
rTHREAT
USER MANUAL
v. 2.1.19

Overview

The purpose of this document is to present a step-by-step guide on how to use rThreat.

rThreat is a Next-Generation Attack Emulation Platform, which allows the user to perform tests by using developed and manipulated artifacts to truly test the different cybersecurity systems, processes, and personnel that oversee security.

rThreat enables security operations centers, information security professionals, and incident response teams to perform a pragmatic evaluation of implemented cybersecurity solutions focused on objectively addressing real threats. To achieve this goal, rThreat uses artifacts and samples used by attack groups to test the company's security measures.

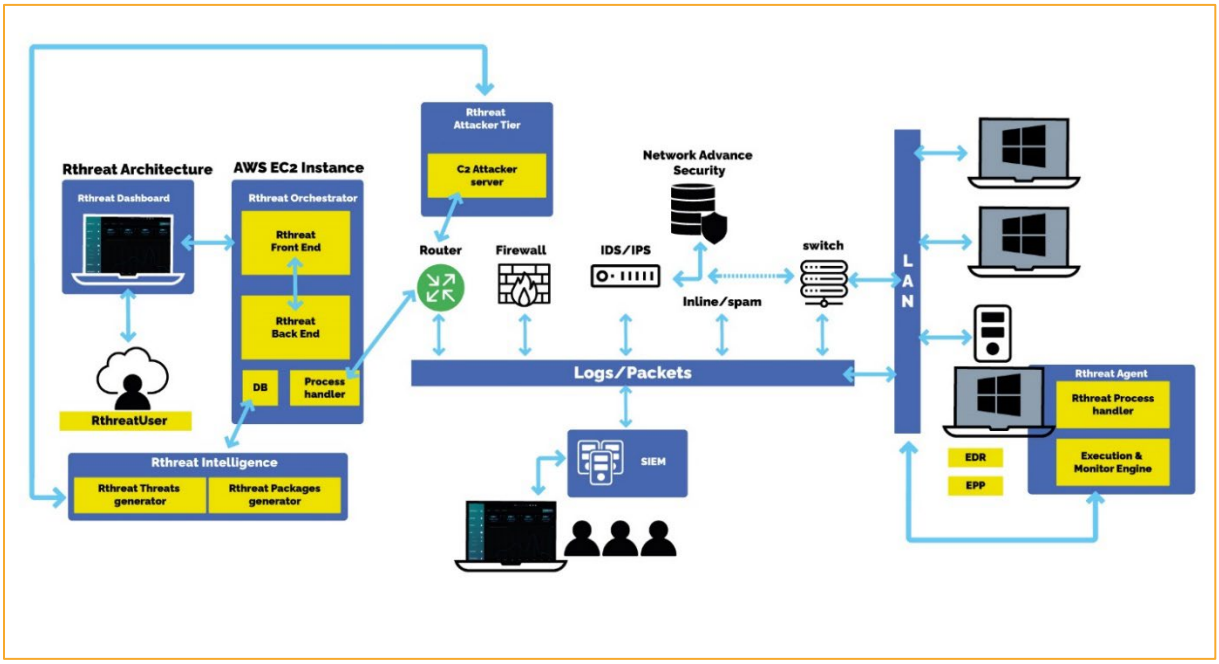
CHAPTER 1: Architecture of rThreat

Deployment Architecture

At the network architecture level, the rThreat Platform is installed on AWS in the cloud and given access to an EndPoint within the organization behind security controls (Golden image).

rThreat emulates real scenarios and cyber-attacks targeting an organization from the cloud console/instance.

This is the flow that artifacts follow once sent in a corporate environment:



The rThreat artifacts contained in emulation packages are sent over the network and executed on the virtual machine (Endpoint) with the client's golden image. The rThreat Software applies control mechanisms and sends the response to the Orchestrator with the obtained results.

EndPoint

In the rThreat environment the Endpoint is the virtual machine (preferably) with the golden image of the system the user want to test. This image must be behind all the cybersecurity controls that the company or organization will test; any type of virtualization is supported if the tests are run directly on the operating system.

For the Endpoint to be used in rThreat Emulations the user must consider these points:

- Virtual Machine with golden image.
- rThreat software Installed.
- Added exceptions in security solutions.
- Allowed IP addresses configured.
- Snapshot of Virtual Machine.

Considering these points, the Endpoint can be considered ready for evaluations.

The preferred form of the Endpoint is using a Virtual Machine, but it is possible to install the rThreat software on physical machines. Whereas it is more difficult to restore physical machines in case they are compromised. Therefore, the preferred form of installation is on virtual machines. This means, rThreat is not targeting or interacting with the production servers of the organization.

Platform

In the rThreat environment, the Platform is the solution deployed in the cloud, which is accessible from the Internet.

By default, the HTTPS protocol is used to allow secure communication using the Platform URL.

It is possible to access the Platform via the IP address associated with the URL, however, the certificate is only valid for the Platform URL. Accessing via the URL is the preferred method.

The information presented on the Platform may differ depending on the privileges associated with the logged-in account. See Types of Accounts.

CHAPTER 2: rThreat Endpoint

Hardware Requirements

A virtual machine with the golden image of the system is required, it must be behind all the cybersecurity controls that the company or organization requires to evaluate; any type of virtualization is supported if the tests are run directly on the operating system.

The virtual machine with a functional operating system must have the following characteristics:

MINIMUM:

- Requires a processor and a 32-bit operating system.
- Processor: Intel Pentium or equivalent.
- Memory: 4 GB RAM.
- Storage: 500 MB of available space.

RECOMMENDED:

- Requires a 64-bit processor and operating system.
- Processor: Intel Core or equivalent/superior.
- Memory: 8 GB RAM.
- Storage: 1 GB of available space.

Operating System Requirements

Supported Versions for a Windows Endpoint

The rThreat Software is available to run on physical endpoints or virtual machines, with all the following versions of Windows:

- Windows 7
- Windows 8
- Windows 10
- Windows 11
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Supported Versions for a Linux Endpoint

The rThreat Software is available to run in environments with all the following Linux distributions:

- GNU/Linux Ubuntu 18.4 and higher.
- RedHat 8.4 and higher

Requirements for the Custom Threat Module

rThreat works by performing attack emulation on physical endpoints or virtual machines (preferred) installed

The Custom Threats Module allows the execution of scripts. To successfully run emulations with this module the user need to meet these requirements:

1. Interpreter installed.

   Depending on the language the user will use on the endpoint the interpreter should already be installed.(If the user will use python scripts on the endpoints, python should be already installed)

2. Libraries installed.

   All the modules/imports that the script will use should also be already installed on the endpoint before sending the emulation (e.g., if the script needs `import socket`, the user need to install socket)

3. Global Path Variables Configured

   The scripts run as if the user execute the directly on the endpoint, if the user can run from cmd `python script.py` , the script the user send will also work as the Global Path Variables are configured, if not, the user will need to configure them.

Additionally, there are some qualities that the scripts being used should follow to run successfully using rThreat such as (but not limited):

- Scripts should terminate all the operations and exit the interpreter, this means no “infinite” scripts are permitted. If presented, after a time out the script will be terminated, and no information will be presented on the logs.
- Scripts should not rely on other script, files, or resources. Unless they are downloaded first in the same script and properly referenced, otherwise the script will fail.
- Use exceptions to catch errors, the logs will include the data displayed by the script, if an error is presented by the system, it will not be logged.
- If the script performs a request or any other communication to URLs, the user may need to allow the IP addresses related to the URL as well as the IP address of a DNS server to allow the communication, however rThreat recommends doing all the references to IP addresses. See View Details and Make Changes to ISOLATION.

rThreat Software Feature Support Exceptions

The following list shows the feature exceptions of the rThreat software.

1. The Isolation process is supported for Windows operating system only.
2. Real-time notifications by rThreat Software are supported for Windows operating system only.
3. Obtaining the Isolation Log Remotely is supported for Windows operating system only.
4. IoC Validation is supported for Windows operating system only.

Requirements for the rThreat Software Installation

Before installing the rThreat software on the designated Endpoint it is necessary to consider the following:

- Endpoint (physical or VM) with Golden Image.
- Exclusion of rThreat files in third-party Endpoint solutions.
- Third-party communications configuration in the rThreat Platform.
- Privileges to perform installation of rThreat software in virtual machine.
- Communication from the Endpoint to the Platform
- Frameworks

Ensuring that these points are met before downloading and installing the rThreat software allows the installation to proceed successfully.

Endpoint (Physical or VM)

rThreat works by performing attack emulation on physical endpoints or virtual machines (preferred) installed on the customer's network. The rThreat software

(Insider) is installed on this target endpoint and this enables communication with the Attack Emulation Platform. On the designated VM, the representative image of the target endpoint environment (Golden Image) the user wish to test will be loaded, i.e., a standard Workstation or server installation and configuration, with standard endpoint security controls installed and configured. In this image the user will need to install the security solutions that the user have deployed in the corporate environment such as EPP, EDR, or any other endpoint protection solution., if they are not already part of a "golden image" that is normally used for endpoint configuration.

Endpoints should be provided being as similar as possible to a computer that could be susceptible to attack for a threat actor.

Finally, the user will need a snapshot of each virtual machine (if applicable), which saves the state of a virtual machine and allows the user to retrieve it at any time. This is necessary as it will be used as a backup, to revert and reuse images after emulation attacks.

Exclusions

For the correct functioning of the rThreat software in many cases it is necessary to add exceptions in third-party solutions, which flag rThreat processes or files as suspicious.

It is also necessary to exclude the "Downloads" folder in the rThreat installation directory for a correct evaluation of the Network vector. The files, folders, and processes to be excluded are shown below. How they are excluded varies depending on the third-party solution.

- **Processes**

  C:\ProgramFiles(x86)\rThreat\rThreatAgent\rThreatContain\rThreatContain\x64\rThreatContain.exe
  C:\Program Files (x86)\rThreat\rThreatAgent\App\rThreat.Agent.exe

- **Folder**

  C:\Program Files (x86)\rThreat\rThreatAgent\Downloads*

Third-party party communications

Before installing the rThreat software it is recommended to add the IP addresses of the third-party solutions that the user want to allow communication.

The rThreat software isolates or contains the virtual machine, blocking all communications and only allowing those that are explicitly configured in the rthreat Platform and the associated configuration file.

To configure IP addresses of third-party solutions, see View Details and Make Changes to ISOLATION.

Privileges

To install the rThreat software it is necessary to have Administrator Privileges depending on the operating system. This ensures that the software takes control of critical processes such as isolation.

Communication between Endpoint and Platform

Communication between the Endpoint and the Platform is achieved as follows:

Real-time communication through a WebSocket and the Socket.IO v4 library. By this means, all requests sent by a request from the Front End are received and answered. Communication by RESTFUL API: By this means the information required by the rThreat Software for its operation is transmitted. The URL and ports of both the Socket.IO and the Restful API are specified in the Auth.json file. It is essential to make sure that this communication is not blocked. The following ports should be open for rThreat platform - endpoint communications:

Port 8080 - Communication via http protocol with restful services of rThreat platform

Port 8888 - Communication via http protocol and WebSocket between agent and rThreat platform

Port 4003 - Communication via https protocol with restful services of rThreat platform

Port 8899 - Communication via https protocol and WebSocket between agent and rThreat platform

If the software is unable to connect to the rThreat platform after install and configuration, these ports should be checked.

Frameworks

rThreat uses certain frameworks for its correct installation and operation, and it is necessary that they are installed (if they are not already installed) before installing the Insider.

- rThreat requires .NET Desktop Runtime 6.0.0 or later (Windows 7.0 and above), x86 version mandatory. If it is not installed on the device, the user will be redirected to the compatible .NET installation package. For linux systems is also required.

  https://dotnet.microsoft.com/es-es/download/dotnet/thank-you/runtime-desktop-6.0.19-windows-x86-installer

- The isolation process uses Visual C++ Redistributable Packages. It is mandatory to install it.

  https://www.microsoft.com/en-US/download/details.aspx?id=48145

- Some Windows systems also require version 4.7.2 of NET Framework (Windows 7.0 or later). If it is not installed on the device, the user will be redirected to the compatible .NET installation package.

  https://dotnet.microsoft.com/en-us/download/dotnet-framework/thank-you/net472-offline-installer

Obtaining The rThreat Software (Insider)

Once the user have the Endpoint that will be used to make the Emulations considering the details in section Requirements for the rThreat Software Installation the user can download of the rThreat software.

To download the rThreat software follow the instructions below:

1. Enter the credentials provided to the Platform.
2. Go to the Endpoints tab.
3. Click on the Download Agent Insider.

4. Click on the button of the operating system that requires the rThreat Software.
5. For Windows environments, an .msi file will be downloaded. For Linux a .tar file will be downloaded.
6. Click on the file icon above to the operating system to download the json file.
7. The json file will be downloaded on the local host.

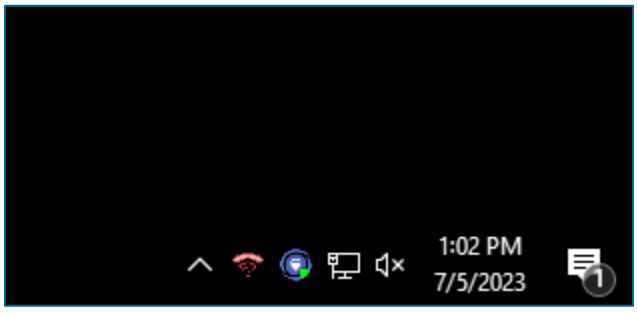
For more information see Download the rThreat Software (Insider) of the section Endpoints.

rThreat Software: Insider

The rThreat software (Insider) will help the Endpoint communicate with the Orchestrator so that it can receive distinct types of threats from different levels, help execute them on the Endpoint and generate the results of each of those threats which it sends to the Platform. The rThreat software is responsible for the isolation process.

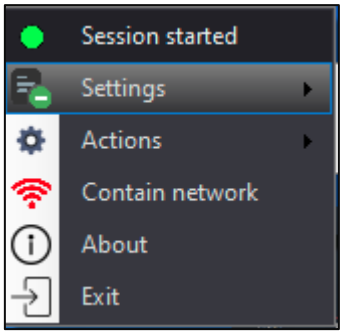
Controls

Usually after installation of the rThreat software the user will find the icons in the taskbar.



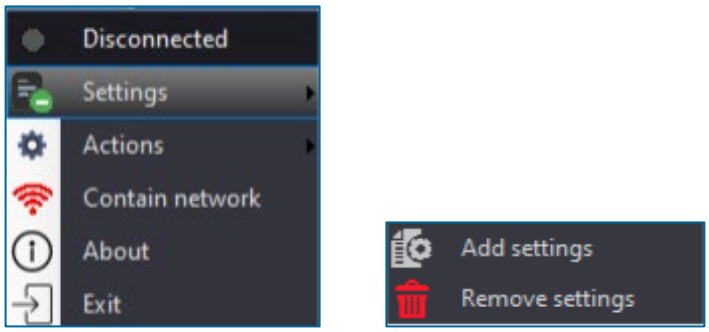
Right-clicking on the blue rThreat icon displays a window with the available manipulation options. The menu shows the control options of the software.

1. Session status indicator, it can have different status.



- **SessionStarted**: The configuration in the Auth.json file was successfully loaded allowing the connection to the Platform Orchestrator.
- **No settings**: When the Auth.json configuration file has not been loaded.
- **Invalid settings**: The Auth.json file contains incorrect data, is not up to date or is from an older version of the rThreat Software.
- **Connecting**: The rThreat software is trying to perform the communication to the platform.
- **Connected**: The rThreat software has a stable communication to the Platform.
- **Disconnected**: The rThreat software is stopped.
- **Session Rejected**: An element in the network is blocking the communication. Also, number of EndPoints exceeds the number specified in the license.

2. Settings: This is the section where the rThreat software configuration file is loaded. Two options are presented:
   - **Add Setting**: Option to load the Auth.json configuration file downloaded from the Platform.
   - **Remove Settings**: Option to delete the loaded configuration file. This option will interrupt the connection between the EndPoint and the Platform. Likewise, the isolation process is interrupted.



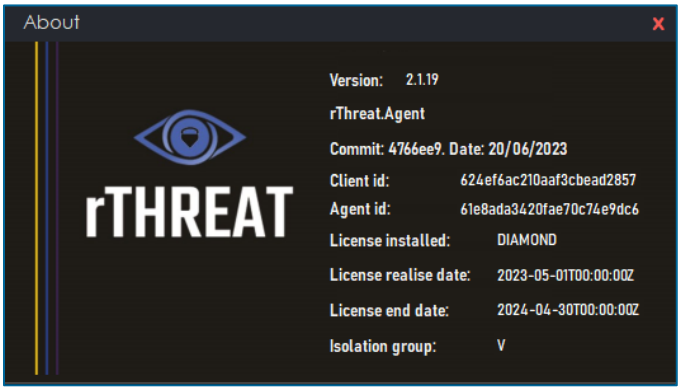
3. Actions: This section allows general manipulation of the rThreat software, and includes the following options:

- **Start**: Allows to start the rThreat software processes which will enable communication to the Platform and initiate the isolation process.
- **Stop**: Stops the rThreat software processes which will disable communication to the Platform and stop the isolation process.
- **Restart**: Restart the rThreat software processes which will temporarily disable communication to the Platform and the isolation process. They will be enabled after a short period of time.

4. Contain Network: Indicates with color in the icon whether the isolation process is enabled or disabled.
   - Network Connected: Isolation disabled.
   - Network Isolated: Isolation enabled.

     This icon is also displayed as a second main icon of rThreat. This indicates that the two processes are independent.

     The description is also displayed if hover over this option.
5. About: Selecting this option opens a new window displaying information about the rThreat Software.



- **Version:** The version of the rThreat software installed.
- **rThreat.Agent:** Name of the installed software.
- **Commit:** It refers to a unique identifier for version control, with this id the user can track within the internal repository the features of the current version.
- **Date:** Indicates the release date of the rThreat Software version.
- **Client id:** Unique identifier for each rThreat Software installed, for each machine where the rThreat Software is installed a unique Client Id is generated.

- **Agent id:** Identifier to track the version of the Auth.json file that is being used by the rThreat software.
- **License Installed:** Type of license found in the subscription.
- **License release date:** Date on which the subscription was initiated.
- **License end date:** Date on which the subscription ends.
- **Isolation Group:** IP Isolation group applied to the endpoint.

6. Exit: Terminates all rThreat software processes including the rThreatAgentService service, which permanently shuts down the rThreat software.

If the user wish to restart the rThreat software from the endpoint without using the option above, follow these steps:

For Windows Systems:

1. Go to Windows Services
2. Locate the rThreatAgentService service.
3. Right click and select the Start option.
4. The rThreat software will start normally.

For Linux Systems:

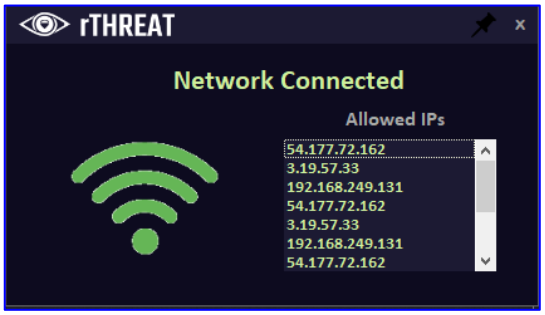
1. Open a command prompt.
2. Type `pm2 restart rThreat`.
3. The rThreat process will restart. Type `pm2 list` to verify that the rthreat process is initiated.

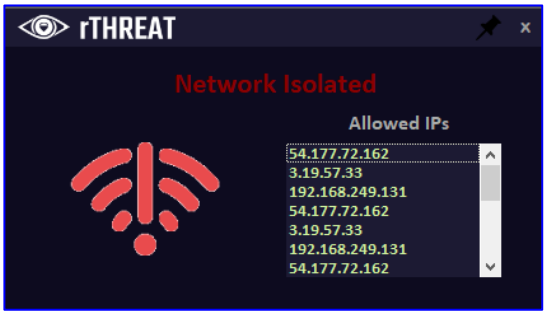
The rThreat software starts automatically at system startup, so when the user restart the EndPoint, the rThreat software will do it as well.

Notifications

Notifications are only available for Windows EndPoints.

- When starting, stopping, or restarting the rThreat software, the following notifications are displayed.

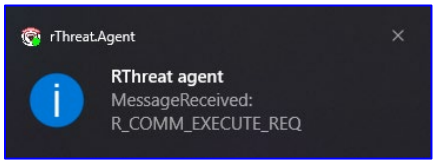




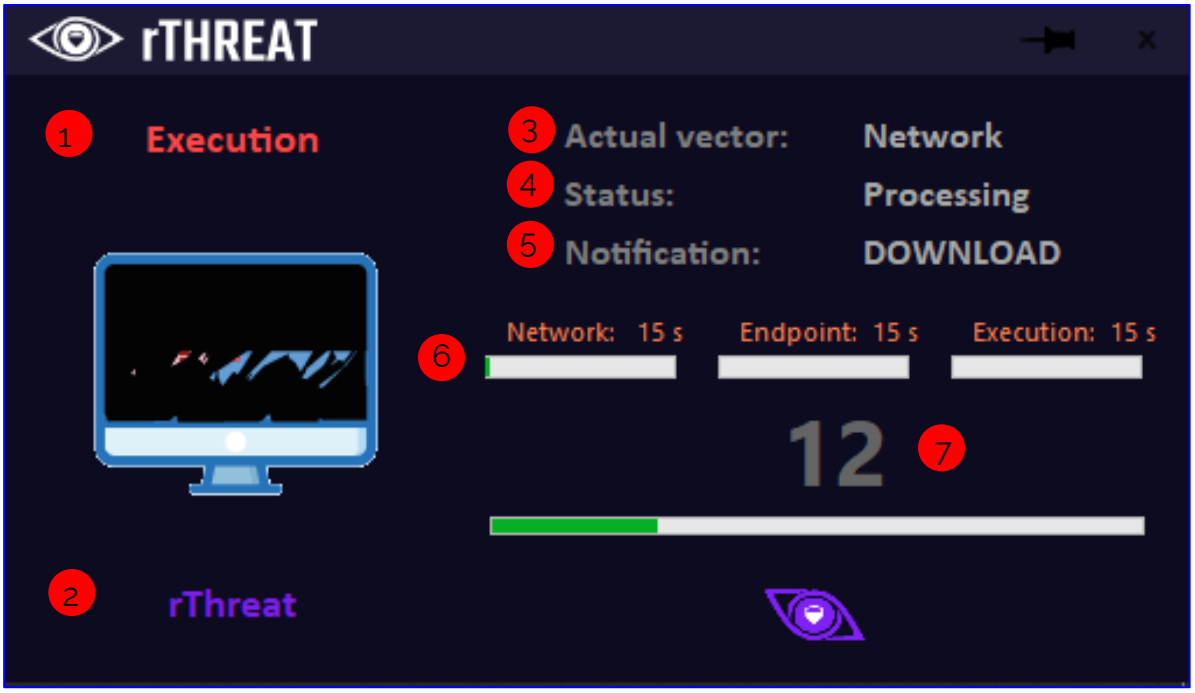
Network Connected: Emphasizing with green color both text and icon, it is expressed that the isolation process is disabled. The list of Allowed IPs shows the IP addresses configured on the Platform.

Network Isolated: Emphasizing with red color in text and orange icon, it is expressed that the isolation process is enabled. The list of Allowed IPs shows the IP addresses configured on the Platform.

- Sending an Emulation: When an Emulation is performed a Windows system notification will be displayed warning that a new Emulation task has been received.



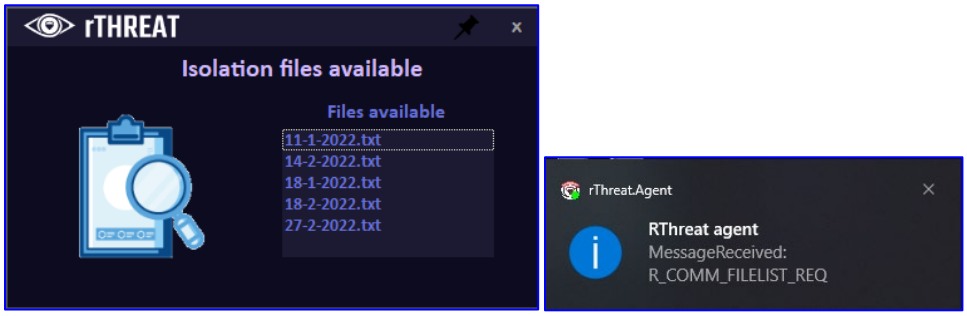
- Sending an emulation: rThreat Software. When an emulation is performed, a window with details about the emulation will be displayed.



1. Displays the type of emulation being performed.
   - Network: Emulation performed only to evaluate the network vector.
   - Endpoint: Emulation performed to evaluate the network vector and EndPoint.
   - Execution Emulation conducted to evaluate all three vectors. See Emulation Vectors.
2. Name of the emulation configured in the Platform.
3. Actual vector: indicates in which stage of evaluation is the emulation, depending on the vectors.
4. Status: Actions being carried out now.
5. Notification: Refers to the Emulation States.
6. Status per vector. Indicates the set evaluation time for each vector. The status bar fills up depending on the configured time.
7. Second status indicator. First it shows the countdown time for each vector involved in the emulation. At the end it will display a message:
   - Mission Complete: The emulation was successful, i.e., all the artifacts in the package were executed.

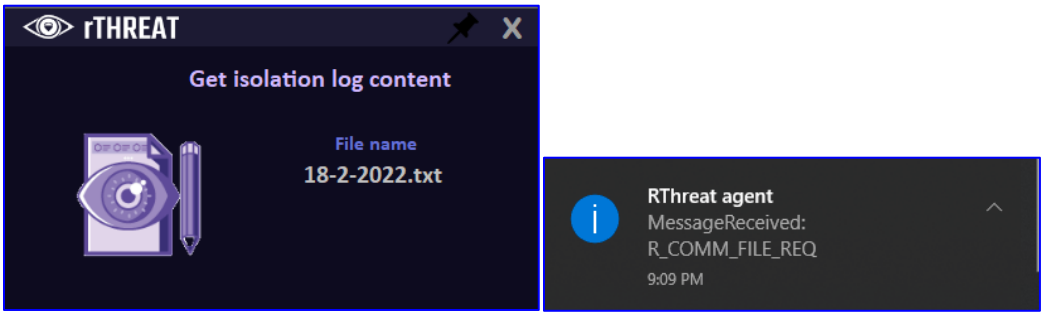
- Errors. It will show details on why the emulation was not successful.

- When an Isolation Logs request is made, the following messages are displayed on the Endpoint.



