ANLYZ®

SOAR - SPORACT

USER GUIDE

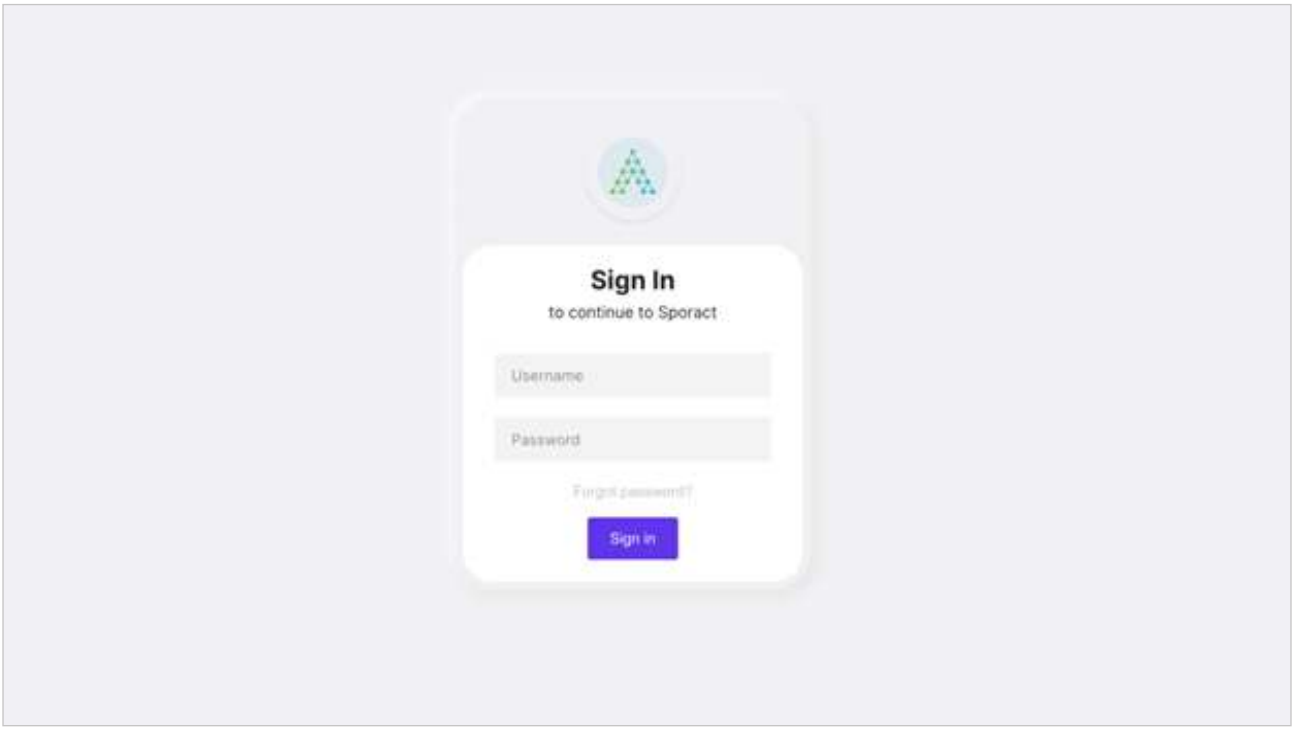
INDEX

GETTING STARTED WITH SPORACT

Sporact is a holistic SOAR platform for case management, incident response, orchestration and automation. This guide will help users to understand Sporact and its functionalities better. Sporact has various components or modules namely: Dashboard, Cases, TrendMicro Search, Reports, Playbooks, Customer Discovery and Settings. In the upcoming sections, each of these components and their respective functionalities are explained, which will be helpful for users or the SOC teams. Kindly note that all these actions like creating dashboards, charts, reports, playbooks, etc. are permissions based. If a user has permissions, then they can perform these actions.

Logging in

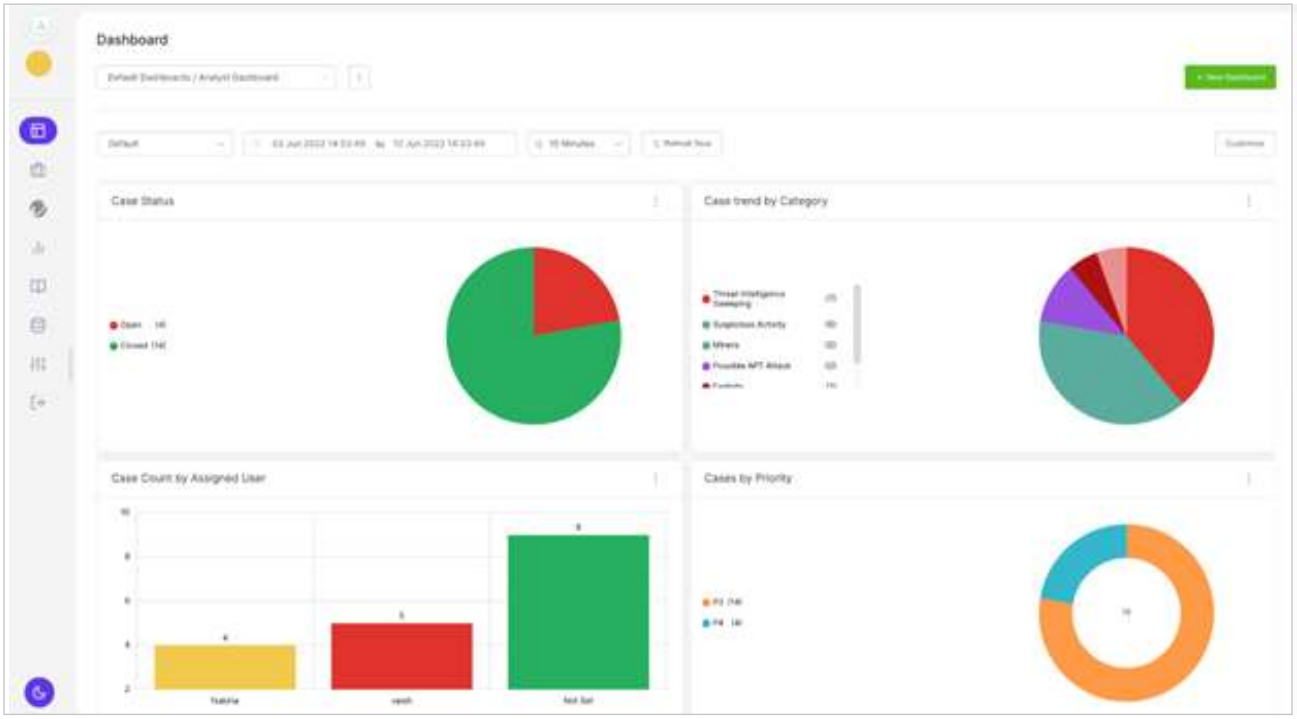
A user can log in to Sporact with their credentials.



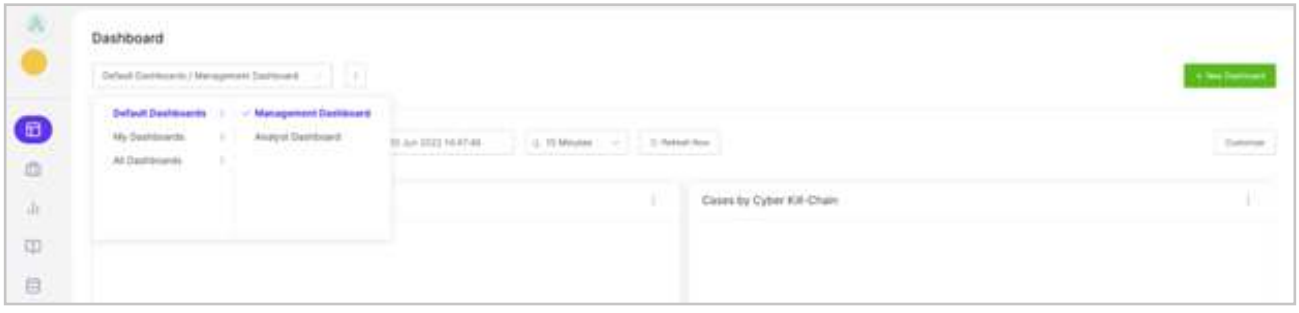
Once the user logs in, they can see the Case listing page. All the alerts that are forwarded to Sporact comes in as cases or tickets, which can be seen in this page.

DASHBOARD

The dashboard provides an intelligent and holistic view of threats and resources of security operations. The analyst and management can have an overview of all the events happening.

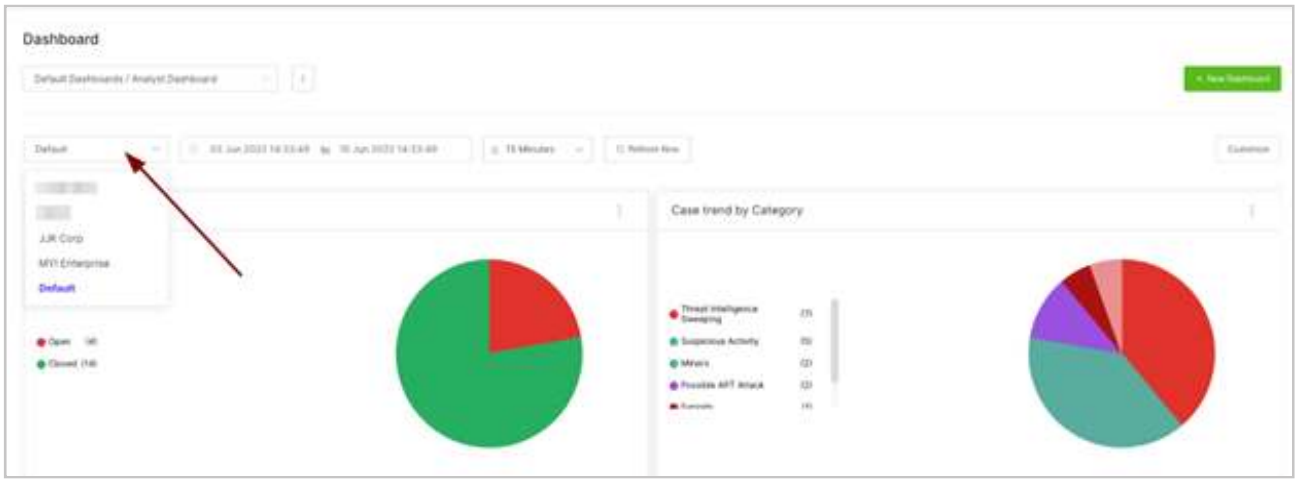


An analyst can create their own dashboards, and customize them based on the data or information they need to see. By default, we have two dashboards: analyst and management dashboard.

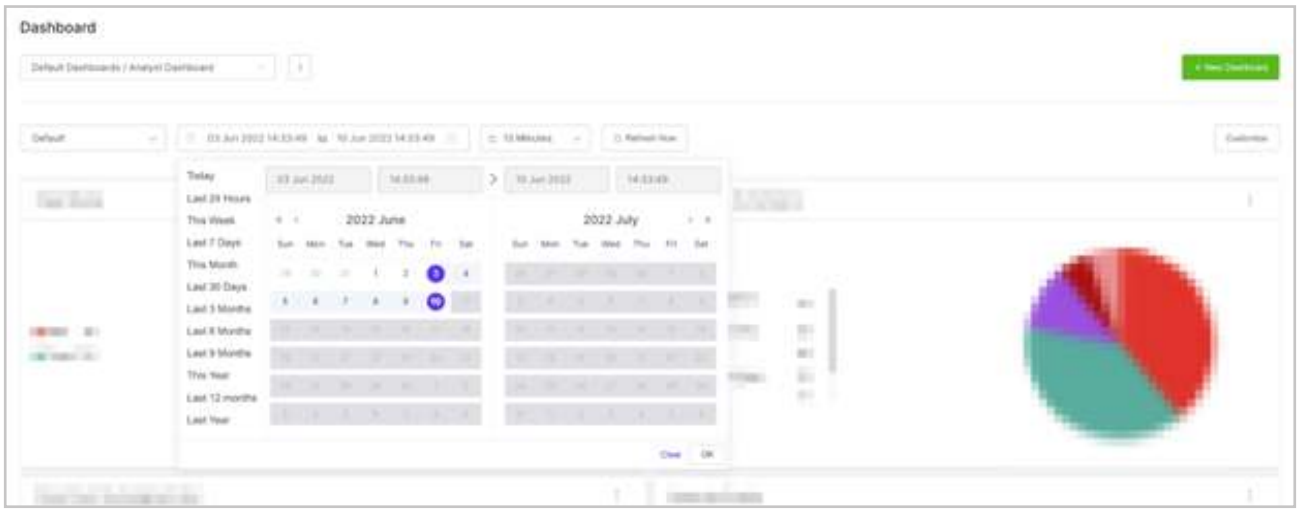


Under My Dashboards, you can see the dashboards that are created by you. All Dashboards gives a list of all available dashboards in Sporact.

An analyst can view the dashboard for other tenants by clicking on the tenant selector and select a tenant from the list.

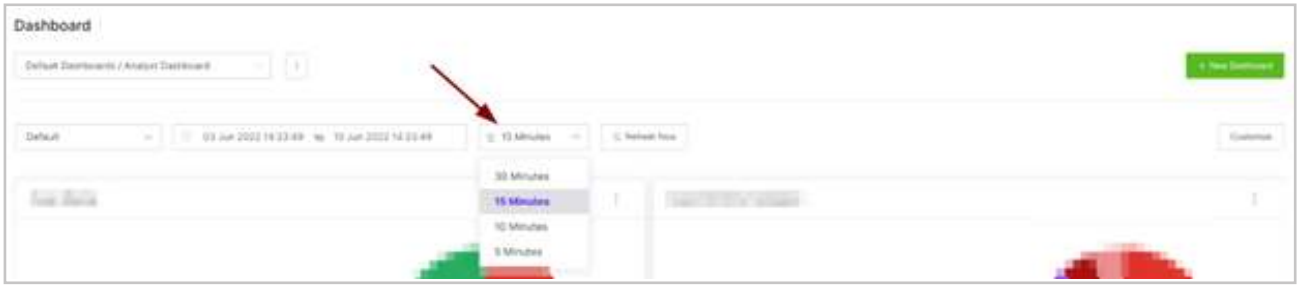


Generally, the dashboard shows data from the last 7 days. An analyst can also select different date and time options to view the dashboards.



