to identify and address potential vulnerabilities. Backup website data regularly to ensure quick recovery in case of a security incident.	Varies*	45

Issue Type	Factor	Breach Risk	Threat Level	Recommendation	Frequency	Age Out
Low-Severity CVSS v3.0 Service Vulnerability in Last Observation	Patching Cadence	LOW	LOW	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.	Daily**	45
Low-Severity CVSS v3.0 Vulnerability Patching Cadence	Patching Cadence	LOW	LOW	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.	Daily**	60
Low-Severity Vulnerability in Last Observation	Patching Cadence	MEDIUM	LOW	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.	Daily**	45
Malformed SPF Record	DNS Health	MEDIUM	LOW	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.	Varies*	15
Malicious botnet C2 server detected	IP Reputation	HIGH	INFO	Investigate the IP listed in the Findings table below. Then perform an incident response management process.	Varies*	15
Malicious Scan Detected	IP Reputation	HIGH	INFO	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	INFO	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	INFO	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	INFO	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 Detected	IP Reputation	HIGH	INFO	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	HIGH	Investigate the devices associated with the IP addresses listed, checking for evidence of malware infections.	Varies*	30
Malware Infection Trail	IP Reputation	LOW	INFO	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	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.	Varies*	45

Issue Type	Factor	Breach Risk	Threat Level	Recommendation	Frequency	Age Out
Medium-Severity CVE Patching Analyzed	Patching Cadence	INFO	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.	Daily**	1
Medium-Severity CVEs Patching Cadence	Patching Cadence	LOW	MEDIUM	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.	Daily**	90
Medium-Severity CVSS v3.0 Content Management System Vulnerability in Last Observation	Application Security	LOW	MEDIUM	Regularly update CMS software, plugins, and themes to patch known vulnerabilities. Implement strong authentication methods such as multi-factor authentication. Configure strict access controls and permissions to limit user privileges. Regularly perform security audits and scans to identify and address potential vulnerabilities. Backup website data regularly to ensure quick recovery in case of a security incident.	Varies*	45
Medium-Severity CVSS v3.0 Service Vulnerability in Last Observation	Patching Cadence	LOW	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.	Daily**	45
Medium-Severity CVSS v3.0 Vulnerability Patching Cadence	Patching Cadence	LOW	MEDIUM	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.	Daily**	90
Medium-Severity Vulnerability in Last Observation	Patching Cadence	MEDIUM	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.	Daily**	45
Microsoft SQL Server Service Observed	Network Security	MEDIUM	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.	Daily**	45
Minecraft Server Accessible	Network Security	MEDIUM	INFO	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.	Daily**	45
Mirai Botnet Traffic Detected	IP Reputation	MEDIUM	INFO	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
MongoDB Service Observed	Network Security	MEDIUM	HIGH	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.	Daily**	45

Issue Type	Factor	Breach Risk	Threat Level	Recommendation	Frequency	Age Out
MOVEit Service in Use (CVE-2023-34362)	Application Security	INFO	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. While MOVEit has released updates to address the vulnerability, make sure all vulnerable instances of MOVEit are removed from the public Internet. MOVEit should be behind technologies that provide access to only those who need it via tools such as Zero Trust (e.g. access gateways secured by MFA) or simple allowlists and blocklists. If you run MOVEit within your organization, ensure that the database is running as a specific user that can only interact with MOVEit and not as a superuser with broader access. The exploit utilizes SQL injection to allow attackers to manipulate server databases and execute arbitrary code, resulting in data exfiltration. Because this breach is an SQL injection leading to remote code execution (RCE), the adversary only gains initial access to the database server and database user.	Daily**	45
MySQL Service Observed	Network Security	MEDIUM	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.	Daily**	45
NetBus Remote Access Service Detected	Network Security	INFO	INFO	Restrict NetBus service to known, essential users.	Varies*	45
Network Attached Storage Device Exposed	Network Security	HIGH	INFO	Assess the business need for exposing a NAS device to the internet, and consider placing it behind a firewall.	Varies*	45
Networking Service Observed	Network Security	MEDIUM	INFO	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.	Varies*	45
Non-standard links detected: Contact information displayed	Application Security	LOW	INFO	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.	Varies*	15
Non-standard links detected: Local file path exposed	Application Security	LOW	INFO	Follow security best practices for creating URLs and impose restrictions on file URLs if possible.	Varies*	15
Non-standard links detected: Unsafe File Transfer Protocol	Application Security	MEDIUM	INFO	Use secure, encrypted protocols for transferring data.	Varies*	15
Non-standard links detected: Unsafe Telnet protocol	Application Security	INFO	INFO	Use secure, encrypted protocols for accessing computers remotely.	Varies*	15
November 2022 OpenSSL 3.X vulnerability detected	Application Security	HIGH	INFO	Note the SSL versions in the Findings table below. Update vulnerable versions to the 3.0.7 patch.	Daily**	45

