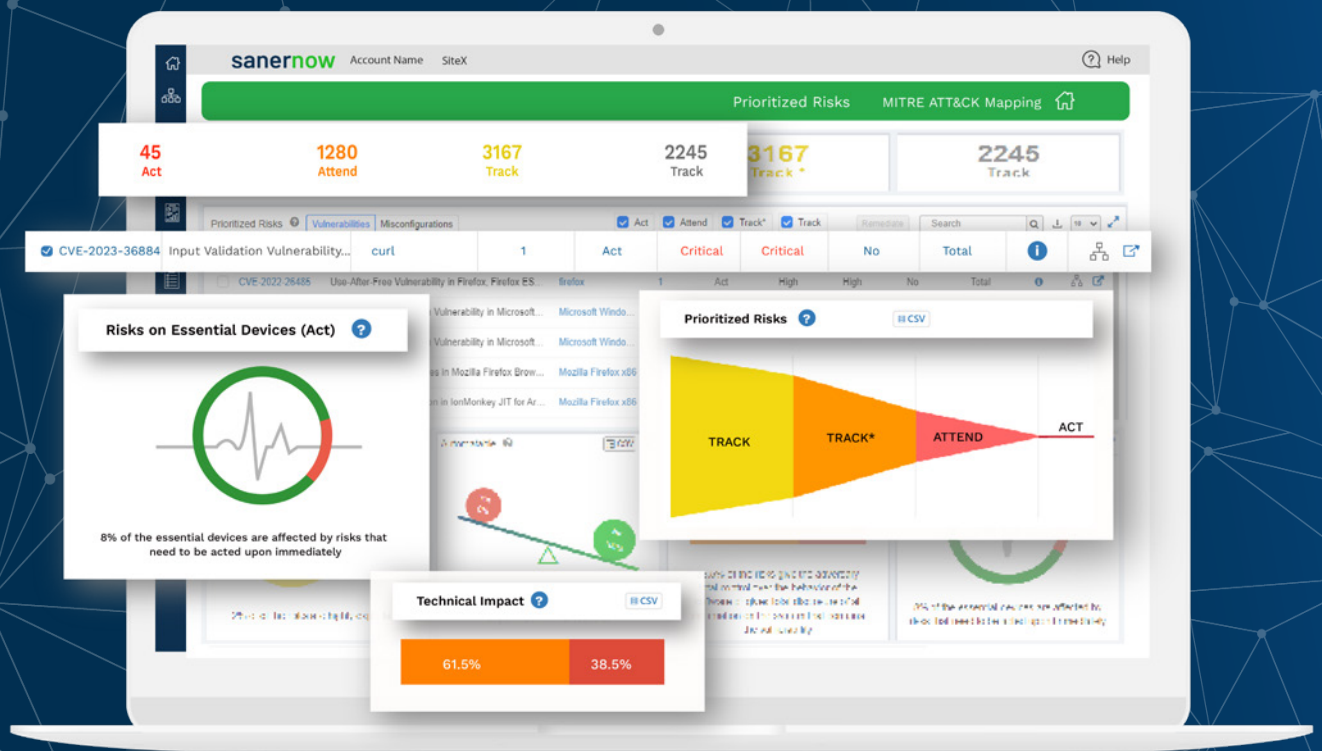


SanerNow Risk Prioritization Technical Brief



secpod

Introduction

In today's dynamic business landscape, organizations face multiple risks, ranging from cybersecurity threats to regulatory compliance deviations. Understanding and addressing these risks are paramount in ensuring the resilience and continuity of business operations. However, with limited time and high potential vulnerabilities getting exploited in a short time, it's crucial for organizations to adopt a strategic approach to manage these risks.

