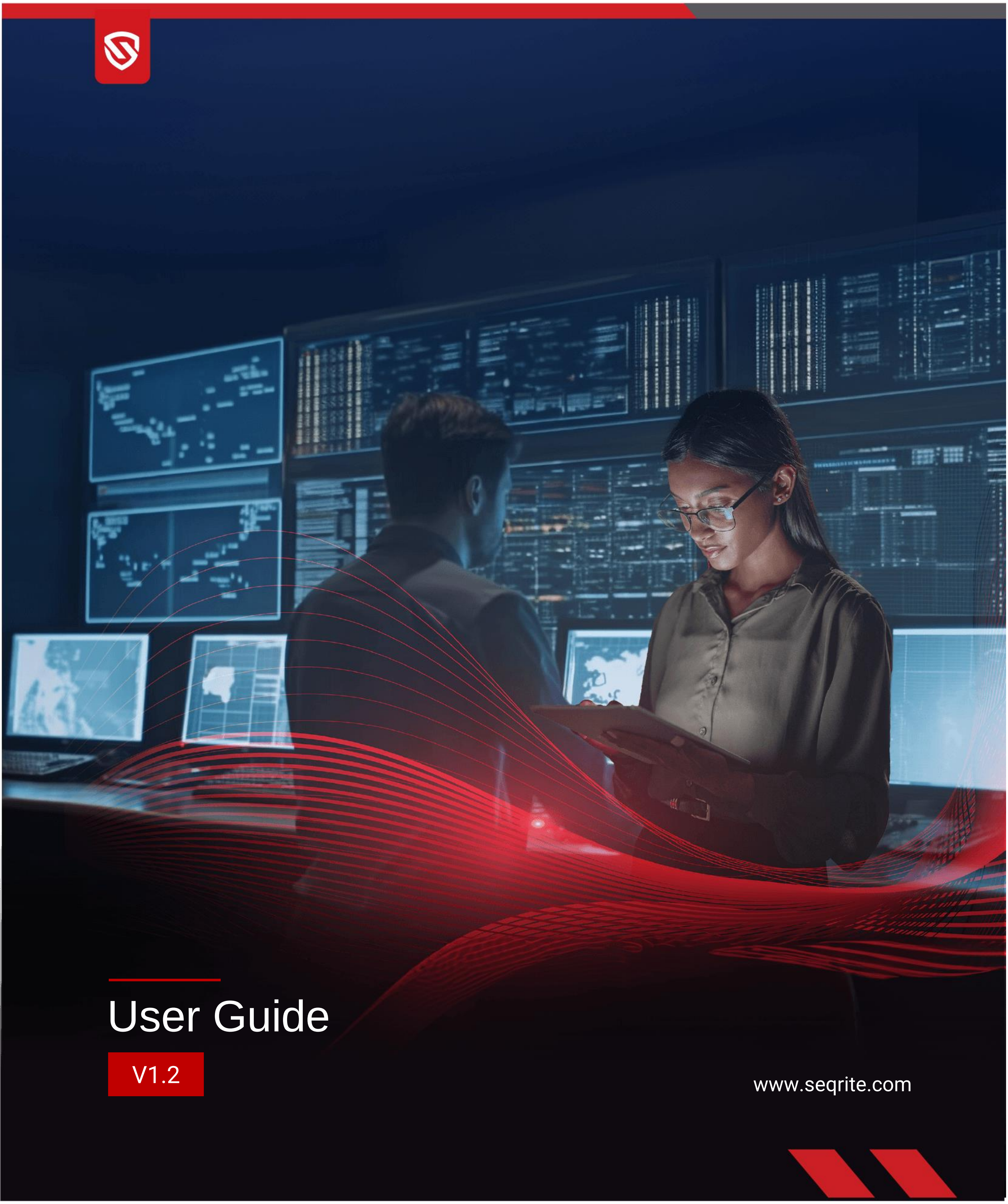
Malware Analysis Platform

SEQRITE



User Guide

V1.2

www.seqrite.com

Copyright & License Information

Trademarks

License Terms

Release date

April 5, 2024.

