Siemplify

User Guide

Table of Contents

1. Introduction

Siemplify is a centralized security orchestration, automation and incident response platform designed for the entire security operation to manage, investigate and automate threat response from a single workstation.

Siemplify provides automated customizable tools for analysts to investigate security incidents in depth and for SOC managers to monitor the status of individual cases as well as analyst and overall SOC performance.

Siemplify provides unprecedented visibility and context across the entire security ecosystem, reduces alerts by up to 80%, significantly increases the case load capacity of analysts, speeds investigation, transforms static security data into actionable intelligence, and dramatically improves ROI.

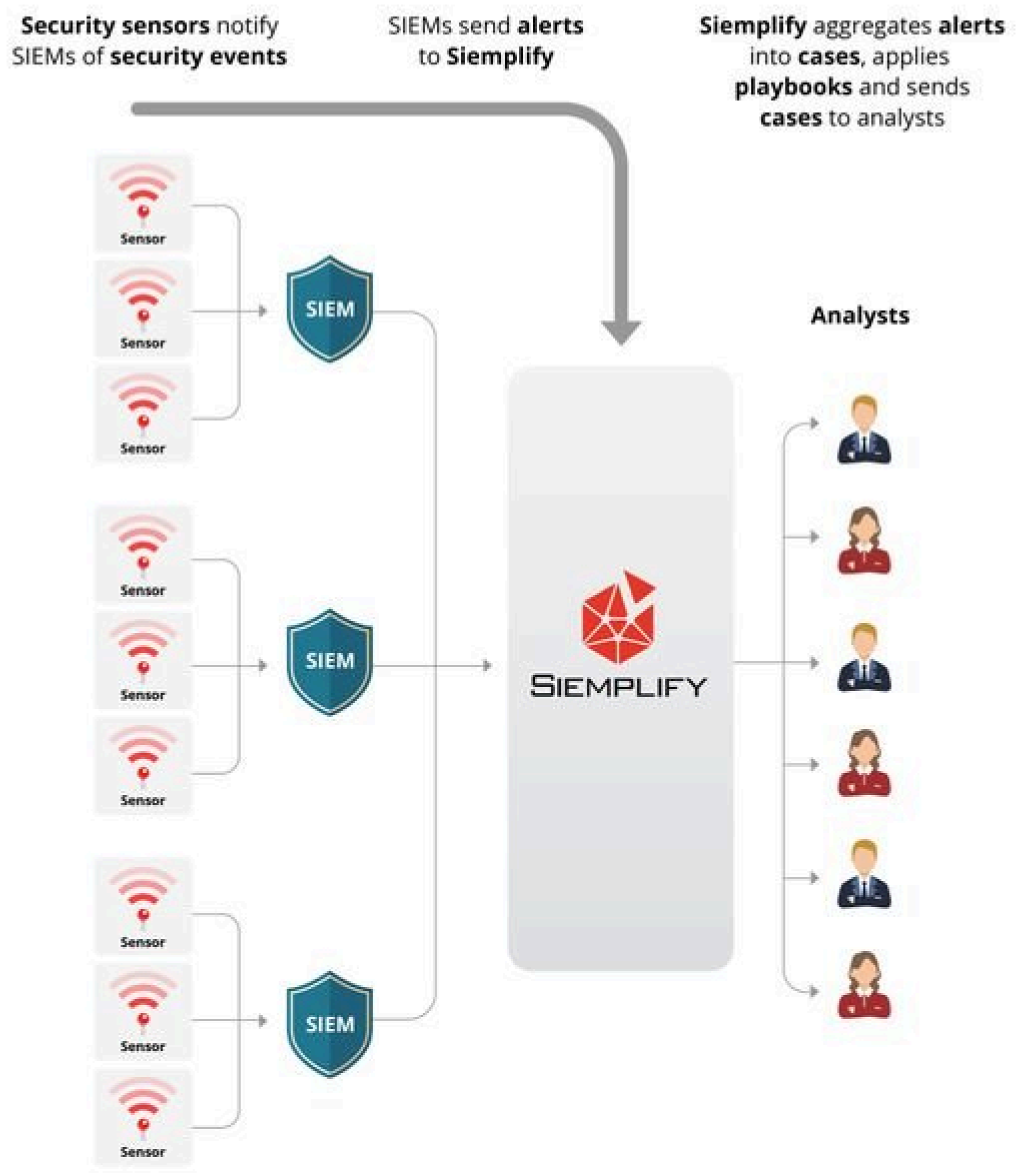
This User Guide takes you through the Siemplify platform enabling you to use our product to make your worklife simpler.

1.1. How does Siemplify work?

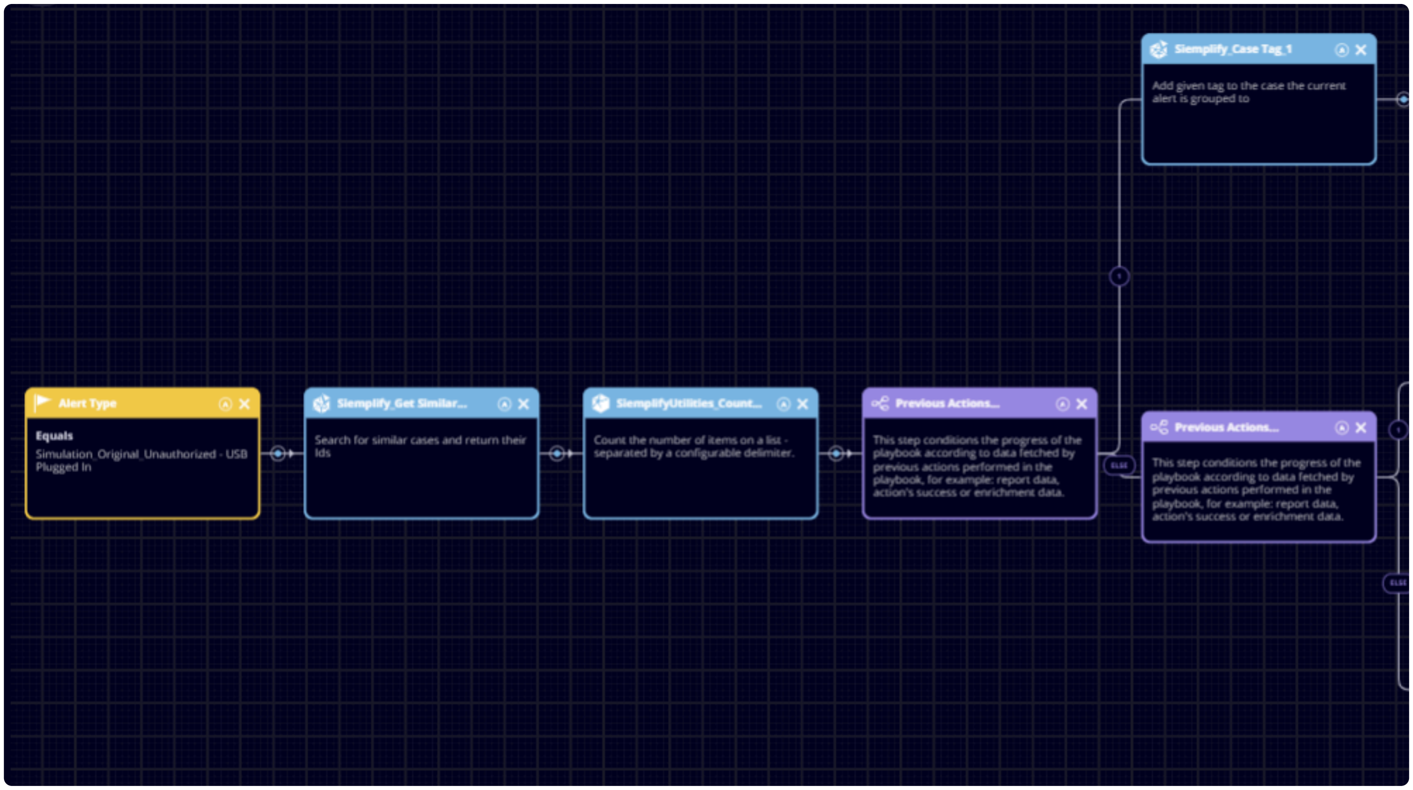
Siemplify receives alerts (indications of security events of interest) from SIEM servers, whose sources include the network devices, workstations, servers etc. Siemplify orchestrates the alerts, that is, it aggregates related alerts into cases, which it assigns to analysts after automatically completing the playbook associated with the alert type. Siemplify uses the Alert Grouping mechanism to intelligently group alerts into cases, by mutual entities and time proximity, and help the analyst to perform contextual analysis of multiple alerts in one case.

A playbook is a predefined set of actions, associated with a specific alert type, which gathers information about the alert from internal and external sources, requests information from users associated with the alert and takes decisions on how to proceed next. These actions are performed automatically by Siemplify for each alert in a case before the case is assigned to an analyst. Analysts can perform additional actions, for example, running a specialized file integrity check, before taking the decision to close or escalate the case.

In this way, the analyst saves considerable time and effort because he or she begins reviewing the case only after much of the additional information needed to properly investigate it has already been automatically gathered by Siemplify, without manual intervention.


Security sensors notify SIEMs of security events
SIEMs send alerts to Siemplify
Siemplify aggregates alerts into cases, applies playbooks and sends cases to analysts
Sensor
SIEM
SIEMPLIFY
Analysts

The following screenshot shows a simplified example of part of a playbook, moving from left to right. Each of the squares represents an action performed by Siemplify, for example, sending an SMS message, determining whether there are similar cases, sending notifications, contacting external servers (to check for viruses, suspicious IP addresses, etc.), enforcing password updates, taking a decision based on results of a previous action, closing a case and more.



Equals
Simulation_Original_Unauthorized - USB Plugged In

Search for similar cases and return their Ids

Count the number of items on a list - separated by a configurable delimiter.

This step conditions the progress of the playbook according to data fetched by previous actions performed in the playbook, for example: report data, action's success or enrichment data.

Add given tag to the case the current alert is grouped to

This step conditions the progress of the playbook according to data fetched by previous actions performed in the playbook, for example: report data, action's success or enrichment data.

Out of the box, Siemplify includes predefined playbooks for the most common scenarios, and you can define additional playbooks for your specific requirements.

When the analyst first sees the case, much of the information needed to properly investigate the case and determine how to resolve it has already been gathered from both external and internal sources, enabling the analyst to respond to the threat more quickly and more accurately.

The Siemplify platform also supports multi-environments (where an environment can correspond to a separate client or a regional division of a corporate company). This enables MSSPs to handle many clients effortlessly.

2. War Room (Beta)

✻ The War Room is currently in Beta mode.

The War Room module enables hands-on crisis management by all relevant departments. There are two main areas of the War Room:

- Workstation where all active participants can add their updates, tasks, decisions, assessments of situation and more
- Dashboard which features all relevant Incident information as well as status update and a visual representation of priority level over time and any countdowns to next updates.

The War Room allows the following:

- End to end management of a critical incident
- Collaboration with all organizational departments and relevant external Personnel.
- Clear time lines of tasks and operations
- Organization of important information in chronological order
- Clear decisions and action plans for all participants.

2.1. Open a Critical Incident

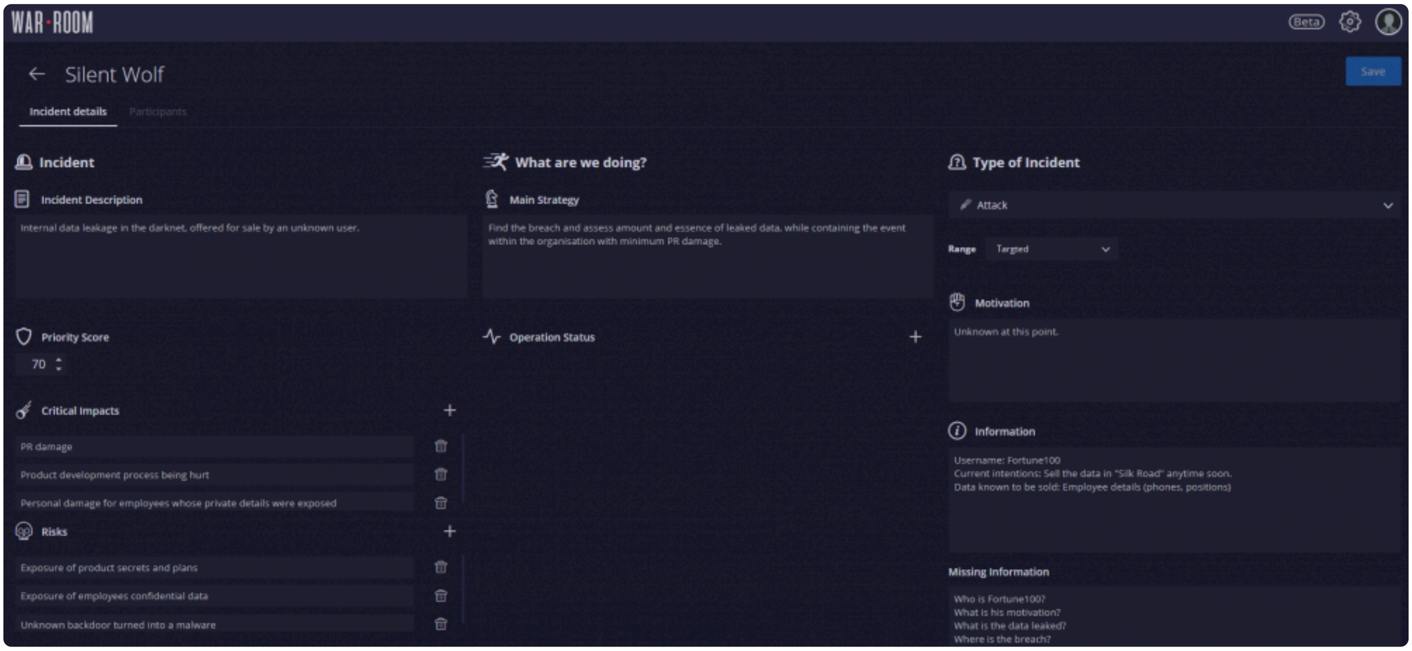
Once an Admin has opened a critical incident, it can then be updated in real time with priority rating changing according to circumstance.
Before you open an Incident, you should define the relevant Departments that will be working in the War Room.

To open an incident,

1. Navigate to the War Room module and click the + icon to add a new incident.
2. At the top of the screen, where it says New Incident, click and add in the name of the Incident. For example, Rogue Attack.
3. Add in the Incident description. For example, hacker attempted to infiltrate system.
4. Choose the Priority Level – from 0 to 100 – where 100 is the highest level. Note that you can (and should) change the Priority level throughout the investigation, containment and action phases. A

graph will display on the Dashboard showing the changes in Priority level over time.

5. Document the Critical Impact this Incident will have on the company – both actual and potential.
6. Document the Risks i.e. what else could happen?
7. Under the What are we doing heading, summarize the Main Strategy your company is taking to handle this crisis.
8. Add in status updates from all the relevant departments (you will take these updates from the Workstation once people start to work on the Incident).
9. Select the type of Incident: Attack or Failure (where failure indicates a problem with the company's infrastructure).
10. Select the range: Unknown, Targeted (aimed at specific individuals in the company), or Wide (ie global company attack).
11. Write down the motivation for the attack (as far as you can tell)
12. Add information that you have so far about the case.
13. Add information that you are still missing.
14. Click Save when done.



Silent Wolf

Incident

Incident Description

Internal data leakage in the darknet, offered for sale by an unknown user.

Priority Score

70

Critical Impacts

PR damage

Product development process being hurt

Personal damage for employees whose private details were exposed

Risks

Exposure of product secrets and plans

Exposure of employees confidential data

Unknown backdoor turned into a malware

What are we doing?

Main Strategy

Find the breach and assess amount and essence of leaked data, while containing the event within the organisation with minimum PR damage.

Operation Status

Type of Incident

Attack

Range: Targted

Motivation

Unknown at this point.

Information

Username: Fortune100
Current intentions: Sell the data in "Silk Road" anytime soon.
Data known to be sold: Employee details (phones, positions)

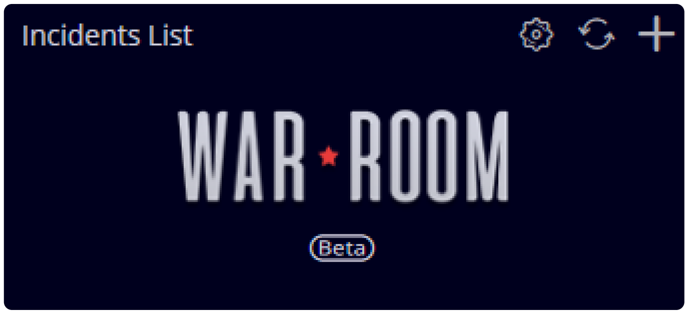
Missing Information

Who is Fortune100?
What is his motivation?
What is the data leaked?
Where is the breach?

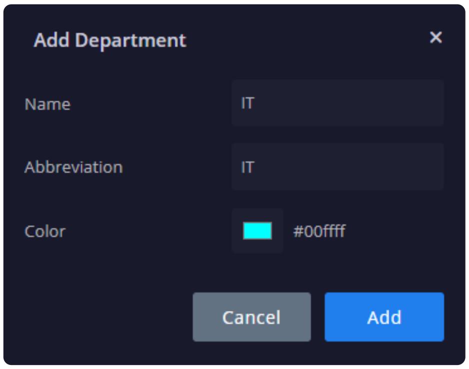
2.1.1. Define Departments

The first step is to define the departments that you will be working with.

1. Navigate to the War Room tab and click the configuration icon.

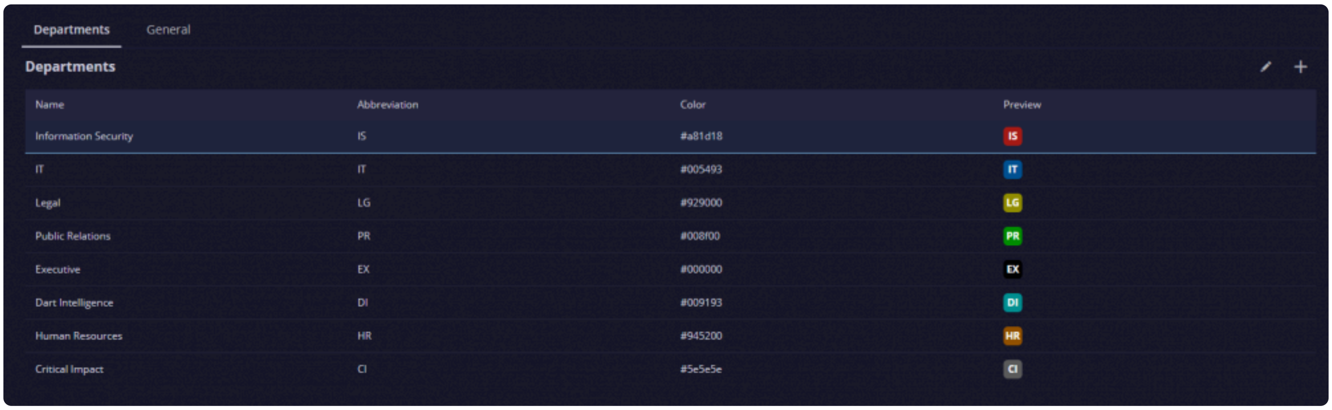


2. In the Departments screen, click the + icon and fill out the new department information.


Add Department

Name	IT
Abbreviation	IT
Color	#00ffff

3. Add in all the departments that you will be working with in the War Room. You can also add departments that are external to your company.



Departments

Name	Abbreviation	Color	Preview
Information Security	IS	#a81d18	IS
IT	IT	#005493	IT
Legal	LG	#929000	LG
Public Relations	PR	#008f00	PR
Executive	EX	#000000	EX
Dart Intelligence	DI	#009193	DI
Human Resources	HR	#945200	HR
Critical Impact	CI	#5e5e5e	CI

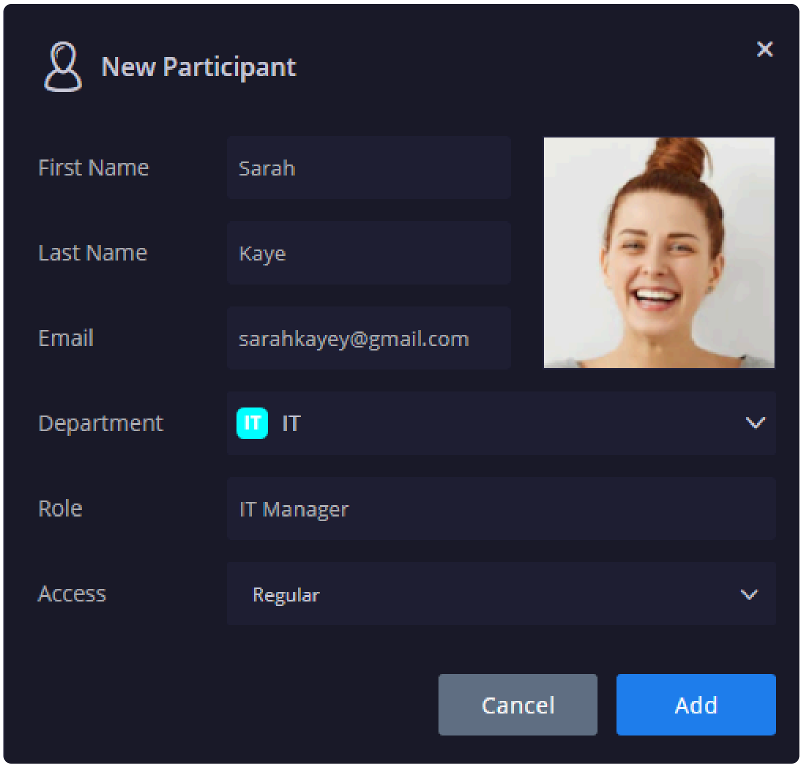
2.2. Invite Participants to War Room

After setting up departments and opening a new incident, the next stage is to invite the relevant people – both from within and outside your company – to work together on containing and eradicating the crisis. There are two ways of inviting participants. Adding directly or Registering through Email

Adding participants directly is recommended for people within the company. Registering through Email is recommended for people outside of the company.

To add participants directly:

1. In the War Room module, next to the Incident Details tab, click on the Participants tab.
2. In the top right corner, click the + icon.
3. Fill out the relevant information to create the new user.



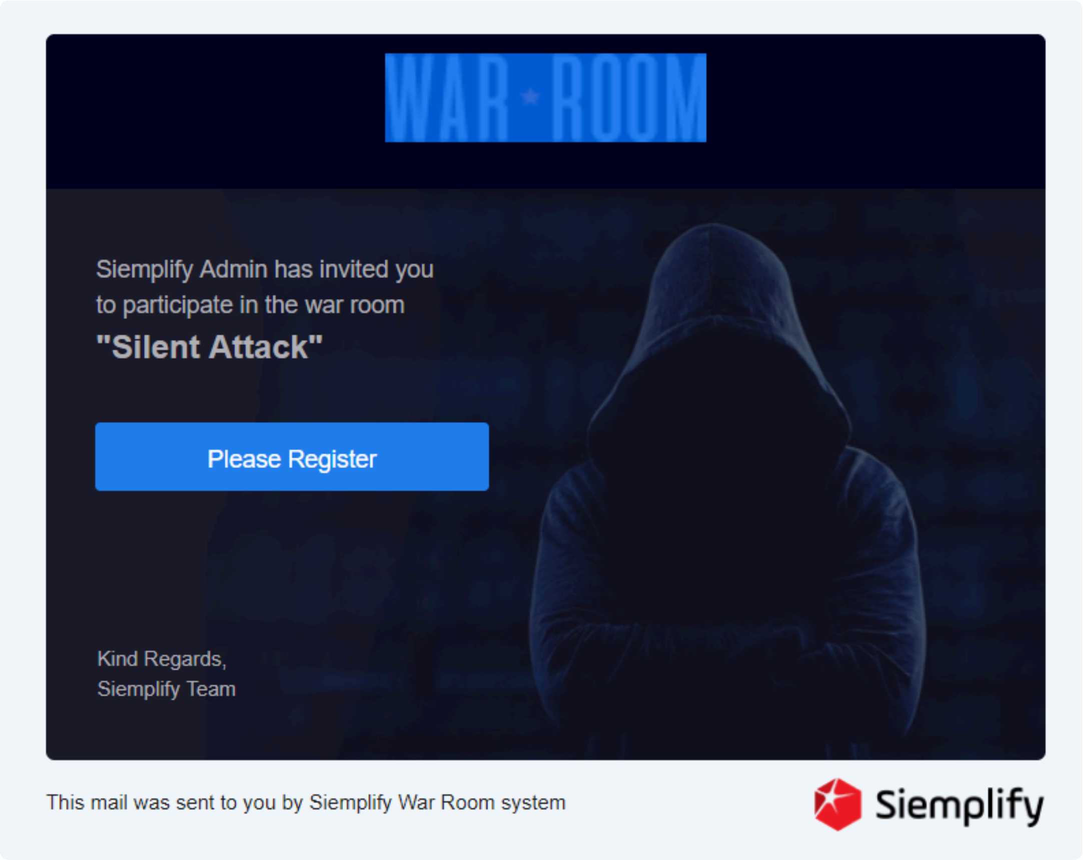
New Participant

First Name	Sarah
Last Name	Kaye
Email	sarahkayey@gmail.com
Department	IT
Role	IT Manager
Access	Regular

4. The user is created and added and will receive an email with the link to enter the War Room. From there, they can also access the Workstation to add in their input and information.

To invite participants to register through email:

1. In the Invite Participants box on the far right of the screen, add in the email address of the participant.
2. Click Send.
3. The participant will receive the following email in their Inbox. (You might want to message them to be on the lookout for it).



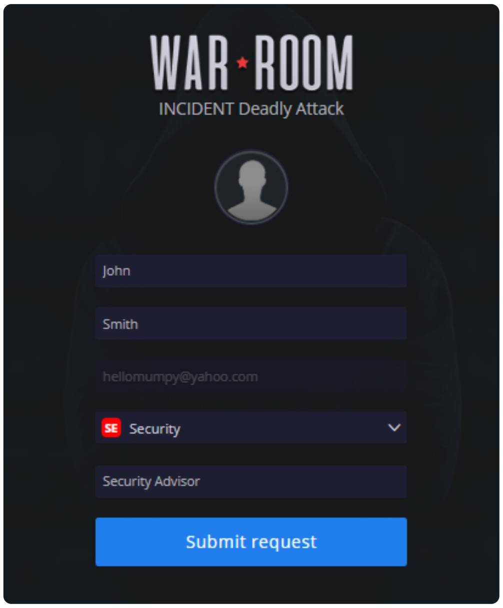
Siemplify Admin has invited you to participate in the war room

"Silent Attack"

Kind Regards,
Siemplify Team

This mail was sent to you by Siemplify War Room system

4. The participant needs to click Register Now and fill out their details in the form.



John

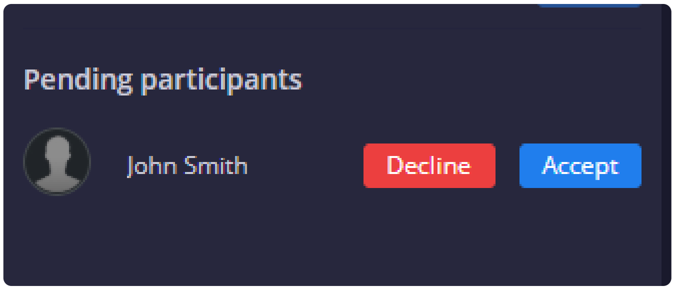
Smith

hellomumpy@yahoo.com

SE Security

Security Advisor

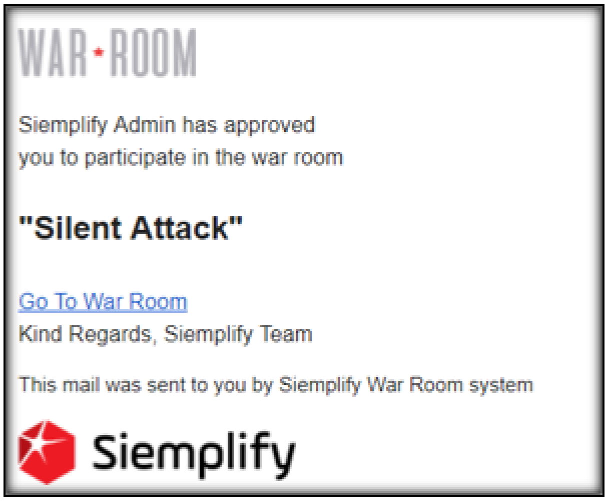
5. Once they have registered, they will see a message saying **Please wait for your registration to be formally approved**.
6. The admin will see their name in the Pending Participants in the Siemplify Platform screen. Click Approve next to their name.



