Release Notes SanerNow 5.3

Published Date: Jan 30, 2023

We're excited to bring you our latest release – SanerNow 5.3. In this release, we offer enhancements, new APIs, and bug fixes.

With SanerNow 5.3, we're confident that our product will help you to prevent cyberattacks and empower you to keep your endpoints safe and secure.

What's New in SanerNow 5.3

Enhancements:

- **Force Reboot on Task Completion:** When creating a patching task or a software deployment job, you can now choose 'Force Reboot' as part of the reboot schedule. This will force all endpoints to reboot, irrespective of whether the patch or software update requires a reboot or not.
- **Flexibility to provide a time range for starting a task:** You can now specify a time range during which a patching task or software deployment task is allowed to start. If the device is offline during the start time window, the task will not start and will be reported as "Scheduled missed".
- **Release Date for Vulnerabilities, Patches, and Misconfigurations:** VM, PM, and CM dashboards will now show the release date for vulnerabilities, patches, and misconfigurations. This will help you identify older vulnerabilities, patches, and misconfigurations. And using these insights you can prepare a mitigation plan accordingly.
- **New filter introduced for Vulnerability Aging Graph:** You can now filter the vulnerability aging graph in the VM dashboard by Device detection or Release date.
- **High Fidelity Attacks pane now displays exploitable assets**: We've enhanced the High-Fidelity Attacks pane in the VM dashboard to provide more detailed information by showing exploitable asset names right next to the exploit. This will give you better visibility into specific assets that are vulnerable to attacks, making it easier to prioritize and mitigate potential security risks.
- **Automation tasks shows next start date:** You can now see the next start date for an existing scheduled automation rule in PM and CM tool.
- **New Device status icons –** 'Patch Collection Ongoing' and 'Vulnerability Scan Done' icons have been added under Status section on Managed Devices page. In addition to this, 'Active/In-Active' status icon has been enhanced to show hosts running Windows that

require a reboot.

New Operating System supported: Introducing support for macOS 13 (Ventura)

Tool Revamp:

EQR tool is now replaced with Posture Anomaly – a unique and powerful tool built to detect and fix anomalies in your IT infrastructure. As part of this change, IOA and IOC features are deprecated. Refer Posture Anomaly User guide for more details.

UI Changes:

Alerts for 'Newly Added Devices' and 'Uninstall Agent' have been moved from Endpoint Management tab to Device Management tab on the Alerts page.

REST API Changes:

Here's an overview of the API changes made in SanerNow 5.3.

Newly Added APIs

- **Get Device Job Summary:** The 'getdevicejobsummary' API will retrieve job summary details for a given host.
- **Get Device Job Details:** The 'getdevicejobdetails' API will retrieve all the job details created for a host in a nested model.
- **Retrieve Audit logs:** The 'getauditlogs' API will retrieve audit logs. You can provide various filters including organization, account, user, tool, actions, date range and limit.
- **Retrieve Audit action code and value**: The 'getauditactioncodes' API will retrieve information of all the action codes and values.

Modified APIs

- A new key 'reportapifilters' has been added to the 'getreportapidata' You can now filter based on reference (CVE ID), severity, hosts, families, application, and limit search results.
- A new key 'fixinfo' has been added to the API response of three APIs namely –'getApplicableRemediation', 'getApplicableNonSecurityRemediation', and 'getPatchesForRollback'.
- Two new keys 'forcereboot' and 'startwindowtime' have been added to the following APIs.
    - createFirmwareRemediationJob

- createNonSecurityRemediationJob
- createRemediationJob
- createMisconfigurationRemediationJob
- createPatchRollbackTask
- createMisconfigurationRollbackTask
- addRemediationRule
- updateRemediationRule
- addSoftwareDeployment
- uninstallSoftware

'forcereboot' will mandate all endpoints to reboot, regardless of whether the patch or software update requires a reboot or not. And 'startwindowtime' will provide a time range by when the task must be initiated. This must be used in combination with 'starttime' to provide a time range.

- A new field 'includeDSI' has been added to 'getdevicereport' API. By default, the value for this field will be set to false. If you need Detailed System Information of any device, the value of this key needs to be set to true.
- A new key 'installoption' has been added to 'uploadcompressedfile' API. You can now specify command-line install options for installers that are in zip format.
- Existing key 'edr' has been replaced with 'postureanomaly' for both request and response for 'updateServiceProvision' and 'getServiceProvision' APIs.

Deprecated APIs

- 'addremediationjob' API has been deprecated. Instead, you can use 'createremediationjob' and 'createmisconfigurationremediationjob' for creating remediation jobs in PM and CM tools.
- 'deleteremediationjob' has been deprecated. Instead, you can use 'deleteremediation' API for deleting remediation jobs in PM and CM tool.
- 'getallapplicableremediation' has been deprecated. Instead, you can use 'getapplicableremediation' and 'getapplicablemisconfigurationremediation' to get applicable remediation for PM and CM tools respectively.

Report API Changes

- We've introduced two new report APIs under VM that provide Aging graph based on Detected Date and Release Date.
    - Vulnerability Aging Graph (Detected Date)
    - Vulnerability Aging Graph (Release Date)

- We've introduced two new report APIs under PM that provide reports on Security Patches based on vendors.
    - Linux Vendor Security Patches
    - MAC Vendor Security Patches
    - Microsoft Windows Vendor Security Patches
    - Third-Party Security Patches
    - Security Patches by Vendor Graph
    - Vendor and Third-Party Patches Graph

- We've added a new column "Release date" to the below mentioned custom reports. This will help in identifying the release date for patches and misconfigurations.
    - Vulnerability Management
        - All vulnerabilities
    - Patch Management
        - Missing Patches
        - Top 10 Critical Missing Security Patches
        - Non-Security Patches Details
        - Outdated Asset Patches
        - Outdated OS Patches
        - Missing Patches of Non-Reachable Devices
        - Missing Configurations
        - Misconfiguration Fixes of Non-Reachable Devices
    - Compliance Management
        - Missing Configurations
        - Outdated OS Misconfiguration Fixes
        - Misconfiguration Fixes of Non-Reachable Devices

- We've added a new filter 'Vendor' to the following custom reports.
    - 'Missing patches' report under PM. You can now filter missing patches based on the vendor.
    - 'Missing configurations' report under CM. You can now filter missing configurations based on the vendor.

- New columns have been added for the following reports:
    - Report Name: Patch Based on vendor.
    - Columns added:
        - Patch Names
        - Asset Count
        - Asset Names
        - References Count
        - References
        - Host Count
        - Family Count
        - Family Names

    - Report Name: Most Critical Patches
    - Column added:
        - Detected Date and Size

We're confident that you will enjoy using SanerNow 5.3. Our teams are constantly working on new features that will be part of our future releases. In the meantime, if you can think of any cool feature or have an enhancement suggestion for SanerNow, don't hesitate. Just send us an email to support@secpod.com, and we'll certainly look into it.