Managing Vulnerabilities Using SanerNow

4.0 User Guide

Contents

Vulnerability Management

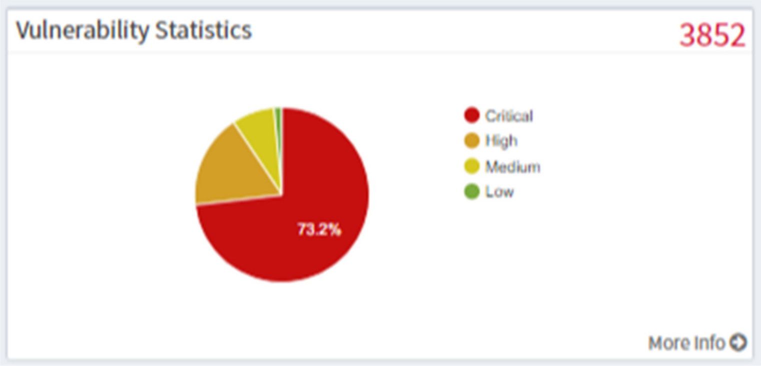
Attackers exploit vulnerabilities or weaknesses in software to gain control of computer systems, steal sensitive information and cause disruption of services. Vulnerabilities can be in the OS components or software applications. IT administrators have to identify and manage the risks associated with these vulnerabilities.

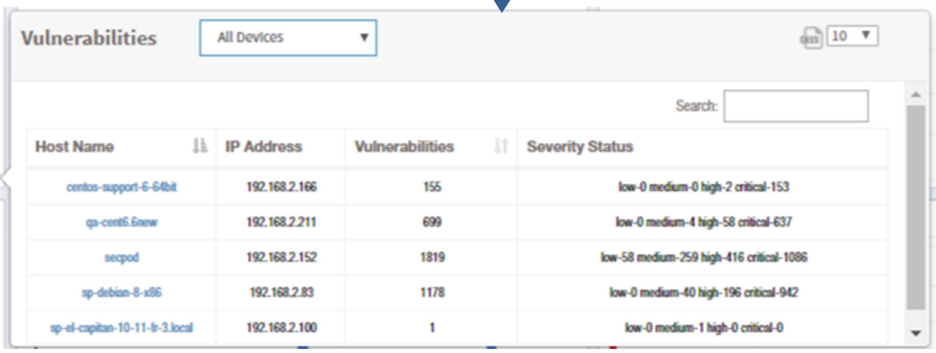
Monitor + Assess + Prioritize + Remediate = Vulnerability Management

SanerNow simplifies the vulnerability management cycle to a daily routine, simplifies remediation and reporting, and reduces the total cost of operation (TCO). The SanerNow solution helps identify, classify, remediate, and mitigate vulnerabilities in an organization. In the following sections, we will see how to accomplish Vulnerability Management with the SanerNow solution.

1. Logon to SanerNow using your SanerNow credentials.
2. Select an account to manage by clicking the icon at the upper left corner of the window. A dashboard with the summary view of the account is displayed.
3. Click the SanerNow icon on the header. Click the Vulnerability Management icon. The Vulnerability Dashboard is displayed, which provides vulnerability details categorized by severity or type, age, affected hosts, devices, and assets, mitigation data and patch statistics.