The dashboard can be refreshed instantly by clicking on the Refresh Now button.

By default, the dashboard gets refreshed every 15 mins. We have the option to select different time duration as well.

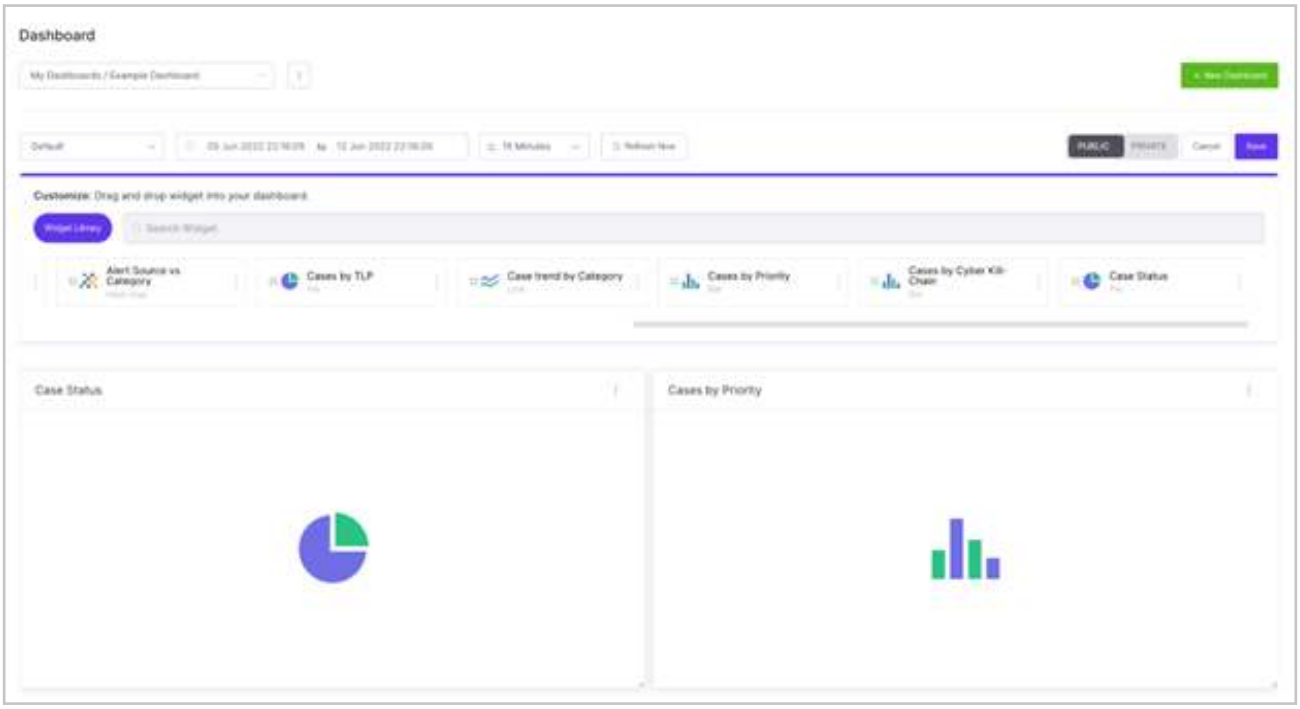


If an analyst wants more charts to be added to the dashboard, they can do so by clicking on Customize.

Create dashboard

A new dashboard can be created by clicking on New Dashboard. The user can provide a title for the dashboard and click on Confirm to save it.

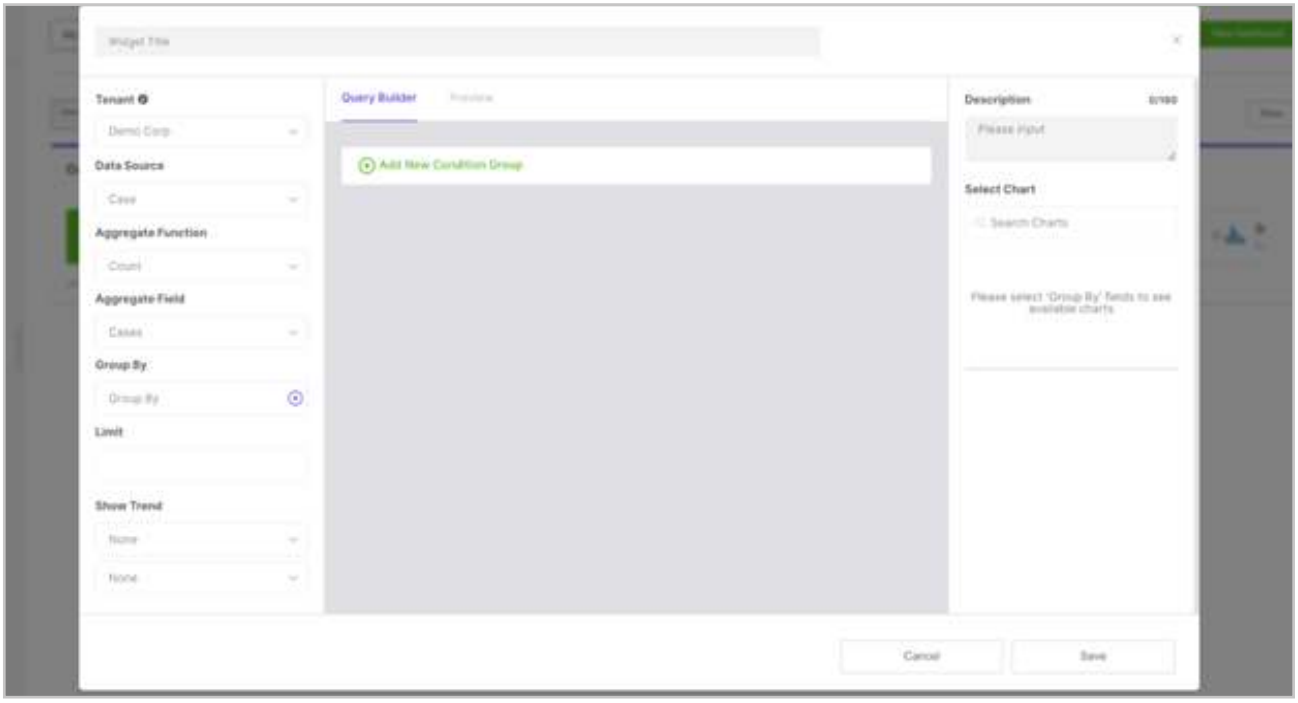
Once the dashboard is created, it can be customized by clicking on Customize. There are various charts or widgets available, which can be dragged and dropped to curate the dashboard.



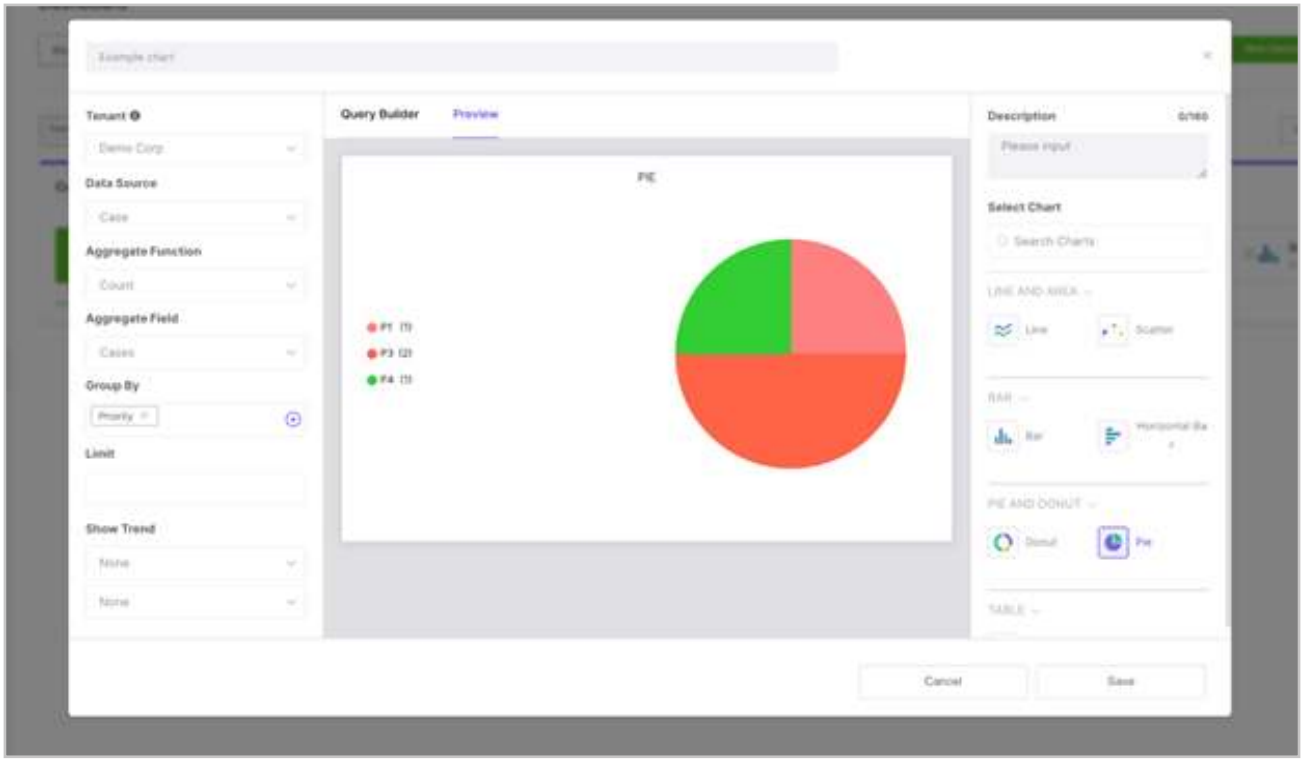
Once the required widgets are selected, the user can click on Save. A dashboard can be made Private if required. A private dashboard can only be visible to the user who created it.

Create Custom Widgets

The user can create customized charts by clicking on Custom Widget. The custom widget library provides a set of fields and a query builder that can be used to create the custom charts or widgets. The custom widget library is common for both Dashboards and Reports. Click on Save to save the chart.



An example chart can be created as shown below.

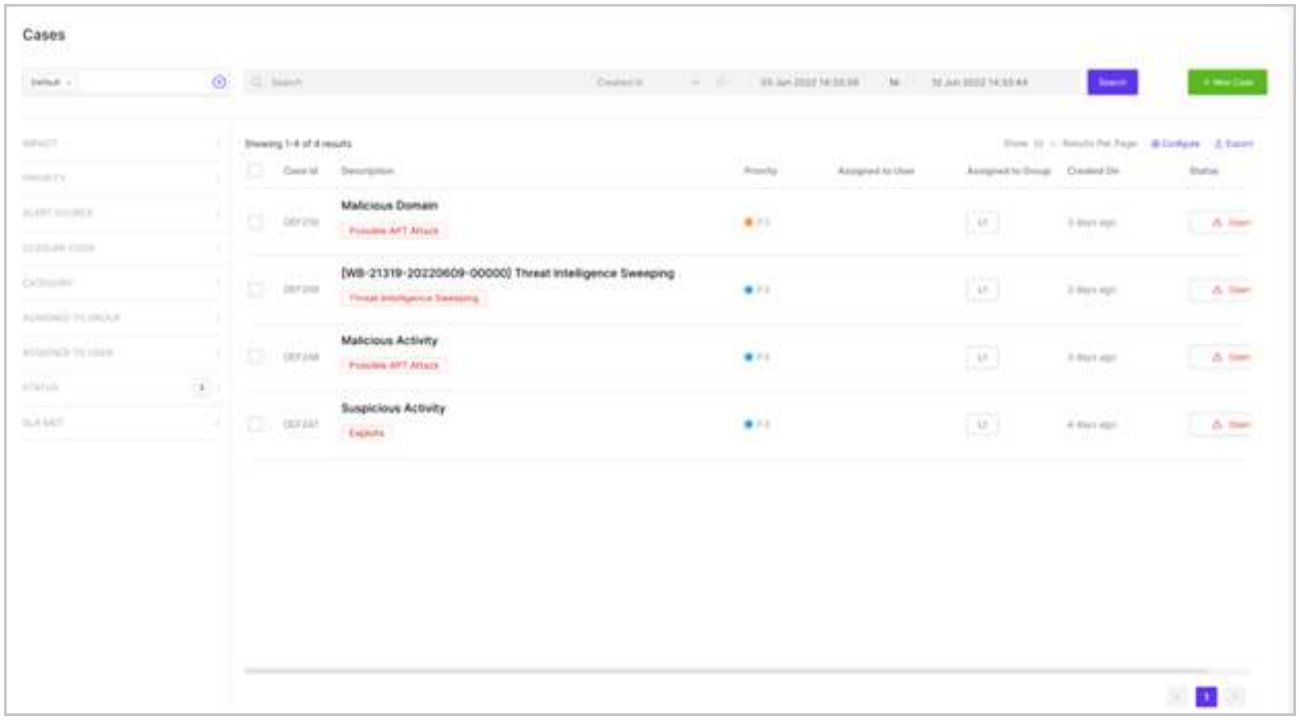


Edit dashboard title and Delete dashboard

The user can edit a dashboard title by clicking on Edit dashboard title, and delete a dashboard by clicking on Delete.