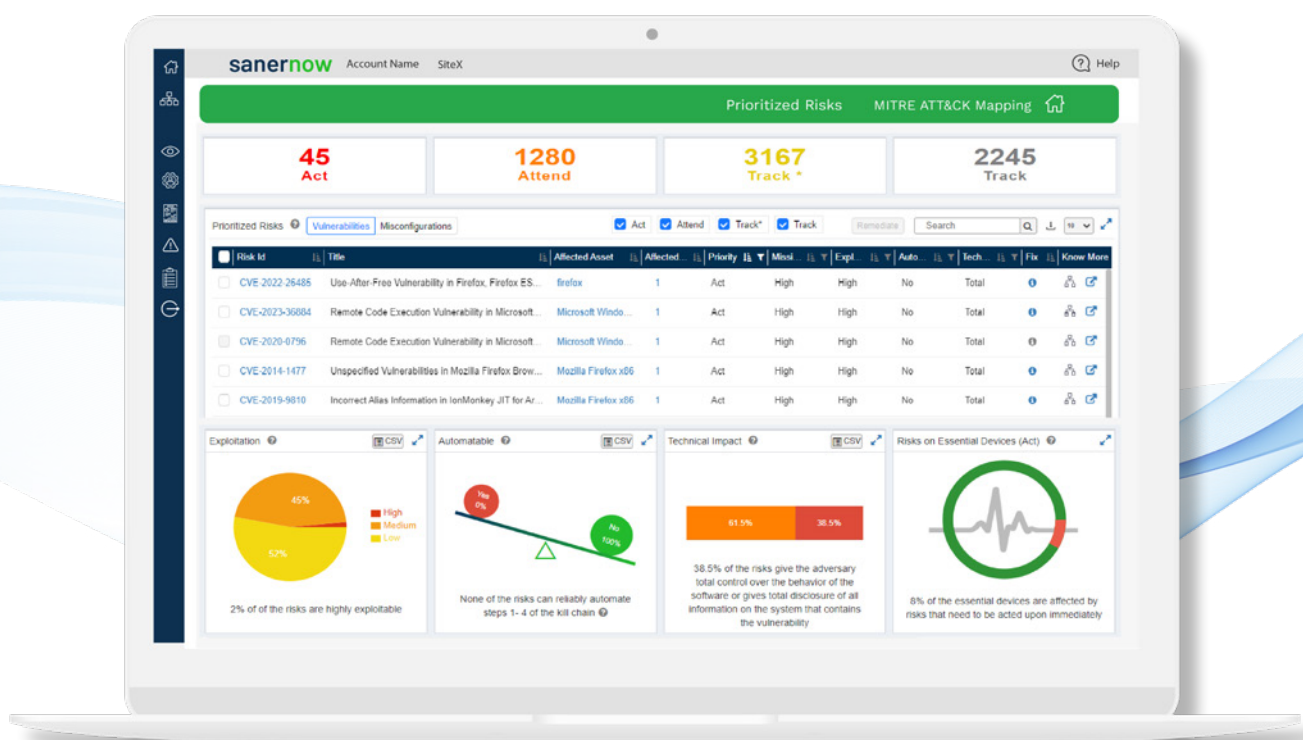
This is where Risk Prioritization comes in handy. It's the process of categorizing risks based on their severity levels, exploitability factor, and other security aspects. By doing so, organizations can focus