Contents

1. Introduction

In the present era of connected world, various devices communicate through the Internet frequently. Data is exchanged, sent, received, and passed through multiple host computers that make the data vulnerable to infection from viruses and malwares. Therefore, it is necessary to check whether the data is clean or infected with malicious programs. Often, malicious programs that spread silently in the devices are unnoticed and can infect the data files and other legitimate program files.

Malware Analysis Platform is a web-based portal that enables users to submit and analyze suspicious files.

How does Malware Analysis Platform Work?

Malware Analysis Platform is an automated malware analysis system hosted in the Quick Heal premises wherein users can upload their data and executable files and get them scanned and analyzed for malwares and viruses. Users can search using MD5, SHA-1 or SHA-256 hash of any file in absence of the actual file. Also, users can check the category of URLs before browsing.

The files submitted by the users are not shared publicly. Hence there is no risk of sensitive user files being available on the Internet as is the case with the other public malware analysis portals.

Users can check whether the file is clean or malicious from the consolidated analysis summary of the submitted file. After analysis, the report generated by various micro services is stored in Malware Analysis Platform database that can be used for searching in case the actual file for scanning is not available with the user.

2. Getting Started

To access Malware Analysis Platform, you require the following:

- Minimum versions of browsers
    - Google Chrome - Version 110.0.5481.178
    - Microsoft Edge - Version 110.0.1587.63
- Users need to have an account on Malware Analysis Platform to upload, search file or URL.
- Hash checksum for the files that you want to search, or the suspicious file that you want to submit for analysis.
    - Supported hashes are MD5, SHA-1, SHA-256.
- Submitted file size should be less than 128 MB.

3. Accessing Seqrite Malware Analysis Platform

If you are an existing subscriber, follow the sign in process. If you are a new subscriber, follow the sign-up process.

Signing Up

1. Enter the URL https://smap.seqrite.com/ in the browser.
   The Login page is displayed.
2. Enter first name, last name, and email address.

   Note: Do not use disposable email service providers such as Yopmail and Mailinator.
3. Enter password and confirm password.

   Password must contain at least ten characters, and must include one letter, one number and one special character.
4. Select the Captcha mark to confirm that you are not a robot.
5. Select the checkbox to confirm your acceptance of the privacy policy. Acceptance of privacy policy is mandatory to complete the Sign-Up process.
6. Click **Register**.

   You will get a link to activate your account on your email address.
7. Click the link for activation. You will be logged on to the Malware Analysis Platform portal.

Signing In

1. Enter the URL https://smap.seqrite.com/ in the browser.
   The Login page is displayed.
2. Enter Email and Password. Select the Captcha mark to confirm that you are not a robot.

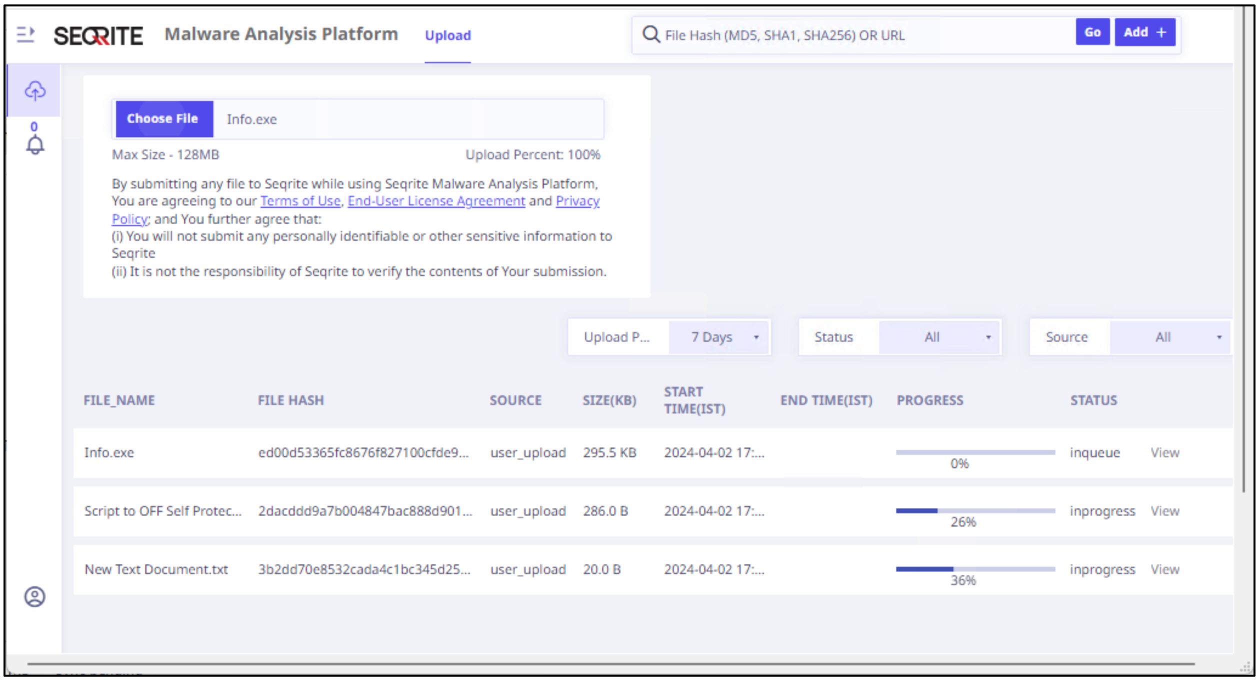
   Note: Do not use disposable email service providers such as Yopmail and Mailinator.
3. Click **Sign In**.
   The Home page is displayed.