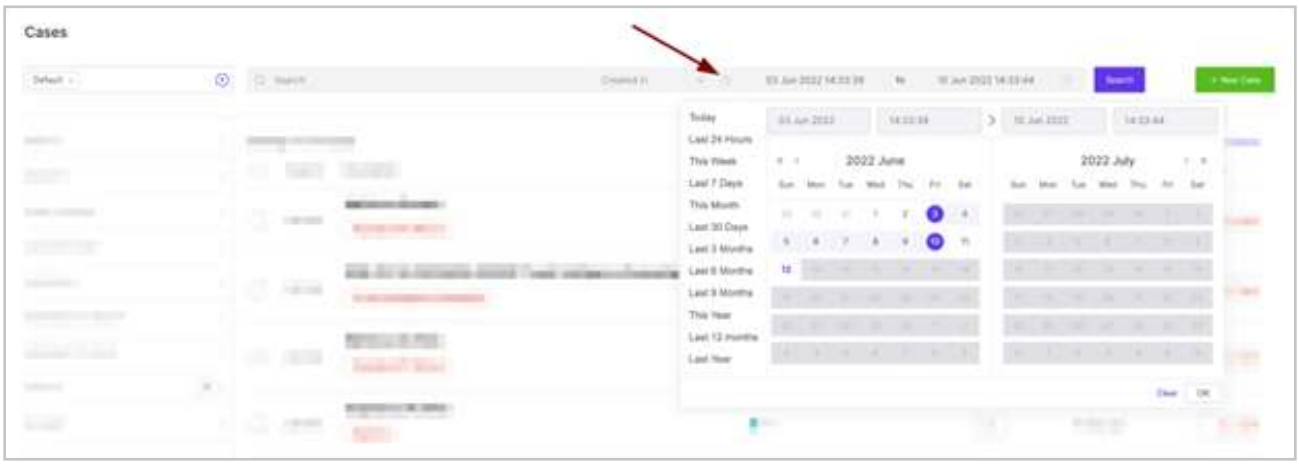
CASES

This page is where case management and incident response takes place. All the alerts forwarded to Sporact can be seen here, as cases.



Search for a case

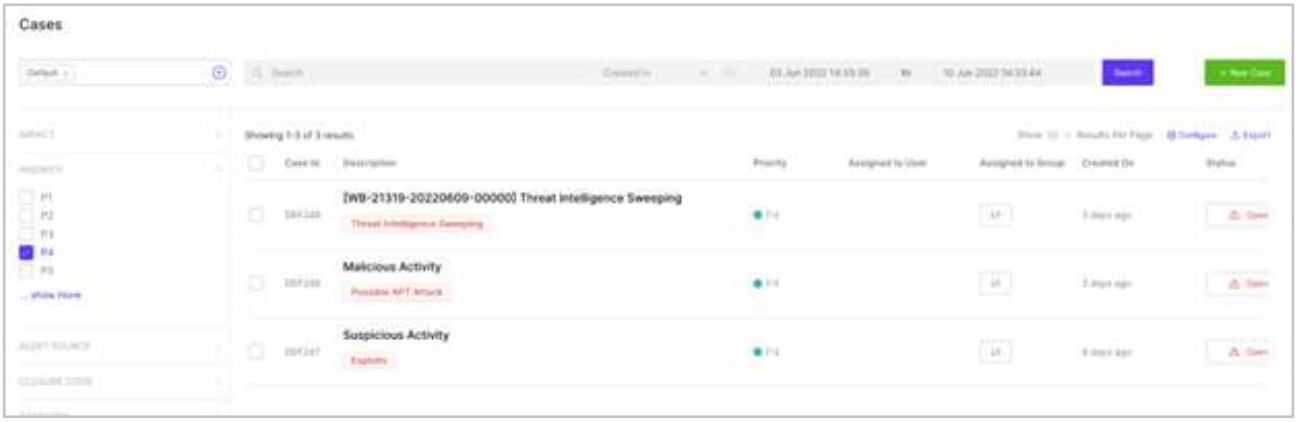
Generally, the cases from the last 7 days can be seen. The user can also search for cases based on different dates and other options available as seen below. The cases can also be searched or filtered based on the dates they were created on or updated in.



The user can search for cases using case id or case title.

Filter a case

The user can use quick filters to filter cases. For example, cases can be filtered based on priority, impact etc.



Configure and export a case

The user can click on Configure to see extra fields apart from the default fields.

The user can search for cases using case id or case title.Filter a case

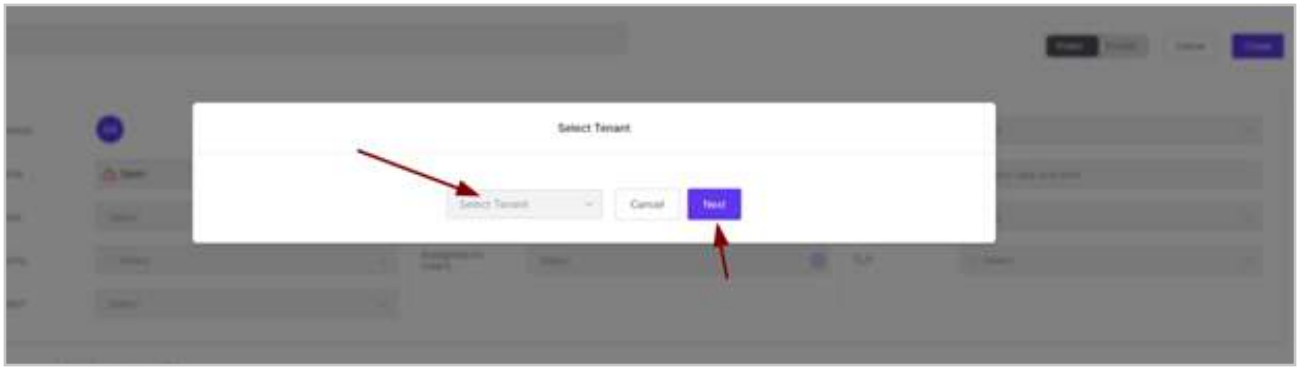
The cases can be exported by clicking on Export and selecting the format (CSV and XLSX).

Create a new case

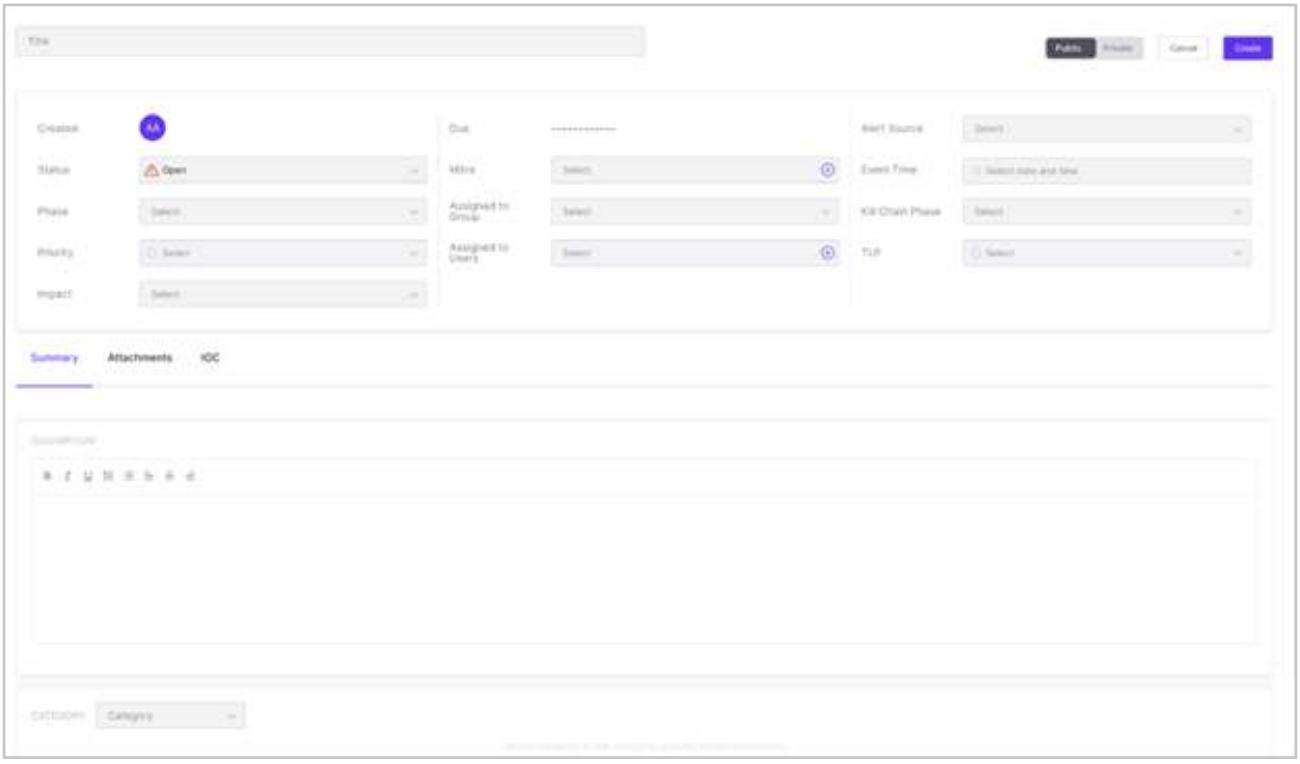
A user can create a new case by clicking on New Case.

The user can search for cases using case id or case title.Filter a case

Select a tenant and click on Next.



The user can provide a title depending on the case. The cases can be made public or private. A case can be made Private when a confidential analysis has to be done and information can be shared on a need to know basis. A private case is visible only to the creator of the case and the user to whom the case is assigned to.



The Status of the case can be open, closed, in-progress, waiting and stalled. A newly created case is always in an open state. Once a user starts working on the case, the status of the case is changed to in-progress. For a case that is waiting for further instructions, or some updates from a superior, or anything similar as such, the case can be assigned the waiting status. Once a case is in waiting state, the SLA stops until the status of the case isn't changed to any other state. A case goes into a stalled status when it's not being worked on for a specified period of time. For instance, if the specified time is 3 days, then a case that doesn't have anyone working on it for 3 days gets its status changed to stalled.

The phase is related to the Incidence Response Framework. The user can select on what phase of the IR is the case currently at.

The priority of the case can be assigned, based on which, the impact also gets assigned. Based on the priority and the SLA assigned to the said priority, the due date of the case gets assigned once the case is saved. The user can tag the cases with attack tactics and techniques by clicking on Mitre.

The user can assign the case to groups and then, the users under those groups. The user can click on alert source to select the source of the alert or threat. The event time is selected to provide the time of the event occurring.

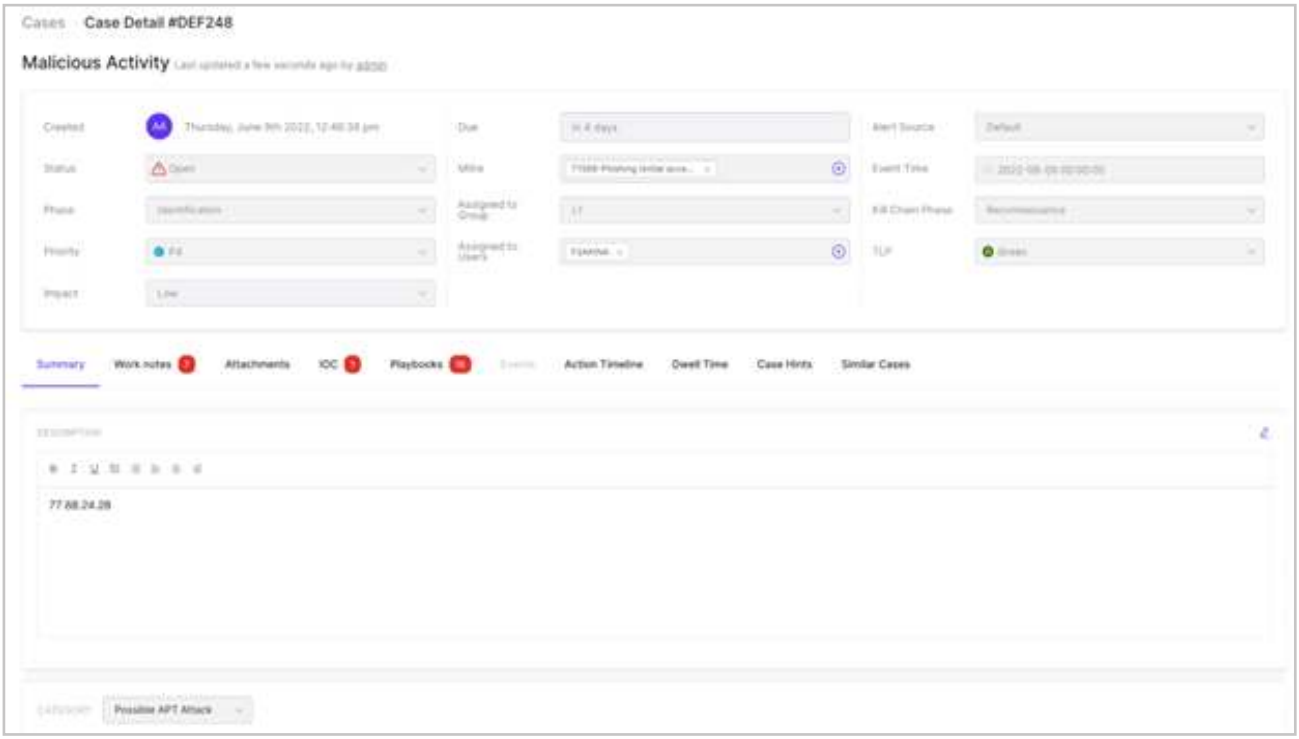
The user can select the Kill Chain Phase to identify what phase of attack or invasion the specific case is in. The user can also decide what data to be shared and between whom by clicking on TLP.

The summary of the case is the description of the case and can be drafted by the user. The user can also attach or upload attachments related to the case.

IOCs or Indicator of Compromises can be added if available. The IOCs also gets detected from the summary description.

Categories can be selected to decide what the case type is. There are custom category fields that are specific to the categories and can be updated with, if the specific information is available.

Once all the required fields are filled, click on Create. Once the case gets created, the summary view of the case can be seen.