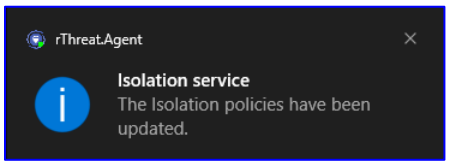
1. Window showing the list of available Isolation Logs.
2. System Notification.

- When downloading one of the files from the Isolation Logs list, the following messages are displayed on the Endpoint.

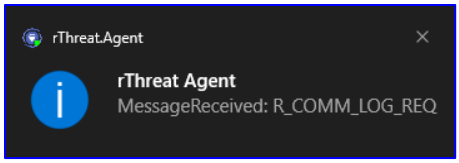


1. Window showing information of the downloaded Isolation Log.
2. System Notification.

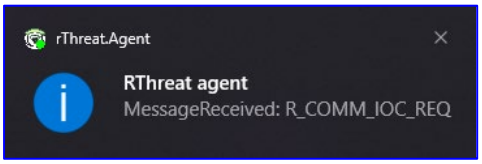
- When making changes to the Isolation Group Policy



- When obtaining the Insider Logs.

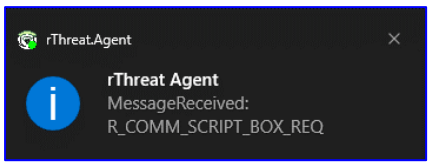


- When performing IoC Validation the following messages are displayed on the endpoint:



1. Window displaying IoC Validation information.
2. System Notification.

- Performing Script Emulations, the following messages are displayed on the endpoint:



Isolation Process

The rThreat software has a module written at the kernel level that prevents network communications of any kind to any unapproved element, i.e., it allows communications to the rThreat Platform itself, as well as to third parties necessary for risk management and blocks everything else at a low level.

In the Platform it is possible to allow IP addresses for third party solutions such as EDR, SIEM, collectors, or any other security product., to which communication is allowed and all other traffic is blocked, so that when an advanced threat is triggered, any lateral movement is completely blocked. To configure these IP addresses, see section View Details and Make Changes to ISOLATION.

The Isolation process is available only for IPv4. If the endpoint uses IPv6 it will be required to be **disabled on the endpoint**.

The isolation process is independent of the Main rThreat process, this ensures that even if security products or malware terminate rThreat, the endpoint maintain the isolation state.

Installing the rThreat Software

Before installing the rThreat Software, make sure to have completed the steps described in the following sections Requirements for the rThreat Software Installation and Frameworks.

The following steps are required to install the rThreat Software.

rThreat Software Installation on Windows EndPoints

The files required for installation on Windows Endpoints are:

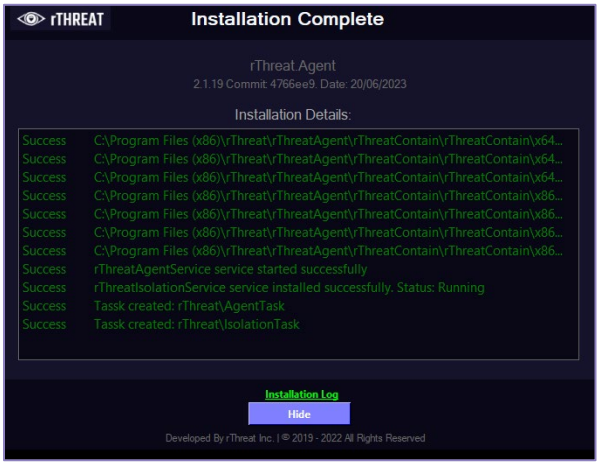
- Installation program insider_2.1.19.msi.
- Configuration file Auth.json.

After the download of the installation files as described in section Download the rThreat Software, Transfer them to the endpoint and follow the steps below for installation:

1. Double-click the installer insider_2.1.19.msi. It is important to note that the rThreat Software installer requires .NET Desktop Runtime 6.0.0 or later (Windows 7.0 and above) version **x86**, if it is not installed on the endpoint, the user should be redirected to the compatible .NET installation package.
2. Once the framework is installed on the system, it is necessary to run the installation insider_2.1.19.msi file again, which will display the installation wizard again.

Some Windows systems also require NET Framework version 4.7.2 (Windows 7.0 or later), if it is not installed on the endpoint, the user should be redirected to the compatible .NET installation package

3. Accept the settings presented by the wizard, as well as the license agreement and continue through the wizard.
4. When the installation is complete, the installation log will be displayed. If there are no errors, close the window.



5. The installation log will show if there were any errors during the process.
6. The installation of the rThreat software is now complete. Next, load the json configuration file to the rThreat Software.

   Look in the taskbar for hidden icons and right-click on the blue rThreat Software icon. Click Settings> Add settings.

   The user will be prompted to find the Auth.json configuration file on the system. Select it and proceed to load the file.

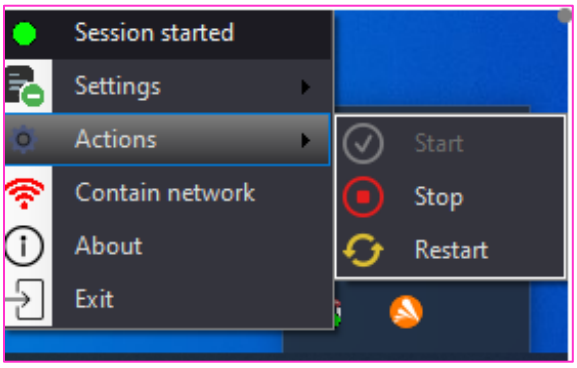
After installation indicates isolation disabled and when it is correctly connected to the Platform it will show isolation enabled, this means that the communications of that virtual machine have been disabled and the rThreat Software is correctly installed.

Once the software is installed, it is recommended to take the snapshot of the virtual machine.

Validating the Installation of rThreat Software on Windows

To validate that the rThreat Software is correctly installed and connected to the Platform, the following can be performed:

1. Right click on the rThreat Software icon, select Actions, and verify that the start action is grayed out, if so the rThreat Software is started.



2. Login to the Platform to validate that the rThreat Software is online.

   On the Endpoints tab the user can see the status of the devices. The green status identifies the "Connected" Endpoints.

   For more information see Endpoints.

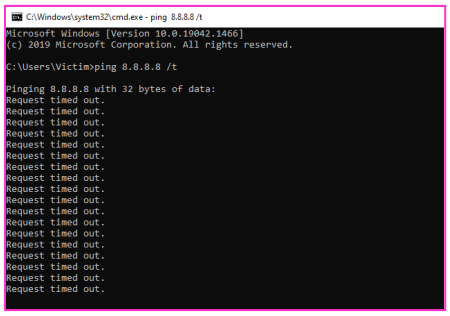
   The user can also check the status of the Endpoints in the Hosts button in the top bar of the Platform. See Dashboard.

3. Validate the containment of the Endpoint.

   Use the command prompt to ping the endpoint to one of the IP addresses configured in the "allowipagent" parameter. The ping should be successful,

confirming that the endpoint can communicate with the designated security, if it times out, that IP address is not allowed.

In the same way the user can open a web page and if it is blocked or cannot be opened. See section View Details and Make Changes to ISOLATION.



With these tests the user can validate and confirm that the rThreat software has been installed correctly and that the user have communication to the Web Platform.

rThreat Software Installation on Linux Endpoints

The files required for installation on linux Endpoints found in the double compressed Insider GNULinux.zip archive are:

- Archive README LINUX.
- Archive redhatInstall.sh.
- Archive removeService.sh.
- Archive ubuntuInstall.sh.
- Folders publish.

After the download of the installation files as described in section Download the rThreat Software, transfer them to the endpoint and follow the steps below for installation:

After transferring the installation package to the Endpoint, unzip the file Insider GNULinux.zip, the .tar.xz file.

1. Authentication file:

Download the Auth.json file from the rThreat platform, copy and paste the file into the publish/AppSettings folder.

2. Grant execution permissions to the installation script:

   Choose the installation script according to the Linux distribution:

   - RedHat, use the installation script: redhatInstall.sh.
   - Ubuntu 18.04 LTS, use the installation script: ubuntuInstall.sh.
   - Ubuntu 20.04 LTS, use the installation script: ubuntuInstall.sh.
   - Ubuntu 22.04 LTS, use the installation script: ubuntu22_04Install.sh.

3. Open the command terminal and navigate to the directory where the installation shell files are located (redhatInstall.sh, ubuntuInstall.sh, ubuntu22_04Install.sh).

   Based on the Linux distribution, enter the following command:

   - RedHat, execute the command: sudo chmod 775 redhatInstall.sh
   - Ubuntu 18.04 LTS, execute the command: sudo chmod 775 ubuntuInstall.sh
   - Ubuntu 20.04 LTS, execute the command: sudo chmod 775 ubuntuInstall.sh
   - Ubuntu 22.04 LTS, execute the command: sudo chmod 775 ubuntu22_04Install.sh

4. Run the installation shell script according to the Linux distribution:

   - RedHat, execute: ./redhatInstall.sh
   - Ubuntu 18.04 LTS, execute: ./ubuntuInstall.sh
   - Ubuntu 20.04 LTS, execute: ./ubuntuInstall.sh
   - Ubuntu 22.04 LTS, execute: ./ubuntu22_04Install.sh

   The installation script adds the rThreat application to the PM2 process manager.

5. To finish configuring PM2, copy, paste, and run the command that will be automatically generated by PM2.

   Example:

sudo env PATH=$PATH:/usr/bin /usr/local/lib/node_modules/pm2/bin/pm2 startup systemd -u myuser --hp /home/myuser

To make PM2 run and manage the rThreat application, run the command:

$ source ~/.bashrc \pm2 save

To make PM2 stop managing the rThreat application, run the script: removeService.sh

Commands to manage the application state using PM2:

Restart: $ `pm2 restart rThreat`
Stop: $ `pm2 stop rThreat`
Delete: $ `pm2 delete rThreat`

Validating the Installation of rThreat Software on Linux

To validate that the rThreat Software is correctly installed and connected to the Platform the following can be done:

1. Login to the Platform to validate that the rThreat Software is online.
2. In the Endpoints tab the user can see the status of the devices. The green status identifies the "Connected" Endpoints.
3. Use the $ `pm2 list` command to ensure that the rThreat service is running. It should have an “Active” State.

Backup of the Virtual Machine with Golden Image

After the user have successfully installed the rThreat software, it is strongly recommended that the user take a snapshot of the virtual machine. It is important to have a snapshot of the system to avoid having to reconfigure the system after an emulation attack that may execute a malicious program artifact on the Endpoint.

It will require rolling back the VM to the snapshot to restore the "clean" VM for repeated testing.

Upgrading rThreat Software

rThreat recommends always having the latest version of the software installed.

To update the rThreat software, follow the instructions below.

1. Uninstall the current version of the rThreat software on the Endpoint as described in section Uninstalling the rThreat Software.
2. Next, install the most recent version of the rThreat software as described in section Installing the rThreat Software.

Uninstalling the rThreat Software

Uninstall for Windows Operating System Endpoints

To uninstall the rThreat software in Windows environments follow the steps below:

1. Stop the rThreat Software. Right-click on the rThreat software icon and select the Exit option.
2. Open control panel and select "Uninstall a program" in the "Programs" section.
3. Locate the rThreat software: rThreatAgent.
4. Right click and select the option "Uninstall".
5. Select the options presented by Windows Programs and Features and UAC for uninstallation.
6. The rThreat Software will be uninstalled.

The user can also use the rThreat installer to uninstall it. Run the installer and will be presented with the repair or uninstall the insider. Select uninstall and follow the instructions.

Uninstall for Linux Operating System Endpoints

To uninstall the rThreat software in Linux environments follow the steps below:

1. Open the path in terminal where the shell is hosted (removeService.sh).

2. Start shell emulation (sudo ./removeService.sh)
3. The rThreat software will be uninstalled from the Linux Endpoint.

Troubleshooting

For Support cases, the rThreat team would ask to send the logs that are generated on the Endpoint.

Obtaining Logs of the Insider from the cloud instance

The user can obtain the rThreat software logs from the cloud instance of an online endpoint, follow these steps:

1. Go to the Endpoints Diagram Tab.
2. Click on the Downloads Logs button of the endpoint the user wants to obtain the logs.
3. Select the logs date the user want to download. If the date is valid the download will start. Otherwise, a warning will appear.

Obtaining Logs locally of the rThreat Software on Windows Systems

To obtain the logs from the rThreat software, follow the steps below:

1. On the Endpoint go to the following folder:

   C:\Program Files (x86)\rThreat\rThreatAgent\Logs For 64-bit environments
2. From the files that appear in that folder, select the files the user want to get.
3. Copy the files to the local host.

Obtaining Logs locally of the rThreat Software on Linux Systems

To obtain the logs from the rThreat software, follow the steps below:

1. On the Endpoint go to the unzipped installation folder
2. Inside the folder go to publish > Logs
3. From the files that appear in that folder, select the files the user want to get.
4. Copy the files to the local host.

Obtaining Logs of the Isolation Process

Feature allowed only for Windows environments.

To obtain the Local Isolation Process logs, follow the steps below:

1. On the Endpoint go to the following folder:

   C:\Program Files (x86)\rThreat\rThreatAgent\rThreatContain\txt For 64-bit environments

2. From the files that appear in that folder, select the files the user want to get.

The user can also obtain these logs remotely, see section View and Download Isolation Log.

CHAPTER 3: rThreat Platform

rThreat has a web interface (Platform) to be operated and configured. The Platform displays the results of the emulation and allows the control of future tests to be executed at the endpoint. It also displays graphs demonstrating the effectiveness of the implemented solutions.

It presents the results of the Emulations and provides visibility on the results obtained, has granularity for on-demand emulation.

Each package has actual samples of advanced threats. An Emulation consists of packages and an EndPoint can have N number of Emulations.

Each available package represents behaviors of different cyber actors. This allows effective testing covering the different stages and phases of the attack.

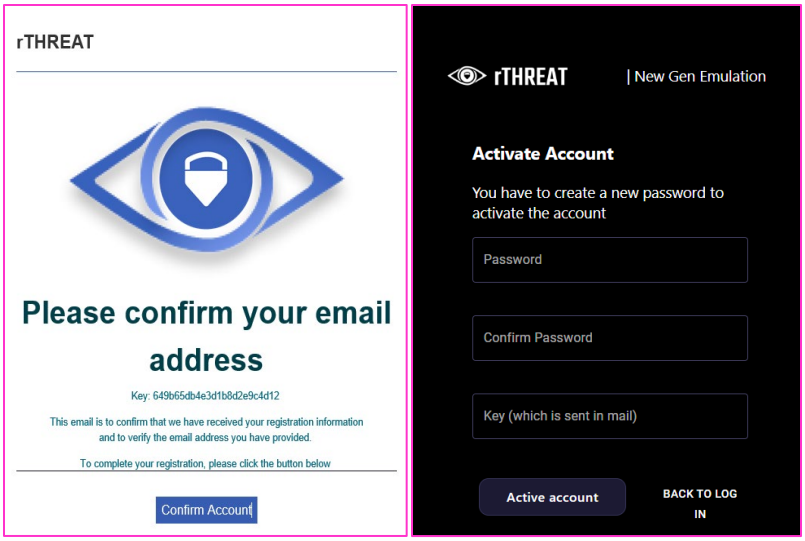
Logging in to the Platform for the first time

With the subscription to rThreat, the user will receive an email with the access to the instance. Logging into the rThreat web interface may vary depending on the browser the user use.

When logging in, the user can have an "Administrator" user account or a "User" account. See Types of Accounts.

To log in to the Platform for the first time follow the steps below:

1. Check the email for the Welcome to rThreat email.
2. Copy the **Key** Provided.



3. Click on the Confirm Account button to access the platform.
4. Create a password and enter the key provided on the email.
5. Click on Active account to activate the account.
6. Click on BACK TO LOG IN to access the main Login Page of the platform.
7. Enter the credentials and click on the Sign In button.

   If a user try to log in too many times with an incorrect username or password, the account will be locked. Contact the administrator to unlock the account.

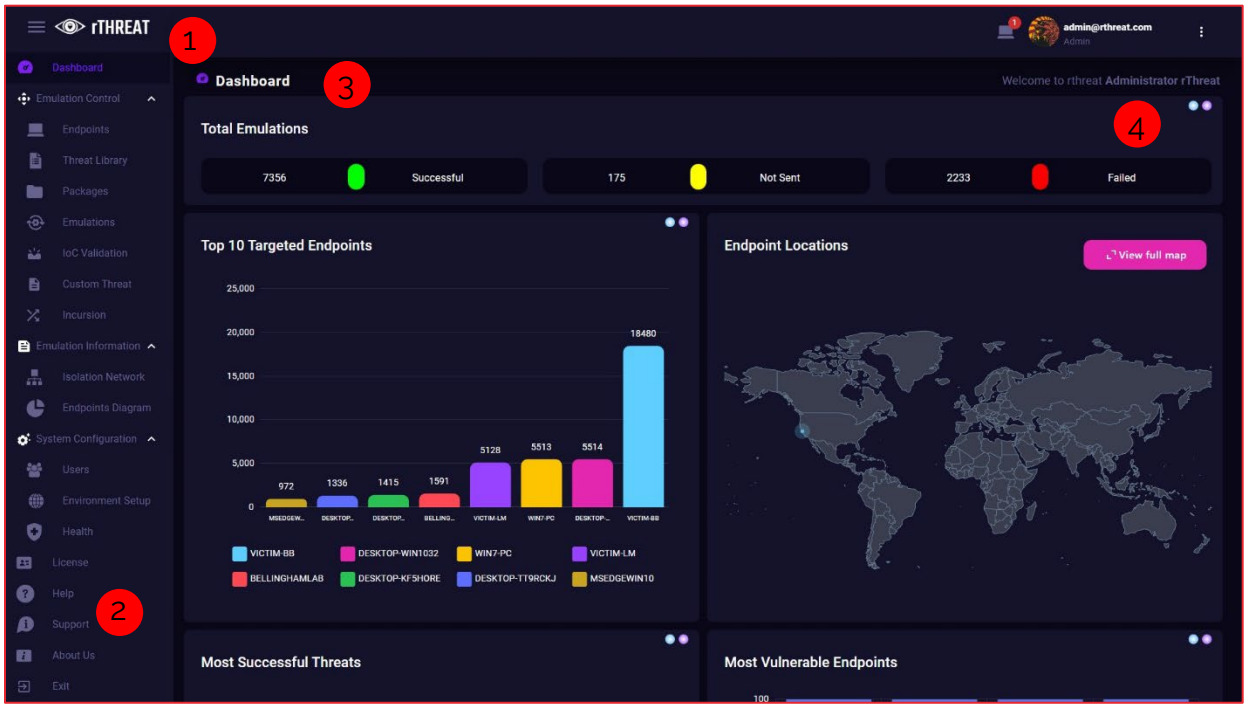
   If the credentials are correct, the user will have access to the Platform with the Dashboard tab being the initial page displayed.

Navigation Tabs

For easy navigation through the Platform there are seventeen tabs in the menu divided into four sections: Dashboard, Emulation Control, Emulation Information and System Configuration. Five tabs are not classified.

The content displayed on each of the pages may vary depending on the role assigned to the user.

Dashboard

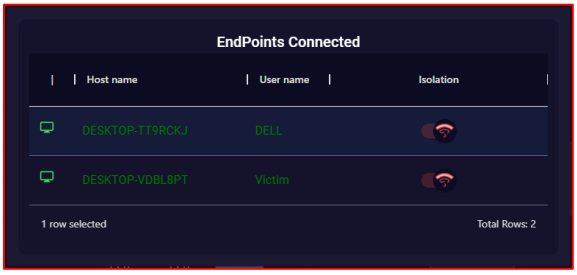


The Dashboard and home page consists of four main sections.

1. Top Bar: Tab panel control, online EndPoints indicator, account information and general options.

   - The icon ☰ allows the user to modify the tab view in the Dashboard. Selecting it will change it to an arrow →, hiding the titles of the Dashboard tabs.

   - The indicator 💻 shows the number of EndPoints that are online. Selecting it will open the "EndPoints Connected" window with details of the Endpoints, as well as a quick check of the Isolation.



   - Next to the EndPoints quick indicator is the profile picture, email, and role of the logged in user. See Types of Accounts.

- The button ⋮ in the upper left corner reveals two quick actions of the Platform: Edit profile, change the current user's password, and exit the Platform.

2. Navigation Tabs

   The general administration tabs of the Platform are displayed as a list.

3. Tab Title

   The current tab and the name of the logged in user are displayed.

4. Widgets

   Widgets are graphical resources that generally and quickly summarize information about the Emulations that have been carried out and information, artifacts and information related to the Platform.

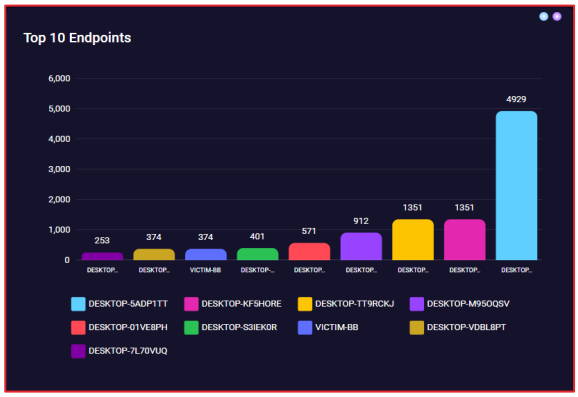
   All widgets, except for Endpoints Locations, can be resized to fit the width of the window. In the upper right corner, there are two buttons:

   The blue button corresponds to the standard size.

   The purple button corresponds to the maximized size.

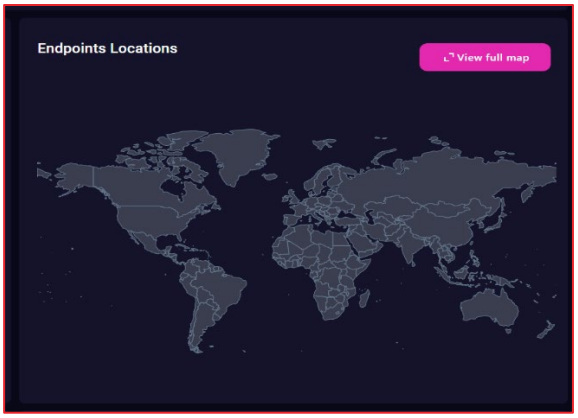
   Total Emulations

   Count of emulations that have been successful, Not Sent, and Failed.



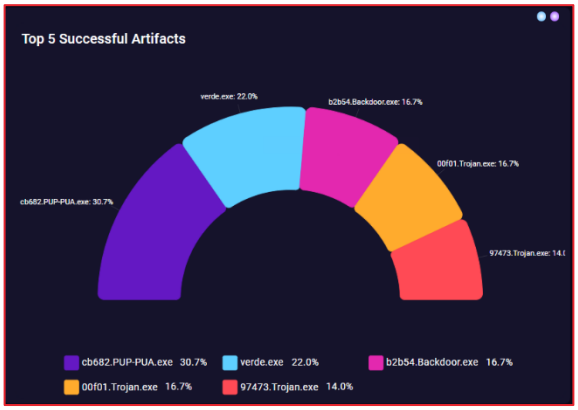
Top 10 Targeted Endpoints

Graphically represents the 10 Endpoints with the most emulations performed along with the count.



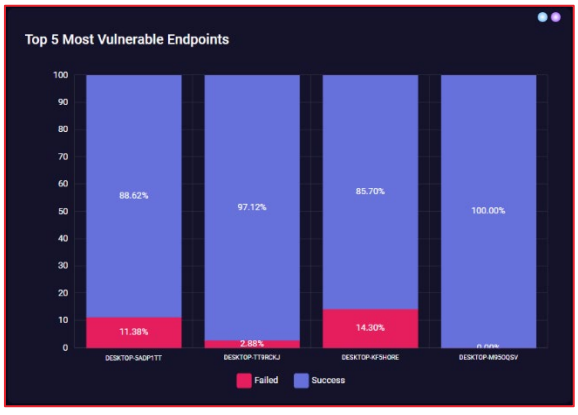
Endpoints Locations

It Displays a scalable interactive map that shows where the EndPoints are located around the world. This is often different infrastructures or VPNs that are deployed around the world. It is also possible to see the world in spherical mode, click on "View full Map".



Most Successful Threats

This is the top five files that were successfully executed from the attacker's point of view, in fact, this information corresponds to the emulations on the Endpoints.

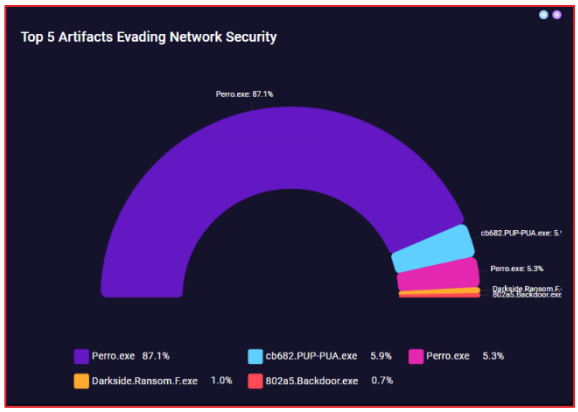


Most Vulnerable Endpoints

Shows the EndPoints in which emulations have been most successful.

-Blue: represent the percentage of threats that were able to successfully circumvent their security measures.

-Red: represent the percentage of threats that failed security.

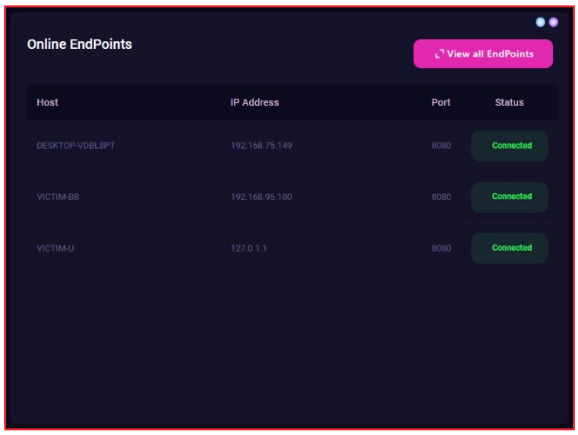


Threats Evading Network

This Shows the top five files that were able to evade the network vector successfully from the attacker's point of view.

Percentage Registered Emulations

Displays the total number of artifacts that were not delivered, failed emulations and successful emulations. Represented in percentages and in total quantities.



Online EndPoints

Indicates the details of the EndPoints that are online, such as their Hostname, Private IP Address, Port, and Status.

By selecting the "View all EndPoints" button the user will be redirected to the Endpoints Tab.