Pending participants

John Smith

7. Siemplify War Room will then send another email to the participant approving them.



WAR•ROOM

Siemplify Admin has approved
you to participate in the war room

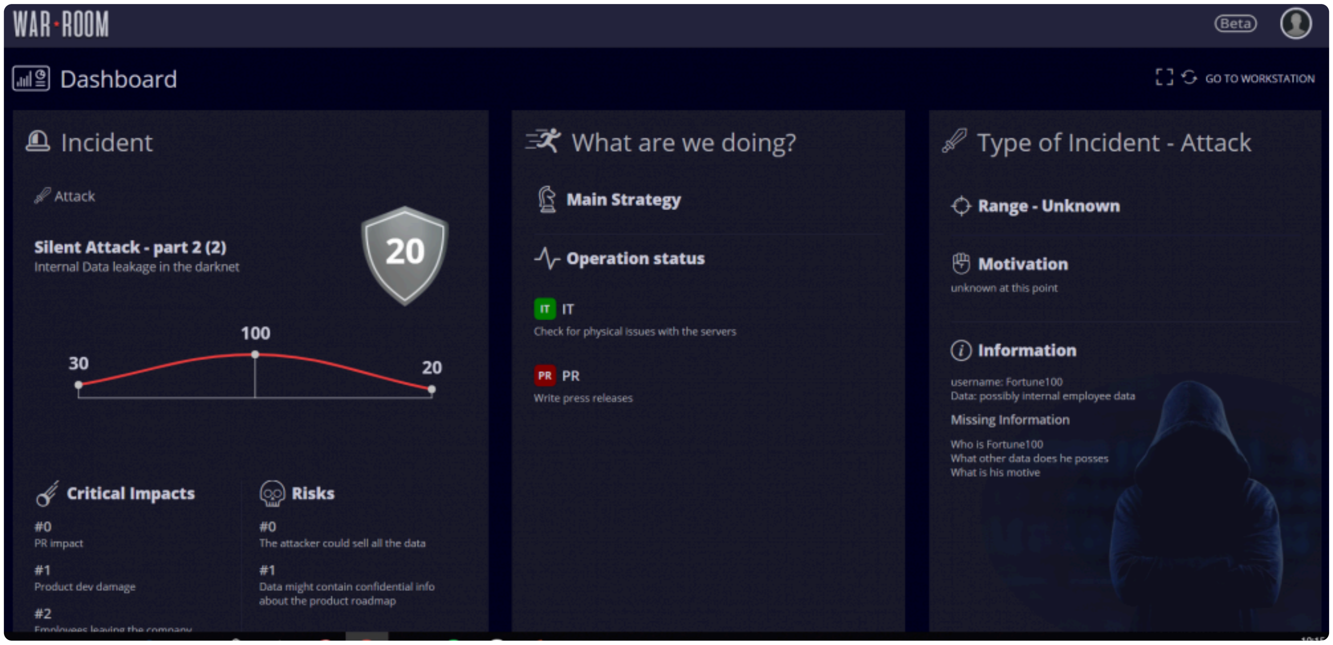
"Silent Attack"

Go To War Room
Kind Regards, Siemplify Team

This mail was sent to you by Siemplify War Room system

Siemplify

8. The participant should click on the link in the mail and they will be directed to the Dashboard screen. From there, they can also access the Workstation to add in their input and information.



Incident

Attack

Silent Attack - part 2 (2)
Internal Data leakage in the darknet

Critical Impacts

#0
PR impact

#1
Product dev damage

#2
Employees leaving the company

Risks

#0
The attacker could sell all the data

#1
Data might contain confidential info about the product roadmap

What are we doing?

Main Strategy

Operation status

IT IT
Check for physical issues with the servers

PR PR
Write press releases

Type of Incident - Attack

Range - Unknown

Motivation
unknown at this point

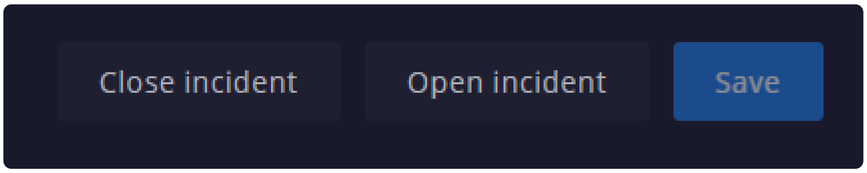
Information
username: Fortune100
Data: possibly internal employee data

Missing Information
Who is Fortune100
What other data does he posses
What is his motive

2.3. Working with the Dashboard

How do I access the Dashboard?

As an admin in the Siemplify platform, you will select the Incident, and click the Open Incident button on the top right of the screen.

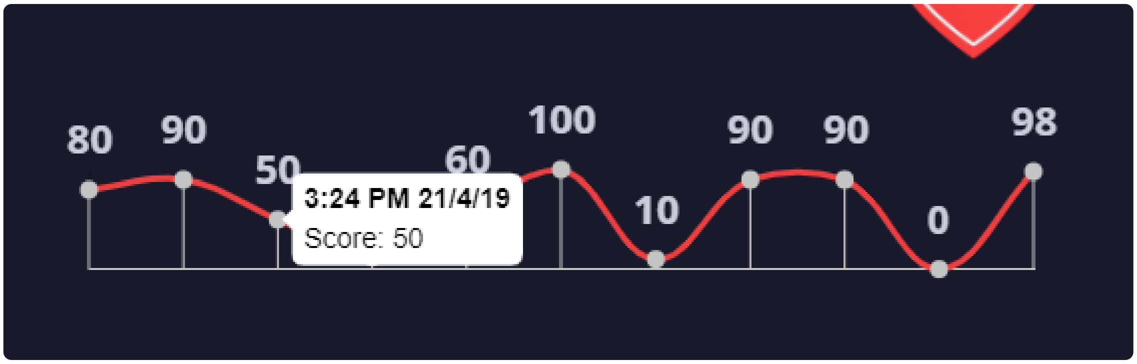


As a regular user, you will click on the Go To War Room link in the email you received.

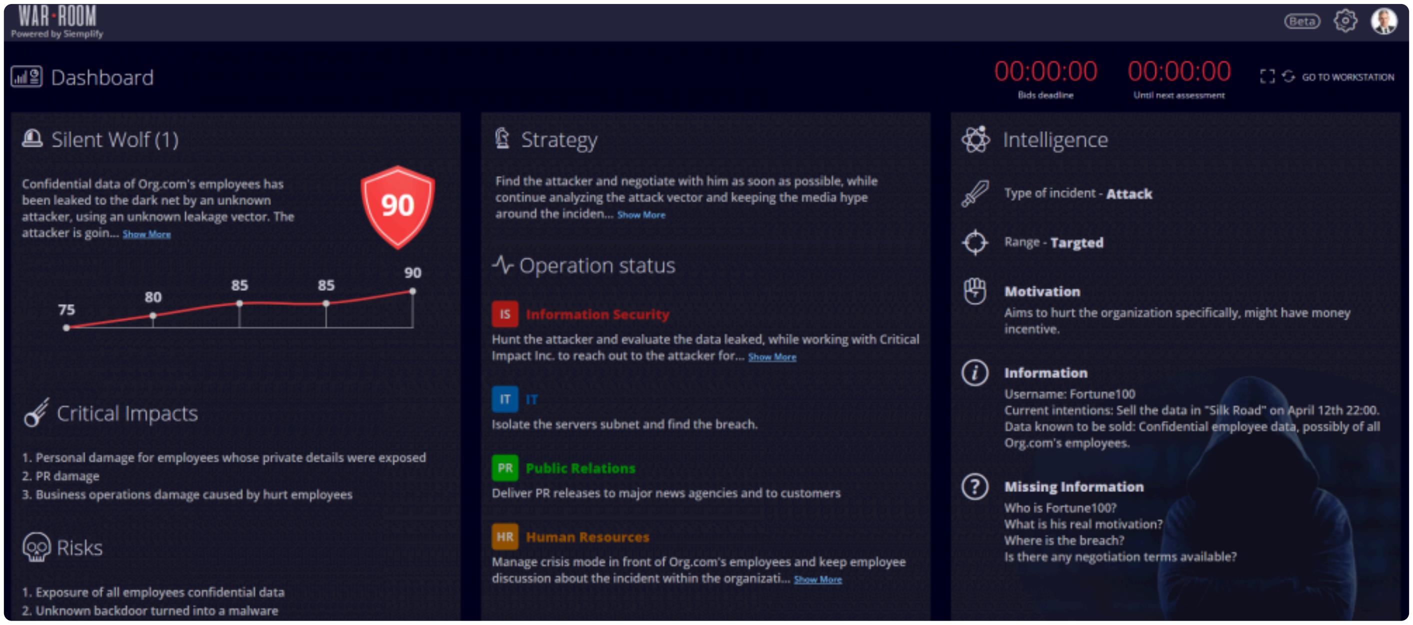
What can I see on the Dashboard?

Both types of users – admin and regular – will have access to the same information.

The top left will display – if configured in the Workstation – **Reminder** time counters to the next Action or Task that needs to be done.
Underneath this will display a graph showing the different Priority levels over a period of time. Place your cursor on a specific spot to see the time the priority level was changed.



The rest of the Dashboard will display the information added or updated by the Admin.



Dashboard

00:00:00 Bids deadline

00:00:00 Until next assessment

Silent Wolf (1)

Confidential data of Org.com's employees has been leaked to the dark net by an unknown attacker, using an unknown leakage vector. The attacker is goin... Show More

Critical Impacts

1. Personal damage for employees whose private details were exposed
2. PR damage
3. Business operations damage caused by hurt employees

Risks

1. Exposure of all employees confidential data
2. Unknown backdoor turned into a malware

Strategy

Find the attacker and negotiate with him as soon as possible, while continue analyzing the attack vector and keeping the media hype around the inciden... Show More

Operation status

IS Information Security
Hunt the attacker and evaluate the data leaked, while working with Critical Impact Inc. to reach out to the attacker for... Show More

IT IT
Isolate the servers subnet and find the breach.

PR Public Relations
Deliver PR releases to major news agencies and to customers

HR Human Resources
Manage crisis mode in front of Org.com's employees and keep employee discussion about the incident within the organizati... Show More

Intelligence

Type of incident - **Attack**

Range - **Targted**

Motivation
Aims to hurt the organization specifically, might have money incentive.

Information
Username: Fortune100
Current intentions: Sell the data in "Silk Road" on April 12th 22:00.
Data known to be sold: Confidential employee data, possibly of all Org.com's employees.

Missing Information
Who is Fortune100?
What is his real motivation?
Where is the breach?
Is there any negotiation terms available?

2.4. Using the Workstation

Every participant in the War Room can add information and input into the Workstation screen. It is the Admin's job to collate the information and update the Incident at regular time intervals – as determined by the Reminder counters.

What can I add to the Workstation?

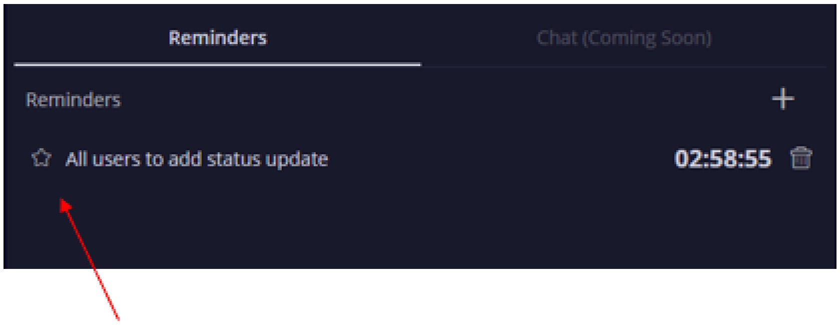
Icon	Description
A	Add a longer message with typesetting options
📎	Add any type of relevant file
❗	Add in a fact and click Save. (If there is an issue adding a fact – check in the Config Setting/General Settings that the Fact Character limit is set correctly.
☑	Add in a task with an assignee and a due date.
📋	Add name, participants, status and any decisions made. Note that the Assessment (Priority Score) will be taken into consideration by the Admin when calculating Priority score for the next update.

⇆	Add decision and click Save

Reminder Counters

You can add as many reminders as you need. However, you can only choose two Reminders to appear as ticking clocks on the Dashboard/Workstation.

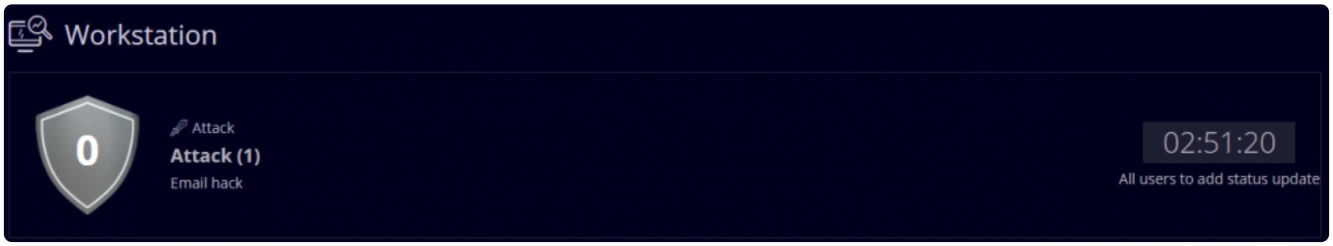
1. In the right of the Workstation, click the + icon.
2. In the Reminder dialog box, fill out the information and choose the time it needs to be done.
3. Click Add. The clock starts ticking!
4. In order to see it on both the Workstation and the Dashboard, click the star next to it.



☆ All users to add status update 02:58:55

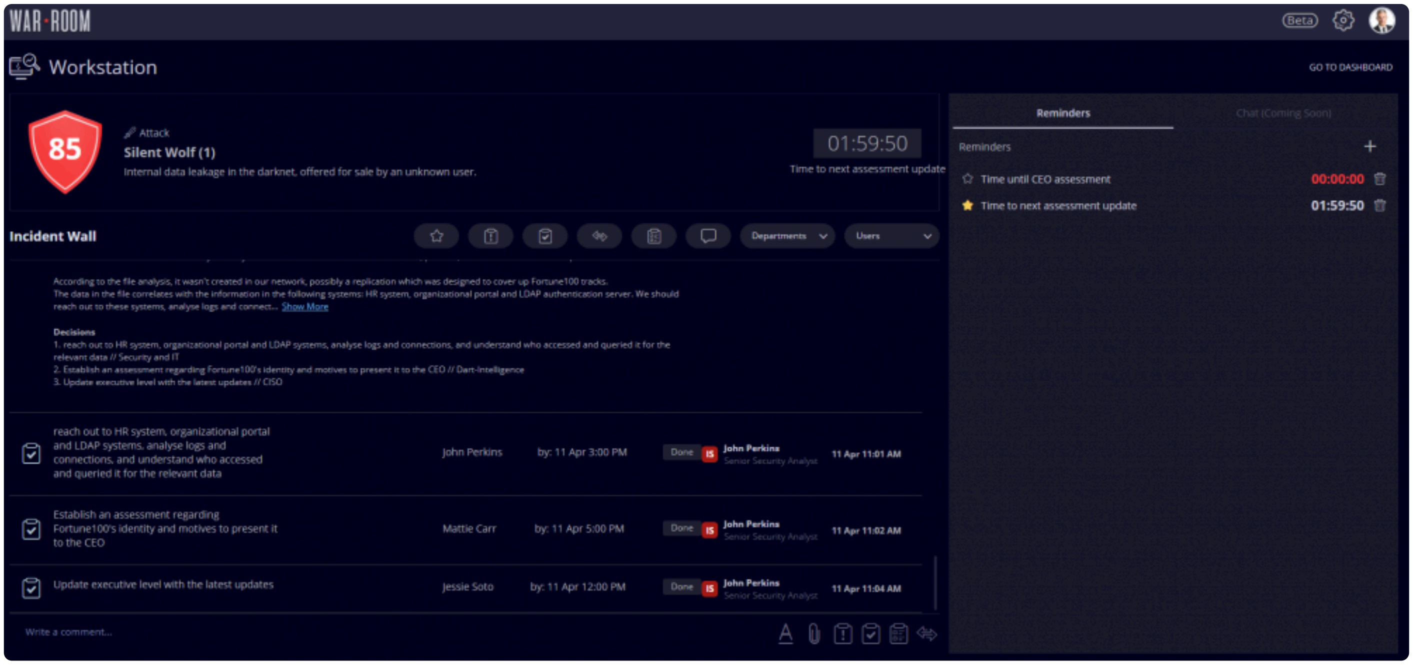
Click star to add
visual reminder

5. The Reminder now appears in both screens as a ticking counter.



Attack (1)
Email hack

02:51:20
All users to add status update



Silent Wolf (1)

Internal data leakage in the darknet, offered for sale by an unknown user.

01:59:50
Time to next assessment update

According to the file analysis, it wasn't created in our network, possibly a replication which was designed to cover up Fortune100 tracks.
The data in the file correlates with the information in the following systems: HR system, organizational portal and LDAP authentication server. We should reach out to these systems, analyse logs and connect... Show More

Decisions
1. reach out to HR system, organizational portal and LDAP systems, analyse logs and connections, and understand who accessed and queried it for the relevant data // Security and IT
2. Establish an assessment regarding Fortune100's identity and motives to present it to the CEO // Dart-Intelligence
3. Update executive level with the latest updates // CISO

✓	reach out to HR system, organizational portal and LDAP systems, analyse logs and connections, and understand who accessed and queried it for the relevant data	John Perkins	by: 11 Apr 3:00 PM	Done	IS John Perkins Senior Security Analyst	11 Apr 11:01 AM
✓	Establish an assessment regarding Fortune100's identity and motives to present it to the CEO	Mattie Carr	by: 11 Apr 5:00 PM	Done	IS John Perkins Senior Security Analyst	11 Apr 11:02 AM
✓	Update executive level with the latest updates	Jessie Soto	by: 11 Apr 12:00 PM	Done	IS John Perkins Senior Security Analyst	11 Apr 11:04 AM

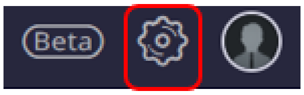
Reminders

☆	Time until CEO assessment	00:00:00
★	Time to next assessment update	01:59:50

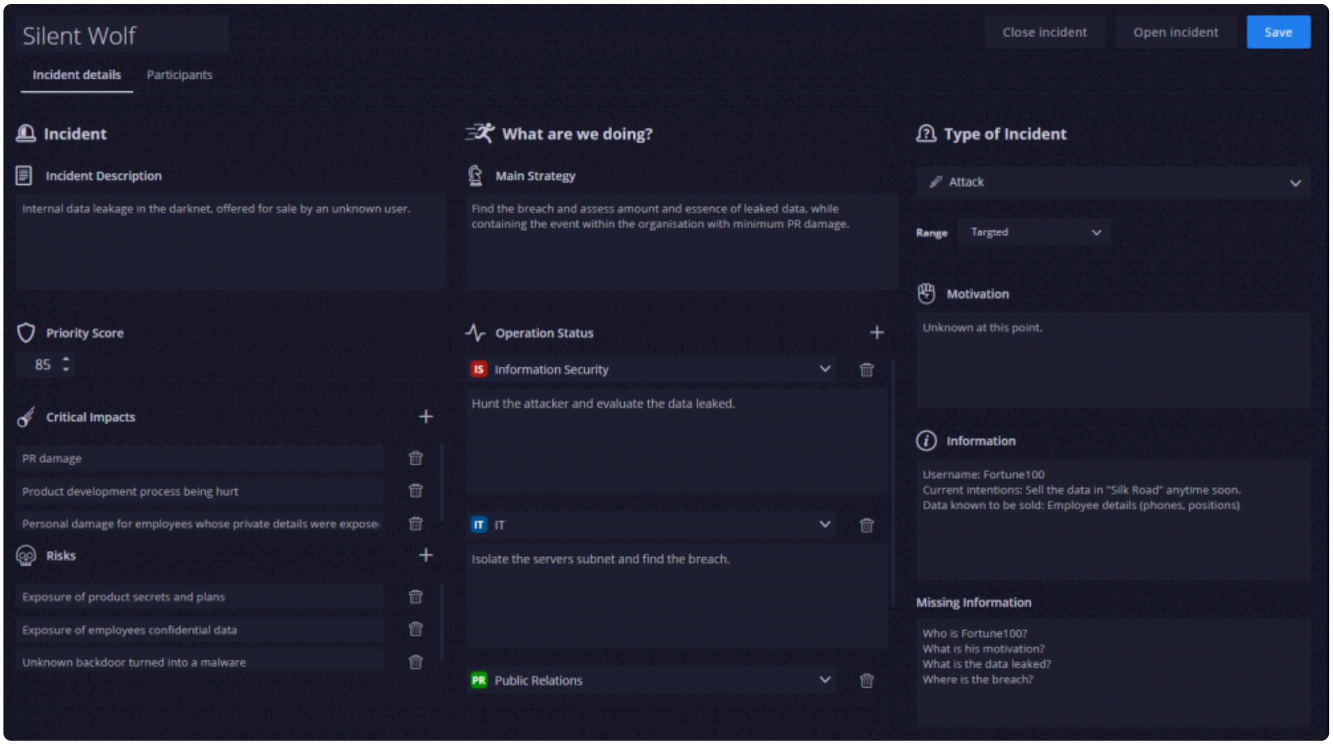
2.5. Update a Critical Incident

An admin user can edit an incident at any time from within the War Room. Often the admin will set a Reminder and ask for status updates. The admin will then use this new information to update the original Incident.

To edit an incident:



1. Click the configuration settings icon at the top of the screen.
2. Select Incident Details.
3. The Incident Details screen appears and is fully editable.
4. Make the required changes and click Save.



Incident

Incident Description

Internal data leakage in the darknet, offered for sale by an unknown user.

Priority Score

85

Critical Impacts

- PR damage
- Product development process being hurt
- Personal damage for employees whose private details were expose

Risks

- Exposure of product secrets and plans
- Exposure of employees confidential data
- Unknown backdoor turned into a malware

What are we doing?

Main Strategy

Find the breach and assess amount and essence of leaked data, while containing the event within the organisation with minimum PR damage.

Operation Status

IS Information Security

Hunt the attacker and evaluate the data leaked.

IT IT

Isolate the servers subnet and find the breach.

PR Public Relations

Type of Incident

Attack

Range Targted

Motivation

Unknown at this point.

Information

Username: Fortune100
Current intentions: Sell the data in "Silk Road" anytime soon.
Data known to be sold: Employee details (phones, positions)

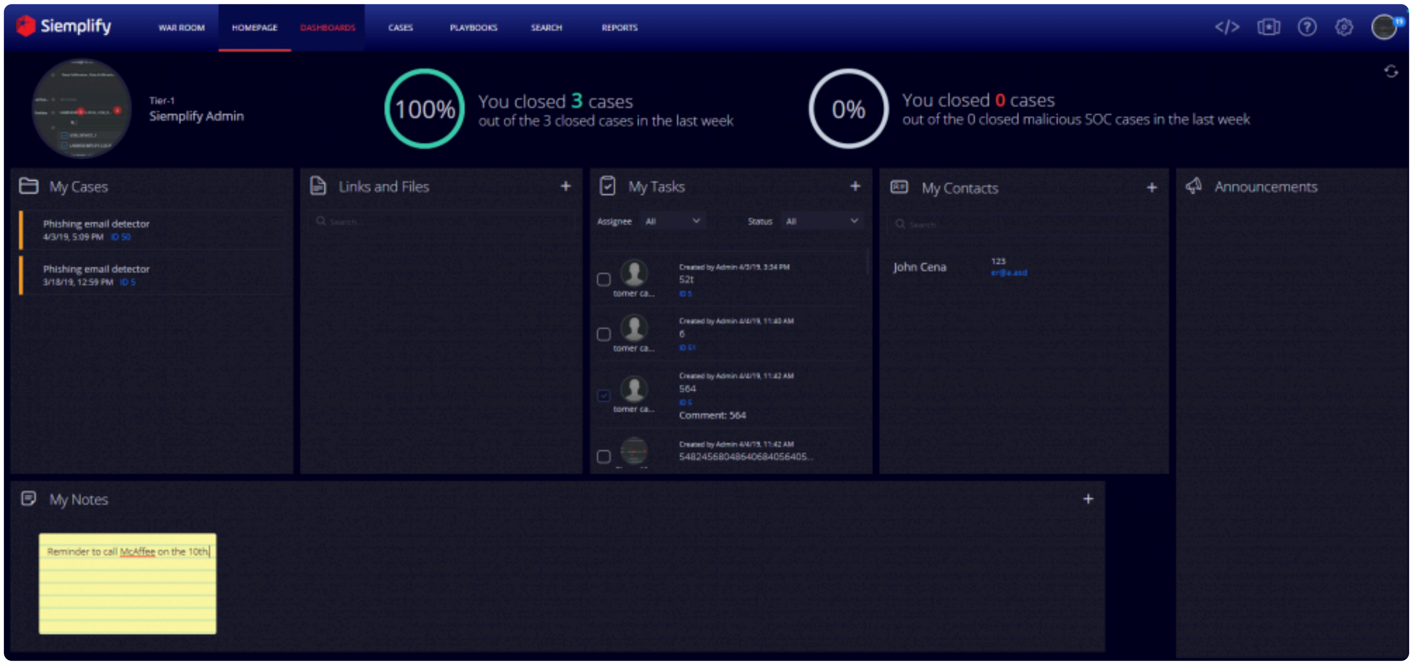
Missing Information

Who is Fortune100?
What is his motivation?
What is the data leaked?
Where is the breach?

3. Homepage

The Homepage displays a list of your open cases, links and files, tasks, contacts, notes, and Announcements arranged in a columnar format. This page allows you to work on your cases and tasks quickly by providing the information you need at your fingertips in a single click. The page also shows the number of cases and malicious SOC cases closed in the previous week.

The Homepage automatically refreshes every two minutes, but you can also refresh it manually by clicking the refresh icon at the top right corner of the page.



Tier-1
Siemplify Admin

100% You closed 3 cases
out of the 3 closed cases in the last week

0% You closed 0 cases
out of the 0 closed malicious SOC cases in the last week

Phishing email detector
4/3/19, 5:09 PM ID 50

Phishing email detector
3/18/19, 12:59 PM ID 5

Assignee: All Status: All

□ Created by Admin 4/3/19, 3:34 PM
52t
ID 5

□ Created by Admin 4/4/19, 11:40 AM
6
ID 51

☑ Created by Admin 4/4/19, 11:42 AM
564
ID 5
Comment: 564

□ Created by Admin 4/4/19, 11:42 AM
548245680486406840564О5...

John Cena 123 er@a.asd

Reminder to call McAffee on the 10th

What can I do on the Homepage?

My Cases: Click on the blue ID of the required case in this section and you will be redirected to the Cases tab.

Links and Files: You can build a clickable list of frequently used URLs (e.g. system admin consoles) and files (e.g. documents, reports, logs, audio and video files) similar to a bookmark in functionality. Click the plus icon underneath either the Links or Files tab to add the required information. Note that files that you add can be downloaded. There is a scroll button to the right of the column to enable support for multiple files and links.

My Tasks: Displays a list of activities that you or your work colleagues need to complete. You can add tasks here for other users – with the option to give them a due date. These tasks are not linked to any case. Once the task is done, click the checkbox to mark it complete.

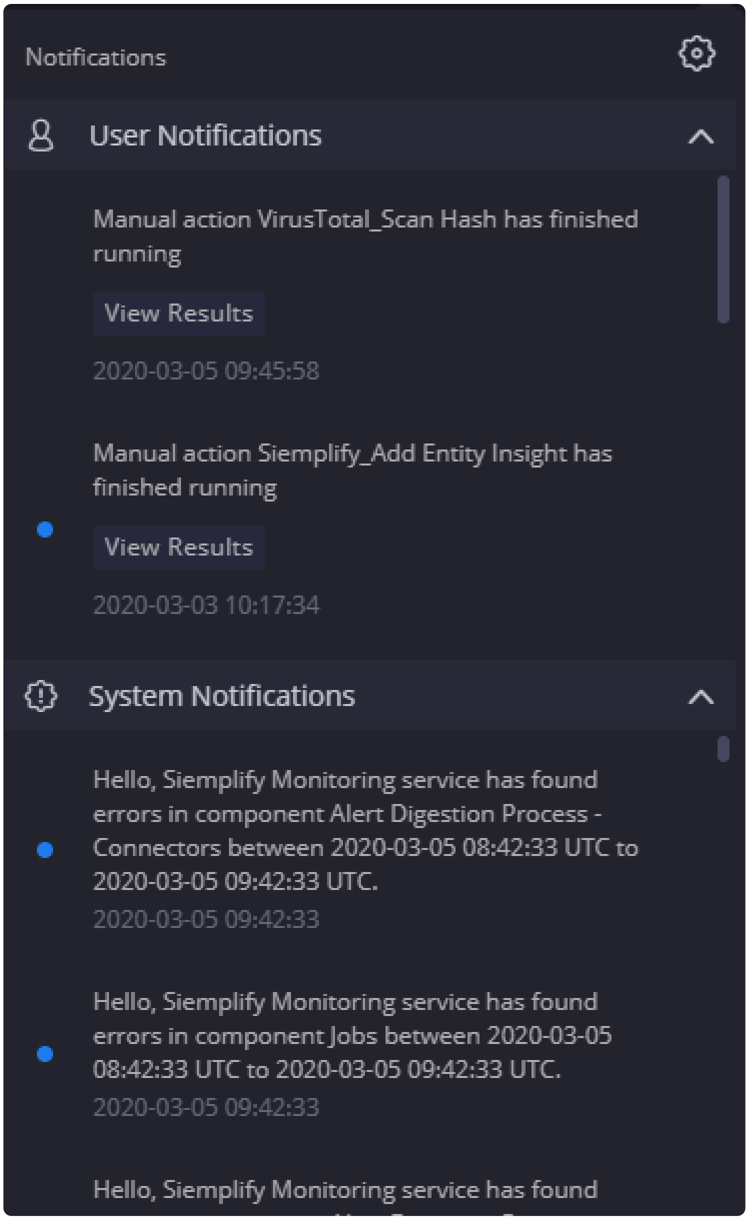
My Contacts: Contains a list of important contacts. You can add here new contacts with their name, phone number and email.

My Notes: Contains a list of post-its to jot down notes. Click the plus icon to add a new note.

Announcements: This is a message feed managed by the SOC manager. Click the plus icon to add a new Announcement to the feed. Note that Announcements cannot be edited once published.

3.1. Notifications

Notifications appear in the bell icon at the top right of the screen. They are composed of both User Notifications and System Notifications. The User notifications consist of messages such as a Playbook waiting for you to answer a question, or if somebody mentioned you on a case. Some of the notifications will have clickable links enabling you to go directly to the relevant place.



Notifications

User Notifications

Manual action VirusTotal_Scan Hash has finished running

2020-03-05 09:45:58

Manual action Siemplify_Add Entity Insight has finished running

2020-03-03 10:17:34

System Notifications

Hello, Siemplify Monitoring service has found errors in component Alert Digestion Process - Connectors between 2020-03-05 08:42:33 UTC to 2020-03-05 09:42:33 UTC.

