Seqrite
Endpoint Protection

SEQRITE

EDR User Guide

EPP 8.3

www.seqrite.com

Copyright Information

Contents

Overview

The Endpoint Detection and Response (EDR) is a platform deployed on an organization's infrastructure rather than on a cloud-based environment. It is a system designed to protect the endpoints from the network from potential cyber threats. EDR helps detect and respond 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

EDR Server Supported OS

EDR Server only supports the Linux OS with Ubuntu 22.04 LTS server edition.

EDR Endpoint Supported OS

- Windows
    - Windows Server 2012, Core 2016 and 2019
    - Windows Server 2022, 2019, 2016

- o Windows 7, 8 (EPP), 10, 11
- Linux
  - o CentOS 7.0+,
  - o Red Hat Enterprise Linux (RHEL) 8.1 and later,
  - o Mint 18.1 SUSE Linux 11.4+,
  - o Ubuntu 18.04+,
  - o BOSS 6,7,8
- Mac
  - o Latest versions from and after Mac 10.15

Installation of EDR Edition

Please refer to the Deployment guide for installing EDR edition.

Glossary

Term	Description
EDR	Endpoint Detection Response
Endpoint	A client agent system.
EPP	Endpoint Protection Policy
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, result in the 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 a 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 block-listed through the blocklist service at the server end. Blocklist data is sent to EPS and the existing protection service will process the block listing the process or file at the 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 IOCs that automatically performs periodic scans on historical data of the enterprise endpoints and takes response actions on match

Architecture
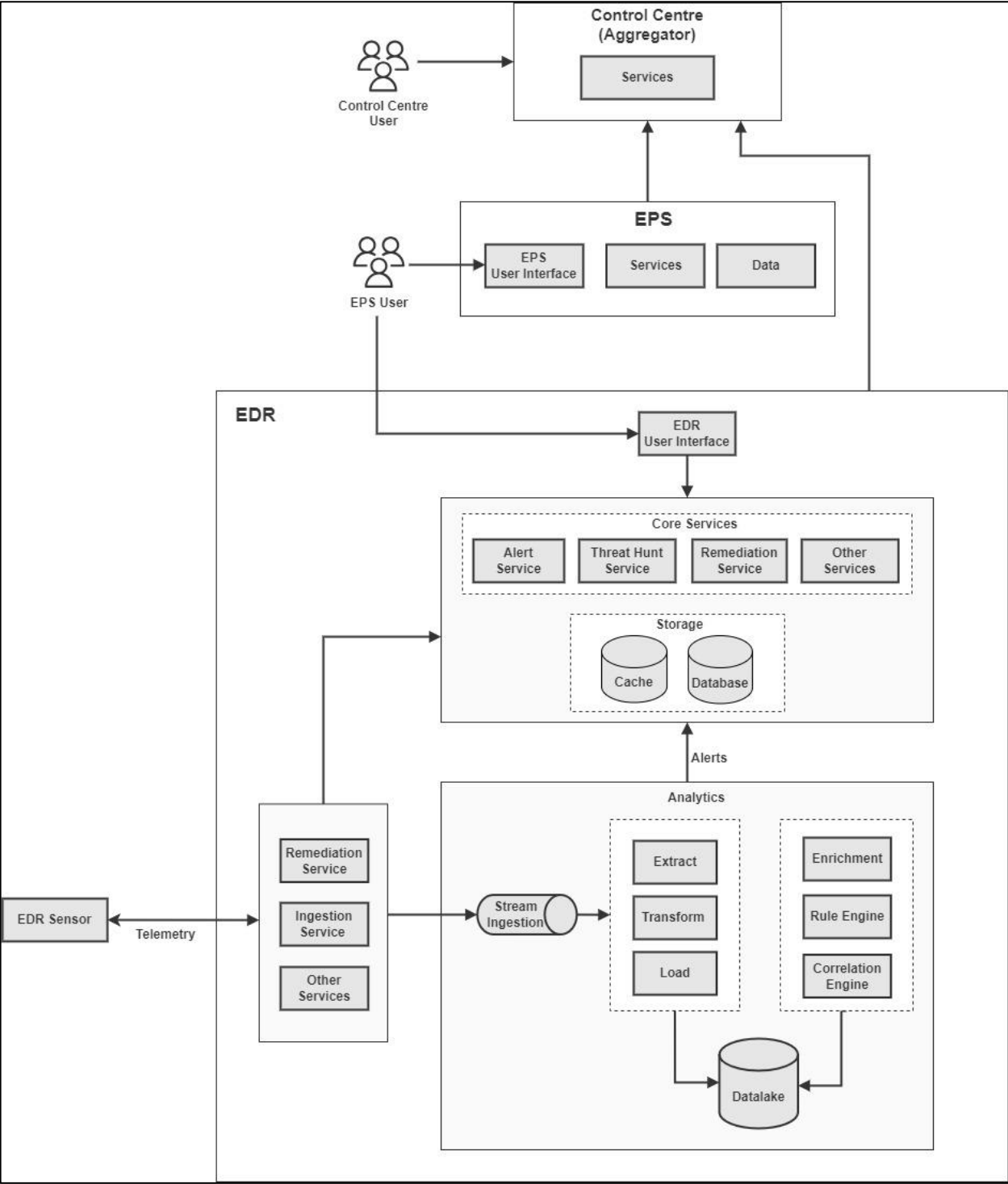
Getting Started

Follow these steps to log in to Seqrite EDR.

