SEQRITE

HawkHunt XDR

Extended Detection and Incident Response Solutions

Release Notes V 2.0

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 HawkkHunt XDR

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

Features released in Seqrite HawkkHunt XDR 2.0

Dashboard

Three Dashboards have been added targeted at the three personas – Administrator, SOC Manager and SOC Analyst.

The Dashboard shows various graphs and tables based on the user roles that give an overall picture of the current possible incidents. The Dashboard provides,

- Overall incident summary
- Incidents Rate
- False Positive Rate
- ROI
- Analysts Allocation
- Average time required to remediate incidents

Dashboards provide a holistic view of the state of Security operations and Security Incidents for the organization.

Threat Hunting enhancement

New IOCs indicator filters added

The enhanced Threat Hunting feature provides new IOC indicator filters as follows,

- Registry Key
- Registry Value

With these filters, you can create, run, and save a query to search the IOCs. If the matching alerts and processes are present, then a Security Operations Manager gets a list of endpoints where the alerts and processes are available. A user gets navigated to the endpoint view, by clicking on any one endpoint.

Alert-Incident Association updates

In the threat-hunting endpoint view, the Security Operations Manager can verify and manage the alerts-incident association with the help of the newly added 'Associated to' field.

A Security Operations Manager can utilize this functionality to associate the alerts with an existing Incident, or associate it with a new Incident with the help of the ‘Associate to Incident’ and the ‘Create New incident’ options respectively.

Scanning of external IOCs

This feature enables fetching external IOCs and searching those IOCs through the last 30 days’ events to generate alerts over a match. It also supports the external IOC alert identification by source name as "IOC".

Threat search with incident key attributes

Ability to perform threat search directly by clicking on incident key attributes.

Playbook enhancements

Following are the playbook enhancements,

- When any playbook executes, an output message is displayed in the output window.
- Also, now several new functions are available in the playbook Internal block, for adding more flexibility to playbook orchestrations.
- Email notification enhancements within the playbook.
  Email notification through playbook with dynamic content calculated for the fields like an email subject, email recipients, Input, Incident, Incident Alert, and Block based on the context.
- Operational changes while creating and executing the playbook.

Remediation enhancement

Now, a user can perform the following remediation actions through playbooks,

- Host Reboot (newly introduced)
- Host Isolation
- Host Reconnection
- Process Kill
- Process Quarantine
- File Quarantine
- Registry Delete

New Integrated Connector

- Network Connectors
- Additional email connectors

Up to 180 days of events data storage

SHH-XDR facilitates data storage for up to 180 days, depending upon the selected License type.

Features released in Seqrite HawkkHunt XDR 1.3

Incident Management

Incident Management combines multiple alerts to a single incident and prioritizes the incident based on pre-defined rules. This facilitates the incident handler to look at a smaller, prioritized set of incidents to respond to.

Playbooks

Playbooks help to orchestrate multiple logical functions to create customized business flows. Playbooks automate many of the triage, enrichment, and response functions of a SOC to reduce the resourcing needs.

SLA Management

SLA Management helps to respond to incident in a phased manner with pre-defined SLA defined for each state of the incident phases. This allows for better tracking, optimal targeting, and process orientation for the SOC.

Connector Framework

A connector framework has been introduced that allows new data sources to be defined, extending the supported data sourced for HawkkHunt XDR. Currently email data support has been added and new data sources will be added in the future without requiring a separate release for the product. Additional enrichment and response connectors can also be defined to extend the enrichment and response capabilities of the product.

Rules Enhancement

The Seqrite EDR Rules Engine has been enhanced with additional features and capabilities to facilitate more granular and advanced rules to be defined. Additionally, tenants can now have better visibility and control over the system defined rules.

Endpoint view enhancement

The Endpoint view has been enhanced with additional features.

Role based access control

As per the roles, Security Analyst, SOC Manager, Administrator or Seqrite Administrator the access to HawkkHunt XDR is controlled.

Features released in Seqrite HawkkHunt XDR 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 XDR 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 XDR 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 XDR Console

HawkkHunt XDR 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