their attention on remediating and mitigating the most impactful risks, thereby minimizing the attack surface, and keeping their organization cybersecure.



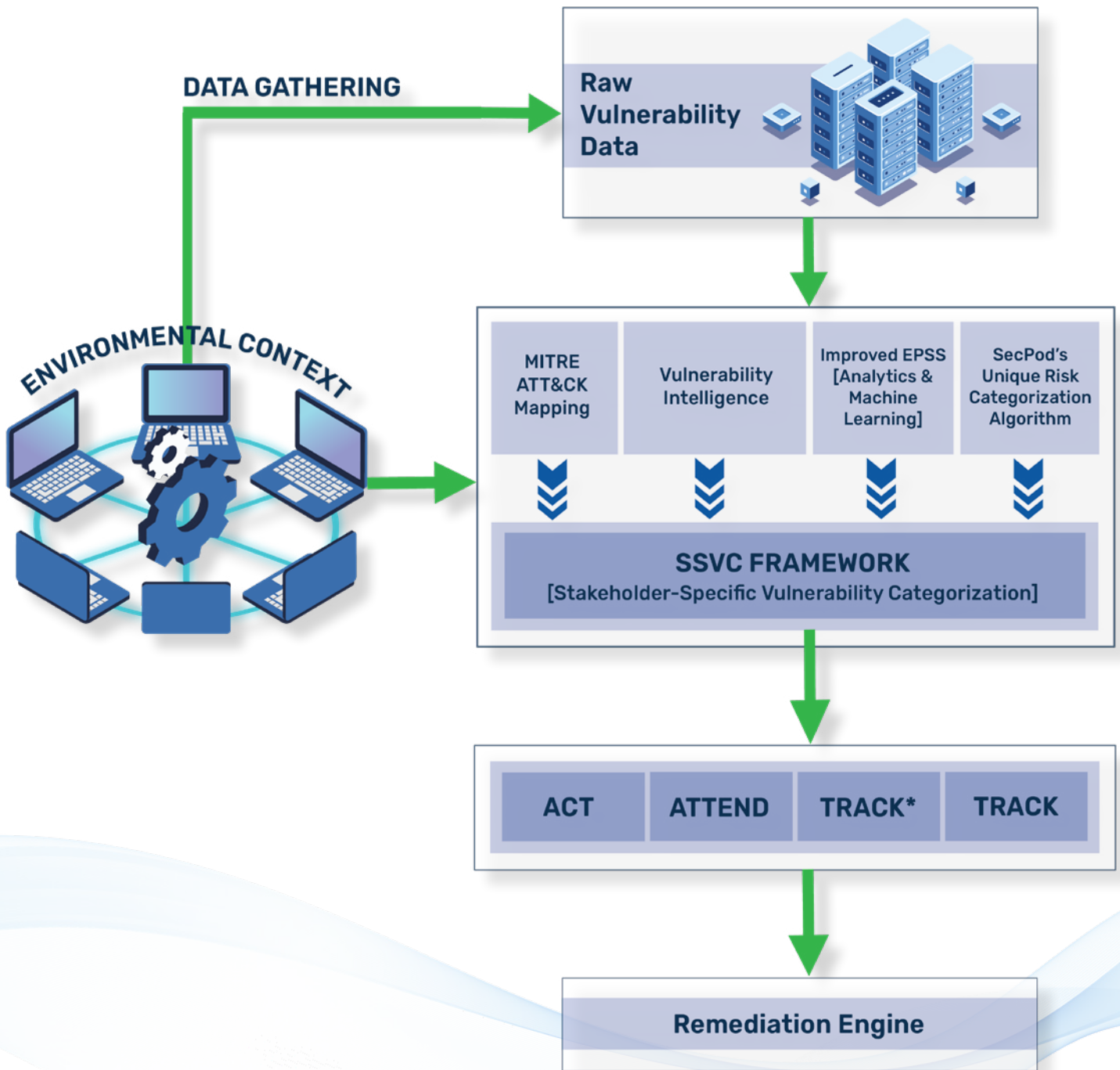
An Overview of SanerNow Risk Prioritization