Events Timeline

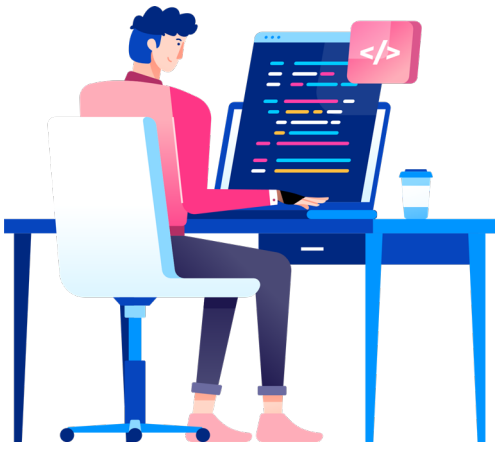
This is the timeline of the actions that were carried out globally on the Platform, which can be:

Loading artifacts, new packages, emulations performed and scheduled, as well as new endpoints registered.

Emulation Control

This section groups the tabs that allow the user to control emulations. Includes Endpoints, Threat Library, Packages, Emulations, IoC Validation, Custom Threat, and Incursion.

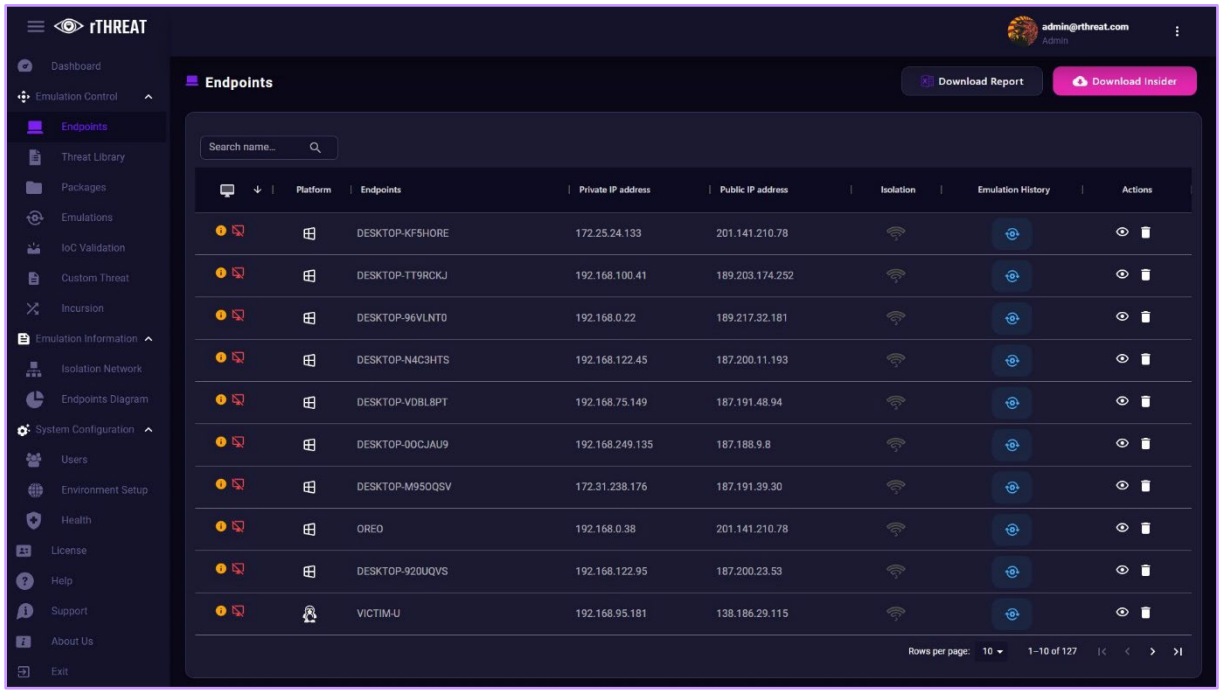
Each of them described below.



Endpoints

This section shows a table with all the Endpoints that have been connected to the Platform at some point in time.

From here the user can carry out Endpoint administration tasks and obtain Endpoint details.



In the upper part the Title of the Page: EndPoints and the options of "Download Report" and "Download Insider".

EndPoints Table

It holds the information regarding the Hosts that at some points have connected to the Platform, where it shows Connection Status and Version, Platform, Host Name, Private IP Address, Public IP Address, Isolation Status, Emulation History and Actions.

By default, the EndPoints will be displayed inline at the top of the table.

By default, ten rows of information are displayed. If the user wish to see more or change the pagination in the lower right corner are the pagination controls.

- Status

  Displays whether the EndPoint is online or offline within the host. Hover over the icon to get details. A red icon shows Disconnected, green icon indicates Connected.

- Host name

  Displays the name given to the Endpoint at the time of configuration.

- Platform

  Shows what type of operating system the Endpoint where the rThreat Software is installed has.

- Private IP address

  This shows which address each Endpoint has.

- Public IP address

  Displays the address that the Endpoints are connected.

- Isolation

  Indicates whether the Virtual Machine communications have been isolated or not. Green color shows isolation disabled (communications allowed), red indicates isolation enabled. See Emulation History of an EndPoint.

- Emulation History

  This opens a window where the user can see graphically the Emulations that have been made in that Endpoint.

- Actions

  Allows the user to view the Endpoint information and remove it.

Obtain EndPoint Details

To view the details of an EndPoint, follow these steps:

1. Click on the icon in the Actions column.
2. The EndPoint Details window will be displayed with information about the selected EndPoint.

- General Information: Connection status, Host Name, Alias, Connection Status, Isolation Status, IP Public, IP Private, Restart Insider, Port.
- Work users: Work Environments, User.
- OS Information: Platform, Name, Version, Compilation.
- Hardware Information: CPU Brand, CPU Speed, CPU Name, RAM, Hard Drive Capacity.
- Agent Information: Name, Version, Platform.

Rename an Endpoint: Alias

The user can rename an Endpoint on the Endpoints Table. This operation only works on this tab, on other sections of the platform the original Host Name will be displayed.

To rename a host do the following:

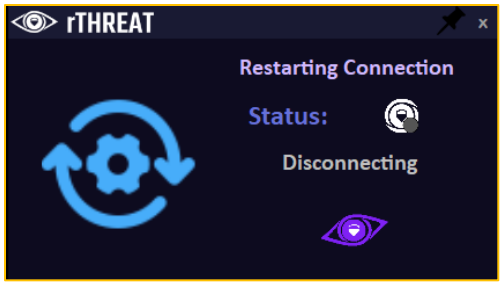
1. On the Endpoint Details Window select the General Information Section.
2. Locate the Alias Section.
3. Click on the edit icon. The Alias can be edited. Select a name for the Endpoint and click on the check icon to save the name.
4. On the Endpoints Table, the Alias name is Displayed.

Restart an Insider

The user can restart an insider. This operation only restart the rThreat software Insider, not the endpoint. The endpoint to be restarted must be online and connected to the platform.

To restart an insider, follow these steps:

1. On the Endpoint Details Window select the General Information Section.
2. Locate the Restart Insider.
3. Click on the SEND button to send the restart instruction. A notification confirms the instruction and, on the endpoint, a window with the retar status is displayed:

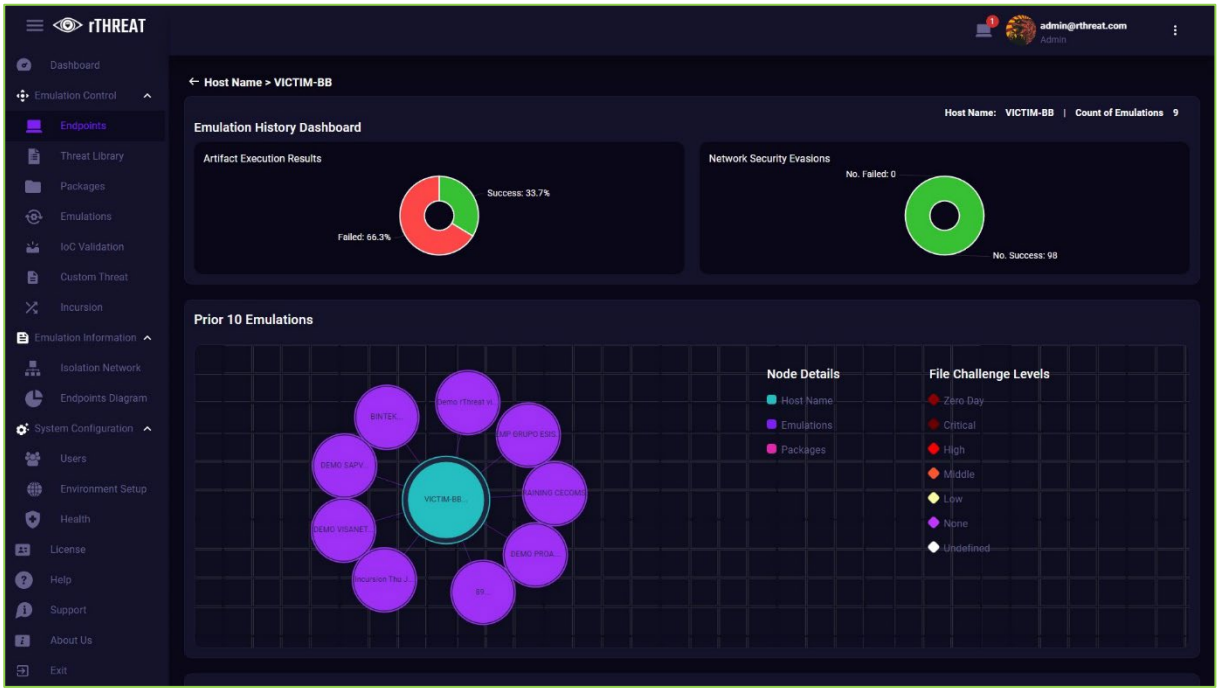


Emulation History of an EndPoint

It is possible to review the History of Emulations that have been carried out in each of the EndPoints registered in the Platform.

To view the emulation history of an EndPoint, follow these steps:

1. Click on the icon from the Historic Emulation column.
2. A new view with details of the selected EndPoint Emulations is displayed.



- **Historic Emulation Results Dashboard**

  Displays basic information such as:

  Host Name: shows the full name of the EndPoint at the top right.

Count of Emulations: number of emulations that have been made this EndPoint.

Artifact Execution Results: It gives a percentage of successful artifacts that were executed and a percentage of unsuccessful artifacts.

Network Security Evasions: It gives a success rate for not bypassing network security and the percentage of not bypassing the network.

- **Prior 10 Emulations Diagram**

It shows in a graph the last 10 emulation that were performed on that host with the following information.

General graphic: It shows the information in the form of pie. Clicking on the circles displays graphically the relationships between Emulations, packages and artifacts.

Node Details: Displays the Host, Emulations and Package categorization represented by colors.

File Challenge Levels: Shows what threat level each artifact is represented by colors

- **Report Table:**

Displays a report of the Emulations that have been performed on the host with the following information.

Emulation: Displays the name of the Emulations that have been made.

Package: Displays the name of the package that was sent within the run.

Success: Shows the number of artifacts that were successfully executed.

Fail: Shows the number of artifacts that were not executed and were failures.

Qualification: shows the result of the total emulation if it has failed, satisfactory or partially satisfactory.

- Failed: All or most of the artifacts were not executed.
- Satisfactory: All or most of the artifacts were executed.
- Partially Satisfactory: There were more executed artifacts than failed ones.

Date: shows the date and time that the emulation was made on the host.

- **Download Report:**

  Download a report of Emulations performed on the selected EndPoint in Excel format.

  To download the report, follow the steps below:

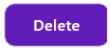
  1. Click on the Download Report Excel button. 

  2. Select the path on the local host to save the report.
  3. Click Save to download the report in .xlsx format.

Remove a Host

rThreat allows EndPoints to be removed from the Platform. Note that if the rThreat software has not been uninstalled from the EndPoint, the EndPoint will be re-registered in the table.

To permanently remove an EndPoint, it is necessary to follow the steps below and uninstall the rThreat software. See Uninstalling the rThreat Software.

1. From the Endpoints tab find the button with icon located in the Actions column.
2. Click on 

to remove the host or in 

to discard the changes.

rThreat Software : Insider

The rThreat software (Insider) will help us to communicate with the Orchestrator so that it can receive different types of threats, of different levels, which allows to execute them in the final EndPoint and to be able to generate the results of each one of those threats.

JSON Configuration File

The configuration file in .json format (JavaScript Object Notation) helps to generate a format for structuring data in the form of The json file is used to transfer link, host, port, and access data from each client's Platform to the Platform so that the rThreat Software can communicate with the Platform and send Emulations such as returning data to the client's Platform.

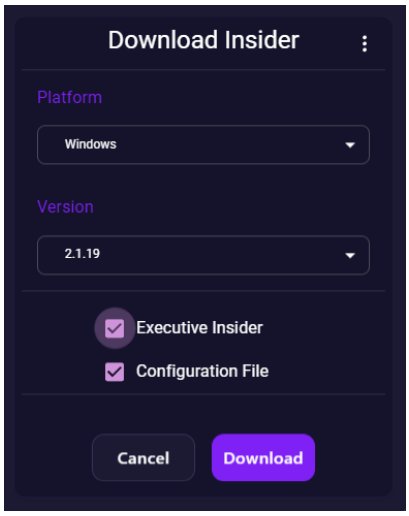
The json file is used to transfer link data, host data, ports, and access data from each Platform to each client, so that the rThreat Software can communicate with the Platform, send Emulations, and return the results of these Emulations.

Download the rThreat Software (Insider)

In this section the user can download the rThreat software and the .json file that handles giving the instructions for the rThreat software to fully perform its functions and work correctly the Emulations and generation of results.

To download the rThreat software follow the steps below:

1. Click on the "Download Agent" button in the upper right corner. 

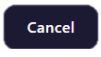


The rThreat software download window with the following options will pop up:

- Windows 10: It is the version for the Windows operating system.
- Linux: It is rThreat's software for the Linux operating system.

2. Click on the download button for the rThreat software depending on the operating system. Make sure to check the box next to Executive Insider, otherwise only the json file will be downloaded.

3. The user can download only the json configuration file, to do it do not check the box next to Executive Insider.
4. Depending on the operating system version, different files will be downloaded.
    - Windows: Insider Windows.zip
    - Linux: Insider GNULinuxtar.tar.xz.zip
5. Click on 

to continue or 

to stop the operation.

Download Report

A report in Excel format can be downloaded with the information of the EndPoints registered in the Platform. The information exported is Host Name, Private IP, Public IP, and Port.

To download the report, follow the steps below:

1. Click on the Download Report button 

found at the top right of the EndPoints tab.
2. Select the path on the local host to save the report.
3. Click Save to download the report in .xlsx format.

Endpoint Search

The "Search" option is displayed at the top of the table. 

for EndPoints search.

To search for Endpoints, follow the steps below:

1. Enter a sample name or a few characters in the Search Name field.
2. Press the ENTER key to perform the search or allow the table to dynamically filter results.

Sort Endpoints

The Endpoints table headers that allow ordering are Status, Platform, Host Name, Private IP Address, Public IP Address.

Each of these columns has quick order options represented by an upward pointing arrow ↑ or downward ↓ . 

To sort the elements in a column, follow the steps below:

1. Position the cursor on the column header text.
2. An upward arrow appears by default ↑.
3. Click on the arrow to sort the items in the column alphabetically (A-Z, smallest-largest).

The Status column will sort the EndPoints Online Offline.

The Platform column will sort the EndPoints Windows-GNU/Linux.

4. Click on the arrow again to reorder the column items alphabetically (Z-A, highest-lowest), the arrow will change downward. ↓.

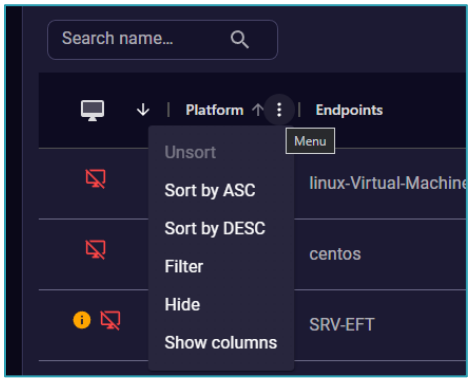
   The Status column will sort the EndPoints Offline- Online.

   The Platform column will sort the EndPoints GNULinux- Windows.

EndPoints Filters

To filter the elements of a column, follow the steps below:

1. Position the cursor at the end of the column header.
2. An icon appears ⋮ of options.
3. Click on the icon to display the advanced sorting and filtering options.



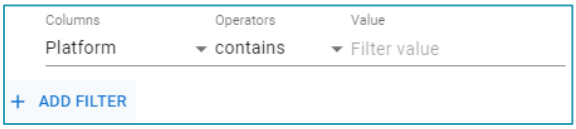
Unsort: When selected the order returns to its default state: Oldest to newest element.

Sort by ASC: This option sorts the information in ascending order.

Sort by DESC: It sorts the information in descending order.

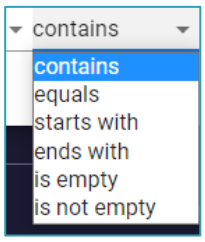
Filter: This is to filter the information according to more specific needs.

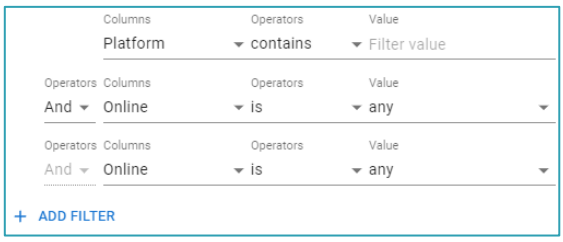
This option displays a new window.



In this menu we find the following options:

- Columns**:** Select the column to apply the filtering to, in any column this option can be used.
- Operators**:** Indicates content, if it is equal to , if it starts with, ends with, if it is empty or not.
- Value: The value to be considered in the filter.





- \+ Add Filter: Allows to add more filtering conditions to the same or other columns.

Hide: this choice allows to suppress or hide the information in the selected column.

Show colums: In this section we can select which columns we want to display in the user table according to our needs to improve the administration of user profiles.

A column search can be performed in the "Find column" section.

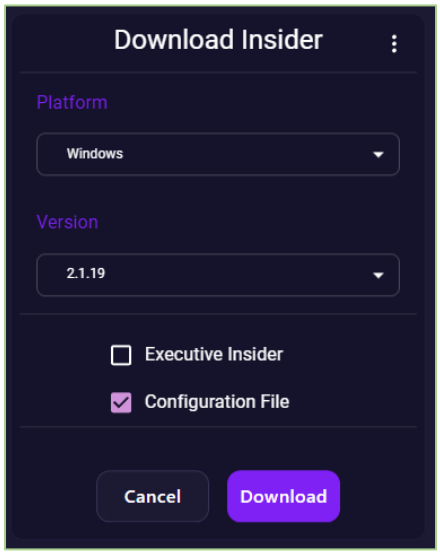
To enable or disable columns, use the switch next to each column name.

The user can hide or show all columns with the quick options at the bottom of the window (HIDE ALL and SHOW ALL).

Manipulating Past Versions of rThreat Software

The user can download older versions that have been uploaded to the Platform, this for both supported operating systems.

To manipulate past versions of the rThreat software follow the steps below:



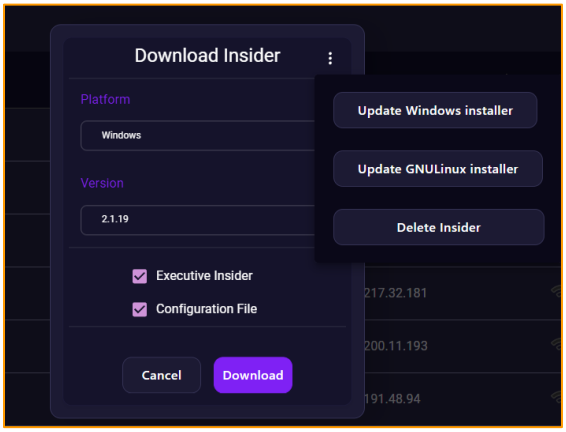
1. Click on the "Download Insider" button in the upper right corner. Download Insider
2. The Download Insider window is displayed.
3. Click on the drop-down menu of version.
4. The list of available past versions will be displayed, select the version the user want to download.
5. Check the box next to Executive Insider to download the software.
6. Click on the Download button to download the rThreat software from an earlier version.

Manipulate Installation Files

The user can manipulate and upload new configuration files and installers for supported operating system versions. This can be useful in case rThreat supplies the files.

To manipulate rThreat software versions, follow these steps:

1. Click on the Download Insider button in the upper right corner.
2. It will display the rThreat software download window.
3. Locate the installation file manipulation options button at the top right. ⋮
4. Click the button to display the installation file manipulation window.



Windows Installer Update

rThreat performs the update of the platform and insider automatically, if needed the user can manually add a new version of the installer. rThreat must supply these files.

To update and add a new Windows installer follow the steps below:

1. Click on the button ⋮ from the Download Insider window, to display the installation file manipulation window.
2. Select the Update Windows installer.
3. Follow the steps in the window presented to load a new configuration file.
    - **Select a File**: The file will be uploaded from the local location of the computer.
    - **Name**: enter the name of the file to be uploaded.
    - **Version**: to place the version of the file to be uploaded.
    - **Load**: Clicking on the upload button will upload the rThreat Software to the Platform.

Linux Installer Update

rThreat performs the update of the platform and insider automatically, if needed the user can manually add a new version of the installer. rThreat must supply these files.

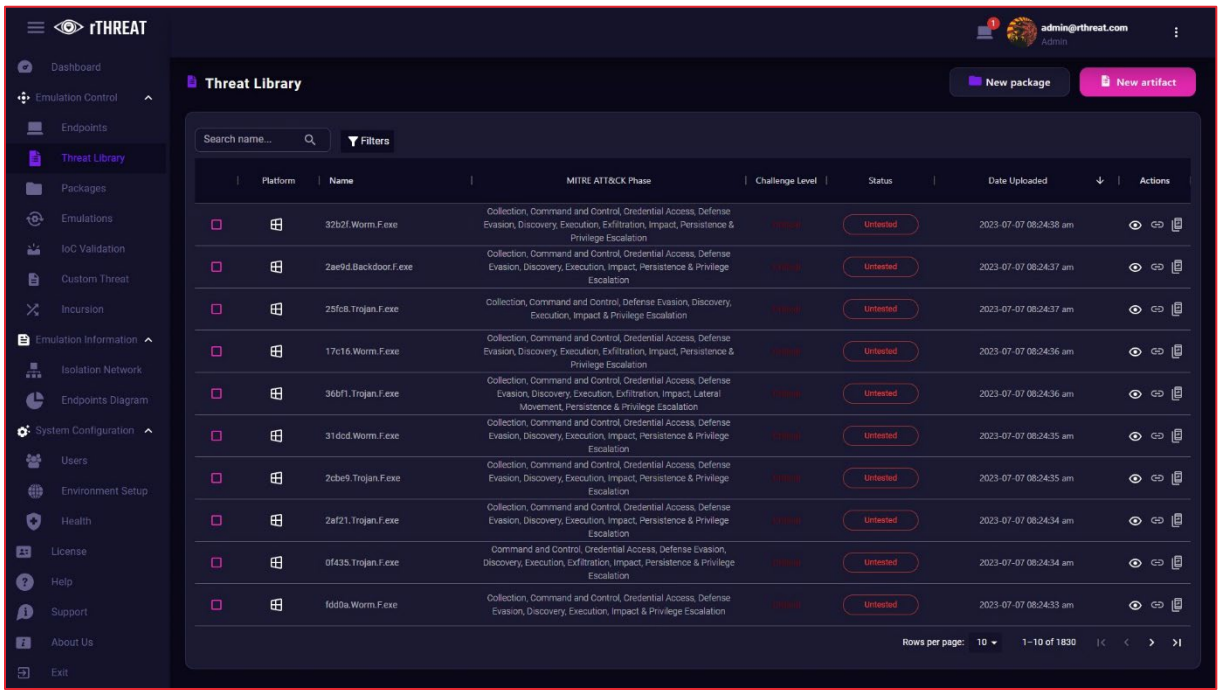
To update and add a new Linux installer follow the steps below:

1. Click on the button ⋮ from the software download window, to display the installation file manipulation window.
2. Select the Update GNULinux installer choice.
3. Follow the steps in the window presented to load a new configuration file.
    - **Select a File**: The file will be uploaded from the local location of the computer.
    - **Name**: enter the name of the file to be uploaded.
    - **Version**: to place the version of the file to be uploaded.
    - **Load**: Clicking on the upload button will upload the rThreat Software to the Platform.

Threat Library

This section presents a table where rThreat makes available a large library of known, modified, real-world zero-day threats.

Here we can find the actual malware samples or "artifacts" that have been uploaded to the Platform which will be tested on the Endpoint.



At the top of the page the title of the page: Artifacts. And the options of "New Package" and "New Artifact."

Threat Library Table

It holds the information regarding the artifacts that have been uploaded to the system. The user can see in a table all the artifacts present showing, Platform, Name, MITRE ATT&CK Phases, Challenge level, status, Date Uploaded and Actions.

By default, the elements in the table are presented from newest to oldest element.

By default, ten rows of information are displayed. If the user wish to see more or change the pagination in the lower right corner are the pagination controls.

- **Platform**

  This column shows which type of operating system the device is intended for.

- **Name**

  It is the name assigned to the artifact or malware sample, it can be a specific or generic name, which also has the type of malware it is.

- **MITRE ATT&CK Phase**

  The artifacts are mapped to MITRE which is a platform that organizes and categorizes different types of attacks, threats, and procedures to understand how attackers run to achieve their objectives. In this column we will find information about the tactics (based on MITRE) used in each artifact.

- **Threat Level**

  This choice shows with different color indicators how dangerous each threat is. This is shown by levels such as None, Low, Medium, High, Critical and Day Zero.

Level	Color	Impact
None	White	These have no action before the host.
Under	Yellow	They are those artifacts, which are being used in cyber-attacks, that are already known and detected by security solutions and that their behavior does not suggest any impact on the host.
Medium	Orange	Artifacts that can be obfuscated or modified and that may or may not be detected by signature by security solutions, their behavior suggests a non-serious impact on the host.
High	Red	Samples that have considerable impact on the host and are not detected by signature security solutions.
Critic	Red	Customized or modified artifacts, or encrypted artifacts, are executed in their entirety and have considerable impact on the host.
Day zero	Red	They are programs with malicious methodologies and a specific target, created by rThreat. The final artifact is unknown; therefore, the hash and URLs are unknown. intended for the callbacks. With which cybersecurity solutions are forced to perform intelligent validations to detect and hold these artifacts.

- **Status**

  This section tells us with color indicators if the artifact has already been tested if it is in emulation or if it has not been tested.

