SecurityScorecard

A Deep Dive in Scoring Methodology

By Bob Sohval, PhD, VP Data Science

SecurityScorecard.com
info@securityscorecard.com

111 W 33rd Street, 11th Floor
New York, NY 10001
1.800.682.1707

Table of Contents

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.

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 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.

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

What do Scores Mean?

SecurityScorecard scores provide insights and a detailed analysis of the security posture of an organization. The Total Score, which consists of an easy to understand letter grade A (100) to F (0) and quickly conveys an overall assessment of security hygiene. The Total Score is a weighted average of 10 Factor Scores, which provide useful insights into detected vulnerabilities grouped into different categories.

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 organizations with a poor score (C or below) are approximately 5x more likely to incur a data breach compared to those with good scores.

Factor	Weight	Description
Network Security	Medium	Detecting insecure network settings
DNS Health	Medium	Detecting DNS insecure configurations and vulnerabilities
Patching Cadence	Medium	Out of date company assets which may contain vulnerabilities or risks
Endpoint Security	Medium	Measuring security level of employee workstations
IP Reputation	High	Detecting suspicious activity, such as malware or spam, within your company network
Application Security	Medium	Detecting common website application vulnerabilities
Cubit Score	Low	Proprietary algorithms checking for implementation of common security best practices
Hacker Chatter	Low	Monitoring hacker sites for chatter about your company
Information Leak	Medium	Potentially confidential company information which may have been inadvertently leaked
Social Engineering	Low	Measuring company awareness to a social engineering or phishing attackz

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.

Each factor has a numerical weight, which reflects the severity or risk that the factor contributes to the overall cybersecurity posture. The magnitude of the weights are presented categorically in the table displayed here.

An organization's Total Score is calculated as the weighted average of its Factor Scores.

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

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

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. 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 below.

Issue Type	Factor	Severity / Weight	Recommendation	Update Frequency	Age Out
High Severity Content Management System (CMS) Vulnerabilities Found in the Last Observation	Application Security	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.	Monthly	45 days
Site does not enforce HTTPS	Application Security	High	Any site served to a user (possibly at the end of a redirect chain) should be served over HTTPS.	Weekly	15 days
Insecure HTTPS Redirect Pattern	Application Security	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.example.com or https://example.com. This redirect should be done before redirecting to any other domain or subdomain.	Weekly	15 days
Medium Severity Content Management System Vulnerabilities Found in the Last Observation	Application Security	Medium	To resolve this issue, review the version of the CMS and plug-ins in use and ensure that they are updated. Put in place a system of constant CMS patching and reviews of new vulnerabilities from the security center of the CMS developer site.	Monthly	45 days
Redirect Chain Contains HTTP	Application Security	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.	Weekly	15 days
Website Does Not Implement HSTS Best Practices	Application Security	Medium	Every web application (and any URLs traversed to arrive at the website via redirects) should set the HSTS header to remain in effect for at least 12 months (31536000 seconds). It is also recommended to set the 'includeSubDomains' directive so that requests to subdomains are also automatically upgraded to HTTPS. An acceptable HSTS header would declare: Strict-Transport-Security: max-age=31536000; includeSubDomains;	Weekly	15 days
Website does not implement X-Frame-Options Best Practices	Application Security	Medium	Add one of the following headers, using the 'DENY' or 'Allow-FROM' directive, to responses from this website: 'X-Frame-Options: DENY', 'X-Frame-Options: Allow-FROM https://example.com/'	Weekly	15 days
Website does not implement X-XSS-Protection Best Practices	Application Security	Medium	Add the following header to responses from this website: 'X-XSS-Protection: 1; mode=block'	Weekly	15 days