Total Number of Vulnerabilities





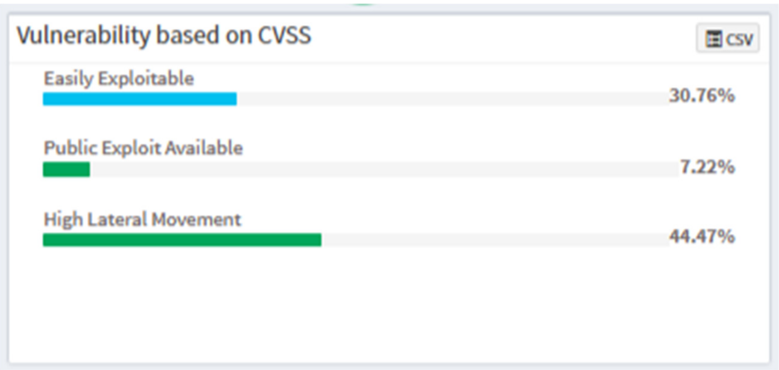
Host Name	IP Address	Vulnerabilities	Severity Status
centos-support-6-64bit	192.168.2.166	155	low-0 medium-0 high-2 critical-153
qa-cent6.6new	192.168.2.211	699	low-0 medium-4 high-58 critical-637
secpod	192.168.2.152	1819	low-58 medium-259 high-416 critical-1086
sp-debian-8-x86	192.168.2.83	1178	low-0 medium-40 high-196 critical-942
sp-el-capitan-10-11-fr-3.local	192.168.2.100	1	low-0 medium-1 high-0 critical-0

- This pie chart shows the total number of vulnerabilities on all devices in the network and classifies the severity of the vulnerabilities as low, medium, high, and critical in the Vulnerability Statistics pane. Click the **More Info** link to display a dialog to filter the vulnerability statistics by all devices, unassigned devices, groups, or a specific group of devices. The affected device or host ID, the IP address, the total number of vulnerabilities for that host, and the severity grouping is displayed in the dialog.

- Click a host or group name to go to the Device Info page, where you can see
  - Hardware and software device details and vulnerability scan details.
  - A detailed view of storage and network details.
- Click Audit Log to view a log file of all the changes made to this device by any user. You can also download a copy of the audit log.
- Click Export Device Report to download a report in pdf format with device details.

Vulnerabilities Based on CVSS

Prioritization of remediation can be done only if there is visibility into the category of the vulnerability. SecPod uses the Common Vulnerability Scoring System (CVSS), which determines the severity of the vulnerability based on principal characteristics that are translated into a numerical score.

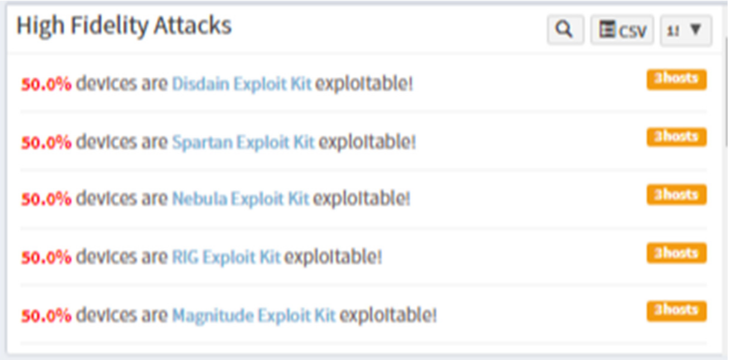


This pane categorizes the vulnerabilities on the network by:

- Easily Exploitable – Vulnerabilities that are known in the public domain, making an exploit easily possible.
- Network Exploitable - Vulnerabilities that can be exploited with network access, often remotely. The attacker's path is through the network layer.
- Public Exploit Available – Vulnerabilities for which exploits are available publicly and which have occurred in the past.
- High Lateral Movement – Vulnerabilities that extend to the network as the threat moves from device to device and asset to asset, and attackers collect valuable data.

High Fidelity Attacks

This pane groups the vulnerabilities by the exploit kits that can be used to exploit the weakness.