1. Login to the EPP console. The login process utilizes Single Sign On authentication.
2. On the EPP console in the left panel Select **Advance Protection**
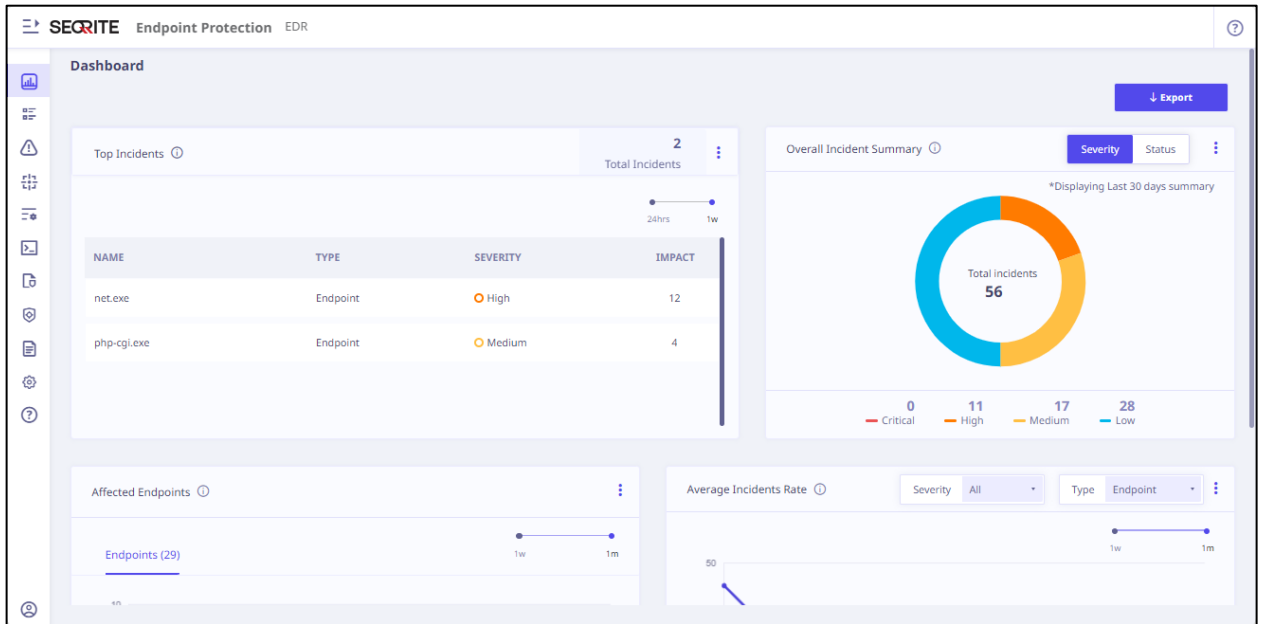3. Click **EDR**.
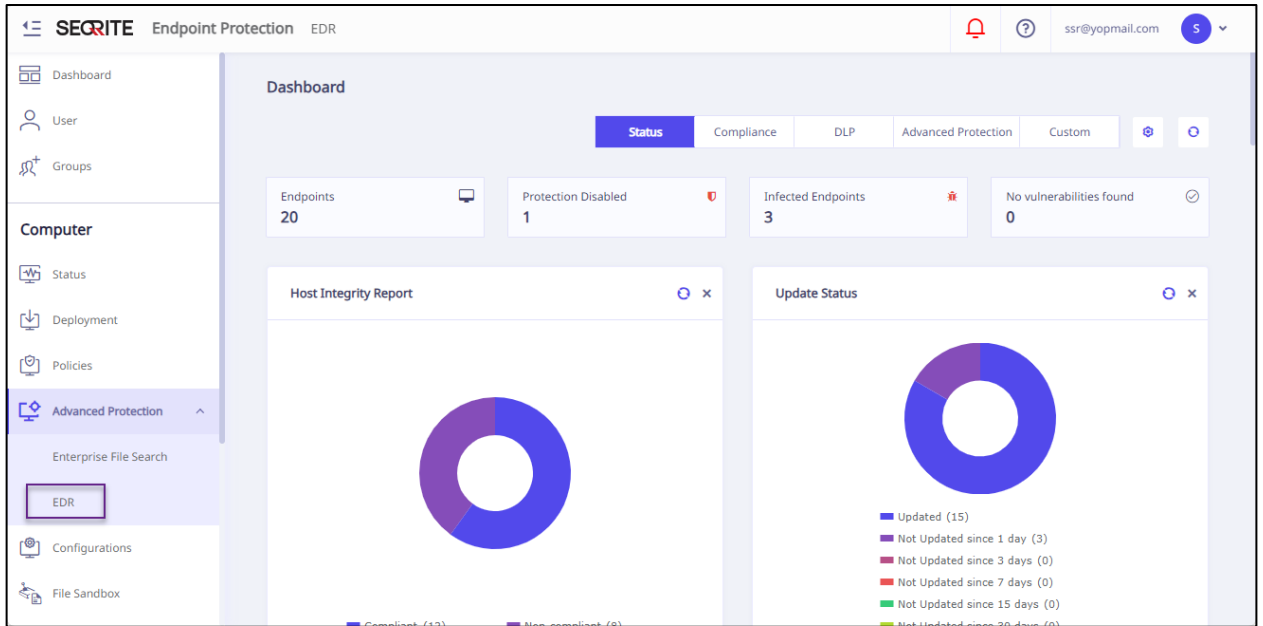
The EDR dashboard page appears in a new window.
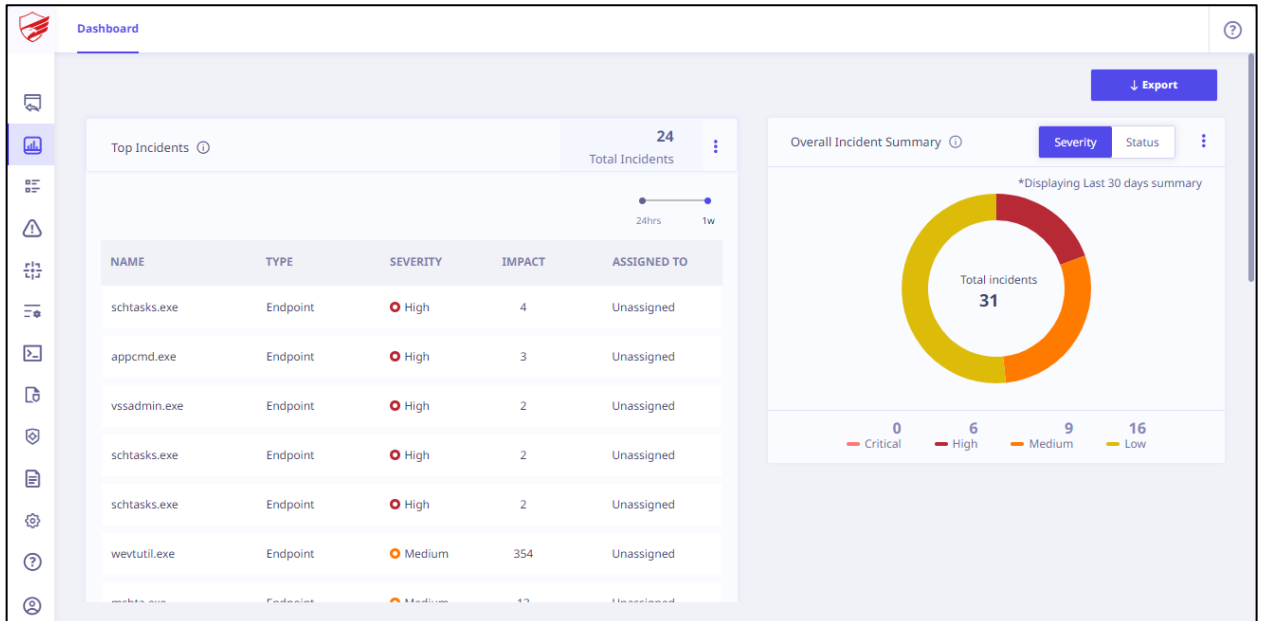
Go to [Dashboard](#) for more information.