Cookie Missing 'Secure' Attribute	Application Security	Low	Change the default 'Secure' attribute from FALSE to TRUE to ensure cookies are sent only via HTTPS. The 'Secure' attribute should be set on each cookie to prevent cookies from being observed by malicious actors. Implement the 'Secure' attribute when using the Set-Cookie parameter during authenticated sessions.	Weekly	7 days
Low Severity Content Management System Vulnerabilities Found in the Last Observation	Application Security	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.	Weekly	45 days
Session Cookie Missing 'HttpOnly' Attribute	Application Security	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.	Weekly	7 days
Website does not implement X-Content-Type-Options Best Practices	Application Security	Low	Add the following header to responses from this website: 'X-Content-Type-Options: nosniff'	Weekly	15 days
Content Security Policy Contains Broad Directives	Application Security	Informational	Explicitly specify trusted sources for your script-src and object-src policies.	Weekly	15 days
Content Security Policy Contains Unsafe Directives	Application Security	Informational	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.	Weekly	15 days
Content Security Policy Missing	Application Security	Informational	Enable CSP headers via your webserver configuration. A full listing of directives can be found at https://content-security-policy.com/	Weekly	15 days
Object Storage Bucket with Risky ACL	Application Security	Informational	Remove the affected grants, since they allow entities not associated with your organization to change the bucket.	Weekly	15 days
Unsafe implementation of Sub-Resource Integrity	Application Security	Informational	Please ensure that all website elements (i.e. <script> and <link>) loading Javascript and CSS stylesheets hosted with external organizations contain the 'integrity' directive with a valid checksum. Example: <script src="https://example.com/example-framework.js" integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC" crossorigin="anonymous"></script>	Weekly	15 days
Website Hosted on Object Storage	Application Security	Informational	Confirm that the bucket in use is carefully configured, and that the use of an object storage service was intentional. We have no way to detect the bucket that is being used for hosting the website, and cannot evaluate the ACL either.	Weekly	15 days
Website References Object Storage	Application Security	Informational	Confirm that the bucket in use is carefully configured, and that the use of an object storage service was intentional. Since we have the bucket's name as part of the reference, we attempt to evaluate the bucket's ACL and generate another issue (Object Service Bucket with Risky ACL) if it is not secured.	Weekly	15 days
Site Uses HSTS Preloading	Application Security	Positive	For the below sites served over HTTPS, ensure that the Strict-Transport-Security header is set with the following flags: * includeSubdomains * preload * max-age of at least 31536000 seconds (1 year) Once those steps have been completed, the site may be submitted to https://hstspreload.org for inclusion in Google's preload list. Non-Google Browsers that support HSTS preloading also use this list	Daily	15 days
Web Application Firewall (WAF) Detected	Application Security	Positive	Companies should consider implementing a web application firewall that can protect against common web vulnerabilities, such as SQL Injection and cross-site scripting (XSS). Many hosting providers offer WAF capabilities as well.	Weekly	15 days

