Release Notes SanerNow 5.2

We’re excited to announce our new release SanerNow 5.2. With a goal of elevating security while using SanerNow, we have enhanced authentication by supporting Single Sign-On (SSO) and multiple vendors for Multi-factor Authentication (MFA). We have introduced the ability to exclude patches and vulnerabilities from reporting and also introduced support for SUSE Enterprise Linux OS based on user requests. The release comprises a lot of enhancements and updates to make your SanerNow experience much more seamless. Read on for further details,

New Features:

- **Introducing Single Sign-on (SSO) for secure and seamless authentication:** Based on SAML V2, we are offering SSO capability that supports integration with all SAML v2 supported identity providers, including PingID, PingFederate, AWS, Azure, Auth0, and Okta. To know how to configure SSO, check out the technical guides listed **here.**
- **Supporting additional Multi-factor Authentication (MFA) providers:**
    - PingID
    - Okta
    - TOTP Authenticator Apps

      To know how to configure MFA, check out the **technical guide.**
- **New Operating System Support:** Introducing support for SUSE Linux Enterprise Server (SLES) 12 and 15
- **Introducing Policy to Exclude Vulnerability from reporting:** You can now exclude/remove vulnerability from reporting after accepting exclusion risk criteria. The exclusion policy can be applied for a single vulnerability, multiple vulnerabilities, or all vulnerabilities for an asset. To know how to exclude vulnerability from reporting, check out the **article.**

- **Introducing Policy to Exclude Patch from being considered for a patching job or rule:** You can now configure an account-wide policy to exclude the patch from listing while creating a patching job or rule. If a patch is not approved or if you would want to prevent OS or service pack upgrades, or if there are development tools that you do not want to update, an exclusion policy can be applied. To know how to exclude a patch from being considered for the patching rule, check out the **article.**

- **Remediating vulnerabilities from Vulnerability Management (VM)**

Dashboard: You can now create a remediation job to fix critical or all vulnerabilities from the Vulnerability Details table in the VM dashboard. A remediation job can be created right within where vulnerability is detected.

- **Introducing vulnerability search based on exploit-specific keywords:** The search can be performed with exploit/malware-specific keywords to quickly act upon those vulnerabilities that are already being exploited in the wild. You can also search by keywords such as "CISA" and "NSA" etc.

- **New icon to highlight Vulnerabilities that are linked to High Fidelity Attack:** Vulnerabilities table and All Vulnerabilities view under VM Dashboard will now have a new icon to indicate Vulnerabilities linked with High Fidelity Attack.

- **Introducing the "All Vulnerabilities" dashboard in VM:** You can now gain better visibility of all the discovered vulnerabilities with easy-to-use search and filter controls in a separate full-page view.
- **Ability to Feed the Activation Token Separately while Installing Agents:** To facilitate users to use the same agent installer for different accounts, we have introduced the ability to feed the activation token separately through the installer command line option. Now, the agent installer is the same even though there are multiple accounts within an Organization.

Enhancements:

- **Providing Detailed Info on CVE ID:** You can now view detailed info of a CVE/SVE/Vulnerability-ID like, Description, CVSS Score, and References through a pop-up by clicking CVE/SVE/Vulnerability ID.
- **Support for Devices with dynamic MAC addresses:** You can now manage devices with dynamic MAC addresses and multiple devices having the same MAC address across different networks.

Rest API Changes:

Adding New API

- **Retrieve job information for a device:** The "getDeviceJobInfo" API is added to retrieve

all the job information for a device.

- **Get account name for a device:** The “getDeviceAccountInfo” API is added to retrieve the Account Name for a Subscriber ID.
- **Get activation conf file for an account:** The “getagentactivationconf” API is added to get the activation conf file for an account.

Deprecated APIs

- Build Management APIs “getbuildstatus”, “createbuild” and “updatebuild” have been deprecated. We no longer need to create, update or get build status for an account.

Report API Changes

- Introducing New Report API “Vulnerabilities with Patches” under VM. This report provides a list of vulnerabilities for which patches are available.
- Devices with Missing Security Patches report has been enhanced to include additional fields – Risk Count, Risk Severity Count, Last Scan, and Last Seen.
- Following Device-specific Report APIs are now grouped under “Device Info” and can be accessed with any one of the tool provisioned (VM, CM, PM, AE, EM and EQR)
    - “All Devices”, “Device Details Summary”, “Device Types, Device based on Family”, “Device based on Groups”, “Device based on OS”, “Device based on Subnet”, “Network Type”, “Newly Added Devices”, “Not Scanned Devices”, “Currently Monitored Systems”, “Hardware Asset”, “Device Details”, “BIOS – Linux”, “BIOS – Mac”, “BIOS – Windows”, “DNS – Linux”, “DNS – Windows”, “Disk – Linux”, “Disk – Mac”, “Disk – Windows”, “Families of Operating Systems – All”, “Group – Linux”, “Groups – Mac”, “Groups – Windows”, “Network Interfaces – Windows”, “Operating System Information – Linux”, “Operating System Information – Windows” and “Operating System Information – Mac”.

Along with these new features and enhancements, this release includes user experience enhancements and bug fixes as well.

Contact Information

We hope SecPod SanerNow 5.2 will make your cyberattack prevention journey more effective. We have our journey ahead and already set our minds on what is coming next. Until then, please mail us at support@secpod.com for any feature requests or enhancements you expect in the product. To learn more about SecPod, visit www.secpod.com.