Issue Type	Factor	Breach Risk	Threat Level	Recommendation	Frequency	Age Out
Open Port Discovered	Network Security	INFO	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. Implement strong authentication mechanisms such as complex passwords, two-factor authentication (2FA), or public-key authentication for RDP and SSH services. Avoid using default or weak credentials. Utilize firewalls, access control lists (ACLs), or network segmentation to control access to RDP and SSH ports. Only allow incoming connections from trusted sources or limit access to specific IP addresses or networks. Regularly update and patch the RDP and SSH services to ensure they are running the latest secure versions, minimizing the risk of known vulnerabilities being exploited. Deploy intrusion detection and prevention systems (IDPS) to monitor network traffic and detect any suspicious or malicious activity targeting RDP and SSH ports. This helps identify and mitigate potential attacks. Conduct periodic security audits to identify and address any vulnerabilities or misconfigurations associated with RDP and SSH services. Review security configurations, apply software updates, and ensure compliance with best practices. Employ network monitoring tools and establish robust logging mechanisms to track and analyze activities related to RDP and SSH ports. This enables the detection of unauthorized access attempts or unusual behavior that may indicate a security breach.	Daily**	45
OpenVPN Device Accessible	Network Security	MEDIUM	INFO	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.	Daily**	45
Oracle Database Server Accessible	Network Security	MEDIUM	HIGH	Move the Oracle database onto a VPN or behind a firewall, and only allow dependent applications to access it.	Daily**	45
Outdated Operating System Observed	Endpoint Security	HIGH	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.	Varies*	30
Outdated Web Browser Observed	Endpoint Security	HIGH	HIGH	Update the web browsers in question. Enable automatic updates if available from your web browser vendor and permitted in your environment.	Varies*	30
POP3 Service Observed	Network Security	MEDIUM	INFO	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.	Daily**	45
Possible Initial Access by Threat Actor	Cubit Score	INFO	INFO	Immediate Audit and Remediation: Review all remote access services to determine if they are necessary. Disable any remote access service (RDP, VNC, Telnet) that is not essential to reduce the overall exposure. Strengthen Authentication: Implement multi-factor authentication (MFA) on all remote access points. Enforce strong password policies that require complexity and regular updates. Enhance Monitoring and Logging: Deploy continuous monitoring tools to detect unusual access patterns and brute force attempts. Regularly analyze logs for signs of unauthorized access or suspicious activity. Patch Management and Configuration Hardening: Ensure that all remote access services are kept up to date with the latest security patches. Harden the configuration settings for these services to eliminate common vulnerabilities. Network Segmentation and Access Control: Segment the network to isolate remote access services from critical systems. Use firewalls and access control lists (ACLs) to restrict remote access to trusted IP addresses only. Implementing these recommendations will help reduce the risk associated with the Possible Initial Access by Threat Actor signal and lower the potential for initial breaches and subsequent lateral movement within the enterprise network.	Varies*	1

