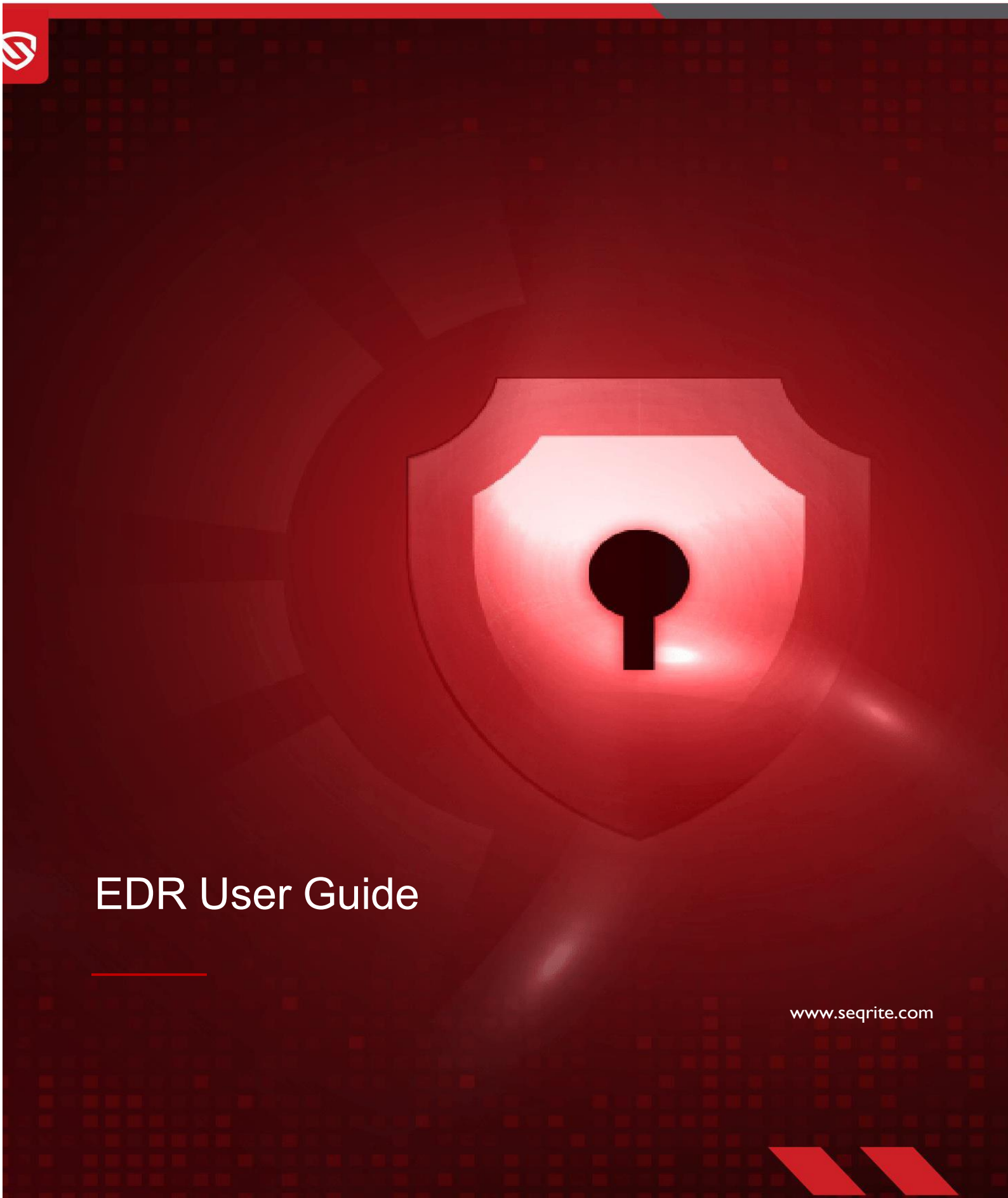
Seqrite
EDR



EDR User Guide

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.

Contents

Overview

The Endpoint Detection and Response (EDR) is a platform deployed on an

organization's own infrastructure rather than on cloud-based environment. It is a system designed to protect the endpoints from the network from potential cyber threats. EDR helps detect and responds to the threats that may evade the traditional antivirus and other security solutions deployed at the endpoint.

Workflow:

1. Monitoring Endpoints: Monitors any potential threat on the endpoints in the network by using an elaborate set of rules.
2. Alerts: Once an event triggers a rule, an alert gets generated in the system.
3. If an Action Policy is defined for the alert, then an action gets triggered in real time for the alert to help respond to the alert.
4. Incident: An alert is also sent to the central console where one or more alerts get correlated to form an incident. It represents any suspicious activity on the endpoint that has to be investigated.
5. Threat Hunting: The EDR then searches for the potential threats that might have invaded the system.
6. Response and Remediation: Once the threat is identified via Incident analysis, the analyst then takes further response and remediation actions to mitigate it, such as kill a process based on the alert, quarantine the endpoint, or isolate the endpoint.

Audience

This guide is useful for the Seqrite Admin, SOC Managers, and Analysts who would be using the system.

System Requirements

- Endpoint Protection installed with EDR product edition
    - EDR Agent Installed
    - EDR Server Installed
    - Sensor services running

Supported OS

Windows (64 bit)	Linux (64 bit)	Mac OS
Windows 8	Ubuntu 16.04,17.04,19.04,20,22.04, 23.04, 24.04, 26.04	macOS 10.15 Catalina
Windows 8.1	RHEL 7.5, 7.8, 8.1, 8.2, 8.6, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 10.1	macOS 11 Big Sur
Windows 10	Fedora 30, 32, 37, 38, 39, 40, 42	macOS 12 Monterey
Windows 11	Debian 10, 11, 12, 13	macOS 13 Ventura
Windows Server 2012	Linux Mint 19.3,20,21.3	macOS 14 Sonoma
Windows Server 2016	CentOS 8, 8.2, 9	macOS 15 Sequoia
Windows Server 2019	Rocky Linux 8.4, 8.10, 9.3, 9.5, 9.6, 10, 10.1	macOS 26 Tahoe
Windows Server 2022	openSUSE 15.1, 15.2, 42.3	
Windows Server 2025	SUSE Linux 12 SP4	
	SUSE Enterprise Desktop 15	
	BOSS 8, 9, 10	
	Oracle Linux 7.9, 8.8, 8.10, 9.6, 10.1	
	AlmaLinux 9.6, 10	

Glossary

Term	Description
OPE	On Prem End Point Detection and Response
Endpoint	A client agent system.
Incident	An incident refers to a security occurrence or an event. They are processed against the defined rules. Multiple alerts which are correlated and further grouped together, result in a creation of a single incident.
Alert	The EDR system identifies an incident according to predefined rules and subsequently triggers an alert, followed by the generation of notifications.
Threat Hunting	Threat Hunting refers to searching for threats that might have attacked the automated EDR mechanism. It involves human driven analysis and investigation to identify and mitigate potential security. Through EDR UI, threats can be identified by applying filters. Based on the filters a particular threat recorded within certain duration is hunted.
Policy	Policy is a set of predefined set of rules designed to control and manage the group of endpoints.
Group	Multiple endpoints can be assigned to a single group.
Whitelist	Remediation actions are not performed when a process is whitelisted. Both, a group or single/multiple endpoints can be selected for whitelisting.
Blocklist	A process, file, or a similar entity can be blocklisted through blocklist service at server end.