SanerNow Risk Prioritization (RP) is the world's first **Stakeholder-Specific Vulnerability Categorization (SSVC)** framework-based prioritization tool. It prioritizes vulnerabilities based on Business Context, and vulnerability characteristics such as Exploitability, Automatable, Technical Impact and Mission Prevalence parameters.

SanerNow RP, powered by in-house vulnerability and threat intelligence, implements an enhanced **Exploit Prediction Scoring System (EPSS)** and SecPod's unique risk categorization algorithm & proprietary mitigation evaluation techniques in the attack kill chain. SanerNow Risk Prioritization consumes raw vulnerability data from the natively integrated vulnerability scanners and business and environment context to prioritize vulnerabilities into Act, Attend, Track* & Track. It provides real-time insights into organization's vulnerability landscape to understand the risks and helps remediation actions effectively.



Architecture of SanerNow Risk Prioritization





SanerNow RP is modeled around CISA's SSVC framework. SanerNow RP consumes raw vulnerability and risk data uncovered by SanerNow Vulnerability Management and SanerNow Compliance Management modules and performs analytics and correlation with natively built vulnerability and threat intelligence information, exploit prediction model, MITRE ATT&CK mappings to technically categorize vulnerability based on their exploitability, automatability, and technical impact.

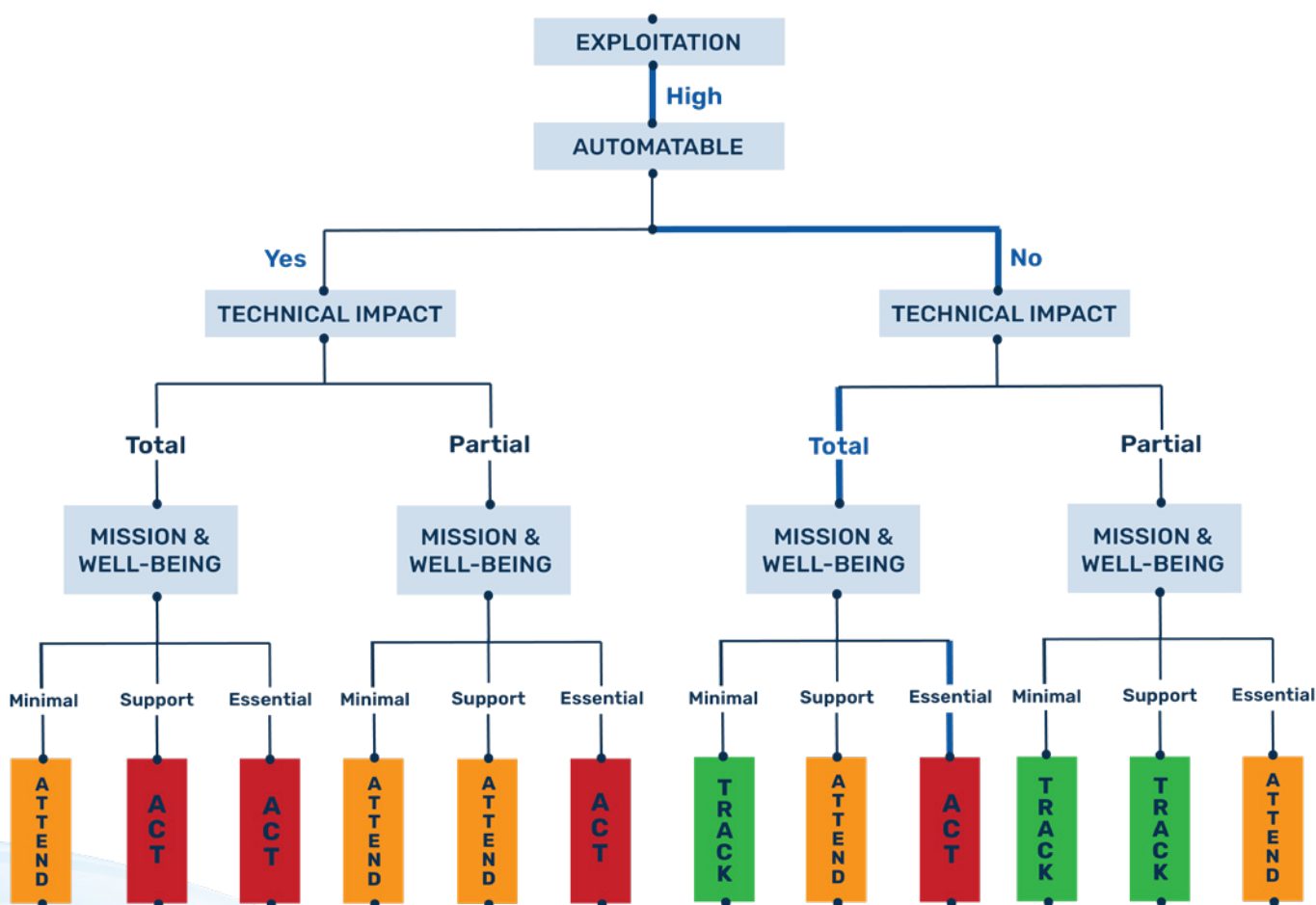
The prioritization apparatus is further enriched with business and environment context learnt through SanerNow Asset Exposure and Open Checklist Interactive Language (OCIL) questionnaire to learn about implemented security controls. The outcome of the processing engine neatly categorizes vulnerability into Act, Track*, Track, and Attend.

SanerNow RP natively integrates with vulnerability mitigation and remediation engine to apply remediation measures that include patches (SanerNow PM), configuration fixes (SanerNow CM), and other remediation (SanerNow EM) measures.

Exploring SanerNow Risk Prioritization

SanerNow Risk Prioritization prioritizes and differentiates the vulnerabilities using the enhanced version of EPSS model and also follows the standard guidelines of CISA's SSVC Framework.

Here, is how the decision tree looks like:

