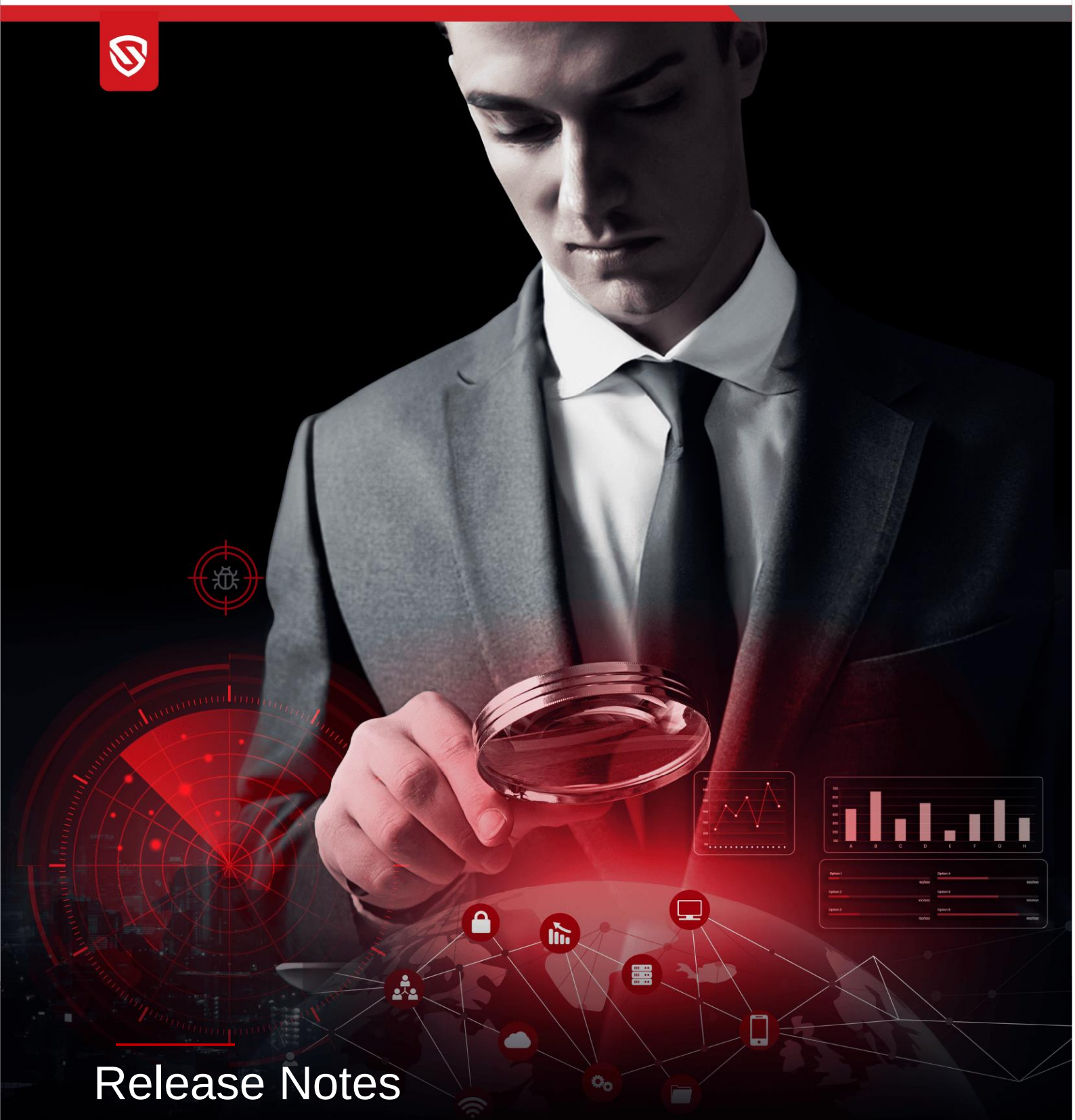
Seqrite
eXtended Detection and

SEQRITE



Release Notes

v2.1 | 11 Aug 2023

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

1. Seqrite XDR 4
   Features released in Seqrite XDR 2.1 4
2. System Requirements 5
3. Known Issues and Identified Behaviors 6
4. Technical Support 7

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

Live Query

Enables obtaining the real-time, latest, specific, and detailed information from the endpoints, augmenting the existing information. The Live query feature helps reduce the visibility gap by obtaining the most up-to-date endpoint status information.