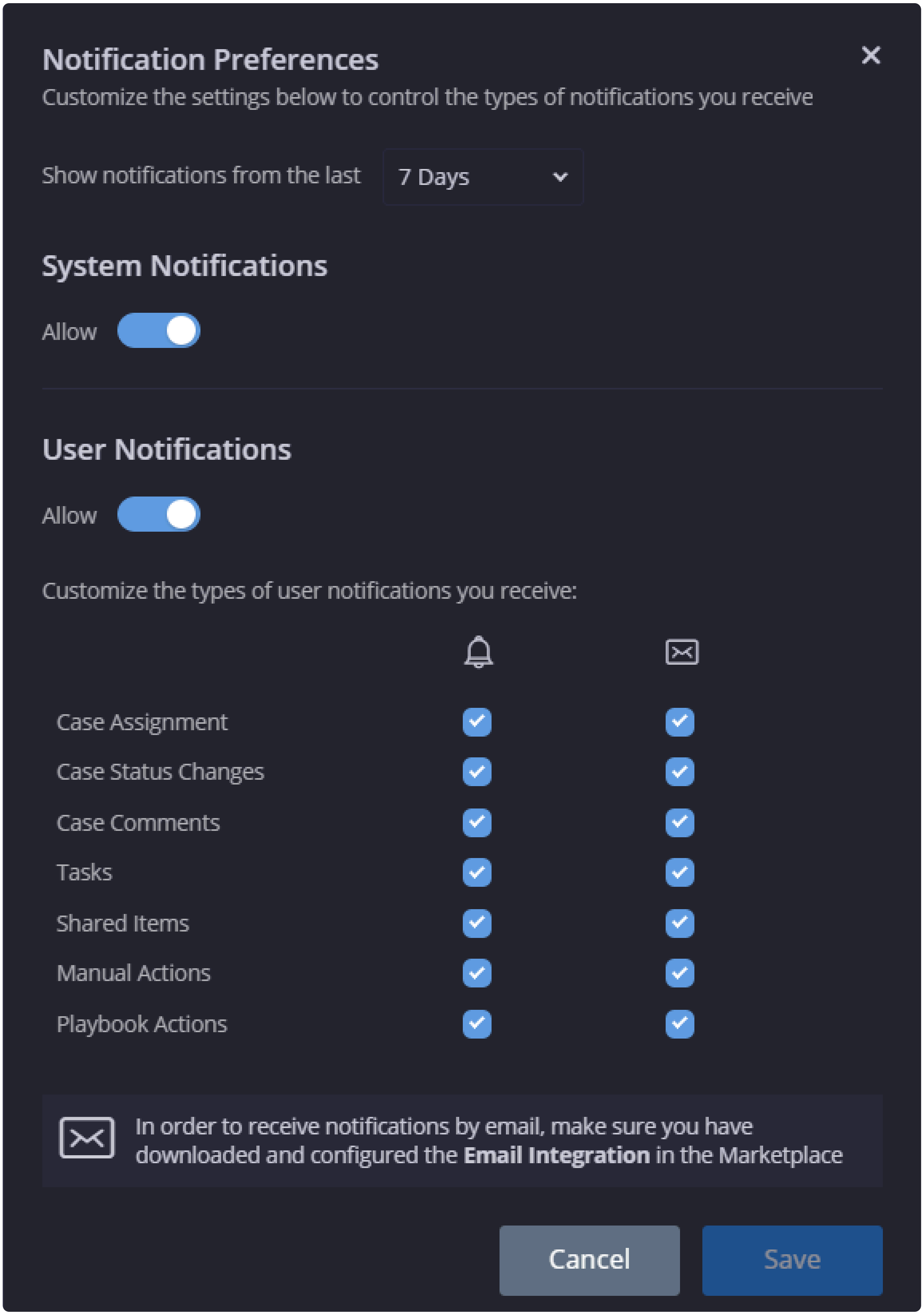
2020-03-05 09:42:33

Hello, Siemplify Monitoring service has found errors in component Jobs between 2020-03-05 08:42:33 UTC to 2020-03-05 09:42:33 UTC.

2020-03-05 09:42:33

Hello, Siemplify Monitoring service has found

You can also choose to configure what type of user notifications you want to receive, and where you want to receive them (Platform and/or Email).



Notification Preferences

Customize the settings below to control the types of notifications you receive

Show notifications from the last 7 Days

System Notifications

Allow

User Notifications

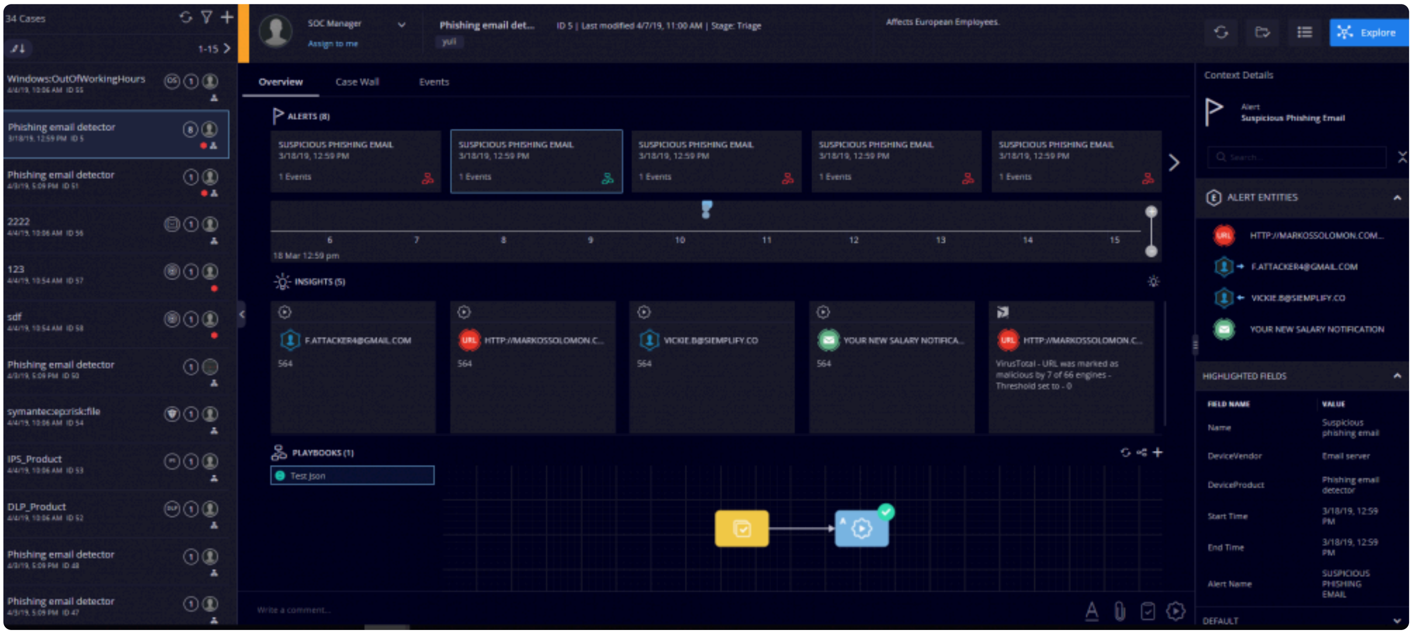
Allow

Customize the types of user notifications you receive:

	🔔	✉
Case Assignment	☑	☑
Case Status Changes	☑	☑
Case Comments	☑	☑
Tasks	☑	☑
Shared Items	☑	☑
Manual Actions	☑	☑
Playbook Actions	☑	☑

In order to receive notifications by email, make sure you have downloaded and configured the **Email Integration** in the Marketplace

4. Case Management



FIELD NAME	VALUE
Name	Suspicious phishing email
DeviceVendor	Email server
DeviceProduct	Phishing email detector
Start Time	3/18/19, 12:59 PM
End Time	3/18/19, 12:59 PM
Alert Name	SUSPICIOUS PHISHING EMAIL

Siemplify ingests alerts from a variety of sources. Each alert is ingested with its underlying base security events. Those security events are analyzed and their indicators (sources, destinations, artifacts etc.) are extracted into objects. Those objects are called Entities. Each entity stored in Siemplify starts collecting data on it (comments, enrichment data, reports etc.) so analysts can review this history when handling future cases the entity appears in. The same entities are also placed on the canvas for the visual representation of the threat.

The Cases tab provides the analysts a way to investigate the incoming security alerts and safeguard workstations. A list of cases that are ingested into the system from the various connectors appear in the left pane of the system. This is also referred to as the Case queue.

The left pane displays a queue of cases with their basic details such as case name, case timestamp, case ID number (unique to a case), number of alerts associated with the case, a thumbnail picture of the analyst handling the case and so on. Cases are generated by alerts from the SIEM platform. Further alerts linked to the same entities may be grouped to an existing case based on a flexible configuration. Refer to Settings > Advanced > Alerts Grouping

The middle plane when on the Overview tab, displays the list of Alerts, Insights (important highlighted information from the Playbook or after executing a manual action) and Playbooks connected to each alert.

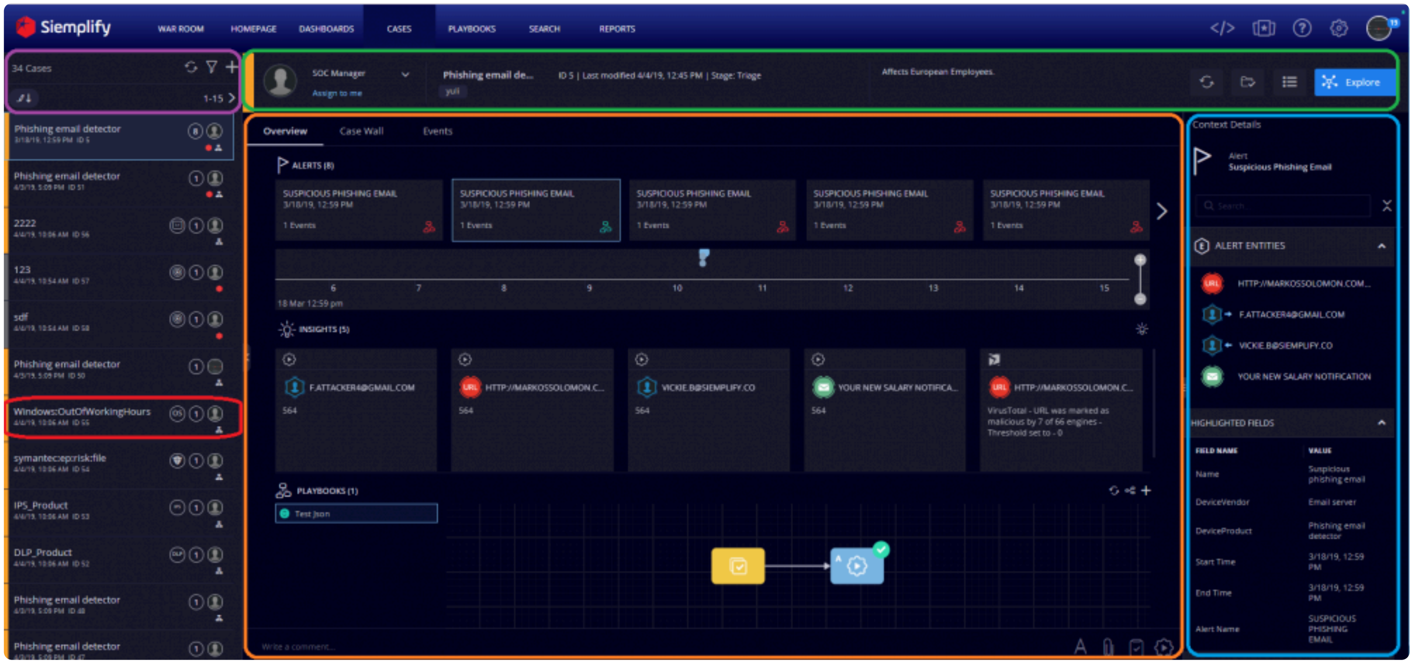
Playbooks are a defined set of actions that gather information about the alerts from internal and external sources and take appropriate decisions on how to proceed with them or conduct an operation on a remote system (i.e. blocking firewall port, disabling active directory user, etc). Siemplify performs these actions automatically or semi automatically based on the playbook triggers upon any alert ingestion.

The right Context Details pane for the Overview tab displays information based on the item you select in the system. For example, if you select a Playbook trigger, the Context Details pane displays the trigger type and its parameters. You can also generate a report in either CSV or PDF format by clicking on the Generate Report icon on the top right of the screen.

> ✻ You can see up to 15 cases at one time. Use the system navigational arrows available on the left pane to move across cases.

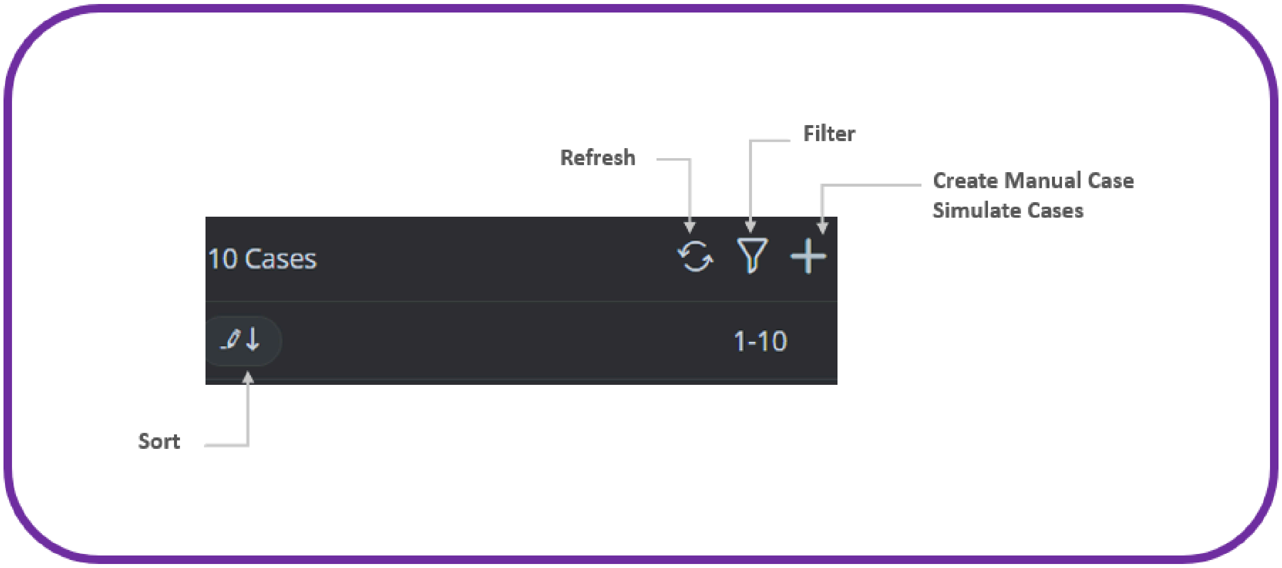
You can refresh the case queue items regularly, sort them as required, use filters to narrow your case queue items, add cases to the existing queue and close cases.

4.1. What’s on the Cases screen?



Case Options

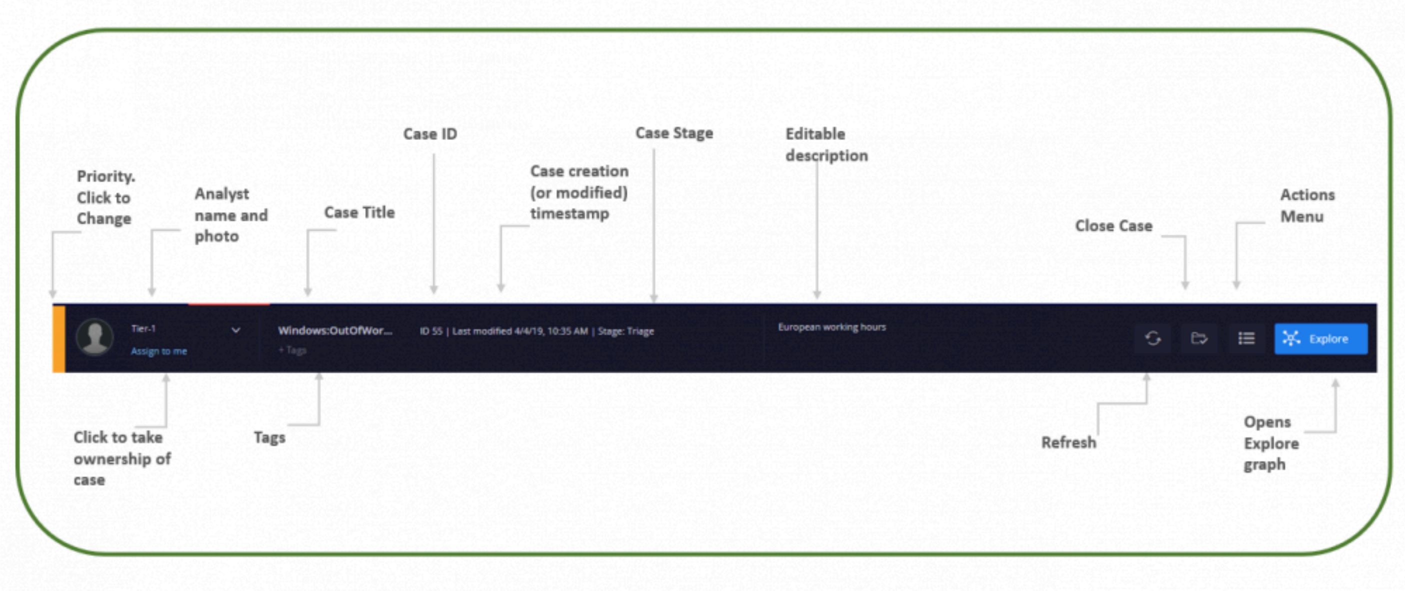
For more information on the case options below, refer to Case Options.



Top Bar

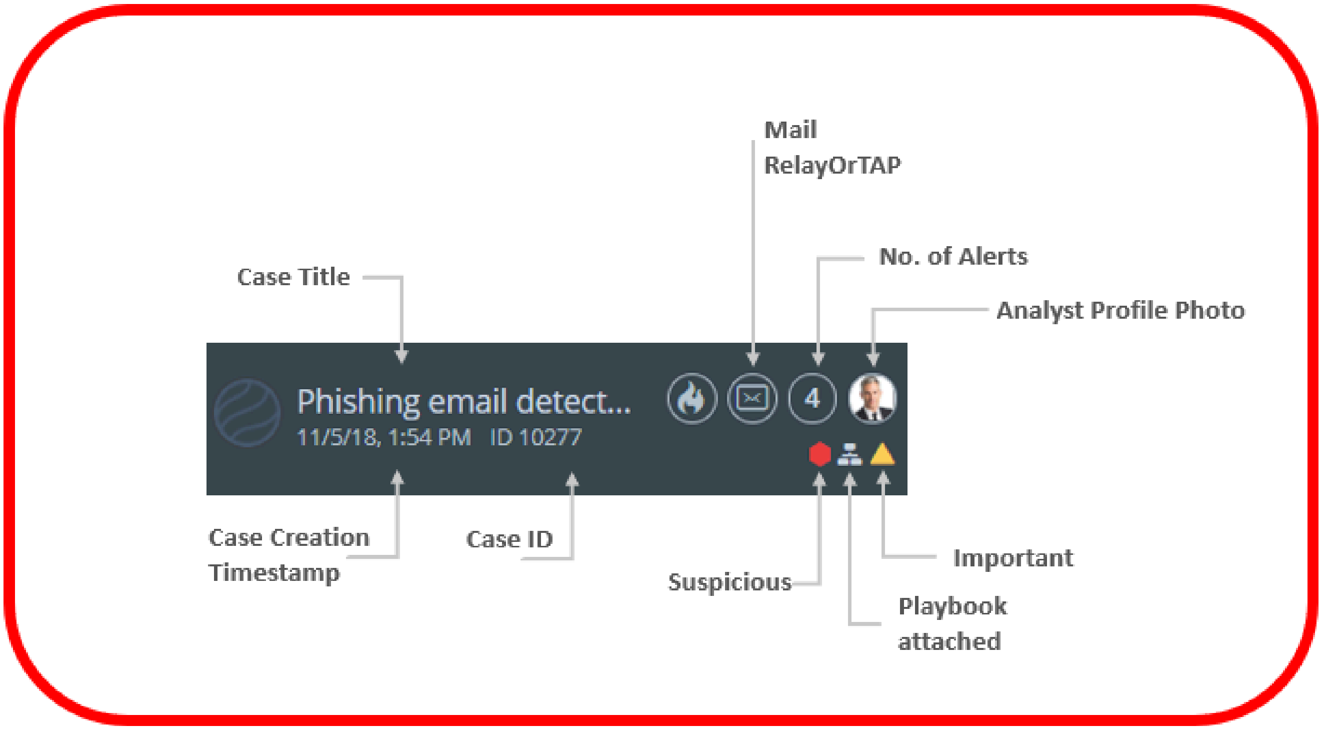
For more information on the Actions menu, refer to Actions Menu

For more information on Explore, refer to Explore Cases



Case Cards

Note that the screen may appear differently depending on the case.



Main Area of Screen

For more information on Overview, refer to Overview Tab

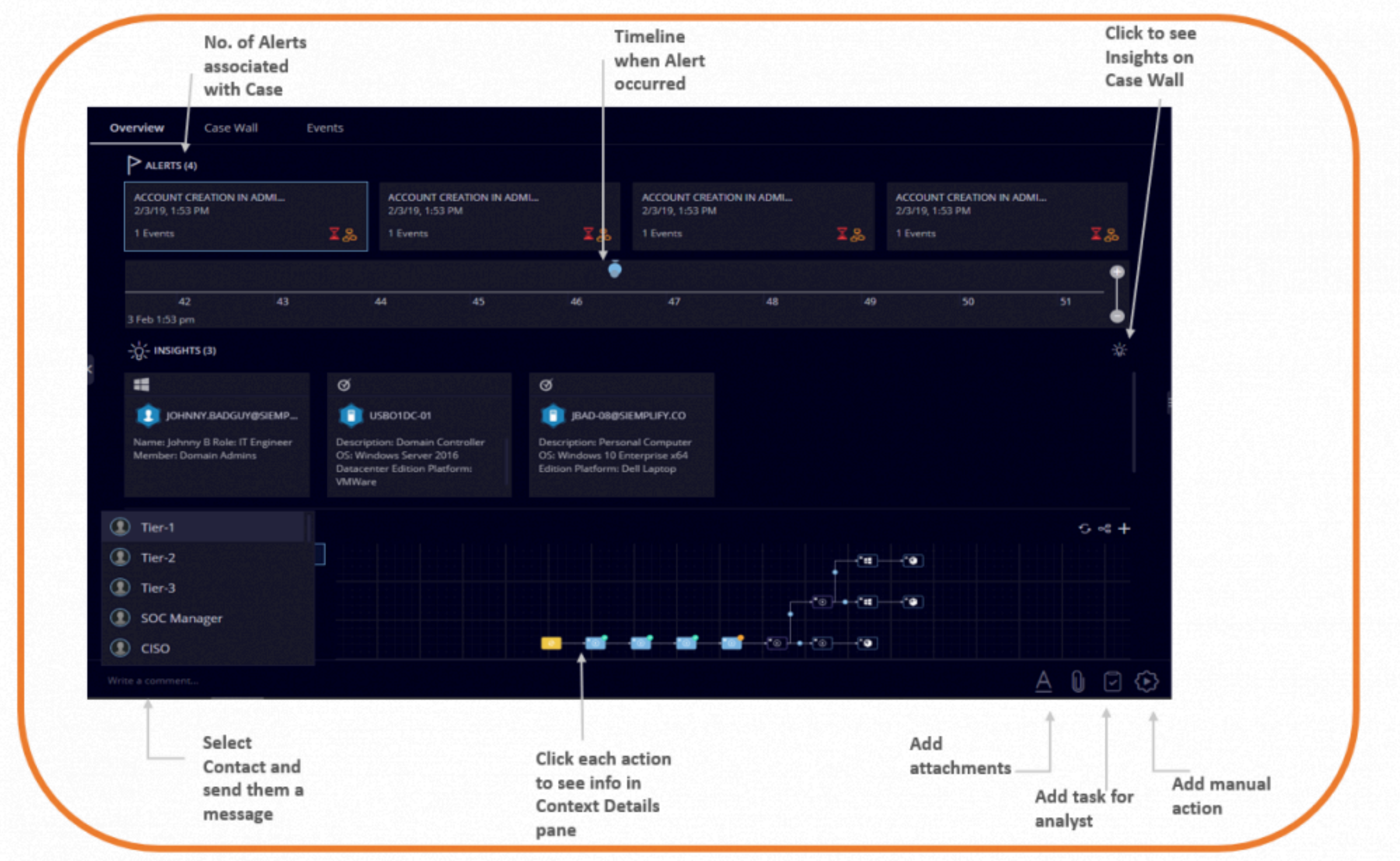
For more information on Case Wall, refer to Case Wall Tab

For more information on Events, refer to Events Tab

For more information on Entities, refer to Entities

For more information on Playbooks, refer to Playbooks

For more information on Manual Actions, refer to Manual Actions



ACCOUNT CREATION IN ADMI...
2/3/19, 1:53 PM
1 Events

ACCOUNT CREATION IN ADMI...
2/3/19, 1:53 PM
1 Events

ACCOUNT CREATION IN ADMI...
2/3/19, 1:53 PM
1 Events

ACCOUNT CREATION IN ADMI...
2/3/19, 1:53 PM
1 Events

JOHNNY.BADGUY@SIEMP...
Name: Johnny B Role: IT Engineer
Member: Domain Admins

USBO1DC-01
Description: Domain Controller
OS: Windows Server 2016
Datacenter Edition Platform:
VMWare

JBAD-08@SIEMPLIFY.CO
Description: Personal Computer
OS: Windows 10 Enterprise x64
Edition Platform: Dell Laptop

No. of Alerts associated with Case

Timeline when Alert occurred

Click to see Insights on Case Wall

Select Contact and send them a message

Click each action to see info in Context Details pane

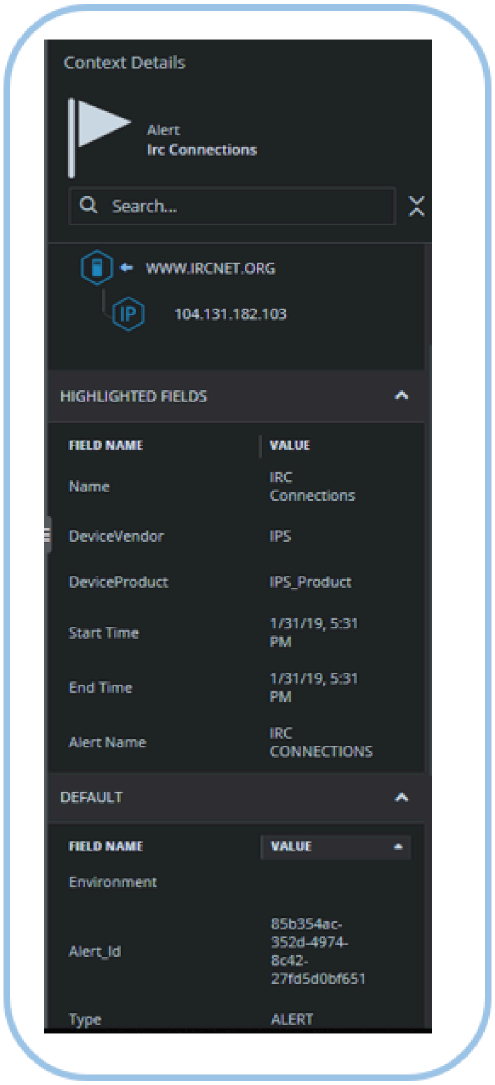
Add attachments

Add task for analyst

Add manual action

Context Details

For more information on Context Details, please refer to Context Details



Context Details

Alert
Irc Connections

WWW.IRCNET.ORG

104.131.182.103

HIGHLIGHTED FIELDS

FIELD NAME	VALUE
Name	IRC Connections
DeviceVendor	IPS
DeviceProduct	IPS_Product
Start Time	1/31/19, 5:31 PM
End Time	1/31/19, 5:31 PM
Alert Name	IRC CONNECTIONS

DEFAULT

FIELD NAME	VALUE
Environment	
Alert_Id	85b354ac-352d-4974-8c42-27fd5d0bf651
Type	ALERT

4.1.1. Actions Menu

The Actions menu contains the following options:

- Escalate
- Mark as Important
- Incident
- Stage
- Priority
- Report
- Close Case (next to the Action menu)

Escalate

You can escalate a case (if it’s assigned to you) to the next tier user as per the organizational hierarchy:

1. Select a case from the queue, then choose ☰ > Escalate in the top right corner of the screen.
2. In Escalate Case, type a valid reason for escalating the case. The reason will be posted on the Case Wall.
3. Click Submit. The case is escalated to the next level tier.

Mark as Important

When an analyst wants to highlight a case, they can mark it as important via ☰ > Mark as Important in the top right corner of the screen. A yellow triangle icon is then displayed with the case. The analyst can also remove the Important tag if required from the same menu.

Incident

When a case is considered extremely crucial and needs immediate attention, the analyst can mark it as an incident. Raising an incident sets the case priority to critical, changes the case stage to Incident, assigns the case to the SOC Manager and a notification is sent to all analysts.

To mark a case that is assigned to you as an Incident:

1. Select a case from the queue, then choose ☰ > Incident in the top right corner of the screen.
2. Click Yes in the Confirmation dialog box.

Stage

You can change a case stage, if it’s assigned to you, based on your organizational case management methods.

