Saner's Continuous, Automated, and Scalable Architecture for Continuous Vulnerability and Exposure Management (CVEM)

www.secpod.com

Overview

Vulnerability Management is the most crucial Cyberattack Prevention process. With attacks rising rapidly & constant changes in the IT security landscape, the age-old vulnerability management process is no longer effective. The traditional vulnerability management tools still rely on siloed tools doesn't have sufficient visibility to IT infrastructure, lack integrated remediation capabilities, & often overlook other security risks beyond Common Vulnerability Enumeration (CVE) or software vulnerabilities. IT Security Teams need a Continuous Vulnerability & Exposure Management solution to reduce attack surfaces to a larger extent and keep attacks at bay.

Challenges with Siloed Solutions

Traditional vulnerability and exposure management relies on multiple tools from gaining visibility over the IT infrastructure, identifying vulnerabilities, misconfigurations, and other risk exposures, and mitigating them with relevant remediation controls. Interrelating results from various siloed solutions is often confusing, making it hard for security teams to respond and gain control over the risk exposure. They also create delays between different stages of a vulnerability management program, leading to huge security gaps in the organization.

Pitfalls of Traditional Vulnerability Management

Slow and ineffective processes

As the horizon of security risk exposures and vulnerabilities expands, conventional scanners lack the intelligence to detect them. Many conventional vulnerability scanners take hours or sometimes weeks to discover the commonly known vulnerabilities or exposures. The time taken to discover all risks, including vulnerabilities, misconfigurations, security patches, and features updates, will be even longer with these traditional scanners. This process tends to consume a huge bandwidth while scanning network devices. Some vulnerability scanners even produce false-positive results. Thus, ineffective vulnerability scanning is a major let down for the whole vulnerability and exposure management process.

Unable to keep up with the volume of vulnerabilities

Tens of thousands of vulnerabilities are discovered every year, and the volume of vulnerabilities released in the NVD database is colossal. The year 2021 ended with a total of 20,061 vulnerabilities, 9.3% more than the previous year. Security teams face numerous challenges in keeping up with the increased volume of vulnerabilities. Compounding the problem further, there are other types of security risks such as misconfigurations, deviations in security controls, and posture anomalies, that are as critical as vulnerabilities and must be managed as a part of cyberattack prevention efforts.

Not Managing vulnerabilities beyond CVEs

More than 40% of vulnerabilities do not have a CVE identifier assigned, or CVE information is not up-to-date in the commonly available databases. Exposures, posture anomalies, misconfigurations and other security risks are often ignored. Many vulnerability and exposure management products focus on vulnerabilities with such CVEs, which leaves organizations using them under huge risks.

Lack of Deeper Insights into the IT infrastructure

IT security teams do not have deeper visibility over the IT infrastructure. Traditional tools typically provide limited view to hardware and software details with insufficient actionable insights. As a result, IT security teams overlook the most obvious attack vectors that can increase the attack surface and lead to massive security breaches.

Poor clarity on what to remediate first

According to a study by **ESG**, 43% of security administrators have challenges prioritizing vulnerabilities for remediation. After detecting a huge pile of vulnerabilities and risks, it is critical to identify and remediate the high-risk ones to minimize attacks. Traditional vulnerability management tools lack the right technique to highlight vulnerabilities and risks, merely depending on severity score and not considering other significant factors.

Delay in patching and remediating vulnerabilities & exposures

With new vulnerabilities and exposures being discovered every passing day, security teams have difficulty keeping a tab on patching them. Many conventional programs rely on a different tool to patch the vulnerabilities and face hiccups in correlating the vulnerability data to execute the patching process. Delay in patching increases vulnerability exposure, opening gates for numerous cyberattacks. Most of the attacks use a long-standing known vulnerability that has been present but ignored in the organization for over a year.