State	Color	Representation
Tested	Green	

Partially tested	Orange	Partially Tested
No tested	Red	Untested

- **Date Uploaded**

  This column shows the date on which the artifact was loaded onto the Platform.

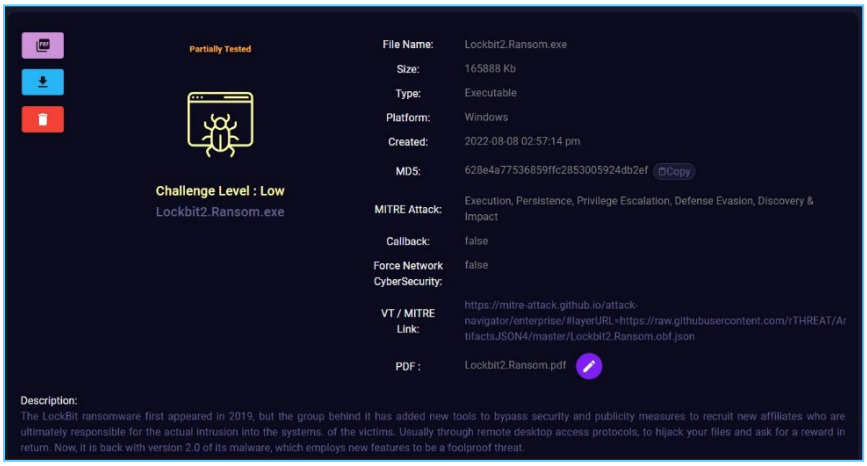
- **Actions**

  It allows to visualize the information of the artifact; the link is shown to visualize the table of MITRE ATT&CK and link to total virus of the artifact.

Obtaining Artifact Details

To view the details of an artifact, present in the library, follow these steps:

1. Click on the name of the artifact the user wish to obtain details of in the Name column or click on the icon in the Actions column.
2. A window with the details of the selected file will be displayed.

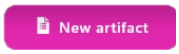


3. The information presented in this sale is described below:
   - **Name:** This is the name given to the artifact.
   - **Size:** Shows the size of the file in Kb.
   - **Type:** File type. Example: executable.

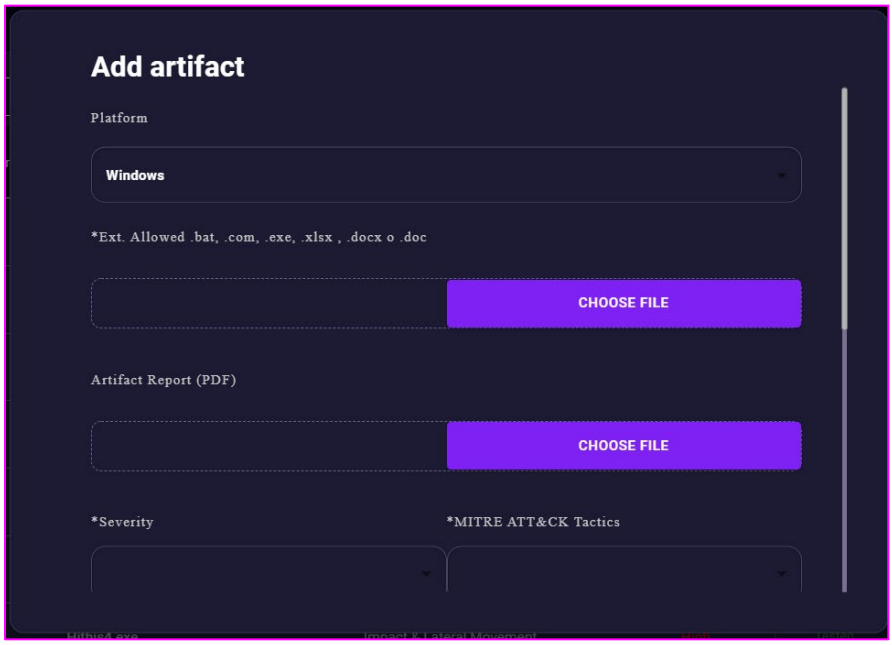
- **Platform:** Shows the operating system on which the device can be used.
- **Created:** Refers to the date on which the artifact was loaded onto the Platform.
- **MD5:** Hash associated with the artifact.
- **MITRE Attack:** These are the MITRE ATTACK tactics that the sample uses.
- **Callback:** If it shows "True" it can send a callback to the remote rThreat server, "false" if it does not send a callback. For more information see the
- **Force Network CyberSecurity:** True" is shown if the artifact is encrypted, and "false" if it is not.
- **VT / MITRE Link:** A link to VT or MITRE ATT&CK.
- **PDF:** If the artifact has an attached document with more extensive information about the sample, it can be found in this section and, if necessary, it can be added in the edit choice.  .
- **Description:** Displays information on the type of malware the artifact is, malicious, suspicious, and informative behaviors.
- **Test status of the artifact:** Shows with color indicators whether the artifact has been tested or not with the texts. Untested, PartiallyTested y Tested.
- **Challenge Level:** Severity of each threat showed when loading the sample into the library. An icon of the same color as the text is displayed showing the threat level.
-  : allows the user to download the PDF report associated to the file if exists.
-  : allows the user to download the selected sample.
-  : allows the user to remove the sample from the library.
- **Behavior Activities:** Present the indicators of the sample.

Adding a New Sample to the Library

This option allows the user to add a new artifact to the Platform. To add a new sample to the library, follow the steps below:

1. In the Threat Library tab select the "New Artifact" button at the top right. 

2. A form will open. Fill in all the fields with the information related to the sample.



- **Platform:** Here the user select the type of operating system for which the sample is intended (Windows or Linux).
- **Ext. Allowed**

  When selecting this option, there is a "choose file" section where the user will have to choose which artifact to add to the Platform.
- **Artifact Report**

  If the user have any document with more extensive or specific information about the artifact, it will be added at this point, in PDF format.
- **Severity**

  Here the user select the threat level of the artifact to be added (Critical, High, Low, Midd, None, Zero-Day).
- **MITRE ATT&CK Tactics**

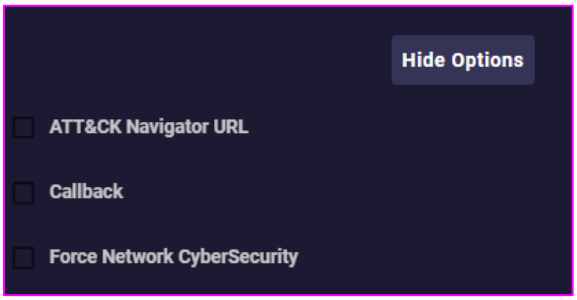
Mitre's tactics and techniques, used in the specific artifact, are selected, which are a set of techniques used by the adversaries to achieve a specific aim. For more information see https://attack.mitre.org/.

- **Description**

  Here the description of the artifact is assigned, i.e., what type of malware it is, what its malicious, suspicious, and informative behaviors are.

- **Show Options**

  Selecting this function will enable more advanced options for the sample.



  - ATT&CK Navigator URL: Here we can attach the MITRE link of the artifact.
  - Callback**:** This option is selected if the artifact or sample can send the callback to the remote server attack.
  - Force Network Cybersecurity: In this option the "manifests" of the encrypted artifacts are added.

- **Show Resolution Actions**

  By selecting this function, we can add more artifact information, the network, Endpoint, and Callback resolution actions are added, which for artifacts loaded by rThreat includes information such as their hashes or flags, string-based YARA Rule, and MITRE-based mitigations. Note that the user can add the own resolution actions to the samples the user load.

3. Click on Save to save and load the sample to the library. The sample is now available for testing and/or emulation.

Create a Package From the Threat Library Section

This option allows the user to create a new package to the Platform. To add a new package, follow the steps below:

1. Select the artifacts or samples that will be part of the new package using the checkboxes in the first column of the Threat Library table.
2. At the top right select the "New package". 

This will open a window where the user can see the selected artifacts and the fields that need to be filled in.
    - **Name:** This is the name we want to assign to the new package.
    - **Type:** The type of package is defined according to the samples it holds. See Package Categories.
    - **Description:** This section has information or characteristics of the created package.
    - **Report:** If the user have any informative document of any artifact, it is added in this section.
3. Click on 

to store the new package. The package is now available for testing and/or emulation. The user can view the created package in the Packages tab.

Download a Sample from the Threat Library

rThreat allows the download of samples to carry out actions such as creating the own rules or reverse engineering.

To download a sample, follow the steps below:

1. From the Threat Library tab click on the name of the artifact the user want to download in the Name column or click on the icon in the Actions column.
2. Locate the icon button next to the artifact name. This button allows the user to download the selected sample.
3. Click on the icon and then click on the button. 

to continue with the download or on the button 

to cancel the download.
4. After accepting the download, select the download path of the compressed file on the host.

5. Click Save and the artifact will be downloaded to the local host.

Artifacts downloaded from the rThreat library are compressed into a .zip file. Unzip this folder to get the compressed sample into a new zip and a file .txt with the password.

Delete a Sample from the Library

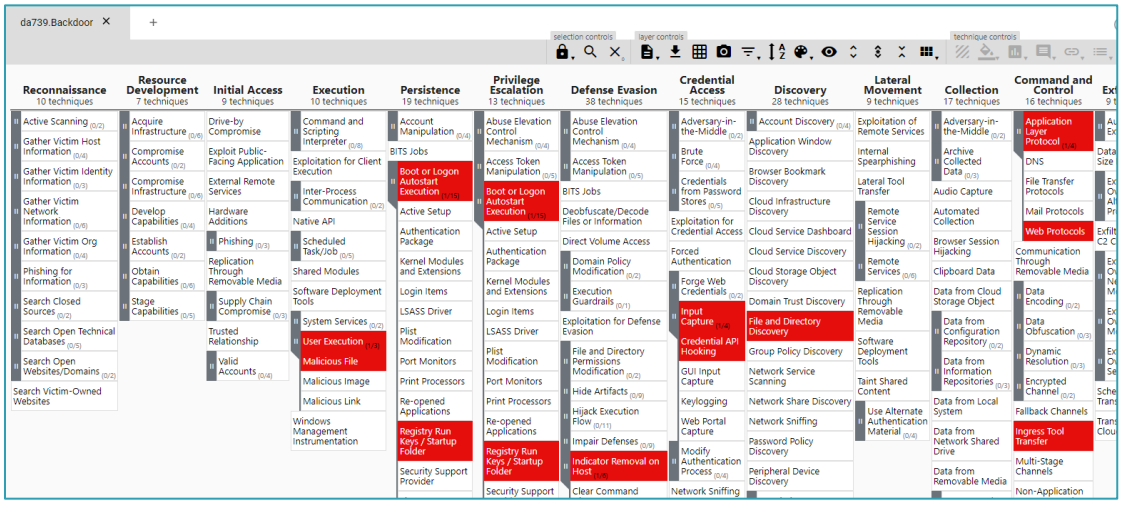
rThreat allows to remove samples from the library including samples supplied and those manually added.

To remove a sample from the library, follow the steps below:

1. From the Artifacts tab click on the name of the artifact the user want to download in the Name column or click on the icon in the Actions column.
2. Locate the button with icon button below the artifact name and the MITRE Url and Download PDF report buttons. This button allows the user to remove the selected sample.
3. Click on the icon and then on the button Yes to continue with the deletion or on the button No to cancel the download.
4. The artifact will be removed from the library.

View the MITRE Matrix Related to a Sample

The MITRE link shows the MITRE Table of the threat or artifact, including its tactics, techniques, and sub techniques, as shown below:



rThreat provide access to the coverage of the MITRE ATT&CK framework in the web interface for each emulation and package, the tactics of the MITRE ATT&CK are presented. For each sample a link to the MITRE ATT&CK Matrix is presented.

This view shows a map of all the phases that the sample could use during the attack.

To view the MITRE table related to a sample, follow the steps below:

1. From the Threat Library tab find the icon in the Actions column.
2. Click on the button and a new browser tab will open the MITRE ATT&CK Matrix. For more information visit https://github.com/mitre-attack/attack-navigator.

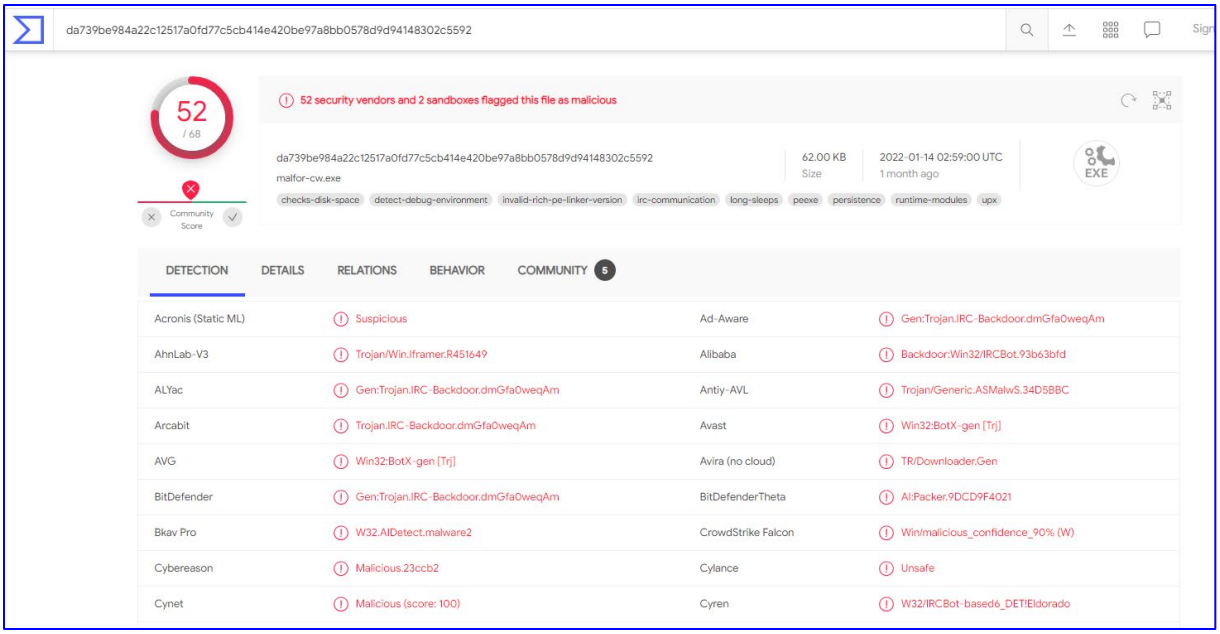
View VirusTotal Information Related to a Sample

The artifacts have a direct link to open the VirusTotal report related to the sample analysis. VirusTotal is a website that analyzes applications for malware, so we can see the result of the analysis and have at our disposal more than fifty different antivirus engines. For more information visit https://www.virustotal.com.

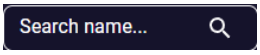
Links are available for all samples, however, for obfuscated samples there will be no information available in VirusTotal as these samples were manipulated by rThreat.

To view VirusTotal information related to a sample, follow the steps below:

1. From the Threat Library tab, find the icon associated with the sample found in the Actions column.
2. Click on the icon and a new browser tab will open the VirusTotal report associated with the selected sample.



Threat Library Search

The "Search Name" option is displayed at the top of the table. 

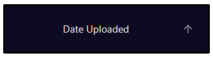
to search for Artifacts.

To search for artifacts, follow the steps below:

1. Enter a sample name or a few characters in the Search Name field. In this field the user can enter the name, or the nomenclature of the malware category (Trojan, miner, ransomware, or any other.) the user are looking for.
2. Press the ENTER key to perform the search or allow the table to dynamically filter results.

Sort Threat Library

The Threat Library table headers that allow ordering are Platform, Name, MITRE ATT&CK Phase, Threat Level, Status and Date Uploaded.

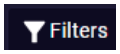
Each of these columns has quick order options represented by an upward pointing arrow ↑ or downward ↓. 

To sort the elements in a column, follow the steps below:

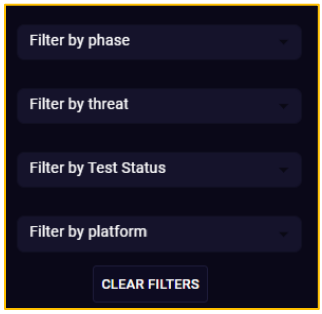
1. Position the cursor on the column header text.
2. An upward arrow appears by default ↑.
3. Click on the arrow to sort the column items alphabetically (A-Z).
4. Click on the arrow again to reorder the column items alphabetically (Z-A), the arrow will change to downward. ↓.

Threat Library Filters

To filter the elements of a column, follow the steps below:

1. Click on the button next to the "Filters" artifact search field. 

   Selecting this choice will display a small window like the following one:



2. Select the type of filter the user want to apply.
   - **Filter by phase:** Allows artifacts to be filtered according to Mitre's tactics.
   - **Filter by threat:** This option performs filtering according to threat levels.
   - **Filter by test status:** Filter out artifacts that have been tested, untested or partially tested.
   - **Filter by platform:** This last filtering choice is performed according to the operating system, i.e., Windows or Linux.

The table will be updated automatically. The user can combine the four types of filters to have a more exact result.

Artifacts Severity

Zero Day

Artifacts created by rTHREAT, modified, may have obfuscation, are not detected by security solutions, is not detected by heuristics, its emulation is performed in its entirety has considerable impact on the host may have callback and forced network security evasion.

Critical

Custom or modified artifacts, not detected by signature by security solutions, not detected by heuristics, has obfuscation, its emulation is fully executed and has considerable impact on the host, may have callback and forced network security evasion.

High

Files that are not detected by signature security solutions, can be detected by heuristics, have obfuscation, are partially or fully executed, and have a practical and considerable impact on the host.

Medium

Medium severity to files that may or may not be detected by signature by security solutions, may be detected by heuristics, their behavior suggests a non-serious impact on the host and may have obfuscation.

Low

Files that are detected by signature by security solutions and whose behavior does not suggest any impact on the host are considered low severity.

None

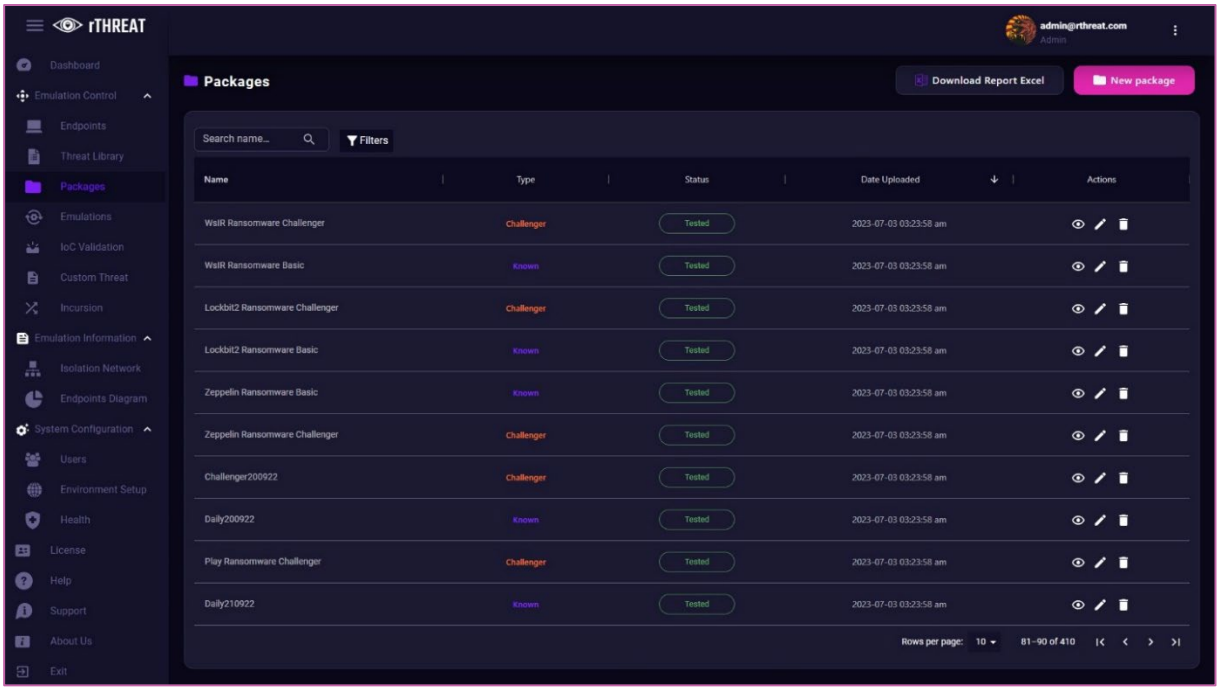
No impact on the host as it is not malicious.

Undefined

It is not defined how malicious the sample is.

Packages

This tab presents a table with all the Packages that rThreat or a User has created. From here the user can carry out tasks of managing the packages and obtaining details.



The user can see at the top the Title of the Page: Packages. And the "Download Report Excel" and "New Package" options.

Packages Table

The created packages are displayed in this table. By default, the EndPoints will be displayed inline at the top of the table.

By default, ten rows of information are displayed. If the user wish to see more or change the pagination in the lower right corner are the pagination controls.

The sections of the table include:

- **Name**

  Displays the name given to the package when it was created.

- **Type**

  Displays the type of package that was assigned to it when it was created. See Package Categories.

- **Status**

  Shows whether a package has been tested or not.

  Untested Indicates that the package has not been tested on any Endpoint.

Partially Tested Indicates that some of the artifacts in the package have already been tested.

Tested Indicates that the package has been tested on some Endpoint.

- **Actions**

  Allows the user to view package information, edit and remove the package.

Create a New Package

This option allows the user to create a new package in the Platform. To add a new package, follow the steps below:

1. In the Packages tab select the "New Package" button on the top right. New package
2. A package creation wizard will open.
3. Add the required fields such as Name, Type, Description, PDF File and Artifacts. Note that all fields except PDF File are needed.
4. Use the NEXT and BACK to navigate through the wizard.
5. In the Artifacts part the user can make use of the field Search... to search for the sample the user want to include in the package
6. Click on FINISH to save the changes.
7. The message "The package was created successfully" will confirm the creation of the package.
8. Click on ACCEPT to exit the wizard.

Editing an Existing Package

To edit an existing package in the table, follow the steps below:

1. Click on the Edit icon in the Actions column.
2. A package editing wizard will open.
3. Modify the required fields such as Name, Type, Description, PDF File and Artifacts.

4. Use the NEXT and BACK to navigate through the wizard.
5. In the Artifacts section the user can use of the field Search... to search for the sample the user want to include or remove from the package. By default, samples already in the package are selected.
6. Click on FINISH to save changes.
7. The message "The package was edited successfully" will confirm the package update.
8. Click on ACCEPT to exit the wizard.

Deleting an Existing Package

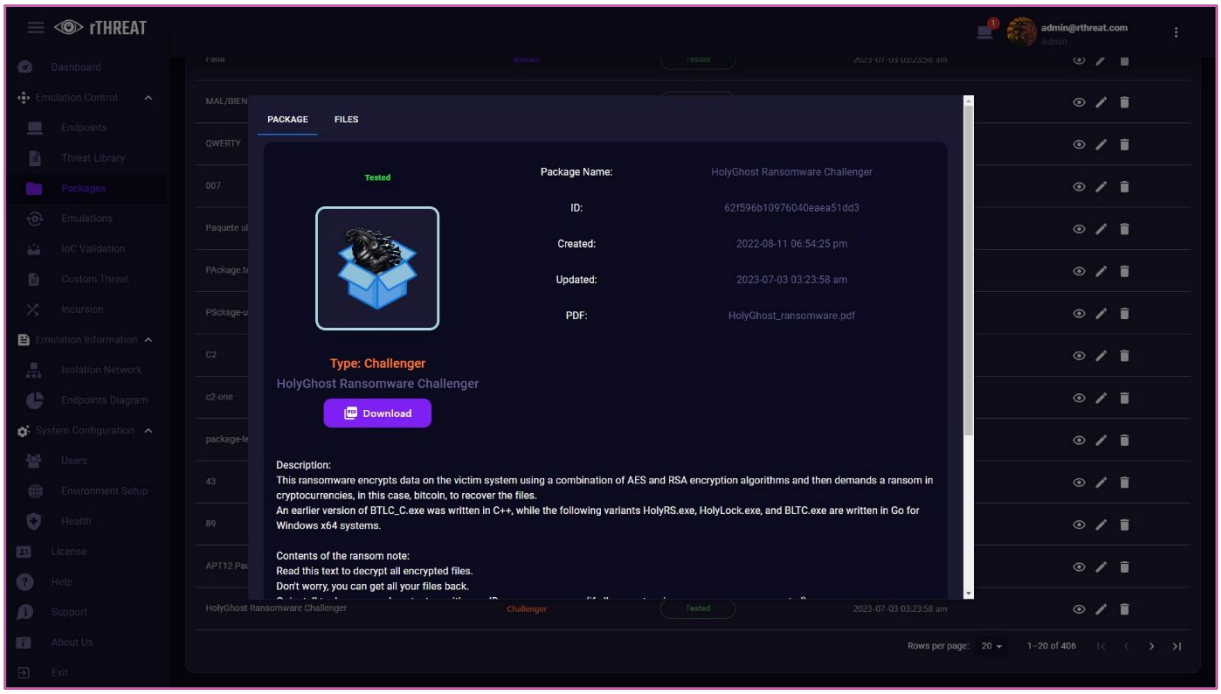
To remove an existing package from the database, follow the steps below:

1. Click on the remove package icon in the Actions column.
2. Click on Delete to remove the package or in Cancel to discard the changes.

Obtain Package Details

To view the details of a package, follow these steps:

1. Click on the icon in the Actions column.
2. A window with the details of the selected package will be displayed.



3. The information presented in this sale is described below:

- **PACKAGE** : Displays package details such as:

  Status: Whether it has been tested, partially tested, or not tested.

  Type. Refers to the category of the package.

  Download: Button to download the report associated with the package.

  Package Name: Name assigned when the package was created.

  Id: Package identifier in the rThreat database.

  Created: Displays date, time, user, and contact of the package creator.

  Updated: Displays date, time, user, and contact of the package creator.

  PDF: Name of the report assigned to the package. Not all packages have a report.

  Description: Description associated with the package.

- **FILES**

  Displays the artifacts that make up the package. The information presented for the artifacts is:

  Artifact name y Threat Level.

  Click on an artifact for more details such as Id, Size, MITRE Attacks, and MD5.

Download Report

A report in Excel format can be downloaded with the information of the Platform's packages. The information exported is package name, update date and package type.

To download the report, follow the steps below:

1. Click on the Download Report button 

found at the top right of the Packages tab.
2. Select the path on the local host where the user want to save the report.
3. Click Save to download the report in .xlsx format.