Dashboard

The Dashboard provides a comprehensive overview of endpoint incidents through various charts and graphs, offering a high-level perspective of your organization's security status.

The Dashboard consists of the following tables, graphs, and other details.

Export

This feature enables you to download a report in both PDF and Excel format.

Top Incidents

It presents a tabular format listing the top incidents that occurred on an endpoint.

Column	Description
NAME	Displays the name of the incident that occurred.
TYPE	Displays the type of device where the incident occurred. It could be an endpoint email, network, and so on.
SEVERITY	Displays the severity under which the incident occurred. The severity level is pre-defined in the policy. It could either be Critical, High, Medium, Low, or Base.

IMPACT	Displays the number of alerts generated due to this incident. Displays the number of alerts linked to the defined incident.

Overall Incident Summary

It presents a doughnut chart providing statistical data on all the incidents.

Tab	Description
Severity	Displays the total number of incidents segmented by severity levels. • Critical • High • Medium • Low • Base
Status	Displays the total number of incidents categorized by their status, including: • New • Investigation • Remediation • Closed

Affected Endpoints

Displays the number of endpoints affected over time.

Average Incident Rate

Displays the incoming incidents and closed incidents listed. You can sort it depending on the severity of the status.

Column	Description
Severity	Select the severity from the drop-down values.
Type	Select the type of incident from the drop-down values.

Incidents

An incident occurs when a group of alerts is detected across all endpoints in an interconnected environment based on predefined rules.

Incidents are the final culmination of all detections that happen in the environment.

One or more alerts are correlated and grouped to form Incidents. The Security Analyst will work on the Incidents list and perform various investigation and response functions.

Alerts are linked by internal analytics based on multiple parameters such as source, rule, qualities, location, or a combination of these. Alerts are used to classify and produce incidents, which are then assigned a severity and priority.

Applying filters will enable incident classification based on severity. The System Analyst assigns the Incident priority.

Multiple alerts can be added to an incident during the investigation, either automatically or manually.Incident details can be exported for reporting purposes. Detailed information on New, Closed, Remediation, incidents can also be identified from the list.

Column	Description
INCIDENT ID	Select the severity from the drop-down values.
INCIDENT NAME	Select the type of incident from the drop-down values.
TYPE	The type of Incident is based on the Source of the initial alert based on which the Incident is formed. It could be one of the following: • Endpoint • Insider Threat
SEVERITY	The severity of the incident is based on the combined severity of the alerts that are part of the incident.
PRIORITY	The System Analyst assigns priority.
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.
UPDATED On	Displays the updated time stamp for which an alert was linked with the incident.

Filter

You can add filters to refine your search criteria for displaying the incidents. You can filter by Severity, Status, and Alert Details such as Process Name, Host Name, and Tactics.

My Incidents

Toggle the **My Incidents** button to true to view only the incidents that are assigned to you (logged-in user).

View

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

- Hour wise
    - o Last 1 hour
    - o Last 24 hours
- Day wise
    - o Last 7 days
    - o Last 15 days
    - o Last 30 days
- Custom – Clicking Custom opens calendar control. Select **From Date** and **To Date** from the calendar. Click **Save**.

View Details

When you click **View Details**, an **Incident Summary** side panel appears on the right of your screen.