Seqrite XDR as a Standalone Product

Introducing Seqrite XDR as a standalone product, independent of EPS, to complement the existing Seqrite Centralized Security Management product line.

Improved Visibility: From displaying IP addresses to showing URLs

More user-friendly URLs have been substituted for IP addresses to enhance the user experience.

Improved Correlation for Outlook Activity

Enhanced correlation to accurately track Outlook attachments and clicked links as Outlook-initiated activities, providing a more comprehensive view of user interactions.

Improved Incident Alert Source Field

The type field in incidents will now reflect the alert source from the first alert added, ensuring better visibility and clarity in incident management.

Automated Attribute Search with Connector

Introducing an internal block function enabling automated URL, IP, and MD5 hash search on recent events (last 24 hours), generating specified severity alerts for matched events. Empower your cybersecurity with enhanced automation and threat detection.

Incident Audit Log Enhancements: Internal Block Calls Added

- Added logging for internal block calls to the Incident audit log.
- Internal block calls now include logging for all update functions' responses.

System Requirements

The Seqrite XDR client supports the following Windows operating systems:

Operating System	Minimum System requirements
Windows 10	Processor: 1 gigahertz (GHz) or faster RAM: 1 gigabyte (GB) for 32-bit or 2 GB for 64-bit
Windows 8.1 / Windows 8	Processor: 1 GHz or faster RAM: 1 GB for 32-bit or 2 GB for 64-bit
Windows 7	Processor: 1 GHz or faster RAM: 1 GB for 32-bit or 2 GB for 64-bit
Windows Vista	Processor: 1 GHz or faster RAM: 1 GB
Windows Server 2003	Processor: 550 MHz for 32-bit or 1.4 GHz for 64-bit RAM: 256 MB for 32-bit or 512 MB for 64-bit
Windows Server 2008 R2/ Windows Server 2008	Processor: 1 GHz for 32-bit or 1.4 GHz for 64-bit RAM: Minimum 512 MB (Recommended 2 GB)
Windows Server 2019, Windows Server 2016, Windows Server 2012 R2/Windows Server 2012	Processor: 1.4 GHz Pentium or faster RAM: 2 GB

The Seqrite XDR Linux Sensor supports the following 64-bit Linux distributions:

- Red Hat Enterprise Linux (RHEL) 7.2
- Red Hat Enterprise Linux (RHEL) 8.1
- Red Hat Enterprise Linux (RHEL) 9.1
- openSUSE 15.1
- Ubuntu 19.04
- Ubuntu 20.04
- Ubuntu 22.10

Known Issues and Identified Behaviors

Here are the known issues and identified behaviors in the Seqrite XDR 2.1 version:

- **File Alerts: Alert Analysis and Remediation Limitations only for Linux OS**
  In the current release of Seqrite XDR, the alert analysis and remediation functionality for file alerts is not supported specifically on Linux operating systems. However, users can still leverage the threat hunting feature to investigate file events on Linux.

- **Limited File Event Logging for Move to Trash and Restore from Trash Operations**
  File events are not logged for the move to trash operation and the restore from trash operation.

- **Status of Remediation Action for Second Alert in Linux Alert Remediation**
  In the context of Linux alert remediation, in a scenario where the process remains consistent for both alerts, if the remediation action for the first alert is successfully executed, the status of the remediation action for the second alert will be either marked as "Ignored" or "In Progress" on the user interface.

- **macOS Remediation Scope and Limitations**
  macOS remediation is available for processes only.

- **Linux Persistence Development and Playbook Scenario Challenges**
  The UI cannot display the reboot and isolated statuses due to the unavailability of persistence in Linux. Additionally, when executing the playbook for Host remediation actions, there might be failures in isolating and rebooting the host.

- **Linux UI Reboot Issue and Status Display**
  Initiating a host reboot remediation action through the UI will successfully reboot the host machine. However, there might be a failure in updating and displaying the reboot status on the UI.

- **Unsupported OS Queries Upgrade for Mac OS Ventura with M1 and M2 Chips**
  For Mac OS Ventura distros with M1 and M2 chipsets, the upgrade of OS queries is not supported.

- **Missing App Launch Events for Certain Processes in Mojave**
  For the Mojave app launch events are not properly generated for some of the processes. For instance, the creation events of apps like Calculator or Notes are not being captured.

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