Package Search

The "Search" option is displayed at the top of the table. 

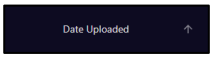
to search for packages.

To search for artifacts, follow the steps below:

1. Enter the name of a package or some characters in the Search Name field.
2. Press the ENTER key to perform the search or allow the table to dynamically filter results.

Sort Packages

The Packages table headings that allow ordering are Name, Type, Status y Date Uploaded.

Each of these columns has quick order options represented by an upward pointing arrow ↑ or downward ↓. 

To sort the elements in a column, follow the steps below:

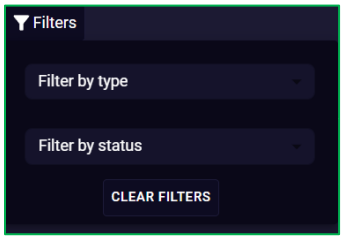
1. Position the cursor on the column header text.
2. An upward arrow appears by default ↑.
3. Click on the arrow to sort the column items alphabetically (A-Z).

4. Click on the arrow again to reorder the column items alphabetically (Z-A), the arrow will change to downward. ↓.

Packages Filters

To filter the elements of a column, follow the steps below:

1. Click on the button next to the "Filters" artifact search field.
2. Selecting this choice will display a small window like the following one:



3. Select the type of filter the user want to apply.
   - **Filter by type:** Allows to filter the artifacts according to the type of package.
   - **Filter by status:** This option performs filtering according to the test status of the package.

The table will be updated automatically. The user can combine the two types of filters to have a more exact result.

Package Categories

In rThreat, the following terms are used to name packages:

Known

This type of package only holds samples that are already known and detected by security solutions and whose behavior is of low impact on the host.

Challenger

This package has obfuscated samples.

Interactive

It has samples that can use command and control (C2) callback functionality, or samples that can be interacted with in the EndPoint after emulation.

Zero

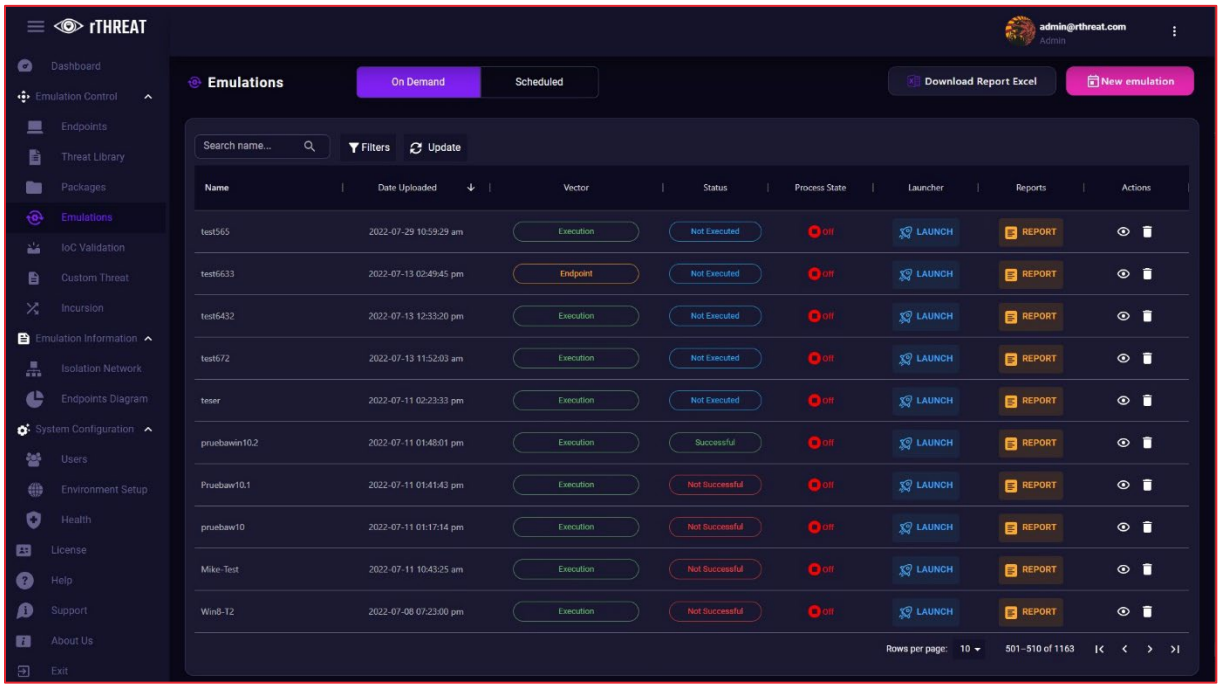
It has samples created by rThreat with malicious methodologies and a specific target, dangerous and challenging for security solutions.

Uncategorized

If the user are not sure in which category to place the package, the user can use this option.

Emulations

This tab holds the section to perform tests on the corresponding EndPoints that have the rThreat software installed, using the packages that were created in the Platform with a specific number of artifacts, as well as the reports generated after the emulation and creation of new emulations.



In the upper section: the Title of the Page: Emulations. The sections of "On Demand", "Scheduled" and options "Download Report Excel" and "New Emulation".

On Demand Emulations Table

A table shows the Emulations created, to be sent and sent on demand.

By default, the most recent configured or sent Emulations will be displayed at the top of the table.

By default, ten rows of information are displayed. If the user wish to see more or change the pagination in the lower right corner are the pagination controls.

- **Name**

  Displays the name given to the Emulation when it was created.

- **Date Uploaded**

  Displays the date on which the emulation took place, showing day, month, year, and time.

- **Vector**

Displays the vector or vectors that were evaluated with the emulation. See .

- **Status**

  Displays the status of the emulation result.

  One or more artifacts of the sent package were not executed.

  The emulation has not been sent.

  All artifacts in the given package were executed.

- **Process State**

  Displays in real time statuses of the emulation. See Emulation States.

- **Launcher**

  Allows the user to send a created Emulation or resend it.

- **Reports**

  Displays the detail of the results of the emulation performed.

- **Actions**

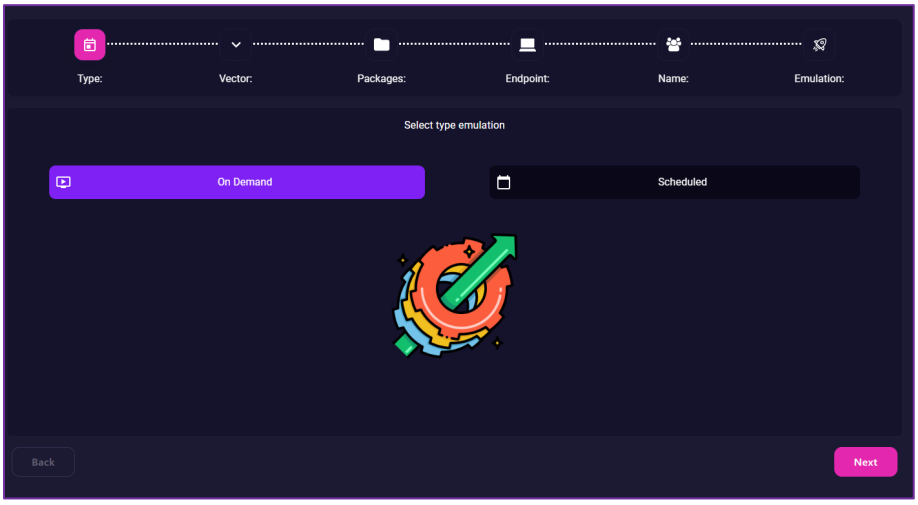
  Allows the user to view the emulation information and remove it.

Create a New On Demand Emulation

This option allows the user to create a new Emulation-on demand. This type of emulation requires that the EndPoint to which the user want to send the emulation is online. To create a new on demand Emulation, follow the steps below:

1. In the Emulations tab select the "New Emulation" button on the top right. 

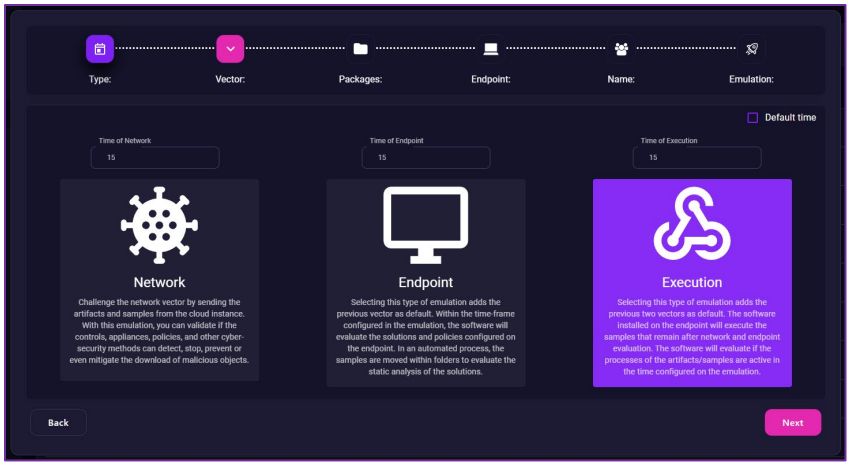
2. An Emulation creation wizard will open.



3. By default, the On Demand option is selected. Click on 

to continue.
4. Specify the vectors to be challenged. By default, an emulation with Real Emulation is selected.
5. The emulation time is specified by the indicator 

. If the user want to change the times of the Emulation being created, uncheck the Default time box. Three layers will appear where the user can show in seconds the time the user want for the evaluations in each vector.



The evaluation time is 15 seconds per vector. See View Details and Make Changes to EMULATION to change the default times.

6. Next, choose the catalog package the user want to send in the Emulation. The user can make use of the Search name... field to quickly locate the package. By default the most recently created packages are shown.

   Select Packages 20 Use the Select Packages filter to display in the same window 5, 10 or 20 packages.

   It is possible to select multiple packages in the same emulation.

7. Select the Endpoints to which the user want to send the emulation.
8. Provide a meaningful name to the emulation.
9. Finally select one of the three options presented:

   - Choose Emulate to send the emulation instantly.
   - Select Save emulation to save the Emulation. It will be displayed in the Emulations Table with status Not Executed.
   - Choose No to cancel the Emulation. This option will return the user to the first page of the Emulation creation wizard.
   - Back to edit the current emulation.

Scheduled Emulations Table

The Scheduled Emulations are shown in a table. By default, the most recent configured or sent Emulations will be displayed at the top of the table.

By default, ten rows of information are displayed. If the user wish to see more or change the pagination in the lower right corner are the pagination controls.

To display it, click on the "Scheduled" option. 

next to the section title.

- **Name**

  Displays the name given to the Emulation when it was created.

- **Updated By**

  Displays the user who scheduled or changed the Emulation.

- **Date Created**

  Displays the date on which the emulation was scheduled, showing day, month, year, and time.

- **Date Uploaded**

  Displays the date on which the emulation was scheduled, showing day, month, year, and time.

- **Date Started**

  Displays day, month, year, and time that the emulation was scheduled to be sent.

- **Calendar**

  Displays a window with details of the emulation.

  - Emulation Scheduled Name.
  - Calendar.
  - Date the Scheduled emulation Start.
  - Packages.
  - EndPoints emulation Scheduled.
  - Vector.

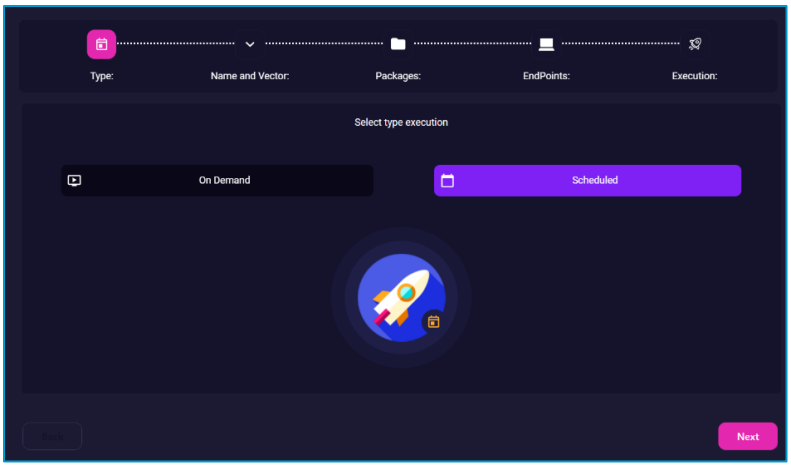
Create a New Scheduled Emulation

This option allows the user to create a new Scheduled Emulation. This type of Emulation does not require the Endpoint to which the user want to send the Emulation to be online. To create a new Scheduled Emulation, follow the steps below:

1. In the Emulations tab select the "New Emulation" button on the upper right-hand side. 

2. An Emulation creation wizard will open.
3. By default, the On Demand option is selected. Click on "Scheduled" to create a scheduled Emulation. Then select 

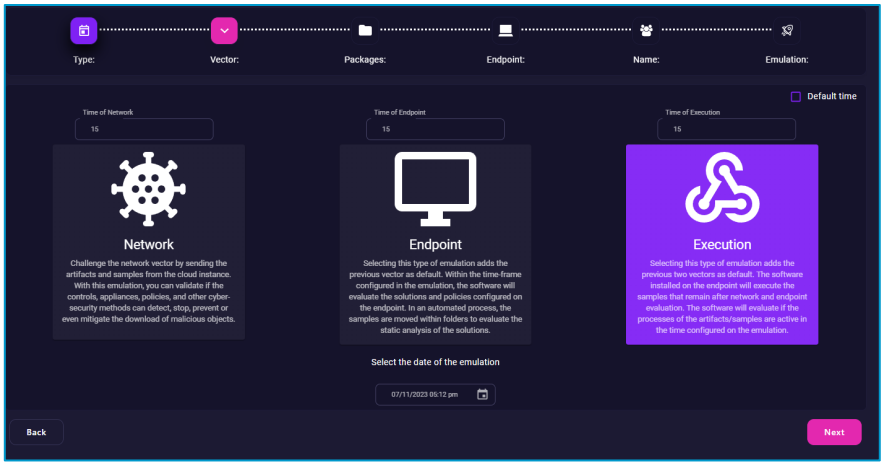
to continue.



4. Specify the vectors to be challenged. By default, an emulation with Real Emulation is selected
5. It is specified by the indicator 

. If the user want to modify the times of the Emulation being created, uncheck the Default time box. Three layers will appear where the user can indicate in seconds the time the user want for the evaluations in each vector.

   The evaluation time is 15 seconds per vector. See View Details and Make Changes to EMULATION to change the default times.
6. Click on the Select the date of the emulation section to pick date and time of the scheduled emulation.



7. Next, choose the catalog package the user want to send in the Emulation. The user can make use of the Search name... field to quickly locate the package. By default the most recently created packages are shown.

   Select Packages 20 Use the Select Packages filter to display in the same window 5, 10 or 20 packages.

   It is possible to select multiple packages in the same emulation.

8. Select the Endpoints to which the user want to send the emulation. In Scheduled Emulation, the user can select endpoints even if they are not online. However, the endpoint must be online at the time and date specified. Otherwise, a no Executed state will be presented on the emulation.

   Use the Search name... field to locate Endpoints.

9. Supply a meaningful name to the emulation.

10. Finally select one of the three options presented:

    - Select Save emulation to save the Emulation. It will be displayed in the Emulations Table with status Not Executed.
    - Choose No to cancel the Emulation. This option will return the user to the first page of the Emulation creation wizard.
    - Back to edit the current emulation.

Emulation Process

Once an Emulation is sent on demand or at the date and time configured in a scheduled Emulation the following steps are followed in an automated manner:

On the Endpoint, the rThreat software receives the instruction for a new emulation. A notification will alert the user of this new task. See Notifications.

1. At the same time, the rThreat software will display the window when sending an Emulation.
2. The states of the when sending an emulation on the rThreat Software window will change at the same time as those present in the Emulations Table. See Emulation States.
3. During the emulation and depending on the step the user are in, other indicators of the rThreat Software window will display related information.
4. At the end of the emulation, the window will remain visible for a moment showing whether the Emulation was successful or if there were errors.
5. In the On Demand Emulations Table, the status of the Emulation will be displayed according to the results and after the Process State will be set to Off.
6. The rThreat software will send to the Platform the results obtained.

When a scheduled Emulation is sent, it will automatically move to the On Demand Emulations table to see the Process State changes and when the Emulation can be sent again, but now on demand, view the report, and act on it.

Emulation Results

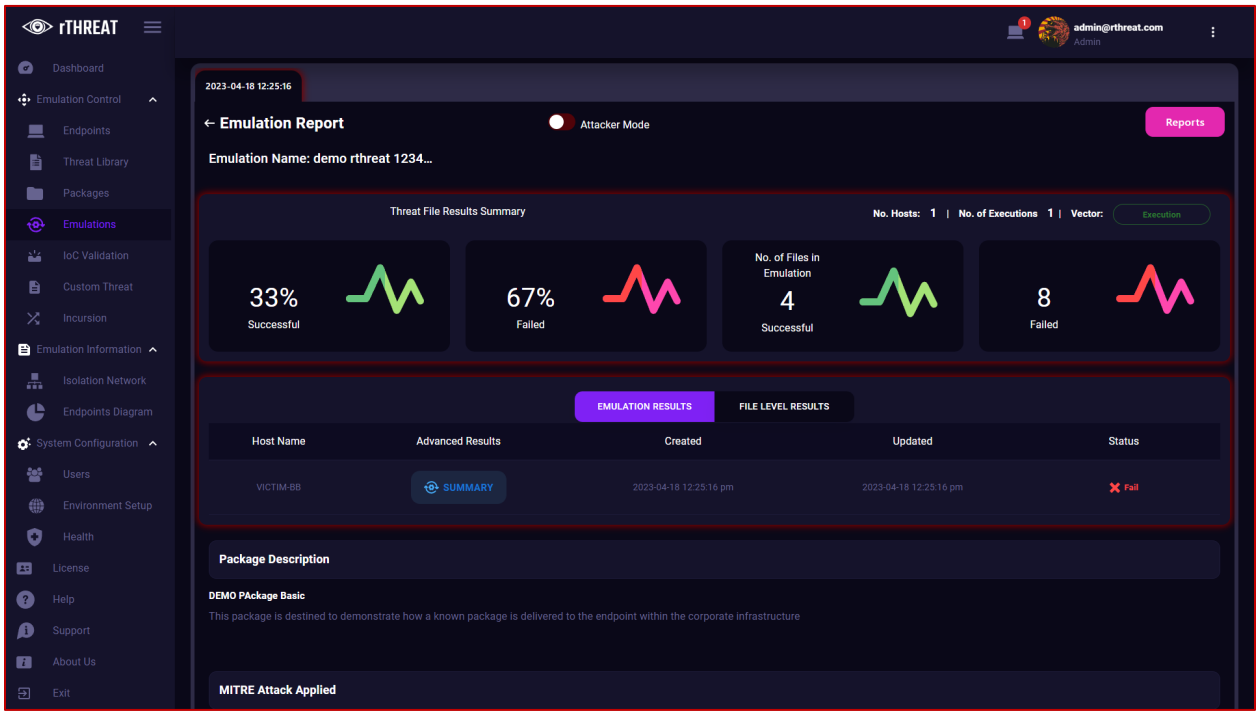
When the emulation is completed, the rThreat software sends the results to the Platform. In a graphical way, the user can see the details of what happened during the emulation.

Once rThreat identifies that a cyber-attack / emulation cannot be halted at the security controls level, the solution platform discloses this information along with potential remediation alternatives that it can provide for the organization's security teams such as firewall, IDS/IPS, NDR, SIEM, EDR, AV, XDR, SOC or any other.

After the completion of the emulation, rThreat provide a report detailing the obtained results and the success level of the attack simulation or emulation. The report include associated recommendations.

To view the results of an Emulation, follow the steps below:

1. In the Emulations On Demand table, click on the REPORT button corresponding to the desired Emulation in the Reports column.
2. The Emulation Report section will open, which presents in detail what was seen during the emulation.



In this section the user can find different elements and actions on the emulation.

- **Change Perspective**

  By default, the attack view and perspective are shown. It can be found by the red color in the margin of the other sections and by the top button is in "Attack Mode". 

  This mode allows the user to see the results of the emulation from an attacker's point of view.

  To switch to defense mode click on the "Attack Mode" button to change it to "Defense Mode". 

The defense mode can be identified by the blue color in the margin of the other sections.

This mode allows the user to see the results of the emulation from the defense point of view.

- **Reports**

  rThreat allows the download of direct reports in PDF format or xlsx. of the selected Emulation.

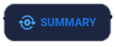
- **Threat File Results Summary**

  Displays the number of hosts that took part in the emulation, the count of Emulations performed and the emulation vector.

  Four widgets display information on the percentage of successful and unsuccessful Emulations as well as the number of artifacts that were successfully and unsuccessfully executed.

- **Emulation Results**

  The results of the emulation are presented in table form in general form as: Hostname, Advanced Results, Created, Updated and Status.

  Click on the 

 to display a window with the count of Emulations sent Emulations with errors and successful Emulations.

- **File Level Results**

  The results of the emulation detailed by artifacts are presented in the form of a table. The information presented corresponds to:

  Hostname: Name of the Endpoint that received the artifact.

  File: Name of the Artifact sent.

  Package: Name of the package to which the artifact belongs.

  Start: Information about the date and time when the emulation of the device was started. If the device is stopped by a security solution and prevents emulation, Not Start will be displayed.

  Finish: Information about the date and time when the emulation of the artifact was finished. If the artifact is stopped by some security solution and prevents emulation, Not Finish will be displayed.

  Network Vector: in this column will show with the indicator ✖ if the artifact was not able to breach the network vector. The indicator ✔ states that the

artifact was able to breach the network vector. To breach the network vector means that the sample was able to download on the endpoint.

Endpoint Vector: in this column will show with the indicator ✖ if the artifact was not able to breach the Endpoint vector. The indicator ✔ states that the artifact was able to breach the Endpoint vector and survived on the endpoint the default time.

Execution: in this column will show with the indicator ✖ if the artifact was not able to run on the Endpoint the default time. The indicator ✔ states that the artifact was able to execute on the Endpoint the entire default time.

C2 : will show with the indicator ✖ if the rThreat Platform did not receive a callback from the artifact upon emulation. The indicator ✔ states that the rThreat Platform did receive a callback from the artifact upon emulation. For more information on samples with callback functionality.

Emulation Status: in this column will display the message **Success** if the artifact was executed on the Endpoint. The message **Fail** will show that the artifact did not run on the Endpoint.

Actions. Click the Actions option to display information about the sample selected. The following information is presented:

- Name : Name of the sample.
- Start emulation: Timestamp of the emulation start.
- Finish emulation: Timestamp of the emulation end.
- Status : Complete emulation of the sample [true/false].
- Callback : Configured in the sample load [true/false].
- C2 : callback communication to rThreat server.
- Interpretation of the Sample: A short description of the overall state of cybersecurity based on the emulation result. This is just based on the rThreat results and should not be considered as a final state.
- Show emulation msg. Click on the 

button to obtain details on the operations rThreat perform managing the samples. A successful emulation operation (without considering the results of the vectors) will this play the artifact step messages. Depending on the type of emulation, these messages will show:
  - Phase one: Downloaded artifact.
  - Phase two: Downloaded artifact persists.

- Phase three: Artifact moved to temporary folder.
- Phase four: Artifact moved to temporary folder persists.
- Phase five: Executed Artifact.
- Phase six: Artifact execution persists.

- Follow Actions

  For each sample, basic resolution mitigations will be presented for each vector. These resolutions are related to the File Level Results Table meaning that only will display information about the vectors that were vulnerated from the attackers perspective or not stopped from the Defense perspective. Usually, Network and Endpoint vector will show the same resolution mitigations that include:

  - MD5, SHA1, SHA256.
  - String based YARA Rule.
  - MITRE ATT&CK Mitigations.

    rThreat is able to display success/failure scenarios within the MITRE ATT&CK framework on a tactical and technical basis in the web interface. This has to do with the success rate of the samples based on each vector. The Techniques and sub-Techniques are mapped to the related Mitigations provided by MITRE.

    For more information go to: https://attack.mitre.org/mitigations/enterprise/

  - Callback resolution mitigations will be presented only for zero-day samples. or the information added in this filed included on the sample load.

- **Package Description.**

  The description of the package sent in the emulation is displayed.

- **MITRE Attack Applied.**

  Describes each of the MITRE ATT&CK Tactics used in the package.

- **Attack Life Cycle**

Graphically shows in which phases of the life cycle of an attack the emulation package is active. This graph is merely illustrative and do not necessarily show that all the attack life cycle presented was performed.

Export a .xlsx Report of an Emulation

To generate a excel (.xlsx) report of an Emulation, follow these steps:

1. Click the button Reports on the top right corner of the emulation report.
2. Select the option and click Next to continue.
3. Select the choice to generate a report from the attacker perspective. Select choice to generate a report from the defensive perspective. Click Next to continue.
4. Select the type of report.

   By default, the Executive report choice is selected. In this type, only following information about the emulation will be exported:

   - File Level Results Table.

   Select the Detailed choice to add more information to the .xlsx report. In this type, the following information about the emulation will be exported:

   - File Level Results Table.
   - Actions.

Export a .PDF Report of an Emulation

To generate a PDF (.pdf) report of an Emulation, follow these steps:

1. Click the button Reports on the top right corner of the emulation report.
2. Select the option and click Next to continue.
3. Select the choice to generate a report from the attacker perspective. Select choice to generate a report from the defensive perspective. Click Next to continue.
4. Select the type of report.

By default, the Executive report choice is selected. In this type, only following information about the emulation will be exported:

- Summary
- File Level Results Table
- List of Artifacts
- Attack Life Cycle

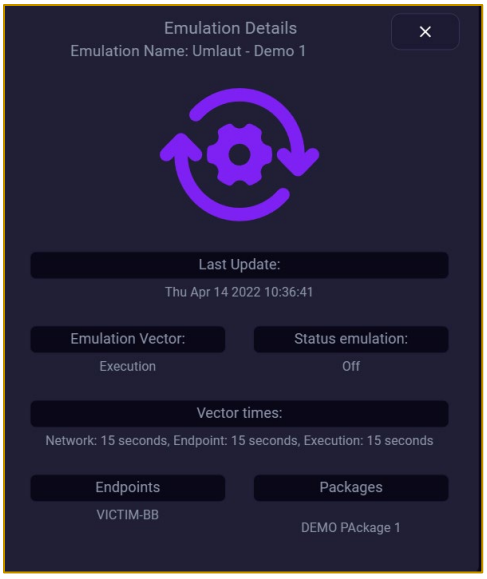
Select the Detailed choice to add more information to the report. In this type, the following information about the emulation will be exported if selected:

- Summary
- File Level Results Table
- Actions
- EndPoints Details
- Package Details
- List of Artifacts
- Artifacts Details
- Interpretation
- MITRE Description
- Attack Life Cycle

Obtain Details of an On Demand Emulation

To view the details of a package, follow these steps:

1. Click on the icon in the Actions column to open the Emulation Details window.
2. A window with the details of the selected Emulation will be displayed.