Incident Summary

Column	Description
View Audit Report	Click the **View Audit Report** icon. The **Incident Canvas** dialog appears. You can access the following 3 tabs: • Investigation Timeline – This tab displays investigation details organized by Date. The window displays the time, name of assignees, status, and notes. • Alert Remediation – This tab displays the actions taken to mitigate any potential threats or issues. • Notes – The Notes tab displays notes added as per time stamp. • Root Cause Analysis – This tab displays the root cause analysis of the incident. • Click **Export Audit Report** to download the report in PDF format.
Add Note	Click the **Add Note** icon to add a note. The **Add Note** dialog appears. Enter the note and click **Save**. The confirmation message appears. In the Notes section of the Incidents Summary, you can view all the Notes.
Basic Information	
Incident ID	Displays the ID of the Incident. You can copy the ID by clicking the copy icon.
Incident Name	Displays the name of the Incident. You can edit the name by clicking the edit icon.
Incident Type	Displays one of the following types of Incidents. • Unknown

	• Phishing • Malware • MITM • Insider Threat • Privilege Escalation • Web Application Attack • Anomaly Detection • APT You can edit the type by clicking the edit icon.
Created On	Displays the date and time when the Incident was created.
Occurred On	Displays on which endpoint the incident occurred.
Last Updated On	Displays the date and time when the Incident was updated.
Number of Alerts	Displays the number of alerts already associated with the incident.
Response Summary	
Severity	Displays one of the following Severity. This is system generated: • Critical • High • Medium • Low
Priority	Displays one of the following priorities: • Critical • High

	• Medium
	• Low
	You can edit the priority by clicking the edit icon.
Status	Displays one of the following statuses: • New • Investigation • Remediation • Closed
Description and Analysis	
Description	Displays description of the incident. You can edit the description by clicking the edit icon.
Notes	
Notes	Displays all notes along with their creators and timestamps. You can view the content of each note by clicking on them individually. Additionally, you can contribute new notes by clicking on the **Add Note** icon.
Endpoints and Users	
Endpoints (#)	Displays the hostname(s) of the endpoint(s) on which the incident took place/connected to the incident.
Users (#)	Displays the email addresses of all users connected to the Incident.
Key Attributes	
Process	Displays the: • count and list the process. • value of the process. • reputation of the process. • the alert to which the incident is associated.

Registry	Displays the • count and list of Registry Keys. • the alert to which the incident is associated
File	Displays the • count and list of infected files. • the value of the file. • the reputation of the file. • the alert to which the incident is associated.
Network	Displays the: • count and list of infected networks. • the Value of the network. • The reputation of the network. • The alert to which the incident is associated.
Vertical ellipse ⋮	If you click the vertical ellipses, the list of playbooks appears with the status of whether the playbook is run or not. You can run the playbook by clicking the run icon.

Navigating to Endpoint View from Incident

You can view the endpoint details such as the alert that appeared on the endpoint, its type, severity, and so on from the Incident page.

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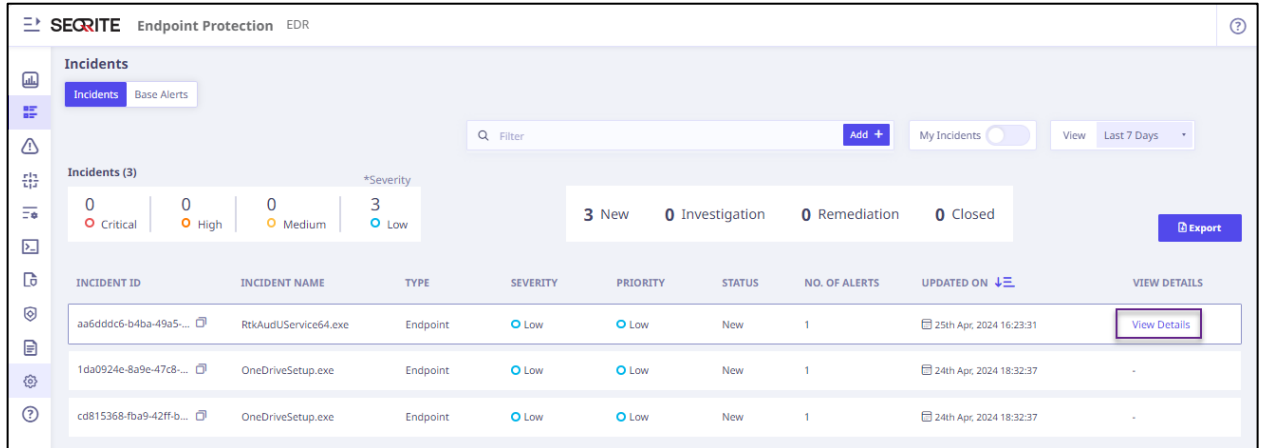
In the right pane, Incident Summary appears.
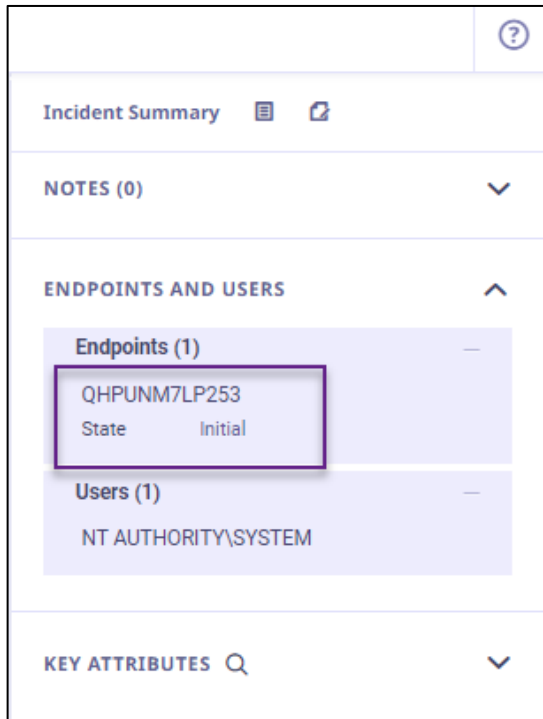
2. Scroll the summary, till the ENDPOINTS AND USERS title appears. You can view the endpoint name.