Issue Type	Factor	Breach Risk	Threat Level	Recommendation	Frequency	Age Out
Possible Typosquat Domains Detected	Social Engineering	INFO	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. Encourage users to install browser extensions that block typosquatting domains, educate them on the risks, and use cybersecurity software to detect threats. Have an incident response plan in place and keep your strategies up to date, as typosquatting tactics can change over time. These steps can help protect your brand and users from the risks of typosquatting.	Varies*	90
PostgreSQL Service Observed	Network Security	MEDIUM	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.	Daily**	45
Potential Ninja Forms Vulnerability Detected	Application Security	INFO	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.	Daily**	45
Potential vulnerability detected	Application Security	INFO	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.	Varies*	20
Potentially Exposed Cisco Web UI	Application Security	INFO	INFO	To mitigate the risk associated with these vulnerabilities, users should take the following steps: Check if the web UI feature is enabled on their Cisco IOS XE Software system by using the command show running-config | include ip http server|secure|active in the CLI. 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. In this case, further action is required. Disable the HTTP Server feature if it is not needed by using the appropriate commands to turn it off. Ensure that the configuration does not contain ip http active-session-modules none (for HTTP) or ip http secure-active-session-modules none (for HTTPS) to prevent exploitation over these protocols. Regularly monitor Cisco's advisory updates for additional releases and fixes related to these vulnerabilities.	Daily**	45
Potentially Vulnerable Application (PVA) Installation	IP Reputation	HIGH	INFO	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	INFO	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
Potentially Vulnerable Cisco RV320/RV325 Router	Network Security	INFO	INFO	Because the vendor no longer provides support or patches for these devices, SecurityScorecard recommends that organizations replace them immediately.	Daily**	45
Potentially Vulnerable Citrix NetScaler Service Detected	Application Security	INFO	INFO	Check the version numbers of NetScaler versions in this domain and immediately apply the latest patch to vulnerable versions: - NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.13 - NetScaler ADC and NetScaler Gateway 13.0 before 13.0-91.13 - NetScaler ADC 13.1-FIPS before 13.1-37.159 - NetScaler ADC 12.1-FIPS before 12.1-55.297 - NetScaler ADC 12.1-NDcPP before 12.1-55.297	Daily**	45
Potentially Vulnerable Ivanti Connect Secure and Ivanti Policy Secure Gateways (CVE-2023-46805)	Application Security	INFO	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.	Daily**	45

Issue Type	Factor	Breach Risk	Threat Level	Recommendation	Frequency	Age Out
Potentially Vulnerable Ivanti Connect Secure or Ivanti Policy Secure (CVE-2024-21887)	Application Security	INFO	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.	Daily**	45
Potentially Vulnerable Ivanti Sentry Device Detected	Application Security	INFO	INFO	Immediately apply the latest security patch for Ivanti Sentry, and use firewall rules to restrict administrative portal access to trusted IPs.	Daily**	45
Potentially Vulnerable RocketMQ (CVE-2023-33246)	Application Security	INFO	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. These updated versions include necessary security enhancements that rectify the permission verification issues and protocol handling vulnerabilities. By upgrading to these versions, users can significantly mitigate the risk of remote command execution attacks. Additionally, it is advisable for administrators to review and limit the exposure of RocketMQ components to the extranet. Implementing network level controls and robust authentication mechanisms can further enhance the security of the RocketMQ deployment.	Daily**	45
Potentially Vulnerable RocketMQ (CVE-2023-37582)	Application Security	INFO	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. These updated versions include necessary security enhancements that rectify the permission verification issues and protocol handling vulnerabilities. By upgrading to these versions, users can significantly mitigate the risk of remote command execution attacks. Additionally, it is advisable for administrators to review and limit the exposure of RocketMQ components to the extranet. Implementing network level controls and robust authentication mechanisms can further enhance the security of the RocketMQ deployment.	Daily**	45
Potentially vulnerable to BIG-IP Configuration utility vulnerability (CVE-2023-46747)	Application Security	INFO	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. Also be sure to follow patching instructions specified on F5 security advisory https://my.f5.com/manage/s/article/K000137368.	Daily**	45
PPTP Service Accessible	Network Security	MEDIUM	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.	Daily**	45
Printer Detected	Network Security	MEDIUM	INFO	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).	Daily**	45
Product Potentially Impacted by CVE-2022-41040 & CVE-2022-41082	Network Security	LOW	INFO	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.	Daily**	45