Lack of remediation controls beyond patching

A software update is not often a single remediation measure to fix vulnerabilities and other security risk exposures. As the horizon of vulnerabilities and security risks expand, numerous remediation controls are needed to fix different types of vulnerabilities. Traditional vulnerability and exposure management tools lack these controls and restrict security teams from going beyond patching to fix other risk exposures.

Unable to align vulnerability management goals with security compliance

Popular industry compliance standards like HIPAA, PCI, NIST, and ISO propose numerous system hardening controls and vulnerability management measures to tighten security. Many conventional vulnerability and exposure management tools in the market are not equipped with sufficient features to align with these security benchmarks. Thus, security teams rely on different tools to enforce security compliance, making it a challenging goal to achieve.

Key Requirements for Effective Vulnerability or Exposure Management:

Capabilities to Manage Vulnerabilities and Beyond

CVEs, exposures and other known software vulnerabilities comprise only a part of the security risks in the IT infrastructure. Numerous risks exist, including software vulnerabilities, poorly configured settings, IT asset exposures, security control deviations, missing patches, and security posture anomalies. Advanced Continuous Vulnerability and Exposure Management must look at these risks as parallel to a vulnerability and provide capabilities in the form of a one-point solution to mitigate all such risks.

Integrated Remediation

Most of the time, vulnerabilities prevail in large numbers in the IT network due to lack of effective remediation tools. Advanced Continuous Vvulnerability and Exposure Mmanagement offers tight integration with patching and other necessary remediation mechanisms to mitigate vulnerabilities and security risks.

Deeper and Holistic Visibility to IT Infrastructure

IT security teams generally have only basic visibility over the hardware and software assets with insufficient actionable insights. Advanced Continuous vulnerability and exposure management provides holistic and deeper visibility to IT and enable you to discover and eliminate the anomalies that threatens IT security.

Unified Solution

The primary goal of Advanced Continuous Vulnerability and Exposure Management is to reduce the complexities and chaos faced in siloed tools. Advanced Continuous vulnerability and Exposure management needs a unified and centralized solution catering to different needs of managing attack surfaces.

The key architecture requirements of the unified solution include:

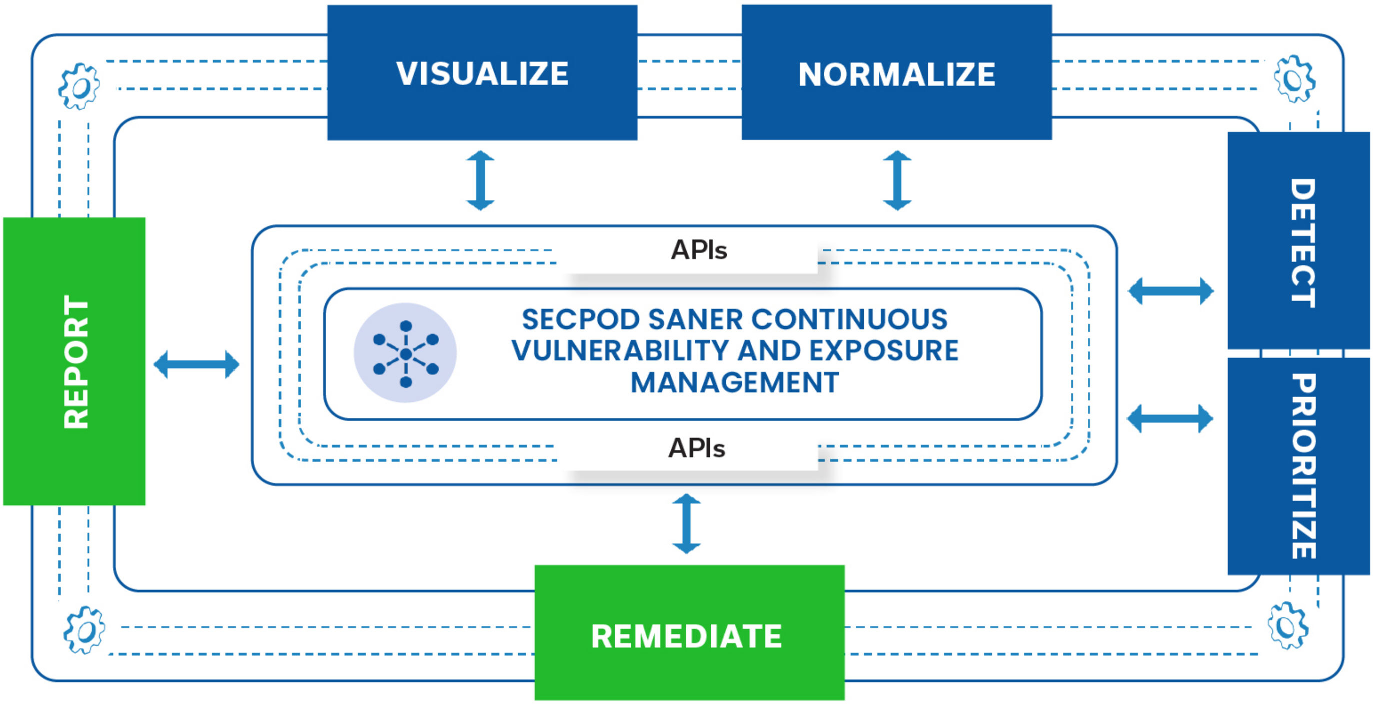
- Integration of various capabilities with machine readable dataset
- Probes to talk to any IT environment
- Query & Respond in real-time
- Scalable & High-performance datastore
- Analytics & correlation