4. Home

Home is the default page that is displayed after you log on to the Malware Analysis Platform console. You can also navigate to the Home page through the Search option on the left pane. The Home page displays the following options:

- Upload
- Global Search
- Search Filters

The Home page also displays the history for the uploaded files.


SEQRITE
Malware Analysis Platform
Upload
File Hash (MD5, SHA1, SHA256) OR URL
Go
Add +
0
Choose File

Info.exe

Max Size - 128MB Upload Percent: 100%

By submitting any file to Seqrite while using Seqrite Malware Analysis Platform, You are agreeing to our Terms of Use, End-User License Agreement and Privacy Policy; and You further agree that:
(i) You will not submit any personally identifiable or other sensitive information to Seqrite
(ii) It is not the responsibility of Seqrite to verify the contents of Your submission.

Upload P... 7 Days | Status All | Source All

FILE_NAME	FILE HASH	SOURCE	SIZE(KB)	START TIME(IST)	END TIME(IST)	PROGRESS	STATUS	
Info.exe	ed00d53365fc8676f827100cfde9...	user_upload	295.5 KB	2024-04-02 17:...		0%	inqueue	View
Script to OFF Self Protec...	2dacddd9a7b004847bac888d901...	user_upload	286.0 B	2024-04-02 17:...		26%	inprogress	View
New Text Document.txt	3b2dd70e8532cada4c1bc345d25...	user_upload	20.0 B	2024-04-02 17:...		36%	inprogress	View

Upload

You can submit a file for analysis, search through the upload history, and filter the upload history of submitted files by days, status, and source of submission.

Choose File

You can upload a single file, that is scanned by Malware Analysis Platform, and then view the generated analysis report. The file size must be less than 128 MB. The threats, if any, are detected by various scanners and highlighted in the generated consolidated report.

Uploading a file

To upload and submit the file for analysis, follow these steps:

4. On the Home page, navigate to **Upload** and click **Choose File**.
5. Navigate and select the file that you want to submit for analysis.

   The file is submitted for analysis, and the progress and status, displayed in the list along with submitted time stamp. See Upload History for more information.
6. Click **View** to view the analysis of the submitted file. See Analysis Report for more information.

   Note: The initial analysis report can take around two minutes to generate, especially if the sample being analyzed is large or system is under heavy load. In case the analysis is not completed in two minutes then the analysis continues in the background. You can refresh the page to view the updated analysis report.

Upload History

Malware Analysis Platform displays the file upload history for submitted files. You can filter the details by upload period, status, and source.

Upload Period

The details of the uploaded files can be viewed for the following intervals:

- 1 Day
- 7 days
- 1 Month
- 3 Month

Status

Status Information for the uploaded files can be one of the following:

- All - To view all the uploaded files.
- Inqueue - Waiting to be processed.
- Invalid - Invalid file request.
- Pending - File analysis pending.
- Failed - Analysis has failed.
- Not Found - File download tried multiple times but not found.
- File Size not supported - Searched file size exceeded limit.
- File Type not supported – Searched file type not supported.