	Blocklist data is sent to EPS and existing protection service will process the blocklisting the process or file at sensor.
Live Query	An interface from which the analyst can query and get the current information about attributes from one or more endpoints instantly.
IOC Search and Response	A Threat Intelligence platform having the latest IOC's that automatically performs periodic scans on historical data of the enterprise endpoints and takes response actions on match

Getting Started

Follow these steps to log in to Seqrite EDR.

1. Login to EPP console. The login process utilizes SSO authentication.
2. Click **Advanced Protection** > **EDR** from the left panel on the EPP console. The EDR dashboard page appears in a new window.

Dashboard

The Dashboard shows various charts, graphs and tables based on the user roles that give an overall picture of the current possible incidents. It helps to get a high-level view of the security posture of your organization.

- Administrator
- SOC Manager
- Security Analyst

Dashboard provides a holistic view of the state of Security operations and Security Incidents for the organization.

The widgets can be viewed by days 7/15/ 30 by selecting the View dropdown filter available in the top right corner.

The widgets and their details are provided here-

Overall Alerts Summary

The pie chart summarizes all generated alerts. Severity levels are represented by color:

- Purple: Base
- Sky blue: Low severity
- Light orange: Medium severity
- Dark orange: High severity

Daily Alert Rate

Displays the number of alerts generated for the tenant, organized by date. Select the dots on the graph, to view the exact number of alerts.

Overall Incident Summary

Tab	Description
Severity	Gives a doughnut chart that displays the Overall Incident Summary of total incidents as per Critical, High, medium, and Low Severity.
Status	Gives a doughnut chart that displays the Overall Incident Summary of total incidents as per Open, Investigation, Remediation, and Closed Status.

Unassigned Incidents

Displays the number of incidents that are not assigned to any analyst.

Closed Incidents Summary

This doughnut chart that displays the number of incidents that are Suspicious, False Positive, and True Positive. Clicking the doughnut takes you to the Incidents page.

Average Incidents Rate- Open vs Closed

Filter	Description
Severity, Type 1 Week, 1 Month	Gives a line graph of the Average Incident Rate Open vs Closed. Hovering over the points in the graph display the incident stats.

Endpoints with Alert Count Top 10

Displays the number of alerts for the ten endpoints with the highest alert counts.

Affected Endpoints Trend

Displays the number of affected endpoints for the selected period (week or month). Hover over any point on the graph to view the number of alerts for that date.

Incidents – Missed SLA

Displays details of incidents that did not meet the SLA. Results are shown by severity.

Alerts by MITRE Attacks

Displays a bar graph showing the number of alerts by tactic. Hover over any bar to view the number of alerts and the associated tactic.

Mean Time to Detect

The Mean Time to Detect is the duration from an incident created time to an incident remediate time.

This graph shows the data for the last 30 days for the critical, high, medium, and low-severity incidents.

The following filter is available on the graph,

Filter	Values
Incident Types	Unknown, Phishing, Malware, MITM, Insider Threat, Privilege Escalation. Web Application Attack, Anomaly Detection, APT, Endpoint, Email, Network, EPP. and UBA Credential Access

Mean Time to Respond

The Mean Time to Respond is Time Taken to change the status of an Incident to Investigation from Incident creation Time.

This graph shows the data for the last month for the critical, high, medium, and low-severity incidents.

The following filter is available on the graph,

Filter	Values
Incident Types	Unknown, Phishing, Malware, MITM, Insider Threat, Privilege Escalation. Web Application Attack, Anomaly Detection, APT, Endpoint, Email, Network, EPS, and UBA Credential Access

Mean Time to Remediate

The Mean Time to Remediate is the time Taken to change the status of an Incident to Closed from Incident creation Time.

This graph shows the data for the last month for the critical, high, medium, and low-severity incidents.

The following filter is available on the graph,

Filter	Values
Incident Types	Unknown, Phishing, Malware, MITM, Insider Threat, Privilege Escalation. Web Application Attack, Anomaly Detection, APT, Endpoint, Email, Network, EPS, and UBA Credential Access

Incidents assigned v/s Active

This dashlet displays the number of analysts assigned per incident types.Hovering over the bars will display the number of analysts assigned to that incident type.

Daily Active Endpoints

Provides a line graph that displays the count of active endpints as per the selected period. Hovering over the points on the peaks in the graph will display the number of active endpoints for that.

Daily Isolation Rate

Displays a line graph showing the number of endpoints by status (Isolated, Reconnected, and Failed) for

the selected time period. Hover over a data point to view the exact endpoint count. Clicking an Isolated data point redirects you to the Isolated Devices page, while Reconnected and Failed data points do not provide redirection.

Downloading Consolidated report

To download the Seqrite EDR consolidated report in PDF format, click **Export**. The report will be downloaded immediately on the working machine.

Incidents

Effective incident management requires a clear and structured interface that allows SOC teams to quickly identify, investigate, and remediate threats. The List View provides a consolidated overview of incidents and alerts, while the Incident Summary pane offers detailed information and actionable options for each incident. This document describes the fields, filters, and actions available to users for managing incidents efficiently.

List View

Scroll through the list to view previously generated alerts. Clicking on a host name opens the **Device View** for that alert.

Incident Fields

Column	Description
INCIDENT ID	Select the severity from the drop-down values.
INCIDENT NAME	Select the type of an incident form the drop-down values.
TYPE	Type of Incident is based on the Source of the initial alert based on which the Incident is formed. It could be one the following: • Endpoint • Insider Threat
SEVERITY	Severity of the incident is based on the combined severity of the alerts that are part of the incident.
PRIORITY	Priority is assigned by the analyst.
STATUS	The status value is initially set to **Initial** when the Incident is generated. As the analysis progresses, analysts have the flexibility to update the status to **Investigation**, **Remediation**, or **Closed**.
NO. OF ALERTS	Displays the count of alerts in the Incident.
CREATED ON	Displays the date on which the Incident was created.
ASSIGNED TO	Displays the name of the assignee.

Alert Fields

Field	Description
ALERT NAME	Displays the name of the alert.
ALERT TYPE	Displays alert type: Custom, Associated Alerts, Unassociated Alerts.
SOURCE	Displays the source of the alert.
SEVERITY	Displays severity: High, Medium, Low, Base.
TACTICS	Displays tactics associated with the alert.
CREATED ON	Displays the date and time when the alert was created. Sortable.

View Options

You can view incidents by time slots:

- **Hour-wise**: Last 1 hour, Last 24 hours
- **Day-wise**: Last 7 days, Last 15 days, Last 30 days
- **Custom**: Select From Date and To Date using the calendar control, then click **Save**

My Incidents

Click **My Incidents** to view only the incidents assigned to you (logged-in user).

Filter

Apply filters to narrow down search results. You can filter by:

- Severity
- Status
- Alert details (Process Name, Host Name, Assignee, Tactics)

View Details

Click **View Details** to navigate to the Alerts page.

Incident Summary

Clicking any row displays the incident summary in the right pane. Available actions include:

- **View Audit Report** – Access detailed audit reports.
- **Add Notes** – Add notes to the incident, visible in the *Notes* section.

Basic Information

Field	Description
Incident ID	Displays the incident ID. Copyable via icon.
Incident	Displays the incident name. Editable via icon.

Name	
Incident Type	Displays type: Unknown, Phishing, Malware, MITM, Insider Threat, Privilege Escalation, Web Application Attack, Anomaly Detection, APT. Editable via icon.
Created On	Displays the creation date and time.
Occurred On	Displays the endpoint where the incident occurred.
Last Updated On	Displays the last update timestamp.
Number of Alerts	Displays the number of alerts linked to the incident.
View Details	Redirects to the Alerts page.