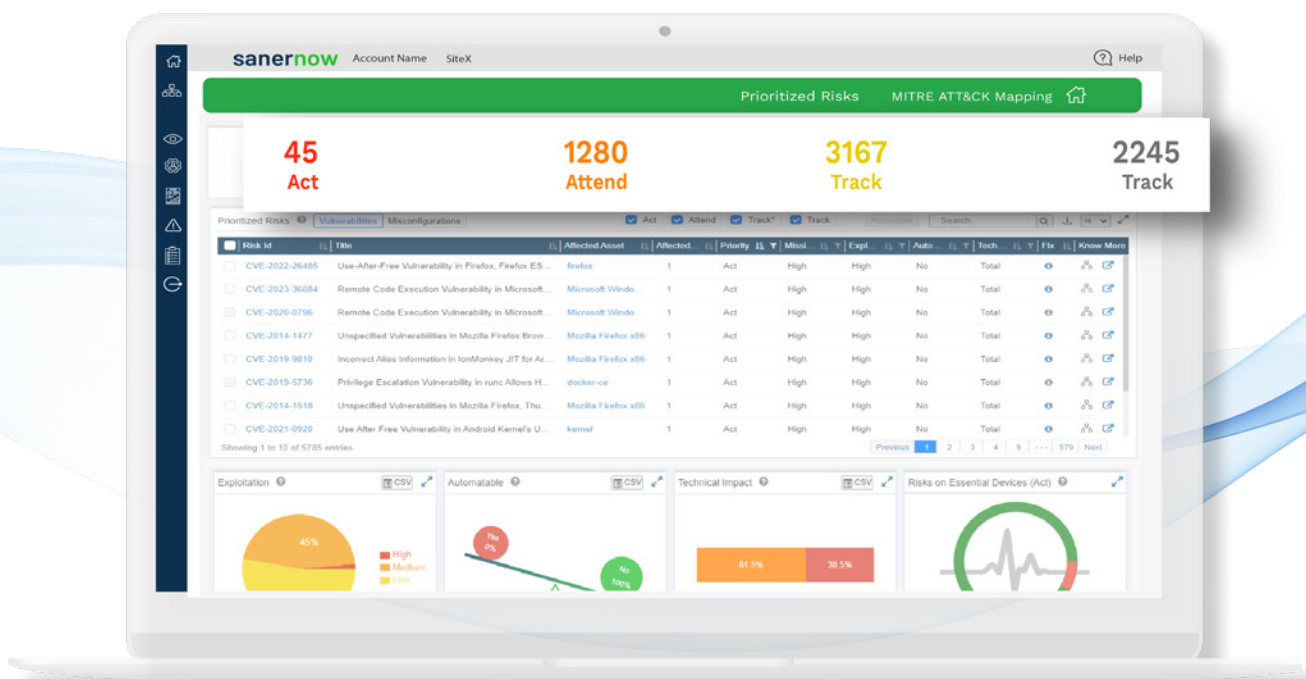


Act - The vulnerability requires attention and necessary actions should be taken including requesting assistance or information about the vulnerability, as well as publishing a notification either internally or externally. CISA recommends remediating Act vulnerabilities as soon as possible.

Attend - It is similar to Act but needs to be remediated sooner than the standard time-lines according to recommendation given by CISA.

Track* - Vulnerabilities detected will have specific characteristics and will require closer monitoring for changes. Remediation should be done within the standard update time-lines.

Track - The vulnerability in this section does not require action immediately. Continue to track the vulnerability and reassess it if new information becomes available.

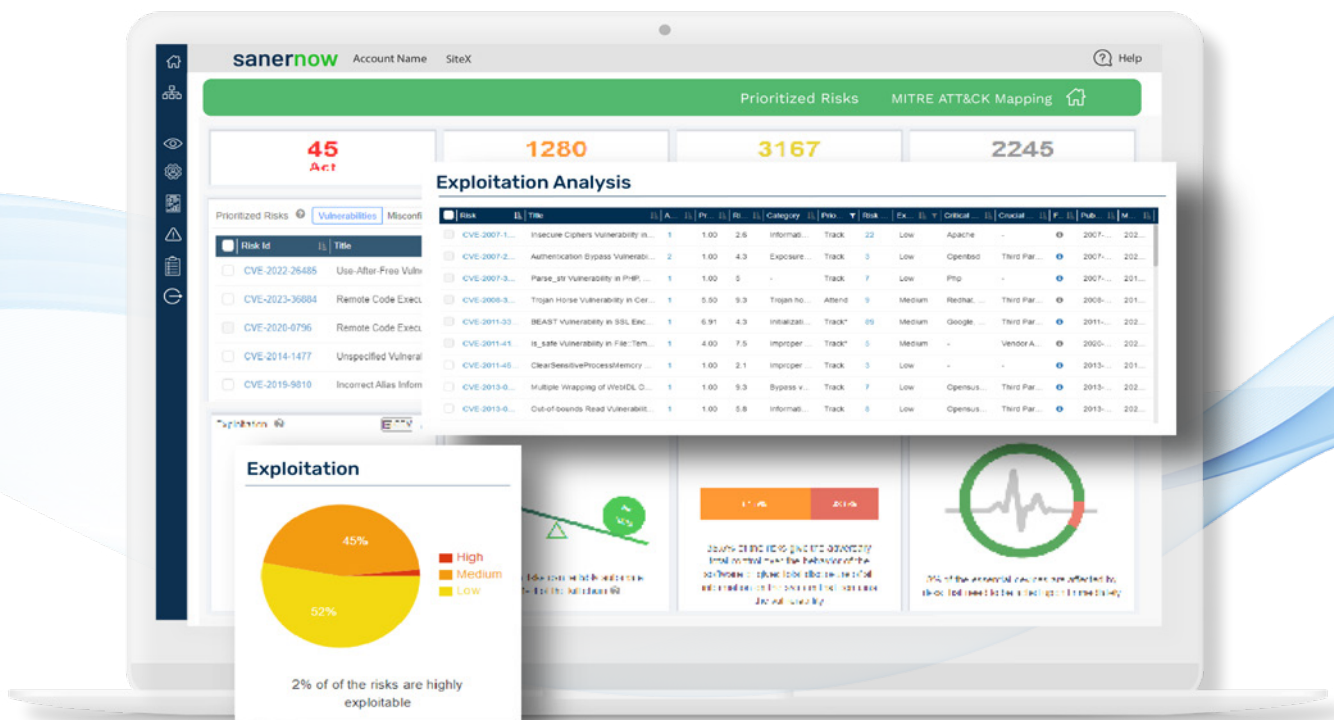


SanerNow Risk Prioritization Technical Details

EXPLOITATION

It is primarily driven by SecPod's Unique Risk Categorization Algorithm. This algorithm employs data analytics to establish correlations between various factors such as Malware Vulnerability Enumeration (MVE) Mapping, CISA Known Exploit Vulnerabilities (KEVs), Google Project Zero findings, and other relevant data points. The result is the computation of a Risk Exploitability Score for each finding.