High Fidelity Attacks

50.0% devices are Disdain Exploit Kit exploitable! 3hosts

50.0% devices are Spartan Exploit Kit exploitable! 3hosts

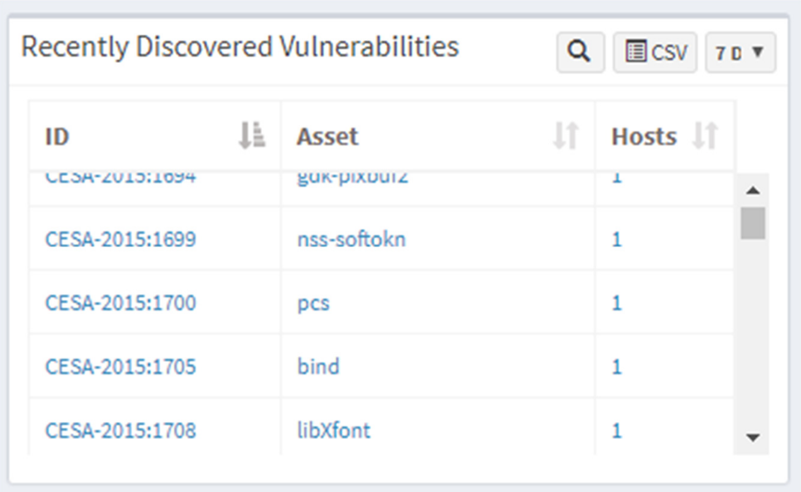
50.0% devices are Nebula Exploit Kit exploitable! 3hosts

50.0% devices are RIG Exploit Kit exploitable! 3hosts

50.0% devices are Magnitude Exploit Kit exploitable! 3hosts

Recently Discovered Vulnerabilities

This pane shows vulnerabilities that have been recently discovered. You can filter the list by 7 days, 30 days, or 90 days.

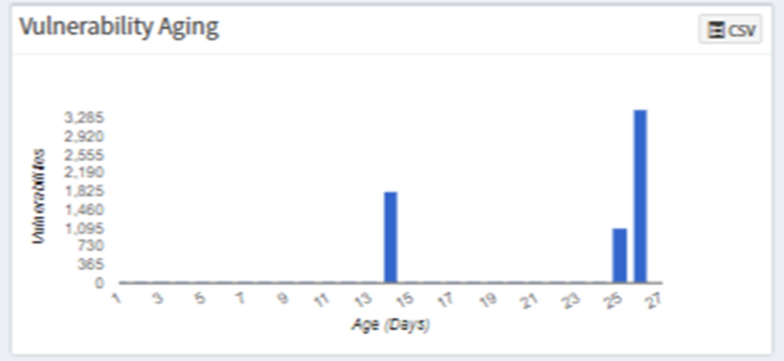


Recently Discovered Vulnerabilities

ID	Asset	Hosts
CESA-2015:1694	gdk-pixbuf2	1
CESA-2015:1699	nss-softokn	1
CESA-2015:1700	pcs	1
CESA-2015:1705	bind	1
CESA-2015:1708	libXfont	1

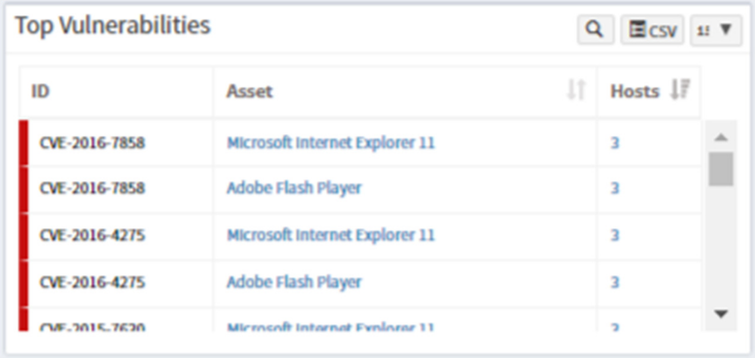
Vulnerability Aging

This pane shows vulnerabilities grouped by the number of days since they were detected and that have not been fixed.