3. The information presented in the Emulation Details window is Emulation Name, Last Update, Emulation Vectors, Status emulation, Vector times, EndPoints y Packages.

Download Report Excel (Emulations)

To download a report with all the Emulations performed on the Platform, follow the steps below:

1. Click the Download Report Excel button 

found at the top right of the Emulations tab.
2. Select the path on the local host where the user want to save the report.
3. Click Save to download the report in .xlsx format.

If a filter is applied on the table, the emulations presented on the table will be the only ones to be exported.

Emulations Search

The "Search" option is displayed at the top of the table." 

to search for Emulations.

To search for an Emulation, follow the steps below:

1. Enter the name of an Emulation or some characters in the Search field.

2. Press the ENTER key to perform the search or allow the table to dynamically filter results.

Sort Emulations

The Emulations table headers that allow ordering are Name, Date Uploaded, Vector, Status and Process State.

Each of these columns has quick order options represented by an upward pointing arrow ↑ or downward ↓ . 

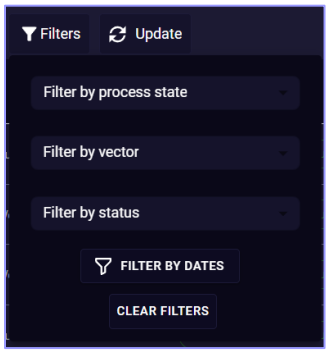
To sort the elements in a column, follow the steps below:

1. Position the cursor on the column header text.
2. An upward arrow appears by default ↑.
3. Click on the arrow to sort the column items alphabetically (A-Z).
4. Click on the arrow again to reorder the column items alphabetically (Z-A), the arrow will change to downward. ↓.

Emulations Filters

To filter the elements of a column, follow the steps below:

1. Click on the button next to the "Filters" search field.
2. Selecting this choice will display a small window like the following one:



3. Select the type of filter the user want to apply.

- Filter by Process state: Allows to filter the artifacts according to the status of the process: Finished or Off.
- Filter by Vector: This option performs filtering according to the emulation vectors: Real Emulation, EPP and Network Security.
- Filter by status: This option performs filtering according to the emulation status: Not Executed, Not Successful and Successful.
- Filter by dates: The user can select a range of dates.

Update On Demand Emulations Table

After performing some table emulation, the user should update the table.

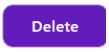
To update the emulations on Demand table, follow these steps:

1. Click the button next to the Filters: button 

.
2. Selecting this choice will update the table.

Deleting an Emulation Record

To remove an emulation record from the database, follow the steps below:

1. Click on the remove emulation icon in the Actions column.
2. Click on 

to remove the package or in 

to discard the changes.

Emulation States

All possible options shown in the notification window that the rThreat software displays that are sent through the WebSocket.

The ENDPOINT column on the table shows the labels displayed on the endpoint in the Notification Window. See Notifications.

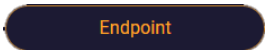
The PLATFORM column on the table shows the statuses in the Process State column of the On Demand Emulations Table.

ENDPOINT	PLATAFORM	Description
START	Start	Notification sent via WebSocket of the start of emulation.
DOWNLOAD	Download	Notification sent via WebSocket of the start of artifact download.
SURVIVEDOWLANDFILE	Survived Download File	Notification sent via WebSocket of the start of validation of the survival of downloaded artifacts.
TMPCOPY	Temporal Copy	Notification sent via WebSocket of the copy of the downloaded artifacts to the Emulations folder in the EndPoint.
SURVIVEDFILE	Survived File	Notification sent via WebSocket of the validation of the survival of artifacts copied to the Emulations folder in the EndPoint.
EXECUTE	Execute Artifact	Notification sent via WebSocket of artifact emulation.
SURVIVEEXEC	Survived Execute Artifact	Notification sent via WebSocket of the validation of the survival of an emulation.
Finish	Finish	Notification sent via WebSocket of the end of an emulation.
	Off	The emulation has been halted.

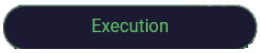
Emulation Vectors

1. Network: This vector choice is intended to test security platforms such as firewall, IPS/IDS, and others.

2. Endpoint: This vector choice is intended to test security platforms such as anti-malware, Endpoint Detection and Response (EDR) and others. This vector includes the combination of the previous vector: Network security.



3. Execution: This vector possibility is intended to perform the real execution of samples on the Endpoint. This vector includes the combination of the two previous vectors: Network security and EPP. This vector is the default possibility.



Network Vector Validation

In this vector, we send actual malware through an unencrypted channel, bypassing any VPN or tunnel. As the malware encounters your cybersecurity elements, it tests the efficacy of your security solutions.

Whether it be firewalls, IDS, IPS, NDR, or other products, their performance is determined by how well they identify, prevent, and alert in response to the real threat. Our platform does not rely on integrations, guaranteeing genuine assessments of your cybersecurity posture.

Endpoint Vector Validation

For this validation, we deploy the rThreat software (Insider) on a virtual machine (recommended) that mirrors the configuration, policies, and integrations of the zone being evaluated. The threat software creates a safe and isolated environment, blocking all communications and ensuring nothing escapes. If the malware reaches the endpoint, it assesses the effectiveness of your security products, such as antivirus, EDR, XDR, or other solutions. The objective is to validate whether these security measures generate real alerts, quarantine samples, and adhere to company protocols.

Execution Vector Validation

In the final phase, we execute the malware to challenge advanced agents claimed or believed to be functioning. This rigorous execution evaluates the effectiveness of

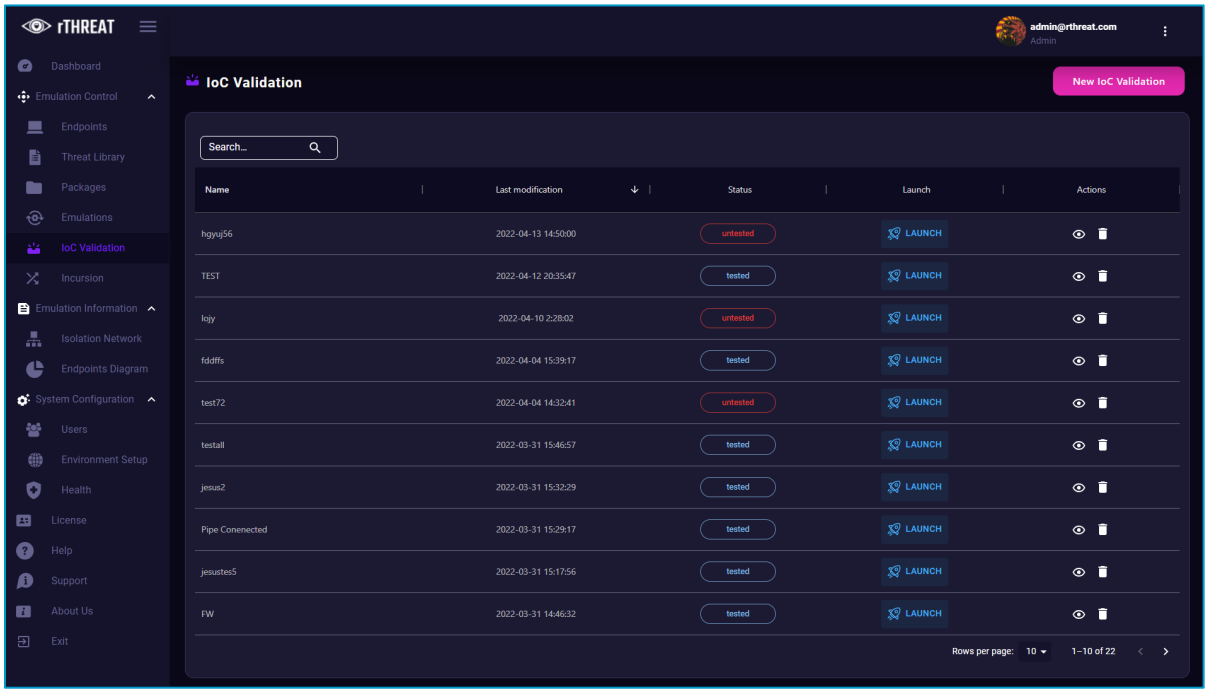
your security solutions in identifying and mitigating malicious samples. If the security products perform as expected and mitigate the threat successfully, the endpoint remains uncompromised. However, if the malware persists and the security products fail, the endpoint will be marked as compromised.

Our platform ensures a robust and secure environment for these assessments. With the capability to create snapshots, we can revert to a clean state and retry the emulation. This process allows your analysts, engineers, and incident response teams to validate their mitigation and response protocols effectively.

Our commitment to using real malware sets us apart from others, enabling us to deliver unparalleled validation of your cybersecurity defenses. The absence of licensing restrictions on event-based emulation allows us to perform simulations as many times as necessary to ensure your organization's utmost protection.

IoC Validation

This section allows the management of individual indicators of compromise (IOCs) Emulations.



In this Page, the title of the page: IOC Emulations, and the "New Emulation" button are shown.

IoC Validation Table

Holds the information regarding the IOC Emulations performed, where the Name of the emulation, the date it was modified, the status of the emulation, the emulation option (Launch) and Actions that can be taken are presented.

- **Name**

  Displays the name of the run that was configured when the run was created.

- **Last Modification**

  Displays the date and time when the last change was made to the run, which can be creation or emulation.

- **Status**

  Displays the status of the emulation.

  untested Indicates that the emulation has not yet sent.

  tested Indicates that the emulation has already taken place.

- **Launch**

  Displays the button LAUNCH used to start the emulation process.

- **Actions**

  Allows to view the emulation information and remove it.

By default, the most recent IOC Runs will be displayed at the top of the table.

By default, ten rows of information are shown. If the user wish to see more or change the pagination in the lower right corner are the pagination controls.

Obtain Details of an Unsent Validation

To view the details of an Emulation that has already been configured but not yet sent, follow these steps:

1. Click the icon in the Actions column.
2. The General Details window will be displayed with information of the selected run with the following data:
   - Name
   - Emulation Status
   - Selected Endpoint
   - Latest change information (date and time)
   - IOCs. Indicators selected in the emulation.

Obtain Details of a Sent Validation.

To view the details of an Emulation already sent, follow these steps:

1. Click on the icon of the Actions Column.
2. The General Details window will be displayed with information of the selected run with the following data:
   - Name
   - Emulation Status
   - Selected Endpoint
   - Latest change information (date and time)
   - IOCs. Indicators selected in the emulation.
3. Click on the Report Emulation section for details of each of the Indicators. The following information is displayed:
   - Name of emulation
   - Date and time of emulation
   - Indicators included in the emulation and their emulation status.
   - Click on each of the indicators to obtain the interpretation of the IOC. This interpretation will be displayed in the Interpretation of the IOCs selected section.

Create a New IoC Validation

To create a new IOC emulation, follow the steps below:

1. Click on the button New Execution found at the top right of the screen.
2. The Emulation creation wizard will appear.

To create an emulation, at least one EndPoint must be connected to the platform, otherwise the wizard will not allow the user to continue creating the emulation.

3. Click on the button Start to start the run creation.
4. The IOC Commands section is displayed. Click on the check box next to each command to select it or to select all click on the check box at the top of the column (Choices).

5. Click on the button > to move the choice to the Chosen column.
6. Click the button < to remove commands from the Chosen column.
7. Click the button Next to continue.
8. The EndPoint section will be displayed. Here the user can select the EndPoint to which the emulation will be performed.

   Please note that only one EndPoint can be evaluated at a time regardless of its licensing.

   Click on the icon for EndPoint details.
9. Click the Next to continue.
10. The Name section is displayed. Enter in the Name IOC Emulation field, the name the user wish to provide to the Emulation. Setting a name to the emulation is mandatory to continue.
11. Click the button Next to continue.
12. The Created IOC section displays the summary of the configured run information. Click Save to save the run. It will be saved and displayed in the IOC Emulations Table.
13. Click on the button LAUNCH to send the Emulation.
14. A confirmation window will appear. Click on Launch to send the emulation.

Some indicators require user-entered parameters. For more information on the indicators go to the IoCs section.

IoC Validations Search

In the upper section of the table there is a "Search" Search... option to perform a search for IOCs Emulations.

To search for IOCs Emulations, follow the steps below:

1. Enter the name of an IOC Run or some characters in the Search field.
2. Press the ENTER key to perform the search or allow the table to dynamically filter results.

IoCs

For the emulation of IOCs, there are twenty-six different options of indicators that can be tested, which are described below.

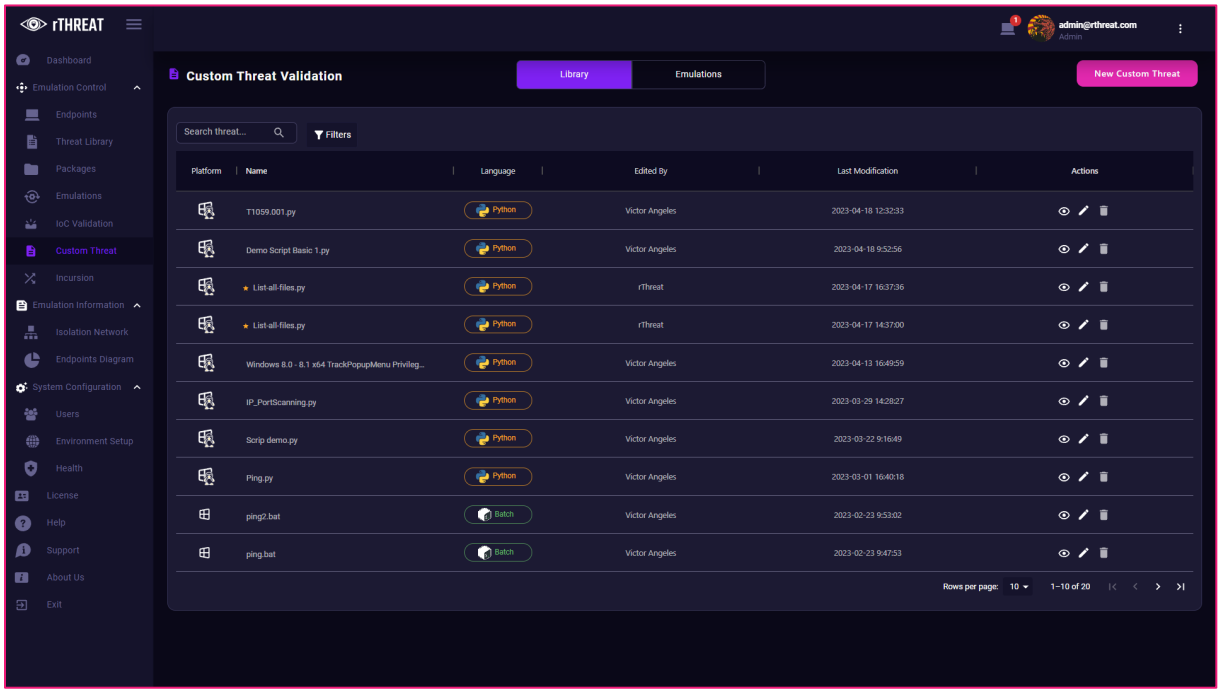
1. Process creation: A new process will be created.
2. A process changed a file creation time: A process will explicitly change a file creation time.
3. Network Connection: A new network connection event will be created.
4. Disable firewall: The firewall will be disabled.
5. Process terminated: A process is ended. It is necessary to specify the PID of the process to be stopped.
6. Driver Loaded: A driver is loaded in the system.
7. Image Loaded: A module is loaded into a process.
8. CreateRemoteThread: A process will create a thread in another process.
9. RawAccessRead: A process will perform read operations from the unit using the denotation.
10. ProcessAccess: A process will open another process.
11. FileCreate: A new file is created.
12. RegistryEvent (Object create and remove): An operation of creation or deletion of Registry key and value is performed.
13. RegistryEvent (Value Set): The modification of a Registry value is performed.
14. RegistryEvent (Key and Value Rename: The renaming of a registry value is performed.
15. FileCreateStreamHash: A named file stream is created.
16. ServiceConfigurationChange: A configuration change is made.
17. PipeEvent - Pipe Created: A named pipe is created.
18. Pipe Connected: A connection of a named pipe is made.
19. WmiEvent - WmiEventFilter activity detected: A WMI filter event will be registered.
20. WmiEventConsumer activity detected: A WMI consumer will be logged.

21. WmiEvent - WmiEventConsumerToFilter activity detected: A WMI consumer shall join a filter.
22. DNSEvent - DNS query: A process will execute a DNS query.
23. File Deletion Event: A file will be removed.
24. ClipboardChange - New content in the clipboard: Changes will be made to the contents of the system clipboard.

For more information:
https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

Custom Threat

This tab has the section to perform emulations on the corresponding EndPoints that have the rThreat software installed, using scripts that are uploaded or created in the Platform.



In the upper left side, the Title of the Page: Custom Threat Validation. The sections “Library” and “Emulations” in the top middle and the “New Custom Threat” button at the top right.

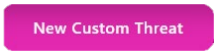
The custom Threat Validation table is presented. Custom threat in rThreat relate to scripts.

The user can create a New script or upload existing scripts to the rThreat platform. The supported languages for scripts are python ".py", perl ".pl", ruby ".rb", powershell ".ps1", bash ".bat", shell ".sh".

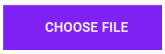
New Custom Threat: Upload an existing script

Before creating a new custom threat make sure the user have met the requirements for the Custom Threats Module. See Requirements for the Custom Threat Module.

To upload an existing script, follow this process:

1. In the Custom Threat tab select the "New Custom Threat" button on the top right. 

2. A New Script creation wizard will open.
3. By default, the 

choice is selected. This choice allows the user to upload a script to the platform. Click on 

to select the script the user want to upload.
4. Add a Description to the selected script (mandatory).
5. The user can add Execution Parameters if needed on the Optional parameters configuration field.
6. Click 

.

New Custom Threat: Create a script in the Platform

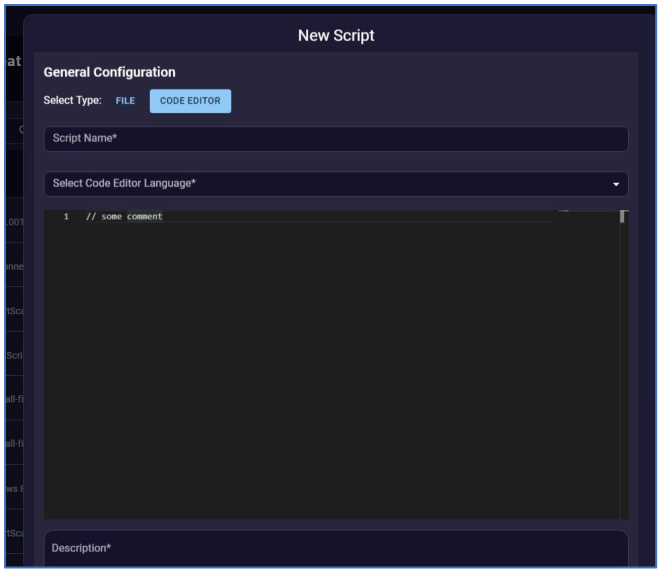
Before creating a new custom threat make sure the user have met the requirements for the Custom Threats Module. See Requirements for the Custom Threat Module.

To create a script directly in the platform, follow this process:

1. In the Custom Threat tab select the "New Custom Threat" button on the top right. 

2. A New Script creation wizard will open.
3. Click 

This option allows the user to write a script on the platform.
4. Give the script a name and select The code Editor Language. (Mandatory)
5. Write the script on the editor section.



6. Add a Description to the selected script (Mandatory).
7. The user can add Execution Parameters if needed on the Optional parameters configuration field.
8. Click Save Script .

Obtain Details of an Existing Script

To see details of an existing script, do the following:

1. In the Custom Threat tab, the Library view is active by default.

2. Click on the name of the script or select the icon in the Actions column.
3. A window will be displayed with details of the script.
   - Name
   - Platform
   - Language
   - Last Modification
   - MD5 Hash.

Editing an Existing Script

To Edit an existing script, follow these steps:

1. In the Custom Threat tab, find the script to edit.
2. Click on the Edit icon in the Actions column.
3. The Edit script Editor will appear.
4. Edit the part of the script the user need. The sections that can be edited are:
   - Alias
   - Code
   - Description
   - Execution Parameters.

   Name, language, and Platform are not editable.
5. Click Save Script to keep the changes.

Deleting an Existing Script

To delete an existing script, follow these steps:

1. In the Custom Threat tab, find the script to delete.
2. Click on the Edit icon in the Actions column.
3. Click on Delete to remove the script or in Cancel to discard the changes.

Creating a new Custom Threat Emulation

To create a new Custom Threat Emulation:

1. In the Custom Threat tab, at the top center, click on Emulations.
2. The Custom Threat Validation Table changes to the Emulations View.
3. The top right button will also change. Click on New Emulation.

4. A wizard will be prompted. Supply a Name and Description (Mandatory) and then click Next.
5. Select the Endpoint targets. If no endpoints are online, the user can still configure the emulation to send it later. Click Next to continue.
6. Select the script to send in the emulation. The user can select multiple scripts on one single emulation.

   Use the Search name... field to find the scripts or use the pagination at the button.

   Click Next to continue.
7. Review the emulation details. Click on the Back button to make changes to the emulation. Click Save to store the emulation.
8. The new emulation will be added to the Custom Threat Validation Emulations Table at the top. Click LAUNCH to send the emulation.
9. Confirm the Emulation launch clicking Yes. The emulation will be sent to the endpoints configured.

   To abort the emulation launch, click on the No button.

Report of a Script Emulation

To see details of a Script Emulation, do the following:

1. In the Custom Threat tab, at the top center, click on Emulations.
2. The Custom Threat Validation Table changes to the Emulations View.
3. In this firs table the user will see details of the emulation sent or unsent.
   - **Name :** Title of the emulation
   - **Endpoints :** Number of Endpoints configured to send the emulation.
   - **Custom Threats:** Number of scripts configured on the emulation.
   - **Executed By:** User that configured the emulation.
   - **Execute Date :** Emulation last change (creation/execution).

- **Launcher:** Have the Launch Button.
- **Reports:** Has the Report Button.
- **Actions:** Holds the File Details button and Delete Emulation button.

To see advanced details of a Script Emulation:

1. In the Custom Threat Validation Table, emulations view find the Actions column.
2. Click on the File Details icon .
3. A Summary Window will appear displaying details of the emulation such as:
   - Name
   - Description
   - Status
   - Created By
   - Last change
   - Endpoint(s):
   - Script(s):
4. Click on Close or outside the window to exit.

Removing a Script Emulation

To remove a Script Emulation, follow these steps:

1. In the Custom Threat Validation Table, emulations view find the Actions column.
2. Click on the Edit icon.
3. Click on Delete to remove the Script Emulation or Cancel to discard the changes.

Emulation Results

Once the emulation is completed, the rThreat software sends the results to the Platform. In a graphical manner, the user can see the details of what happened during the emulation.

To view the results of an Emulation, follow the steps below:

1. In the Custom Threat Validation Table, emulations view click on the 

button corresponding to the desired Emulation in the Reports column.
2. The Emulation Report section will open, which presents in detail what was seen during the emulation.
3. This is the information presented on the section:
    - **Emulation name:** Name provided to the emulation.
    - **Custom Threats File Results Summary :** Graphic display of Number of endpoints, Success (Script) Files sent and Number of Failed (Script Files).
    - **Total Scripts in Emulation :** A chart with the Custom Threats File Results Summary information.
    - **Execution Date.** Date of the performed emulation.
    - **Download All Logs** : Button to download all logs in an emulation.
    - **Effectiveness:** An average of Successful emulations.
    - **Endpoints Scripts Emulation:** Per endpoint present the following information:
        - Scripts File Emulation: Name of scripts on emulation
        - Language : Programming language of the script.
        - Script File Platform
        - Status: Displays if script was able to execute or not (regardless of the script task).
        - Errors
        - Actions Presents the Preview and Download Log File of the script.

View and download Script Emulation Logs

The user can download a Script Emulation Logs (results) in this section. This log has what the script performed. It is important to emphasize that the Script should have a result on the console. This result is what is presented on the logs.

To download all the Logs of an Emulation, follow these steps:

1. In the Custom Threat Validation Table, emulations view click on the 

button corresponding to the desired Emulation in the Reports column.
2. Click on the 

button found in the section “Download All Logs.”
3. The Platform will generate a .zip file with all the logs in the emulation. Save this .zip file.

To download the Logs of all Scripts Emulation on a specific endpoint , follow these steps:

1. In the Custom Threat Validation Table, emulations view click on the 

button corresponding to the desired Emulation in the Reports column.
2. Click on the 

button at the right side of the endpoint's name on the Endpoints Scripts Emulation.
3. The Platform will generate a .zip file with all the logs in the emulation. Save this .zip file.

To download the Logs of a specific Script Emulation, follow these steps:

1. In the Custom Threat Validation Table, emulations view click on the 

button corresponding to the desired Emulation in the Reports column.
2. Click on the  button in the Actions Column of the Script used in the emulation in the Endpoints Scripts Emulation Section.
3. The Platform will generate a .zip file with all the logs in the emulation. Save this .zip file.

To View the Logs of a specific Script Emulation, follow these steps:

1. In the Custom Threat Validation Table, emulations view click on the 

button corresponding to the desired Emulation in the Reports column.

2. Click on the button in the Actions Column of the Script used in the emulation in the Endpoints Scripts Emulation section.
3. A window will appear with the log of the emulation. By default, is presented:
    a. Script Name
    b. Hostname
    c. Output (logs) If the script failed, some information will be presented here. This is related to the Language interpreter not rThreat.

Incursion

It is possible to perform an attack emulation in a simpler way and allows the display of attack details. It will also send a package that the user have selected through the network and security controls to the destination endpoint.

Create a New Emulation Using Incursion

This option allows the user to create a new Malware/samples Emulation-on demand in a simpler path. To create a new Emulation using Incursion, follow these steps:

1. Selecting the Incursion tab will display an Emulation Wizard.
2. An Emulation creation wizard will open.
3. Select the type of emulation to be configured.
    - **Now**: Performs on Demand emulation
    - **Scheduled**: Configures an Emulation to be sent later (scheduled). If the user select this option, the Date and Time parameter will be displayed. Set the details of the Emulation in this section.
4. Click on Next to continue.
5. Select the package(s) the user want to include in the Emulation. Use the buttons to navigate between the package categories. See Package Categories.

