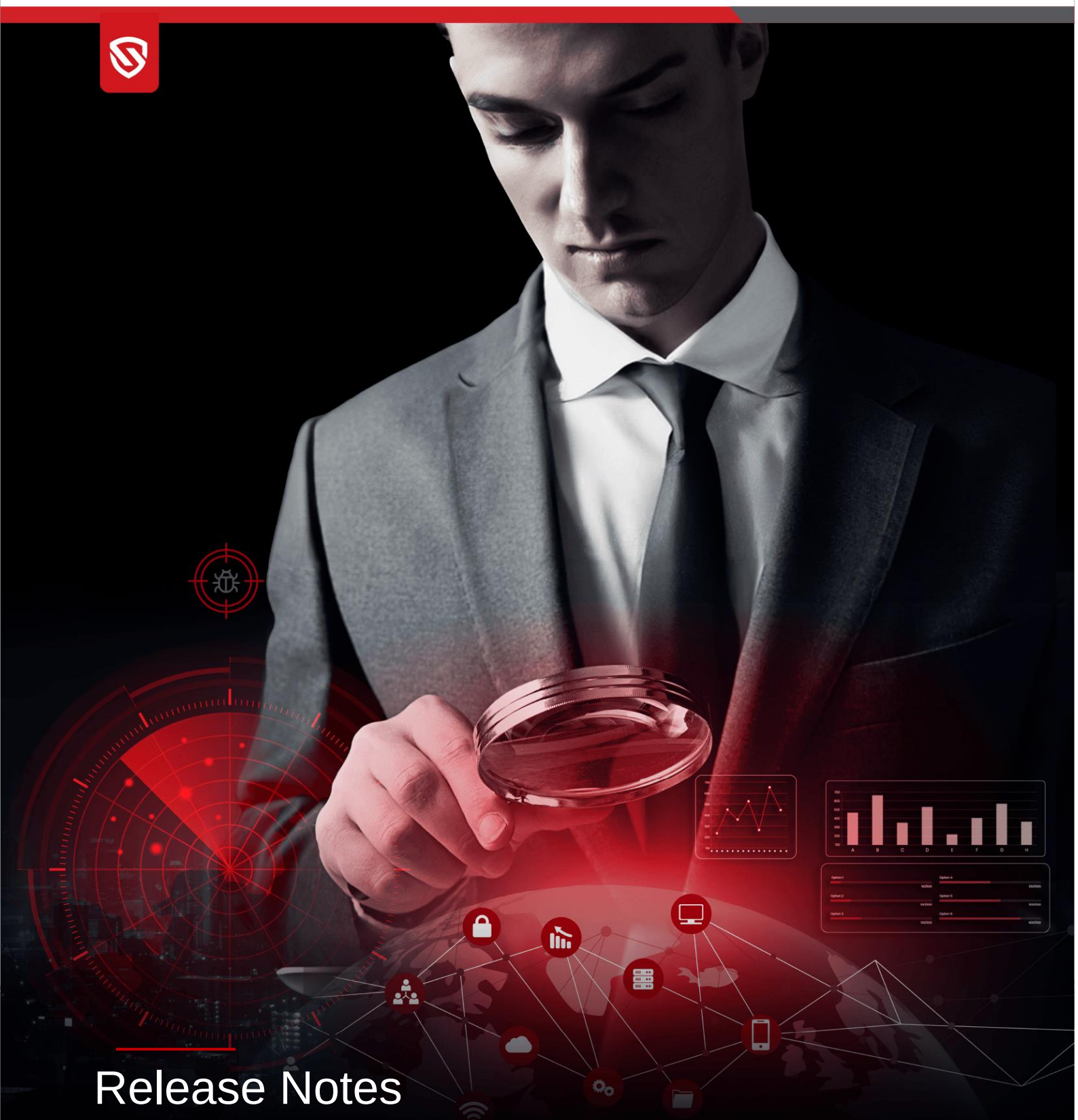
Seqrite eXtended Detection and Response



Release Notes

v2.3.1 | 29 Nov 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 2.3.1

Enhanced Incident Closure and Filtering Options

Seqrite XDR v2.3.1 introduces new features and enhancements for management of the incident statuses:

1. **New Incident Closure Options**:
    - Two new status options available, **True Positive** and **Suspicious Threat**, for choosing while closing incidents.
2. **Updated FP Rate Widget**:
    - The FP rate widget is displayed as Closed Incident Summary on the dashboard.

New Fields in Rule Builder

We have introduced two new operators, **Regex** and **NOT Regex**, to enhance rule creation for the following attributes:

- **nw_local_ip**: Local network IP addresses
- **nw_remote_ip**: Remote network IP addresses

Key Features:

- **Regex Operator**: Define complex patterns for IP address ranges, allowing for more flexible and precise rule configurations.
- **NOT Regex Operator**: Exclude specific IP address patterns, refining the scope of rules by effectively omitting undesired IP ranges.

These additions provide greater control and customization in managing network rules.

Deleting the Attachments in Closing Incidents.

Delete Button: Users can now delete uploaded attachments, providing greater flexibility and control over the attached files.

The delete history will be displayed in the Audit Trail.

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