Open DNS Resolver Detected	DNS Health	High	According to the Open Resolver Project, the following DNS configurations should be implemented to avoid becoming a target for abuse. Recursive servers should be limited only to enterprise or customer IP ranges, and not accept connections from IP addresses outside these ranges. For specific instructions about secure BIND and Microsoft nameservers configurations, it is recommended to examine the resources on the Team CYMRU Website. For users that make use of BIND, the TCP-ANY patch can be deployed to prevent the Open Resolver issue. Authoritative servers should not make recursion available, however they still may be used in an attack. Authoritative DNS servers should be configured to make use of DNS RRL [Response Rate Limiting]. Note about CPE devices: CPE (Customer Premises Equipment) devices should not listen for DNS connections on any WAN interface, including NETWORK and BROADCAST addresses.	Multiple times per day	45 days
SPF Record Missing	DNS Health	Medium	Create a valid Sender Policy Framework (SPF) record. Ensure the configuration of the SPF DNS record to verify syntax and MTA servers. Test the configuration to make sure it's 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 or not the email is authentic.	Every 3 days	15 days
Malformed SPF Record	DNS Health	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.openspf.org/Tools.	Every 3 days	15 days
SPF Record Contains Wildcard	DNS Health	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.	Every 3 days	15 days
SPF Record Contains a Softfail	DNS Health	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.	Every 3 days	15 days
Valid DNSSEC Configuration Detected	DNS Health	Positive	The use of DNSSEC is not widely adopted. An organization should evaluate the appropriate use of DNSSEC. There are valid reasons to avoid the implementation of DNSSEC, such as potential exposure to enumeration of domain zone information However, those organizations that deploy DNSSEC correctly demonstrate mature security practice.	Every 3 days	None
Hacker Chatter Mention	Hacker Chatter	Informational	Monitor the chatter, analyze its context and source. If the chatter indicates a planned attack or identifies a method of exploitation or fraud technique that targets the company, take steps to mitigate the attack/fraud method by restricting the attack vectors being discussed by attackers.	Daily	None
Malware Events, Last Day	IP Reputation	High	Investigate the devices connected to the identified IP addresses; Check for evidence of malware infection.	Daily	1 day
Malware Events, Last 30 Days	IP Reputation	Medium	Investigate the devices connected to the identified IP addresses; Check for evidence of malware infection.	Daily	30 days
P2P Activities	IP Reputation	Medium	Institute persistent Malware protection mechanisms by using up to date AntiVirus software and ensuring all software is up to date. Monitor ALL incoming and outgoing traffic for suspicious behavior utilizing IDS solutions (snort), or WAFs (Web Application Firewall). Block and blacklist any suspicious traffic and follow up investigation of malware incidents.	Daily	30 days
Malware Events, Last Year	IP Reputation	Low	Investigate the devices connected to the identified IP addresses; Check for evidence of malware infection.	Daily	365 days
Unsolicited Commercial Email	IP Reputation	Informational	Confirm with the reporting blacklist if emails are not UCE.	Weekly	1 day

MongoDB Service Exposure Detected	Network Security	High	Implement a firewall rule to disable public access to the database. If access over the Internet is required, implement a VPN.	Monthly	45 days
SSH Software Supports Vulnerable Protocol	Network Security	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.	Monthly	55 days
SSL Certificate(s) have been revoked	Network Security	High	Generate a new Certificate Signing Request and contact the certificate authority to sign and issue a new certificate.	Monthly	45 days
Unauthenticated Elasticsearch Service Observed	Network Security	High	Implement a firewall rule to block public access to the port used by the Elasticsearch REST API. Access to the Elasticsearch REST API should require encryption and authentication by implementing TLS.	Monthly	45 days
Cassandra Database Ports Found on the Network	Network Security	Medium	Review the business necessity of the open ports listed. Close any unnecessary ports, and ensure any remaining open ports are properly patched, require authentication, and configured for security best practices. Ensure that all versions of services running on services that are Internet facing are updated to the latest versions. Implementing an IP whitelist for access to open ports would restrict unauthorized access attempts from successfully connecting via the public Internet.	Monthly	45 days
CouchDB Database Ports Found on the Network	Network Security	Medium	Review the business necessity of the open ports listed. Close any unnecessary ports, and ensure any remaining open ports are properly patched, require authentication, and configured for security best practices. Ensure that all versions of services running on services that are Internet facing are updated to the latest versions. Implementing an IP whitelist for access to open ports would restrict unauthorized access attempts from successfully connecting via the public Internet.	Monthly	45 days
Microsoft SQL Server Ports Found on the Network	Network Security	Medium	Review the business necessity of the open ports listed. Close any unnecessary ports, and ensure any remaining open ports are properly patched, require authentication, and configured for security best practices. Ensure that all versions of services running on services that are Internet facing are updated to the latest versions. Implementing an IP whitelist for access to open ports would restrict unauthorized access attempts from successfully connecting via the public Internet.	Monthly	45 days
MySQL Database Ports Found on the Network	Network Security	Medium	Review the business necessity of the open ports listed. Close any unnecessary ports, and ensure any remaining open ports are properly patched, require authentication, and configured for security best practices. Ensure that all versions of services running on services that are Internet facing are updated to the latest versions. Implementing an IP whitelist for access to open ports would restrict unauthorized access attempts from successfully connecting via the public Internet.	Monthly	45 days
Open IMAP Ports Found on the Network	Network Security	Medium	Review the business necessity of the open ports listed. Close any unnecessary ports, and ensure any remaining open ports are properly patched, require authentication, and configured for security best practices. Ensure that all versions of services running on services that are Internet facing are updated to the latest versions. Implementing an IP whitelist for access to open ports would restrict unauthorized access attempts from successfully connecting via the public Internet.	Monthly	45 days
Open MS-Services / SMB Ports Found on the Network	Network Security	Medium	Review the business necessity of the open ports listed. Close any unnecessary ports, and ensure any remaining open ports are properly patched, require authentication, and configured for security best practices. Ensure that all versions of services running on services that are Internet facing are updated to the latest versions. Implementing an IP whitelist for access to open ports would restrict unauthorized access attempts from successfully connecting via the public Internet.	Monthly	45 days