    Use the search bar to filter the packages.
6. Click on Next to continue or in Back to return to the Type window.

7. Select the vector to be confirmed. Real Emulation is displayed by default. Move the bar to the EPP or Network Security vectors if the user want to perform the emulation to those vectors.
8. In the same window, the user can change the default times for each of the Vectors of the Emulation. Click on the option Default Time to deactivate the default times. Three new fields will appear where the user must set in seconds the preferred time for each vector.
9. Click on Next to continue or in Back to return to the Package window.
10. Select the Endpoints to which the user want to send the Emulation.
11. Click on Next to continue or in Back to return to the Vector window.
12. By default, a generic name for the Emulation is displayed. Including the word Incursion followed by the date and time at which the Emulation configuration is being performed.

    The user can remove that name and set a new one.
13. Click on Next to continue or in Back to return to the Endpoints window.
14. If I set up an On Demand emulation, click on the button Execute to send the emulation at that time. The user will be redirected to the On Demand Emulations table in the Emulations tab.

    If the user have configured a scheduled Emulation, click on Scheduled to schedule the Emulation. The user can find the scheduled Emulation in the Scheduled Emulations Table section of the Emulations Tab.

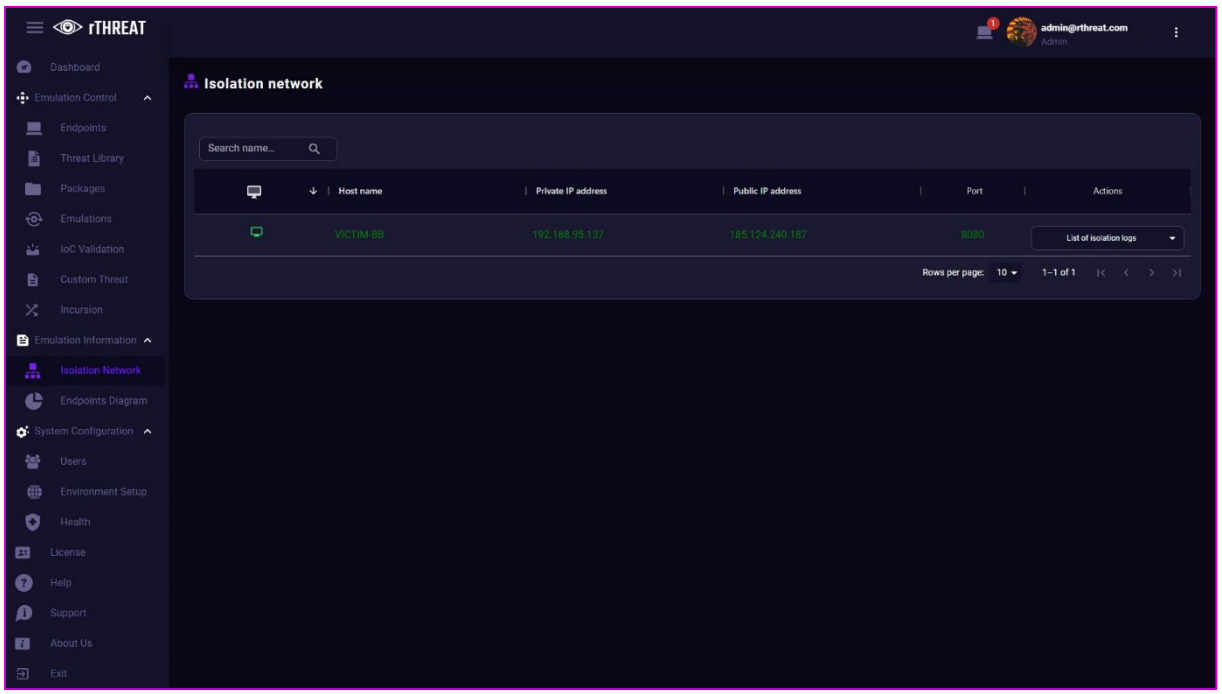
Emulation Information

This section groups the tabs that allow the user to get more information related to emulations. Includes Isolation Network and Endpoint Diagrams.

Each of them is described below.

Isolation Network

In this section the user can download the log of the Isolation Network process.



At the top of the page the title of the page: Isolation Network. And the Isolation Network table.

Isolation Network Table

Has information regarding Hosts that are online and information such as Connection Status, Host Name, Public IP Address, Private IP Address, Port and Shares.

This table will only show EndPoints information that is online.

By default, ten rows of information are displayed. If the user want to see more or change the pagination in the lower right corner, there are pagination controls.

- **Connection status.**

  Shows whether the EndPoint is online.

- **Host name**

  Displays the host name.

- **Public IP Address**

  Displays the public IP address of the Endpoint.

- **Private IP Address**

  Displays the private IP address of the Endpoint.

- **Port**

  Displays the port used for communication. The default port is 8080.

- **Actions**

  Allows the download of the Isolation log.

View and Download Isolation Log

To download the Isolation log of an Endpoint that is online, follow these steps:

1. Click on the Download Isolation Report button.  located in the Actions column.
2. A new option "List of Isolation Logs" will be displayed. 

3. Click on 

to display the list of available logs. The task requesting the list of available logs will be sent to the rThreat software.
4. Click on the log the user want to download. A task will be sent to the rThreat software and a notification will be displayed.

   Logs are named according to the date they were created.

   For more information on the messages displayed on the endpoint in this process see Notifications.
5. A window will be displayed with the information of the Isolation Log.
6. Click on the button 

to download the Isolation Log in .txt format.

Isolation Log

The Isolation Log holds the information of all IP Addresses that have been blocked by the Isolation Process.

The information presented in the Isolation Log is as follows:

- **BLOCK**

  Indicates the blocking action.

- **ip.SrcAddr**

  Indicates the IP address that generates the traffic. This IP corresponds to the Private IP of the Endpoint.

- **ip.DstAddr**

  Indicates the destination IP address of the traffic.

- **tcp/udp.SrcPort**

  Source port used in the communication according to the protocol.

- **tcp/udp.DstPort**

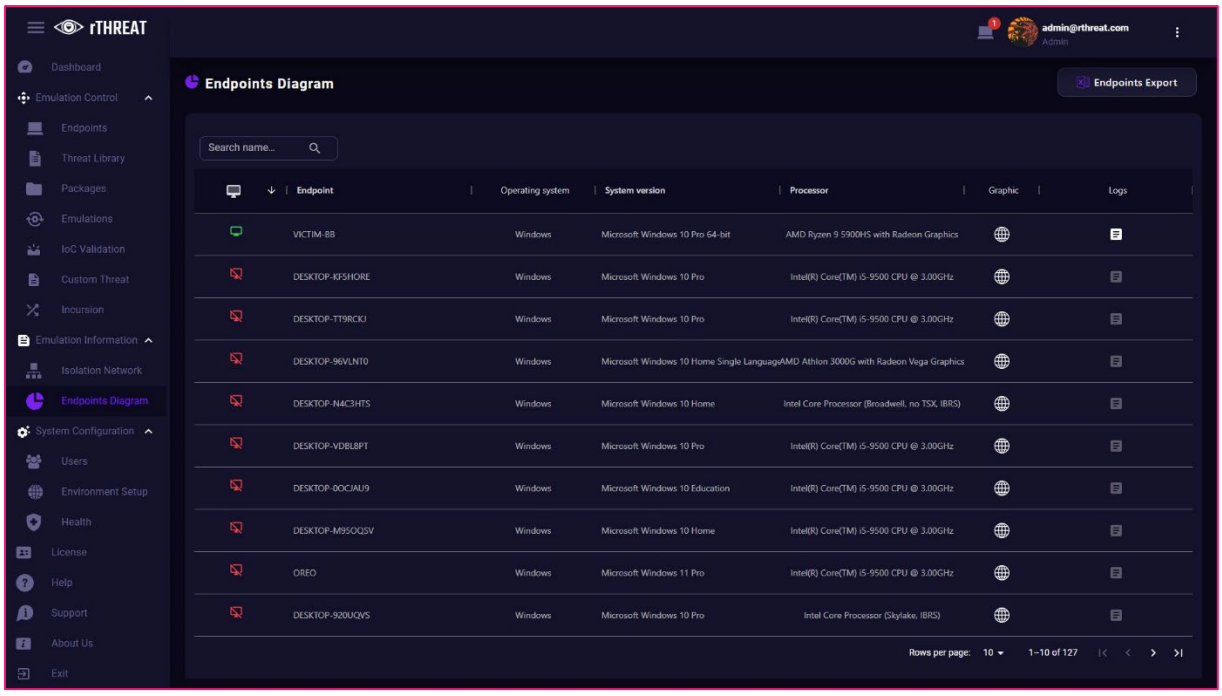
  Destination port used in the communication according to the protocol.

- **tcp.Flags**

  Information on TCP protocol flags.

Endpoints Diagram

The Endpoints Diagram section shows a simpler way of displaying EndPoints information.



In the upper part the Title of the Page: EndPoints Diagram. And the options of "Endpoints Export."

Endpoints Diagram Table

By default, ten rows of information are displayed. If the user want to see more or change the pagination in the lower right corner, there are pagination controls.

It has the information regarding the Hosts that at some times have connected to the Platform where information such as is presented:

- Host name.
- Operating System.
- Operating System Version.
- Processor Information.
- Graph
- Logs

By default, the EndPoints will be displayed in line at the beginning of the table.

By default, ten rows of information are shown. If the user wish to see more or change the pagination in the lower right corner are the pagination controls.

View Diagram of Latest Endpoint Emulations

To view the Endpoint Last Emulations Diagram, follow the steps below:

1. Click on the icon  in the Actions column of the Endpoint the user wish to view the diagram.
2. The Prior 10 Emulations window will be displayed.

Download an Endpoint Logs

To view the Endpoint Last Emulations Diagram, follow the steps below:

1. Go to the Endpoints Diagram Tab.
2. Click on the Downloads Logs button of the endpoint the user want to obtain the logs.
3. Select the logs date the user want to download. If the date is valid the download will start. Otherwise, a warning will appear.

Sort Endpoints Diagram Elements

The Artifact table headers that allow ordering are Host Name, Operating System, System version and Processor.

Each of these columns has quick order options represented by an upward pointing arrow ↑ or downward ↓ . 

To sort the items in a column, follow these steps:

1. Position the cursor on the text in the column header.
2. An upward arrow appears by default ↑.
3. Click on the arrow to sort the items in the column alphabetically (A-Z, smallest-largest).
4. Click on the arrow again to reorder the column items alphabetically (Z-A, highest-lowest), the arrow will change downward. ↓.

EndPoints Diagram Filters

To filter the elements of a column, follow these steps:

1. Position the cursor at the end of the column heading.
2. An icon appears ⋮ of options.
3. Click on the icon to display the advanced sorting and filtering options.

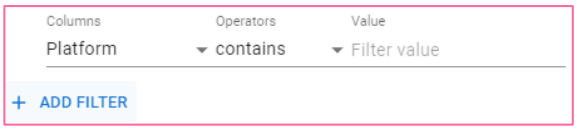
Unsort: That when the user select the user return in the order by defaut of the table: Oldest to newest element.

Sort by ASC: This option sorts the information in ascending order.

Sort by DESC: It sorts the information in descending order.

Filter: This is for filtering information according to more specific needs.

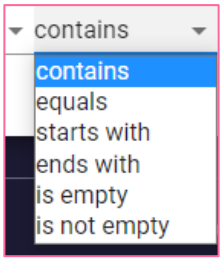
This option displays a new window.



In this menu we find the following options:

Columns**:** Select the column the user want to apply the filtering, in any column the user can use this option..

Operators**:** Indicates content, if it is equal to , if it begins with , if it ends with , if it is empty or not.



Value: The value to be considered in the filter.

+ Add Filter: Allows to add more filtering conditions to the same or other columns.

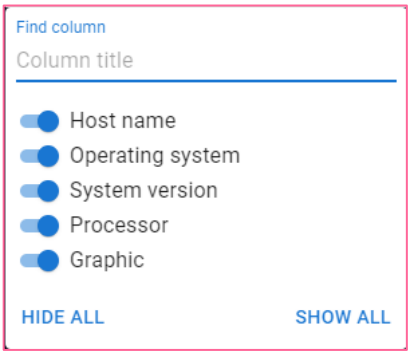
Hide: this choice allows us to suppress or hide the information of the selected column.

Show colums: In this section we can select which columns we want to display in the user table according to our needs to improve the administration of user profiles.

A column search can be performed in the "Find column" section."

To activate or deactivate columns, use the switch next to each column name.

The user can hide or show all columns with the quick options at the bottom of the window (HIDE ALL and SHOW ALL).



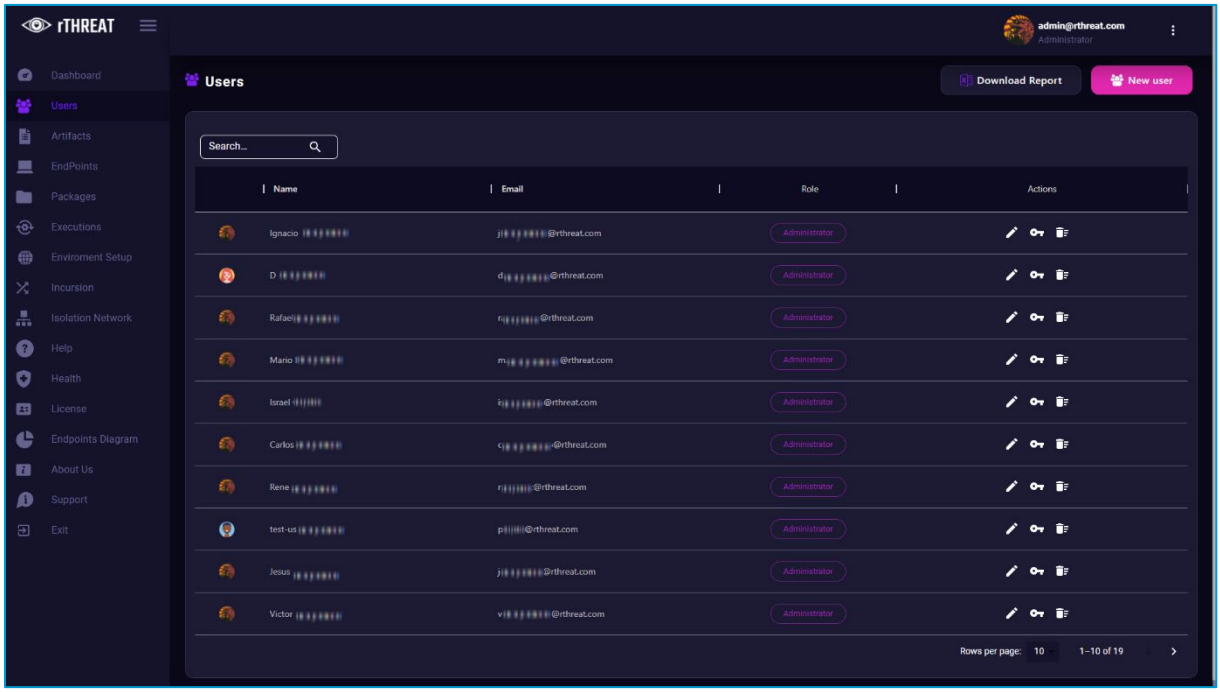
System Configuration

This section groups the tabs that allow the user to get more information related to emulations. Includes Isolation Network and Endpoint Diagrams.

Each of them is described below.

Users

In this section the user can configure the users that can access the Platform.



At the top of the page the title of the page: Users. And the options of “Download Report Excel” and “New User.”

Users Table

Holds the information about the users that are allowed to enter the system. The user can see in a table all the users already configured, where the Username, E-mail, Role, and Actions are displayed.

Here we can have a better administration of user profiles, it allows us to create, manage accounts and assign privileges.

By default, the elements in the table are presented from oldest to newest element.

By default, ten rows of information are displayed. If the user wish to see more or change the pagination in the lower right corner are the pagination controls.

- **Name**

  It is the name assigned to the user when it was registered.

- **Email**

  E-mail address associated with the user when it was registered.

- **Role**

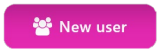
  The role assigned to the user when it was registered. See Types of Accounts.

- **Actions**

  Actions that can be taken for users such as editing information, change password, or removing it.

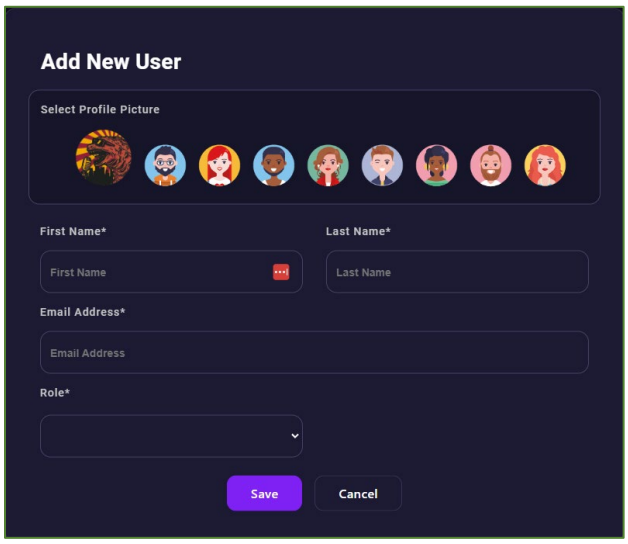
Adding a New User

To add a new user, follow the steps below:

1. Click on the "New User" button. 

   By selecting this option, the user can register a new user profile an provide access to the Platform.

2. A window will appear asking the user to fill in the necessary fields to create a new user.



3. Fill in the new user fields, which include:

- Select Profile Picture: This section presents different image alternatives that can be selected.
- First Name: In this field the user enter the first name of the person to whom the user profile will be assigned.
- Last Name: In this field the user enter the last name of the person to whom the user profile will be assigned.
- E-mail: This section is to register the email address of the person to whom the new profile will belong. Verify that the email is correct as the verification email will be sent to this address.
- Role: In this option for the privileges that the new profile will have can be set to user or with administrator privileges. See Types of Accounts.

4. Click on Save to save or in Cancel to discard the changes.
5. An email will be sent to the email address provided. The user should follow the process of account creation. See Logging in to the Platform for the first time.

Download Report

To download the report in .xlsx format of the users registered in the Platform follow the steps below:

1. Click on the "Download Report" button. Download Report in the upper right part of the window.

   When the user select this option, the user will be asked to specify the path on the computer where the user want to save the report.

2. Click Save to download the report.

This action downloads a file in Excel format with the user table information.

Actions

For already configured users, three actions can be performed.

- **Edit**

  Clicking on this action allows the user to change the selected user's data such as Profile picture, First name, Last name, Email address, Role, and 2FA.

- **Change password**

  Selecting this icon will show a small window to change the user password.

- **Delete an existing user**

  This option allows the user to permanently remove the user account from the Platform.

Edit an Existing User

To edit an existing user in the table, follow the steps below:

1. Click on the Edit icon
2. Modify the required fields.
3. Click on Save to save or in Cancel to discard the changes.

Change Password of an Existing User

To change the password of an existing user in the user table follow the steps below:

1. Click on the Change Password icon
2. Enter the current password, enter the new password, and confirm the new password.
3. Click on Save to save or in Cancel to discard the changes.

Delete an Existing User

To remove an existing user from the user table, follow the steps below:

1. Click on the delete user icon
2. Click on Delete to remove the user or in Cancel to discard the changes.

Types of Accounts

Administrator" user accounts are global to the rThreat Platform and have full privileges in the system, from assigning roles to downloading various malicious artifacts. Users with the "User" role can log in to the rThreat Platform and receive role-based permissions. Under this role, it is possible to perform system operation without making any changes to the system.

If the user are an "administrator" user and cannot access the rThreat Platform or view the required information, please contact the system administrator assigned to the user during the rThreat license purchase. The administrator will be able to assign the appropriate roles to the account.

The following table shows the features an administrator and a user can perform within the Platform:

Feature	Admin	User
Endpoints Tab		
Download Software	Yes	No
Connect Agent via Config file	Yes	Yes
Toggle Isolation	Yes	No
Delete Endpoint	Yes	Yes
View Endpoint History	Yes	Yes
Threat Library Tab		
Upload Artifact	Yes	No
Obtain / Edit related PDF	Yes	No
Download Samples	Yes	No
Delete Samples	Yes	No
Packages Tab		
New Package	Yes	Yes
Delete Package	Yes	Yes
Details of Package	Yes	Yes
Emulations Tab		
Create Emulations	Yes	Yes
Launch Emulations	Yes	Yes
Delete Emulations	Yes	Yes
Download Reports	Yes	Yes
View Records	Yes	Yes
IoC Validation Tab		
Create Validations	Yes	Yes
Launch Validations	Yes	Yes

Delete Validations	Yes	Yes
View Records	Yes	Yes
Access to other tabs		
Custom Threat	Yes	No
Isolation Network	Yes	Yes
Endpoints Diagram	Yes	Yes
Users	Yes	No
Environment Setup	Yes	No
Health	Yes	Yes
License	Yes	Yes
Help	Yes	Yes
Support	Yes	Yes
About Us	Yes	Yes
Exit	Yes	Yes

Users Search

The "Search" option is displayed at the top of the table. 

to search for Users

To search for artifacts, follow the steps below:

1. Enter a sample name or a few characters in the "Search Name" field. In this field the user can enter some indicator data such as the name, alias, or email of the user profile for whom the user are searching.
2. Press the ENTER key to perform the search or allow the table to dynamically filter results.

Sort and Filter of Users

The user table headers that allow sorting and filtering are Name, Email and Role.

Each of these columns has quick order options represented by an upward pointing arrow ↑ or downward ↓ and filtering, which are represented by three dots ⋮. 

To sort the elements in a column, follow the steps below:

1. Position the cursor on the column header text.
2. An upward arrow appears by default ↑.

3. Click on the arrow to sort the items in the column alphabetically (A-Z).
4. Click on the arrow again to reorder the column items alphabetically (Z-A), the arrow will change to downward. ↓.

To filter the elements of a column, follow the steps below:

1. Position the cursor at the end of the column header.
2. An icon appears ⋮ of options.
3. Click on the icon to display the advanced sorting and filtering options.

   Unsort

   When selected the order returns to its default state: Oldest to newest element: Oldest to newest element.

   Sort by ASC

   This option sorts the information in ascending order.

   Sort by DESC

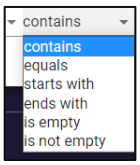
   It sorts the information in descending order.

   Filter:

   This is to filter the information according to more specific needs.This option opens a new window.

In this menu we find the following options:

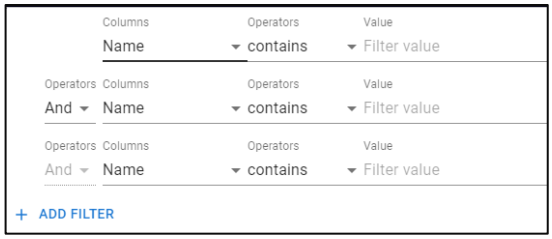
Columns: Select the column the user want to apply the filtering, in any column the user can use this option.



Operators: Indicates content, if it is equal to , if it starts with, ends with, if it is empty or not.

Value: The value to be considered in the filter.

+ Add Filter: Allows the user to add more filtering conditions to the same or other columns.



Hide

This option allows us to suppress or hide the information in the selected column.

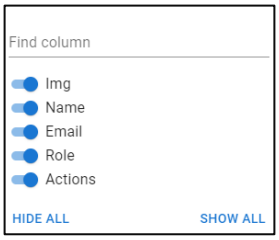
Show colums.

In this section we can select which columns we want to display in the user table according to our needs to improve the administration of user profiles.

A column search can be performed in the "Find column" section.

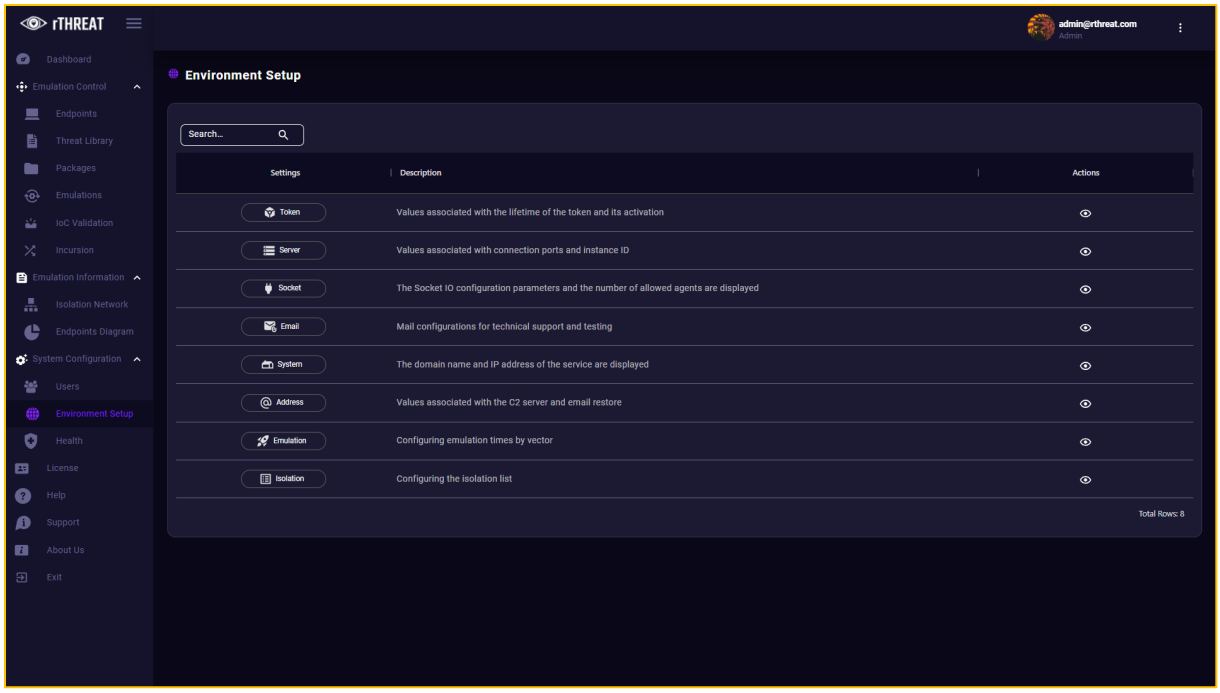
To activate or deactivate columns, use the switch next to the name of each column.

The user can hide or show all columns with the quick options at the bottom of the window (HIDE ALL and SHOW ALL).