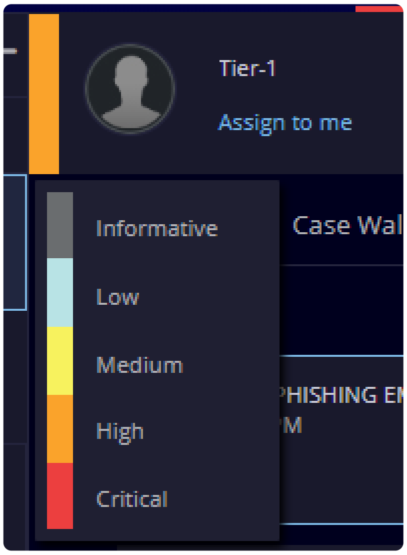
1. Select a case from the queue, then choose ☰ > Stage in the top right corner of the screen.
2. Select a stage from the following:
    - Triage - Default and the initial phase of a case once it is created.

   - Assessment - The case is assigned to the next tier for assessment.
   - Investigation - The case is assigned for further investigation of the alerts and entities involved.
   - Improvement - Can mark case as Improvement as a reminder to improve SOC rules or for further investigation after the analysts have finished handling it.
   - Research - The case is further researched for factors such as how the external entities got into your organization and so on.
   - Incident - The last phase of the case where it becomes crucial. After marking a case as an incident, you cannot revert/change it to any other stage.
3. Click Save.

Priority

You can change the priority of a case based on the importance with which it must be handled.

1. Select a case from the queue, then click ☰ > Priority in the top right corner of the screen.
2. Select a priority from the following. Note that each priority is represented by the following colors:
   - Informative (grey)
   - Low (blue)
   - Medium (yellow)
   - High (orange)
   - Critical (red)
3. Click Ok. The case priority is changed.
4. You can also click the color directly on the top bar and change it from there.



Report

You can download a report as a Word document which contains the following information:

- Case details
- Alerts, entities and insights of the case
- User and system activities on the case
- Playbook action and Case Activity

1. Select a case from the queue, then click ☰ > Report in the top right corner of the screen.
2. Open the downloaded Word document to see the results.

Close Case

You can close a case once it’s resolved.

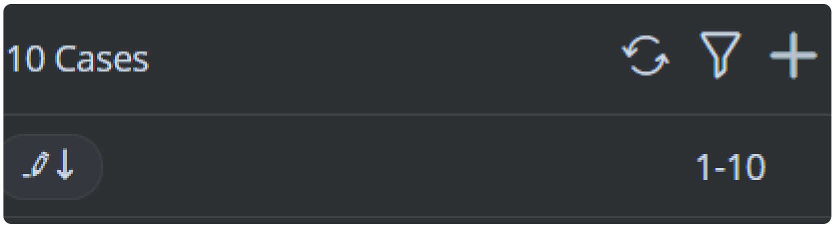
1. Select a case from the queue, then click 📂 in the top right corner of the screen.
2. In the Close Case popup, select a valid reason and a root cause for closing the case and type any additional comments. These will be posted on the Case wall.
3. Click Close.

> You can also close a case from the queue itself, by clicking on the three vertical dates to the right of the case in the Case Queue and clicking on Close Case. The Close Case dialog box will appear as above.

4.1.2. Case Options

The following options are available:

- Refresh
- Sort
- Filter
- Create Manual Case
- Simulate Case



Sort

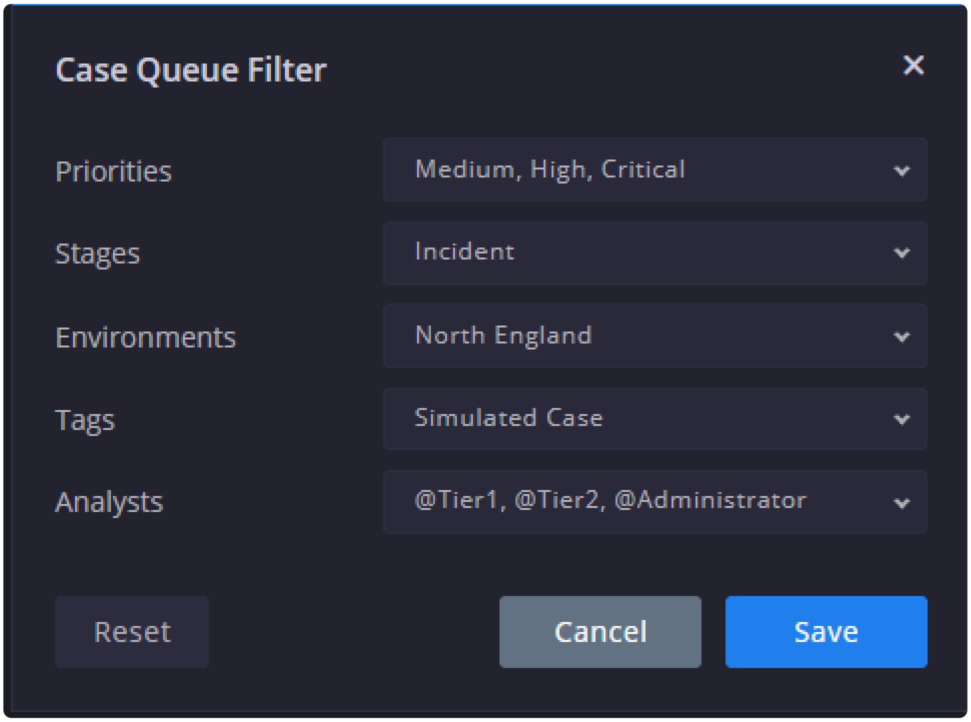
Sort cases in the queue based on the following options:

- Descending order of case ID numbers
- Ascending order of case ID numbers
- Newest to oldest based on the time they were created
- Oldest to newest based on the time they were created
- Newest to oldest based on the time they were modified
- Oldest to newest based on the time they were modified
- Highest priority to the lowest priority
- Lowest priority to the highest priority
- Case that took the longest SLA time to resolve followed by the ones with the shortest SLA time
- Case that took the shortest SLA time to resolve alerts followed by the ones with the longest SLA time

Apply Filter

Filters enable you to narrow your case search in the queue.
To apply a filter:

1. Click the filter icon to specify filters.
2. You can select several options from the following parameters: Analysts, Tags, Environments, Priorities, Stages. If you want to clear the filters, click the Reset button.



Case Queue Filter

Priorities: Medium, High, Critical

Stages: Incident

Environments: North England

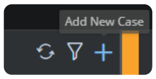
Tags: Simulated Case

Analysts: @Tier1, @Tier2, @Administrator

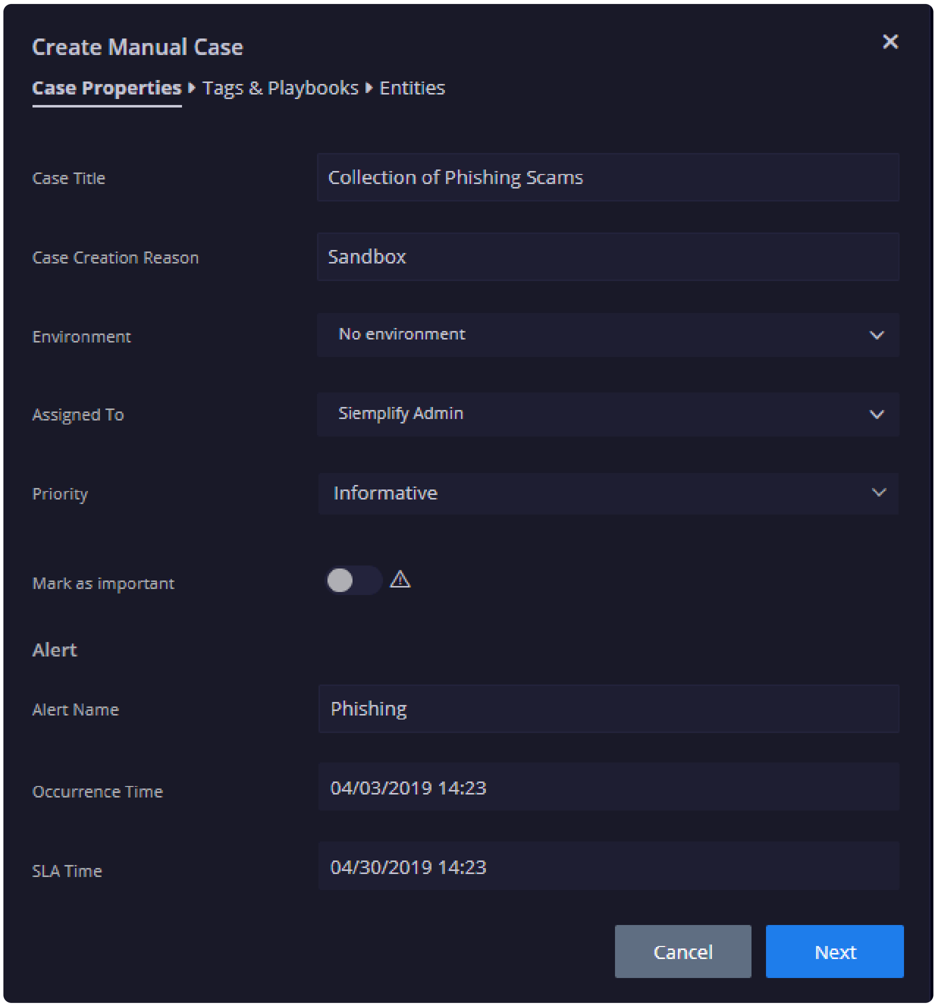
3. Click Save.

Create Manual Case

You have the option to manually create a case. This can be useful in staging environments or for trial purposes.

1. Click the plus icon  and select Create Manual Case.

2. In Case Properties, specify the following:
   - **Case Title**: Title for the new case.
   - **Case Creation Reason**: Type a reason for creating the case.
   - **Environment**: Select the specific environment being monitored. The default is No Environment.
   - **Assigned To**: Assign the case to a specific role/user.
   - **Priority**: Set a priority for the case based on the preference with which the case has to be handled.
   - **Mark as Important**: Toggle between the keys to mark a case as important or not important as required.
   - **Alert Name**: Type a name for the security alert.
   - **Occurrence Time**: Specify the date and time of the occurrence of the alert (using the calendar).
   - **SLA**: Specify a date and time within which the SOC team commits to resolve the alert in the case.



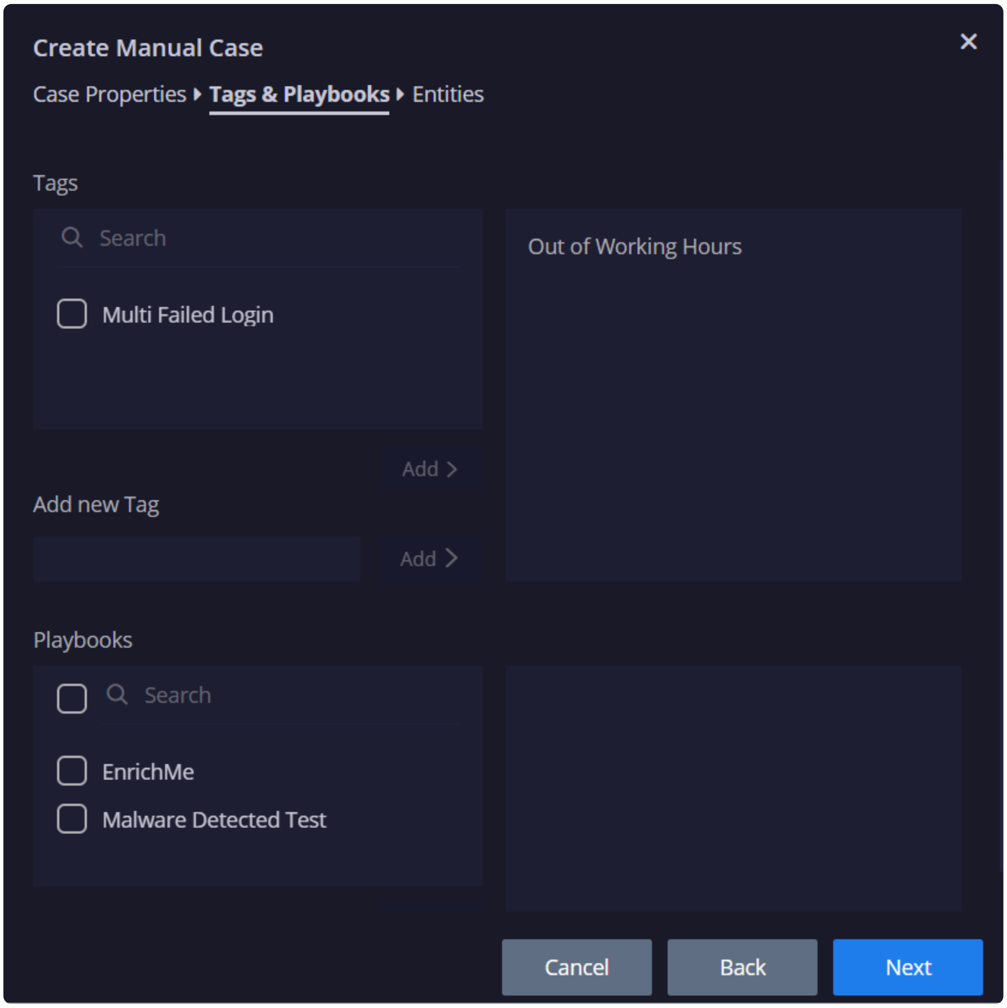
Create Manual Case

Case Title	Collection of Phishing Scams
Case Creation Reason	Sandbox
Environment	No environment
Assigned To	Siemplify Admin
Priority	Informative
Mark as important	○

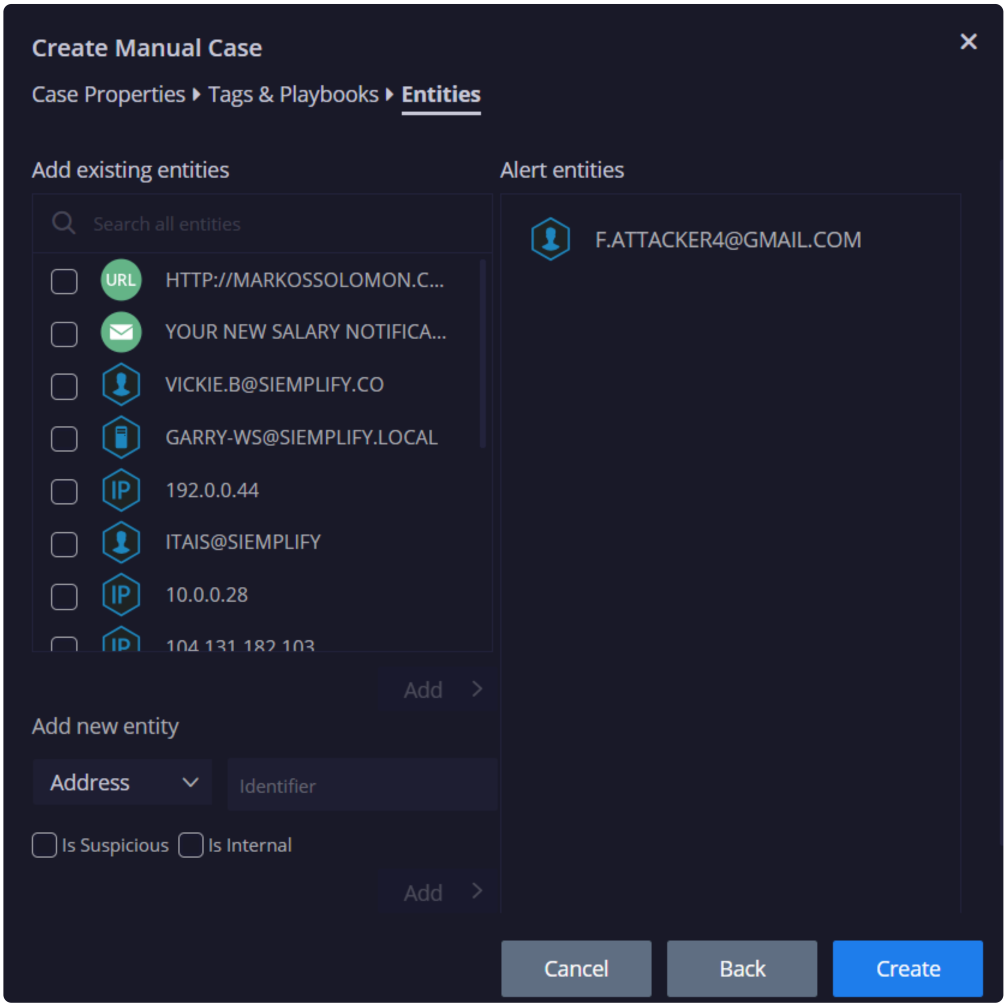
Alert

Alert Name	Phishing
Occurrence Time	04/03/2019 14:23
SLA Time	04/30/2019 14:23

3. Click Next when done.
4. In the Tags and Playbooks screen, select the required tags and playbooks and add them to the right column. You can also create a new tag in this dialog box if needed.



5. Click Next when done.
6. In the Entities screen, select any required existing entities and add them to the right column.
7. If required, you can add an entirely new identity with a corresponding identifier. You can choose to mark the entity as suspicious which marks them in red in the display. You can also choose to mark them as part of the organization's internal network. Make sure to Add them to the right column after defining them.



Create Manual Case

Case Properties ▸ Tags & Playbooks ▸ **Entities**

Add existing entities

Search all entities

- □ URL HTTP://MARKOSSOLOMON.C...
- □ YOUR NEW SALARY NOTIFICA...
- □ VICKIE.B@SIEMPLIFY.CO
- □ GARRY-WS@SIEMPLIFY.LOCAL
- □ IP 192.0.0.44
- □ ITAIS@SIEMPLIFY
- □ IP 10.0.0.28
- □ IP 104.131.182.103

Add >

Add new entity

Address | Identifier

□ Is Suspicious □ Is Internal

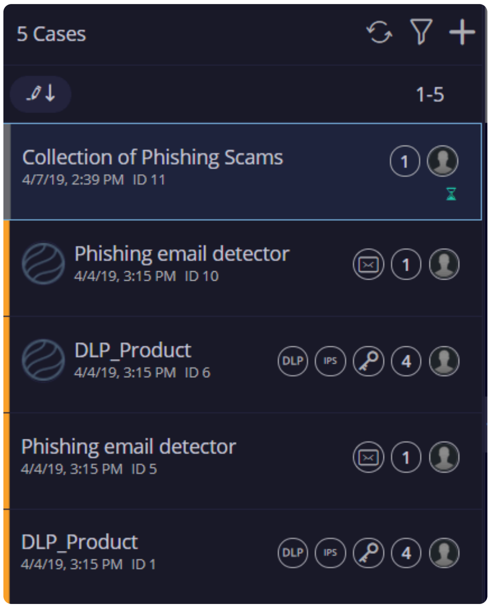
Add >

Alert entities

F.ATTACKER4@GMAIL.COM

8. Click Create.

   The new case now appears in the case queue with all the details displayed.



5 Cases

1-5

Collection of Phishing Scams
4/7/19, 2:39 PM ID 11 — 1

Phishing email detector
4/4/19, 3:15 PM ID 10 — 1

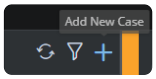
DLP_Product
4/4/19, 3:15 PM ID 6 — DLP IPS 4

Phishing email detector
4/4/19, 3:15 PM ID 5 — 1

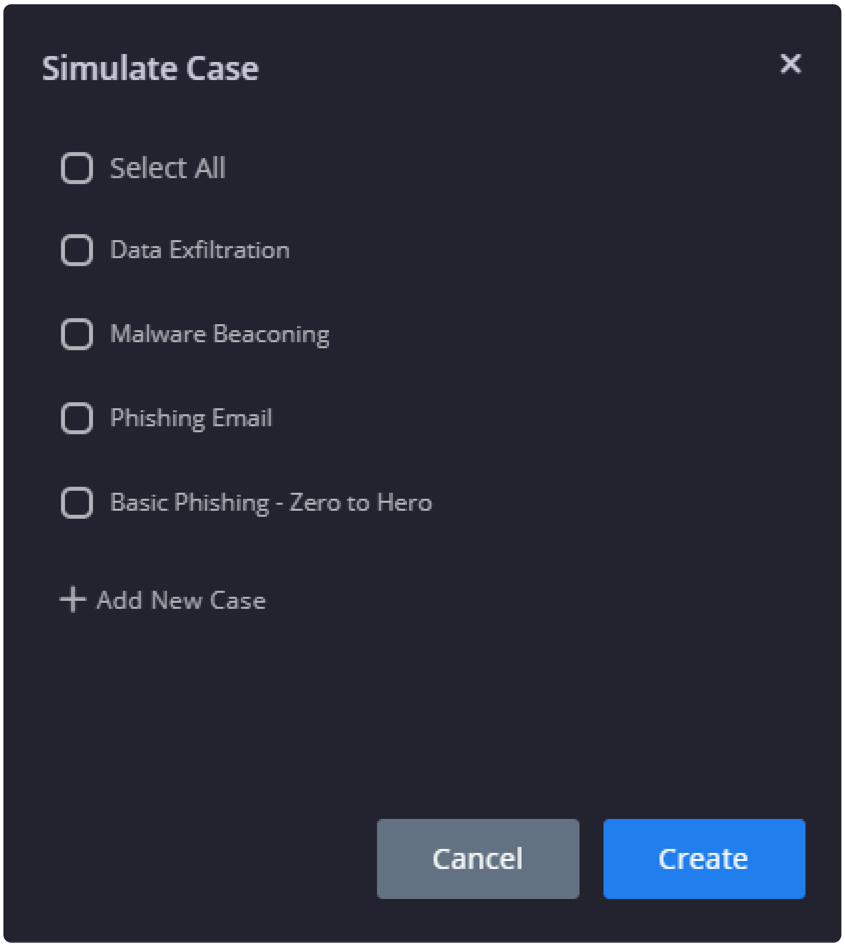
DLP_Product
4/4/19, 3:15 PM ID 1 — DLP IPS 4

Simulate Case

You have the option to create a “ready made case” by simulating a case populated with system default alerts. This can be useful for example when you want to test a new playbook on a case that includes existing alerts.

1. Click the plus icon  and select Simulate Cases.

2. Select the requested simulated attacks or any use cases that you have downloaded from the Marketplace and click Create.



Simulate Case

□ Select All

□ Data Exfiltration

□ Malware Beaconing

□ Phishing Email

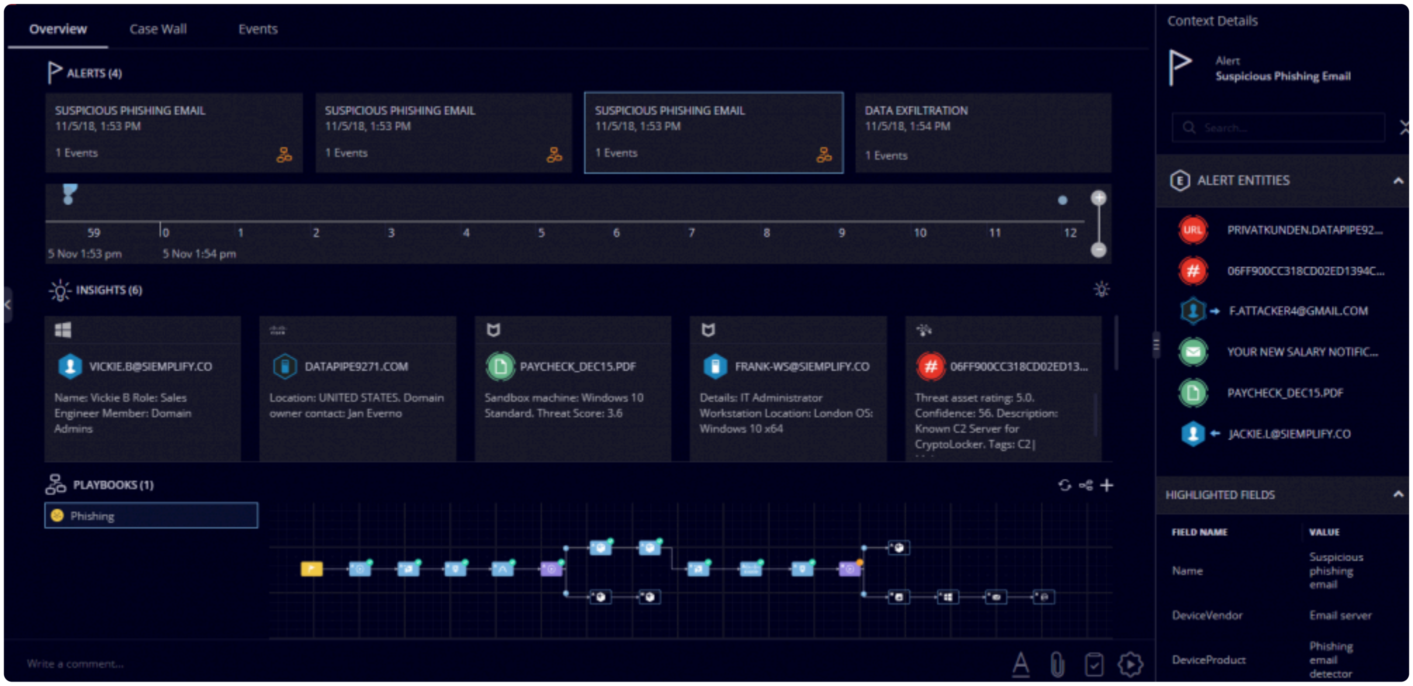
□ Basic Phishing - Zero to Hero

3. Next, select the required environment (or no environment at all) and click Simulate. The new case will appear in the queue.

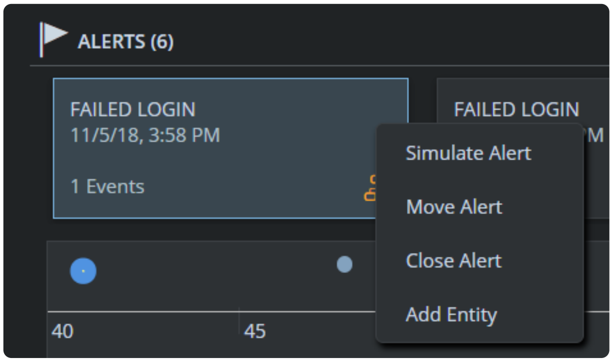
4.1.3. Overview Tab

The Overview tab provides a comprehensive glance at the Case in your system. The screen includes all the alerts that comprise your case, the timeline that they occurred, any warnings or Insights generated by the

Alerts. playbooks associated with each alert, as well as a context sensitive Context Details which display information on whatever is highlighted.


Overview
Case Wall
Events
ALERTS (4)
SUSPICIOUS PHISHING EMAIL
11/5/18, 1:53 PM
1 Events
SUSPICIOUS PHISHING EMAIL
11/5/18, 1:53 PM
1 Events
SUSPICIOUS PHISHING EMAIL
11/5/18, 1:53 PM
1 Events
DATA EXFILTRATION
11/5/18, 1:54 PM
1 Events
5 Nov 1:53 pm
5 Nov 1:54 pm
INSIGHTS (6)
VICKIE.B@SIEMPLIFY.CO
Name: Vickie B Role: Sales Engineer Member: Domain Admins
DATAPIPE9271.COM
Location: UNITED STATES. Domain owner contact: Jan Everno
PAYCHECK_DEC15.PDF
Sandbox machine: Windows 10 Standard. Threat Score: 3.6
FRANK-WS@SIEMPLIFY.CO
Details: IT Administrator Workstation Location: London OS: Windows 10 x64
06FF900CC318CD02ED13...
Threat asset rating: 5.0. Confidence: 56. Description: Known C2 Server for CryptoLocker. Tags: C2 |
PLAYBOOKS (1)
Phishing
Write a comment...
Context Details
Alert
Suspicious Phishing Email
Search...
ALERT ENTITIES
PRIVATKUNDEN.DATAPIPE92...
06FF900CC318CD02ED1394C...
F.ATTACKER4@GMAIL.COM
YOUR NEW SALARY NOTIFIC...
PAYCHECK_DEC15.PDF
JACKIE.L@SIEMPLIFY.CO
HIGHLIGHTED FIELDS
FIELD NAME
VALUE
Name
Suspicious phishing email
DeviceVendor
Email server
DeviceProduct
Phishing email detector

In the Alerts section at the top, hover over an Alert to display the Action icon ⋮ and the corresponding dropdown list.



The following actions are displayed:

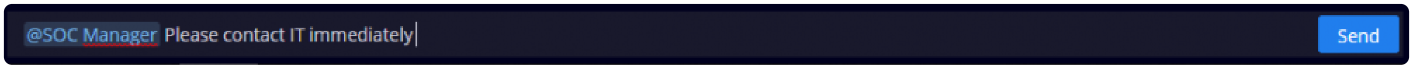
- **Simulate Alert**: Clone an alert. It re-ingests the alert for testing purposes. None of the information and metrics from simulated alerts are counted in the dashboards and reports metrics. Simulated alerts will not be grouped by design.
- **Move Alert**: When assigned to you, you can move the alert to a new separate case in the Case Queue.
- **Close Alert**: Close the specific Alert while keeping the Case open.
- **Add Entity**: Manually add an entity to the specific Alert. Let’s look at a quick user case for this.

1. Alert is titled IRC Connections. This means somebody within the organization has tried to access this website.
2. Click on the relevant trigger in the Playbook, in this case, CiscoUmbrella_GetWhoIs.
3. In the Context Details pane on the right, copy the email address of the User.
4. Click Add Entity. The new entity will appear in the Context Details of the Case, and of this specific alert.
5. Click Save.

- In the Timeline section, use the plus/minus buttons to scale the timeline.
- In the Playbooks section, you can click on each trigger and each action to see full details and information on the Context Details pane.

Send Message to Specific User

At the bottom of the screen, type the @ button and then select either an individual Analyst or a User Group to send a message to. Click Send after you've written the message. The message will appear in the User's notification list.