- In Progress - File analysis in progress.
- Completed - Analysis is completed on time.
- Timed Out - Malware Analysis Platform may take longer than 30 mins to complete analysis. Analysis will continue in the background and later status may change to completed.
- Expired - Analysis request is kept for seven days in the queue. If analysis is not completed in seven days message is expired from Malware Analysis Platform.

Source

- All - To view the uploaded files from all sources.
- User Upload - File uploaded by the user.
- Seqrite Lab - Hash obtained from Seqrite lab.
- Rescan - Rescan the submitted sample to obtain the new analysis report.

The following details are displayed for the uploaded file history.

- File Name
- File Hash
- Source
- Size(KB)
- Start Time
- End Time
- Progress
- Status whether In Progress, Timed out, Completed and Expired.
- Report for the uploaded file can be seen by clicking “View”.

Global Search

Users can search using hash (MD5, SHA-1 or SHA-256) of any file. Only a single hash can be searched using this option. If analysis report is not available for a searched hash, however, the corresponding file exists in the Malware Analysis Platform storage, then that file is submitted for scan to all microservices, and the analysis report is displayed.

If the searched hash is not available in the Malware Analysis Platform storage, then the hash is searched in the Virus Total database. If a match is found in Virus Total database, the file is then downloaded in Malware Analysis Platform storage, and the scanning starts automatically. The corresponding analysis result is displayed.

Malware Analysis Platform provides a basic URL search for categories. URLs are grouped under one or multiple categories. Malware Analysis Platform displays a maximum of three categories of the URL based on the content.

Searching the hash or URL

To search and analyze the hash from the database, follow these steps:

1. On the Home page, in the Global Search box on the upper right side, enter the file hash or URL and click **Go**.

   For the submitted file hash, you are redirected to the analysis report page. For the submitted URL, the categories are displayed.

5. Notifications

Notifications generated by Malware Analysis Platform are displayed by clicking the **Notification** tab (bell icon) on the left pane. The notification messages are displayed in tabular format by date. Click **View** to see the individual notification message details.

6. User Setting

You can view your personal details such as First Name, Last Name, and email address. You can change account password, view API usage by quota allowed and quota used. You can also view the list of the open-source tools/library and licenses. Additionally, you can change the User Interface theme to light or dark as required.

You can access the user settings by clicking User Setting tab on the left pane.

Account Settings

My Account

You can view the details such as first name, last name and email address by clicking **My Account**. Log out from Malware Analysis Platform using the **Logout** option.

Change password

You can set a new password and save it for future use.

2. Navigate to the User Setting tab on the left pane.

   You are redirected to Account Settings dialog box.

3. Click **Change Password**.
4. Enter the Old Password, New Password, and Confirm Password.
5. Click **Change Password** button.
   The new password is set for the user.

Usage

View your upload and search usage from API allowed quota limit and used quota.

Open Source Tools

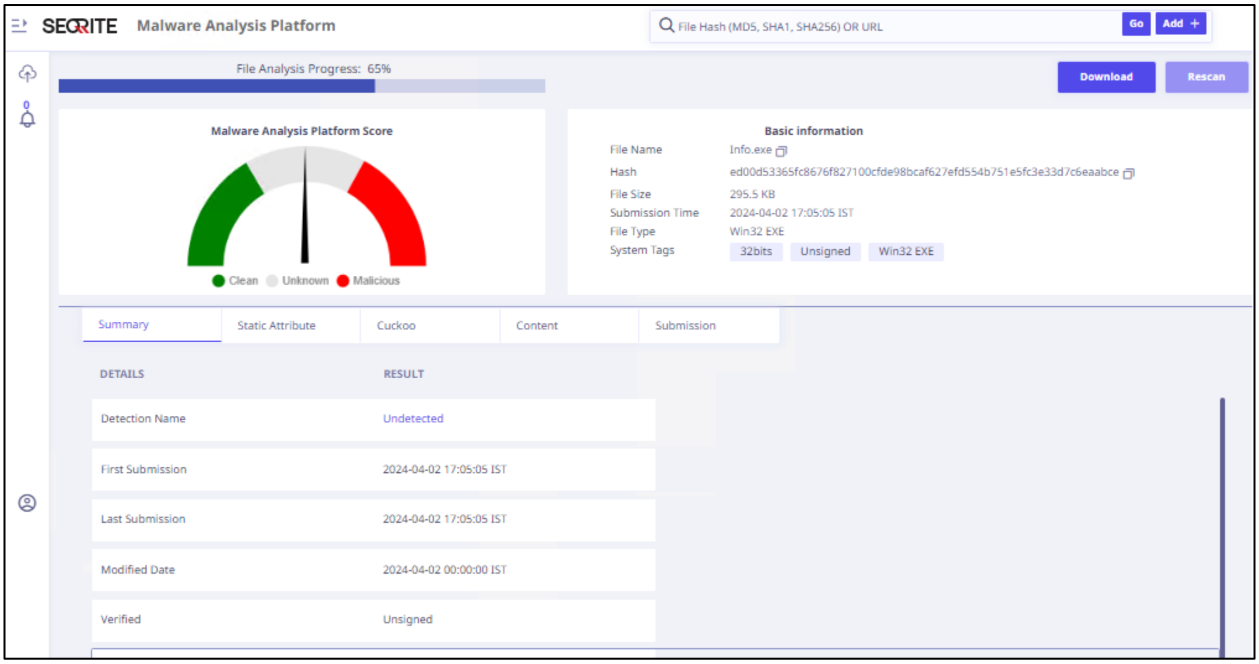
View the list of open-source tools used in Seqrite Malware Analysis Platform.