Saner's Continuous, Automated, and Advanced Vulnerability and Exposure Management Architecture

Saner CVEM Advanced Continuous Vulnerability and Exposure Management is a unified, continuous and automated cyberattack surface management or security risk and compliance posture management program that helps effectively prevent cyberattacks. It incorporates the Weakness Perspective to revolutionize Vulnerability/-Exposure Management and IT Security as a whole.

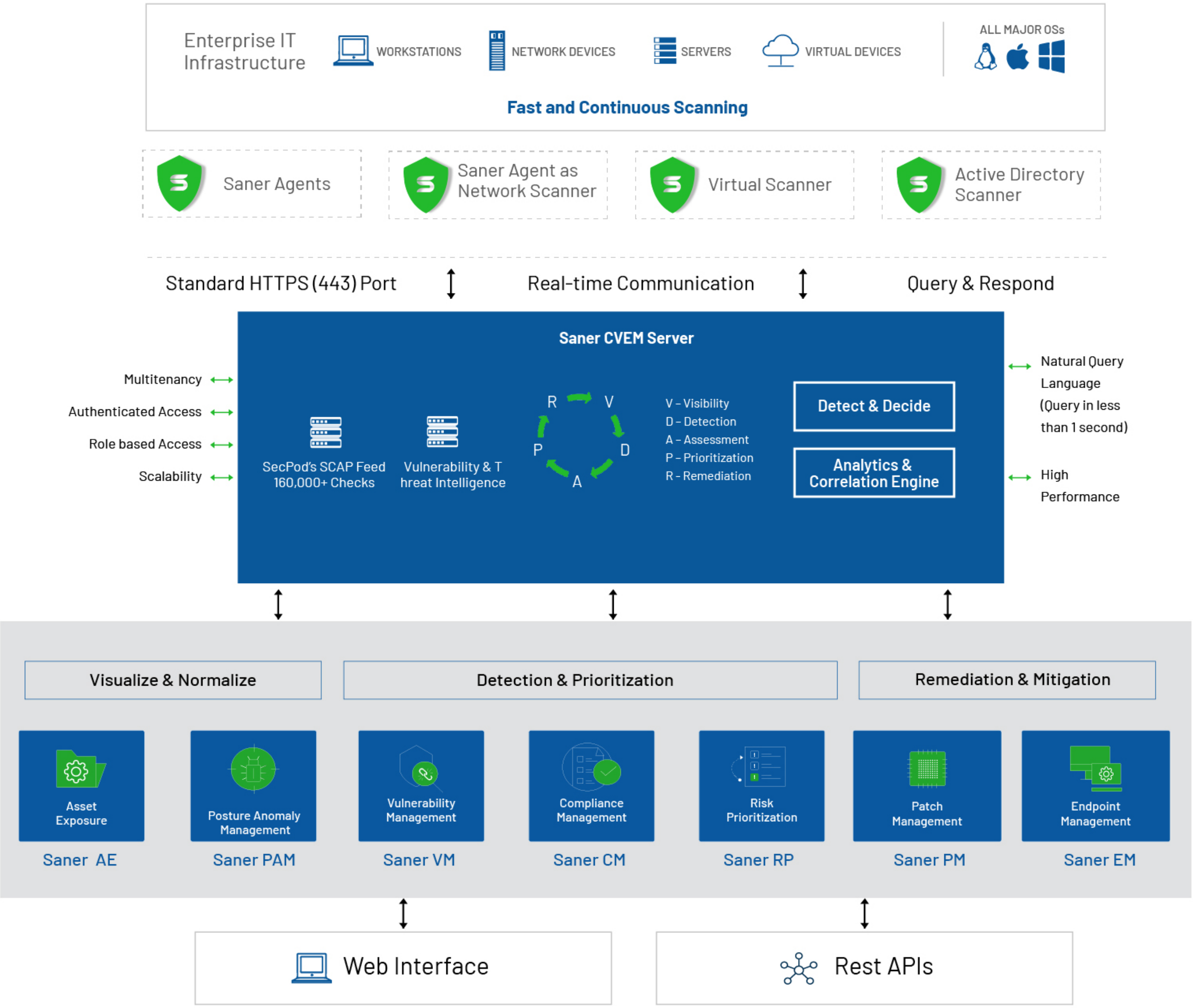
A Continuous Vulnerability and Exposure Management program,

