Quantifying Cyberdefense with SanerNow Cyber Hygiene Score

Solution Brief

www.secpod.com

Introduction

A modern IT attack surface is made up of risks more than just vulnerabilities. From typical software vulnerabilities to other dangerous security risks like security misconfiguration and posture anomalies , IT Security teams and security admins must cater to fix them. Further, tracking the amount of vulnerability data and measure the effort taken to process and mitigate it. And it's difficult to measure attack surface and gauge the effectiveness of your security measure without a metric to quantify it.

A cyber hygiene score or a cyber risk score is the missing piece that allows IT Security teams to quantify the attack surface and measure the impact of security measures you take. From planning your vulnerability mitigation efforts and prioritizing remediation to making informed decisions and continuously improving cyber hygiene, a cyber hygiene score is a critical tool that should be present in every IT Security team's arsenal.

Benefits of a Cyber Hygiene Score

Quantify your Cybersecurity Posture

Measure your organization's security posture with a data-driven mathematical scoring model to understand how exposed your organization is to potential cyber-attacks. With a clear picture, you will get insights into what cyber risks are exposing your network and take effective actions at the right time.

Gauge the Effectiveness of your Cybersecurity Measures

With a cyber hygiene score, you can see how effective your cyber security measures, like patching and other mitigation strategies, are in real-time. Further, you can evaluate, visualize and monitor changes in the cyber hygiene score to pinpoint particularly dangerous risks in your network as well.

Track & Achieve Compliance Goals

A continuously improving cyber hygiene score can demonstrate your commitment to your organization's safety. Implementing compliance benchmarks when clubbed with a cyber hygiene score, allows for easier enforcement. Additionally, the hygiene score helps identify non-compliant devices in your network, further allowing you to achieve compliance continuously and easily in your network.

Proactively Plan Mitigation Strategies

A cyber hygiene score provides IT and Security teams with data on how effective the mitigation strategies are. And the impact on the cyber hygiene scores allows you to understand the impact of these measures and helps proactively make informed decisions on which strategies work and improve your risk management.

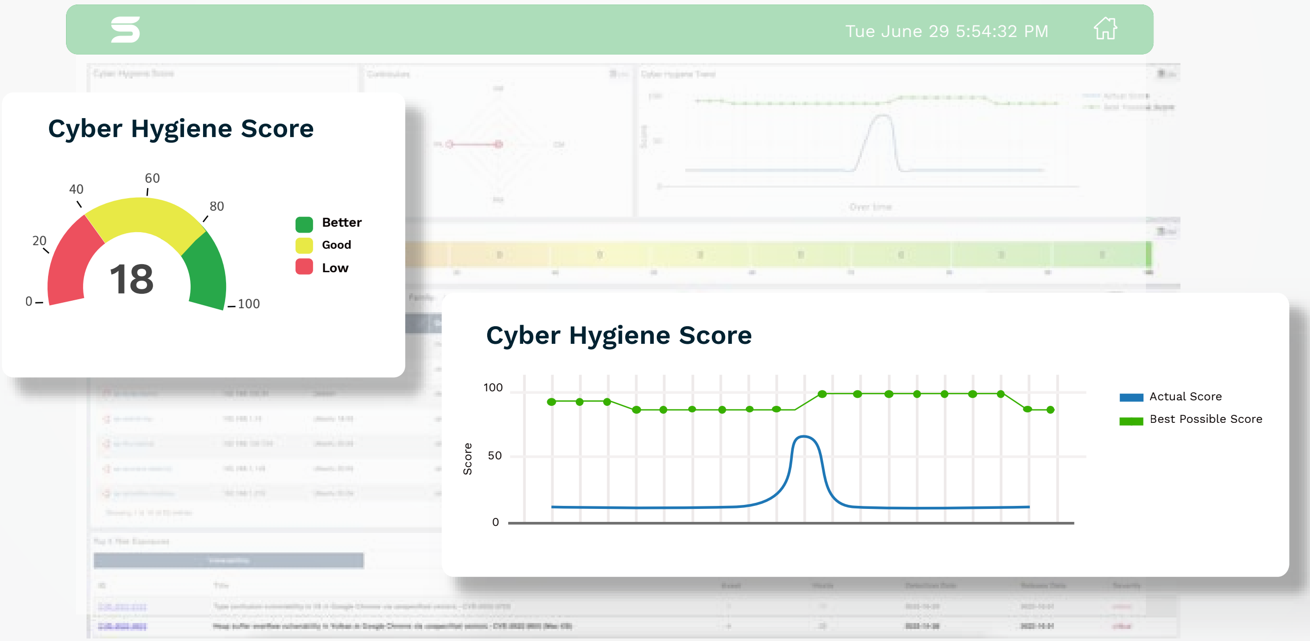
Simplify Risk Communication with Stakeholders

A singular standard cyber hygiene score is easier to communicate to stakeholders and members of management when compared to lengthy reports filled with technical jargon. Alongside simplified risk communication, it also acts as a measure of how secure your organization is and demonstrates cyber readiness.