Product Theme

You can change the user interface theme to dark or light as required by clicking the corresponding moon and sun icons.

7. Analysis Report

After you upload a file for analysis through the Search tab on the left pane, an analysis report is generated for the uploaded file and searched hashes that are already present in the database as shown in the screenshot. Various modules in the report display the corresponding analysis data.


SEQRITE
Malware Analysis Platform
File Hash (MD5, SHA1, SHA256) OR URL
Go
Add +
File Analysis Progress: 65%
Download
Rescan
Malware Analysis Platform Score
● Clean ● Unknown ● Malicious
Summary
Static Attribute
Cuckoo
Content
Submission

Basic information

File Name	Info.exe
Hash	ed00d53365fc8676f827100cfde98bcaf627efd554b751e5fc3e33d7c6eaabce
File Size	295.5 KB
Submission Time	2024-04-02 17:05:05 IST
File Type	Win32 EXE
System Tags	32bits Unsigned Win32 EXE

DETAILS	RESULT
Detection Name	Undetected
First Submission	2024-04-02 17:05:05 IST
Last Submission	2024-04-02 17:05:05 IST
Modified Date	2024-04-02 00:00:00 IST
Verified	Unsigned

The following table provides the file details displayed on the analysis report page.

Item	Description
Progress and Final Verdict	Displays the progress meter with clean, unknown, and malicious status.
File Name	Displays the submitted file name.
Hash	Displays the submitted file hash.
File Size	Displays the uploaded file size.
Submission Time	Displays the time stamp when the file was submitted for analysis.
File Type	Displays the file type.
System Tags	Displays the system tags.
Analysis Progress	Displays a progress bar with the analysis percentage.

File Tags

The following table shows the report with system-generated file tags that are assigned to the samples based on the analysis. Click the displayed file tags to view the similar search results from the database.

Note: Display of the file tags depends on the submitted file and the results may vary.

Tag Name	Description
signed	File is signed (Windows Authenticode Portable Executable Signature/Apple signed/etc.)
Unsigned	File is not signed
invalid-signature	Digital signature not verified
32bits	Sample targets 32bit architectures
64bits	Sample targets 64bit architectures
.NET	.net file
peexe	Executable
upx	UPX packer
themida	Themida packer
c/c++	Microsoft Visual C/C++ Compiler
delphi	Delphi Compiler/Linker
DLL	DLL linker
sys	IMAGE_SUBSYSTEM_NATIVE file
overlay	File contains an overlay, appended data at the end of the file
corrupt	Flags the sample as a corrupted file

Modules

Visibility of some modules, tabs, or information is based on the availability of the data. You can view the following Module tabs.

Summary

The submitted file or hash is scanned and the summary is displayed. The displayed details may vary depending on the submitted file type.

1. Click **Summary**.
   The tabs with the related information such as Quick Heal Detection, File Type, First and Last Submission dates and other details are displayed.