3. Click the endpoint name.

Summary

Column	Description
Incident Details	
Incident ID	Displays the ID number of the incident.
Incident Name	Displays the name of the incident.
Type	Displays the type of the incident where it occurred.
Severity	Displays the severity of the incident.
Priority	Displays the priority of the incident.
Status	Displays the current status of the incident.
No. of Alerts	Displays many alerts that occurred in the incident.
Updated On	Displays the date and time of the last update.
View Details	Click the **View Details** link to open the incident summary.
Endpoint Details	
Endpoint Name	Endpoint Name
Severity	The Alert with the highest severity for the endpoint
Infected on	The first date when alerts were seen on the endpoint
Associated Alerts	
Operating System	The Operating System of the endpoint
Platform	The OS platform
Platform Architecture	The OS Architecture

IP Address	The IP Address of the endpoint
MAC Address	The MAC Address of the endpoint
Reputation Score	The Reputation set for the endpoint
Endpoint status	Whether the endpoint is connected or isolated
Incidents Associated with Endpoint	
Active Incidents	This shows the number of active incidents associated with the Endpoint.
Past Incidents	This shows the number of past incidents associated with the Endpoint.
Key Attributes	
Process	• Displays the count and list of processes. Also, • Displays Value of the process. • Displays Reputation of the process. • Displays Associated To which alert.
Registry	• Displays the count and list of Registries. Also, • Displays Value of the registry. • Displays Reputation of the registry. • Displays Associated To which alert.
File	• Displays the count and list of infected files. Also, • Displays the Value of the file. • Displays the Reputation of the file. • Displays Associated To which alert.
Network	• Displays the count and list of infected networks. Also,

|	
	• Displays the Value of the network. • Displays Reputation of the network. • Displays Associated To which alert. • If you click the vertical ellipse, the list of playbooks appears with the status of whether the playbook is run or not. You can run the playbook by clicking the Run icon.
Remediation	• Set Reputation o Poor o Normal • Isolate Confirm if you need to isolate the endpoint.

Base Alert - Alert List View

The Alert list view shows all the alerts on the specific endpoint in the selected timeframe. You can change the time frame filter or other filter at the top.

The fields are:

Column	Description
ALERT NAME	Displays the name of Alert.
ALERT TYPE	Displays one of the following Alert types: Custom Associated Alerts Unassociated Alerts
RULE NAME	The Rule Name due to which the alert was triggered
SOURCE	Displays the source 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.
TACTICS	Displays Tactics of the Alert

The list view is the default view. This can be switched to Timeline view.

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.

Remediation Actions

You can take manual remediation actions on the endpoint:

Isolate or Unisolate: Isolate the endpoint or if it is already isolated, you can unisolate the endpoint.

Set Reputation: Analyst can set the reputation of the endpoint to: Poor, Normal, Good, depending on investigation.

Alerts

Alerts are automatically triggered on the endpoints when a MITRE Rule condition is met and are then sent to the server, where they are displayed on the dashboard.

When an event is generated at an endpoint, if the condition of the event matches any preexisting rule, it triggers an alert which is sent from EDR agent to the central console.

Whatever policy is applied for that alert is shown here on the alerts screen as well. It also displays what action was taken as a part of that policy.

Alerts can be viewed based on the endpoint view or on the alerts list. The endpoint option lists the name of the machine along with the alert type and severity of the alert.

Endpoints view:

Alerts List view:

Rule Builder

Rule Builder allows users to configure personalized rules to monitor unusual activity on endpoints.

In Seqrite EDR, you can create rules based on exclusive activity by some process, host or network host, or a combination of multiple events across hosts. After you create and save a rule, it is automatically pushed to the endpoints and the events from endpoints are analyzed as per the conditions in the rules. If the conditions specified in that rule are met, then custom rules get executed on the server. The alerts may generate Incidents and the administrator can then assign these Incidents to the SOC Manager, or the SOC Analyst. Later assign the cases to self or another SOC Manager/Analyst to find out the root cause, and range of infection, and carry out any mitigation activity as required.

The following table lists the indicators that you can use to build rules with appropriate operators and values.

You can use logical operators such as AND, and OR for the rules.

Process Name	Process Path	Process Command Line	Parent Name	Host Name
Command Line Length	Is Browser Process	File Download Option	Is Process Signed	user_name
proc_sha2	proc_md5	Parent Path	Parent Command Line	Parent_Bin_Is_Signed
Grand Parent Name	Grand Parent Path	Grand Parent Command Line	Grand_Parent_Bin_Is_Signed	cp_event_type
cp_given_access	cp_desired_access	cp_target_proc_name	File Name	File Path
SHA2	MD5	file_path	file_attr	file_new_path
file_md5	file_type	mod_md5	mod_sha2	mod_path
ehp_type	ehp_md5	ehp_sha2	ehp_path	action

Protocol	Port	IP	URL	nw_method
nw_domain _name	nw_dns_ips	nw_conn_typ e	Registry Key	Registry Value
Registry Value Data	Windows Event Id	Field of Interest		

Alert Analysis

Alert analysis – Remediation Actions

On Endpoint

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

- 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 when there is at least one alert from the infected endpoint. During the isolation state, the infected endpoint can communicate only with the EDR server to receive further remedial actions.

- 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.

- Set Reputation: The reputation of the endpoint can be set to Poor, Normal or Good

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.

Color Code Legend

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

Additionally, you can do the following:

- You can zoom in and out using a mouse. You can adjust the 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 you click on this solid circle on this view, then you can see respective event on tree as well as details on right side panel.

- When you click on concentric circles, then on right side panel all the concurrent events occurred at that same time are displayed. You 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.

Alert Summary

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.

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. Any alert that matches the whitelisted rule becomes visible under the "Whitelisted alerts view" tab. 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. These alerts are then listed under the Whitelisted Alerts.