Top Vulnerabilities

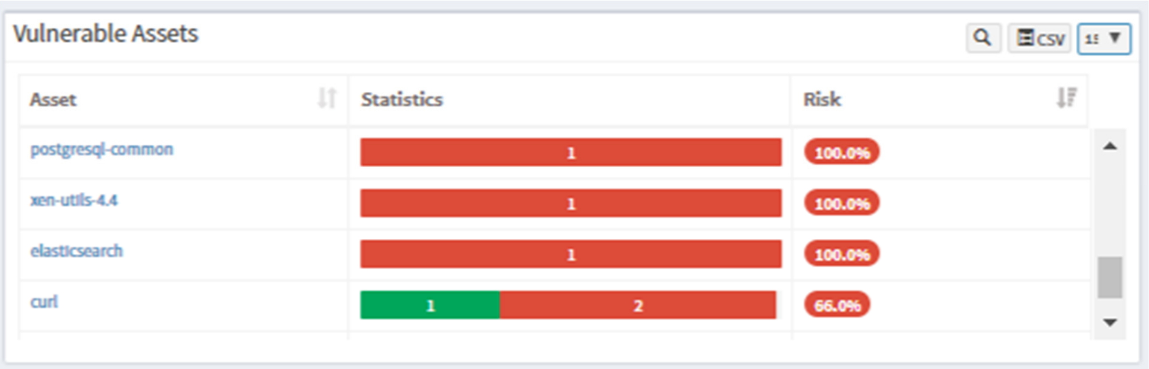
This pane shows top vulnerable assets by their CVE ID, and the number of devices at risk.


Top Vulnerabilities

ID	Asset	Hosts
CVE-2016-7858	Microsoft Internet Explorer 11	3
CVE-2016-7858	Adobe Flash Player	3
CVE-2016-4275	Microsoft Internet Explorer 11	3
CVE-2016-4275	Adobe Flash Player	3
CVE-2015-7620	Microsoft Internet Explorer 11	3

Vulnerable Assets

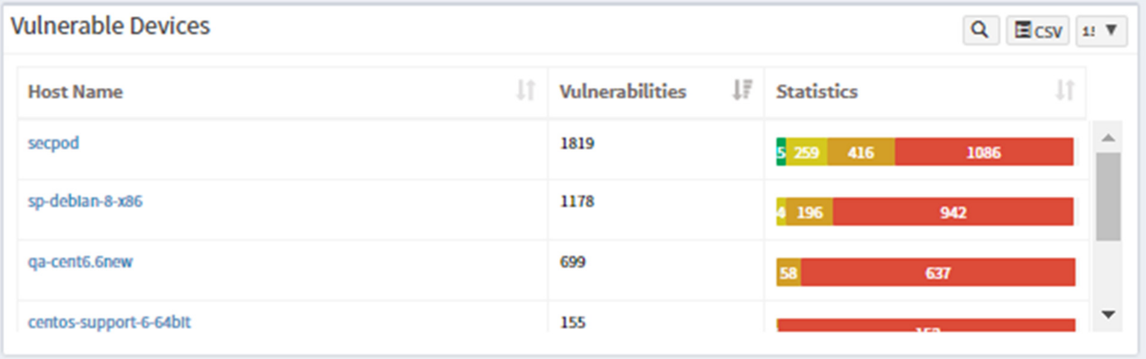
This pane displays the software assets installed on systems in the organization and the risk associated according to their level of vulnerability. Click an asset name to see the details of the affected hosts.


Vulnerable Assets

Asset	Statistics	Risk
postgresql-common	1	100.0%
xen-utils-4.4	1	100.0%
elasticsearch	1	100.0%
curl	1 2	66.0%