An Overview of SanerNow Cyber Hygiene Score

SanerNow Cyber Hygiene Score(CHS) is a data-driven, intelligent mathematical scoring model that quantifies your organization's attack surface by individually evaluating the cyber hygiene of each device and computing it as a whole.

With SanerNow's natively built vulnerability scanner that detects software vulnerabilities, misconfigurations, posture anomalies, asset exposures, and missing patches, CHS is a holistic and comprehensive scoring model that leaves no stone unturned to ensure every possible inch of attack surface is calculated



Understanding SanerNow Cyber Hygiene Score

Cyber hygiene Scores

To compute the Cyber hygiene score, SanerNow uses an intelligent, statistically computed data-driven model to compute scores for individual devices and the organization as a whole

Device-Specific Cyber Hygiene Scores

Raw Score

Quantification of the total attack surface of your organization. A raw score is a real number that can range from zero to infinity and is a sum total of the weightage of CCE, CVE, Posture Anomalies, and missing patches.
The default weightage for each of the four types of security risks is 25% and can be customized accordingly.

Note: Higher the Raw score, the less secure the device is.

Global Score

The Global Score is a normalized Raw Score ranging from 0 to 100 and measures how secure a device is. While the Raw Score quantifies the 'risk,' the Global Score measures the 'secureness' of a device.

Note: Higher the Global Score, the more secure the device is.

Local Score

The Local Score is another normalized score that determines where a particular device stands in an organization. Every device in the organization is assigned a score from 0 to 100, where 100 is assigned to the most secure device and 0 to the least.

Final Score

The Final Score of a device is the weighted average of the Local and Global Scores of a device that ranges from 0 to 100. By default, the weightage of Global and Local Scores are 80% and 20%, respectively. The Final Score can be divided as

Scoring Scale

Low	Good	Better
0-40	41-80	81-100

Account-Specific Cyber Hygiene Score

An organization might have different accounts which handle different segments or departments, and Saner-Now calculates Cyber Hygiene Score based on how the organization is segmented. Accordingly, every account will have its own CHS dashboard to provide insights on the attack surface of the devices in the account.

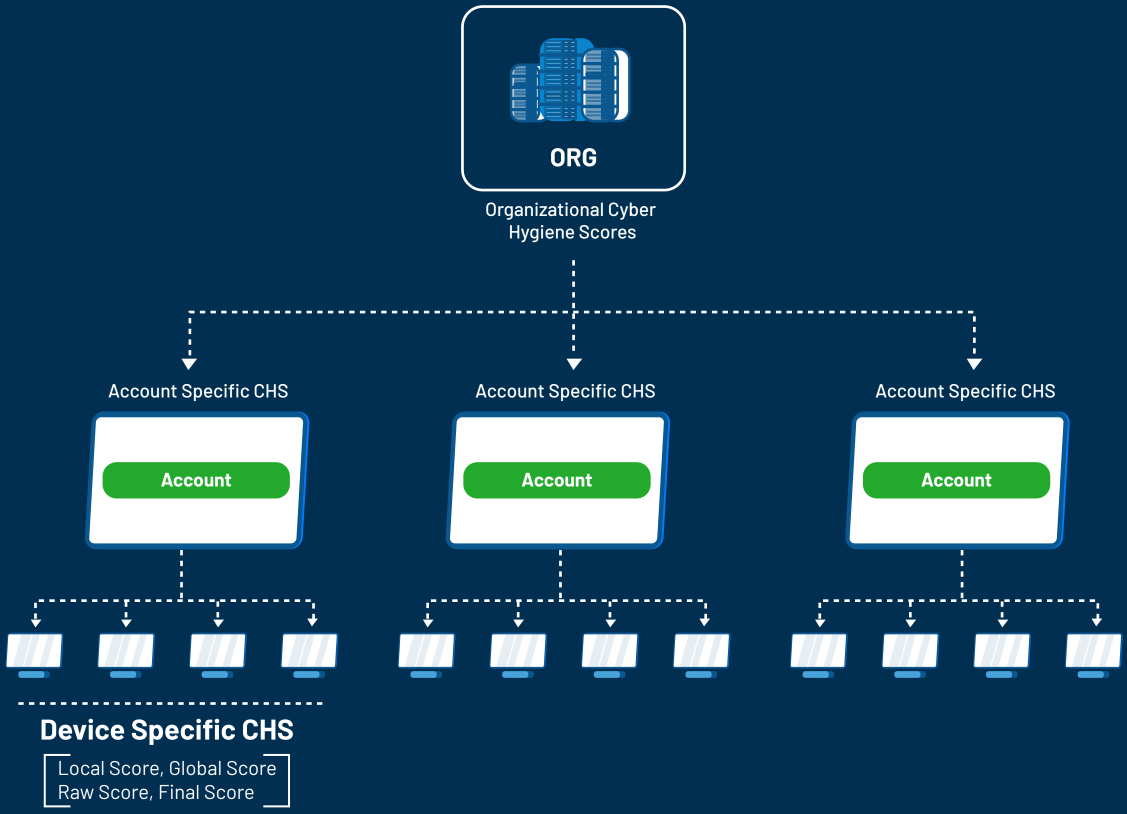
Based on the CHS of the individual devices in an account, Cyber Hygiene Score is calculated by taking its weighted average for the particular account.