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.
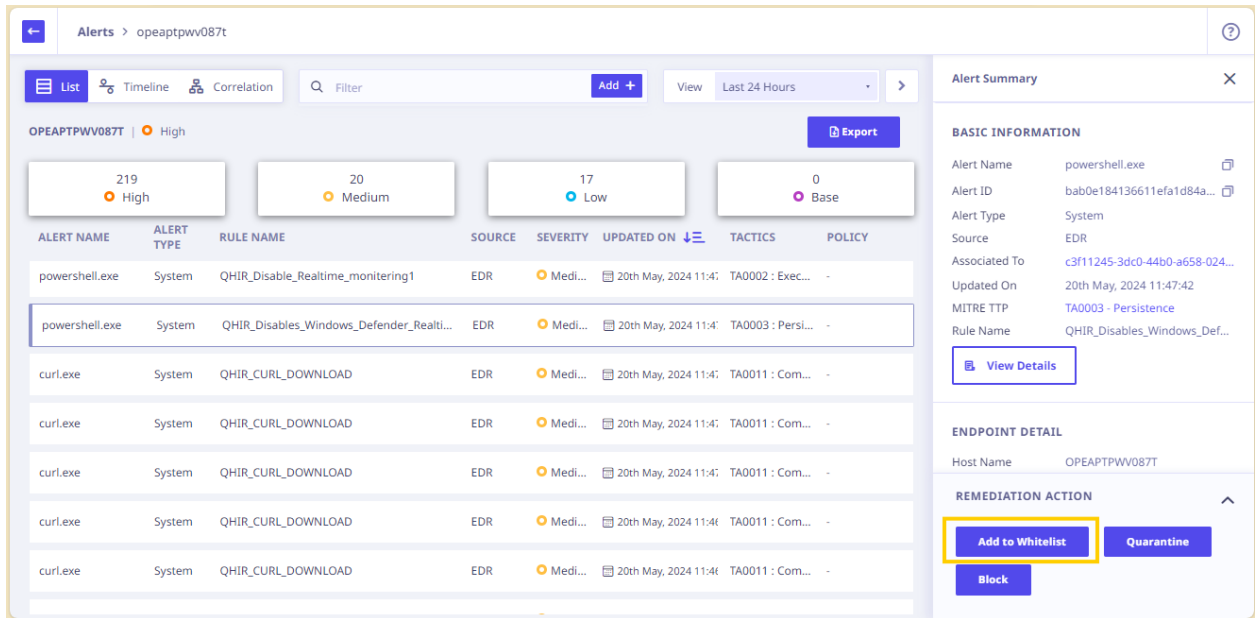
4. In the Add to Whitelist dialog, enter a name for the Whitelisted rule.
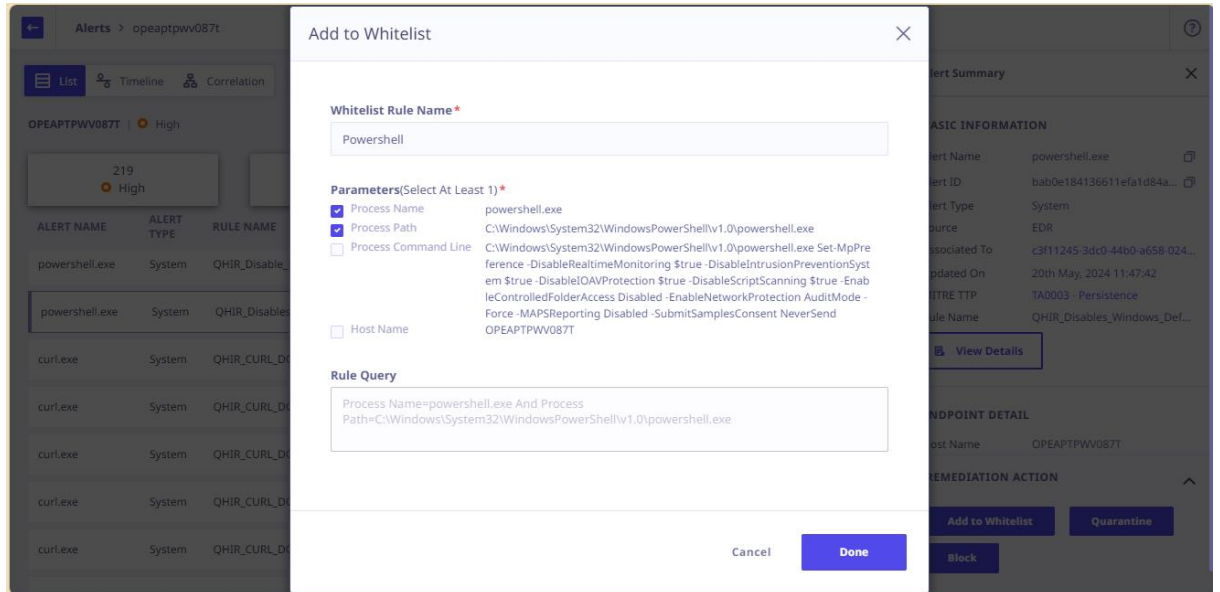
5. Select the parameters as required from the displayed parameters. The parameters will appear depending upon the process.

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. Alerts generated for this rule would be available under the **Whitelisted Alerts** only. You

can sort the Whitelisted Rules by Timestamp. You can delete the Whitelist Rule with the help of the **Delete icon**.

Base Alerts

Base alerts are alerts that are informational in nature and are not correlated with any incidents by default. It can be manually associated to an Incident, or a new Incident can be created from it.