Further, SanerNow categorizes calculated Exploitation Score of a risk into High, Medium, or Low based on a range and provides you the percentage of vulnerabilities that can be easily exploited.





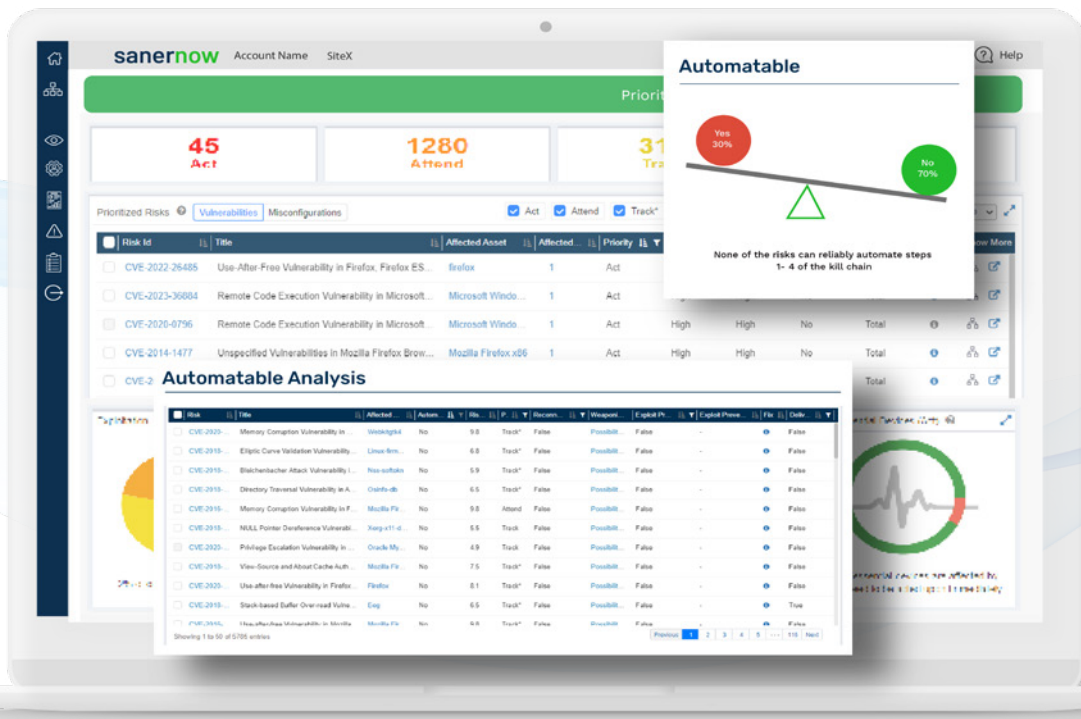
AUTOMATABLE

When critical vulnerability is detected, there's always a fear of it being exploited in wild. But, is it that easy for attacker to exploit an critical vulnerability? Each risk is checked to be evaluated for Automatable i.e. Yes or No. Automatable value 'Yes' for a risk is concluded if the risk can be reliably automated with steps 1-4 of the kill chain, otherwise it is set to 'No'.

Multiple factors help determine that Steps 1-4 of Kill Chain can be reliably automated such as:

- Determining if a device is internet facing and enumerable on the network
- If CVE weaponization is possible through chaining
- Delivery that checks if channels that cannot be blocked by widely deployed network security configurations
- If there is an exploitation mitigation mechanism that is already in place that frustrates attackers from automating the attack, this considers MITRE ATT&CK Techniques, Tactics and Mitigation mapping with CVEs and CCEs, and evaluating these automated checks with scan

