Seqrite
eXtended Detection and Response

SEQRITE

Release Notes

v2.3 18 Sept 2024

www.seqrite.com

Copyright Information

Trademarks

License Terms

Content

Seqrite XDR

Seqrite XDR, Extended detection and Incident Response Solutions, helps you monitor your network for any signs of active cyber threats and respond appropriately. Seqrite XDR facilitates proactive threat detection, investigation, and effective remediation to modern day cyber threats. Seqrite XDR supports threat hunting, system and custom alerts, detailed alert analysis and high-level reports that give you a bird’s eye view of the organization’s security posture. Seqrite XDR brings stability, reliability, security, and an intuitive UI.

Features released in Seqrite XDR 2.3

Introducing SKU: EDR Advanced

EDR Advanced: XDR has introduced a new version called EDR Advanced. It's a simpler variant focusing on essential features for a better user experience. Although it doesn't have Playbook and Connector features, it's crafted to provide focused solutions tailored to individual user requirements.

OS Tagging for Detection Rules

New Filtering Option: Users can now filter detection rules by operating system (OS) on the rules list page. This enhancement allows for more efficient management and organization of rules based on the OS.

Alert Description on Incident List Page

Enhanced Incident Details: The incident list page now includes an alert description column. This addition provides users with a summary of each alert, facilitating better and quicker analysis of incidents.

Hostname Filter for Incident Page

Hostname Filtering: Users can now filter incidents by hostname on the incident list page, enabling more precise incident management.

Filter Data Retention During Navigation

Persistent Filter Settings: Alert filter settings are now retained throughout a single user session, ensuring that filter preferences remain consistent as users navigate between pages

Immediate Remediation Action Enhancement

Introduced advanced capabilities for immediate remediation actions. The system now efficiently restricts potentially infected hosts and facilitates automated or manual response actions to mitigate threats swiftly.

Action Policy Orchestration and Risk-Based Response

Enhanced support for both real-time and offline response policies. The update includes a refined scope for risk-based auto-responses, allowing for the application of generic or custom policies tailored to specific risk scenarios.

Alert Generation Time Improvement

Optimized the alert generation time to ensure that users receive timely notifications about anomalies. This improvement aims to enhance the overall responsiveness and effectiveness of the XDR system in identifying and addressing potential threats.

Usage Information

- Microsoft has deprecated support for SHA-1 and recommends using only SHA-2 signed certificates for its OS updates. Accordingly, the SHA-1 certificates that Seqrite was using expired on 4th June 2021, so the following operating systems are not supported unless the appropriate patches are applied.
    - Windows Vista – Not supported
    - Windows Server 2008(below R2) – Not supported
    - Windows 7. To continue using this operating system without any issues, please apply "KB4474419" and "KB4490628" service packs.
    - Windows Server 2008 R2. To continue using this operating system without any issues, please apply "KB4474419" and "KB4490628" service packs.
- All process events whose process create event is older than 30 days, return a "No data found" error in response and Alerts are not generated for these processes even though corresponding rule may exist.

Technical Support

Seqrite provides extensive technical support for its users. In case you face any technical issue, you can contact our Technical Support center using the options available at the following URL:

https://www.seqrite.com/seqrite-support-center