The Cyber Hygiene Trend for the account will also be calculated accordingly.

Organizational Cyber Hygiene Score

The organization is a combination of multiple accounts, and the Cyber Hygiene Score for the organization is calculated by taking the weighted average of all the cyber hygiene scores of the accounts to which the user is currently logged in and has access.

The Organizational Dashboard provides insights into the attack surface of the organization and also predicts the CHS score with Cyber Hygiene Trend. Further, it also provides insights into high-risk devices, top-risk exposures, and more.

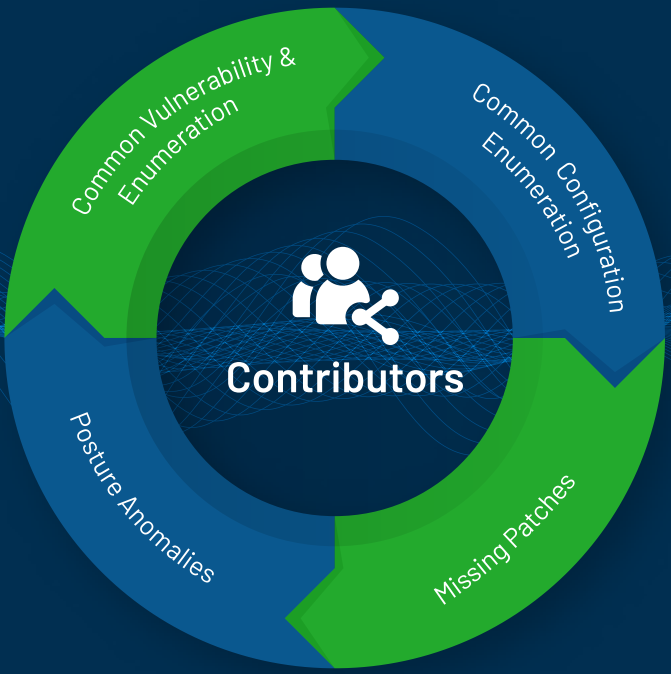


Contributors

The Cyber Hygiene Score computes the effect of security risks that make up your organization’s attack surface. The main contributors to CHS are

- Common Vulnerability & Enumeration
- Common Configuration Enumeration
- Missing Patches
- Posture Anomalies

By default, each of the four main contributors is given an equal weightage of 25%.


Common Vulnerability & Enumeration
Common Configuration Enumeration
Contributors
Missing Patches
Posture Anomalies

Cyber Hygiene Trend

By tracking the Cyber Hygiene Score over a period of time and plotting a graph, you get a visual representation of the change in CHS over time. This representation allows you to picture the impact of your mitigation strategies and the effect of security risks and make informed decisions.

