Seqrite eXtended Detection and

Release Notes

v2.1.3 | 15 Dec 2023

www.seqrite.com

Copyright Information

Trademarks

Seqrite is registered trademarks of Quick Heal Technologies Ltd. while Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and product titles are trademarks of their respective holders.

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 2.1.3

Enhanced Network Protocol Event Capture

- The sensor now intercepts and captures key attributes of various network protocols, including SMB, Http, Https, and ICMP.
- Major SMB commands such as SESSION_SETUP, LOGOFF, TREE_CONNECT, TREE_DISCONNECT, CREATE, READ, WRITE, and QUERY_INFO are now captured.
- Outgoing Ping command details are captured for ICMP.

Digital Signer Information Capture

The sensor gains the capability to capture Digital Signer Information, certificate validity, and related details for executed processes.

Comprehensive Script Execution Capture

PowerShell commands, Command line scripts (both inline and script files), and Python commands are now captured.

Loading of Python libraries like GZip and Ping3 is also logged.

Windows Event Logs Capture

Specific Windows events relevant to EDR detection and remediation are now captured by the sensor.

Linux Originated Attack Tracking

The sensor is now equipped to track attacks originating from Linux-based hosts.

File Lateral Movement Capture

File movements between endpoints and shared/network drives are captured by the sensor, enhancing lateral movement detection.

Single Risk and Importance Scores for Managed Endpoints

With the latest update, each managed endpoint will now feature a singular risk score and a singular importance score. This enhancement aims to simplify the assessment process, providing a clear and concise overview of the risk and importance associated with each endpoint. Users can now easily prioritize and address potential issues, making the management of endpoints more efficient and intuitive.

Scheduled Report Delivery in Selected PDF or Excel Formats via Email

Introducing an advanced scheduling feature for reports, now available in Dashboard, Incidents, Alerts, and Threat Hunting. Users can seamlessly schedule and send reports in their preferred PDF or Excel format through email. With the addition of set frequency options, this enhancement provides a powerful tool for automating and optimizing your reporting workflows. Stay organized and informed with scheduled reports tailored to your specific needs.

Note: It is recommended to obtain the latest Seqrite Universal Agent installer from Seqrite Centralized Security Management after each new release to ensure optimal performance and avoid potential issues. An outdated installer may cause compatibility issues or limit functionality.

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 2.1.3 version:

- **File Event Capture Limitations**

  Deletion, modification, and changes to file attributes are currently not captured by the system. We are actively working to enhance file event monitoring in future releases.

- **File Privilege Attribute Omission**

  The file privilege attribute is not captured in file events. This exclusion is acknowledged and will be addressed in upcoming updates.

- **Shared Drive Movement Details**

  When files are moved between the host and a shared drive, the shared drive letter is not captured in the events. We recognize this limitation and plan to incorporate this information in subsequent releases.

- **Regex Operations in Windows Events**

  The rule builder currently lacks support for regular expression (regex) operations in Windows events, specifically for the Windows Message attribute. We understand the importance of regex operations and aim to integrate this functionality in future iterations.

- **HTTP 404 and 405 Responses Not Captured for Threat Hunting Purposes**

  Http Incoming Requests with 404 and 405 responses are not being captured for threat hunting purposes. This issue has been acknowledged and will be addressed in the upcoming release.

- **Synchronization Delays Between Seqrite Centralized Security Management and Seqrite XDR Importance Scores**

  The Importance Score in Seqrite XDR may not immediately reflect changes made in Seqrite Centralized Security Management, resulting in synchronization delays between the two interfaces. The expected behavior is for the Importance Score to seamlessly update across both Seqrite Centralized Security Management and Seqrite XDR. However, real-time synchronization may experience delays until the next alert generation in Seqrite XDR.

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