Vulnerable Devices

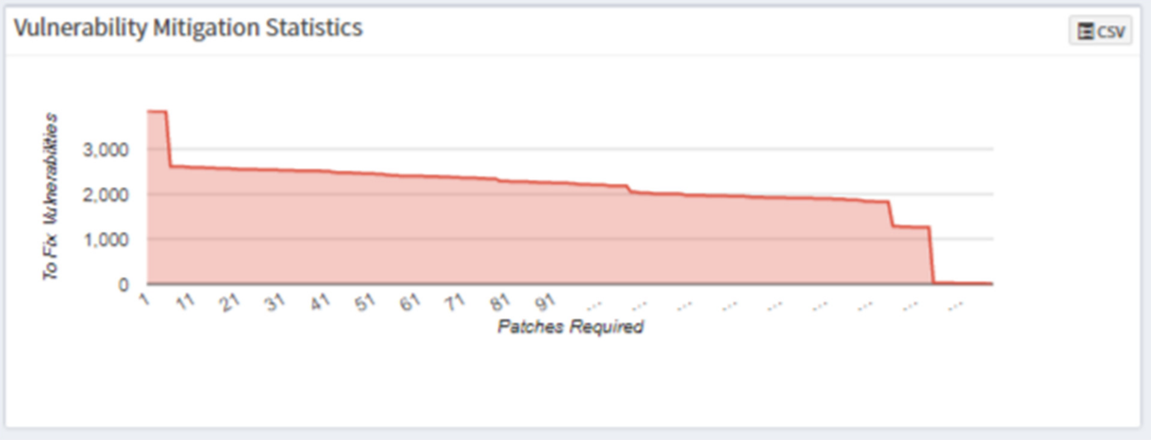
This pane shows the total number of vulnerabilities that a host has, and the severity rating by which they are grouped.


Vulnerable Devices

Host Name	Vulnerabilities	Statistics
secpod	1819	5 259 416 1086
sp-debian-8-x86	1178	4 196 942
qa-cent6.6new	699	58 637
centos-support-6-64bit	155	

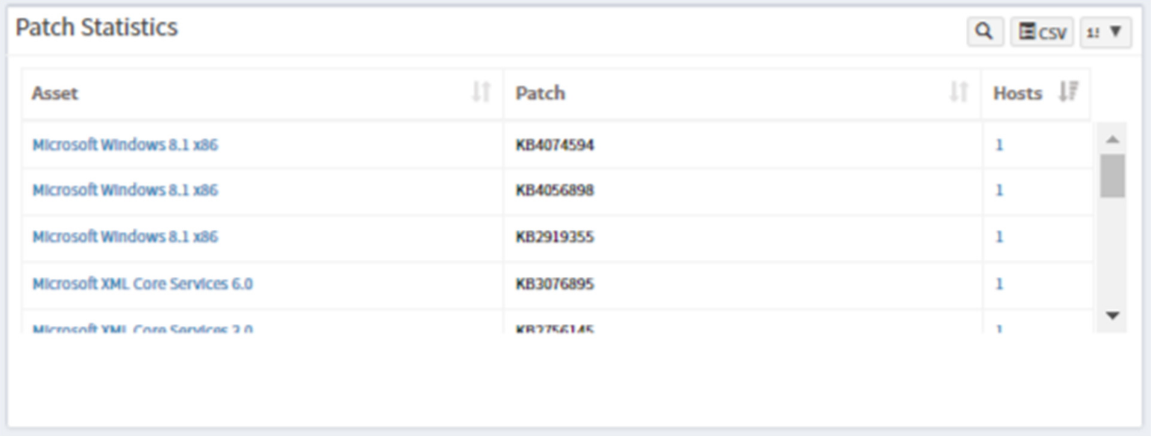
Vulnerability Mitigation Statistics

This pane displays the total number of open vulnerabilities on the network and graphs how the application of a fixed number of patches can bring down the vulnerability statistics correspondingly.



Patch Statistics

This pane displays the missing patches for the software assets and the number of hosts that require the patches. You can click the asset name to view details.



Asset	Patch	Hosts
Microsoft Windows 8.1 x86	KB4074594	1
Microsoft Windows 8.1 x86	KB4056898	1
Microsoft Windows 8.1 x86	KB2919355	1
Microsoft XML Core Services 6.0	KB3076895	1
Microsoft XML Core Services 3.0	KB2756145	1

Setting Alerts for Vulnerabilities

The Alerts feature sends a notification alert to the specified email on detection of new vulnerabilities after a scheduled scan. This setting must be set before the first scheduled scan. The notification for vulnerabilities is based on their criticality.

