SecurityScorecard

Understand the cyber health of your ecosystem across 10 risk factor groups

Network Security

Detecting insecure network settings

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

DNS Health

Detecting DNS insecure configurations and vulnerabilities

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

Patching Cadence

Displaying out of date company assets which may contain vulnerabilities or risks

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

Endpoint Security

Measuring security level of employee workstations

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 The information gathered allows companies to identify outdated versions of these data points which can lead to client-side exploitation attacks.

IP Reputation

Detecting suspicious activity, such as malware or spam, within your company network

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

SecurityScorecard

Application Security

Detecting common website application vulnerabilities

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

Cubit Score

Checking for implementation of common security best practices through proprietary algorithms

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

Hacker Chatter

Monitoring hacker sites for chatter about your company

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

Information Leak

Providing potentially confidential company information which may have been inadvertently leaked

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

Social Engineering

Measuring company awareness to a social engineering or phishing attack

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

About SecurityScorecard

SecurityScorecard helps security professionals work collaboratively to solve mission-critical, cybersecurity issues in a transparent way. The SecurityScorecard platform provides continuous, non-intrusive security monitoring of any organization and its ecosystem.

info@securityscorecard.com
1-800-682-1707 • securityscorecard.com