Static Attributes

Malware Analysis Platform processes the data statically using certain tools and generates the analysis for the submitted sample.

Note: The tools are displayed as per the submitted file type.

1. Click **Static Attributes**.

   The following table shows the Tools tabs and the corresponding information displayed on the page. These tools provide various insights about the sample.

Tools	Description
Basic Properties	Displays the static details for the file such as MD5, SHA1, and others
Sections	Displays section information of portable executable file
Trid	Displays file types based on signature database
Exiftool	Displays exif metadata of all file types
Pelib	Displays static attributes of file
Sigcheck	Displays file version number, timestamp information, and digital signature details including certificate chains
Die	Determines types of files and examines file properties

2. Click the corresponding tabs to view the details.

Behaviour

Sections data may vary for samples depending upon the dynamic behavior of the submitted sample file. You can also reanalyze the file on Cuckoo.

Note: Analysis report for the submitted samples is displayed as per the available data only.

1. Click **Behaviour**.

   The following table shows the Sections tabs and the corresponding information displayed on the page.

Sections	Description
QH Score	Malicious score (in range of 0 to 10) given to a sample based on various malicious behaviour it exhibits
Signatures	Various actions performed by the file when it is executed
File System Actions	Details about file opened, read, created, written, deleted and an existence check
Directory Actions	Details about actions performed on the directory such as enumerated, created, deleted, and other details
Modules Loaded	List of modules or libraries loaded during execution
Registry Actions	Details about registry read, write, delete, and update actions
Process and Service Actions	Details about services and processes launched
Other	Miscellaneous behavioral information

2. Click the corresponding tabs to view the details.

Content

This module displays the string and hex raw data for the submitted sample.

1. Click **Content**.
2. Select one of the following to view corresponding data:
    - String

      The strings in the submitted sample are displayed.
    - Hex

      Only the first 1000 bytes of the submitted sample are displayed due to the limitations of the browser.

Submission

This module displays the historical data for the submitted sample from the database.

1. Click **Submission**.

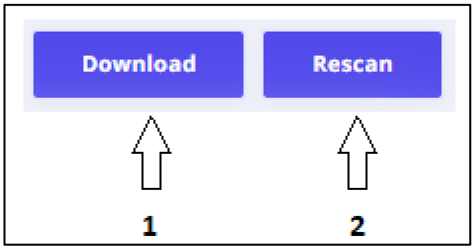
   The following table shows the tabs and the related information displayed on the page.

Type	Information
Graphical Visualization	Displays a graphical view of number of submissions by date.
Submission data	Displays the last rescan, submission count, rescan count, lookup count, first upload and last upload.

2. Click the corresponding tabs to view the details.

Additional options

The upper right corner of the analysis report page displays the download icon that you can utilize to download the report.



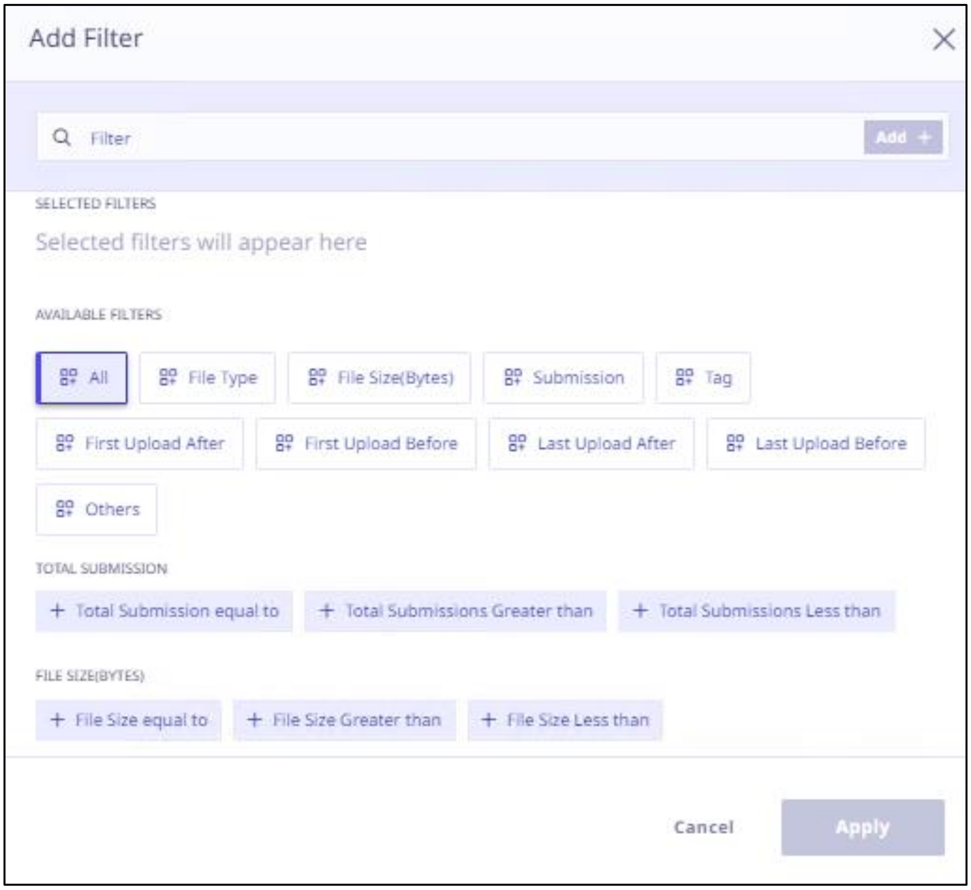
The following table describes the options that are available on the analysis report page.