Open Remote Desktop Protocol (RDP) Ports Found on the Network	Network Security	Medium	Review the business necessity of the open ports listed. Close any unnecessary ports, and ensure any remaining open ports are properly patched, require authentication, and configured for security best practices. Ensure that all versions of services running on services that are Internet facing are updated to the latest versions. Implementing an IP whitelist for access to open ports would restrict unauthorized access attempts from successfully connecting via the public Internet.	Monthly	45 days
Open Virtual Network Computing Ports Found on the Network	Network Security	Medium	Review the business necessity of the open ports listed. Close any unnecessary ports, and ensure any remaining open ports are properly patched, require authentication, and configured for security best practices. Ensure that all versions of services running on services that are Internet facing are updated to the latest versions. Implementing an IP whitelist for access to open ports would restrict unauthorized access attempts from successfully connecting via the public Internet.	Monthly	45 days
Open rsync Ports Found on the Network	Network Security	Medium	Review the business necessity of the open ports listed. Close any unnecessary ports, and ensure any remaining open ports are properly patched, require authentication, and configured for security best practices. Ensure that all versions of services running on services that are Internet facing are updated to the latest versions. Implementing an IP whitelist for access to open ports would restrict unauthorized access attempts from successfully connecting via the public Internet.	Monthly	45 days
PostgreSQL Database Ports Found on the Network	Network Security	Medium	Review the business necessity of the open ports listed. Close any unnecessary ports, and ensure any remaining open ports are properly patched, require authentication, and configured for security best practices. Ensure that all versions of services running on services that are Internet facing are updated to the latest versions. Implementing an IP whitelist for access to open ports would restrict unauthorized access attempts from successfully connecting via the public Internet.	Monthly	45 days
Redis Database Ports Found on the Network	Network Security	Medium	Review the business necessity of the open ports listed. Close any unnecessary ports, and ensure any remaining open ports are properly patched, require authentication, and configured for security best practices. Ensure that all versions of services running on services that are Internet facing are updated to the latest versions. Implementing an IP whitelist for access to open ports would restrict unauthorized access attempts from successfully connecting via the public Internet.	Monthly	45 days
SSH Supports Weak Cipher	Network Security	Medium	Configure the SSH server to disable Arcfour and CBC ciphers.	Monthly	55 days
SSH Supports Weak MAC	Network Security	Medium	Configure the SSH server to disable the use of MD5.	Monthly	55 days
SSL Certificate Uses Weak Signature	Network Security	Medium	Contact the authority that manages your SSL Certification to ensure that you have an updated signature–such as SHA-2.	Monthly	45 days
SSL Certificate is Expired	Network Security	Medium	Generate a new Certificate Signing Request and contact the certificate authority to sign and issue a new certificate.	Monthly	45 days
SSL Certificate is Self Signed	Network Security	Medium	Based on your relationship, determine whether a self-signed certificate poses a risk. If necessary, request an SSL Certificate from a mutually trusted Certificate Authority.	Monthly	45 days
TLS Protocol Uses Weak Cipher	Network Security	Medium	It is recommended to configure the server to only support strong symmetric ciphers and to use sufficiently large public key sizes. Specifically, avoid RC4 encryption as there have been multiple vulnerabilities discovered that render it insecure. Additionally, it is recommended to use a public key size of more than 2048 bits.	Monthly	45 days