- Unifies the entire vulnerability adn exposure management lifecycle into one single console. Eliminates the need to implement and operate on multiple siloed products and interfaces.
- Automates the implementation of vulnerability and exposure management into a continuous process.
- Helps achieve continuous and measurable cyber hygiene posture through cyber hygiene scores to prevent attacks.


VISUALIZE
NORMALIZE
DETECT
PRIORITIZE
REPORT
APIs
SECPOD SANER CONTINUOUS VULNERABILITY AND EXPOSURE MANAGEMENT
APIs
REMEDIATE

Under the Hood of Saner CVEM's Technology

Saner CVEM's backend technology is built with a robust Query, Detect, and Response Model, homegrown world's largest Security Intelligence Feed, powerful Analytics & Correlation Engine, and intelligent Radars to support operations on a wide range of devices and multiple operating systems including Windows, Mac, and Linux platforms.



Query, Detect, and Respond

Saner CVEM allows IT security teams to perform real-time, on-demand actions to keep IT security in check. SanerNow provides instant visibility over what's happening across your IT infrastructure and provides you with the necessary capabilities to act upon them through its intuitive console.

Saner CVEM provides hundreds of prebuilt queries to detect various security risks in the network, including vulnerabilities on all IP-enabled devices, misconfigurations across operating systems, missing patches, password aging, screen lockout, bit locker status, firewall status, CPU utilization, unwanted programs, wireless security status, sensitive security data like social security numbers, credit card stored in clear texts, antivirus status,

status of systems which are running more than seven days, disk space less than 100MB, windows registry values, user information in desktops, installation of malicious applications and devices, and more.

Saner CVEM platform provides an innovative metadata model to support instant searches using unstructured natural language queries. Along with prebuilt checks, you can also create customized checks to detect everything within your IT infrastructure.

The architecture also provides a built-in search to query almost anything in the IT network. With this, you can get details in the network based on IP address, MAC address, system name, hostname, and more.

Security Automation in Saner CVEM's Powerful Architecture

Saner CVEM hosts the world's largest security intelligence feed and vulnerability threat intelligence feed to provide continuous and automated security updates to the Saner CVEM Server.