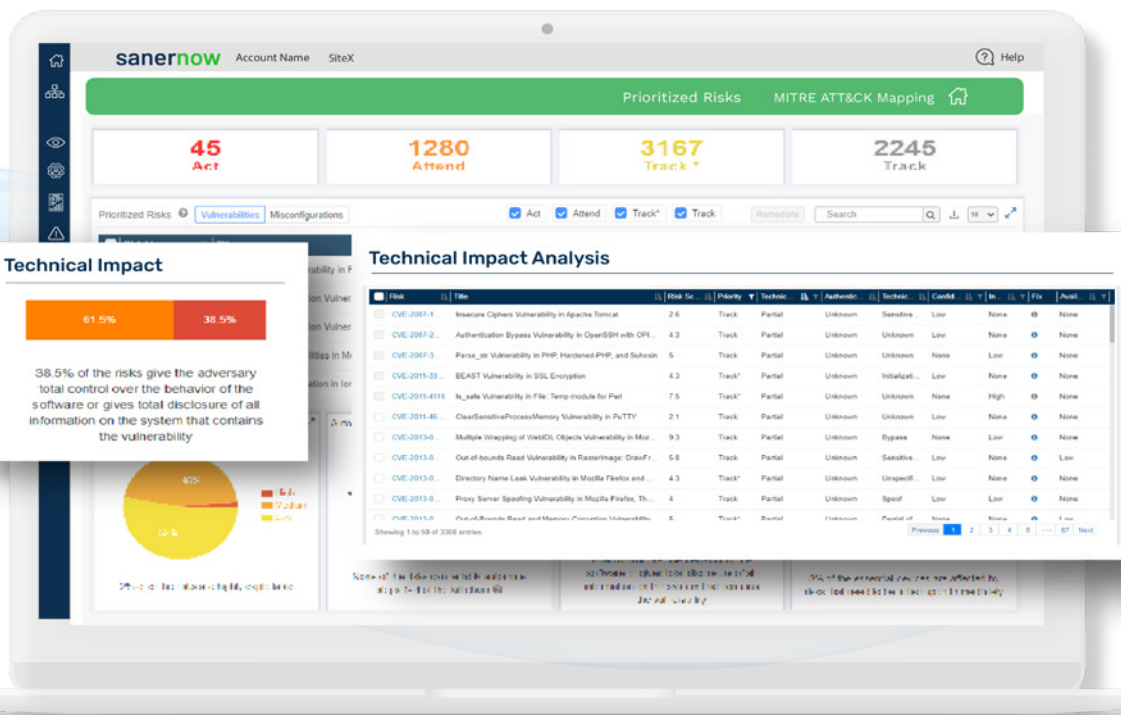
Automatable feature represents the ease and speed with which a cyber threat actor can cause exploitation events. SanerNow provides you the data from which you gain clear clarity of vulnerabilities that can be easily automated for exploitation.



TECHNICAL IMPACT

Technical impact is similar to the Common Vulnerability Scoring System (CVSS) concept of “severity.” It defines how severe is the vulnerability in IT organization. SanerNow represents this in the form of adversary total score which defines total disclosure of all information on the system that contains the vulnerability.

Risk Prioritization Scanner detects Technical impact through various means, CVSS Score Metrics, Information disclosure CWEs mapped to CVEs, Intelligent Text Search Algorithm to determine credential exposure and other techniques, to conclude the value of Technical Impact of Risks on Devices.