Response Summary

Field	Description
Severity	Displays severity: High, Medium, Low, Base.
Priority	Displays priority: Critical, High, Medium, Low. Editable via icon.
Assigned To	Displays the assignee's name.
Status	Displays status: New, Investigation, Remediation, Closed. Also shows response timeliness (On Time, Late, Closed). Editable via icon. Allows document uploads. Note: Max 5 files per incident, each ≤ 1 MB. Supported formats: .xlsx, .pdf, .docx, .jpeg, .jpg, .png.

Description and Analysis

- **Description** – Editable incident description.

Notes

- **Notes** – Displays notes with author and timestamp. Add notes via **Add Note** icon.

Endpoints and Users

- **Endpoints (#)** – Displays endpoint hostnames.
- **Users (#)** – Displays associated users.

Key Attributes

- **Process, Registry, File, Network** – Each displays count, value, reputation, and associated alerts.

Add Note

1. Click the **Add Note** icon (top-right corner).
2. Enter the note in the **Note** field.
3. Click **Save**.
4. A confirmation message appears.

Notes are visible in the **Notes** section of the Incident Summary.

Scheduling Incident Reports

Note: Only users with Admin, or SOC Manager privileges can schedule incident reports.

To schedule reports, follow the instructions here.

Auto Incident Creation

Overview

In Seqrite EDR, most detections are currently generated as **alerts only**. Incidents are not created automatically, so SOC analysts must manually convert alerts into incidents. This creates operational overhead and affects how analysts:

- Track investigation ownership
- Manage lifecycle (assignment, escalation, closure)
- Use incident-level automation and reporting

With this module enabled, alerts can automatically generate incidents, and related alerts can be grouped into the same incident.

What auto incident creation does

When enabled, the auto-incident creation module:

- Automatically creates an incident for eligible alerts
    - Each qualifying alert triggers an incident if no related open incident exists.
- Groups related alerts into a single incident (where applicable)
    - Related alerts are correlated using the legacy EDR logic (for example, same host, user, or campaign, depending on your implementation).
- Restores incident-centric workflows
    - Ownership, prioritization, and lifecycle are managed at the incident level instead of per alert.

Before and after

Behavior	Without auto incident creation	With auto incident creation
Alert handling	Alerts only	Alerts and automatically generated incidents
Incident creation	Manual: analyst converts alert to incident	Automatic: system creates incident from alert
Grouping of related alerts	Limited / manual	Automatic grouping (legacy correlation logic)
SOC workload	Higher manual effort	Reduced manual conversion and triage effort

Investigation focus	Alert-centric	Incident-centric

How auto incident creation works

The following steps describe the high-level behavior of the module. Exact criteria may depend on your environment and policies.

1. **Alert is generated**
    - A detection rule or engine generates an alert in EDR.
2. **Alert is evaluated for incident creation**
    - The system checks if the alert meets the criteria used by the earlier EDR incident creation logic. Examples:
        - Alert severity (for example, Medium and above)
        - Alert type or category (for example, endpoint, email, cloud)
        - Source entity (host, user, tenant)
3. **System finds an existing related incident (if any)**
    - The module checks for an **open incident** that matches correlation conditions such as:
        - Same asset, user, or tenant
        - Same or related detection rule
        - Within a defined time window
4. **System creates or updates an incident**
    - If no related incident is found:
        - A **new incident** is created automatically from the alert.
    - If a related incident exists:
        - The alert is attached to the existing incident.
5. **Incident appears in the SOC console**
    - The incident is available to SOC analysts, who can:
        - Assign an owner
        - Change status (for example, Open, In progress, Resolved)
        - Add notes and evidence

Benefits of Auto incidents

Auto incident creation provides the following benefits:

- Reduced manual work
    - Analysts no longer need to convert each alert to an incident.
- Consistent incident lifecycle management
    - Teams can manage assignment, escalation, and closure at the incident level.

- Better correlation and context
    - Related alerts are grouped into a single incident, giving analysts end-to-end context.
- Improved readiness for future correlation
    - SOC workflows remain stable while the new correlation model is being developed and rolled out.

Using incidents in daily operations

After auto incident creation is enabled, SOC analysts can use incidents as the primary unit of work.

Typical actions include:

- View incidents
    - Navigate to the **Incidents** area in EDR to see all automatically created incidents.
- Assign incidents
    - Assign incidents to specific analysts or queues.
- Investigate
    - Open an incident to:
        - Review associated alerts and entities.
        - Add investigation notes and evidence.
- Escalate or reassign
    - Change ownership or priority as required by your SOPs.
- Resolve and close
    - When investigation is complete, update the status and close the incident.

Tip
Use incident filters (severity, status, owner, time range) to quickly find the most critical or active investigations.

Correlation

Correlation is the process of linking security events from various sources—such as endpoints, networks, and cloud services—to build a complete picture of an attack. Automated analysis powered by machine learning and behavioral analytics connects isolated alerts into a single incident, enabling faster detection, more accurate investigation, and quicker response compared to using siloed tools.

Based on the correlation rule, the alerts will be grouped in a single incident.

Alerts

Alerts in Seqrite EDR are real-time notifications generated whenever the platform detects potential security incidents or anomalies within your IT environment. They act as the first line of defense, drawing your attention to activities that may indicate threats such as malware infections, unauthorized access attempts, or suspicious user behavior.

Unlike traditional point solutions that often produce isolated or noisy signals, Seqrite EDR alerts are designed to be contextual and correlated. Each alert provides detailed information about the nature of the event, the affected assets, and the potential impact. The alert name identifies the specific detection, while visual indicators help you quickly distinguish between a single alert and a cluster of related alerts that may represent a broader attack pattern.

By consolidating signals from endpoints, networks, email, and cloud services, the Seqrite EDR platform delivers comprehensive visibility across your environment. Alerts are enriched with actionable insights, enabling administrators to triage efficiently, investigate root causes, and respond to threats in a timely and effective manner. In this way, alerts serve not just as warnings, but as entry points for investigation and response, helping you maintain a proactive security posture.

Alerts Workflow

After an alert is generated on a host and displayed on the Seqrite EDR console, it is designated an open status by default.

1. The IR will assign the open status alert to self or another IR in the team for investigation, analysis, and appropriate remediation action.
2. After the alert is assigned to an IR, the IR starts working on the alert.
3. The assigned IR will analyze the alert, perform root cause analysis. After the analysis is complete, IR takes appropriate remediation action if required.
4. After analysis is completed, the IR changes the status of the alert to closed.
   All the activities carried out during the analysis such as status change, assignee change, comments entered during the analysis, and remediation actions taken are logged. The IR can see these logged activities on the investigation workflow page.

Endpoints View

When logging into the Seqrite EDR portal, the Endpoints view serves as the default landing page for Incident Responders (IR). This means that upon logging in, the Alerts page will automatically open in the Endpoints view. The Endpoints view presents a holistic view of the endpoints that have communicated to the Seqrite EDR portal for the past 7, 15, 30 day period or the hours as selected from the drop-down options along with the alert severity count and the status whether Open, Closed or In-Progress. By default, the dashboard displays the alerts for all the endpoints in the entire network. You can choose to view the alerts assigned to you by clicking the My Alerts button.

The navigation pane (highlighted in yellow on upper left) lets you navigate to the other pages of the Seqrite EDR portal for Threat Hunting, Rule Builder, Reports, Settings and Help Center. Hover anywhere on the navigation pane to expand the pane and navigate to other pages. The navigation pane displays the name of the logged in user in User Settings on the extreme lower corner besides the zoom control widget.