Security Intelligence feed

Saner CVEM is powered by its homegrown world's largest vulnerability intelligence feed with more than 160,000 security checks. The SCAP repository offers a natural language-based search interface to extract security information. After continuous research and analysis, all the latest vulnerability updates are fed into the homegrown security intelligence feed every day. The security intelligence feed is automatically synced with the Saner CVEM server to enable continuous discovery of vulnerabilities in the IT network.

The security research team at SecPod continuously works on getting the latest vulnerability and security updates, including CVE, OVAL, CPE, CCE, CWE, CVSS score, severity range, exploit potential, and relevant patch fixes.

- Additionally, SecPod provides **SVE (SecPod Vulnerability Enumeration)** information for those vulnerabilities that are acknowledged by vendors but still lack complete CVE information on common publicly available CVE databases.
- Saner CVEM's native **CRE (Common Remediation Enumeration)** technology maps all the discovered vulnerabilities with remediation enumeration data to patch vulnerabilities and misconfigurations on time.
- Saner CVEM's **ERI (Extended Remediation Information)** technology provides patch information, prerequisites for the patching activity, and evolution of patches over time to aid the complex vulnerability remediation process.
- Saner CVEM's **XCCDF(Extensible Configuration Checklist Description Format)** provides information for benchmarks like HIPAA, PCI, ISO, NIST & SOC 2 to achieve compliance. SanerNow also provides remediation patches to harden configurations.
- Saner CVEM's **SQRL (SecPod's Query & Response Language)** provides a wide range of prebuilt detection and response scripts to manage vulnerabilities and security risks in the IT infrastructure.

Vulnerability Threat Intelligence Feed

Saner CVEMs Vulnerability threat intelligence feed consists of the Malware Vulnerability Enumeration (MVE) data. Saner CVEM maps the detected vulnerabilities with **MVE (Malware Vulnerability Enumeration)** data to identify the vulnerabilities causing high-fidelity attacks. With this, Saner CVEM showcases the threatening vulnerabilities causing dangerous attacks and alerts the IT security teams to remediate them instantly.

Powerful Analytics and Correlation Engine (ANCOR)

Saner CVEM's ANCOR is scalable analytics and correlation engine that operates on multiple sets of data to perform methodical investigations. The data set include vulnerability information, IT asset exposures, missing patches, deviation in security controls, endpoint security metrics, and security posture anomalies. ANCOR correlates all these data to uncover the network's vulnerability and security risk exposure.

Ancor enables detection, assessment, prioritization, remediation, reporting of vulnerabilities & security risks from a single centralized console by analysing data from devices and correlating it with the homegrown security intelligence.

SanerNow Radars

Agent

The smart, lightweight, multifunctional agent must be installed on the endpoints to implement the advanced vulnerability management tasks. The agents receive the tasks from the Server and silently execute them on the devices without interrupting the users. With Saner CVEM, you can,

- Scan the entire virtual and physical infrastructure
- Establish a live communication channel between the agents installed on the devices and the Server to perform real-time, on-demand queries and responses
- Run active directory scan
- Perform network scan
- Customize the agent-server sync time according to your organization's requirements
- Manage remediation tasks and execute a wide range of actions

Agent as Network Scanner

The powerful agent also takes up the role of a network scanner to scan other devices in the network, saving additional costs over purchasing new hardware. The agents can be configured to scan the entire network to detect vulnerabilities across your IT infrastructure. The agent performs network scanning without consuming excessive bandwidth and system resources. Different scan profiles can be configured to suit your organization's needs.

Agent as an Active Directory (AD) Scanner

The powerful agent also takes up the role of an AD scanner to configure users and devices available in the network. This activity also works without consuming excessive bandwidth and system resources.

Features & Benefits of SanerNow Architecture

Robust, Natively Built, and Truly Integrated Solution

Saner CVEM Cyberhygiene platform is built completely in-house to provide a truly integrated solution. All security tasks can be easily performed from a single place without having to juggle different tools.