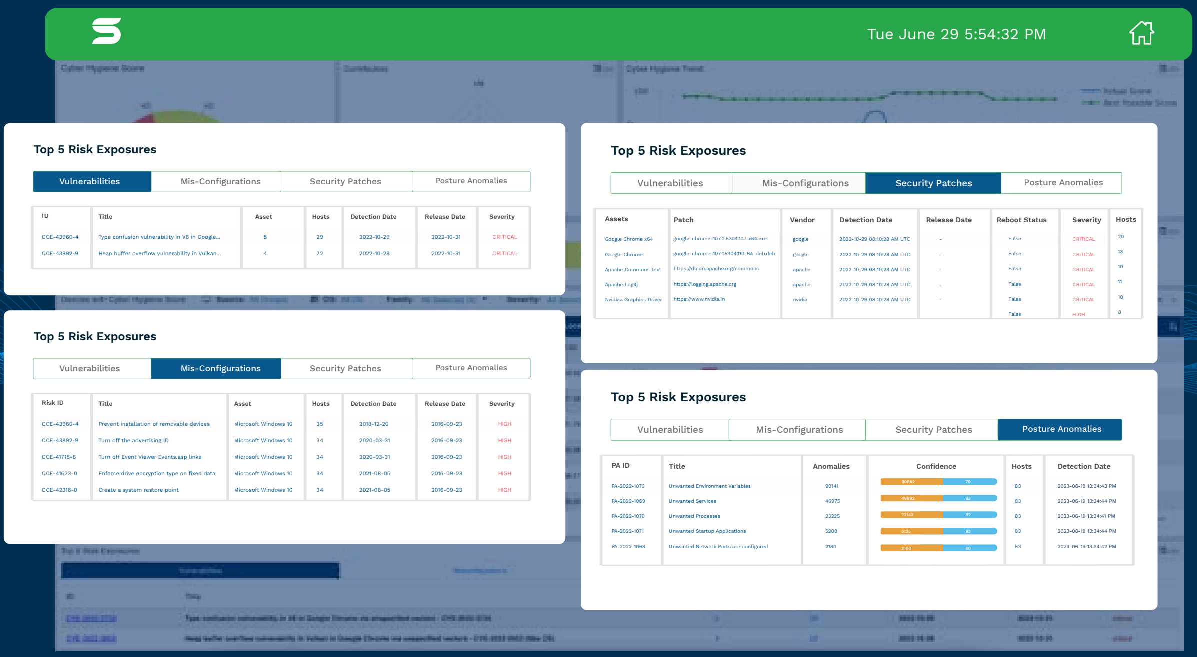
Taking a step further, SanerNow Cyber Hygiene Trend predicts the CHS score for the next day, assuming you take all the required remediation actions. The difference in the predicted and actual scores will demonstrate the impact of your remediation actions

Frequency Distribution of Devices

In the Cyber Hygiene Dashboard, you also get a frequency distribution of the cyber hygiene scores of all the devices in the account/organization. SanerNow automatically generates a frequency distribution that will allow you to instantly quantify devices based on a range of scores.

Top 5 Risk Exposures

In the Cyber Hygiene Dashboard, you will get an overview of the top 5 risk exposures categorized based on the type of risk like CVE, CCE, Posture Anomaly, or Missing Patches. This list allows you to prioritize remediation efforts and focus on mitigating risks in your network.



Top 5 Risk Exposures

ID	Title	Asset	Hosts	Detection Date	Release Date	Severity
CCE-43960-4	Type confusion vulnerability in V8 in Google...	5	29	2022-10-29	2022-10-31	CRITICAL
CCE-43892-9	Heap buffer overflow vulnerability in Vulkan...	4	22	2022-10-28	2022-10-31	CRITICAL

Top 5 Risk Exposures

Risk ID	Title	Asset	Hosts	Detection Date	Release Date	Severity
CCE-43960-4	Prevent installation of removable devices	Microsoft Windows 10	35	2018-12-20	2016-09-23	HIGH
CCE-43892-9	Turn off the advertising ID	Microsoft Windows 10	34	2020-03-31	2016-09-23	HIGH
CCE-41718-8	Turn off Event Viewer Events.asp links	Microsoft Windows 10	34	2020-03-31	2016-09-23	HIGH
CCE-41623-0	Enforce drive encryption type on fixed data	Microsoft Windows 10	34	2021-08-05	2016-09-23	HIGH
CCE-42316-0	Create a system restore point	Microsoft Windows 10	34	2021-08-05	2016-09-23	HIGH