List view

Click the List button next to the Canvas button to view the listed alerts serially with hostname, count, severity and the status.

You can sort the displayed list on the number of alerts from high to low count for the corresponding hosts. Scroll down the list as required to view the earlier generated alerts. Clicking on a particular host name opens the Device view for that alert.

The Analysis Workflow

The Analysis workflow helps the IR investigate the suspicious event(s) that generated the alerts. The Analysis workflow displays the processes that triggered the alert based on the corresponding rule. The first file that started the sequence of security events and the following processes are displayed in a collapsible tree like flow. Starting from the first process/file, clicking on an event displays the further events that occurred and the corresponding details. You can explore the process flow up to the last occurred event.

The following screenshots show, step by step, how an IR starts the analysis for an alert.

1. First the IR opens the analysis workflow for an alert by clicking on the caret (highlighted in yellow square) on the upper-right corner of the alert in the Details pane. The Details pane is located below the Alerts dashboard.
2. IR then clicks on host QHPUNML7LP121 icon displayed on the screen.
3. The filename **rundl32.exe** is displayed on the screen which further led to execution of some modules.
4. To investigate further, the IR then clicks on **rundl32.exe** icon.
   The screen displays the following:
   — Count of modules that were loaded by the **rundl32.exe** executable and any exploitable host programs.
   — The basic information for the process **rundl32.exe**, time of execution, start time, end time, path, MD5 count, SHA count, the command line, and the drive type is displayed.
   –The binary information, and the endpoint details such as the Username, Hostname and the operating system on the host are displayed in the right pane.
   — The filename and time stamp details for the 38 modules that were loaded are displayed in the right pane.
   — The screen also shows that the file rundl32.exe loaded on exploitable host program in memory.

This analysis can be followed further, right up to the last action that was initiated by the alerted process.

Alert analysis – Remediation actions

On Endpoint

During Alerts analysis, if you find any endpoint is running malware, you can perform the following remediation actions on that endpoint.

The endpoint isolation and restore feature allows IR to isolate the endpoint from the network when an endpoint is running malware, to ensure the malware doesn't spread to other endpoints.

When the endpoint is isolated, IR runs an investigation and resolves security issues. Once the endpoint is clean, IR can reconnect the endpoint to the internet.

- **Isolate**: This action will isolate the endpoint from the network. This action will ensure that the malware is not spread in the network. This option is available only if the endpoint is infected. After isolation, IR runs an investigation and resolves security issues.
- **Reconnect**: This action will reconnect the endpoint to the network. Once the endpoint is clean, IR can

reconnect the endpoint to the network with this action. This option is available only if the endpoint is isolated.

On File

During Alerts analysis, if you find any suspicious file activity, you can perform the following remediation actions on that file.

- Kill: This action will kill the process/file activity. Note that the file still will be available on the host computer and can be spawned/activated later. This option is available only if the file has spawned an active process. You can check the start time of that process under Process Details tab. This option is not available for a process that has ended.
- Quarantine: You can quarantine a file on the host PC. This 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. The Quarantine action might fail if the sensor access to the file or folder is denied on the host PC. You cannot quarantine valid system files or installed program files as these files are Whitelisted by default when installed.

Note: Kill option will be displayed only for executable files in addition to Quarantine and Restore options. For other files, Quarantine and Restore options will be displayed.

On Registry entries

From the alert, you can navigate to the process file that has spawned the regedit.exe file which is used to create/edit entries in the system registry. Clicking on the Values Created will display the registry entries in the right pane.

For any registry keys that are created as a result of any suspicious activity, you can select the registry keys and click **Delete**.

Note: You may not be able to delete a registry entry that has been renamed, or deleted already.

Switching from Timeline View to Type View

This view lets you view the Alert analysis for a host in terms of types of activities triggered by the process. These can be file actions, process, network or Registry type.

1. You (IR) are currently on the Timeline view for Alert analysis on a host.
2. Click the Type view. The Type view is displayed for the same alerted process as follows:

The details for the alert are displayed in types. Here we can see that the file **WMIC.exe** has triggered 39+ File activities and 1 other process.

3. Click the + sign besides File to view the related details.

Activating the Date and Time View

You can view the progression of the process that triggered an alert on a date and time scale. This scale also displays whether the activity was related to a Process, Files, Registry or a Network activity.

1. To enable the Date and Time view, click the caret in the lower left corner (highlighted in a yellow square).

The Date and Time view is displayed with the activity type.

2. Click the white caret in the lower left corner to close the Date and Time view.

Color Code Legend

Color of dots	Activity related to
Yellow	Process
Purple	File
Blue	Network
Green	Registry

Additionally, you can do the following:

- We can zoom in and out using mouse. We can adjust time window, if there are multiple events at same time, then there will be concentric circles on this view, else it will be a solid circle for a single event.
- Also, when user clicks on this solid circle on this view, then user can see respective event on tree as well as details on right side panel.
- When user clicks on concentric circles, then on right side panel all the concurrent events occurred at that same time are displayed. User can see further details of event by clicking on the events.
- View the time sequence of activities performed by a process or its parent or siblings during the course of an alert generation.

Other actions available on Alerts > Analysis workflow Page.

- You can avail the following functionality by clicking the designated buttons on upper right corner of the user interface.

Functionality	Action
To return to the alert after you have traversed far into the analysis workflow.	Click the View Alert button.
To view the activity logs for an alert.	Click the clock icon.
To enter comments during analysis.	Click the comments box.
To view similar alerts on other hosts.	Click the Graph shaped corresponding icon.
To go to full view.	Click the white caret to expand the view to full page view. To return, click the inverted caret that is pushed to the far right.
To view the Alert details such as basic timestamp information, generated by which rule, and the status and severity of the alert and assignee.	Click the Alert Details tab.
To view the process details that triggered the alert such as process name, binary size and endpoint details.	Click the Process tab.

Alert Details

Alert Summary

Alert ID: Unique identifier for the alert instance.
Rule Name: Indicates the detection rule triggered (e.g., "network event").
Description: Brief label or tag associated with the alert (e.g., "win").
Incident Name: Grouping label for related alerts.
Created On: Timestamp when the alert was generated.
Source: Origin of the alert (e.g., EDR).
Severity: Risk level assigned by the system (e.g., Low).
Assigned To: Analyst or team responsible for triage (may be "Unassigned").
MITRE TTP: Mapping to MITRE ATT&CK techniques (if applicable).
Host Name: Device where the event occurred.
Users: Logged-in user at the time of the event (e.g., Administrator).
Events Timeline
The timeline section provides a chronological view of key activities associated with the alert. For example:
14:21:04 – Network event involving chrome.exe
This may indicate outbound or inbound traffic initiated by the Chrome browser, which could be benign or warrant further inspection depending on context.
Recommended Actions
Review Host Activity: Check recent activity on the host OPEAPTPWW090T for anomalies.
Validate User Context: Confirm whether the Administrator account was expected to be active.
Analyse Network Traffic: Use packet capture or flow logs to inspect the nature of the Chrome network event.
Assign for Triage: If not already assigned, route the alert to a security analyst for review.
Document Findings: Record any observations or decisions in the incident tracking system.