Gain holistic visibility into IT infrastructure and eliminate outliers

Get collective and deeper visibility over you IT infrastructure. Spot the most obvious attack vectors including outliers in the network, unapproved software & devices, incorrectly configured security controls and much more, and eliminate them instantly.

Multi-tenant Support with Segregated User Data

Efficiently manages multiple business units and system users with a single server. Neatly segregates business users' data and offers the ability to create various user roles with defined access rights to manage different areas of a corporate network.

Real-Time Communication with Distributed Devices

Saner CVEM allows you to talk and respond to your devices anytime and anywhere in real-time. You can run on-demand operations and establish real-time communication with your organizational devices.

High-Performance Scalable Architecture

The platform is highly scalable with a Big Data architecture, efficiently supporting the management of a large number of devices through a single server without performance degradation.

Rapid, Continuous, and Automated Operations

With Saner CVEM, you can run the industry's fastest scans in less than 5 minutes and automate all security tasks end-to-end and achieve continuous operations.

Leverage cloud or on-premises solution as per requirement

Saner CVEM supports operations on both cloud and on-premises variants. You can opt for either of the ones which suit your business needs.

Seamless Integration & Interoperability

The flexible architecture of the platform allows integration with various systems. The REST APIs enable access to all collected data from endpoints and supports search queries.

Operates on a lightweight Agent

Saner CVEM platform work on a single, lightweight, multifunctional agent which weighs less than 20MB and executes all the tasks. The agent also takes up the role of network scanner and saves cost on integrating additional hardware.

Protects BYOD, Remote Office, and Transient Devices

Ensures security of organizations' devices across perimeter limits. Provides efficient protection and control of transient, remote, and BYOD devices from a centralized console.

Leverage Machine Learning to deep learn IT

Saner CVEM analyses various parameters in the network and uses machine learning concepts to provide deep insights into the IT infrastrucre and discover outliers.

Deviation Computations of Standard Configurations

Saner CVEM uses 40+ checks to assess if configurations are set differently from others. Through this it identifies the deviated configurations that needs to be looked upon immediately.

Easy Setup and Onboarding

Saner CVEM can be set up in less than 30 minutes, and you can kick start your operations in no time. SanerNow offers multiple modes to deploy agents seamlessly across your network.

Provides Multi-factor Authentication

The platform provides multi-factor authentication to protect the SanerNow account and add an extra layer of security.

Supports Natural Language Search Queries

The innovative metadata model of the platform supports instant searches using unstructured natural language queries. Saner CVEM understands it all and provides valuable insights to our customers.