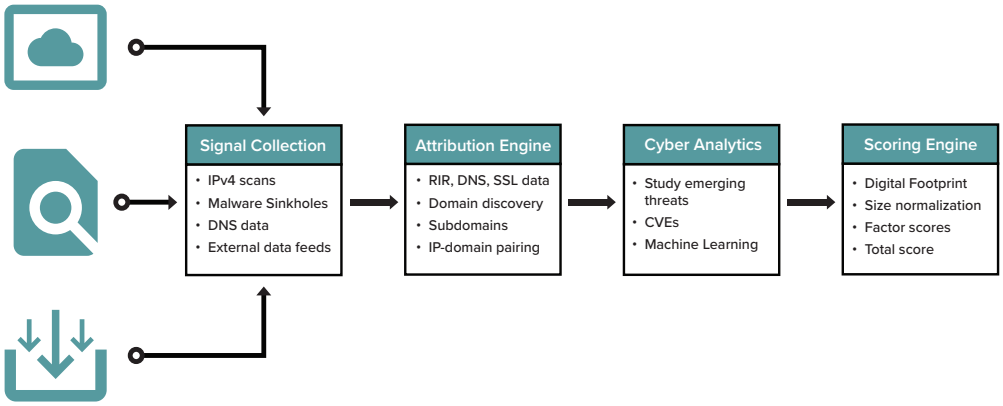
No CRL found on SSL Certificate	Network Security	Low	Contact the Certificate Authority (CA) about including a CRL for the SSL.	Monthly	45 days
Open FTP Ports Found on the Network	Network Security	Low	Review the business necessity of the open ports listed. Close any unnecessary ports, and ensure any remaining open ports are properly patched, require authentication, and configured for security best practices. Ensure that all versions of services running on services that are Internet facing are updated to the latest versions. Implementing an IP whitelist for access to open ports would restrict unauthorized access attempts from successfully connecting via the public Internet.	Monthly	45 days
Open Telnet Ports Found on the Network	Network Security	Low	Review the business necessity of the open ports listed. Close any unnecessary ports, and ensure any remaining open ports are properly patched, require authentication, and configured for security best practices. Ensure that all versions of services running on services that are Internet facing are updated to the latest versions. Implementing an IP whitelist for access to open ports would restrict unauthorized access attempts from successfully connecting via the public Internet.	Monthly	45 days
SSL Certificate Expiration is Longer Than Best Practices	Network Security	Low	Issue a new Certificate Signing Request and contact the Certificate Authority to sign the new certificate. Ensure that the expiration date is less than 39 months.	Monthly	45 days
Exposed TCP Ports Discovered	Network Security	Informational	Review the business necessity of the open ports listed. Configure any unnecessary ports to drop connection attempts, and ensure any remaining open ports are properly patched, require authentication, and are configured for security best practices. Implementing an IP whitelist for access to open ports would restrict unauthorized access attempts from successfully connecting via the public Internet.	Monthly	None
Open POP3 / Email Ports Found on the Network	Network Security	Informational	Review the business necessity of the open ports listed. Close any unnecessary ports, and ensure any remaining open ports are properly patched, require authentication, and configured for security best practices. Ensure that all versions of services running on services that are Internet facing are updated to the latest versions. Implementing an IP whitelist for access to open ports would restrict unauthorized access attempts from successfully connecting via the public Internet.	Monthly	45 days
DDoS Protection Service Detected	Network Security	Positive	Companies should consider implementing DDoS protection for any piece of digital infrastructure with high availability requirements (examples include content-serving websites for media organizations, e-commerce web portals, and SaaS platforms). DDoS protection can either be implemented in-house or can be purchased from SaaS providers (such as Cloudflare or Akamai) - the right solution depends on an individual company's needs, traffic patterns, and specific digital infrastructure.	Daily	15 days
Extended Validation Certificate Detected	Network Security	Positive	Despite being more expensive than “domain validated” certificates, Extended Validation certificates should be strongly considered by a company if the users of the company’s website(s) are at risk of Man-in-the-Middle attacks via typo-squatted domain-names (i.e. domains that look similar to the legitimate domain but redirect to a malicious site). Users of the legitimate site who are accustomed to the visual signals of an EV certificate are more likely to notice an attacker who attempts to give a malicious site a legitimate appearance (without being able to produce an EV certificate).	Monthly	45 days
TLS Certificate Status Request (OCSP Stapling) Detected	Network Security	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.	Monthly	45 days

