SEQRITE
HawkHunt

Detection, Analysis, and Response against Advanced Threats

Release Notes

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 HawkkHunt

Seqrite HawkkHunt helps you monitor your network for any signs of active cyber threats and respond appropriately. Seqrite HawkkHunt facilitates proactive threat detection, investigation, and effective remediation to modern day cyber threats. Seqrite HawkkHunt 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 HawkkHunt brings stability, reliability, security, and an intuitive UI.

Features released in Seqrite HawkkHunt 1.2.1

Host Isolation/Reconnect

This feature helps to isolate an endpoint from the network if a suspicious activity is detected in that endpoint. This helps in preventing any lateral movements of suspicious activity in the network.

The feature also helps to reconnect the endpoint in the network once the investigation of the activity is complete.

Features released in Seqrite HawkkHunt 1.2

- Alert and alert analysis
  - Alert Management - Bulk action
  - Addition of alert category
  - Filtering System and custom alerts
- Report
  - Auto scheduling of reports email

Alert and alert analysis

Alert management - Bulk action

- User can select multiple Alerts at a time and perform the bulk actions on them.
- Bulk actions supported for selected alerts are like assigning alerts to a user, changing their severity and /or status.

Addition of Alert Category

- Apart from severity of alerts, the alerts can be filtered based on category as **Severe** or **Informative**.
- All the high, medium, and low severity type alerts fall under **Severe** category.
- All the alerts that give information and not severe for investigation fall under **Informative** category.

Filtering System and Custom Alerts

- You can filter the alerts generated according to their type, alerts using **System rule** or **Custom rule** available in the Filter section.

Report

Scheduling of reports

- You can schedule report and sent to added email addresses daily, weekly, or monthly in the PDF or Excel sheet format.

Notes

- A maximum of 10k records is displayed on the console for any DB query.
- Report received through email scheduling will be as per IST time zone and email will be received at 6 AM IST by the recipient on the scheduled day.

System Requirements

System requirements for Seqrite HawkkHunt client are as follows:

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

Supported Web Browsers for HawkkHunt Console

HawkkHunt Console will run on any one of the compatible, HTTPS enabled web browsers listed below, regardless of operating system.

Desktop/Laptop web browsers

- Google Chrome 96, 95, 94
- Mozilla Firefox 95, 94, 93
- Microsoft Edge 96, 95, 94

For all browsers

- HTTPS protocols must be enabled
- JavaScript must be enabled
- Cookies must be enabled
- Images must not be blocked

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