Top 5 Risk Exposures

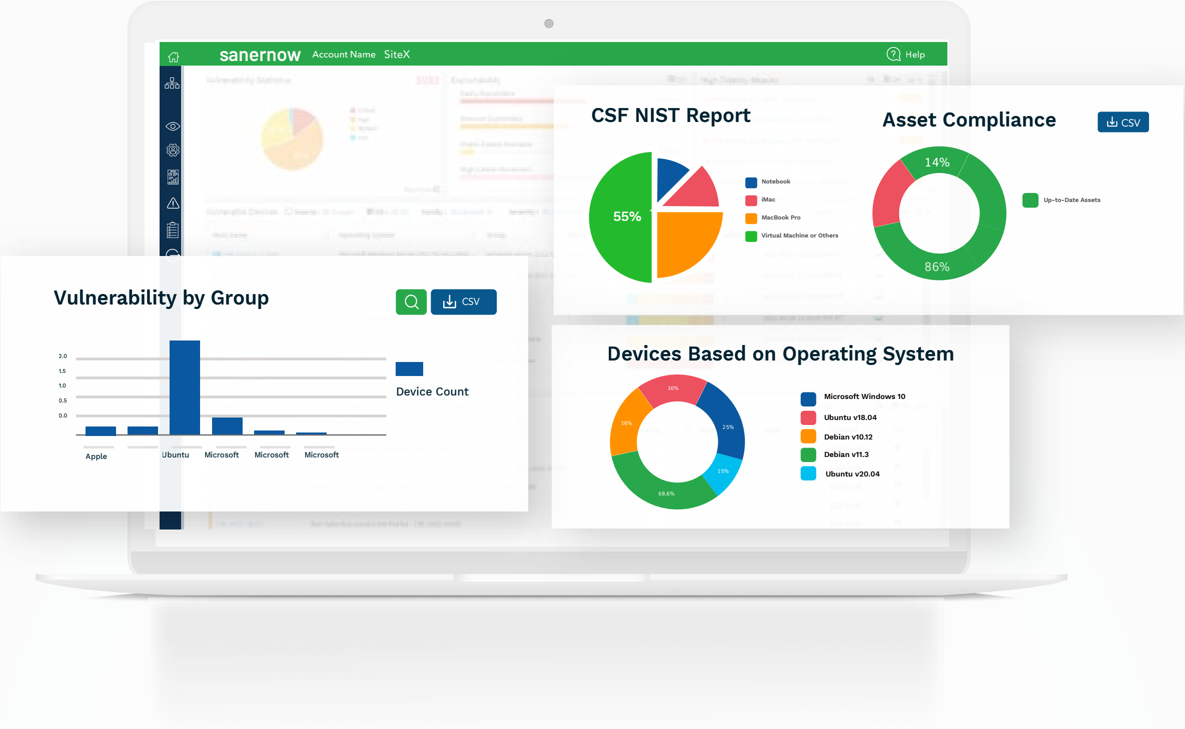
Assets	Patch	Vendor	Detection Date	Release Date	Reboot Status	Severity	Hosts
Google Chrome x64	google-chrome-107.0.5304.107-x64.exe	google	2022-10-29 08:10:28 AM UTC	-	False	CRITICAL	20
Google Chrome	google-chrome-107.05304.110-64-deb.deb	google	2022-10-29 08:10:28 AM UTC	-	False	CRITICAL	13
Apache Commons Text	https://dlcdn.apache.org/commons	apache	2022-10-29 08:10:28 AM UTC	-	False	CRITICAL	10
Apache Log4j	https://logging.apache.org	apache	2022-10-29 08:10:28 AM UTC	-	False	CRITICAL	11
Nvidiaa Graphics Driver	https://www.nvidia.in	nvidia	2022-10-29 08:10:28 AM UTC	-	False	CRITICAL	10
					False	HIGH	8

Top 5 Risk Exposures

PA ID	Title	Anomalies	Confidence	Hosts	Detection Date
PA-2022-1073	Unwanted Environment Variables	90141	90062 79	83	2023-06-19 13:34:43 PM
PA-2022-1069	Unwanted Services	46975	46892 83	83	2023-06-19 13:34:44 PM
PA-2022-1070	Unwanted Processes	23225	23143 82	83	2023-06-19 13:34:41 PM
PA-2022-1071	Unwanted Startup Applications	5208	5125 83	83	2023-06-19 13:34:44 PM
PA-2022-1068	Unwanted Network Ports are configured	2180	2100 80	83	2023-06-19 13:34:42 PM

Customizing Cyber Hygiene Score based on Security Risks / Modules Purchased

SanerNow Cyber Hygiene Score can also be customized based on the modules you have purchased or the type of security risks. You can configure the weightage of each of the four security risks according to how much you would like it to be. This customization helps you categorize and prioritize which security risk you want to provide more importance for.



Schedule a Demo

CONTACT US

info@secpod.com / www.secpod.com

About SecPod

SecPod is a cyber security technology company. We prevent cyberattacks. We do everything to prevent attacks on the computing environment. Our product helps implement cyber hygiene measures, so attackers have a tough time piercing through.

Our SanerNow CyberHygiene platform provides continuous visibility to the computing environment, identifies vulnerabilities and misconfigurations, mitigates loopholes to eliminate attack surface, and helps automate these routines. Our product philosophy is offering simplicity and automation to make the job of security administrators slightly better.