Environment Setup

This page allows the user to view details and make changes to the general configuration of the Platform. Most configuration options are set to default values for parameters, which should be maintained in most cases and cannot be changed, although some can be modified to meet the specific requirements of the environment.



Environment Setup Table

The configurable parameters of the Platform are shown in a table. rThreat recommends consulting with the administrator before making a change.

By default, the eight rows of configurable parameters are displayed.

- **Settings**

  Displays the name of the configuration.

- **Description**

  Description of the configuration.

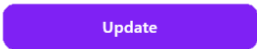
- **Actions**

  Allows the user to view and modify the configuration parameter.

View Details and Make Changes to TOKEN

To make changes to the TOKEN parameter, follow the steps below:

1. Click on the icon in the Actions column corresponding to TOKEN.

2. The Token Parameters window is displayed, make the desired change according to the available fields.
    - Time Until Token Expiration: Expressed in hours.
    - **Active token?** Select "Yes" (default) to enable TOKEN. Select "No" to deactivate it.
3. Click on the button 

to save and update the parameters.

If the user want to cancel, click out of the window.

View SERVER Details

To view details of the SERVER parameter, follow the steps below:

1. Click on the icon of the Actions column corresponding to SERVER.
2. The Settings window is displayed.
    - **Port HTTP**: Displays the configured port through which HTTP communication takes place.
    - **Port HTTPS**: Displays the configured port through which HTTPS communication is performed.
    - **Instance**: Displays the Platform identifier.
3. To exit, click outside the window.

View SOCKET Details

To view details of the SOCKET parameter, follow the steps below:

1. Click on the icon of the Actions column corresponding to SOCKET.
2. The Settings window is displayed.
    - **Max HTTP buffer size**: TCP packet size in bytes.
    - **Origin**: WebSocket address.
    - **Path**: path to the socket io library
    - **Port WS**: WebSocket port.
    - **Port WSS**: Secure WebSocket port.

- **Number of Agents**: EndPoints valid on the subscription.

3. To exit, click outside the window.

View Details and Make Changes in EMAIL

rThreat **DO NOT** recommend making changes to this section, please contact the administrator for more information.

To make changes to the EMAIL parameter, follow these steps:

1. Click on the icon of the Actions column corresponding to EMAIL.
2. The Token Parameters window is displayed, make the desired change according to the available fields.

CONFIGURE

- **Host Domain**: Define the e-mail server to be used.
- **Port**: E-mail server port
- **Active Secure?** Select the "Yes" option to enable secure communication. "No" to deactivate it.
- **From Email**: E-mail address from where the e-mails will be received.
- **Auth User**: Authorized e-mail user.
- **Auth Password**: User Password.

TEST

- **Email Test**: Enter an e-mail address to perform a test mailing.

3. Click on the button Update to save and update the parameters or Send if the user are testing an email.
4. If the user wish to cancel, click outside the window.

View SYSTEM Details

To view details of the SYSTEM parameter, follow the steps below:

1. Click on the icon in the Actions column corresponding to SYSTEM.
2. The Settings window is displayed.

- **Host Name**: Displays the URL assigned to the Platform.
- **IP Address**: Displays the IP Address Assigned to the Platform.

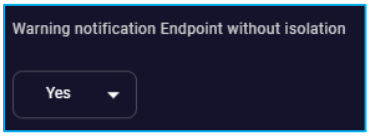
3. To exit, click outside the window.

View Details and Make Changes to EMULATION

To make changes to the emulation's parameter follow these steps:

1. Click the button in the Actions column for EMULATIONS.
2. The Update times of Emulations window is displayed, make the change the user want according to the available fields.
   - **Time of Network Security**: Modify the default time of the Network vector.
   - **Time of EPP**: Modifies the default time of the EPP vector.
   - **Time of Real emulation**: Modifies the default time of the emulation vector.
3. Click the Update button to save and update parameters.
4. If the user want to cancel, click outside the window.

The user can enable an extra layer of protection when launching an emulation, to ensure that isolation is enabled. By default, is on a Yes state, the user can change it by clicking on the drop-down menu and selecting No.



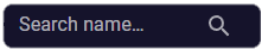
View Details and Make Changes to ISOLATION

To make changes to the ISOLATION parameter follow the steps below:

1. Click on the icon of the Actions column corresponding to ISOLATION.
2. The table of IP Groups is displayed.
3. By default, only one IP Group is listed, with the IP Addresses of rThreat.

There are actions that the user can perform on this section including:

- **Search IP Group**

  The user can search an IP Group by entering the name on the 

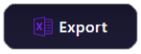
field.

- **Create a new Isolation Group**

  The user can create a new IP isolation group by clicking on the 

button. For more information see Create and apply an IP Group Policy on ISOLATION.

- **Export the IP Groups table**

  The user can export the Table of IP Groups by clicking on the 

button.

- **Sort the IP Groups table**

  To sort the items in a column, follow these steps:

  1. Position the cursor on the text in the column header.
  2. An upward arrow appears by default ↑.
  3. Click on the arrow to sort the items in the column alphabetically (A-Z, smallest-largest).
  4. Click on the arrow again to reorder the column items alphabetically (Z-A, highest-lowest), the arrow will change downward. ↓.

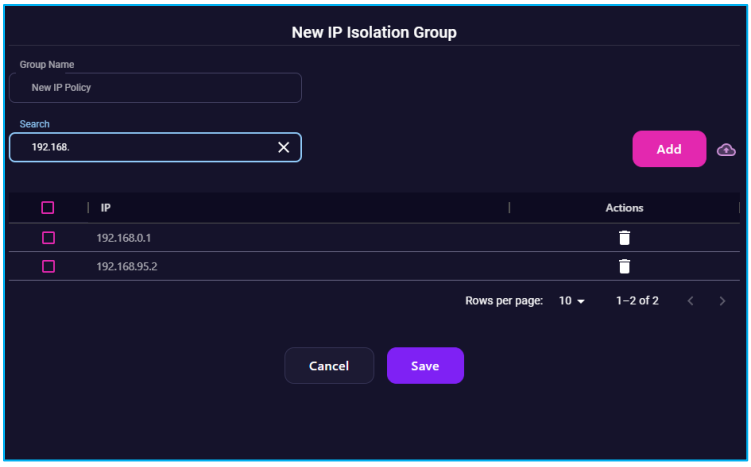
Create and apply an IP Group Policy on ISOLATION

The rThreat Platform allows the creation of IP Group Policies to narrow the IP addresses allowed on individual endpoints.

To Create and IP Group Policy on ISOLATION follow the steps below:

1. Click on the icon  of the Actions column corresponding to ISOLATION.
2. The IP Groups Table is displayed.
3. Click on the 

button located at the top right of the screen. The New IP Isolation Group Section displays.



4. Enter a Name in the Group Name Field (Mandatory)
5. Enter an IP address in the Search Field and click on Add to include the IP Address on the table below.

   To add more Ip addresses to the same policy do not change the Groups Field Name. and click the Add button. Up to 254 IP addresses are allowed per policy.

   The user can add multiple IP addresses using the button located next to the Add button.

   Here the user can load a .txt file with an IP address per each line of the file. While loading the file, the platform perform a validation of the IP Addresses and will load to the table only the IP addresses that are valid.

   Click on the delete button to remove an IP address of the list.
6. Click Save to update the Newly created Policy. Click Cancel to discard all changes.
7. Go to the Endpoints Tab.
8. Select The endpoint the user want to apply the policy an click the on the Actions Column.
9. Click on the Agent Information Section.
10. On the group section, the default policy is selected.

11. Click on the drop-down menu and select the new policy created.

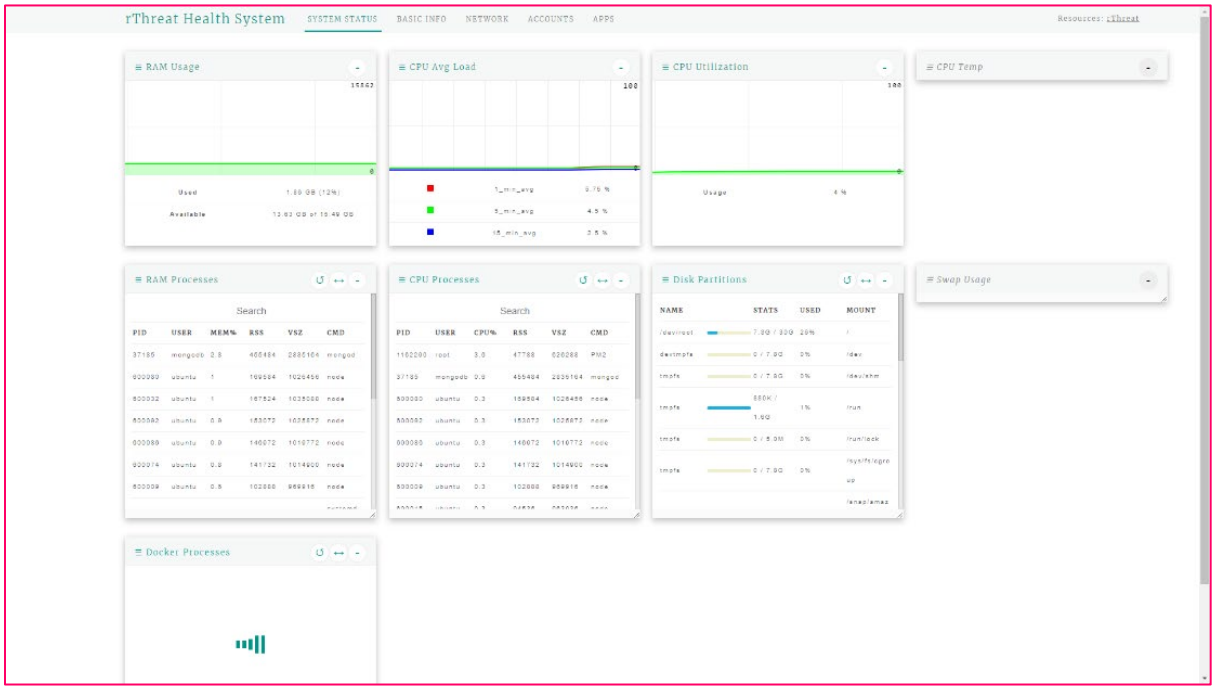
12. Automatically the IP Group Policy is selected, the Insider will receive the instruction; however, we recommend restarting the insider the user can do it from the platform, See Restart an Insider.

The isolation process supports IP addresses and IPv4 Protocol only.

Health

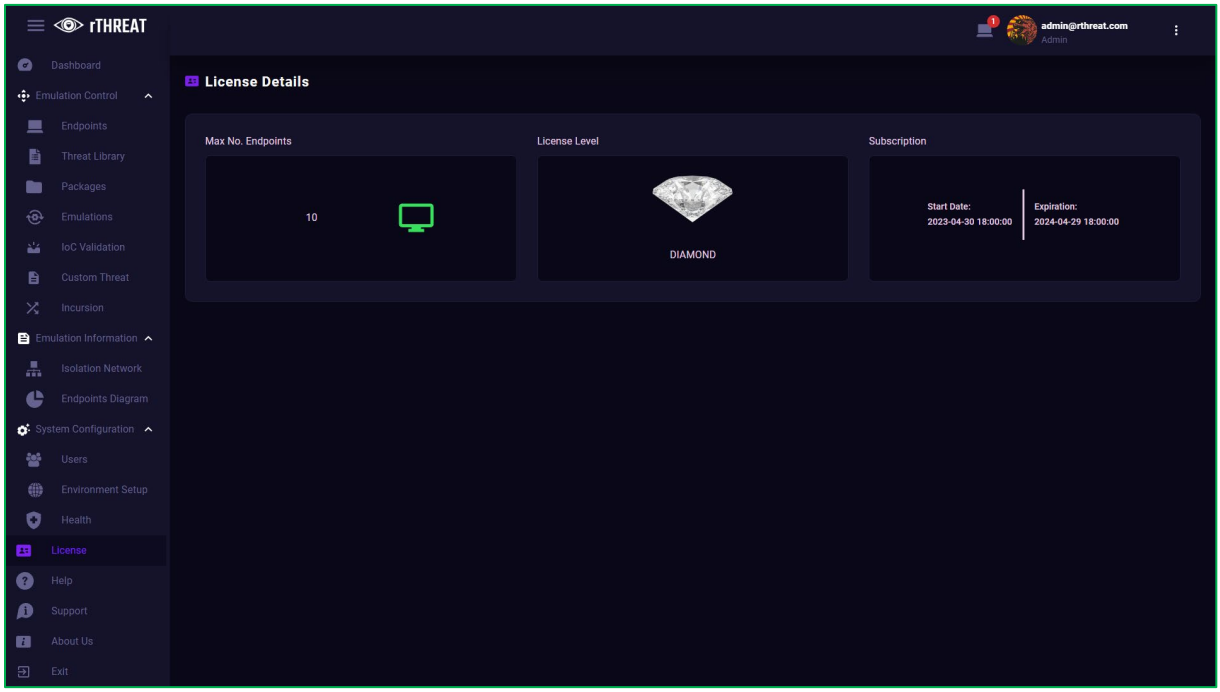
This section graphically shows the monitoring of the resources that the AWS instance is using for the instance.

These metrics are merely informative which are divided into sections such as System Status, Basic Info, Network, Account and Apps.



License

This section displays information about the subscription.



Displays the following details:

- **EndPoints Allowed**

  Specifies the number of EndPoints allowed under the current license.

  This number represents how many EndPoints can receive an emulation concurrently. If an attempt is made to send an emulation to a greater number of EndPoints than shown in this section, at the Endpoint, the rThreat Software will display a Session Rejected message. See Controls.

- **License Installed**

  Indicates the license level of the subscription.

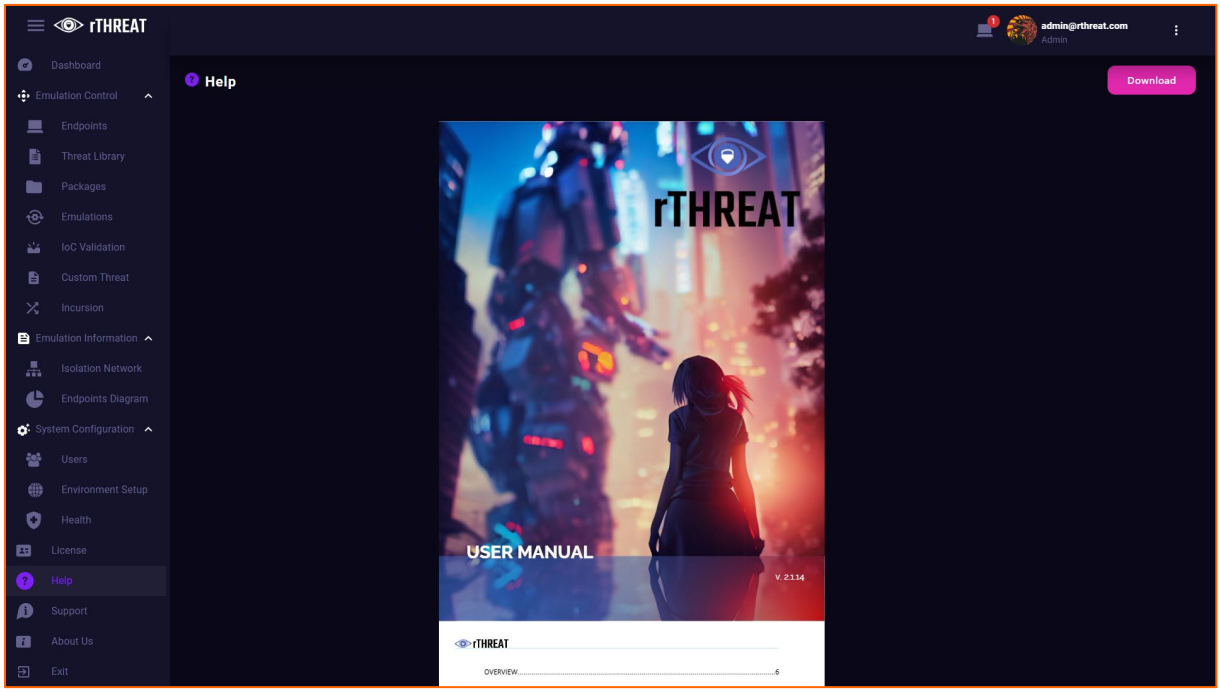
- **License Dates**

  Start Date: Date and time when the subscription started.

  Expiration: Date on which the subscription will expire.

Help

This section shows this document.



Download User Manual

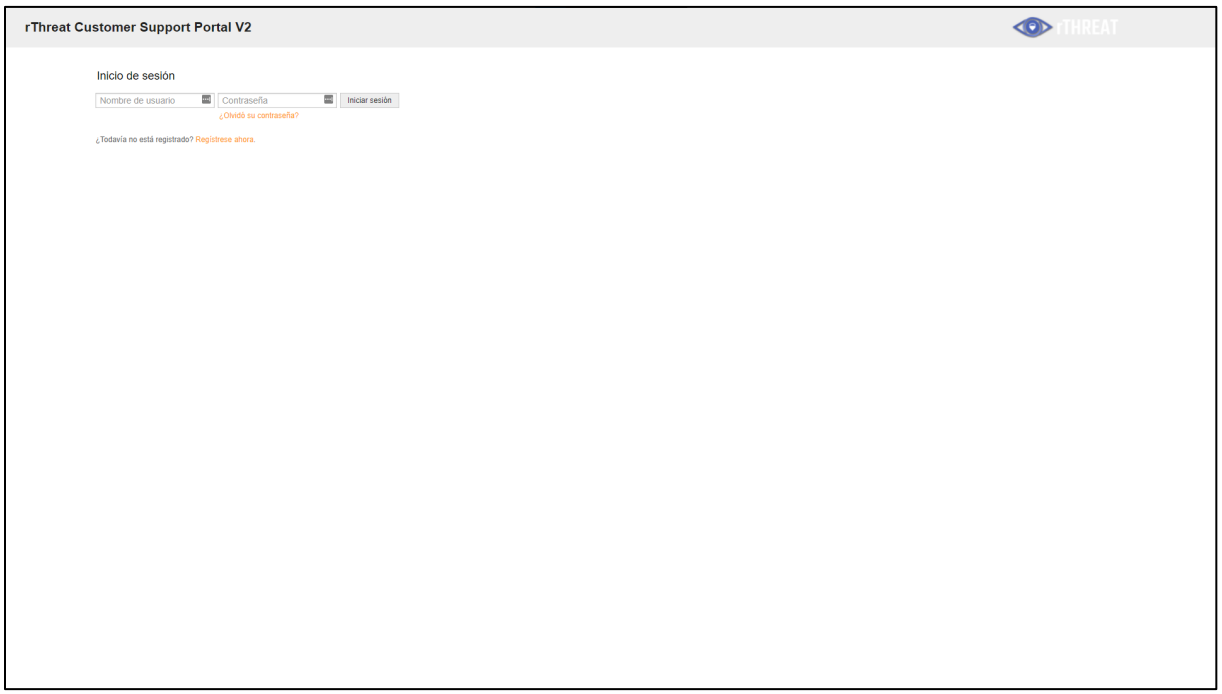
To download the User's Manual in PDF format, follow the steps below:

1. On the Help Tab, click on the "Download" button. 

2. Specify the path on the local host where the user want to save the report.
3. Click Save to download the User Manual.

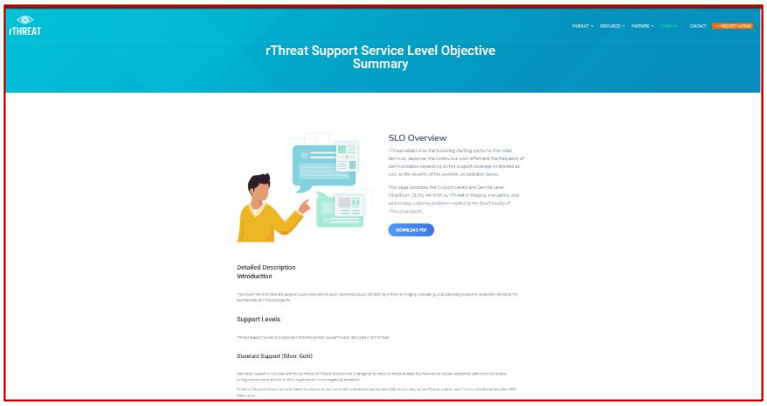
Support

This section redirects to the rThreat Customer Support Portal.



For more information contact the administrator.

rThreat Support Service Level Objective Summary



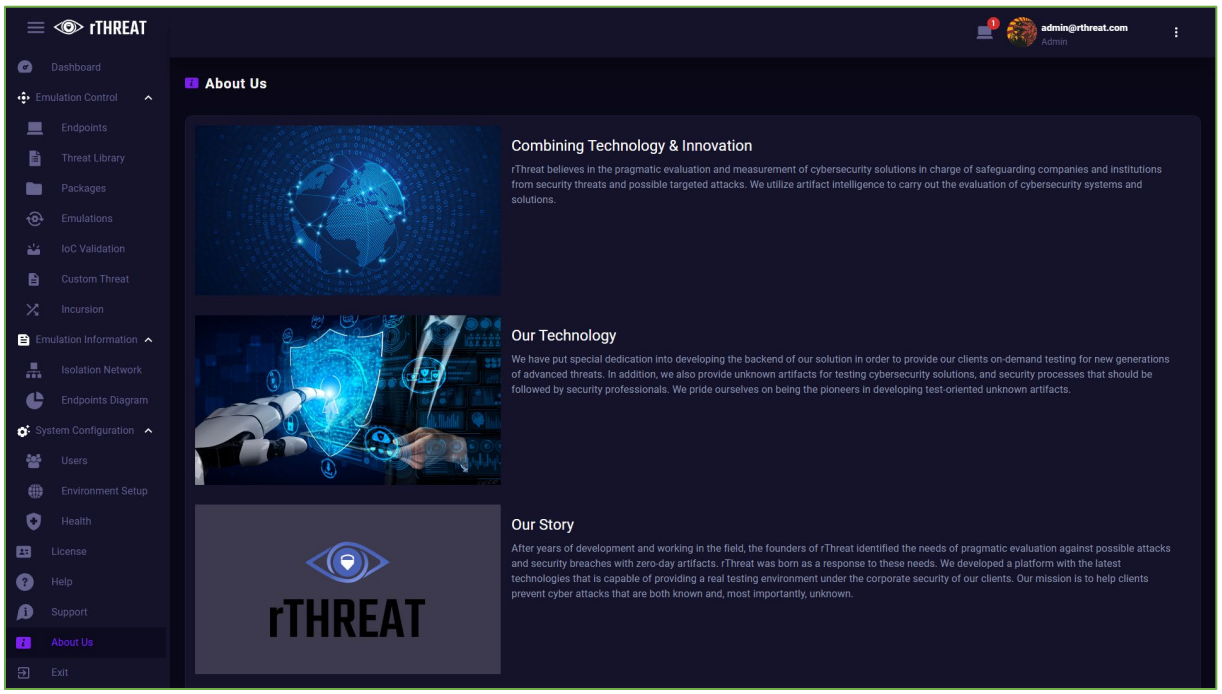
¿ Do the user have a problem with the Platform, rThreat Software or artifacts.?

For instructions on how to open a ticket with rThreat's support teams, please go to: https://rthreat.net/slo/

This page describes the support levels and service level objectives (SLOs) established by rThreat to classify, evaluate, and address customer issues related to the functionality of rThreat products.

About Us

This section allows the user to visualize information about rThreat in a summarized form and the most important points that as a company it is important to show to our customers.



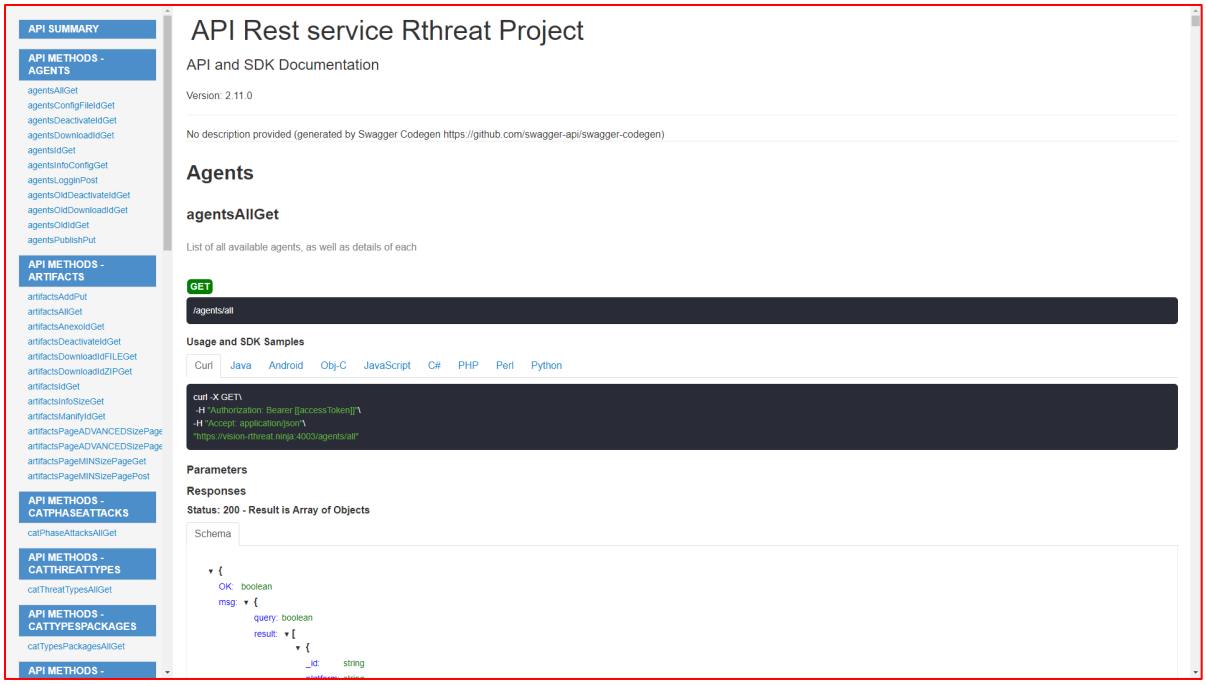
Exit

This section allows the user to log out and returns the user to the login window.

It is also possible to log out from the top bar options present in all windows in the upper right corner. See Dashboard.

API

This The rThreat Platform includes the API Rest service. The user can access it by adding ":4003/doc/api/ " to the url of the instance. (e.g., rthreat.instance.ninja:4003/doc/api/).



All methods are listed, with the description, the parameters, and responses.

To use the API a token is required. The user can obtain a token utilizing the **usersLogginPost** method. Use the user email and the password on this method and the response will be information related to the user and the token. Use this token to perform operations with other methods listed in the API REST service page.