Whitelisting rules for alerts

Alerts are generated based on default rules specified in the Seqrite EDR engine and displayed on the dashboard. You may come across some alerts that are triggered by valid activity in your network. A whitelisted rule allows you to specify a combination of parameters to whitelist the generated alerts. You can add the corresponding alert conditions to the Whitelist rules so that future alerts and same old alerts based on the file execution or activity under that rule are no longer displayed on the Regular Alerts dashboard view.

Adding an alert rule to Whitelisted rules

1. On the dashboard, in the right panel, click the alert for which you want to Whitelist the corresponding rule.
2. The Alert Analysis view opens. The right pane displays the details for the selected process or any other processes.
3. Click **Add to Whitelist**.
4. In the Add to Whitelist dialog, enter a name for the Whitelisted rule.
5. Select the parameters as required from the displayed parameters. The parameters will appear depending upon the process.
6. The Rule Query preview pane shows the corresponding rule query that would be Whitelisted.
7. Click **Done** to save the rule to the Whitelisted Rules.
   You can view the rule under **Whitelist Rules** tab on the **Rules** page.

You can delete the Whitelist Rule with the help of the **Delete icon**.

Threat Hunting

Overview

Seqrite Universal Agent continuously monitors all activities on your machine and generates events in EDR. These events are evaluated against the rules defined in EDR. If an event matches a rule, an alert is generated. Events that do not match any rule are not ignored—they are stored in Threat Hunting for further analysis.

Threat Hunting enables detection and monitoring of events that are not yet documented in Seqrite or included in the rule builder. This feature helps track new or unknown malicious activities emerging in the cyber world.

Alerts generated from unmatched events are displayed under the Alerts tab.

Raw events are stored under the Processes tab.

Independent of rule creation or alert generation, users can proactively hunt threats using this feature.

Threat Hunting Interface

The Threat Hunting screen provides two search options:

- **Manual Search**
- **File-based Search**

Data Retention

- Alerted events: retained for **30 days**
- Raw events: retained for **7 days**

Manual Search

The **Manual Search** tab allows you to search events using filters and parameters.

- Use the search bar with **View** and **Host** filters.
- Add parameters, select the view period, and choose a host from the dropdown.
- Search results are displayed under the **Alerts** and **Processes** tabs.

Actions

- **Export Results:** Use **Schedule Export** or **Export** buttons to download search results.
- View Event Details:
    - Select a raw event to open its details in the right panel.
    - Click **View details** to access the **Timeline** page.
    - The timeline displays a tree structure of the event's generation history.
    - Apply filters in the search bar to highlight specific information.

This detailed view helps determine whether an event is malicious and supports deeper analysis.

File-Based Search

The **File-based Search** tab allows bulk searching using a CSV file.

1. Download the sample CSV template.
2. Add desired details under the following headers:
    - IP Address
    - URLs
    - Domains

- Hash Values

3. Upload the CSV file to conduct the search.
4. Uploaded files are listed on the File-based Search screen and can be used to run searches.

Creating a Query

To create a query, follow these steps:

1. On the Seqrite EDR portal, click the Threat Hunting page in the left navigation pane. The Threat Hunting tab is highlighted with a yellow square. You can directly search using appropriate search parameters or create a new query using the query builder.
2. Click the Add + button to add the filter values. The Filters dialog box is displayed.
3. In the Search textbox, click and select from the filters that are displayed.
4. Enter the value of the filter that you want to use in the search query. For example, Name. The filter is selected and displayed in the Search box, enter a value for the indicator. For example, we shall add Name: Powershell.exe
5. Click Add+ to add the selected IOC and the search value. The value is selected and displayed under Selected Filters.
6. Click in the Search box and repeat above steps to add other IOC values for the search query. For example, and IP address IP:”202.145.202.114”.
7. Add more IOC as required. To remove a particular filter, click the corresponding x mark for that value.
8. Click Apply to apply the search criteria.
9. Once you are done with adding the filters and their values, click Save Query. The query is saved with time stamp and moved to the Saved Queries tab.
10. Enter a name for the query in the Query Name column (highlighted in the yellow box). For example, Powershell+IP, and click Save. A confirmation message is displayed and the query is saved.

Using Saved Query to create a new query

1. On the Seqrite EDR portal, click the Threat Hunting page in the left navigation pane. Click Add+. The Filter dialog is displayed.
2. Click the Saved Queries tab. The saved queries are displayed in order of the created timestamps.
3. Scroll down the query list, or use the sort icons besides the Time Stamp and Query Name columns to sort entries as required. Select the query that you want by clicking on the query. The query tags are displayed in the Query tags section for the selected query.
4. To add the Filters from the selected query to a new query, click Add Filters. The query is moved to the Add Filter tab and 2 extra buttons, Update Query and Save Query are displayed.
5. To update the query, add/remove filters as required and click Update Query.
6. To save as a new query, click Save Query. If you click Save Query, the query is moved to the Saved Queries tab.

7. Enter a name for the query in the Query Name column, and click Save. A success message is displayed and query is saved.

Deleting Saved Query

You can delete the saved queries if not required.

1. On the Seqrite EDR portal, click the Threat Hunting page in the left navigation pane.
2. Click Add +.
3. On the Filter dialog box, click **Saved Queries**. The saved queries are listed.

Running a Query

You can create a new query with required indicators and apply the query to get results or you can use previously saved queries to search for threats in the Seqrite EDR database.

1. On the Seqrite EDR portal, click the Threat Hunting page in the left navigation pane.
2. Click Add+. The queries filter dialog is displayed.
3. Create a new query or click the Saved Queries tab to view the Saved Queries and select the query that you want to run. For this example, we click on Saved Queries tab and select the first query in the list.
4. Click Add Filters, to add/modify and filters in the selected query.

   As a result of previous action, some indicator filters are displayed. Add or remove the indicator filters as required.
5. Click Apply to run the final query. The results are displayed in two tabs: Alerts and Processes. The Alerts tab displays the alerts that match the query, and the Processes tab similarly displays the matching processes.
6. Running a saved query
7. To obtain more information about an alert, click the alert row.
8. To view the Process details for that host, click the Process tab on the upper left corner. The details for only the processes that match the query are displayed.
9. To start the investigation for a process, click the particular process.

Search History

The search History tab displays all the search queries carried out recently. You can use a query from the recent queries or applied queries.

1. On the Seqrite EDR portal, click the **Threat Hunting** page in the left navigation pane.
2. Click **Add +**.
3. On the Filter dialog box, click **Search History**. The recently run queries are listed.
4. Select the query you want to apply. Modify the query if required.
5. Click **Apply**. The query is applied, and search results displayed.

Note:
There is fix list of parameters for which you can do threat hunting. If such parameters are present as key attributes for any of the incidents or alerts you can do threat hunting from that incident's Page or alert's Page respectively.

Rule Builder

Overview

The **Rule Builder** in Seqrite EDR allows you to define custom detection logic that evaluates **all events generated across the platform**. Every incoming event—including process activity, file events, network communications, registry operations, and system events—is analyzed against the rules you create.

If an event matches the defined rule conditions, an **alert is automatically generated** and displayed on the **Alerts** page. Within the alert details, you can view the **Rule Name** that triggered it.

Rules help you:

- Generate actionable alerts for specific behaviors
- Increase visibility across your infrastructure
- Forecast and mitigate attacks
- Maintain a forensic trail for investigations
- Distinguish normal events from malicious activity

Once created, rules are immediately applied in real-time and influence alert generation across your environment.

How Rules Work

- Rules evaluate **all event types**.
- You can build rules using process, file, network, registry, and system indicators.
- Rules may be simple (single condition) or complex (multi-condition with AND/OR logic).

