SEQRITE HawkHunt

Detection, Analysis, and Response against Advanced Threats

Release Notes

V 1.1

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.

Contents

Features of 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 & custom alerts, detailed alert analysis & 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.

Here is a summary of new features in Seqrite HawkkHuntv1.1:

- Alert and alert analysis
  - Alerts Whitelisting
  - Selecting the View duration
  - Additional remediation action - Quarantine
- Threat hunting
  - Data retention window of 30 days
- Report
  - Exporting reports
  - Change the granularity of view of reports

Alerts and alert analysis

Alerts Whitelisting

- Alerts are generated based on default rules specified in the HawkkHunt engine and displayed on the dashboard.
- You may come across some alerts that are triggered by valid activity in your network that may seem a false positive in your network.
- Alerts can be Whitelisted. After an alert is Whitelisted, future alerts with same information will also be Whitelisted. A whitelist rule allows you to specify a combination of parameters to whitelist the generated alerts. Any alert that matches the whitelisted rule is displayed under the "Whitelisted alerts view" tab.
- This feature will help you to reduce number of alerts to be analyzed by IR team.

Selecting the View duration

- Filtering helps to narrow down the search criteria for alerts.

- With this you can filter alerts by following hours, days, weekly or monthly slots:
    - Last 1 hour
    - Last 3 hours
    - Last 6 hours
    - Last 12 hours
    - Last 24 hours
    - Today (Since midnight 12.00 AM)
    - Last 7 days
    - Last 15 days
    - Last 30 days
    - This week (since Sunday midnight 12.00 AM)
    - This month (since beginning of the month)

Additional remediation action - Quarantine

- Apart from regular remediation actions like kill or delete now you can also quarantine files on host PC for further analysis.
- The Quarantine action will ensure that the process will not be launched by the file next time. You can restore a quarantined file anytime using the Restore button.

Threat hunting

Data retention window of 15 and 30 day period

- Previously threat hunting and analysis was possible only for a 7 day period. Now you can perform the same actions on 15 and 30 days data.
- This will give you more context to co-related events happening in your network.

Reports

Exporting reports

- You can now export reports in the PDF or Excel format as required for the selected time frame using the Export as button.

Change the granularity of view of reports

- You can change view of reports by filter with Last 7 Days, Last 15 Days and Last 30 Days.

Minimum system requirements

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 /Browsers

The following browsers are supported:

- Firefox
- Google Chrome
- Microsoft Edge

Notes

- You can add alerts only to the Whitelist. You cannot edit a Whitelisted alert rule. You can delete and write a new rule if you want a modified rule.
- 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 is using currently will expire on the 4th June 2021, after which the following operating systems would not be 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.
- A maximum of 10k records is displayed on UI for any DB query.