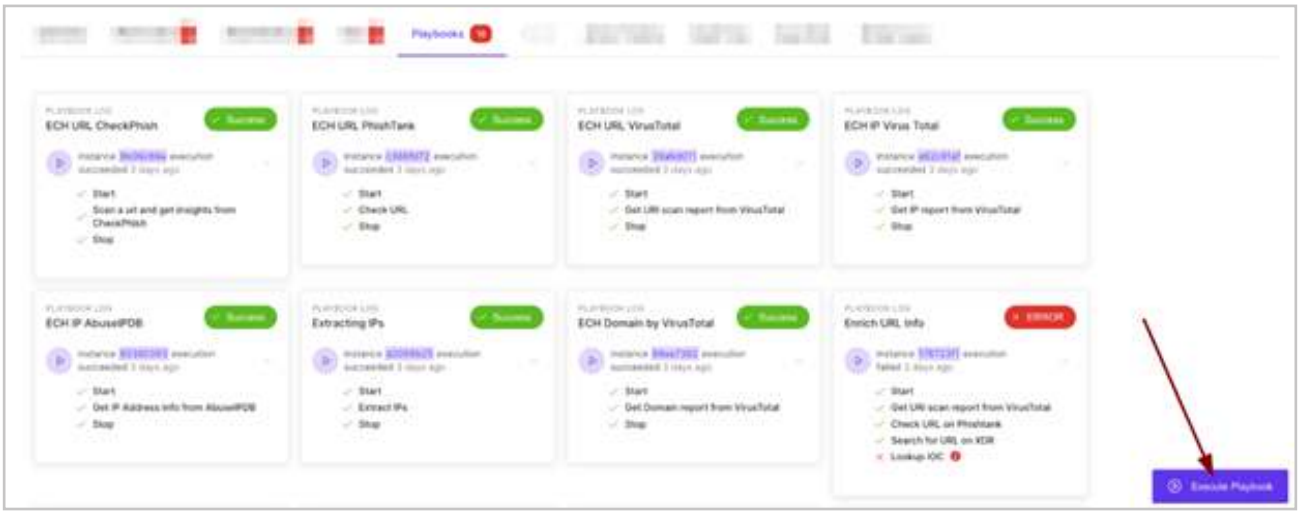


The Summary can be edited by clicking on the edit icon, if needed. Work notes can be added by clicking on Add. Work notes are meant for information sharing, collaboration and case enrichment. The results of various playbooks executed can be seen under Work notes as well.

The user can click on Attachments to view if any attachments are uploaded. If needed, additional attachments can be uploaded as well. A user can search and upload an attachment. Attachments can also be deleted and downloaded.

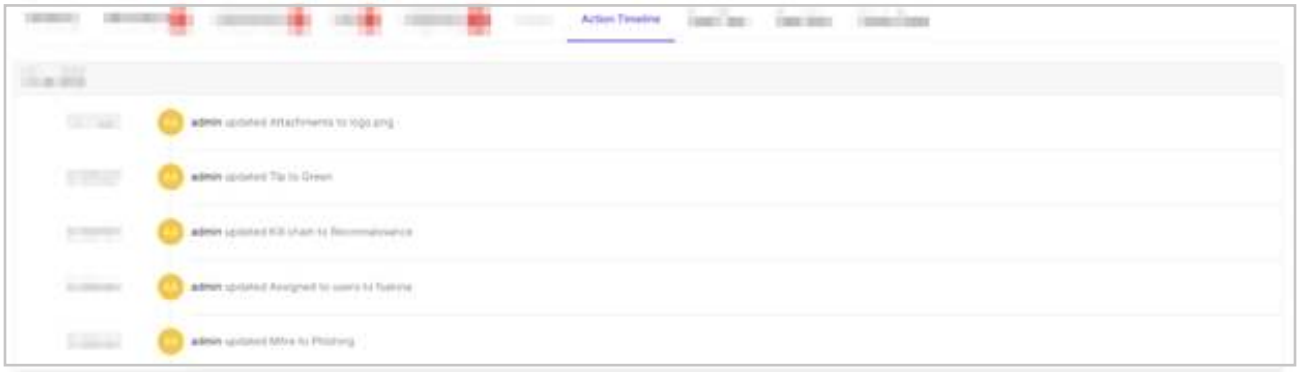
The user can also get details about the IOCs. IOCs can be edited and deleted. A user can also search for an IOC and add a new one.

Under Playbooks, the user can see details about the playbooks executed. The user can see which all playbooks were executed successfully and which weren't.

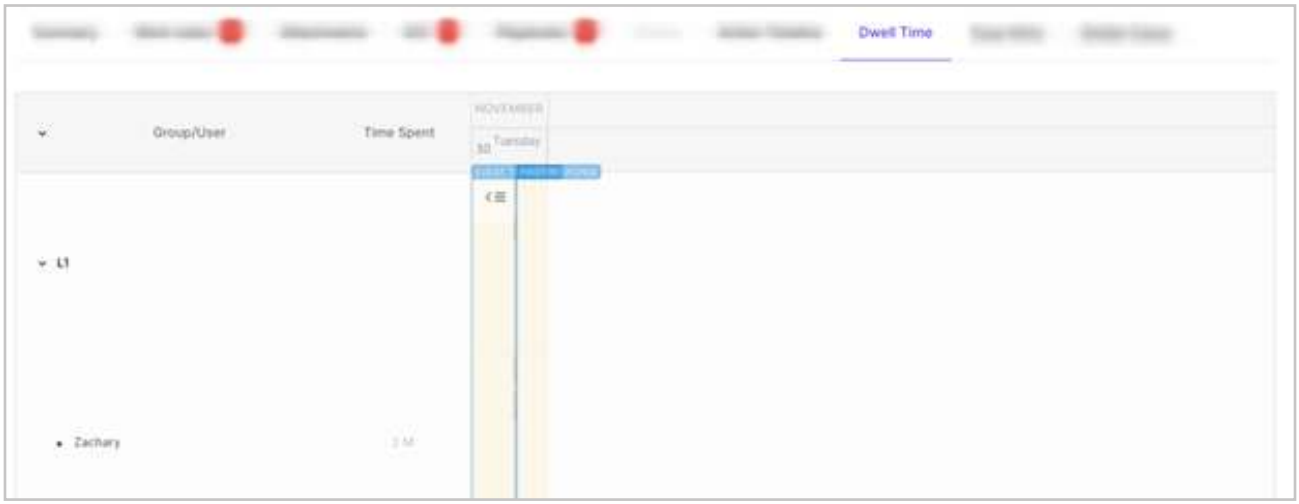


Playbooks can also be executed manually by clicking on Execute Playbook. Select the playbook and click on Confirm.

The Action Timeline gives the logs of all the actions that were performed with respect to the case.



The user can also check the Dwell Time which gives the amount of time a user spends on a particular case.



Case Hints give information about artifacts or indicators that are common to other cases and also information about the concerned cases.

Similar Cases provides the user with details about a case which is similar to the current case.

Close a case

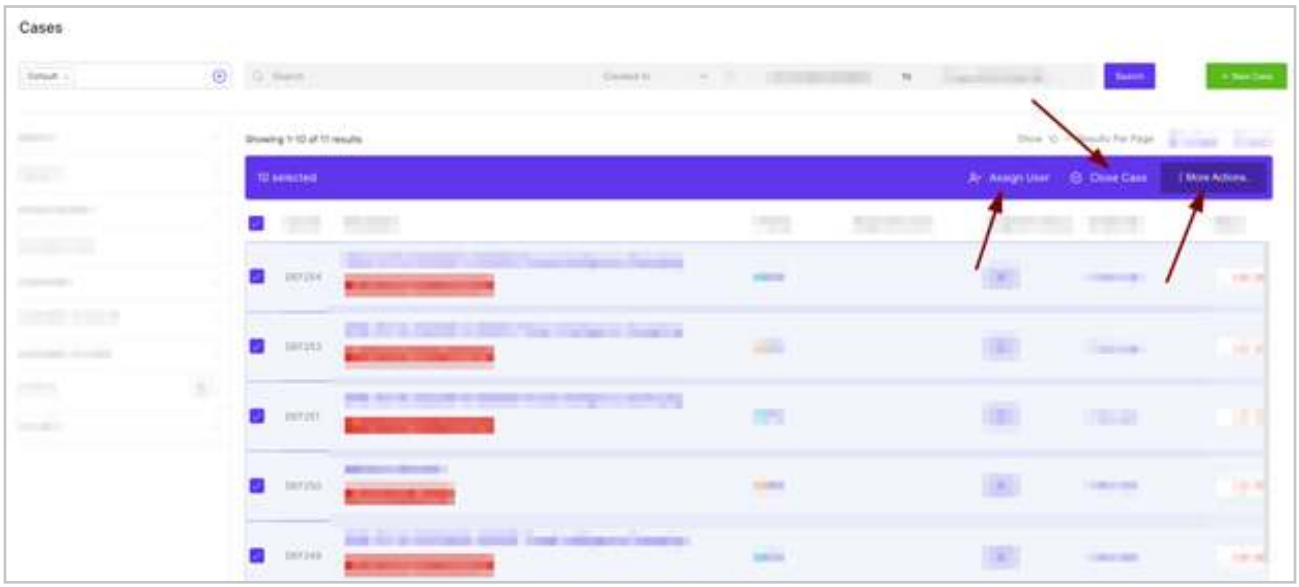
When the status of a case is assigned Closed, the user has to select a closure code and provide the appropriate details in the work notes.

When a case is closed, the status of SLA gets updated.

If the SLA is not met, it gets updated as shown below.

Bulk actions

Bulk actions can be performed on multiple cases at the same time. For example, if multiple cases have to be assigned the same user, bulk actions can be used by selecting the cases and clicking on Assign User. Similarly multiple cases can be closed as well. The user can click on More Actions to see a list of actions available and select the one required.

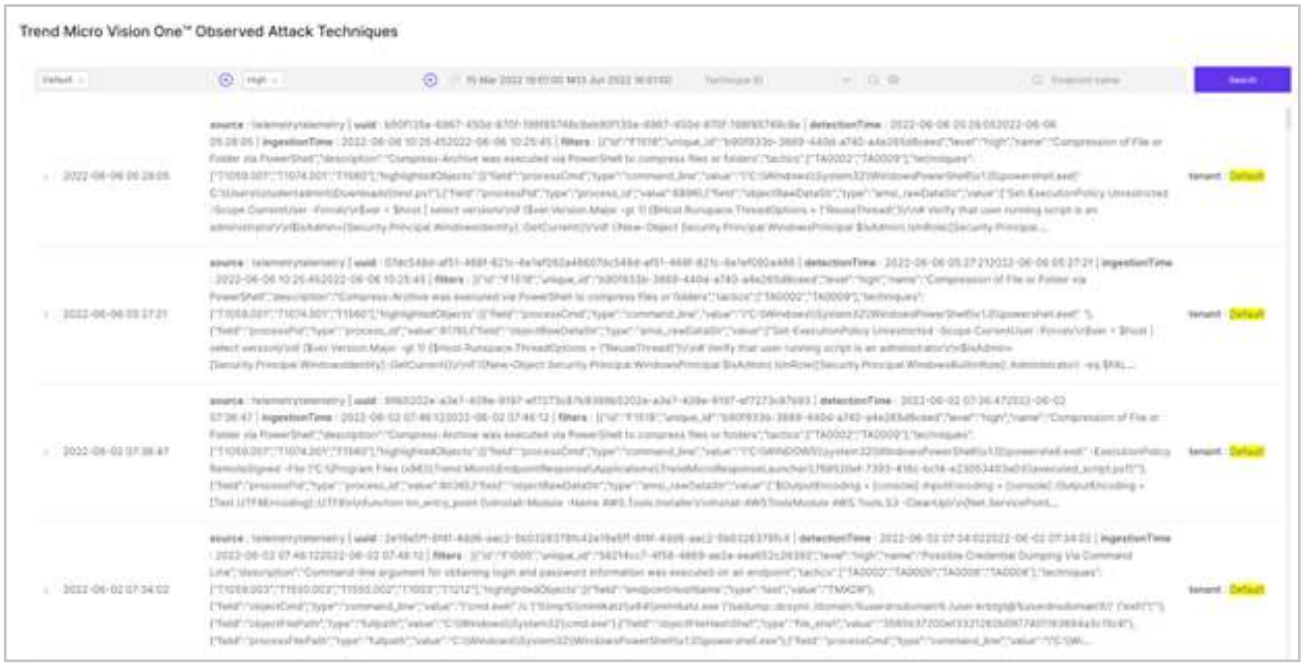


TRENDMICRO SEARCH

The TrendMicro Vision One searches for Observed Attack Techniques, Intelligence Reports and General Search can be done using this feature from Sporact itself, instead of logging in to Vision One console.

Observed Attack Techniques

The Observed Attack Techniques app displays the individual events detected in your environment that may trigger an alert and any related MITRE information. The user does not have to log in to Vision One for different tenants, they can select the tenant here and search for the OATs.



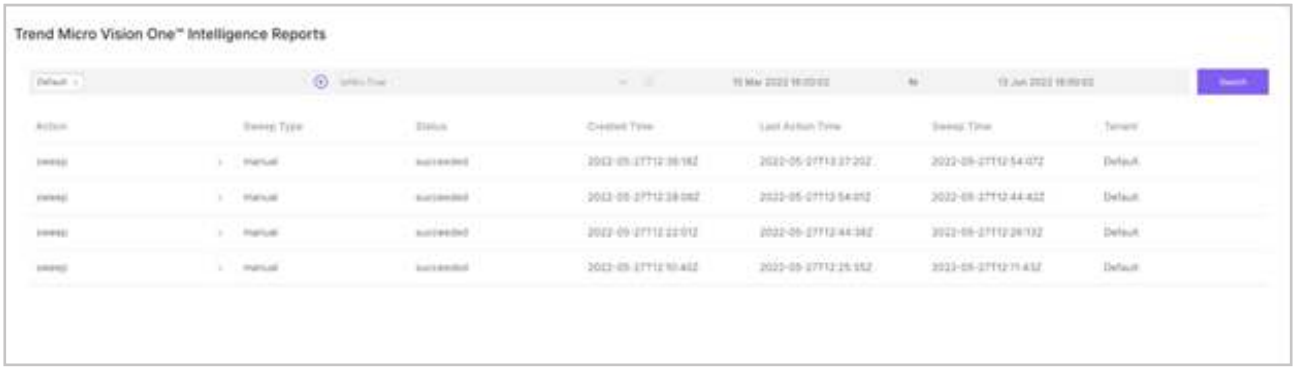
Search

This search is the equivalent of the General Search in Vision One.