Alert Flow

1. An event is generated.
2. The event is evaluated against all active rules.
3. If matched → **alert generated**.
4. The alert appears on the Alerts page with the triggering rule name.
5. Admins/IR can assign alerts and investigate further.

Types of Rules

System Rules

- Predefined by **Seqrite Labs**.
- Automatically loaded for every new tenant.
- Generate alerts like custom rules.

Restrictions:

- Cannot be edited

- Cannot be copied
- Cannot be deleted

Allowed: Activation / deactivation only.

Custom Rules

Created by users based on their environment-specific requirements.

You can:

- Create
- Edit
- Copy
- Delete
- Activate / Deactivate

Deactivation is useful for rules generating false positives or noise.

Access Permissions

Role	Can Create/Edit Rules?
SOC Manager	Yes
Security Analyst	No
Admin	No
Read-Only User	No

Whitelisted Rules

Whitelisting allows you to suppress alerts for known safe behaviors while keeping the original detection rule active.

When to Whitelist?

- Repeated alerts for validated internal processes
- Trusted IPs or domains used internally
- Legitimate command-line patterns

You can whitelist based on:

- Process Name
- Process Path
- Process Command Line
- Network Protocol, Port, IP
- Other indicators

Create a Whitelist Rule

Method 1 — From Rule Builder

1. Select **Whitelist Rules** from the Rule Builder menu.
2. Click **Create Rule**.
3. Specify desired indicators and conditions.
4. Save the whitelist rule.

Method 2 — From Alerts Page

1. Open the alert.
2. Click **Add to Whitelist** in the right pane.
3. Configure whitelist fields.
4. Save.

Rule Builder Interface & Filters

Available Filters

- All
- Rule Name
- Timestamp
- Indicators
- Created By

Platform Selection

You can specify the target OS:

- Windows
- macOS
- Linux

MITRE Mapping

Each rule can be mapped to related **MITRE Tactics** and **Techniques**. These details appear in generated alerts.

Indicators Supported

Process Indicators

Process Name, Process Path, Command Line, Parent Name, Command Line Length, Is Browser Process, Is Process Signed, User Name, SHA2, MD5, Parent/Grandparent hashes & paths, Access permissions, cp_event_type, etc.

File Indicators

File Name, File Path, SHA2, MD5, File Type, File Attributes, New Path, Modified Hashes, etc.

Network Indicators

Protocol, Port, IP, URL, Domain Name, DNS IPs, Method, Connection Type.

Registry Indicators

Registry Key, Registry Value, Registry Value Data.

System Fields

Windows Event ID, Field of Interest.

Supported Operators

Logical Operators

- AND
- OR

Comparison Operators

- =
- contains

Best Practices

- Always use the dropdown suggestions for indicators and operators.
- Add a space after each indicator, operator, value, and bracket.
- Use parentheses for complex rule structures.
- Avoid manually typing entire expressions to prevent formatting errors.

Creating a Detection Rule

1. Click **Create Rule**.
2. Enter:
    - Rule Name
    - Severity
    - Description
    - MITRE Tactic & Technique
    - Platform (Windows/macOS/Linux)
3. Select indicators, operators, and values from dropdowns.
4. Add AND/OR logic as required.
5. Preview the rule.
6. Save the rule.

Example Rules

Example 1: Suspicious External Communication

IP = 4.4.4.4 AND Port = 80

Example 2: Process Using Network Port

Process Name = teams.exe AND Port = 80

Example 3: Suspicious PowerShell Activity

(Parent Name = svchost.exe AND Process Name = powershell.exe)

AND

(Process Command Line contains start OR Process Command Line contains add)

Example 4: MSI → CMD → Suspicious Child Process + Persistence

(Grand Parent Name = msiexec.exe AND Parent Name = cmd.exe)

AND

(Process Name = iexplorer.exe OR Process Name = reg.exe)

AND

(Registry Value contains REGISTRYSOFTWAREMicrosoftWindowsCurrentVersionRun

OR

Registry Value contains REGISTRYSOFTWAREWow6432NodeMicrosoftWindowsCurrentVersionRun)

Live Query

Live Query functionality allows users to run real-time queries against endpoints to gather information for security analysis and IT hygiene purposes.

Live Query Execution

To execute a Live Query, follow these steps:

- Click 'Live Query' option in the left menu. The Live Query Page appears.
  Note: Users can also access the Live Query feature directly from the Alert Page.
- On the Live Query Page, select the desired platform from the Platform list. This selection determines the target platform for running the query.
- Select the table from the list.

Note ☛ There are over 100 suggested tables to choose from. Visit this URL https://www.osquery.io/schema/5.6.0 for further reference and information.

- Select the hosts from the dropdown list by selecting multple checkboxes. These are the endpoints on which you want to run the query.
- The query will be displayed in the designated box on the page. Review and ensure it reflects your intended query then click Run Query. Within 30 seconds, the result of the query will appear on the screen. In the event that the query cannot be resolved within the given time frame, an error message will be displayed instead.
- If desired, you can export the query result by using the "Export as XLS" button.

Additionally, you can utilize the Search feature to find a specific parameter or information within the Live Query interface.

Query Limitations
Query execution time : 30 seconds

Search History

The Search History feature allows you to access and retrieve previously executed queries, as they are automatically saved for your convenience. A specific query can be searched within the saved records using this feature.

Note☛
The Live Query feature is compatible with Windows, Linux distributions such as Ubuntu, Linux Mint, Red Hat Enterprise Linux (RHEL), openSUSE Leap, as well as macOS.

Saving and Managing Live Queries

In the Live Query Page, users have the option to save queries they have executed for future reference or repeated use. This guide outlines the process of saving, viewing, and managing saved queries.

Saving a Live Query

1. **Go to Live Query Page:** Navigate to the Live Query Page where you have executed the query you want to save.
2. **Execute and Save Query:**
   - After executing the desired query, locate the Save Query button.

- Clicking this button opens a modal pop-up named Save Query.

3. **Provide Query Details:**
   - In the modal, users are prompted to provide the following mandatory fields:
     - Query Name: Enter a unique name to identify the saved query.
     - Description: Provide a brief description for reference.
4. **Review Query:**
   - The executed query will be displayed in the Query field for review.
5. **Save Query:**
   - After verifying the details, click the "Save" button to store the live query as a saved query.

Viewing Saved Queries

1. **Locate Saved Queries Button:**
   - To access saved queries, locate the Saved Queries button. This button is present within the Live Query Page.
2. **Access Saved Queries:**
   - Clicking the Saved Queries button opens a modal pop-up window displaying all saved queries.

Actions Available for Saved Queries

1. **Search:**
   - Utilize the search functionality to quickly locate specific saved queries by name.
2. **Run:**
   - Execute a saved query directly from the list of saved queries by clicking the "Run" action.
3. **Edit:**
   - Modify the details of a saved query by selecting the "Edit" action. Users can update the query name, description.
4. **Delete Query:**
   - Remove unwanted queries from the list by selecting the "Delete" action. This action permanently removes the saved query.

Note: ☛

- While saving or editing a saved query, ensure that a unique name is provided to prevent conflicts or confusion.
- Users are encouraged to provide meaningful descriptions to facilitate easier identification and understanding of saved queries.

Policy

Policies are used for automated response actions on alerts. Policies define either generic actions on alert criticality, or specific actions on alerts that are triggered by specific rules.

One or more endpoints where a specific alert is seen are all remediated immediately if the remediation action policy is defined.