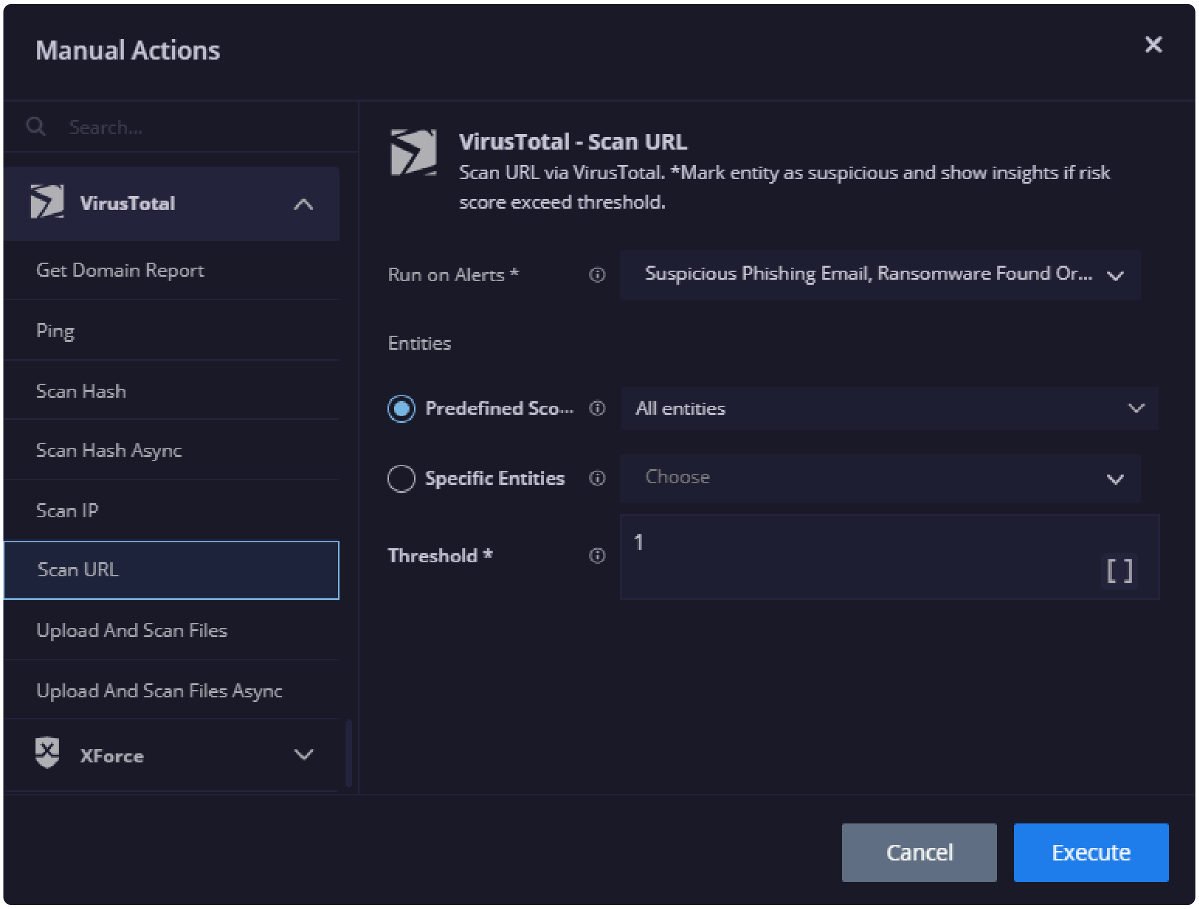
@SOC Manager Please contact IT immediately

Manual Actions

Both the Manual actions and the Actions that appear in the Playbook are populated after you download the corresponding integration in the Marketplace.

To perform a manual action:

1. In the highlighted case, click ⚙ icon on the bottom right of the screen. (If you don't see this icon, adjust your zoom accordingly). The Manual Action screen displays.
2. Select the required Action. For example, select Virus Total > Scan URL. Make sure to fill in the required information.



VirusTotal - Scan URL

Scan URL via VirusTotal. *Mark entity as suspicious and show insights if risk score exceed threshold.

Run on Alerts *: Suspicious Phishing Email, Ransomware Found Or...

Entities

● Predefined Sco...: All entities

○ Specific Entities: Choose

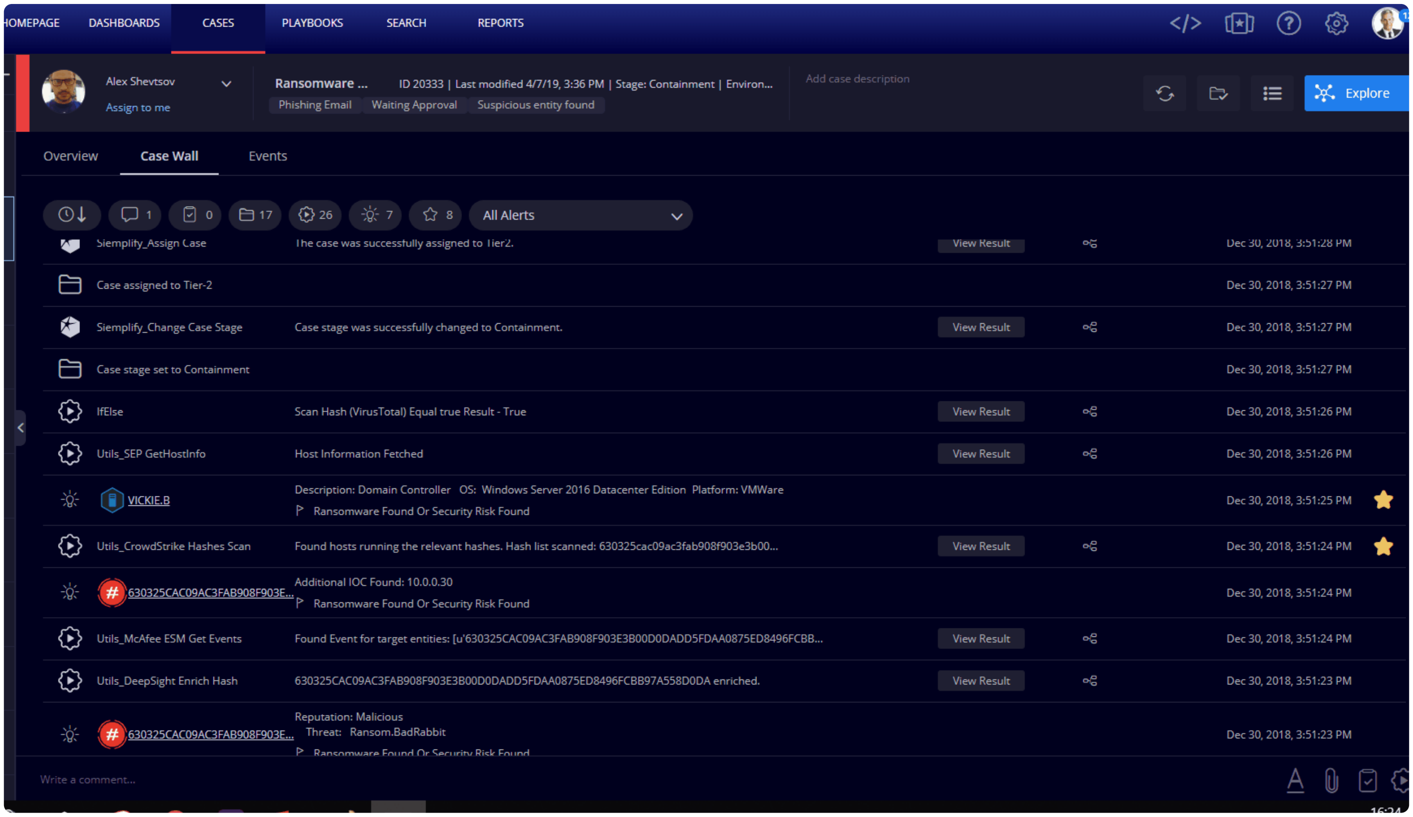
Threshold *: 1

3. Select the Alerts and Entities that you want the action to run on. Click Execute. The action details will appear in the context details and will be documented on the Case wall.

4.1.4. Case Wall Tab

Case Wall is a repository of all event logs related to a case since the time the case was created until it is closed. Click the Case Wall tab to view information on the tasks, user comments, manual and system actions, file attachments, insights and so on, related to a case. Each of them are indicated by icons located at the top segment of the Case Wall tab.

Click on View Results where displayed to see both the regular UI results and the JSON Results.



Ransomware ... ID 20333 | Last modified 4/7/19, 3:36 PM | Stage: Containment | Environ...

Phishing Email · Waiting Approval · Suspicious entity found

Siemplify_Assign Case	The case was successfully assigned to Tier2.	View Result	Dec 30, 2018, 3:51:28 PM
Case assigned to Tier-2			Dec 30, 2018, 3:51:27 PM
Siemplify_Change Case Stage	Case stage was successfully changed to Containment.	View Result	Dec 30, 2018, 3:51:27 PM
Case stage set to Containment			Dec 30, 2018, 3:51:27 PM
IfElse	Scan Hash (VirusTotal) Equal true Result - True	View Result	Dec 30, 2018, 3:51:26 PM
Utils_SEP GetHostInfo	Host Information Fetched	View Result	Dec 30, 2018, 3:51:26 PM
VICKIE.B	Description: Domain Controller OS: Windows Server 2016 Datacenter Edition Platform: VMWare Ransomware Found Or Security Risk Found		Dec 30, 2018, 3:51:25 PM
Utils_CrowdStrike Hashes Scan	Found hosts running the relevant hashes. Hash list scanned: 630325cac09ac3fab908f903e3b00...	View Result	Dec 30, 2018, 3:51:24 PM
630325CAC09AC3FAB908F903E...	Additional IOC Found: 10.0.0.30 Ransomware Found Or Security Risk Found		Dec 30, 2018, 3:51:24 PM
Utils_McAfee ESM Get Events	Found Event for target entities: [u'630325CAC09AC3FAB908F903E3B00D0DADD5FDAA0875ED8496FCBB...	View Result	Dec 30, 2018, 3:51:24 PM
Utils_DeepSight Enrich Hash	630325CAC09AC3FAB908F903E3B00D0DADD5FDAA0875ED8496FCBB97A558D0DA enriched.	View Result	Dec 30, 2018, 3:51:23 PM
630325CAC09AC3FAB908F903E...	Reputation: Malicious Threat: Ransom.BadRabbit Ransomware Found Or Security Risk Found		Dec 30, 2018, 3:51:23 PM

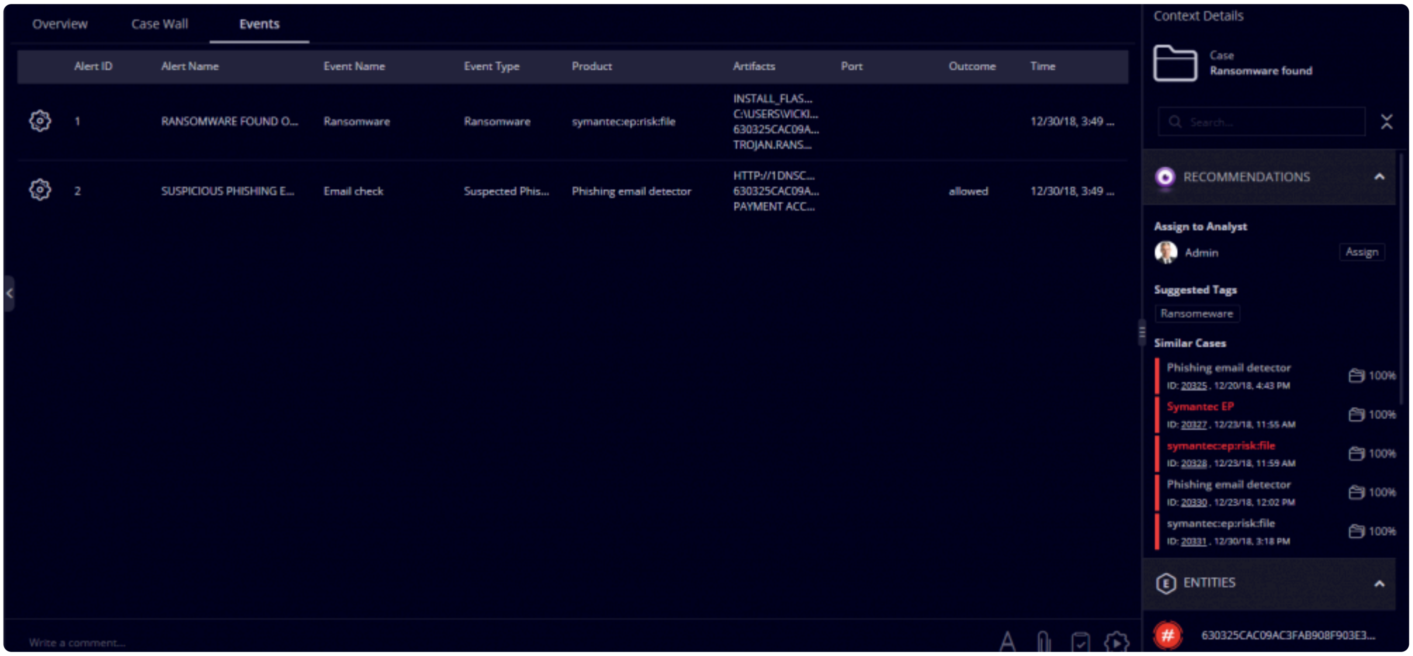
Click on one or more of the following event icons to view their details. You can select an alert from the drop-down menu (located beside the event icons) for which you want to see the related events. To view events for all the alerts of the case, select All Alerts.

Icons	Description
🕓↓	Sorts event logs based on the time they were created (from the newest to the oldest, and vice versa).
💬 2	Displays any useful comments (pertaining to alerts) that were left by the users while handling the case – including number of comments.
📋 0	Displays details on tasks. Once the task is completed, click Complete Task. The task status displays Completed with the completion timestamp followed by your comments.
🗀 17	Displays the details of all status changes of a case carried out by users or the system in a tabular form. These changes include updating case title, case stages, priority, case assignment to a different user, case closure and so on.
⚙ 6	Displays the details of actions assigned to each alert in a tabular form. Details include the action timestamp, action name, alert name, the status of the action taken (Completed or Faulted) and its result. Note: Click Show More to expand the view of the action results, involved parameters and entities

	in a tabular form. To collapse the view, click Show Less.
💡 0	Displays any warnings and general insights about the case and the involved entities.
☆ 1	Displays case wall items that you have previously favorited (by clicking the yellow star on the right).

4.1.5. Events Tab

Click the Events tab to view a list of events and their basic details in a tabular form. The right Context Details pane for the Events tab displays raw data of the selected event.



	Alert ID	Alert Name	Event Name	Event Type	Product	Artifacts	Port	Outcome	Time
⚙	1	RANSOMWARE FOUND O...	Ransomware	Ransomware	symantec:ep:risk:file	INSTALL_FLAS... C:\USERS\VICKI... 630325CAC09A... TROJAN.RANS...			12/30/18, 3:49 ...
⚙	2	SUSPICIOUS PHISHING E...	Email check	Suspected Phis...	Phishing email detector	HTTP://1DNSC... 630325CAC09A... PAYMENT ACC...		allowed	12/30/18, 3:49 ...

Case
Ransomware found

Assign to Analyst
Admin

Suggested Tags
Ransomeware

Similar Cases

Phishing email detector ID: 20325 , 12/20/18, 4:43 PM	100%
Symantec EP ID: 20327 , 12/23/18, 11:55 AM	100%
symantec:ep:risk:file ID: 20328 , 12/23/18, 11:59 AM	100%
Phishing email detector ID: 20330 , 12/23/18, 12:02 PM	100%
symantec:ep:risk:file ID: 20331 , 12/30/18, 3:18 PM	100%

630325CAC09AC3FAB908F903E3...

Mapping and Modelling

> For full information on mapping events and creating visual families, refer to Ontology.

To add a model family or map new fields:

1. Select a case from the case queue.
2. Click the wheel icon on the left of the event to which you want to assign the visual family or the mapping.

3. Continue to Event Configuration for more details.

4.1.5.1. Event Configuration

✻ For a full explanation of this subject, refer to Ontology first.

You will arrive at the Event Configuration screen after clicking on a Configure icon from one of the following places in the Siemplify platform:

- Events Tab
- Ontology Status Screen

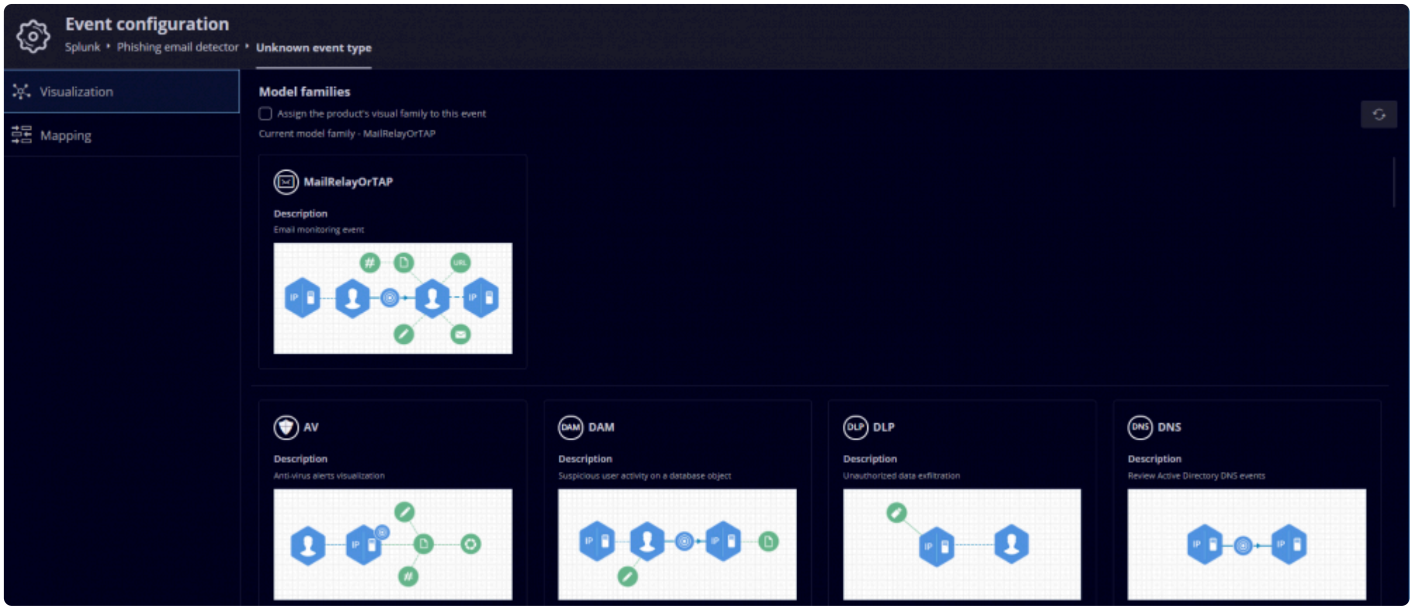
In the Event Configuration screen, you can assign visual model families at source/product/event level in the Visualization screen as well as being able to configure mapping at field level in the Mapping screen. The model family will provide you with a graphic explanation of the relationship between all the events and actions that take place.

So for example, if an event comes into Siemplify platform and you can see that there is missing or incorrect information, you would click the Configure icon from the Events tab and check to see that it's assigned to the right visual family, and only after checking this is correct, you would navigate to the Mapping screen to edit and add specific field information that is missing or change to correct information.

Visualization

The point of this screen is that you assign the event/product/source to a specific "family" – i.e. a visual map of relationships and entities that will provide you with the best graphic explanation of what happened. This visual family is displayed on the Explore Cases screen.
You can assign a model family at source level (this is the top level), product level (this is the second level), or event level (this is the ground level). The model family is inherited from the "parent". In other words, if you assign a family at source level, then both the product and the event inherit the model family from the Source level. However, you can edit the mapped fields at each level and this will override the "parent" settings.

In the screenshot below:
Source = Splunk
Product = Phishing Email Detector
Event = Unknown Event Type



Event configuration

Splunk • Phishing email detector • Unknown event type

Model families

□ Assign the product's visual family to this event

Current model family - MailRelayOrTAP

MailRelayOrTAP

Description

Email monitoring event

AV

Description

Anti-virus alerts visualization

DAM

Description

Suspicious user activity on a database object

DLP

Description

Unauthorized data exfiltration

DNS

Description

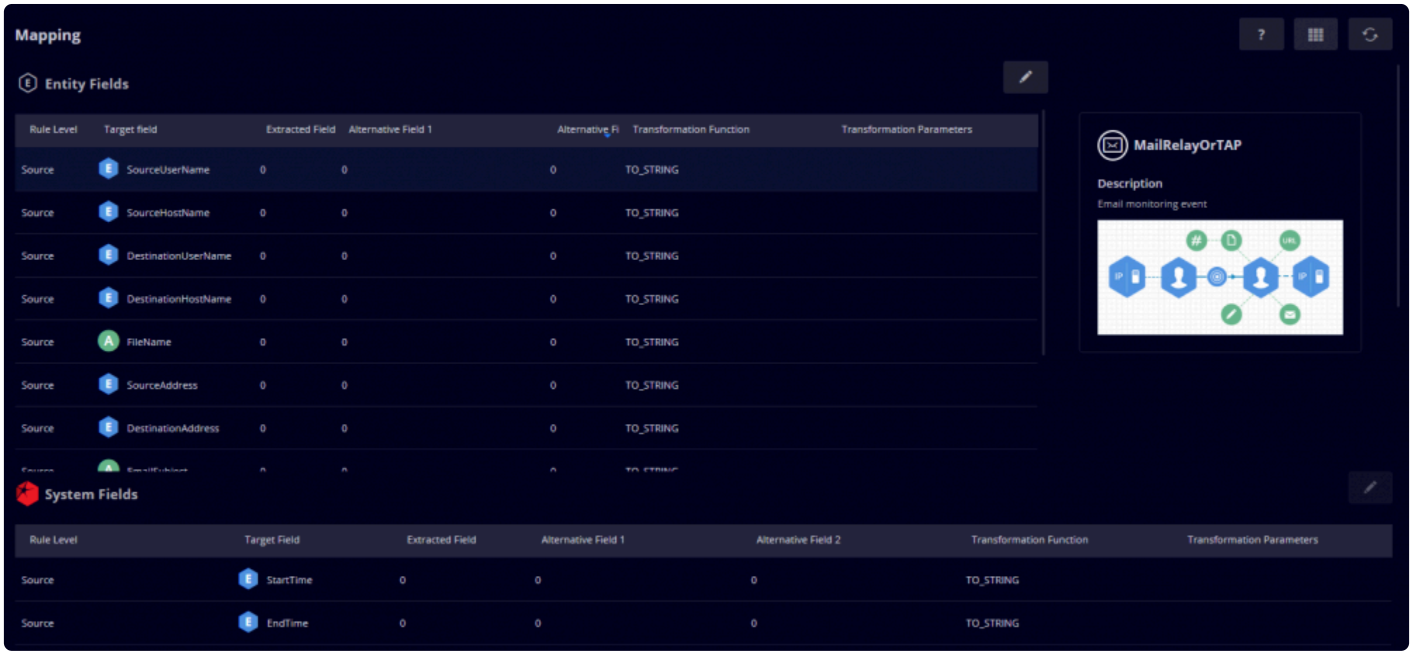
Review Active Directory DNS events

To assign a model family:

1. Select the model family that most resembles the relationship between events and actions that occur in this situation. Note that Siemplify provides 24 model families out of the box and you can add as many as you need. For cloning, editing and adding families, refer to Visual Families
2. Confirm the assignment.

Mapping

In this screen you can see the fields belonging to the Model Family that is assigned to this product (or event or source) and edit them.



Mapping

Entity Fields

Rule Level	Target field	Extracted Field	Alternative Field 1	Alternative Fi	Transformation Function	Transformation Parameters
Source	E SourceUserName	0	0	0	TO_STRING	
Source	E SourceHostName	0	0	0	TO_STRING	
Source	E DestinationUserName	0	0	0	TO_STRING	
Source	E DestinationHostName	0	0	0	TO_STRING	
Source	A FileName	0	0	0	TO_STRING	
Source	E SourceAddress	0	0	0	TO_STRING	
Source	E DestinationAddress	0	0	0	TO_STRING	
Source	A EmailSubject	0	0	0	TO_STRING	

MailRelayOrTAP

Description

Email monitoring event

System Fields

Rule Level	Target Field	Extracted Field	Alternative Field 1	Alternative Field 2	Transformation Function	Transformation Parameters
Source	E StartTime	0	0	0	TO_STRING	
Source	E EndTime	0	0	0	TO_STRING	

The following fields can be edited:

Field	Description
Rule Level	Either Source, Product or Event (non editable)
Target Field	Field name used by Siemplify
Extracted Field	Main field name in the integration data source to take information from
Alternative Field 1	Fallback field in the integration data source to take information from
Alternative Field 2	Fallback field in the integration data source to take information from if both primary and secondary cannot be located

Transformation Function/ Transformation Function Parameter	This enables you to “transform” information from the data source to be compatible with the Siemplify database. Available functions are: TO_STRING, FROM_UNIXTIME_STRING_OR_LONG, FROM_CUSTOM_DATETIME, EXTRACT_BY_REGEX, TO_IP_ADDRESS. Once you have chosen the function, you would add the appropriate parameter. For example, select the function EXTRACT_BY_REGEX, TO_IP_ADDRESS and add the parameter:
	`\b(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.`
	`(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.`
	`(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.`
	`(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\b`

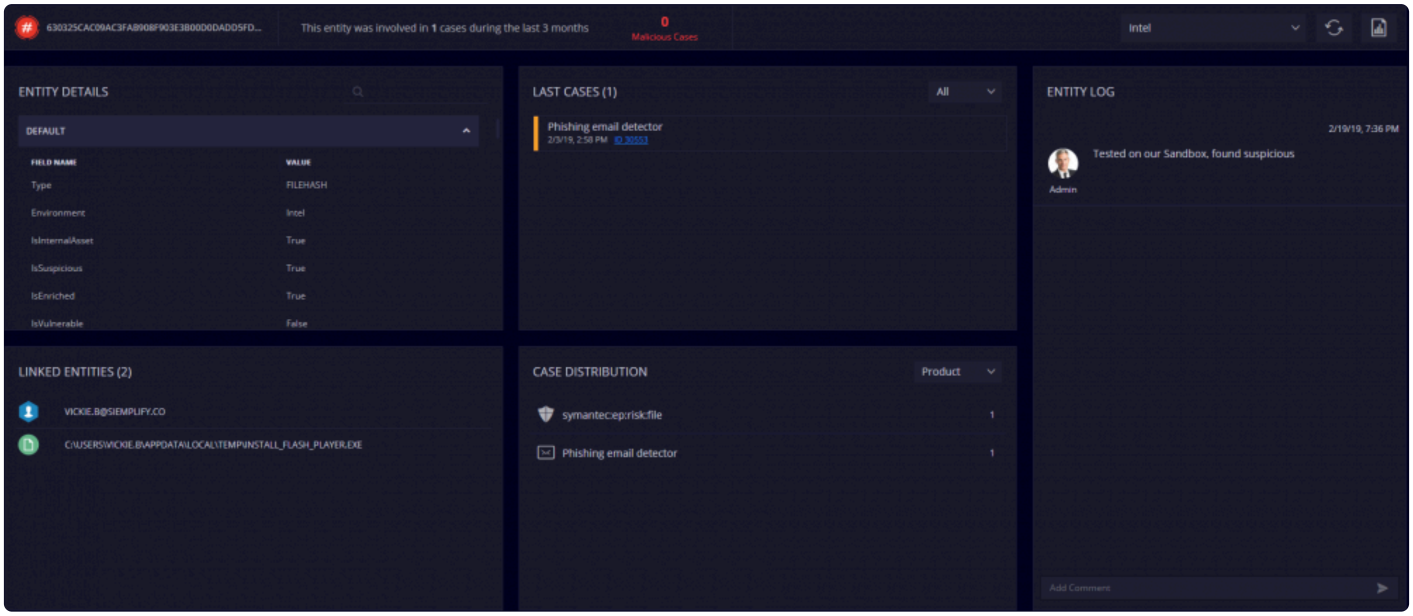
Note that you can extract data from one source field and map it to different target fields. For example, if a source field has both a hostname and an IP address, you can separate them out using Regex expressions.

4.1.6. Entities

Entities are the objects which form the basis of the security events.
You can reach the Entities screen by clicking on an Entity from the Cases screen.
The Entity screen gives you insight into:

- The number of and specific cases this entity was involved with during the last three months. This provides information about the entity throughout the cases in the system. This explains why the information presented here might be different from the information you will see for a specific entity in the Context Details screen. For example, a URL where is suspicious = true and is highlighted in red in the Context Details, might appear here as false if this same URL is defined according to different criteria in a few other cases.
- The details about the entity including basic information and enrichment information gathered about this entity from different cases
- The linked entities such as users and IP addresses
- The frequency of each type of case
- A list of log entries

You can expand or contract of each category by clicking the arrow at the right side of the category name (Entity, Default, etc.).



630325CAC09AC3FAB908F903E3B00D0DADD5FD...