Intelligence Reports

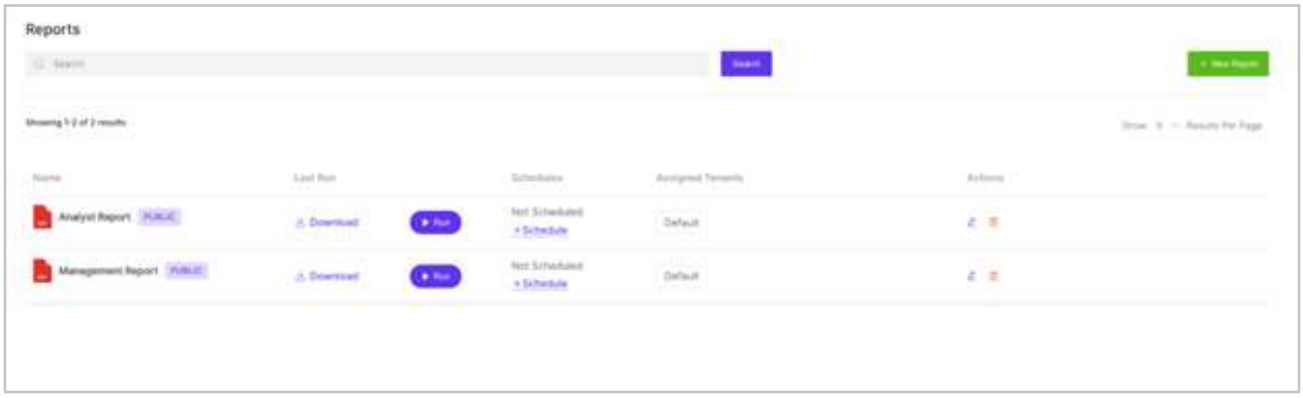
The Intelligence Reports app allows you to leverage valuable indicators of potential threats from both curated intelligence reports and your custom intelligence reports. Trend Micro Vision One supports auto and manual sweeping based on curated and custom intelligence to search your environment for indicators of compromise. If there are indicator matches, you can check the sweeping results for further investigation and analysis.


Trend Micro Vision One™ Intelligence Reports


Trend Micro Vision One™ Intelligence Reports

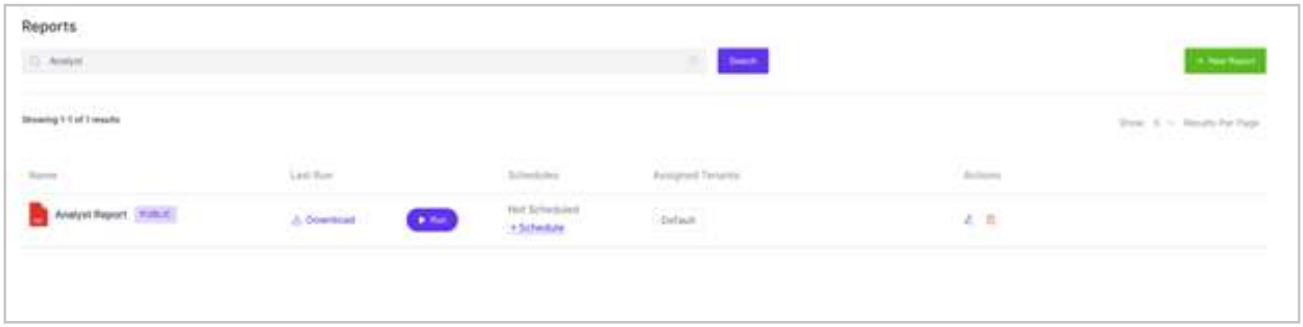
REPORTS

Reports help with running reports and scheduling the reporting.



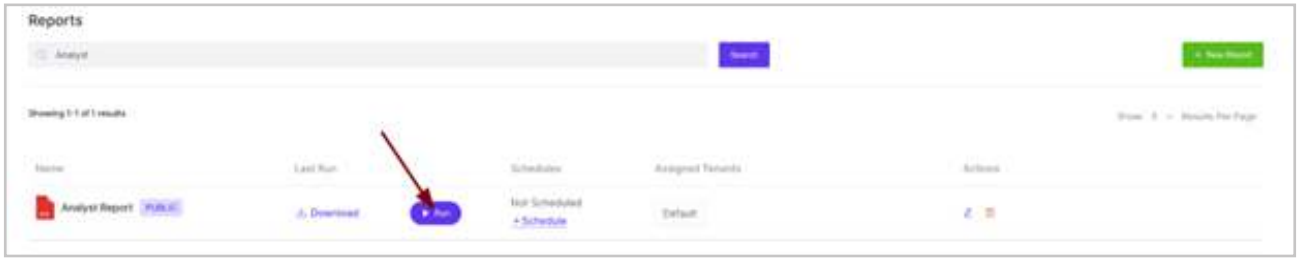
Search a report

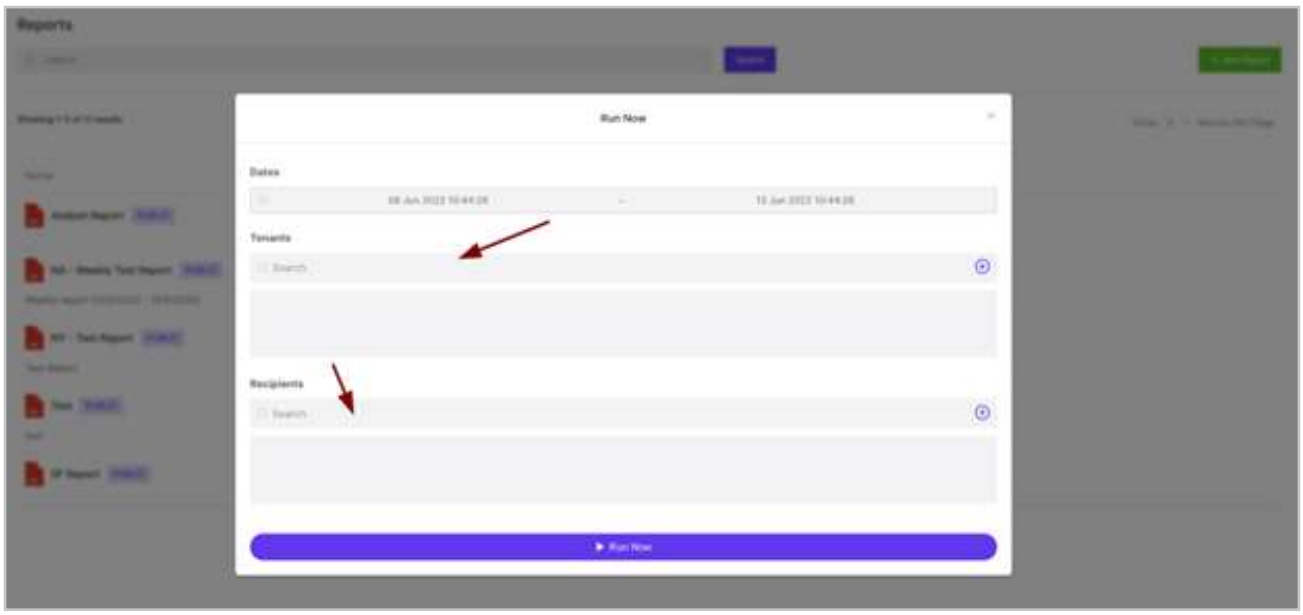
The user can search for a specific report using the report name.



Run a report

Click on Run to run a report. Select the tenant for which you want to run the report.

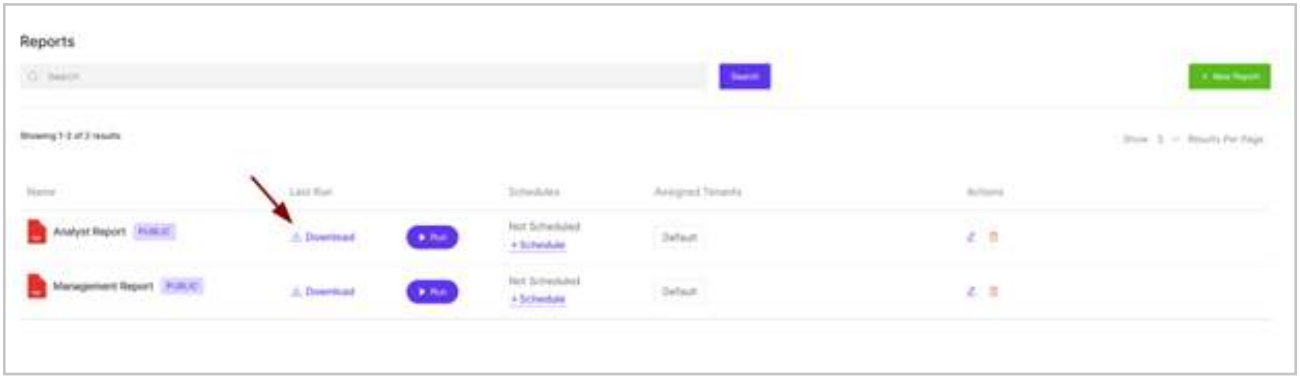




If you want the report to be sent to an email address, for example, the customer or the managers etc, select the recipient and then click on Run Now. If the user wants to look at the report without sending out an email, they can do that as well by not adding any recipient and running the report.

Download a report

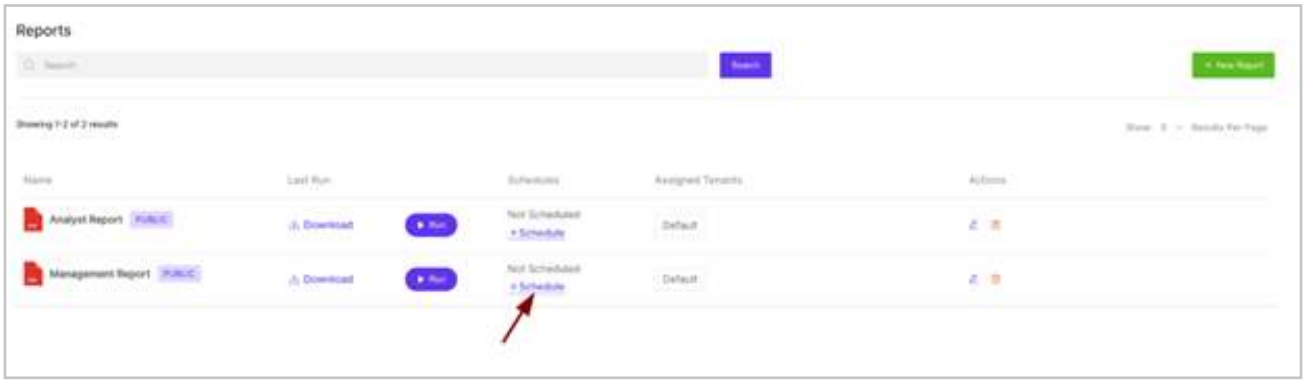
A report can be downloaded by clicking on Download. The report that was last runned gets downloaded.

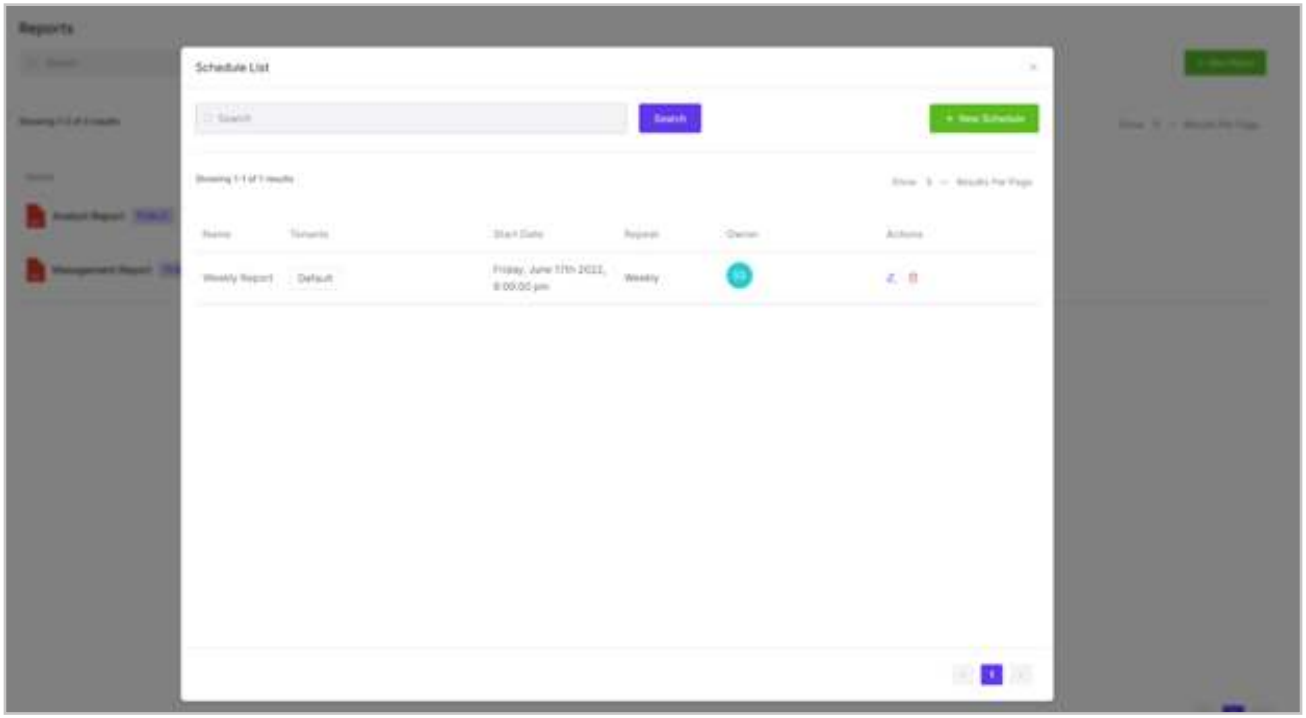


Schedule a report

A schedule can be created to send reports to users. This can be made recurring on a daily, weekly or monthly basis.