Threat Hunting

Hackers and malicious players are using new techniques to infiltrate your network, remain in stealth mode for a long period, and collect confidential information, or login credentials from the endpoints in your network. This information is later used to access other systems in your network. Threat hunting capability in Seqrite EDR helps you detect such hidden threats, unusual behavior, and infiltration activities in your network before they cause actual harm. You can then mitigate these threats and secure your IT infrastructure.

An incident responder (IR) usually relies on investigation of such known Indicators of Compromise (IOCs), and Indicators of Attack (IOAs).

An IOC is digital evidence on a computer that points to a breach of network security. These may be an MD5 hash, a C2 domain or hardcoded IP address, a registry key, filename, etc.

- An altered MD5 hash may point to a file being compromised.

- Callbacks to command-and-control (C2) servers indicate breach or compromise. You may receive information about C2 servers through your own analysis or through threat sharing groups. This may be a particular domain name or a hard-coded IP address.

- A change in typical registry values, or a change in filename may be a red flag. If you find anything from the above IOCs, your systems may already have been compromised.

In Seqrite EDR, analysts can proactively search for such instances in your historical verbose telemetry database collected over 30 days from across the endpoints or hosts in your network. Threat hunting helps you detect compromised processes even though an alert may not have been generated for a process. You can create and run queries that are a combination of specific IOCs indicator filters and store the queries for future use. After you run a specific query on the Threat Hunting page, Seqrite EDR performs a search through the database and displays the corresponding alerts or compromised processes. You can use saved queries to run a fresh query or use the filters from a saved query to create a new query and save it for future use.

You can use the following IOC indicator filters to create, run, and save a search query. For the purpose of brevity, we shall call these indicators as filters in the following tasks:

Filter	Description
SHA2	Enter a specific value of SHA2 that you want to search in the EDR database.
MD5	Enter a specific MD5 checksum that you want to search in the EDR database.
Command line	Enter a command line argument that is used to run a particular file or execute a particular process.
Name	Enter a name string that you want to search. You can enter a filename also.
Path	Enter a file or directory path that you want to search.
IP	Enter the IP address of a C2 server that you want to search from the logs.

URL	Enter the URL for a suspicious domain to which you suspect that a callback has been made from your network.
Host Name	Any specific host that you want to search for
Time frame	The time frame for which to search the data in

Theat Intelligence based IOC Search

Seqrite acquires latest Threat Intelligence from multiple Threat feeds in various transfer formats including STIX/TAXI and stores in centralized Threat Intelligence Platform. Seqrite also as well as sources Theat Intelligence from Seqrite Labs, on the latest malware targeting endpoints. These Threat Intel Indicators of Compromise are updated on the Threat Intel server and are periodically (every 24 hours) searched across the events store database, in order to see if these threats are ever seen in the environment.

A Security Analyst can also add custom IOCs to the Threat Intelligence platform.

If any event matches any IOC stored in the Threat Intelligence platform, a high severity alert is raised.

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 host from the list. This is the endpoint 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. The scope of the query should be reduced, if required, in this case.

- 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 available for Windows, Linux and macOS.

Saving Live Query

Analyst can save a Live Query and can invoke it later, by choosing from a list of saved queries.

Reports for Alerts

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.

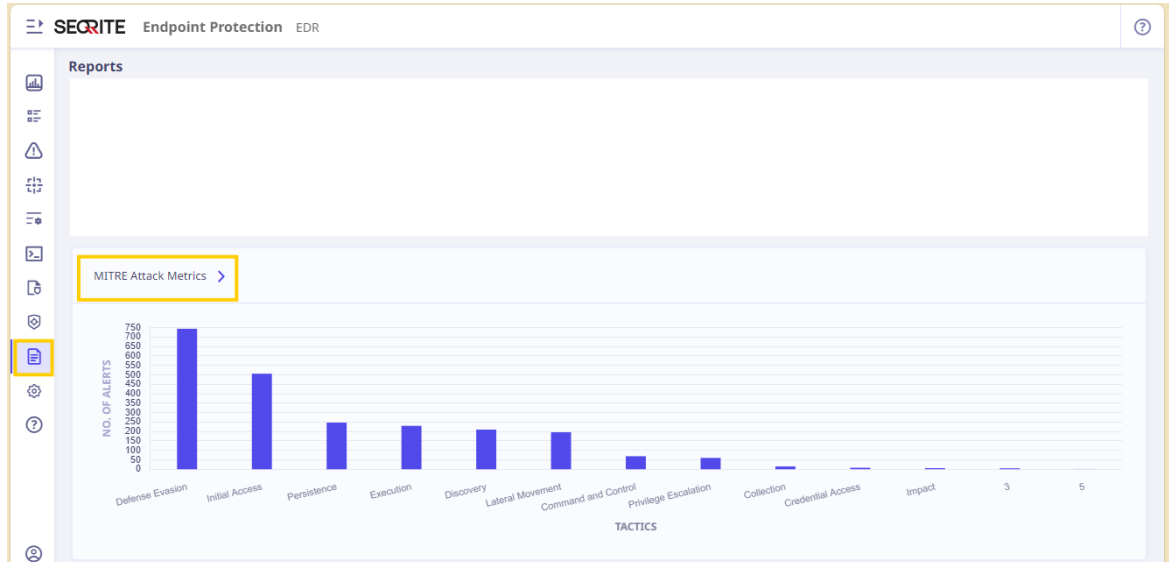Reports can be exported immediately or scheduled for export.