Obsolete Browsers Detected	Endpoint Security	Medium	Upgrade all browsers to the latest stable build for your platform operating system. Many browsers include an auto-update facility which should be enabled. Also, manually validate browser security settings, and ensure configurations are set to not allow unknown or unauthorized Javascripts from running.	Daily	30 days
Obsolete Operating System Endpoint Detected	Endpoint Security	Medium	Upgrade all operating systems to the latest stable build. Many operating system vendors include an auto-update facility which should be enabled.	Daily	30 days
Multiple Browsers Detected	Endpoint Security	Informational	Verify that the use of multiple browsers and associated versions are for legitimate business use. Confirm that the endpoint policy for use of web browsers meet the risk tolerance of the organization.	Daily	None
Credentials at Risk	Information Leak	Low	Ensure employees are not using the same credentials for any corporate or 3rd-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.	Continuous	180 days
High Severity CVEs Patching Cadence	Patching Cadence	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 software and hardware in use within your enterprise, ensuring that all the latest patches are implemented as they are released.	Monthly	335 days
High Severity Exposed Vulnerabilities Found in the Last Observation	Patching Cadence	High	Update or patch software indicated. 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.	Monthly	45 days
End-of-Life Product	Patching Cadence	Medium	Assure that the product vendor has an extended support contract that includes security patches. Review the manufacturers statement about end of life guidelines for replacement products and upgrade to a new product line or manufacturer.	Monthly	45 days
End-of-Service Product	Patching Cadence	Medium	Replace or upgrade the product. Review the manufacturers statement about end of service guidelines for replacement products or contact the manufacturer. In some cases, it may be possible to negotiate a custom support plan for the EOS product.	Monthly	45 days
Medium Severity CVEs Patching Cadence	Patching Cadence	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.	Monthly	275 days
Medium Severity Exposed Vulnerabilities Found in the Last Observation	Patching Cadence	Medium	Update or patch software indicated. 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.	Monthly	45 days
Medium Severity Exposed Vulnerabilities Found in the Last Observation	Patching Cadence	Medium	Update or patch software indicated. 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.	Monthly	45 days

Low Severity CVEs Patching Cadence	Patching Cadence	Low	Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the BugTraq mailing list to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular updating schedule for all software and hardware in use within your enterprise, ensuring that all the latest patches are implemented as they are released.	Monthly	185 days
Low Severity Exposed Vulnerabilities Found in the Last Observation	Patching Cadence	Low	Update or patch software indicated. 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.	Monthly	45 days
Exposed Subdomain	Cubit Score	Low	Resolve all private subdomains using a segregated, internal DNS server. If public exposure is required for these subdomains, it is advised that the integration of either two-factor authentication or IP address whitelisting be put in place to prevent unauthorized access to the subdomains, either through exploitation or credential compromise.Implementing an IP whitelist for access to internal administrative subdomains would restrict unauthorized access attempts from successfully connecting via the public Internet.	Weekly	15 days
Possible Typosquat Domains Detected	Cubit Score	Informational	Verify that the typosquat domain does not pose a risk to the organization. If necessary, perform a domain take-down of malicious domains which may be used for phishing.	Monthly	45 days
Leaked Company Emails Open to Spear-Phishing	Social Engineering	Informational	Provide security awareness training to help educate employees about spear phishing, credential reuse, and how to properly respond to a spear phishing campaign. Additionally, such awareness training should teach employees about use of social networks and their privacy settings that they are less susceptible to spear phishing attacks.Consider the implementation of a policy about using email frameworks that cannot be derived solely by names as this makes it easy to find a person's social networking account.	Continuous	180 days

Signal Processing Workflow

Generating meaningful cybersecurity ratings consists of four distinct processing stages: Signal Collection, Attribution Engine, Cyber Analytics, and Scoring Engine.