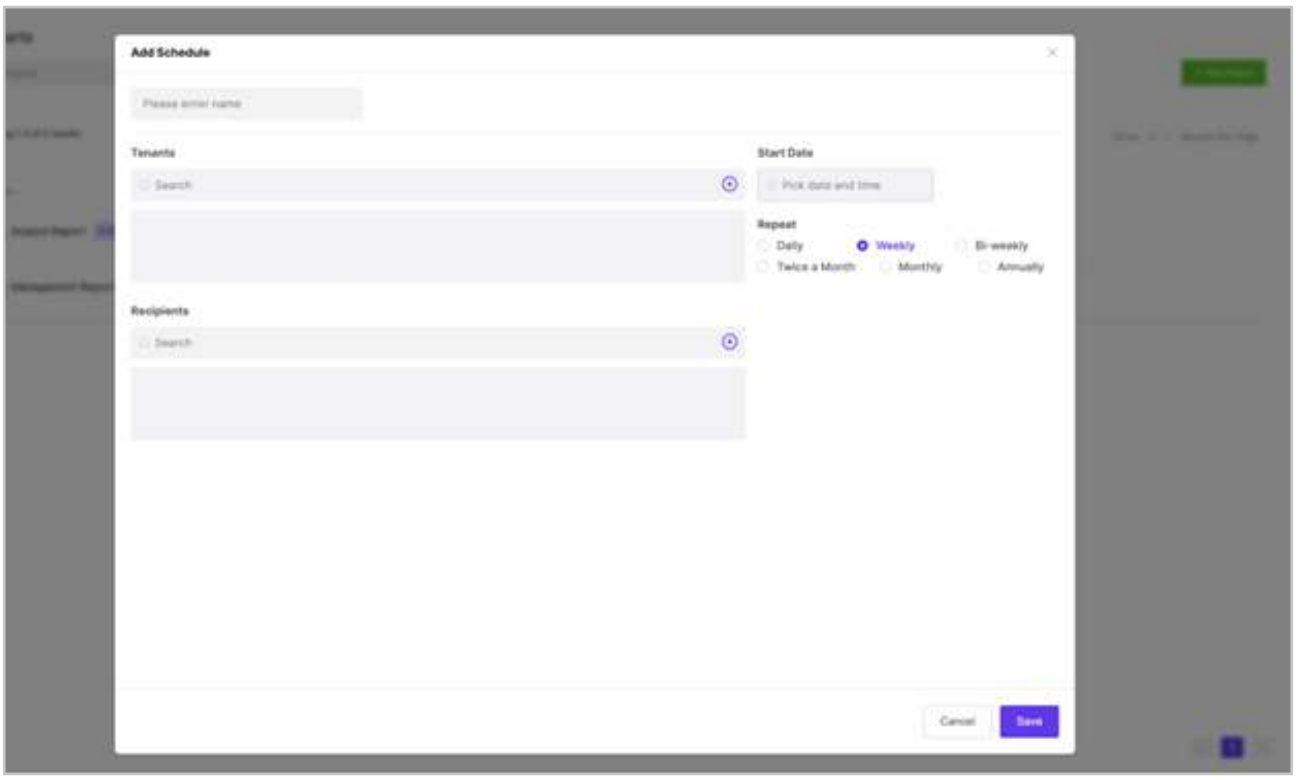
Click on Schedule to go to the Schedule list page.





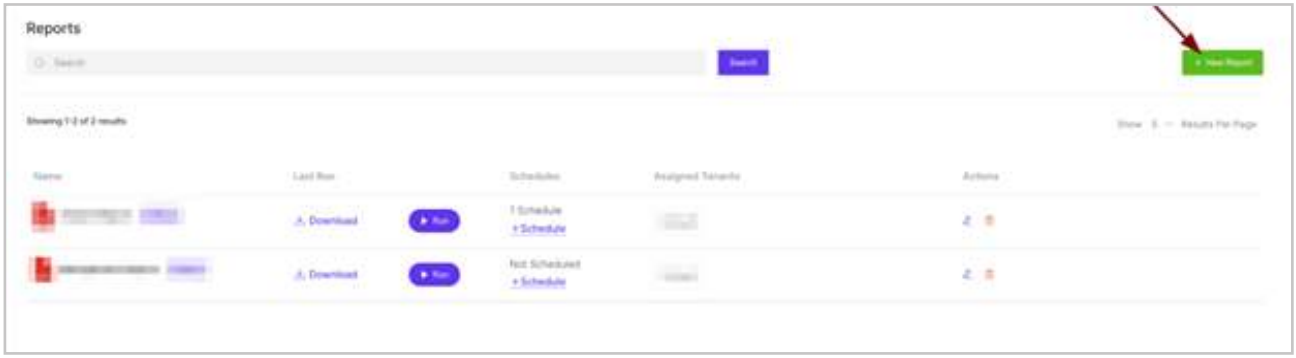
We can search for schedules and edit or delete an existing schedule.

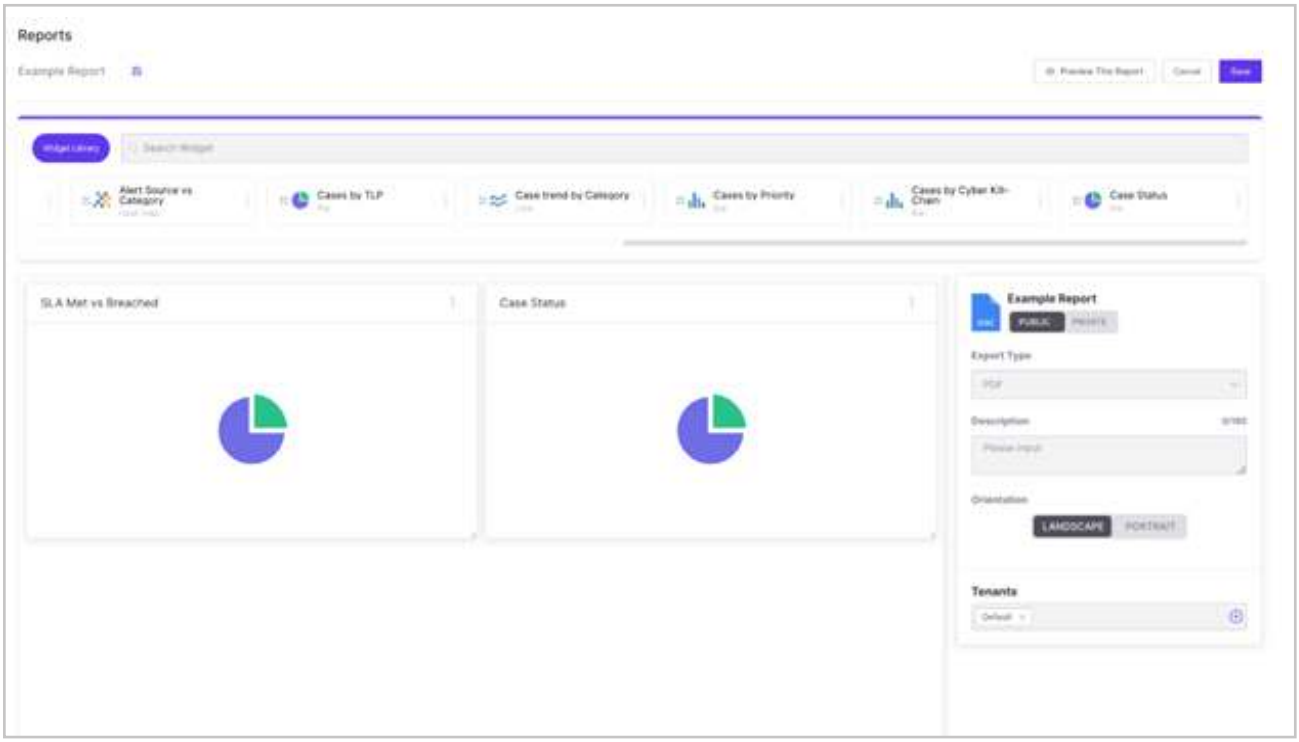
Click on New Schedule to add a new schedule.



Create a report

Click on New Report to create a new report.

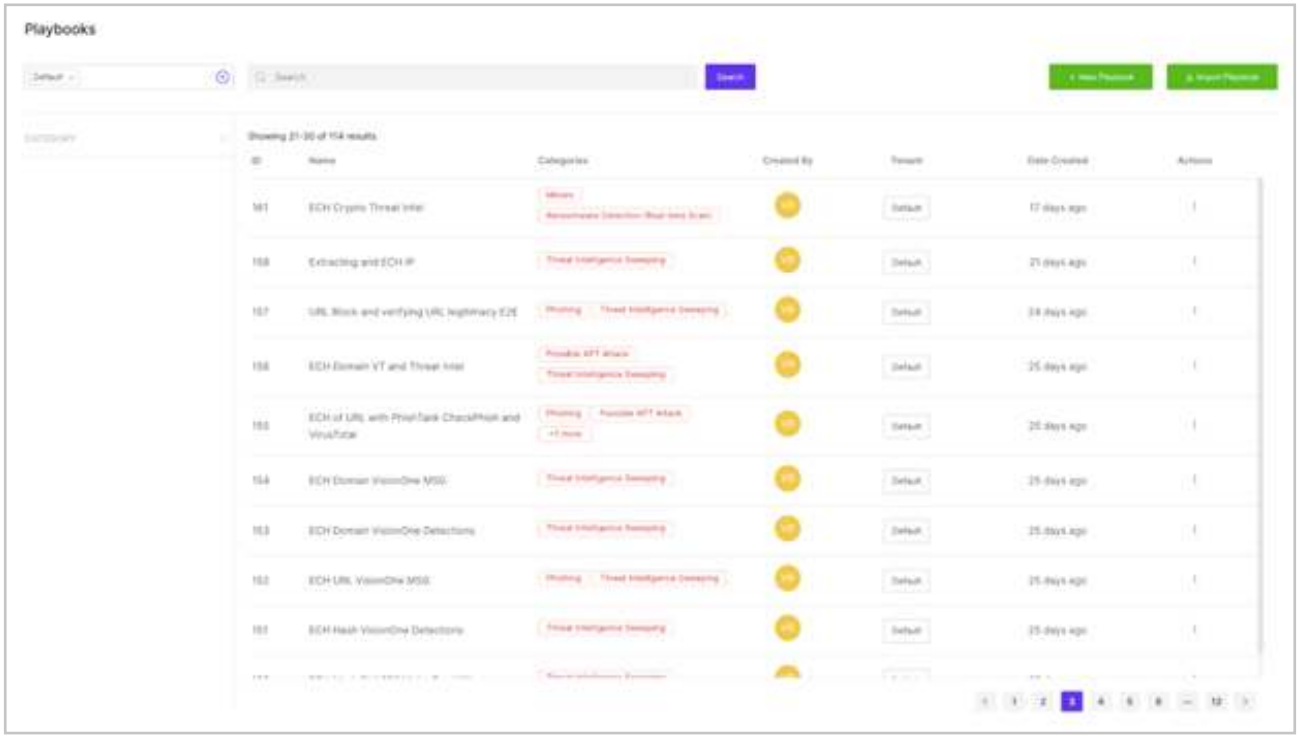




The user can drag and drop the widgets or charts, or create a custom chart from the widget library to create the report. The report can be saved in HTML or PDF format. The user can click on 'Preview This Report' to have a preview of the report before saving it.
The report can be made Private if needed. The report can be made into portrait or landscape format. The user has to select the tenant for whom the report is to be made. An extra page can be added by clicking on Add page if required.

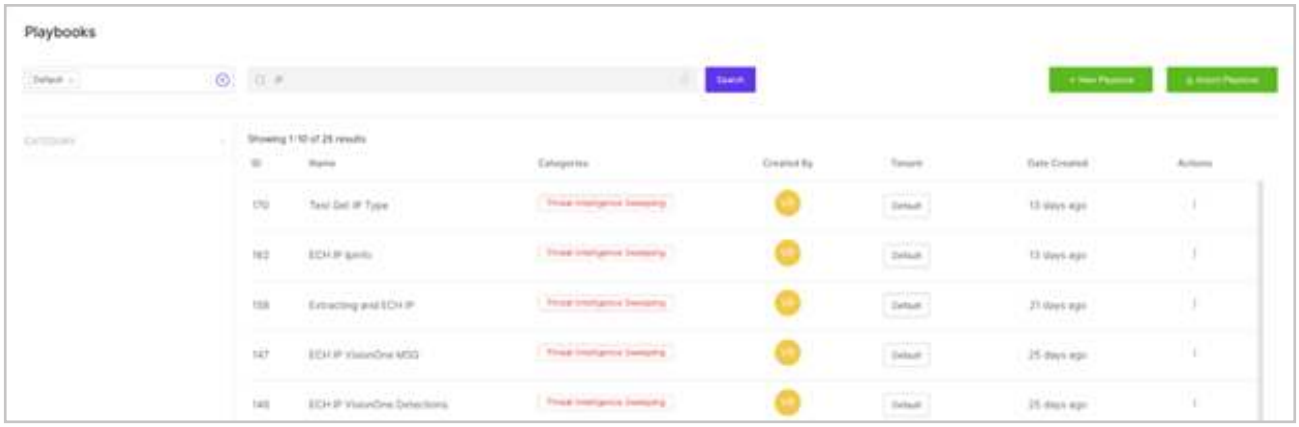
PLAYBOOKS

Playbooks are workflows that enable users to perform tasks related to incident response in a fast manner due to their automated nature and integrations with various security tools and services, thus handling alerts, creating automatic responses and resolving issues accurately and efficiently.