Issue Type	Factor	Breach Risk	Threat Level	Recommendation	Frequency	Age Out
Product Potentially Impacted by PowerShell Remoting RCE	Network Security	LOW	INFO	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.	Daily**	45
Product Running Vulnerable Log4j Version	Network Security	HIGH	INFO	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.	Daily**	45
Products Susceptible To Ransomware Exploits Exposed	IP Reputation	LOW	MEDIUM	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.	Daily**	45
Pulse Connect Secure VPN Product Observed	Network Security	MEDIUM	INFO	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.	Daily**	45
Ransomware Infection Detected	IP Reputation	HIGH	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	INFO	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	HIGH	Enforce strong authentication methods, such as multi-factor authentication (MFA), to verify user identities before granting remote access. Implement encryption protocols, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to secure data transmitted over remote access connections. Use virtual private networks (VPNs) to establish secure and encrypted connections for remote access sessions, especially when accessing sensitive data or systems over untrusted networks. Implement robust access controls and limit remote access privileges only to authorized users and resources necessary for their roles. Regularly update and patch remote access solutions and software to address known vulnerabilities and enhance security posture. Monitor remote access activities closely through logging and auditing mechanisms to detect and promptly respond to suspicious or unauthorized access attempts.	Varies*	1
RDP Service Observed	Network Security	MEDIUM	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	Daily**	45
Redirect Chain Contains HTTP	Application Security	HIGH	MEDIUM	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.	Daily**	45
Redis Service Observed	Network Security	MEDIUM	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.	Daily**	45

Issue Type	Factor	Breach Risk	Threat Level	Recommendation	Frequency	Age Out
Remote Access Service Observed	Network Security	LOW	MEDIUM	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.	Daily**	45
rsync Service Observed	Network Security	MEDIUM	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.	Daily**	45
Server certificate issued by country on denylist	Application Security	LOW	INFO	Audit the site for any certificates issued by CAs in countries on denylists. Replace such certificates with those issued by CAs in reputable nations.	Varies*	15
Server error detected	Application Security	LOW	INFO	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.	Varies*	15
Server with Expired Certificate Contacted	Application Security	LOW	INFO	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.	Varies*	15
Session Cookie Missing 'HttpOnly' Attribute	Application Security	HIGH	LOW	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.	Varies*	15
Session Cookie Missing 'Secure' Attribute	Application Security	HIGH	LOW	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.	Daily**	15
Site does not enforce HTTPS	Application Security	LOW	HIGH	Any site served to a user (possibly at the end of a redirect chain) should be served over HTTPS.	Daily**	15
Site Does Not Use Best Practices Against Embedding of Malicious Content	Application Security	LOW	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/'	Daily**	45
Site emits visible browser logs	Application Security	LOW	INFO	Prevent emission of browser logs in the developers console.	Varies*	15
Site fails to load page components	Application Security	LOW	INFO	Maintain a regular audit cycle for website code, replace bad code, and enforce secure coding standards.	Varies*	15
Site links to insecure websites	Application Security	LOW	INFO	Avoid providing links to insecure websites whenever possible.	Varies*	15
Site may use WebSockets to send user data	Application Security	LOW	INFO	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	Varies*	15
Site receives data over Websockets	Application Security	LOW	INFO	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.	Varies*	15
Site requests data over insecure channel	Application Security	LOW	INFO	Ensure that all web pages and all content they contain is delivered over a SSL channel with HTTPS protocol.	Varies*	15
SMB Service Observed	Network Security	MEDIUM	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.	Daily**	45