On deployment, a large set of generic and rule specific policies are automatically activated by the product based on well-known attacks and exploits. The analyst can add new policies or modify existing policies as suitable for a specific environment.

Generic Policies

Generic Policies apply across alerts and define the generic actions that will be taken in the environment. If no rule specific policies are defined for a particular rule, then the generic policy that applies, if defined, will be invoked. The policy match of a generic policy with an alert occurs on Alert Severity or endpoint scope or reputation of the endpoints or a combination of these.

Defining a Generic policy

Analyst can define a generic policy by selecting the following:

The Alert Severity, Scope, Reputation and Whitelisted processes, if any

Actions to be taken on Policy match include: Kill process, Add to BlockList, Quarantine Process, Isolate Endpoint, Set the Endpoint Reputation, Restore the Endpoint, Delete process, Notify user

Rule Specific Policies

Rule Specific policies mandatorily have a Rule selected, primarily based on this rule trigger that the policy action is executed.

Defining a Rule Specific Policy

Analyst can define a rule specific policy by selecting the following:

The Rule Name, Scope, Reputation and Whitelisted processes, if any

Actions to be taken on Policy match include: Kill process, Add to BlockList, Quarantine Process, Isolate Endpoint, Set the Endpoint Reputation, Restore the Endpoint, Delete process, Notify user.

Scope

Endpoints can be added to scopes based on the priority. Typically there are 4 types of scopes

- Critical
- High
- Medium
- Low

Critical scope Endpoints and Groups are the endpoints that are essential to the operation of the business. A critical Endpoint can descend along with the hierarchy, such as Critical -> High-> Medium-> Low.

A Low scope can be opened for assertive automated response actions, while a Critical scope can be defined for more stable impact actions.
On the View page, the groups can be filtered by the scope, and by the selected

Activity Logs

The **Activity Log** section allows you to track and review actions performed by users across various modules. It provides a clear overview of system activity for auditing and monitoring purposes.

The Page Display

The log is displayed in a grid format with the following columns:

- **Date & Time** – Timestamp of the activity.
- **Modified By** – The user who performed the action.
- **Item Modified** – The item or entity that was changed.
- **Log** – A description of the action taken.
- **Entity ID – The Entities listed**

Filtering Options

You can refine the log view using filters:

- **Modified By**: Click the **Add** button on the top menu bar to filter by specific users.
- **Date & Time**: Use the dropdown to select a custom time range.

Activities Captured in the Log

Incident Activities

- Create and edit incidents
- Assign incidents
- Change priority
- Close incidents
- Upload documents
- Flag as suspicious, false positive, or true positive

Alert Activities

- Perform remediation actions
- Add alerts to the whitelist

Whitelist Rule Activities

- Add whitelist rules
- Edit whitelist rules
- Delete whitelist rules

Note: You can export the activity logs in MS Excel format. Click the Export button in the top right corner to execute the same.

Reports

Seqrite EDR has a variety of reports that give you a bird's eye view of the security situation in your network infrastructure, specific to alerts. The information is presented in 2 widgets, you can scroll down to view the reports. Navigate to the Reports tab on the EDR console.

Reports can be exported immediately or scheduled for export.

Alerts Report

The first widget gives information about the number of Alerts and severity over a 7, 15, or 30 day -period on a line chart. The count by severity and total number of devices/endpoints is displayed in upper right corner. Use the **Severity** filter to display the alerts by severity as required.

Tip: You can navigate directly to the Alerts page with the filter that is applied by clicking the forward facing caret highlighted in yellow as shown below.

Endpoints

The second part has two widgets as follows: One gives information about the count of affected endpoints over a 7-day period.
The second widget gives other information about the top 5 affected endpoints along with the Hostname. A table in the widget displays the count of alerts based on their current status and severity for respective host.

Remediation

In this widget, counts for remediation by Delete or Kill action are displayed date-wise for the past 7 days. The Total count for devices is displayed in upper right corner. Hover above each graph to view Remediation activity counts for that date.

Active Endpoints

A widget in the 4th part of the reports page displays the count of the active endpoints over the dates for a 7- day period along with the total endpoint count displayed on upper right corner.
Active endpoints are those endpoints that have communicated with Seqrite EDR portal over the past 7 days.

Quarantine Files

Seqrite EDR generates alerts and you can see them all in XDR UI. You may require to Quarantine some of the alerted processes. To Quarantine the alerts, select the desired alert and click the **Quarantine** button available at the bottom of the right panel opened for the selected alert.

The quarantined files can be seen in the under the **Reports** section. Once you quarantine the file, it gets deposited to the Quarantined folder on sensors installed system.
To view the list of Quarantine files, click the **Quarantined Files** under Reports.

Here you can see the Quarantined files with the following details-

- File Name
- Hash
- Original File path

- Endpoint
- Alert ID
- Restore

You can sort the list based on the time by choosing the Time sorter available at the right side of the grid.

To add filters to the Quarantined files' list, click the Add button available near the filter search bar and you can choose the filters to see the desired files.

Restore quarantined files

To restore a quarantined file:

1. Go to **Reports > Quarantined Files**.
2. Locate the required file.
3. Click the **Restore** icon.
4. Click the **Restore** button on the confirmation pop-up window.
5. The status appears as **Restoring** .

Note: To export the Quarantined file details, click 'Export' button.

Isolated Devices

The Isolated Devices page displays all endpoints that are currently isolated from the network. It provides a centralized view of isolated endpoints and allows authorized administrators to review their status, update isolation settings, and reconnect one or more endpoints when required.

View Isolated Devices

The Isolated Devices page displays the following information for each isolated endpoint:

- Device Name
- OS
- Group
- IP Address
- Status
- Isolation Time
- Reconnect
- Search and Filter Endpoints

Use the search box to locate endpoints by:

- Device Name
- Group
- IP address
- OS

Reconnect an Isolated Endpoint

To reconnect an isolated endpoint:

1. Go to Reports > Isolated Devices.
2. Locate the required endpoint.
3. Click the Reconnect icon in the Actions column.
4. Click the Reconnect button on the confirmation pop-up window.
5. The status appears as Reconnecting.

The endpoint is reconnected to the network after the request is processed successfully, and the endpoint status is updated automatically.

Note: If the endpoint has active critical detections, the system displays a warning before reconnecting the endpoint.

Isolation Status

The following isolation statuses are displayed for each endpoint:

Status	Description
Reconnected	The endpoint is now reconnected
Isolated	The endpoint is currently isolated from the network
Reconnecting	The reconnect request is in progress

The endpoint status is refreshed automatically.

Settings

Report Schedule

Here you can create schedulers to generate reports and send reports to added email address.

Create New Schedule

In Seqrite EDR, you can create schedulers to generate reports and send reports to added email address. You can configure them to include data from Alerts, Incidents and Threat Hunting. You can create daily, weekly, or monthly reports. You can generate reports in the PDF or Excel sheet format. You can add email address to whom the reports are sent.

Note ☛

Only users with Admin or SOC Manager privileges have the ability to schedule reports.

SLA Configuration

Service Level Agreements (SLAs) in Seqrite EDR define the expected timelines for handling and addressing security incidents. They establish measurable commitments for how quickly incidents must be investigated, remediated, and closed. By setting clear deadlines, SLAs help security teams prioritize tasks, track progress, and ensure consistent response across different types of threats.

With Seqrite EDR , SLAs are often configurable by incident type and severity. For example, a phishing alert may require investigation within 2 hours, while a malware outbreak could demand immediate containment. SLA timers are displayed in the grid, and notifications are triggered if deadlines are approaching or breached, ensuring that no incident is overlooked.