Alert over time Report:

This shows the number of alerts over time in the environment.
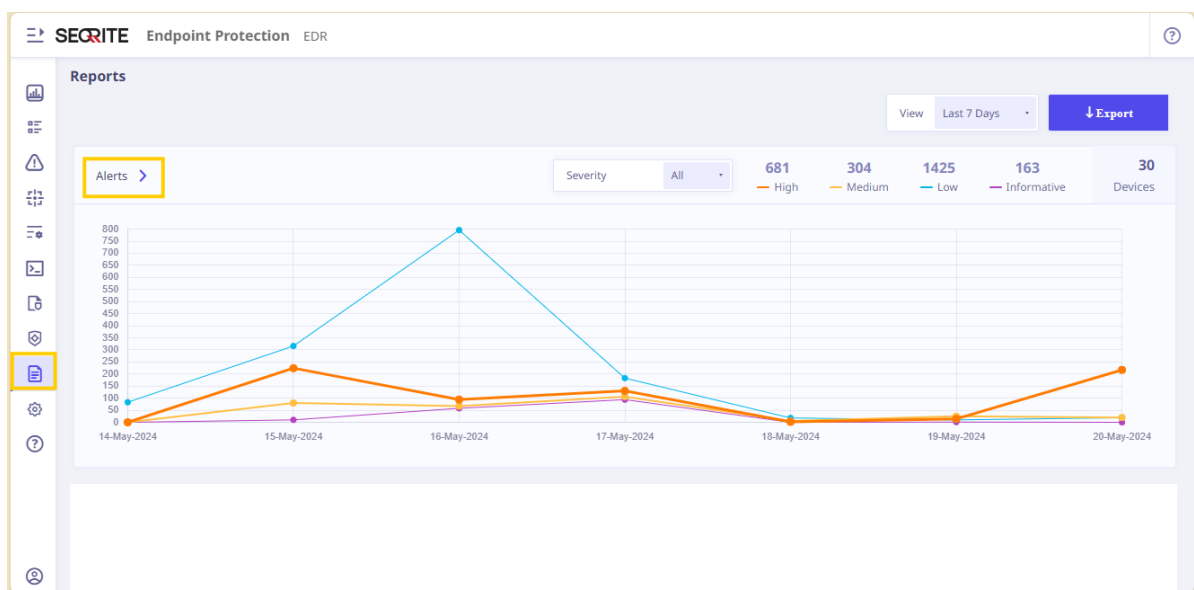
MITRE attacks metrics

This shows the cumulative metrices of MITRE Attack Tactics of the various alerts in the environment:

Risk based Response Actions

Seqrite EDR allows Risk based response actions to be taken. The way this is done is through definition of endpoint groups as well as individual endpoints that can be added to scopes. Action Policies are defined for particular scopes that define the actions to be taken in case a specific alert is seen for an endpoint in the scope.

The devices in a particular environment can be imported from Active Directory or via excel manually.

Groups

Groups can be defined based on AD attributes, or it can be based on dynamic tags as defined by Administrator. Endpoints that are tagged with certain attributes can be part of specific groups. This allows for well-defined, granular, and dynamic grouping of endpoints.

Scope

There are 4 scopes – Critical, High, Medium, Low. There is also an Undefined scope.

Endpoints can be added to scopes based on the criticality of the endpoints.

Critical scope endpoints and groups are those endpoints that are critical to the running of the business. The critical of the endpoint is reduced as it move down the hierarchy Critical -> High->Medium->Low. Low scope can be opened for more aggressive

automated responnse actions whereas Critical scope can be defined for more conservative impact actions.

In the view, the groups can be Filtered by the scope, and by the selected
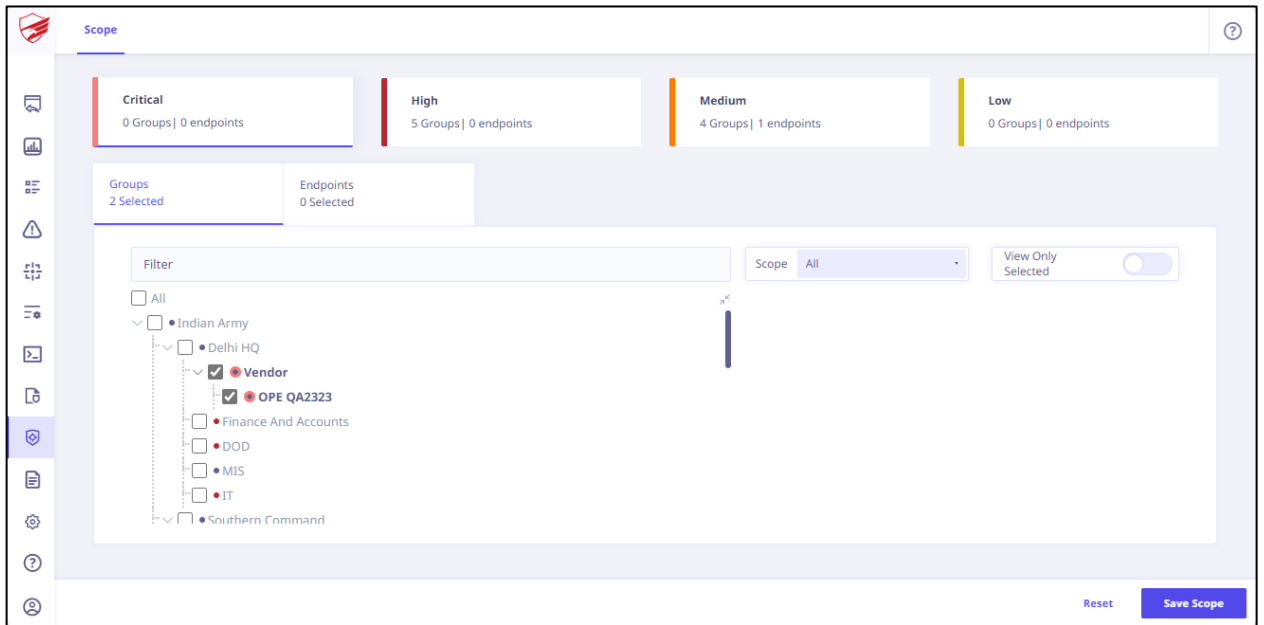
Policies

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.