Leverage a New Weakness Perspective for Better Attack Surface Reduction

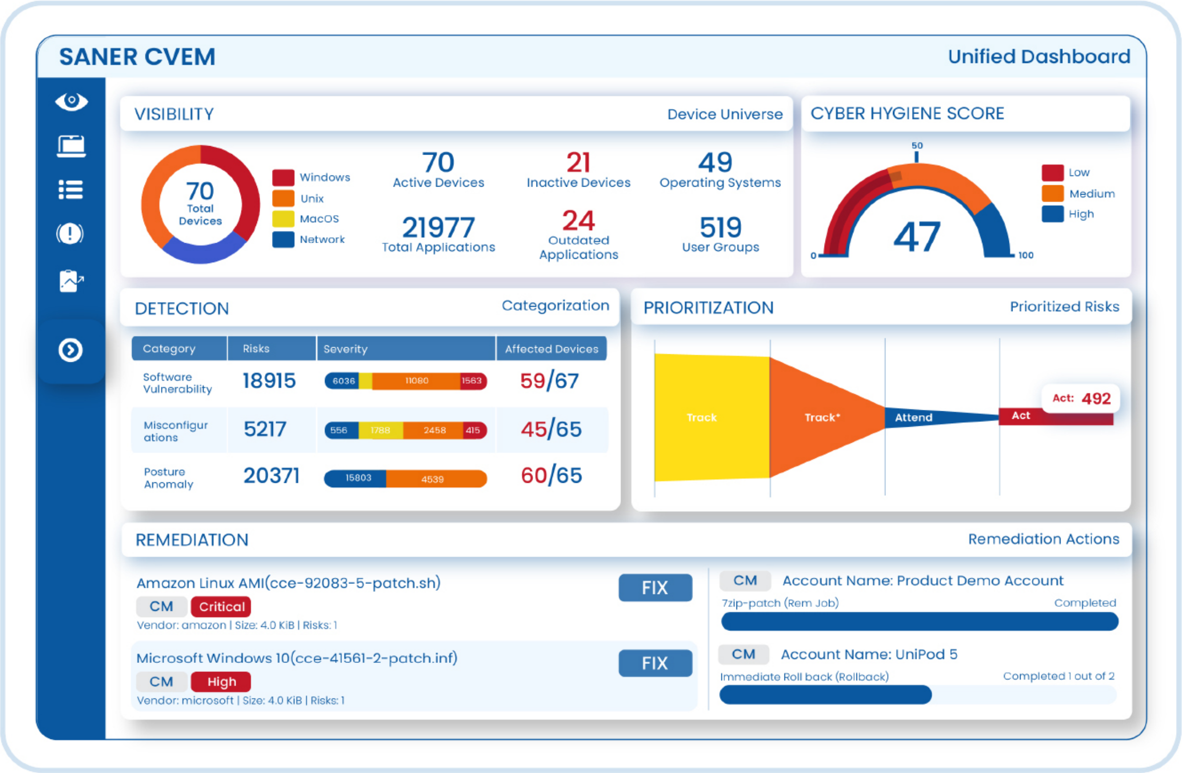
Revamp the way you manage vulnerabilities and exposures with a new perspective. Get granular visibility, understand weaknesses,& take complete control over the reduction of your organization's IT attack surface.

Rule & Trend based Analysis to Discover Anomalies

Saner CVEM uses rule and trend-based analysis where it collects some parameters over a period to spot any aberrations or abnormalities in regular pattern.

Cyber Hygiene Scores

Know how secure your organization and devices are with Saner CVEM cyber-hygiene scores. Further, know the top 5 risk exposures and top contributors of the risk.



SANER CVEM

Unified Dashboard

VISIBILITY

Device Universe

70 Active Devices

21 Inactive Devices

49 Operating Systems

21977 Total Applications

24 Outdated Applications

519 User Groups

CYBER HYGIENE SCORE

DETECTION

Categorization

Category	Risks	Severity	Affected Devices
Software Vulnerability	18915	6036 11080 1563	59/67
Misconfigurations	5217	556 1788 2458 415	45/65
Posture Anomaly	20371	15803 4539	60/65

PRIORITIZATION

Prioritized Risks

REMEDIATION

Remediation Actions

Amazon Linux AMI(cce-92083-5-patch.sh)

CM Critical

Vendor: amazon | Size: 4.0 KiB | Risks: 1

FIX

Microsoft Windows 10(cce-41561-2-patch.inf)

CM High

Vendor: microsoft | Size: 4.0 KiB | Risks: 1

FIX

CM Account Name: Product Demo Account

7zip-patch (Rem Job) Completed

CM Account Name: UniPod 5

Immediate Roll back (Rollback) Completed 1 out of 2

About SecPod

SecPod is a leading cybersecurity technology company committed to preventing cyberattacks through proactive security. Its mission is to secure computing infrastructure by enabling preventive security posture.

At the core of SecPod's offerings is the Saner Platform - a suite of solutions that help organizations establish a strong security posture to preempt cyber threats against endpoints, servers, network and cloud infrastructure, as well as cloud workloads. With its cutting-edge and comprehensive solutions, SecPod empowers organizations to stay ahead of evolving threats and build a resilient security framework.

Contact Us

Email us on:info@secpod.com