Backup and Restore

The Backup and Restore page allows you to back up selected security configurations and restore them when required. Only custom configurations are included in the backup.

To access this page, go to Settings > Backup and Restore.

Create a Backup

Use the **Backup Configuration** section to export selected configuration settings to a backup file.

Select Configuration Types

The **Select Type** field lets you choose one or more configuration types to include in the backup.

The following configuration types are available:

Configuration Type	Description
Custom Detection Rules	Backs up all user-created detection rules
Whitelist Rules	Backs up all configured whitelist rules
Custom Policies	Backs up all custom policies

You can select multiple configuration types. To remove a selected type, click the **×** icon next to its name.

Back Up Configurations

To create a backup:

1. Go to Settings > Backup and Restore.
2. In the **Select Type** list, select one or more configuration types.
3. Click **Backup**.

The system generates and downloads a backup file containing the selected configurations.

Note: System default configurations are not included in the backup.

Restore a Backup

Use the Restore Configuration section to restore previously backed-up configuration settings.

Upload a Backup File

You can upload a backup file by using either of the following methods:

- Drag and drop the backup file into the upload area.
- Click Browse and select the backup file from your local system.

Supported file format: ***.json***

Restore Configurations

To restore a backup:

1. Go to Settings > Backup and Restore.
2. Under Restore Configuration, upload a valid .json backup file.
3. Click Restore.

The system imports the configuration settings from the backup file.

Note: Restoring a backup replaces the existing custom configurations with the configurations contained in the backup file, if applicable.

SMTP Settings

This feature helps you set the SMTP Host Details. All emails from Seqrite Endpoint Protection such as Notification mails and Report mails will be sent to the SMTP Server for further routing.

To configure the SMTP Settings, follow these steps:

1. Go to Settings > SMTP
2. Select the **Enable SMTP Settings** check box.
3. In the **SMTP Server** text box, type the IP Address or domain name of SMTP server.
4. In the **Port** text box, type the port number.
5. Specify the file size in MB. The default value is **10 MB**.
6. In the **Senders Email Address** text box, type the email address.
   This email address will appear as From Address in all the emails sent from Seqrite Endpoint Protection server.
7. Select the **Require Server Authentication** check box.
8. For user authentication, type the user name in the **Username** text box.
   The Username field depends on your SMTP server. It may ask you to provide either user name or email ID.
9. In the **Password** text box, type the password.
10. In User Authentication Method, select one of the following:
    • None: Select this option to send email notification through HTTP protocol.
    • SSL: Select this option to send email notification through SSL (Secure Sockets Layer) protocol.
    • TLS: Select this option to send email notification through TLS (Transport Layer Security) protocol.
11. Seqrite recommends that to ensure the SMTP host details are correct, test the SMTP settings. To test the SMTP settings, click **Test Mail**. After successful verification, click **Apply**.
12. In the Test Mail for SMTP dialog, in the **To** text box, enter the email ID of the user.
13. Click **Send Email**.
    Seqrite Endpoint Protection cannot send emails if the SMTP settings are configured using public mail server (Example: Gmail) and if Allow less secure apps setting is disabled in the public mail servers.

Endpoint View

Navigating to Endpoint View

1. On the Incidents page, in the Incidents table, click **View Details**. In the right pane, Incident Summary appears.
2. Scroll the summary, till the ENDPOINTS AND USERS title appears. You can view the endpoint name.
3. Click the endpoint name.

The endpoint view appears on the page. The endpoint name appears on the topmost line.

List View

The list view is the default view. The List, Timeline are the 2 views available.

The total count of Alerts is shown. You can select one of the following to show the count and the list:

- All Alerts
- Associated Alerts
- Unassociated Alerts

The counts of alerts as per the following Severity are shown.

- High
- Medium
- Low
- Base

The severity is displayed in the color code, also.

The following table describes fields that you can view in the table in the List view.

Field	Description
ALERT NAME	Displays the name of Alert.
ALERT TYPE	Displays one of the following Alert types: Custom Associated Alerts Unassociated Alerts
SOURCE	Displays the source of the Alert
SEVERITY	Displays one of the following Severity: High Medium Low Base
TACTICS	Displays Tactics of the Alert

CREATED ON	Displays the time and date of when the current alert was created. You can sort the displayed list as per the created date of alerts from latest to older.

Actions

Combine With Current Incident

1. Click the caret near count of Active Incidents in the Summary pane. The Other Incidents Associated with Endpoint dialog appears.
2. In the Active Incident tab, list of active incidents appears. Select the incident that you want to combine with current incident by clicking the respective check box.
3. Click **Combine with Current Incident**. The confirmation dialog appears.
4. Click **Combine**.

The success message appears when the incident is combined.

Associate with Incident

1. Select Unassociated Alerts option. The list of unassociated alerts appears.
2. Select the alert that you want to associate with the incident by clicking the respective check box. The **Associate with Incident** button is enabled.
3. Click the **Associate with Incident.** The Select Incident dialog appears.
4. Select an incident with which you want to associate these base alerts. You can search the incident by name or ID in the list.
5. Click **Associate with Incident.**

Remediation actions

During Alerts analysis, if you find any endpoint is running malware, you can perform the following remediation actions on that endpoint.

The endpoint isolation and restore feature allows IR to isolate the endpoint from the network when an endpoint is running malware, to ensure the malware doesn't spread to other endpoints.

When the endpoint is isolated, IR runs an investigation and resolves security issues. Once the endpoint is clean, IR can reconnect the endpoint to internet.

- **Isolate**: This action will isolate the endpoint from the network. This action will ensure that the malware is not spread in the network. This option is available only if the endpoint is infected. After isolation, IR runs an investigation and resolves security issues.
- **Reconnect** : This action will reconnect the endpoint to the network. Once the endpoint is clean, IR can reconnect the endpoint to the network with this action. This option is available only if the endpoint is isolated.

Selecting the View duration

You can view the alerts in the following hours, days, or weekly or monthly slots:

- Hour wise
    - Last 1 hour

    - Last 3 hours
    - Last 6 hours
    - Last 12 hours
    - Last 24 hours
    - Today (Since midnight 12.00 AM)
- Day wise
    - Last 7 days
    - Last 15 days
    - Last 30 days
- This week (since Sunday midnight 12.00 AM)
- This month (since the beginning of the month)

Filter option

Using the Filter View

Apply the filters to narrow down your search criteria for displaying the alerts. You can filter by Incident and Incident Type.

Timeline view

You can view the number of alerts as per Severity on a date & time scale. The single alert is represented as a small solid circle and a cluster of alerts generated at the same time is represented as a count+ in a circle.

Color Code Legend

Color of dots	**Activity related to**
Yellow	Process
Purple	File
Blue	Network
Green	Registry

Additionally, you can do the following:

We can zoom in and out using mouse. We can adjust the time window, if there are multiple alerts at the same time, then there will be a circle with a count on this view, else it will be a solid circle for a single alert.

Also, when the user clicks on this count in the circle on this view, the user can see details on the right-side panel.

Also, when the user clicks on this solid circle on this view, the user can see alert details on the right-side panel.

When the user clicks on the count in the circle, then on the right-side panel all the alerts that occurred at that same time are displayed. The User can see further details of the alert by clicking on the alert name.

Also, we can select the timeline view as per Day/Week or Month from the upper right corner list.

Using the Filter View for Key Attributes

Apply the filters to narrow down your search criteria for displaying the alerts. You can filter by Key Attributes name, type, and reputation.