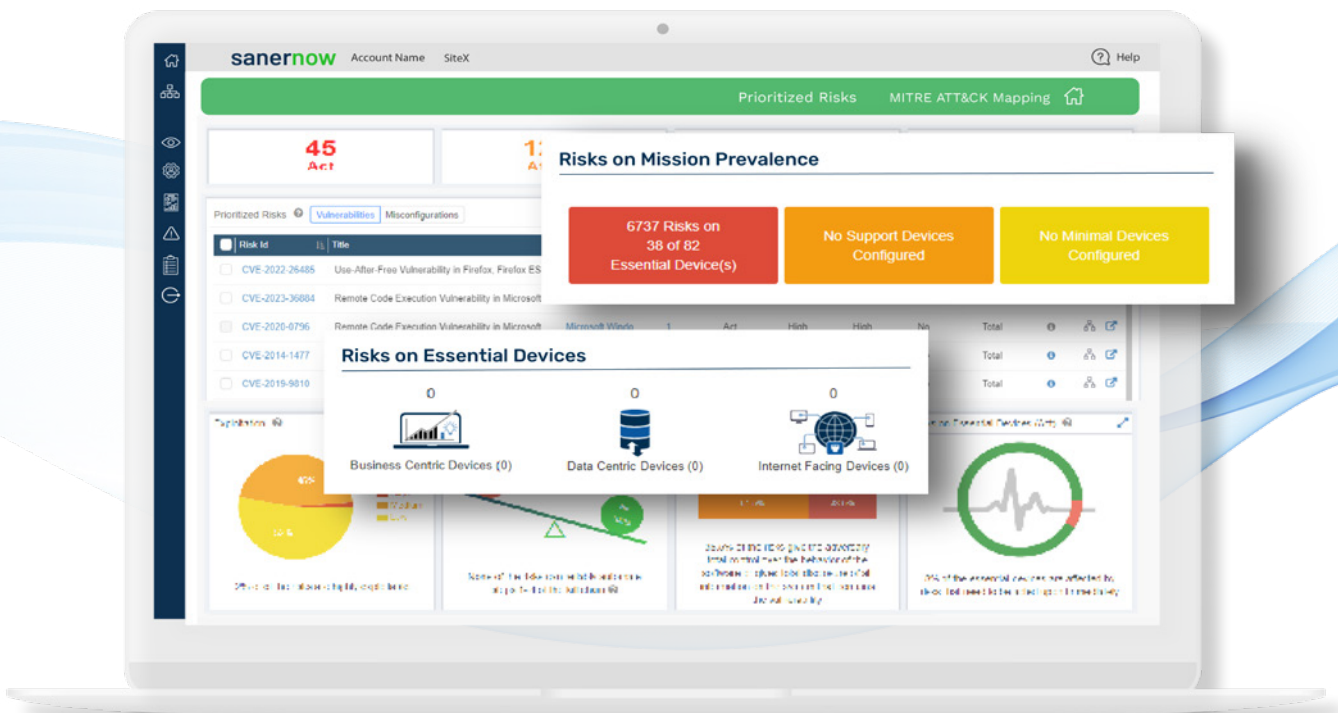


MISSION PREVALENCE

A mission essential function (MEF) is a function “directly related to accomplishing the organization’s mission as set forth in its statutory or executive charter.” SanerNow categorizes the risks on mission prevalence which is the visualization of risk count on devices. And all Essential, Support, Minimal devices can be remediated on click.

The mission is the reason an organization exists, and MEFs are how that mission is realized. Non-essential functions support the smooth delivery or success of MEFs rather than directly supporting the mission.

VALUE	DEFINITION	MARKED AS
Essential	The vulnerable component directly provides capabilities that constitute at least one MEF for at least entity; component failure may (but does not necessarily) lead to overall mission failure	High
Support	The vulnerable component only supports MEFs for two or more entities	Medium
Minimal	Neither support nor essential apply. The vulnerable component maybe used within the entities, but it is not used as a mission-essential component, nor does it provide impactful support to mission-essential functions	Medium



Unique Capabilities of SanerNow Risk Prioritization



01

Comprehensive Risk Prioritization model based on SSVC, vulnerability intelligence, machine learning based exploit prediction, kill-chain validation, business context, data analysis and more



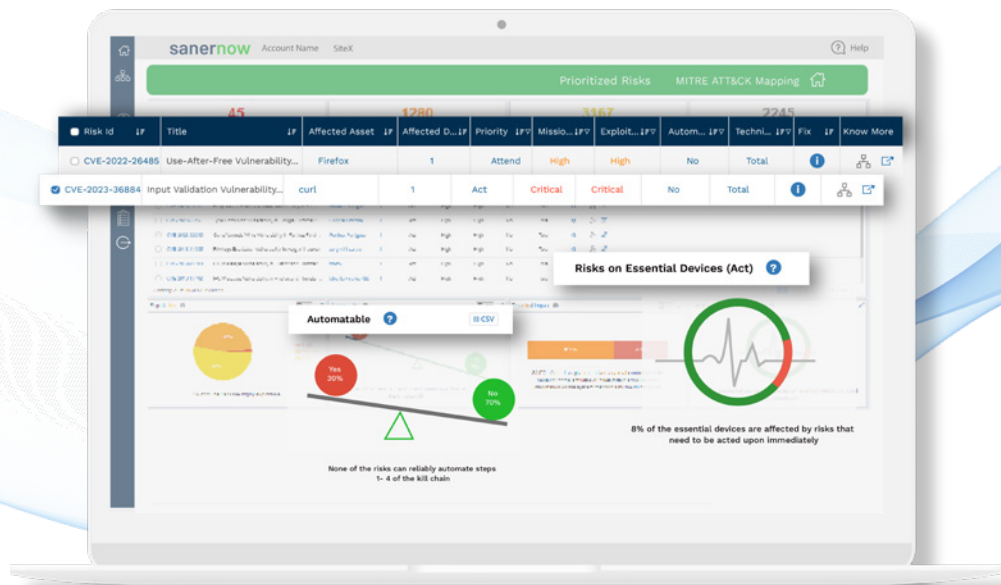
02

Natively integrated vulnerability scanner for accurate and faster detection of vulnerabilities, eliminating the need for external vulnerability ingestion



03

Natively integrated remediation engine to rollout fixes to effectively eliminate vulnerabilities



Seamlessly Prioritize Security Risks with SanerNow RP

SCHEDULE A DEMO

About SecPod

SecPod is a cyber security technology company with a mission to prevent cyberattacks on organizations. Our Advanced Vulnerability Management platform helps implement cyber hygiene measures, making it more difficult for attackers to access systems and companies' vital information.

SecPod SanerNow is a Cyber Hygiene platform providing continuous visibility to IT infrastructure. It identifies vulnerabilities, misconfigurations, and security risk exposures, mitigates loopholes to reduce the attack surface, measures compliance, and helps automate remediation. Our product philosophy is offering an easy-to-use solution with fast time to value that improves an organization's IT risk posture at a lower total cost of ownership Vs. using point solutions.



Contact Us

Email us on:
info@secpod.com

www.secpod.com