Issue Type	Factor	Breach Risk	Threat Level	Recommendation	Frequency	Age Out
SMTP Server on Unusual Port	IP Reputation	MEDIUM	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.	Daily**	45
SOAP Server Accessible	Network Security	MEDIUM	INFO	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.	Daily**	45
SOCKS Proxy Service Detected	Network Security	MEDIUM	INFO	Assess whether your use of a SOCKS proxy has a legitimate business purpose. If not, consider making it inaccessible to the internet.	Daily**	45
SPF Record Contains a Softfail without DMARC	DNS Health	MEDIUM	LOW	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.	Varies*	15
SPF Record Found Ineffective	DNS Health	MEDIUM	LOW	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.	Varies*	15
SPF Record Missing	DNS Health	MEDIUM	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.	Varies*	15
SQL Payload Using Tor proxy Detected	Network Security	INFO	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. These measures collectively minimize the risk of SQL injection attacks and safeguard critical data and applications.	Varies*	90
SSH Software Supports Vulnerable Protocol	Network Security	MEDIUM	HIGH	Configure the SSH service to support only SSH protocol version 2 or higher. Upgrade the SSH service software to the latest version of software.	Daily**	55
SSH Supports Weak Cipher	Network Security	MEDIUM	MEDIUM	Configure the SSH server to disable Arc four and CBC ciphers.	Daily**	55
SSH Supports Weak MAC	Network Security	MEDIUM	MEDIUM	Configure the SSH server to disable the use of MD5.	Daily**	55
SSL/TLS Service Supports Weak Protocol	Network Security	HIGH	HIGH	Disable the protocols listed in the evidence column of the measurement.	Daily**	45
Telephony/VoIP Device Accessible	Network Security	INFO	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.	Daily**	45
Telnet Service Observed	Network Security	MEDIUM	LOW	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.	Daily**	45
TLS Certificate Status Request ("OCSP Stapling") Detected	Network Security	INFO	POSITIVE	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.	Daily**	45
TLS Service Supports Weak Cipher Suite	Network Security	LOW	MEDIUM	Disable the cipher suites listed in the evidence column of the measurement.	Daily**	45

***There is no regular scanning frequency for this issue type. We collect data from multiple sources when it is available.**
****Daily scanning for paid customers and their followed vendors. Weekly (approx.) for remaining scorecards.**

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 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:

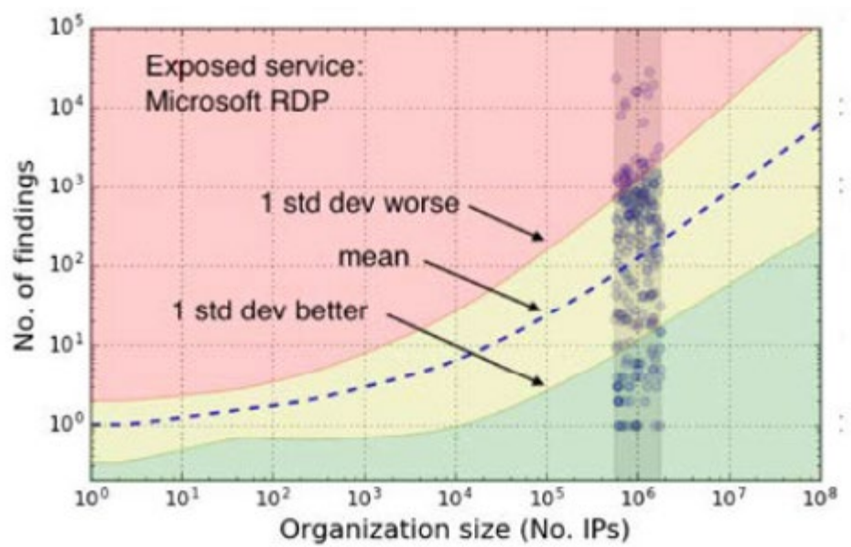
- Richter scale for measuring earthquakes over more than 9 order of magnitude.
- Decibel scale for measuring sound amplitude over 12 orders of magnitude.
- pH scale for measuring chemical acidity over 14 orders of magnitude.