To set alerts for vulnerabilities

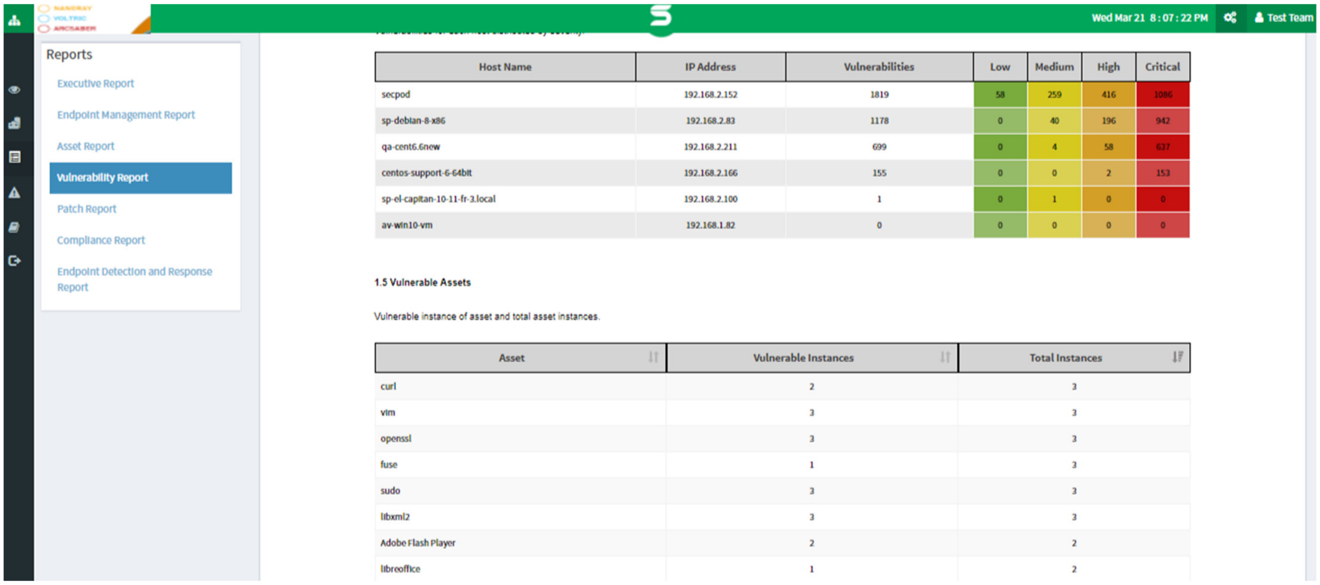
1. Click Alerts on the left pane.
2. Turn on “Subscription Status” to enable vulnerability alerts.
3. Specify an email address to which the alerts will be sent and the category of vulnerability on which notifications will be based. You can also specify a custom condition, based on CVEs.

4. Click Update.

Vulnerability Reports

This report lists vulnerability details based on device groups and specific devices. It includes the vulnerability instances for each vulnerable asset and a description of each vulnerability. Vulnerabilities for each group and host are categorized by severity. The severity of vulnerabilities is represented using color codes:

- Red: Critical
- Orange: High
- Yellow: Medium
- Green: Low



Host Name	IP Address	Vulnerabilities	Low	Medium	High	Critical
secpod	192.168.2.152	1819	58	259	416	1086
sp-debian-8-x86	192.168.2.83	1178	0	40	196	942
qa-cent6.6new	192.168.2.211	699	0	4	58	637
centos-support-6-64bit	192.168.2.166	155	0	0	2	153
sp-el-capitan-10-11-fr-3.local	192.168.2.100	1	0	1	0	0
av-win10-vm	192.168.1.82	0	0	0	0	0

1.5 Vulnerable Assets

Vulnerable instance of asset and total asset instances.