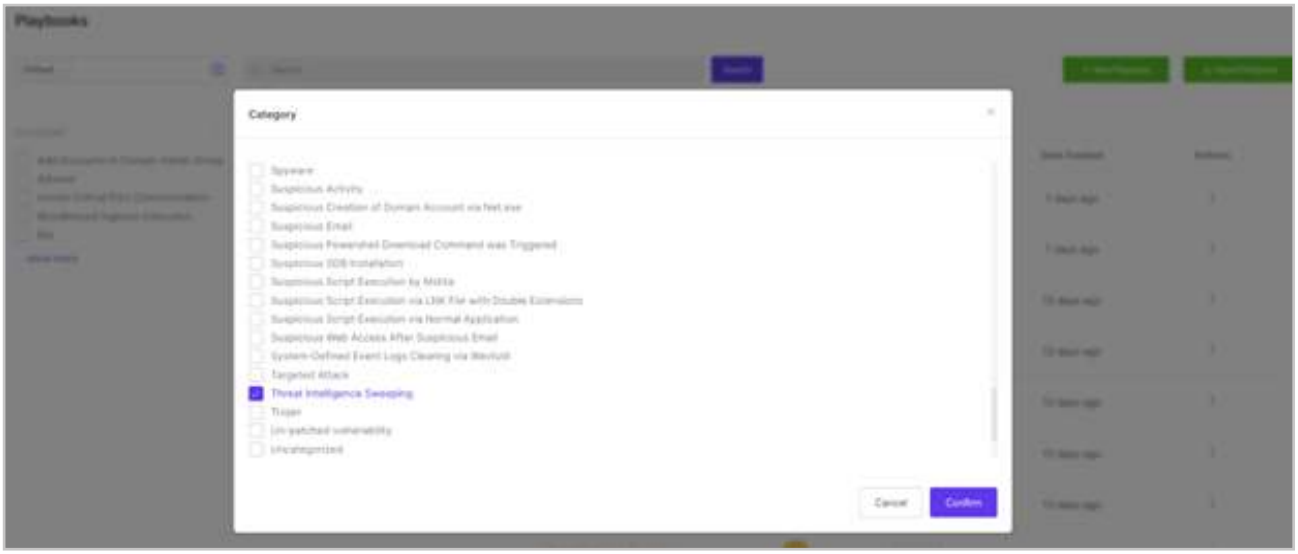
Search for playbooks

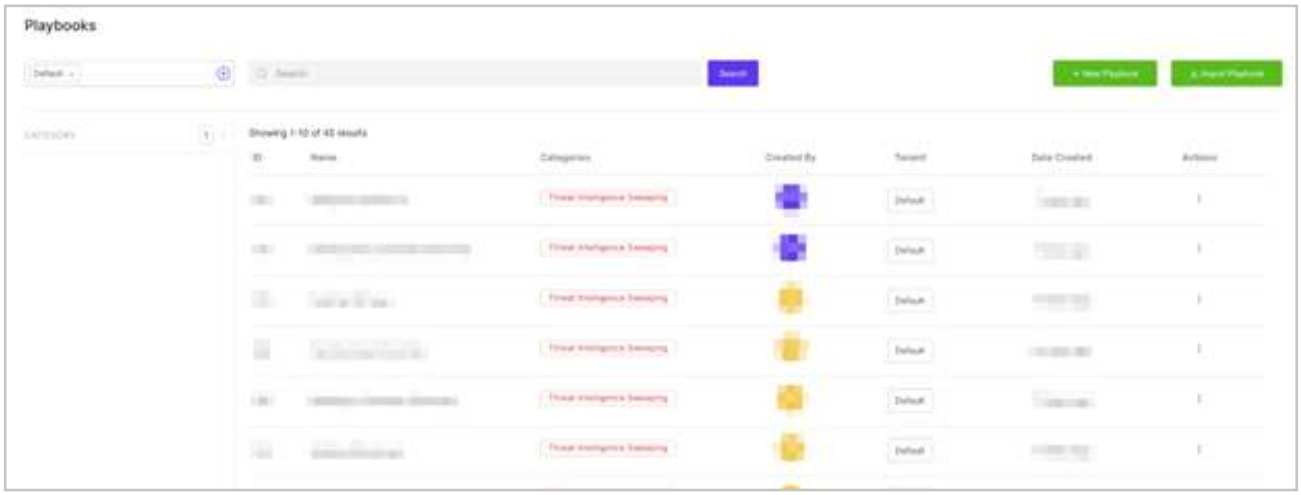
A user can search for a playbook using a playbook name.



Filter playbooks

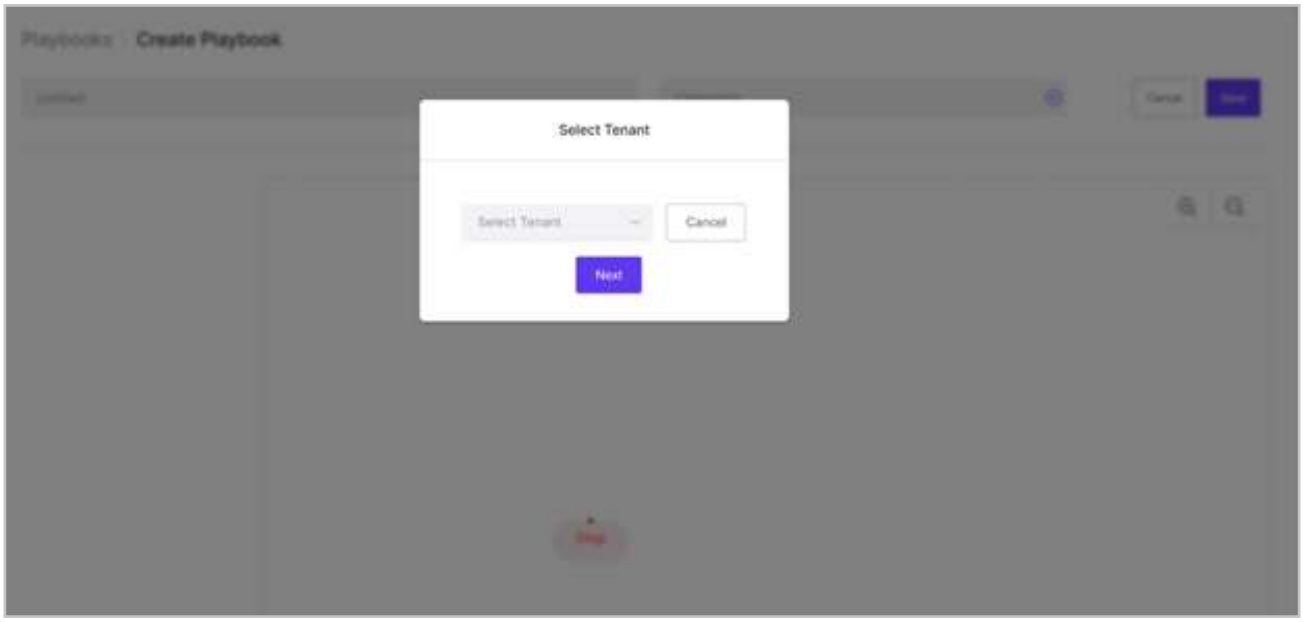
Playbooks can be filtered based on Categories of the cases.



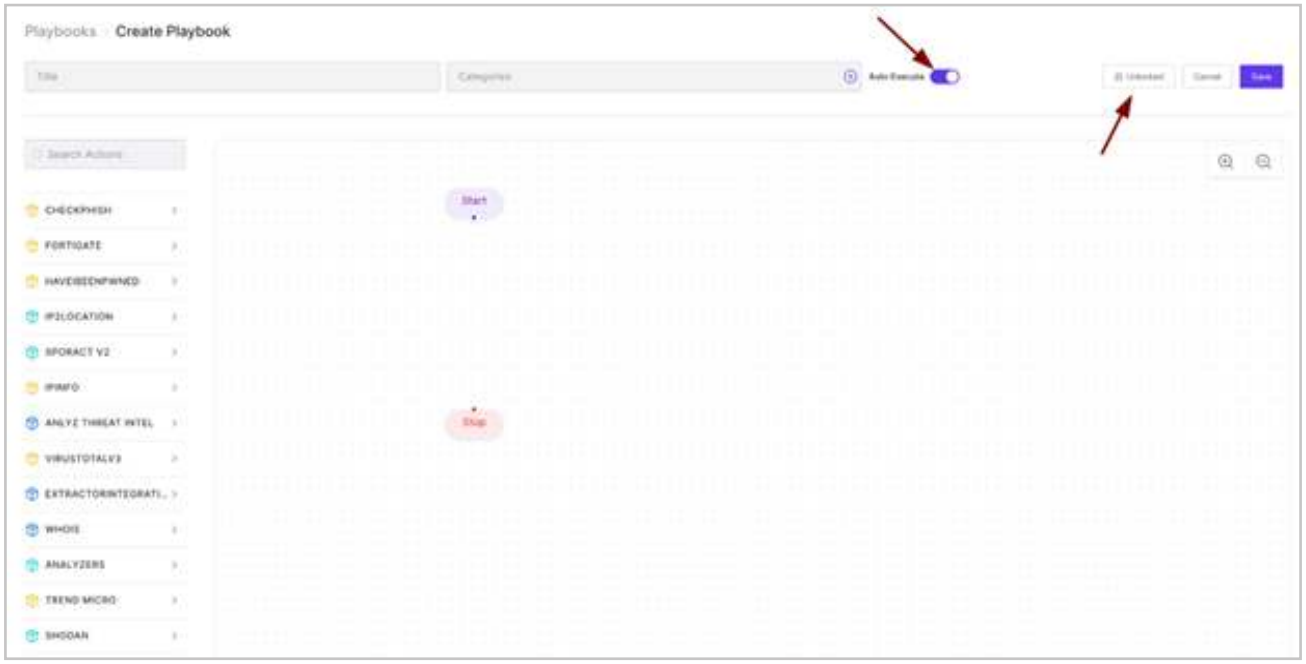


Create new playbooks

A new playbook can be created by clicking on New Playbook.
Note: Generally, Sporact has a standardized set of playbooks. Most of time, if there is any requirement for newer playbooks, we at Anlyz , can create the playbooks provided that proper protocols were followed.



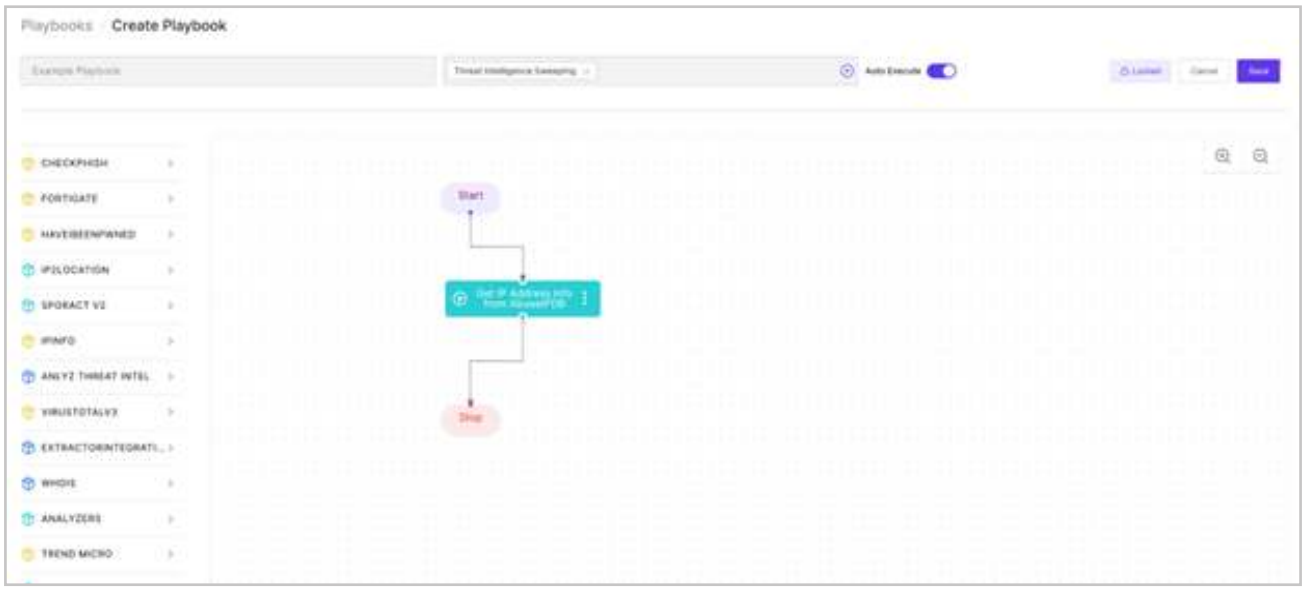
It is important that the integrations are activated for creating dynamic playbooks, since actions from these integrations are used in creating playbooks.



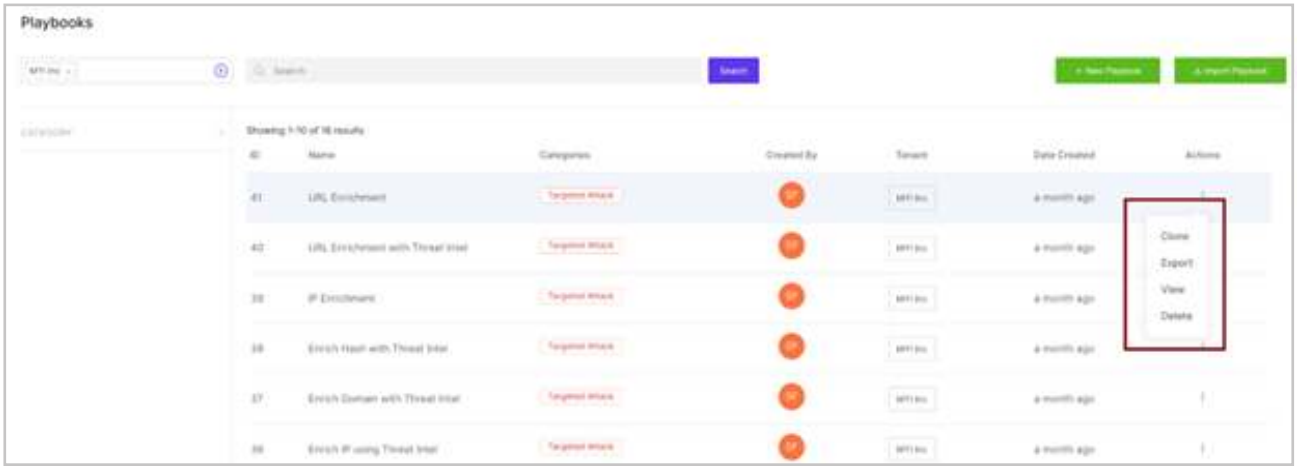
To create a playbook, an action from the integrations is dragged and dropped on the screen. Proper inputs and conditions have to be given for the actions selected and then click on Save.

There is an Auto-execute option, which when selected, the playbook runs automatically every time a case, with the category associated with the playbook ,comes in or created. A playbook can be Locked. A locked playbook cannot be edited except for the one who created it.

An example playbook can be seen below.