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

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

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

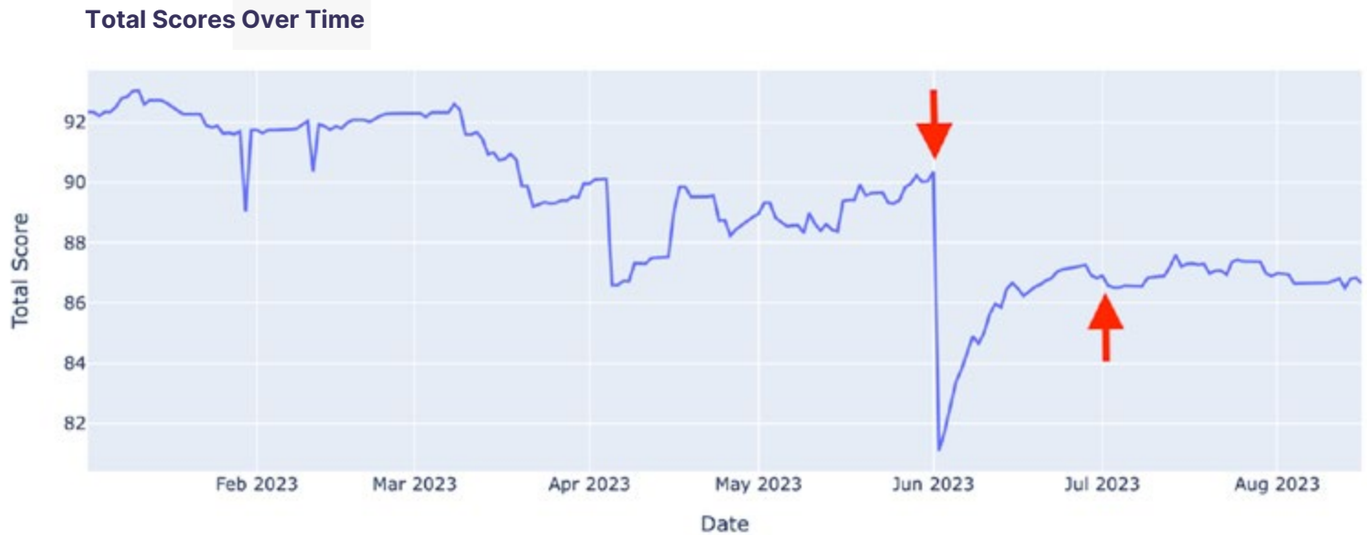
After calculating the raw total score, we scale it based on the expected value of issue finding counts. We want to fairly score an organization by comparing it to others with similar Digital Footprint sizes.

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

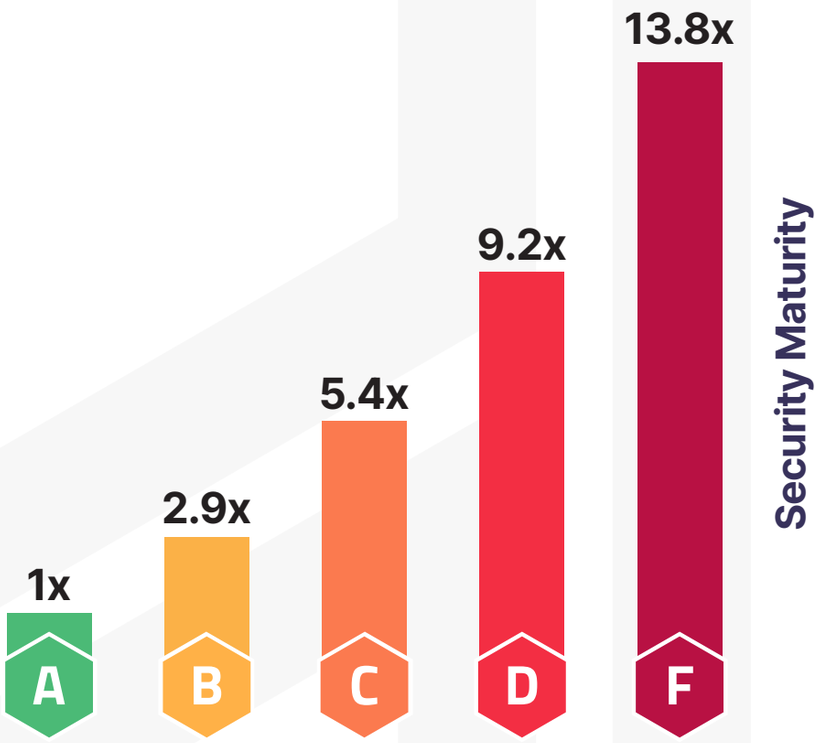
- Construction
- Education
- Energy
- Entertainment
- Financial Services
- Food
- Government
- Healthcare
- Hospitality
- Information Services
- Legal
- Manufacturing
- Non-profit
- Pharmaceutical
- Retail
- Technology
- Telecommunications
- Transportation

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