Asset	Vulnerable Instances	Total Instances
curl	2	3
vim	3	3
openssl	3	3
fuse	1	3
sudo	3	3
libxml2	3	3
Adobe Flash Player	2	2
libreoffice	1	2

To generate a vulnerability report

1. Click **Reports** on the left pane.
2. Click **Vulnerability Report**.
3. View vulnerabilities at a glance.

To export the report to a PDF

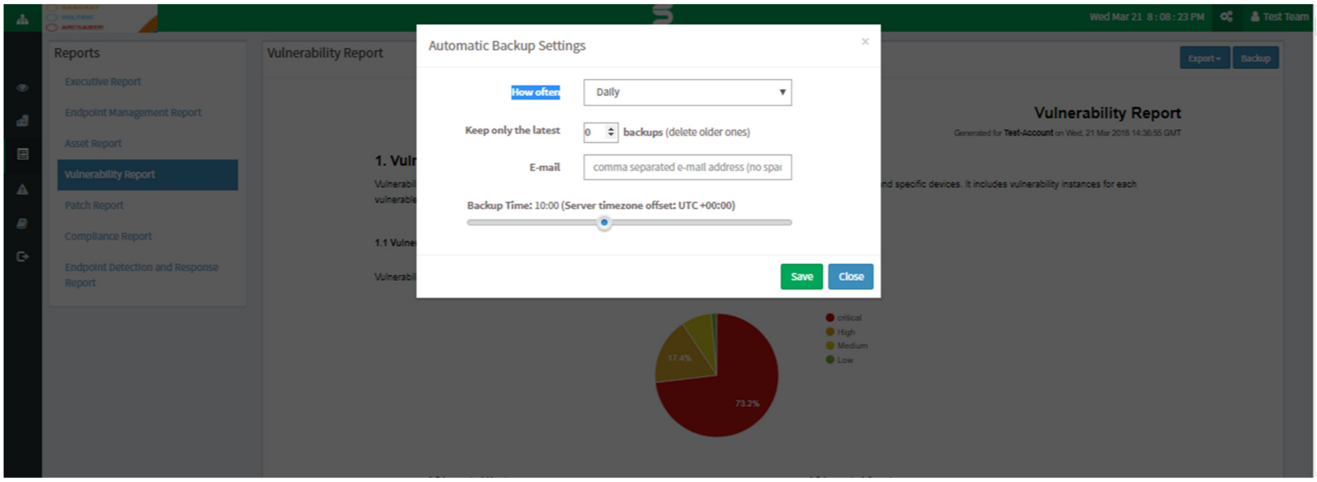
- Click Export > PDF

To export the report and send it via email:

1. Click Export > Email.
2. Specify email addresses.

To Back Up Reports

The backup settings under Reports allow IT administrators to obtain a backup report showing vulnerabilities. The backup time should be scheduled. The backup report can be scheduled to run automatically daily or weekly.



Automatic Backup Settings

How often: Daily

Keep only the latest: 0 backups (delete older ones)

E-mail: comma separated e-mail address (no spac

Backup Time: 10:00 (Server timezone offset: UTC +00:00)

To configure backup settings for reports:

1. Click **Reports** on the left pane.
2. Click **Vulnerability Reports**.
3. Select **Backup**.
4. Specify the frequency of backup in the **How Often** drop-down. You can back up reports daily or weekly. If you choose weekly, you can specify the days.
5. Specify the number of days that a backup should be maintained in the **Keep Only the Latest** box. Files older than the specified value will be deleted. You can maintain backups for a maximum of 30 days.
6. Specify the **Backup Time,** that is, the time when SanerNow will create an archive of the report. Specify **Email** addresses.
7. Click **Save**.

About Us

SecPod Technologies creates cutting edge products to ensure endpoint security. Founded in 2008 and headquartered in Bangalore with operations in USA, the company provides computer security software for proactively managing risks and threats to endpoint computers.

Contact Us

Web: www.secpod.com
Tel: +91-80-4121 4020 | +1-918-625-3023
Email: info@secpod.com