This entity was involved in 1 cases during the last 3 months

0 Malicious Cases

Intel

ENTITY DETAILS

DEFAULT

FIELD NAME	VALUE
Type	FILEHASH
Environment	Intel
IsInternalAsset	True
IsSuspicious	True
IsEnriched	True
IsVulnerable	False

LAST CASES (1)

All

Phishing email detector
2/3/19, 2:58 PM ID 30553

ENTITY LOG

2/19/19, 7:36 PM

Admin: Tested on our Sandbox, found suspicious

Add Comment

LINKED ENTITIES (2)

VICKIE.B@SIEMPLIFY.CO

C:\USERS\VICKIE.B\APPDATA\LOCAL\TEMP\INSTALL_FLASH_PLAYER.EXE

CASE DISTRIBUTION

Product

symantec:ep:risk:file	1
Phishing email detector	1

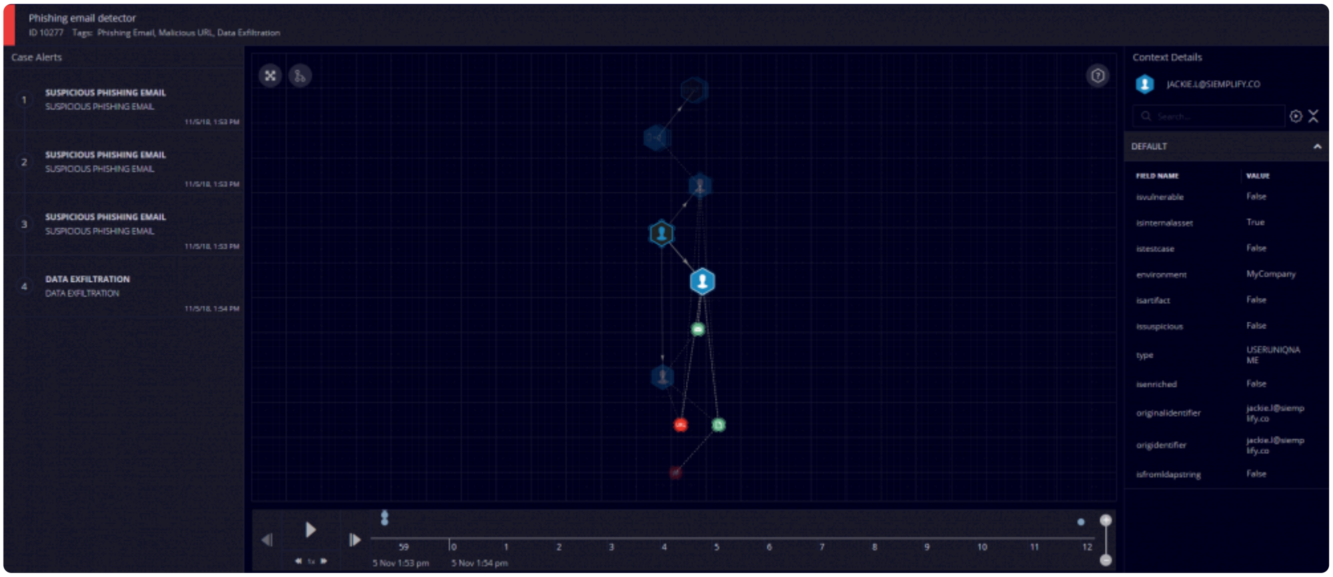
4.1.7. Explore Cases

You can view the alerts and entities of a case in this Explore screen in the form of a visual family in the center of the screen.

The advantage of this visual family is that you can get a keener sense of who or what did x, who is affected by it and in what order it happened. Think of the Explore like a detective's cork board where the detective pins up suspects and events and draws lines between the suspects and events to make the connections. Within the visual family there are two Relationship Types – one is an action which is denoted by an arrow and the other is a connection which is denoted by a dotted line.

Select a case from the case queue and click Explore on the top-right corner of the Cases page. The Explore Cases page displays the following details:

- **Left pane**: Alerts of the selected case and their occurrence time.
- **Middle pane**: Entities interconnected and arranged with a layout, video control buttons to play the events and a graphical representation of the alerts.
- **Right pane**: Context details displaying the details of the selected alerts or entities. Each time you select an alert or an event, the Context Details will display the relevant information.
- **Bottom of screen**: Video control buttons to play the events – together with a visual time range (which can be manipulated further using plus/minus icons). Click play to go through the events in chronological order on the graph.



Phishing email detector
ID 10277 Tags: Phishing Email, Malicious URL, Data Exfiltration

Case Alerts

1 SUSPICIOUS PHISHING EMAIL
SUSPICIOUS PHISHING EMAIL
11/5/18, 1:53 PM

2 SUSPICIOUS PHISHING EMAIL
SUSPICIOUS PHISHING EMAIL
11/5/18, 1:53 PM

3 SUSPICIOUS PHISHING EMAIL
SUSPICIOUS PHISHING EMAIL
11/5/18, 1:53 PM

4 DATA EXFILTRATION
DATA EXFILTRATION
11/5/18, 1:54 PM

Context Details
JACKIE.L@SIEMPLIFY.CO

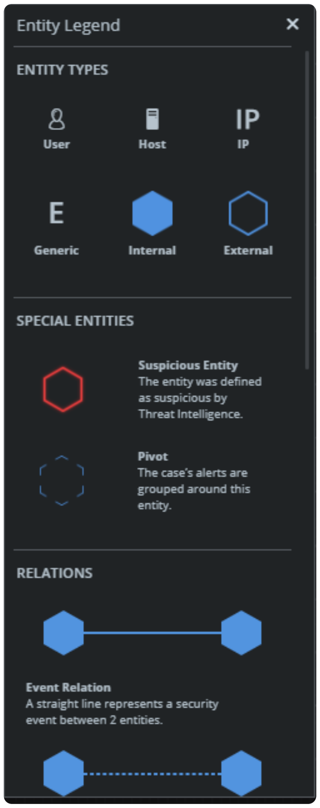
DEFAULT

FIELD NAME	VALUE
isvulnerable	False
isinternalasset	True
istestcase	False
environment	MyCompany
isartifact	False
issuspicious	False
type	USERUNIQNAME
isenriched	False
originalidentifier	jackie.l@siemplify.co
origidentifier	jackie.l@siemplify.co
isfromldapstring	False

Click on an alert in the left pane to view its involved entities highlighted in the middle pane. The node indicating this alert appears bigger than the other nodes (alerts) on the graph. Hover over the nodes to see their respective alert names. Entities not involved in the selected alert are greyed out.

The following options are available on the screen:

Options	Descriptions
⤢	The Fit to Screen option at the top-left corner of the middle pane autofits the entire entity display to its actual size.
⁂	Circular layout is the default layout used by the entities. Clicking the Change Graph Layout icon gives you other layout options for displaying entities for your viewing convenience.
▶	The Play Event button plays all alerts of the case in a sequence. The involved entities for each alert being played are highlighted at that instance. You can also see the alert flow in the graph where each node (alert) is highlighted bigger when being played.
|▶	The Next Event button enables you to play the next single alert (per click), one after the other as per the sequence in the left pane. By default, the first click plays the first alert in the left pane.
◀|	The Previous Event button enables you to play the previous alert. By default, this button is disabled (until the first alert is played).
◀◀ 1x ▶▶	The Fast Forward and Fast Backwards buttons enable you to play all alerts of a case 3 times faster in ascending order or descending order of their occurrence time respectively.
+ −	The Time Range Slider enables you to expand or shrink the time range on the X-axis respectively.

?	This displays an entity legend.  Entity Legend ✕ ENTITY TYPES User Host IP Generic Internal External SPECIAL ENTITIES RELATIONS **Suspicious Entity** The entity was defined as suspicious by Threat Intelligence. **Pivot** The case's alerts are grouped around this entity. **Event Relation** A straight line represents a security event between 2 entities.

Once you have investigated the visual aspects of the Case, you can then execute manual actions in order to investigate further. For example, you can run a manual action to Scan IP addresses to see if any of the IP addresses are known threats. Once you have established there was a specific issue – for example – important company information has been leaked, you can then take action.

Examples of actions you might take once a threat has been established might be to:

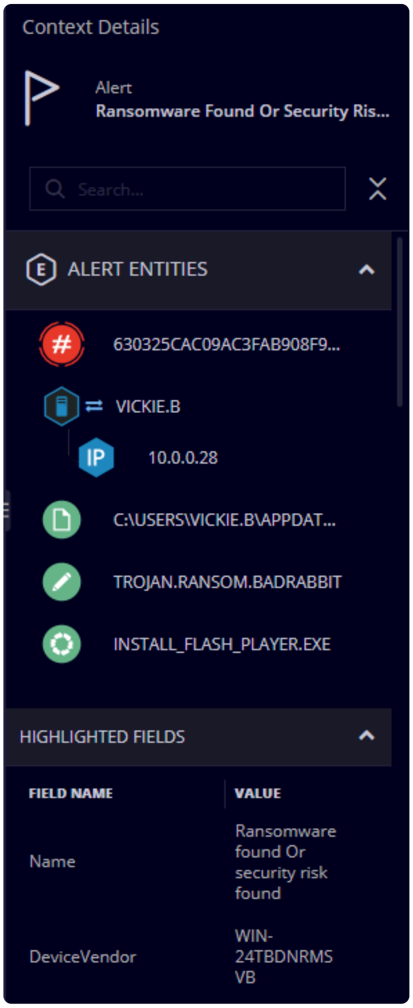
- Quarantine computers
- Check and scan infected computers
- Investigate emails
- Discover missing information

✻ For complete information on mapping and modelling families that appear here, refer to Ontology.

4.1.8. Context Details

The Context Details appears on the right of the Cases screen and provides more details on whatever you have highlighted in the main screen.

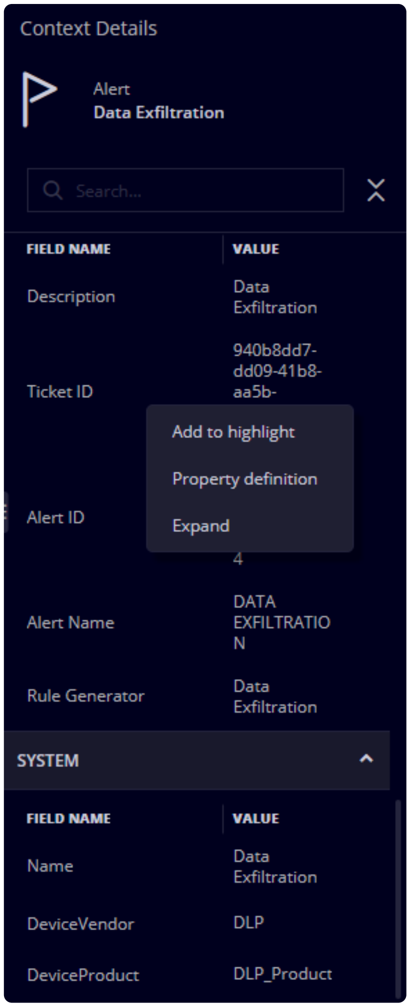
If you have selected the Case, then all the entities pertaining to the selected Case is shown as in the screenshot below. If you have selected an Alert within a Case, then information on all the fields within the Alert will be displayed in the Context Details pane.



FIELD NAME	VALUE
Name	Ransomware found Or security risk found
DeviceVendor	WIN-24TBDNRMSVB

In both the Default and the Highlighted fields in the Context Details, there appears a three dot button. Clicking on this provides the following three options

- Add to Highlight/Remove from Highlight: Depending on where it is, this will either add or remove it to or from the highlighted list in the Context Details pane.
- Property Definition: this opens up the same dialog box as in Settings > Data Configuration > Properties Metadata enabling you to edit the information here.
- Expand: opens up the dialog box a bigger panel to view the entire content.



Context Details

Alert
Data Exfiltration

FIELD NAME	VALUE
Description	Data Exfiltration
Ticket ID	940b8dd7-dd09-41b8-aa5b-
Alert ID	4
Alert Name	DATA EXFILTRATION
Rule Generator	Data Exfiltration

SYSTEM

FIELD NAME	VALUE
Name	Data Exfiltration
DeviceVendor	DLP
DeviceProduct	DLP_Product

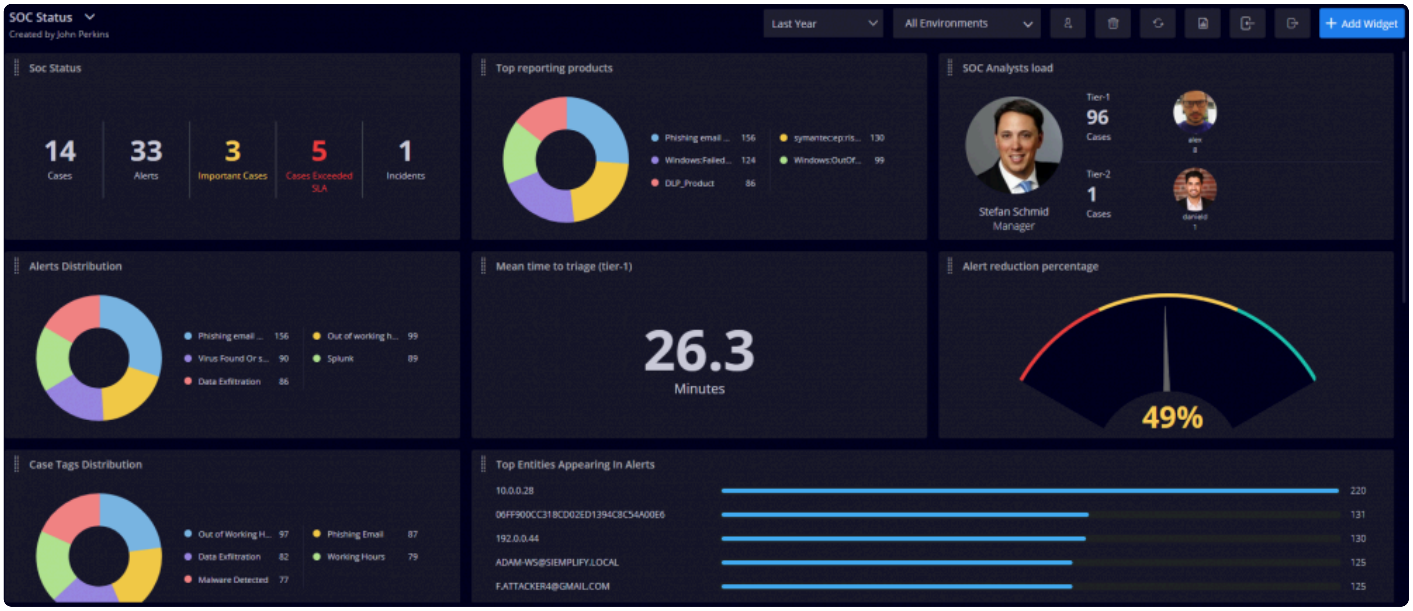
When clicking on a Playbook, the Context Details appears as a Playbook Summary. This shows the following information:

- Playbook Name and Run Length
- Time and Length of Playbook Run
- Waiting for User Input: If the Playbook is waiting for the analyst to do something, this will be displayed prominently at the top of the Playbook Summary. In addition, a Push notification will be sent to the relevant user letting them know that the Playbook is waiting for them.
- Integrations: list of Integrations being used by this Playbook
- Playbook Flow: each Playbook step that ran with its status and step result.
- Errors: any errors will be listed here. Each error is clickable and will direct you to the Kibana logs page. You can also choose to rerun the Action from here. A notification will be sent to the user letting them know the Playbook is stuck.

5. Dashboards

The Dashboard page in the Siemplify platform enables analysts to manage Siemplify dashboards, giving them an overview of the specified Siemplify data in various views in the form of widgets. A dashboard holds a maximum of 12 widgets, which can display data in various forms such as pie charts, horizontal or vertical bars, tables, ROI charts, etc., for any specified SOC environment or case occurrence time. You can customize the widget data by grouping widgets based on analysts or playbooks associated with the case, products or involved entities, important and non-important cases and so on. You can also filter the display data by applying built-in filters such as tags, case status, case priority, case stage, case close reasons and so much more. Simulated alerts are not counted in the dashboard data.

> ✻ Data on the dashboard refreshes automatically every five minutes.



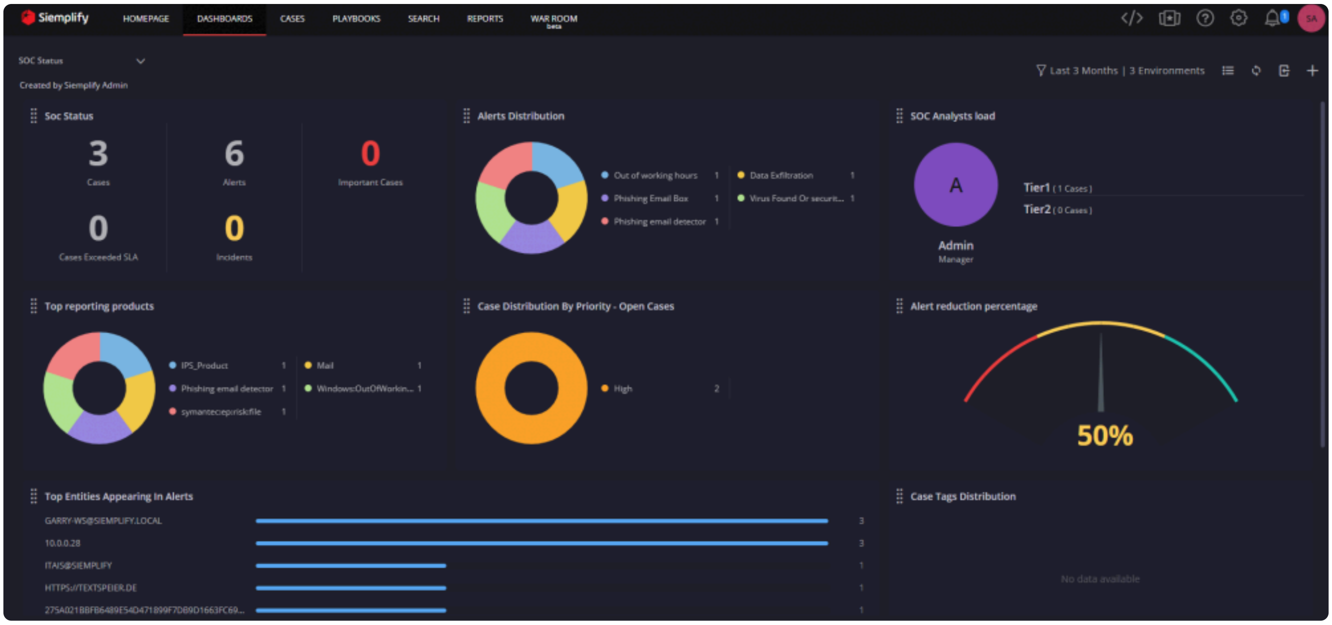
5.1. Add New Dashboards

The Siemplify dashboard comes with a predefined dashboard. However, you can create new custom dashboards (as required by your SOC or MSSP circumstances.)

To create a new dashboard:

1. Click Create New Dashboard.

2. Name the new dashboard and click Create. The next step is to Add Widgets to your new dashboard. Following is a picture of a dashboard with widgets already added.



5.2. Add Widgets

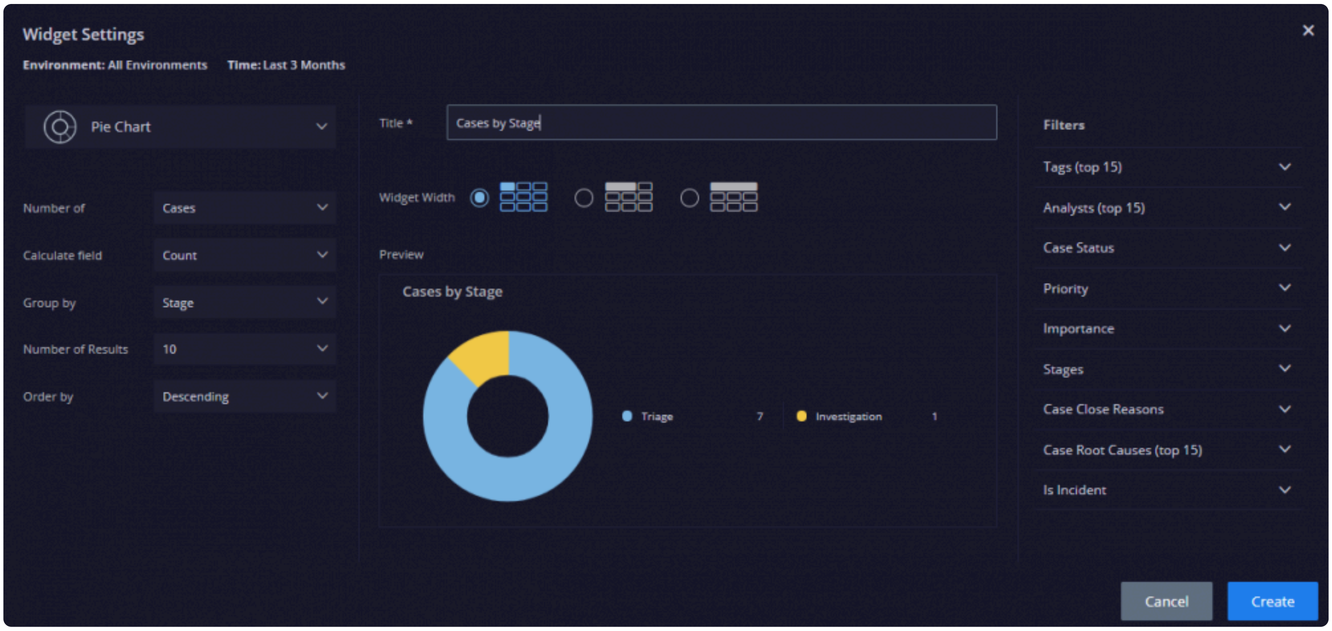
After adding a dashboard, add the widgets as per your requirement. You can add up to 12 widgets in a dashboard.

To add a widget:

1. Click the plus symbol on the dashboard or the Add Widget button on the top-right corner of the system. The Widget Settings window appears.
2. In Title, type a meaningful title for the new widget. This step is mandatory. The time and environment you specified while creating the dashboard applies to all widgets of that dashboard. These fields are auto-populated below the widget title.
3. Choose a Widget Width as required.
4. In the left pane, select the form of the data display using the drop-down menu.
5. By default, the data display is in the form of a Pie Chart. Other forms you can select are Horizontal Bar graph, Vertical Bar graph and Table.
6. For the chosen data display form, specify its corresponding fields in the left pane as required. For example: If you chose Pie Chart as the data display form, its corresponding fields are Number of, Calculate field, Group by, Number of Results and Order by. For more information on the data display form and corresponding fields, refer to [Data Display Forms](#).
   p(banner tip). Depending on whether you choose Cases or Alerts – the Group By options will display

differently.

7. In the right Filters pane, select all the required filters for which you want the data to display. If the filter you want is not in the provided top 15 list, then you can search for it and add it in.
8. Click Create. The new widget with specified data form, parameters and filters is added to the dashboard.



Widget Settings

Environment: All Environments Time: Last 3 Months

Pie Chart

Number of: Cases

Calculate field: Count

Group by: Stage

Number of Results: 10

Order by: Descending

Title *: Cases by Stage

Widget Width: ● ○ ○

5.2.1. Data Display Forms and Fields

Data Display Form	Fields
Pie Chart	• Number of • Calculate field • Group by • Number of Results • Order by
Horizontal Bar Graph	• Number of • Calculate field • Group by • Number of Results • Order by
Vertical Bar Graph	• Number of • Calculate field • Group by

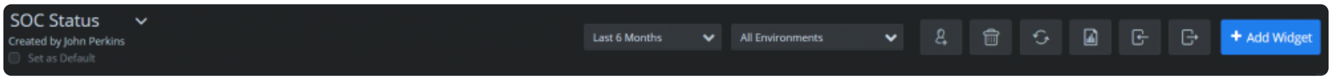
	• Number of Results • Order by
Table	• Number of • Calculate field • Axis A • Axis B

Number of	Group by Fields
If you choose Alerts	• Entity Identifier • Environment • Network • Playbook • Product • Rule Name
If you choose Cases	• Analyst • Environment • Importance • Priority • Tag • Stage
If you choose Playbooks	• Playbook Name • Environment • Blocks

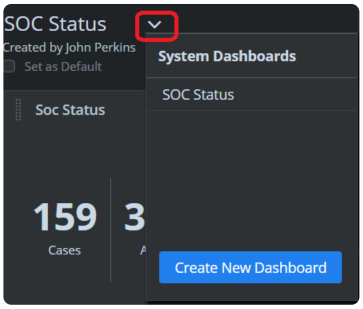
5.2.2. New Widget Example

The following procedure takes you through step-by-step instructions to add a new widget to a new dashboard. The widget displays a pie chart presenting products that have contributed to the top 5 attacks in all environments for the last 6 months (number of attacks in descending order). No filters are applied in this scenario.

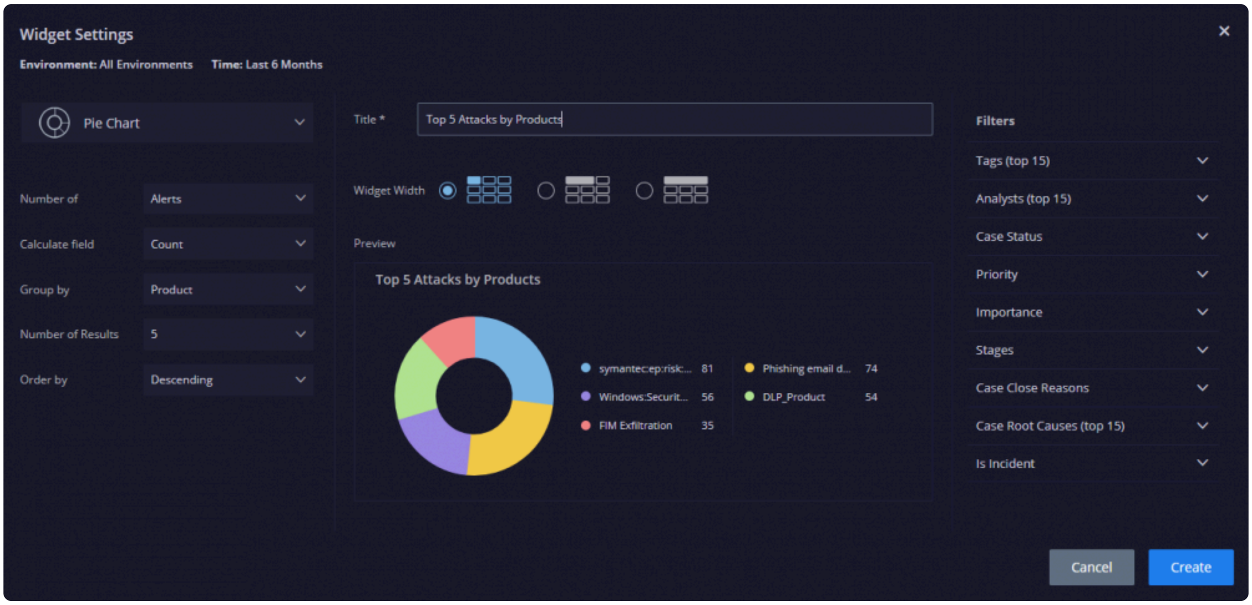
1. Click Dashboards from the main menu of the system located at the top of the user interface.
2. From the drop-down menus at the top-middle segment of the system, select the time as Last 6 Months and environment as All Environments.



3. Click the arrow symbol next to the existing dashboard name located at the top-left corner of the system and click Create New Dashboard.



4. Type the new dashboard name as Attacks and click Create.
5. In the new dashboard, click the plus symbol on the dashboard.The Widget Settings window appears.
6. Type Top 5 Attacks by Products as the title.
7. Choose a desired Widget Width by clicking on a radio button.
8. In the left pane, by default, the data display is in the form of a Pie Chart. Retain it AS IS.
9. Select the following options for the Pie Chart fields below:
   - Number of – Alerts
   - Calculate field – Count
   - Group by – Product
   - Number of Results – 5
   - Order by – Descending



Widget Settings

Environment: All Environments Time: Last 6 Months

Pie Chart

Number of: Alerts

Calculate field: Count

Group by: Product

Number of Results: 5

Order by: Descending

Title *: Top 5 Attacks by Products

Widget Width: ● ○ ○

Preview

Top 5 Attacks by Products

symantec:ep:risk...	81	Phishing email d...	74
Windows:Securit...	56	DLP_Product	54
FIM Exfiltration	35		

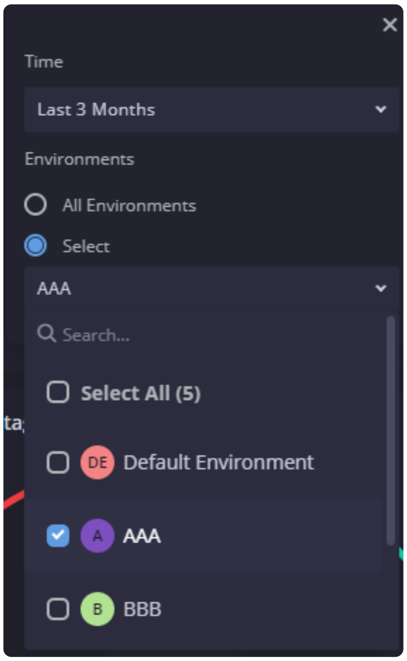
10. Click Create. The new widget is displayed on the dashboard named Attacks.
    You can see the pie chart presenting products contributing to the top 5 attacks in all environments for the last 6 months.

5.3. Dashboard Options

You can share your dashboard with other users on the system, delete the dashboard you no longer require, refresh data on the dashboard as often as you want, save the dashboard as a report template, and import or export the dashboard to a separate platform. You can also choose to set it as the default dashboard.

Select Time Period and Environments

At the top right of the screen, you can select the time period to display data from as well as Environments (All, or multi-select)



Time

Last 3 Months

Environments

○ All Environments

● Select

AAA

Search...