Sr No	Icon Name	Description
1	**Download**	You can download reports in PDF, and JSON as required.
2	**Rescan**	You can rescan the submitted sample to obtain the new analysis report if the generated report is very old.

Note: Large reports may take time to download.

8. Search Filters

You can apply several filters, to search through the Malware Analysis Platform database. Click **Add+** on the upper right corner.



FILTERS

You can select one or more options to search for the file or hash in the Malware Analysis Platform database.

1. On the Add Filter dialog box, select one or more filters as required, enter the required value in the text box and click **Add+**.

   For example:

   i. If you click File Size, further conditions are displayed as follows:

      File Size equal to, File Size Greater than, File Size Less than.

   ii. Select the required condition and enter the corresponding value in the text box.

   iii. Click **Add+**.

2. The selected filter with value is displayed in the SELECTED FILTERS section.

   For example: File Size equal to: ”10 MB”, File Type: ”Word”.

3. Select further filters with the conditions. The following filters are available:

Features	Description
All	Use the following filters as required: • Total Submission • File Size • Tag • Others • File Type
File Type	Search the file for 32-bit or 64-bit machine type. • File type includes Executable, Excel, Word, Power point, PDF, Image, and Compressed. • Machine type includes Executable, Excel, Word, Power point, PDF, Image, and Compressed.
File Size (Bytes)	• File Size equal to • File Size Greater than • File Size Less than
Submissions	Users can search for the file in the database, by specifying the • Total Submission equal to • Total Submissions Greater than • Total Submissions Less than
Tag	• System Tags: System-generated tags. • User Tags: User generated customized tags.
First Upload After	Capture the data from first upload after date and time.
First Upload Before	Capture the data from first upload before date and time.
Last Upload After	Capture the data from last upload after date and time.
Last Upload Before	Capture the data from last upload before date and time.
Others	• Is Packed: Select this option to search for an archive or zipped file.

4. Click **Apply**.

   The report is displayed with related parameters as follows: File name, Hash, Detections, Size, File upload, total submission and File type. Click **View** to view the analysis report.

9. Support

The **Contact Us** option on Malware Analysis Platform portal enables user to send queries directly to Malware Analysis Platform admins. Malware Analysis Platform admins will revert to you over email with answer to your queries.

Users can send emails through the portal for the following scenarios:

- General feedback : To share general feedback related to the portal
- Report an issue : To report issues related to the functionality of Malware Analysis Platform
- Improvement : To share ideas for enhancements in the existing functionalities
- New Requirement : To share new requirements for Malware Analysis Platform

Head Office Contact Details

Quick Heal Technologies Limited
(Formerly known as Quick Heal Technologies Pvt. Ltd.)
Reg. Office: Marvel Edge, Office No.7010 C & D, 7th Floor,
Viman Nagar, Pune 411014, Maharashtra, India.
Official Website: http://www.seqrite.com.
Email: support.smap@seqrite.com