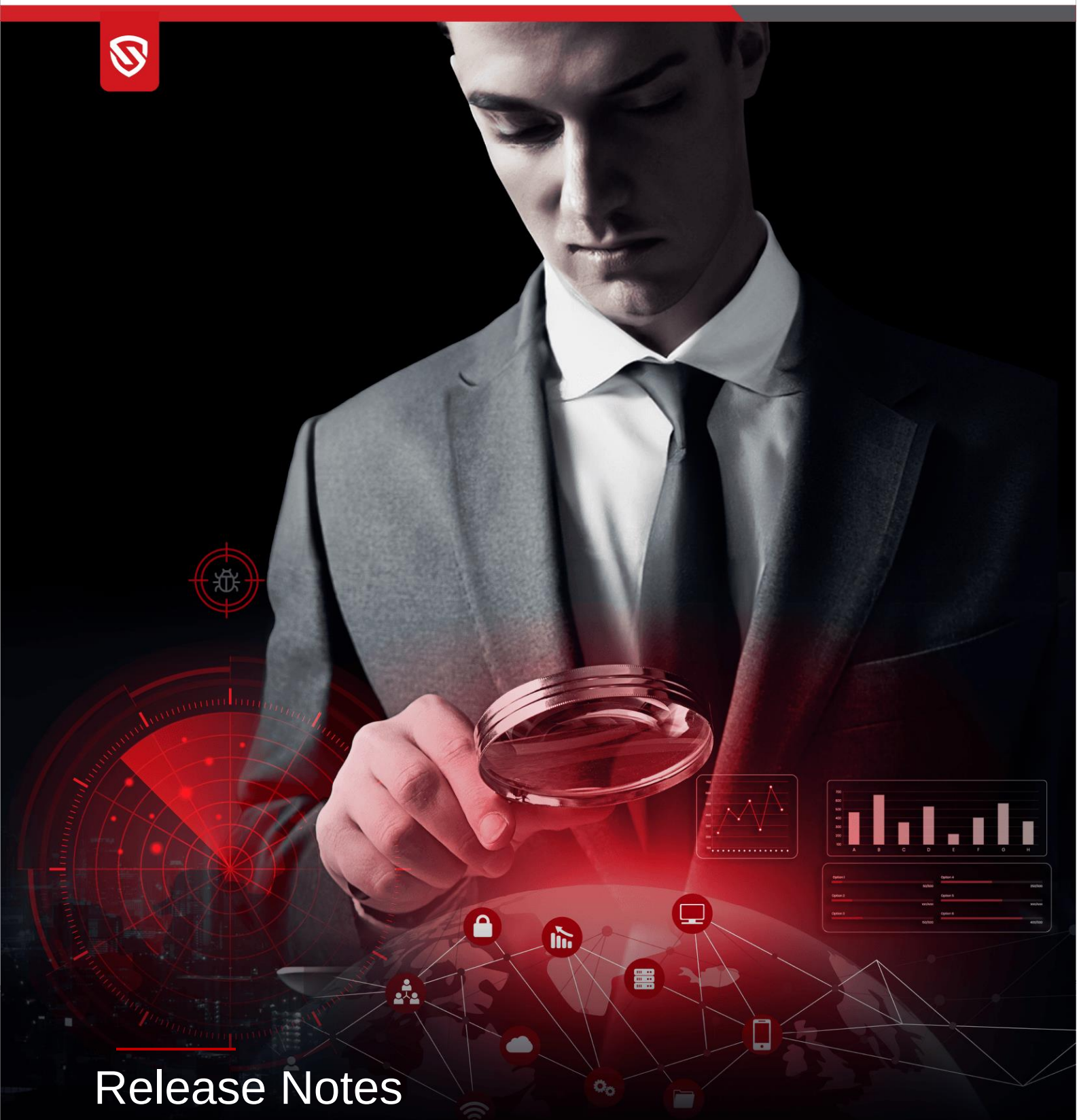
Seqrite eXtended Detection and Response



Release Notes

v2.1.5 | 6 Apr 2024

www.seqrite.com

Copyright Information

Trademarks

License Terms

Installation and usage of Seqrite Endpoint Security is subject to user's unconditional acceptance of the Seqrite end-user license terms and conditions.

To read the license terms, visit http://www.seqrite.com/eula and check the End-User License Agreement for your product.

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 2.1.5

Endpoint List View

A new list view is introduced for better visibility of critical endpoints.

Incident Management Enhancements

Users can now select and close multiple incidents simultaneously, particularly useful for handling false positive cases efficiently.

Improved Alert Generation Time

Critical rule alert generation time has been enhanced to up to 5 minutes, enhancing performance and responsiveness.

Playbook Enhancements

Playbook functions now include IP reputation and endpoint profiling changes, improving response capabilities.

Alert Summary Enhancement

When users navigate to the alerts list from an incident, the alert summary will now include the correlation rule name and description. Correlation rules serve as the basis for associating alerts with incidents.

Agent Communication Service (ACS) Integration

The sensor is now integrated with ACS functionality, facilitating remote management such as upgrades and uninstallations without manual intervention.

Enhanced File Event Capture

File deletion events on shared folders are now captured, enhancing monitoring capabilities.

Enhanced Visibility: Current Working Directory Attribute in Linux Sensor Process Events

Current working directory attribute is now included in Linux sensor process events, enhancing visibility.

MAC Sensor Enhancements

- File I/O information (MAC)Multiple new attributes are now added to File events in MAC sensor.
- Terminal Command Capture (MAC)Process events now include the command executed for running the process.

Introducing the New 'Brand Seqrite'!

In this release, introducing a comprehensive rebranding initiative featuring new product names and logos. This update introduces the following key highlights:

- Effective April 8, 2024, we have refreshed our brand to simplify cybersecurity, making it easier for users to navigate. This includes streamlined product names for a more intuitive experience.
- The **HawkkHunt XDR** product name has been retired and replaced with **Seqrite XDR** to align with industry standards, offering users a clearer understanding of our cybersecurity solutions. The updated product name is reflected in both the Seqrite Universal Agent and the Add/Remove programs.
- Rest assured, despite the brand refresh, our commitment to providing reliable and top-notch security remains unchanged. The Seqrite team continues to prioritize your protection with robust and dependable solutions.
- Take the opportunity to explore 'Brand Seqrite' and discover how our revamped brand can empower your business to thrive in today's ever-changing digital landscape.
  Learn more about the change here.

Event Data Storage for 7 Days

Starting from this release, event data from endpoints will now be stored for 7 days, for analysis and threat hunting capabilities. Note: There is no change in alert data retention period.

Known Issues

Here are the known issues in version 2.1.5:

- In MAC, file operations performed manually through GUI are not captured.
- File delete event is not captured when deleting a Windows shared file from a Linux machine.

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