Signal Collection

SecurityScorecard scans the entire IPv4 webspace at a regular cadence to identify vulnerable digital assets.

Additionally, SecurityScorecard monitors signals across the internet, relying on a global network of sensors that spans the Americas, Asia, and Europe. We operate one of the world's largest networks of sinkholes and honeypots to capture malware signals and further enrich our data set by leveraging commercial and open-source intelligence sources.

SecurityScorecard supplements its data collection with external feeds from approximately 40 third-party public and commercial data sources.

SecurityScorecard ingests approximately 1.5 Terabytes of data daily as part 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. Large netblocks of IPs are typically allocated statically to an organization, while smaller netblocks may be assigned dynamically by Internet Service Providers (ISP), Cloud Service Providers (CSP), and Content Delivery Networks (CDN). Notably, 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, and SSL data as well as 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.

Based on an independent assessment by security firm, the False Positive Rate for domain attribution was close to 0.

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%.

Subdomain discovery is performed using a set of publicly available data sources, including CommonCrawl and 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 near zero.

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 key 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 1.3 million organizations around the world.

Our scoring methodology is described below.

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.

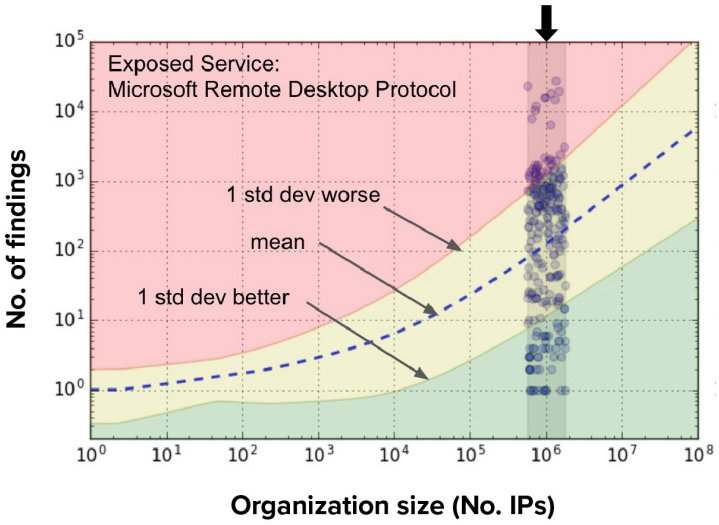
Many types of security issues scale with the size of the organization. Larger organizations typically have a larger “attack surface” compared to smaller entities. More employees mean more devices to be protected and more servers mean more chances for an exposed port which should properly sit behind a 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 orders 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 here 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 1.3 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 here, 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 1.3 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 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.

The modified z-scores are calculated and updated daily for every entity and every issue type monitored on the SecurityScorecard platform. This approach ensures inherently low score volatility. If an entity's digital footprint and issue counts are stable, then its security score will be unchanged.

Calculating Raw Factor Score

Each factor comprises issue types that are topically related, e.g. Network Security, Application Security, etc.. The weighted sum of the issue-level z-scores is used to compute a raw factor score for each scored domain:

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

where RFS_d is the raw factor score for domain d, wi is the severity-based weight for issue i, and z_{di} is the z-score for domain d and issue i. The sum is calculated over all issues i in factor f.

Note: for issues that are informational only or positive, the weight $w_i = 0$. Informational and positive issues do not contribute to the score.

Raw factor scores are converted to final factor scores using a scaling transformation to stretch the factor scores from 0 to a maximum of 100.

Calculating Total Score

Finally, the Total Score is calculated as the weighted average of the individual factor scores:

$$TS_d = \frac{\sum_f w_f \times g(FS_{df}) \times FS_{df}}{\sum_f w_f \times g(FS_{df})}$$

where TS_d is the total score for domain d, w_f is the severity-based weight of factor f, FS_{df} is the factor score for domain d and factor f, and g(·) is a non-linear weighting function which gives greater emphasis to low factor scores. The rationale is that in a security context, "a chain is only as strong as its weakest link". Giving greater weights to low factor scores helps pull down the total score when the entity has low factor scores, reflecting a degraded overall security posture.