□ Select All (5)

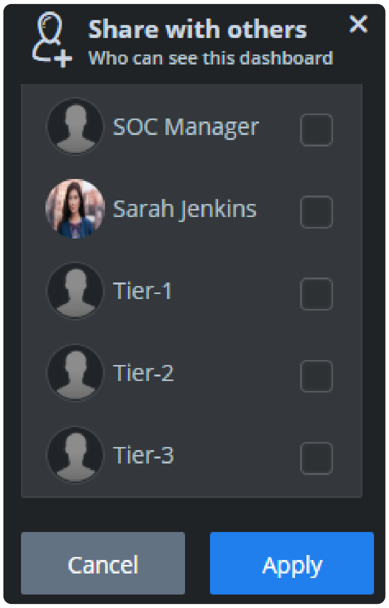
□ DE Default Environment

☑ A AAA

□ B BBB

Share your Dashboard

1. On the top right of the screen, click
2. Select the relevant people.
3. Click Apply.



Share with others

Who can see this dashboard

SOC Manager □

Sarah Jenkins □

Tier-1 □

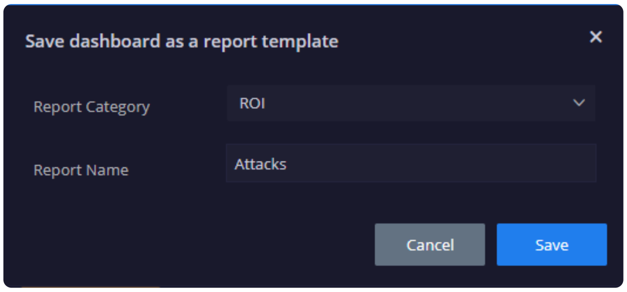
Tier-2 □

Tier-3 □

Save as Report

1. On the top right of the screen, click 📊
2. Choose a Category and enter a name.
3. Click Save. This report is saved in the Reports screen.

> Note that not all the widgets are covered in the Report template.



Save dashboard as a report template

Report Category: ROI

Report Name: Attacks

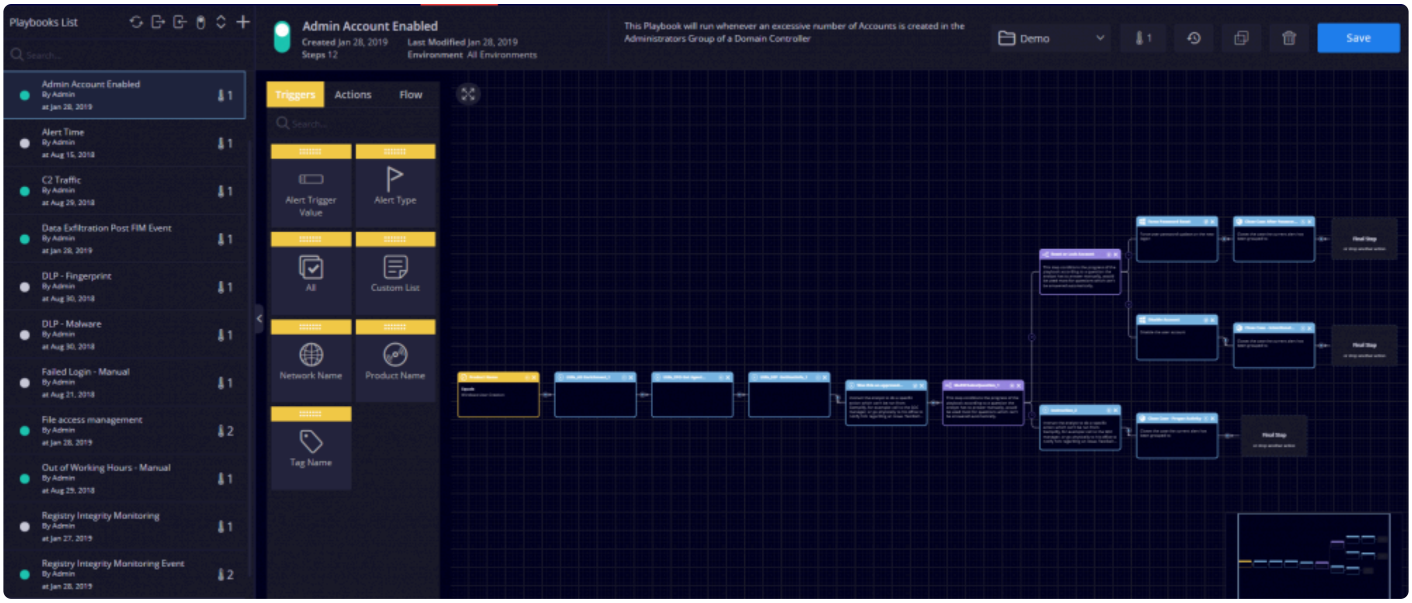
6. Playbooks

What is a Playbook?

A Playbook can best be described as a workflow of actions which are executed following a certain trigger. Playbooks are particularly useful because they can be predefined in advance to respond to various alerts coming from your SIEM and carry out automatic actions – thereby freeing up the analyst's time and efforts.

A playbook is composed of two parts: trigger and actions as defined by the SOC Manager or higher-tier analysts for handling security alerts. Playbooks automatically gather information on alerts from internal and external sources, request essential information from users associated with the alerts and take appropriate actions to proceed with the alerts.

Siemplify includes over 80 predefined playbooks for the most common use cases. You can customize these playbooks or define additional playbooks for your specific requirements. Below is a screenshot of the Playbooks screen with a specific Playbook highlighted.



Admin Account Enabled
Created Jan 28, 2019 Last Modified Jan 28, 2019
Steps 12 Environment All Environments

This Playbook will run whenever an excessive number of Accounts is created in the Administrators Group of a Domain Controller

Admin Account Enabled By Admin at Jan 28, 2019 1
Alert Time By Admin at Aug 15, 2018 1
C2 Traffic By Admin at Aug 29, 2018 1
Data Exfiltration Post FIM Event By Admin at Jan 28, 2019 1
DLP - Fingerprint By Admin at Aug 30, 2018 1
DLP - Malware By Admin at Aug 30, 2018 1
Failed Login - Manual By Admin at Aug 21, 2018 1
File access management By Admin at Jan 28, 2019 2
Out of Working Hours - Manual By Admin at Aug 29, 2018 1
Registry Integrity Monitoring By Admin at Jan 27, 2019 1
Registry Integrity Monitoring Event By Admin at Jan 28, 2019 2

How do I build a Playbook?

There are three main building blocks for building a Playbook: Triggers, Actions, and Flows. You drag and drop each one of the blocks to flesh out a complete Playbook. Refer to Understanding the Playbooks page for more information.

What is a Playbook Block?

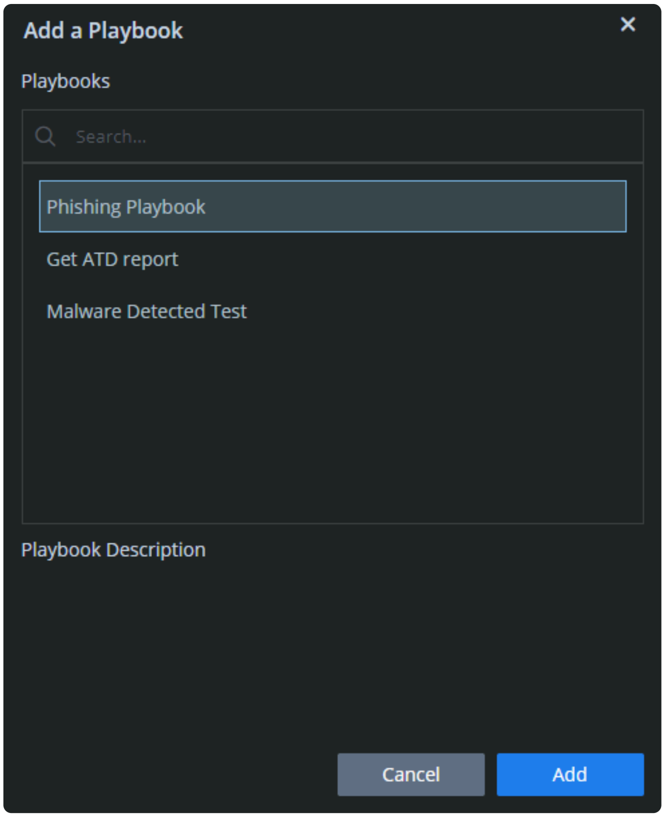
A Playbook block is a mini playbook that is built slightly differently to a regular Playbook and which functions as a snippet that can be inserted into a regular Playbook. It can also be run as a stand alone. The advantage of using a Block is the ease of configuring one time and then reusing it in various Playbooks. For full details on Playbook Blocks, please refer to Playbook Blocks

How do I run a Playbook?

A case can contain several alerts and each alert can have several playbooks attached to it. If there is a playbook attached – it will run automatically until the end unless a manual action has been predefined, in which case it will pause and wait for the analyst to take that action. Thus analysts save considerable time and efforts in reviewing the case, because much of the information needed to investigate the alerts has already been gathered by Siemplify, usually without manual intervention.

Additionally, you can manually add and run a Playbook on from the Case page to an individual alert in a case, if needed.

1. In the Cases screen, highlight the alert.
2. In the Playbooks section, to the right, click on the plus icon to add a new playbook.
3. In the Add a Playbook screen, select the required Playbook and click Add.

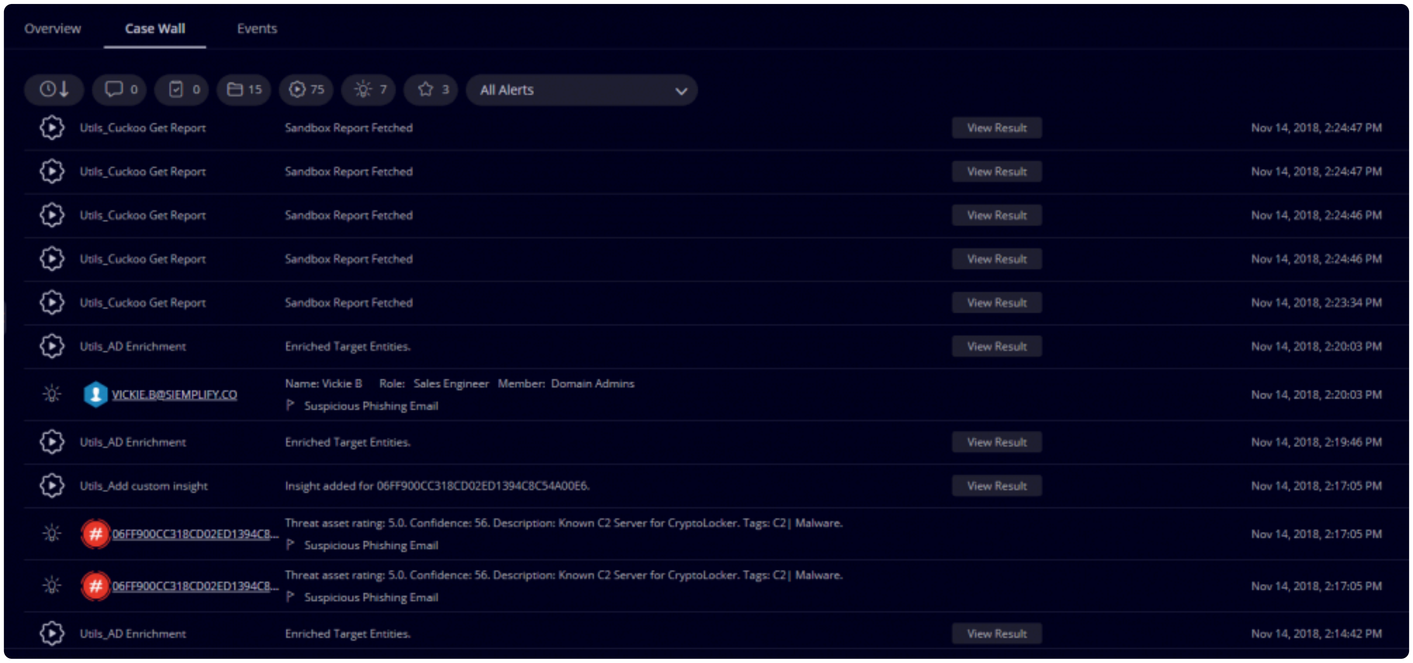


4. The Playbook is added and will run immediately.

How can I see Playbook Results?

The Playbook will display in the bottom part of the screen. To the right of the screen will appear a Playbook Summary section which details all the Playbook steps and results.

You can also view each Playbook action and its corresponding results in the Case Wall screen.

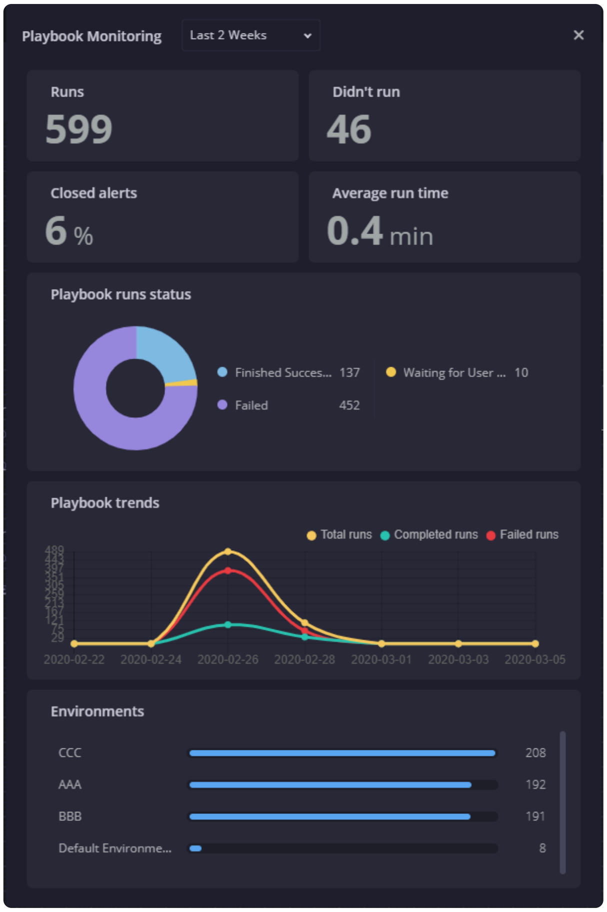


Utils_Cuckoo Get Report	Sandbox Report Fetched	View Result	Nov 14, 2018, 2:24:47 PM
Utils_Cuckoo Get Report	Sandbox Report Fetched	View Result	Nov 14, 2018, 2:24:47 PM
Utils_Cuckoo Get Report	Sandbox Report Fetched	View Result	Nov 14, 2018, 2:24:46 PM
Utils_Cuckoo Get Report	Sandbox Report Fetched	View Result	Nov 14, 2018, 2:24:46 PM
Utils_Cuckoo Get Report	Sandbox Report Fetched	View Result	Nov 14, 2018, 2:23:34 PM
Utils_AD Enrichment	Enriched Target Entities.	View Result	Nov 14, 2018, 2:20:03 PM
VICKIE.B@SIEMPLIFY.CO	Name: Vickie B Role: Sales Engineer Member: Domain Admins Suspicious Phishing Email		Nov 14, 2018, 2:20:03 PM
Utils_AD Enrichment	Enriched Target Entities.	View Result	Nov 14, 2018, 2:19:46 PM
Utils_Add custom insight	Insight added for 06FF900CC318CD02ED1394C8C54A00E6.	View Result	Nov 14, 2018, 2:17:05 PM
06FF900CC318CD02ED1394C8...	Threat asset rating: 5.0. Confidence: 56. Description: Known C2 Server for CryptoLocker. Tags: C2| Malware. Suspicious Phishing Email		Nov 14, 2018, 2:17:05 PM
06FF900CC318CD02ED1394C8...	Threat asset rating: 5.0. Confidence: 56. Description: Known C2 Server for CryptoLocker. Tags: C2| Malware. Suspicious Phishing Email		Nov 14, 2018, 2:17:05 PM
Utils_AD Enrichment	Enriched Target Entities.	View Result	Nov 14, 2018, 2:14:42 PM

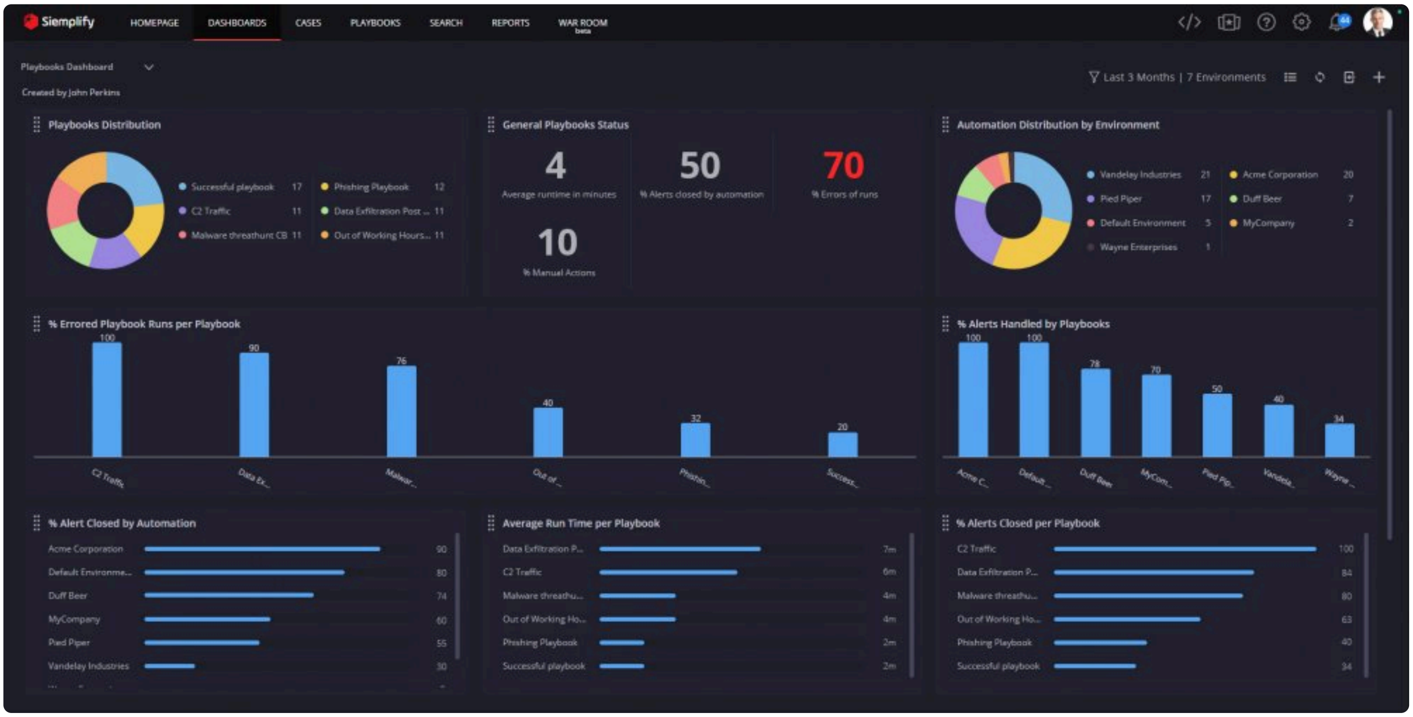
Where can I see metrics on Playbooks?

There are several places to see information on Playbooks:

Individual Playbook > Playbook Monitoring screen.



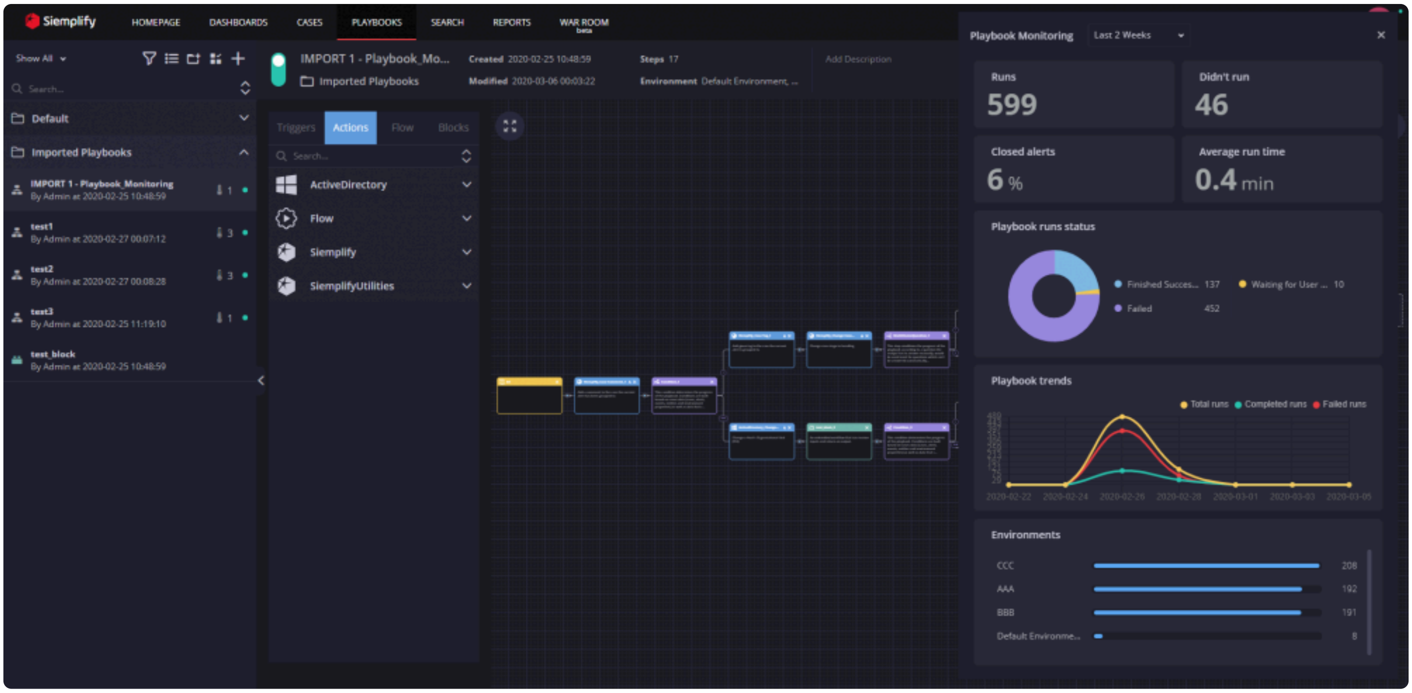
Dashboard > Playbook Dashboard



6.1. Understanding the Playbooks page

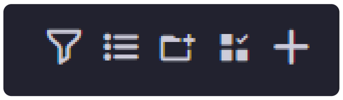
A playbook is built on triggers and actions/flows. Once it is triggered, the playbook moves along the actions to a final resolution. The flow of control executes from left to right beginning with a defined trigger (yellow box) as the first component, which is mandatory. It then moves to the second component that can be a set of defined actions Siemplify must perform (blue box). The last component involves determining the flow of the playbook with an “If then… or else” condition (purple box).

A screenshot of the Playbook page with the Monitoring screen opened is displayed below.



At the top segment of the playbook details pane, you can use the vertical toggling button to enable or disable the playbook. In addition, you can view a summary of the playbook that includes the playbook name, name of the user who created the playbook, playbook creation timestamp, name of the environment for which the playbook was created and a brief description of the playbook.

The following actions are available at the top left of the Playbooks screen.



From right to left:

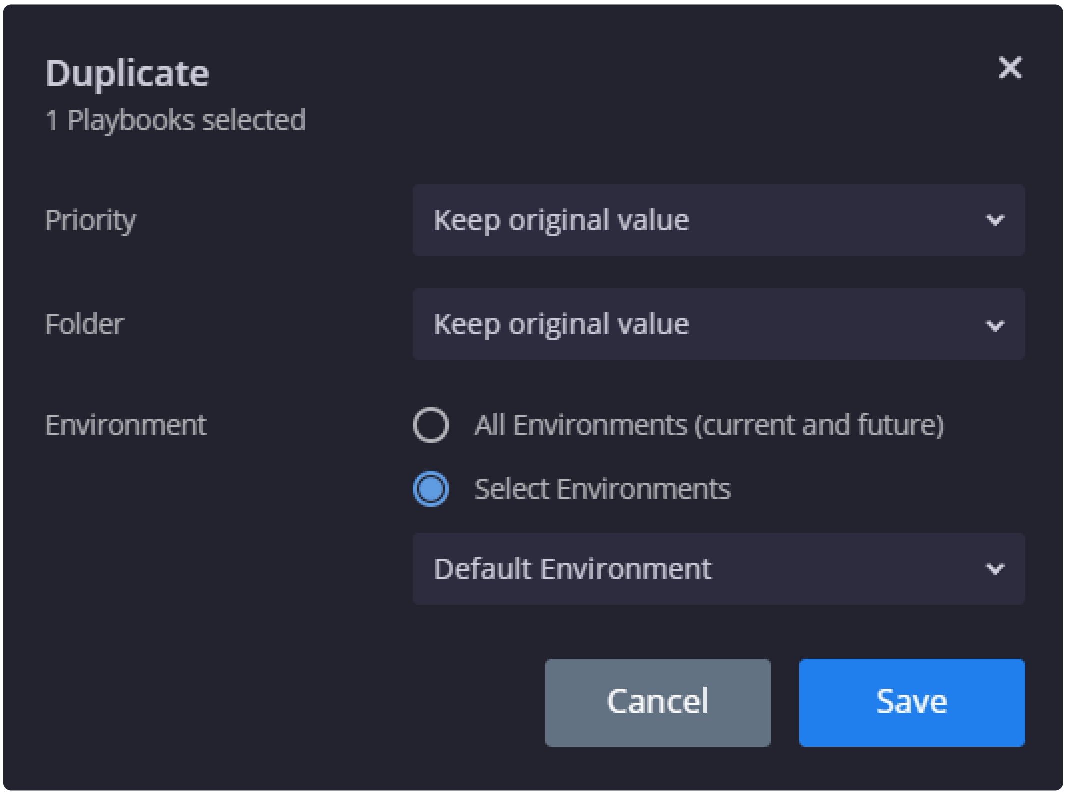
- **Plus** + : Add a new Playbook or Block. Here you can choose which folder and which environment the Playbook/Block belongs to.

- **Edit** : Allows you to select single or **multiple** Playbooks and Blocks for use with the Action menu detailed below. Note that to edit the folder name, you need to click on the Edit icon, and put your mouse on the name, click and then type new name.

- **New Folder** : Adds new folder. The folder will appear at the end of the queue.

- **Menu** : Before clicking on the menu to perform bulk actions, make sure to click Edit and select the required Playbooks/Blocks. Clicking on the Menu opens up the following actions:

- **Duplicate** Click to create a duplicate Playbook with the following options:
  - Keep or Change Priority
  - Keep in same folder or move to a different folder
  - Choose environments it belongs to. Options include single or multiple environments or all environments where “all” means all currently defined environments as well as environments that will be defined in the future.
  - For a single Playbook only, you can choose to save it as a Playbook block.



Duplicate

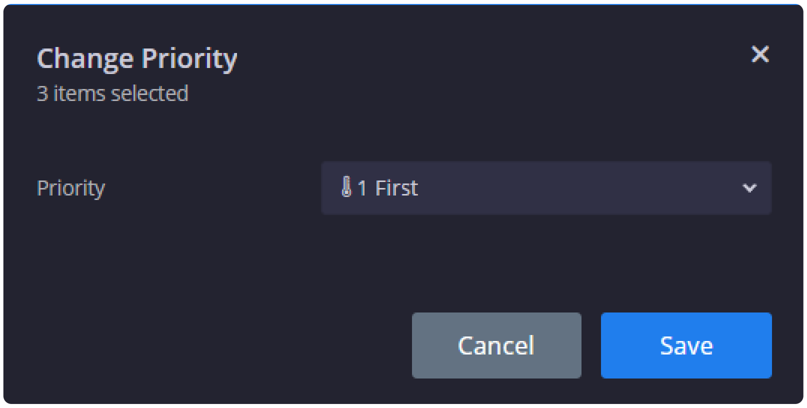
1 Playbooks selected

Priority: Keep original value

Folder: Keep original value

Environment: ○ All Environments (current and future)
● Select Environments
Default Environment

- **Priority** Click to change priority.



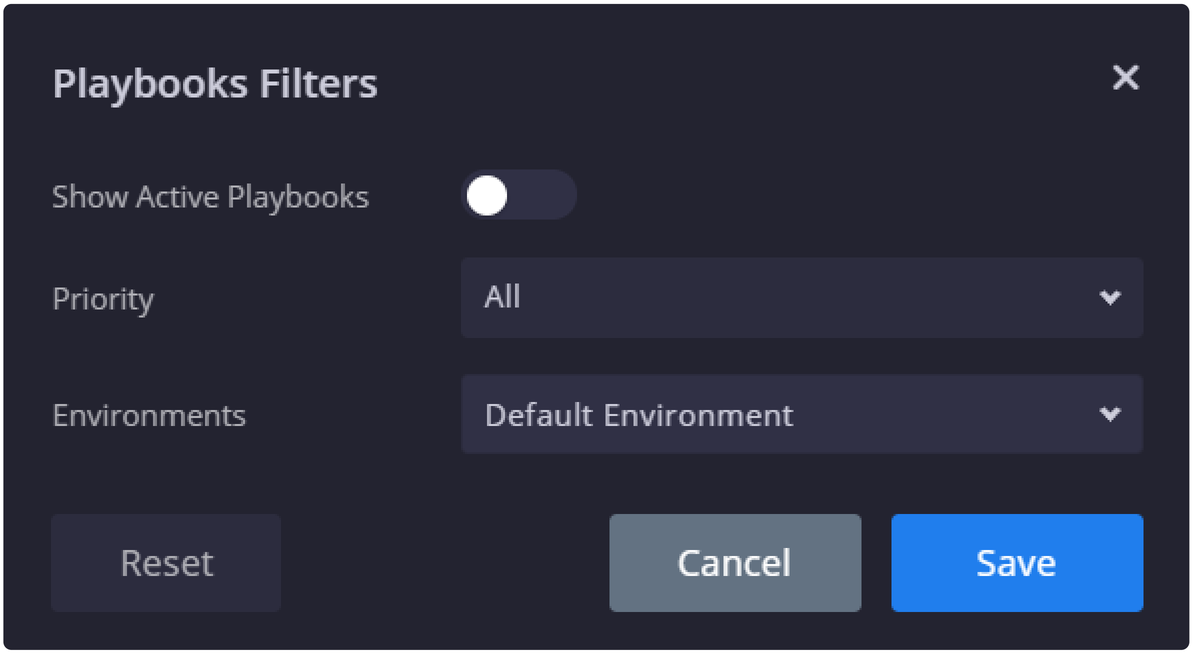
Change Priority

3 items selected

Priority: 1 First

- **Export/Import** Useful for sending both Playbooks and Playbook blocks from staging to production server and vice versa. Note that the system only recognizes zip files for import. (Note that you can import playbooks without clicking on the Edit icon).
- **Move To** Can move Playbooks/Blocks to another folder or even create a new folder from this option.
- **Delete** Delete Playbooks/Blocks.