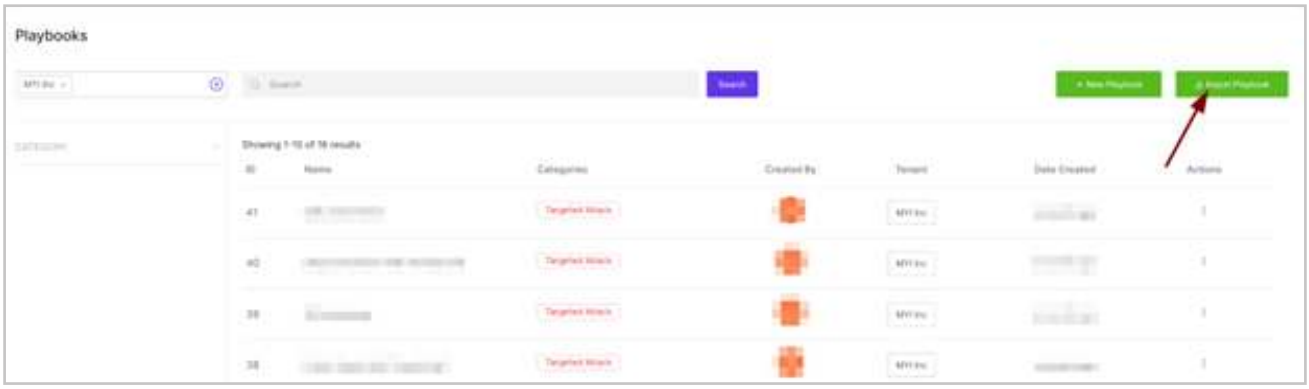


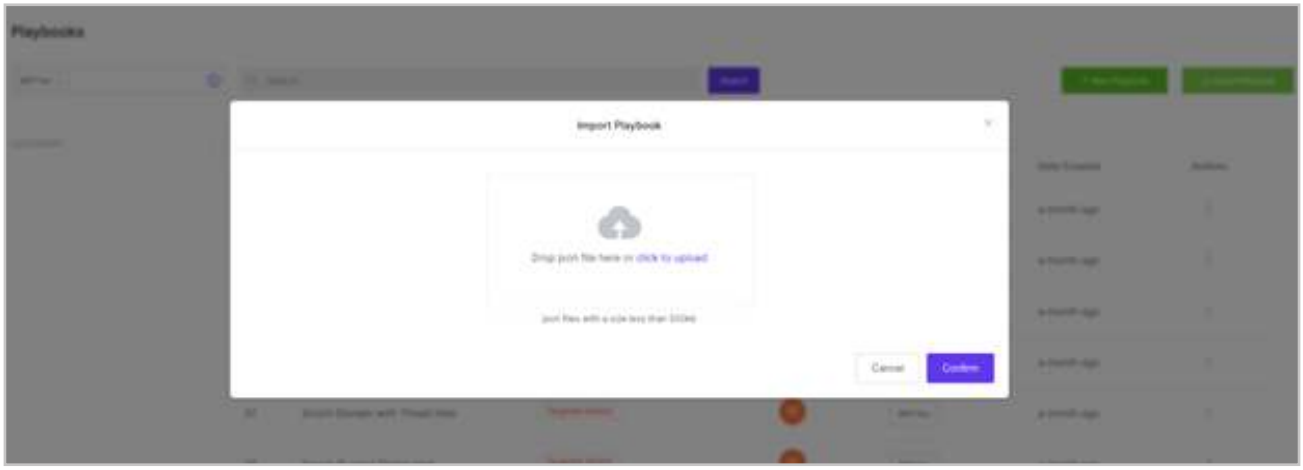
A playbook can be cloned, edited, exported and deleted. When a playbook is cloned, a copy of the playbook is created.



Import Playbooks

Playbooks can be imported by clicking on Import Playbooks.

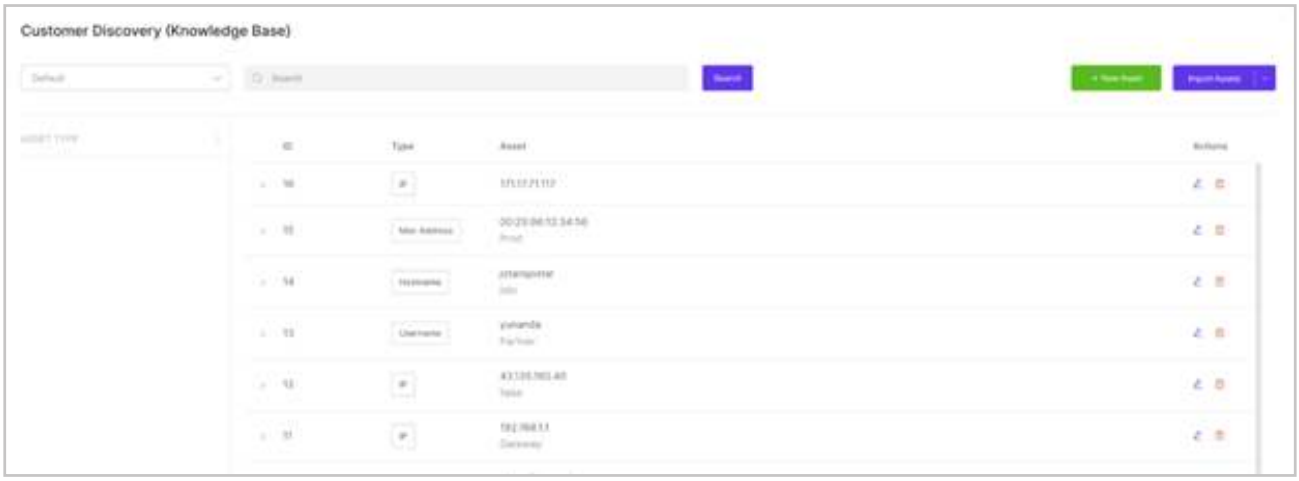




CUSTOMER DISCOVERY

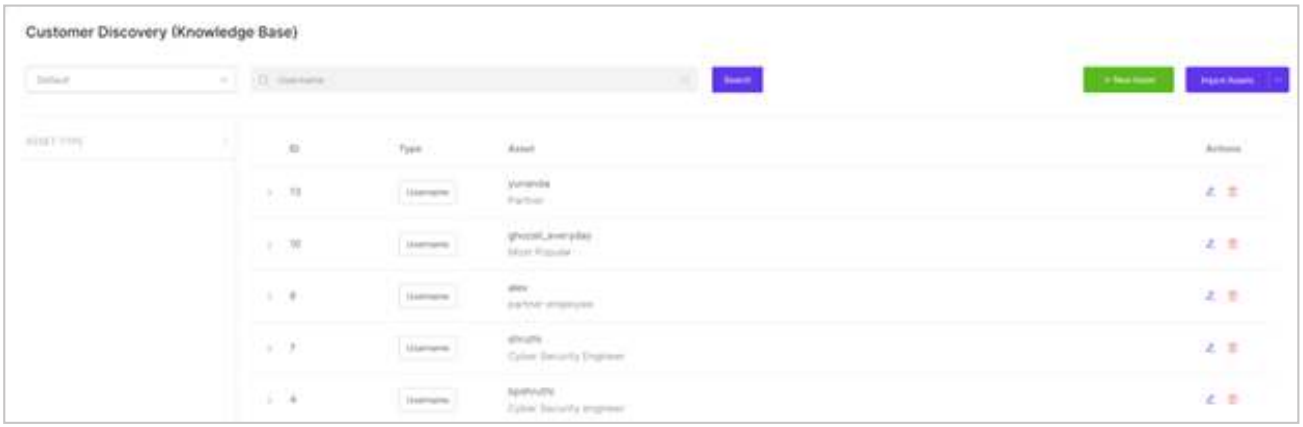
SPORACT's customer discovery is an internal repository of the customer's important assets. Information from customer discovery can be added to a case for enrichment and efficient analysis.

Customer discovery consists of asset types like IP address, Username, Hostname, File hash, Subnet and Mac address.



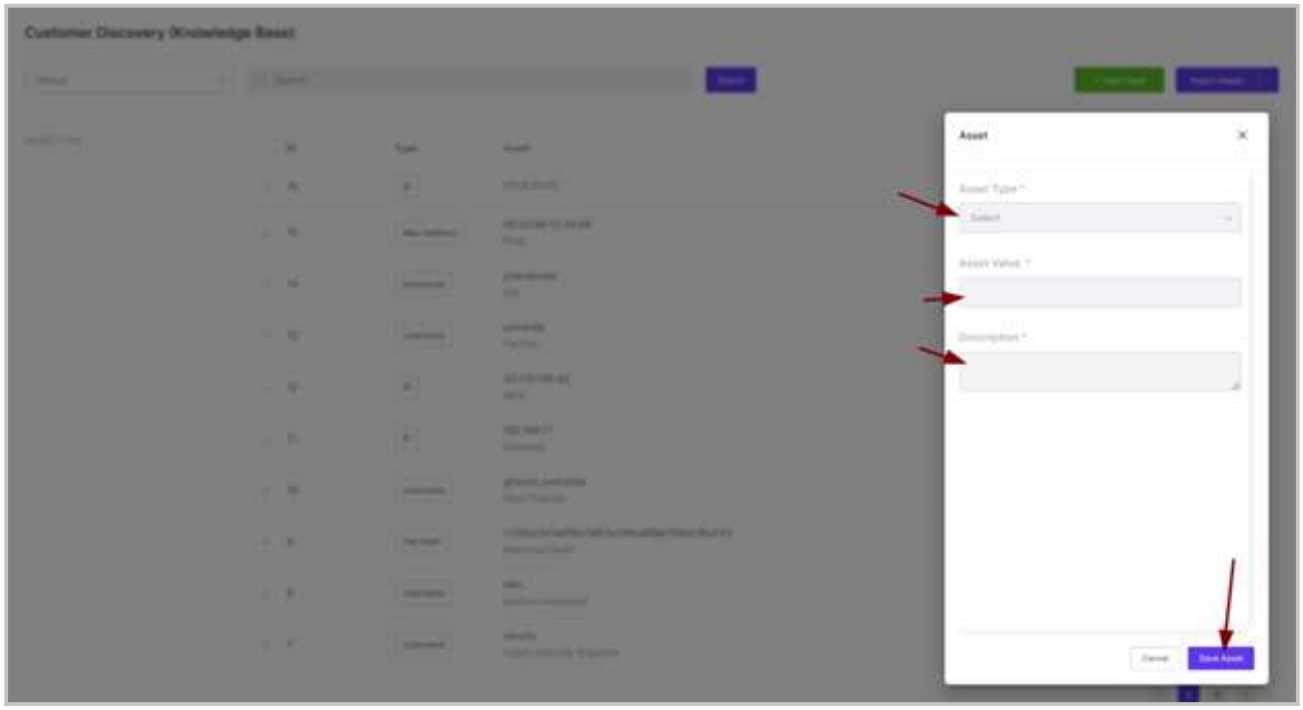
Search an asset

A user can search for an asset using the asset value and asset type.



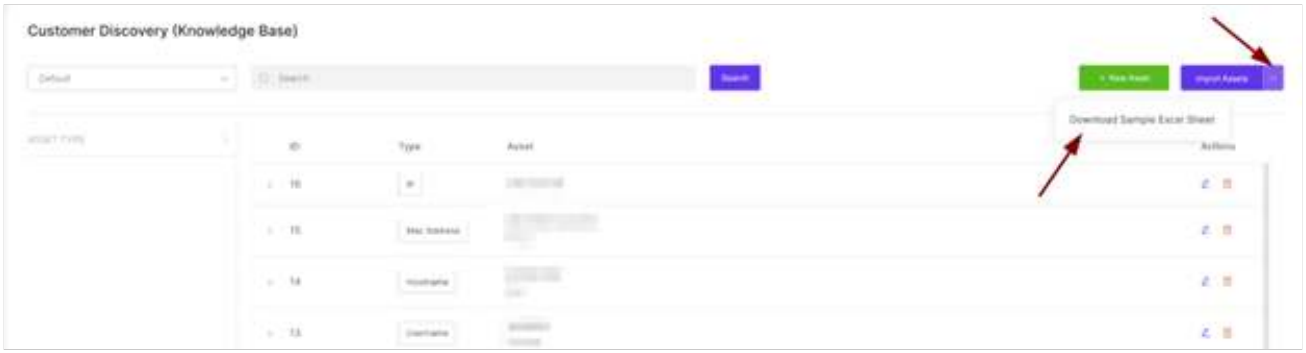
Add new asset

A user can add a new asset by clicking on New Asset.



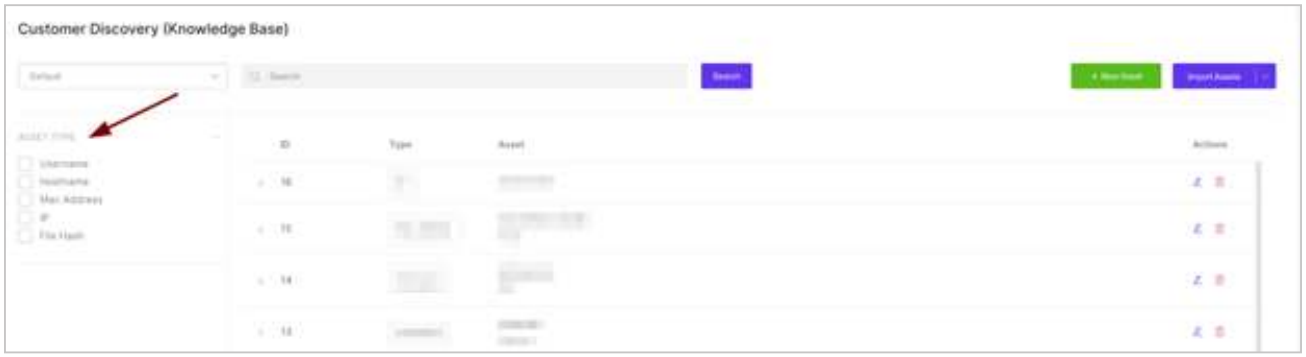
Import assets

A user can import assets by downloading a sample excel sheet and filling it up with the asset values. Once done, this excel sheet can be uploaded by clicking on Import Assets.



Filter assets

A user also can filter assets based on the asset types provided.



Edit and Delete an asset

Assets can be edited or deleted by clicking on the edit or delete icons.