Factor and total scores are refreshed and updated daily.

Breach Penalty

When an organization sustains a data breach, it poses a risk to other entities in its ecosystem. To reflect this risk, its score is reduced by 20% upon disclosure of a breach. The penalty decays (i.e. the score improves) exponentially with a half-life of 30 days and is set to zero after 120 days.

The score history chart above illustrates the impact of a data breach that occurred in late September 2019. The score had been hovering at approximately 80 prior to the breach. The breach penalty initially reduced the score by 20% (from about 80 to about 64) and then decayed away. The company remediated a number of vulnerabilities following the breach and eventually improved their score to 90.

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 at a regular cadence, monthly. 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 1.3 million organizations.

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

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.

Collaboration with End Users

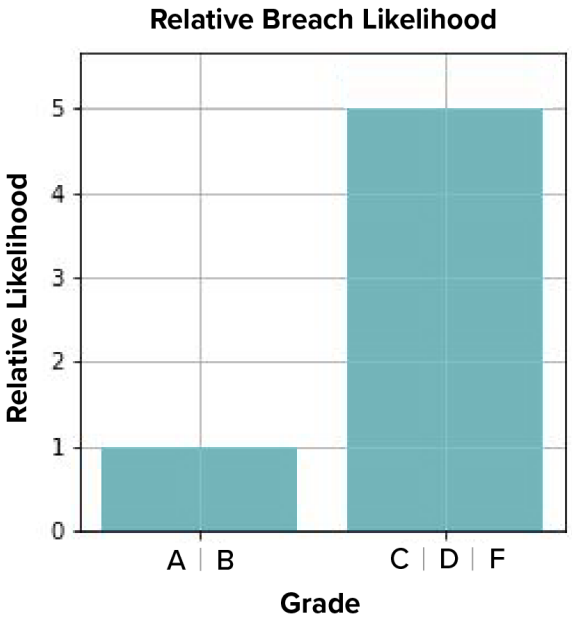
SecurityScorecard maintains a collaborative relationship with its users to improve awareness of cyber risk and to report accurate findings.

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 corrects and updates the scorecard, if warranted, within 48 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, although there is a growing movement in the international community to responsibly disclose the occurrence of data breaches.

Validation testing demonstrated that companies with a poor total score (C, D, or F) had approximately 5x greater likelihood of incurring a data breach compared to companies with a good score (A or B).

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. Refutes are processed and scores updated within 48 hours.
- The internet is dynamic. 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: What cybersecurity issues do you track?
A: SecurityScorecard currently tracks 79 cybersecurity issues, which are topically organized into 10 Factors. A list of all issues and their associated factors and severity-based weights is displayed here.

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.

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: Is a 1-2 point change in score significant? How about a 5-10 point change?
A: A 5-10 point decline in score is significant and warrants a remediation effort. By comparison, a small change in score (1-2 points) is unlikely to reflect a meaningful change in security hygiene. However, when a score reduction of 1-2 points causes a change in letter grade, for example from a B to a C, there may be a psychological impact despite the immaterial change in score.

Q: Does SecurityScorecard benchmark against industry?
A: While SecurityScorecard performs scoring globally, 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 for examining trends over periods up to 12 months.

About SecurityScorecard

SecurityScorecard is the global leader in cybersecurity ratings and the only service with over a million companies continuously rated. Founded in 2013 by security and risk experts Dr. Alex Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 1,000 organizations for enterprise risk management, third-party risk management, board reporting and cyber insurance underwriting. 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 company has the universal right to their trusted and transparent Instant SecurityScorecard Rating.

For more information, visit securityscorecard.com or connect with us on LinkedIn.

1 (800) 682-1707
info@securityscorecard.io

SecurityScorecard HQ
111 West 33rd Street
11th Floor
New York City, NY 10001