- **Filter** : Clicking on the Filter opens up the following dialog box where you can choose to filter the display based on:
    - Active/Inactive Playbooks – also referred to as Enabled/Disabled
    - Priority Level
    - Environments (multi-select option)



Playbooks Filters

Show Active Playbooks: ○

Priority: All

Environments: Default Environment

In the Playbook designer, on the top main part and right of the screen, you can perform the following actions:

- Toggle to enable the Playbook
- Edit Playbook title
- Add Playbook description
- Select Priority for Playbook (this determines the attachment order for the alert. Only three Playbooks can be attached automatically and it works according to priority order.
- Version Control - Click to see the following options:
  - **Save as New Version** - Click to save the playbook as a new version, add your comments, then click Save.
  - **View Version History** - Click to see the version history of the playbook in a tabular form. Click Restore to revert to any of the previous versions anytime. This is only available if you have clicked Save as New Version on a Playbook.

At times, you may not be able to see the entire playbook in case of multiple actions and flows defined for the playbook. In this case, you can:

- Use the mini map at the bottom right for easier navigation
- Use the mouse scroll wheel for zoom in or zoom out of the playbook view.
- Click the Fit to Screen icon at the top-left corner of the middle pane to fit the entire playbook to the screen.
- Hide the left pane by clicking the arrow located in between the left pane and the right pane.

6.1.1. Actions

Actions are the next set of components that you can define for a playbook. Each action is categorized under an Integration in the system. They include tasks or actions to be performed by the playbook.
For instance, you can assign an analyst to a case, or in case of an external product integration (like McAfeeEPO product), you can set an action to update McAfee Agent. For each Integration, there is a list of sub-actions.

In order to use the required Actions, you need to make sure you have the Integrations downloaded and configured from the Marketplace. Refer to Marketplace for more information.

When the playbook runs, each action will return information that can include the following:

- Output message, tables, attachments, links, JSON (these will be displayed on the screen)

- Script result (only valid within the Playbook itself)
  You can see this information either in the Case Wall or in the right side panel of the Case screen.

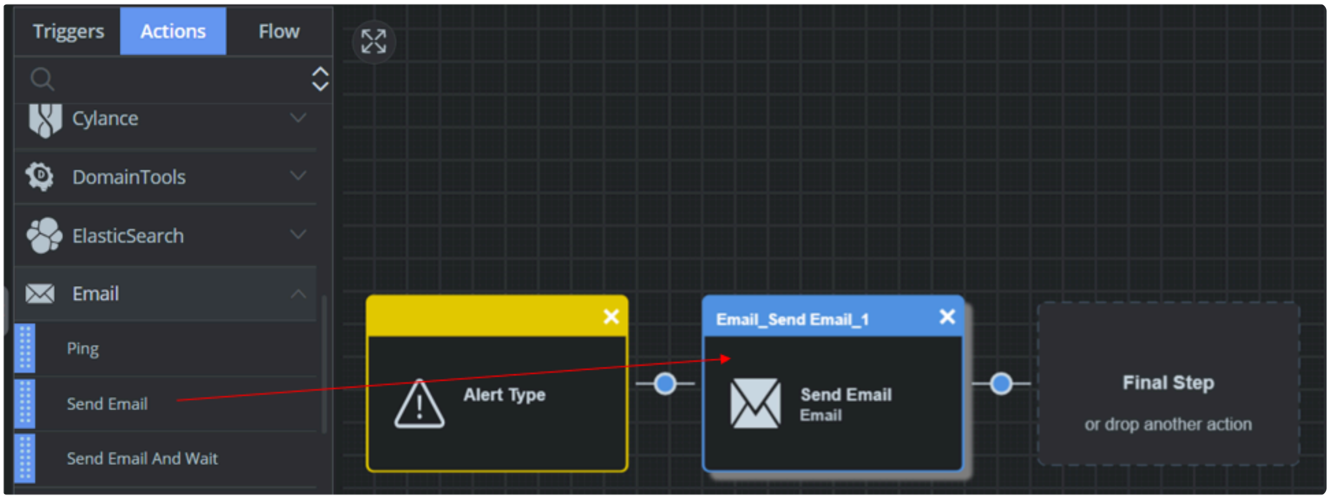
Glossary of Terms used within Actions

- **Parameters**: Input of some type including text and/or placeholder (Siemplify variable), drop-down options, etc
  - **Placeholders**: Siemplify variable which will be populated at running time. See below for further information on Parameters and Placeholders.
- **Enrichment**: Gathers more information and attributes on an entity. See below for further information on using Enrichment.
- **Insight**: An insight highlights a specific result/conclusion in the Playbook to bring it to the analyst's attention. See below for further information on using Insights.
- **Script Result**: Siemplify defined return value of an Action.
- **JSON Result**: Raw data that the Action returns.
- **Expression Builder**: Enables manipulating JSON results and extracting specific data to use in Playbook actions. See Using Expression Builder for more information.

Adding an Action

To add an action to the playbook:

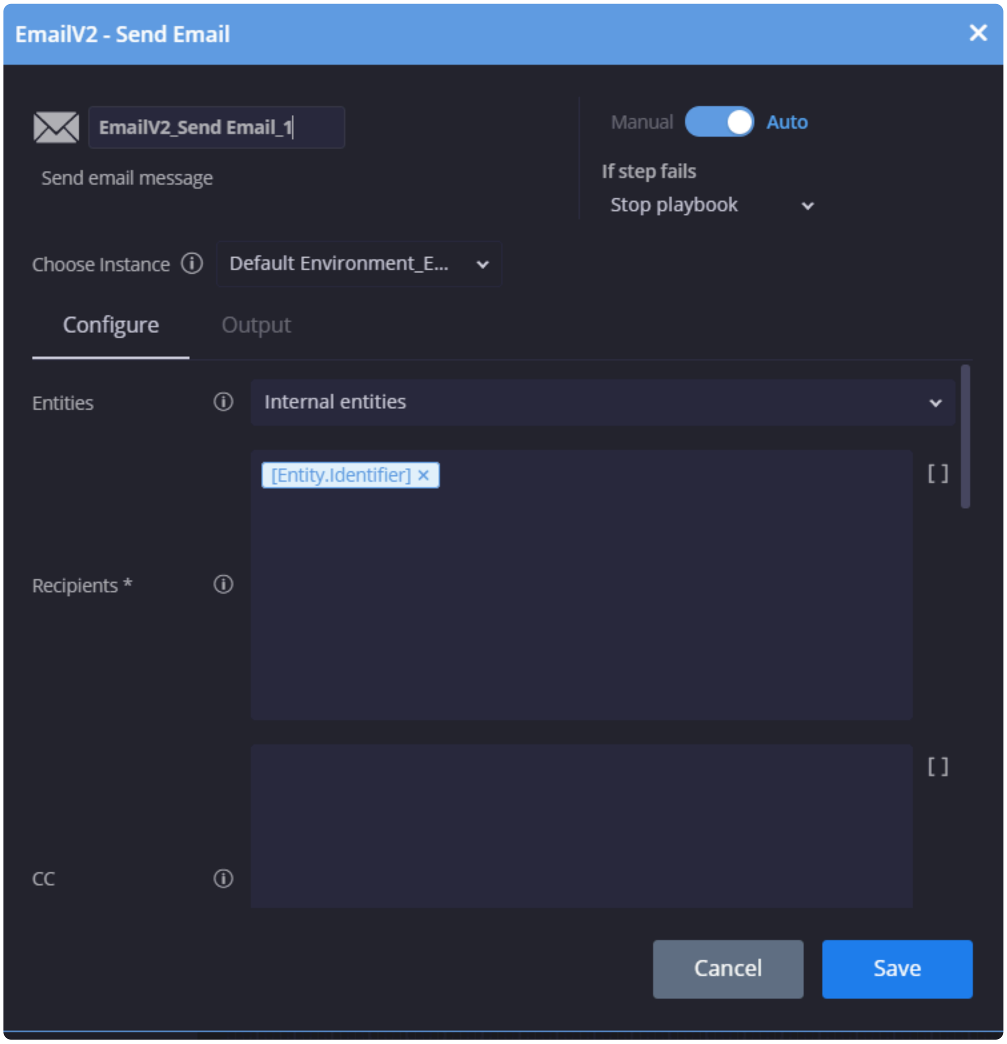
1. in the Actions tab, click on the down arrow next to an Integration name and select the action item. In this example, select Email > Send Email.
2. Drag and drop the Send Email item to the Final Step or to the blue dots between existing actions.



3. Click to open the dialog box. The dialog box shows the name and description of the Action as well as the Action result as shown by the Output Name. For this procedure, we will pretend we are in the

middle of a DLP Use Case Playbook and fill out the fields accordingly.

4. Choose the Instance to use for this Playbook. For more information on Instances, refer to Marketplace.
5. Specify which entities the Action will run on.
6. Specify the email recipient for this action. For this example, we will add an Entity Identifier placeholder.
   To add a placeholder:
   a. In the Recipients field, click the placeholder icon [ ]
   b. In the Placeholder Selection, select Object > Entity. Property > Identifier.
   c. Click OK.
7. Click Save. The Action is saved as the Action name underscore Sub Action name.



EmailV2 - Send Email

EmailV2_Send Email_1

Send email message

Manual / Auto: Auto

If step fails: Stop playbook

Choose Instance: Default Environment_E...

Entities: Internal entities

Recipients *: [Entity.Identifier]

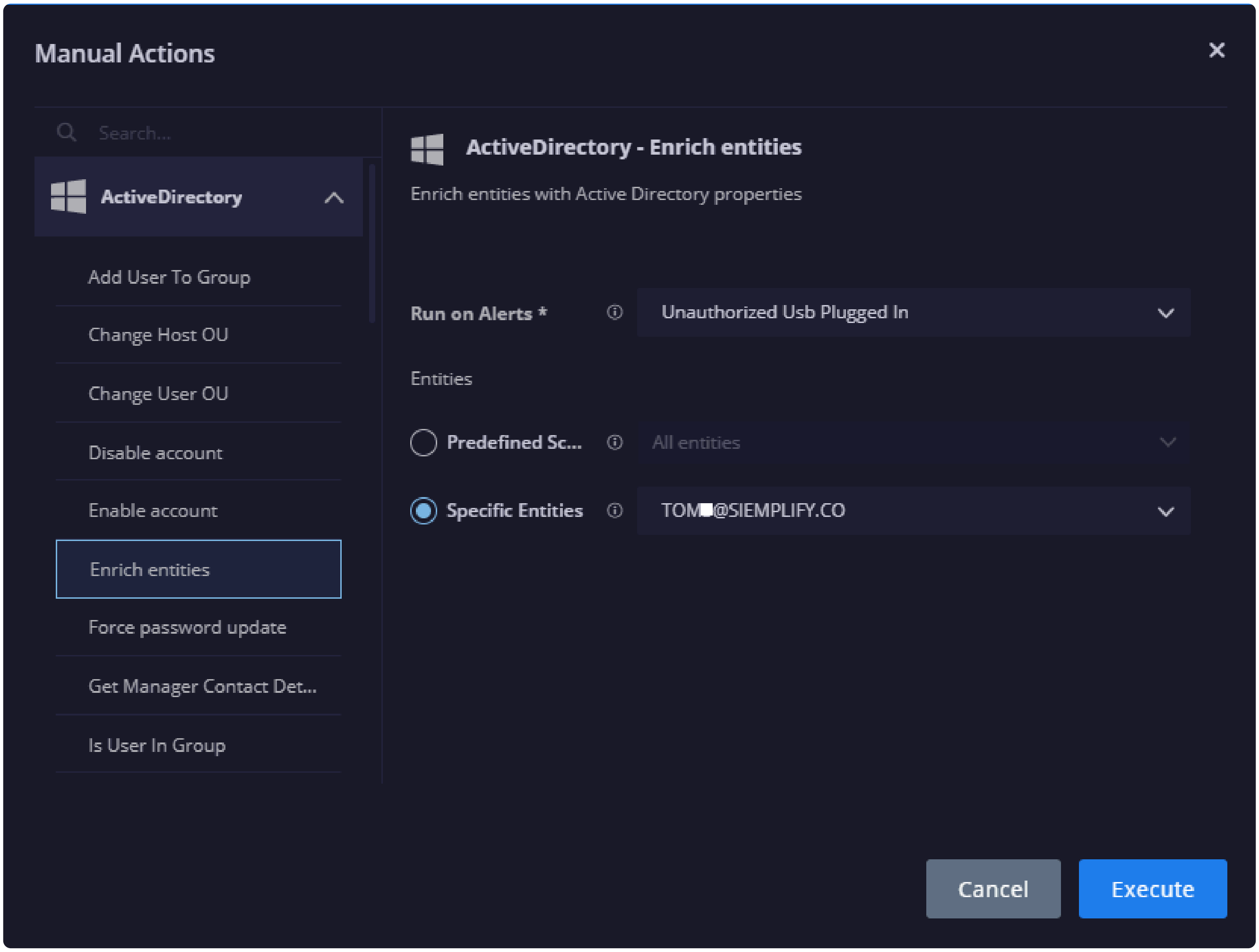
CC:

Enrichment

As defined above, enrichment is additional data collected on an entity (hosts, IPs, artifacts, etc.)

By clicking on an entity on the Cases tab, you can see all the existing attributes that belong to an entity. These attributes, also known as “enrichment” parameters can also be used in placeholders. If you find you are missing attributes on an entity, you can use an Action to execute enrichment on an entity. Below we will use a simple procedure to get more information on a User in Siemplify.

1. Navigate to the Cases screen and highlight a specific case.
2. Click Manual Action on the bottom right.
3. In the Manual Actions screen, select Active Directory > Enrich Entities. And then select a specific entity. In this example, we will select the User Tom. Click Execute. Once the green arrow appears, close this box.



ActiveDirectory - Enrich entities

Enrich entities with Active Directory properties

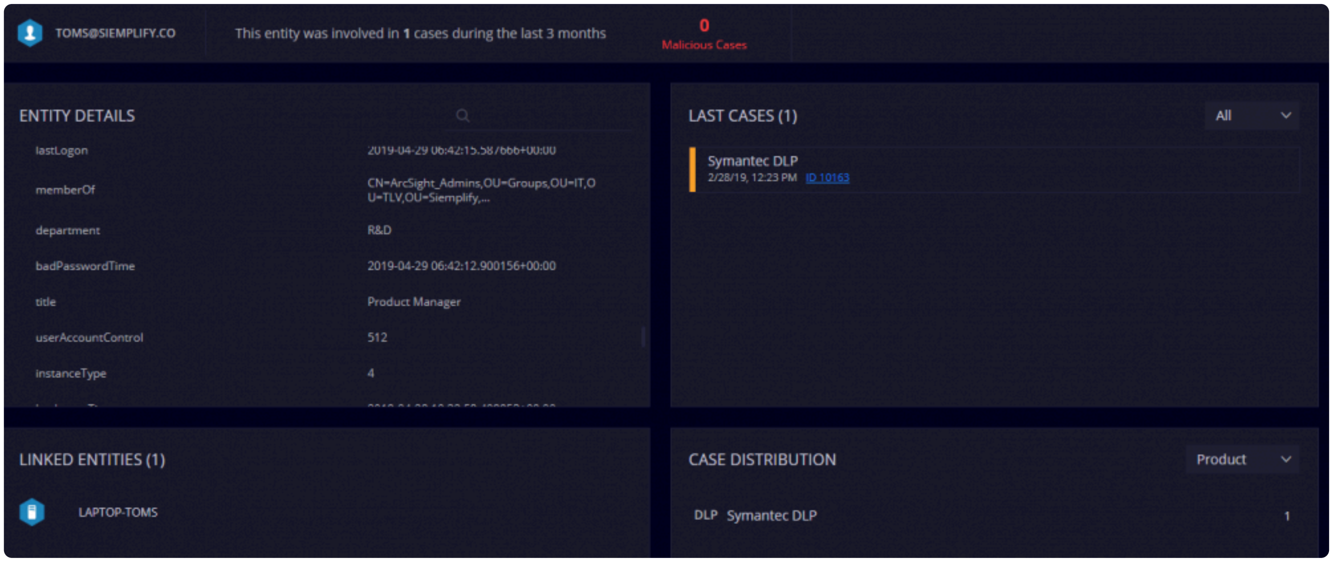
Run on Alerts * ⓘ Unauthorized Usb Plugged In

Entities

○ Predefined Sc... ⓘ All entities

● Specific Entities ⓘ TOM[redacted]@SIEMPLIFY.CO

4. In the Context Details pane, click on the entity Tom. A new Entity screen appears. Scrolling down displays the department that Tom belongs to.



TOMS@SIEMPLIFY.CO — This entity was involved in 1 cases during the last 3 months — 0 Malicious Cases

ENTITY DETAILS

lastLogon	2019-04-29 06:42:15.587666+00:00
memberOf	CN=ArcSight_Admins,OU=Groups,OU=IT,OU=TLV,OU=Siemplify,...
department	R&D
badPasswordTime	2019-04-29 06:42:12.900156+00:00
title	Product Manager
userAccountControl	512
instanceType	4

LAST CASES (1) — All

Symantec DLP
2/28/19, 12:23 PM ID 10163

LINKED ENTITIES (1)

LAPTOP-TOMS

CASE DISTRIBUTION — Product

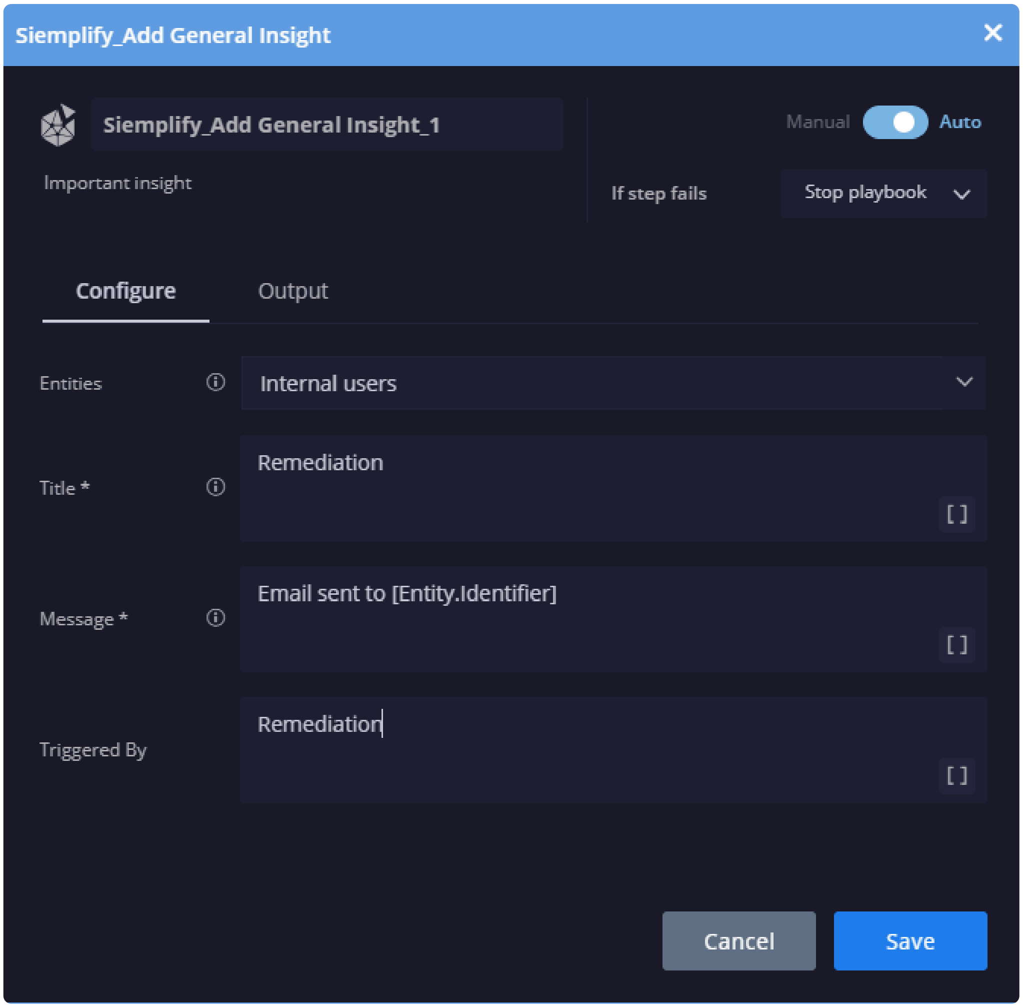
DLP	Symantec DLP	1

5. Return to the main Case screen. All the enrichment attributes are now in the Siemplify platform and are treated as entities in and of themselves. For example, department now can be chosen as an entity. This will be shown in the Create a new Entity procedure below.

Insights

During a Playbook you can choose to highlight specific Insights that are the result, or conclusions, of an action. You can choose to run an Insight on an entity (this will run on all selected entities as part of the Playgroup) or run a general Insight (which will run once during the Playbook). In the procedure below, we will choose an Action that you might find in the middle of a DLP Detection Use Case Playbook. In this procedure we will highlight the Remediation Email.

1. In the Actions column, select Siemplify > Add General Insight, and drag and drop it into the Final Step box.
2. Click on the Siemplify_Add General Insight box. Fill out Title, Message and Triggered by. Notice that we used a Placeholder for the Entity_Identifier in the Message field. Click Save.



Siemplify_Add General Insight

Siemplify_Add General Insight_1

Important insight

Manual / Auto

If step fails: Stop playbook

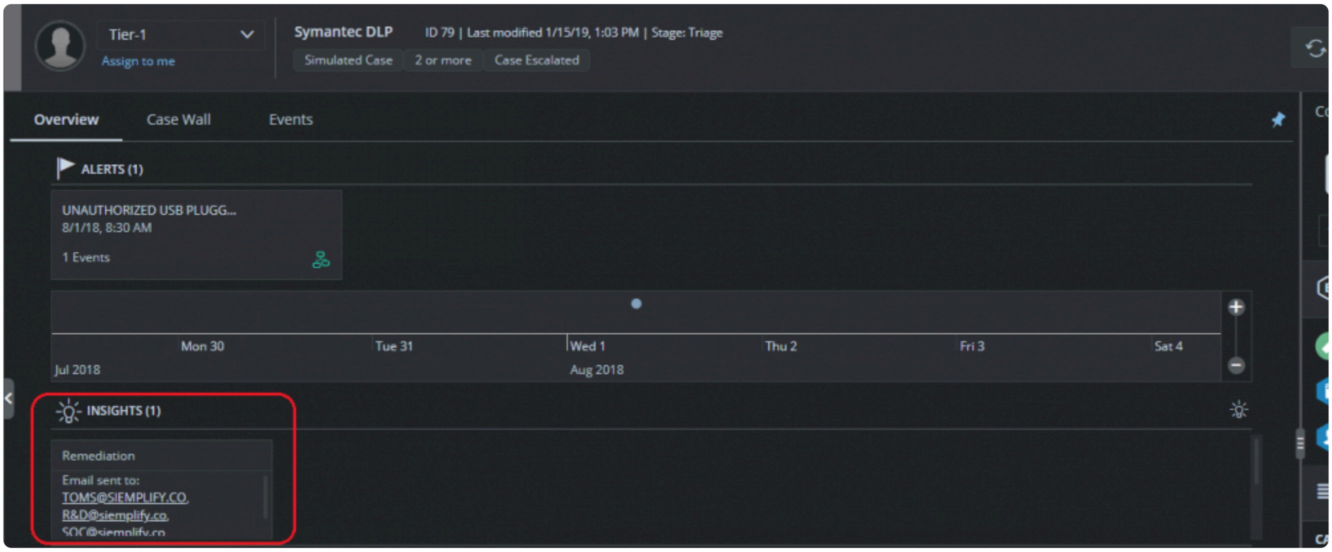
Entities: Internal users

Title *: Remediation

Message *: Email sent to [Entity.Identifier]

Triggered By: Remediation

3. When this Playbook is run, you will see this Insight highlighted in the Insight field as follows.



Symantec DLP ID 79 | Last modified 1/15/19, 1:03 PM | Stage: Triage

Simulated Case | 2 or more | Case Escalated

UNAUTHORIZED USB PLUGG...
8/1/18, 8:30 AM
1 Events

Remediation

Email sent to: TOMS@SIEMPLIFY.CO, R&D@siemplify.co, SOC@siemplify.co

Entity

The analyst will choose the required entity when building the Playbook. There are different sets of entities that the Action will run on. You can also choose to add new entity sets.

To create a new entity for a single Playbook:

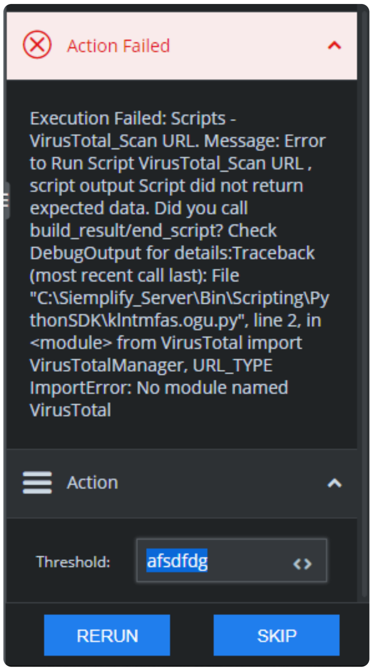
1. In the Actions column, select Flow > Entity Selection, and drag and drop it into the Final Box.
2. Click on Entity Selection.
3. Select the required entity parameters. In this example, we will select the Department entity (that is now populated in the system due to the Enrichment Action we ran above). And have it equals to R&D. Click Save.
4. The new entity set is saved under the name Entity_Selection_1. and is available for use when choosing any new entity in the specific Playbook. Note that if you create several new Entity Selections – they will be named according to ascending numbers after the underscore.

Removing an Action

During the building of the Playbook, you can remove an Action from the Final Step without any warning. If you remove an action which is connected to another action, you will receive a confirmation message as this could significantly impact the running of the Playbook.

Re-running an Action

The Playbook builder might have designated a Playbook to stop if an Action fails. If this happens, click on the failed Action and an error message will display in the right pane. This gives you the chance to correct a parameter that you might have mistakenly inputted and then you can Re-Run the action.



Execution Failed: Scripts - VirusTotal_Scan URL. Message: Error to Run Script VirusTotal_Scan URL , script output Script did not return expected data. Did you call build_result/end_script? Check DebugOutput for details:Traceback (most recent call last): File "C:\Siemplify_Server\Bin\Scripting\PythonSDK\klntmfas.ogu.py", line 2, in <module> from VirusTotal import VirusTotalManager, URL_TYPE ImportError: No module named VirusTotal

Threshold: afsdfdg

6.1.1.1. Using Expression Builder

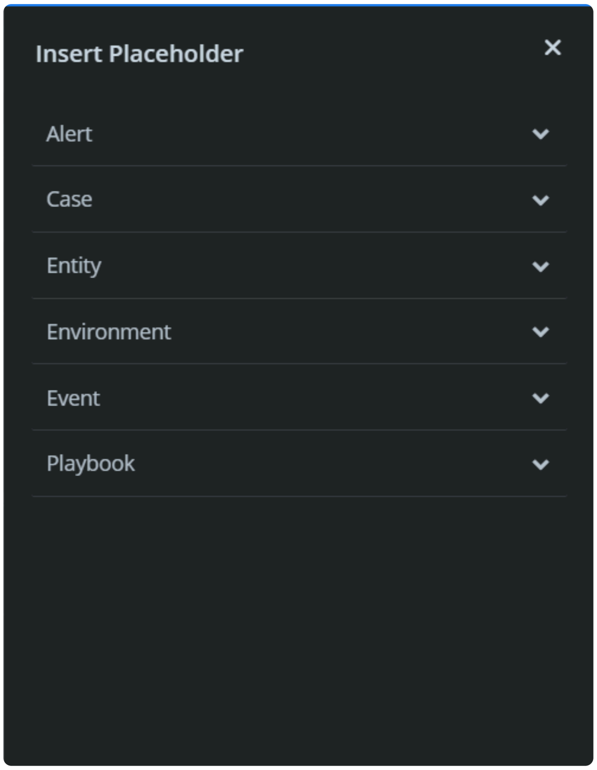
Once you have selected a Placeholder to use for the Parameter within the Action, you have the option to use the JSON results. Having access to the JSON results provides you with a huge amount of information that the action returns which you can then utilize in successive Playbook actions and flows.
The JSON result data can be manipulated using the Expression Builder in order to extract the relevant data for the action input.

The following Pipe functions are supported:

- First (x) – Return first X elements of an array
- Last (x) – Return last X elements of an array
- Min (KeyPath) – return an element of an array by the minimum
- Max (KeyPath) – return an element of an array by the maximum
- Filter (ConditionKey, Operator, Value) – Filter objects by field
- DateFormat (“pattern”) – format date by specific pattern (‘yyyy/dd/mm HH:mm:ss’) to supported format (“YYYY-MM-DDThh:mm:ssZ”)
- Count () – return the number of elements in expression
- OrderBy (KeyPath, “Direction”) – order array by specific child field
- toLower () – convert expression to lower case letters
- toUpper () – convert expression to upper case letters
- Replace (“x”, “y”) – replace string in an expression

- Distinct () – remove duplicates from an array

Below are some examples of using the new functions.
To add a new placeholder:
Click [] in the Parameter. The Placeholder window opens with various categories.



Insert Placeholder

Alert

Case

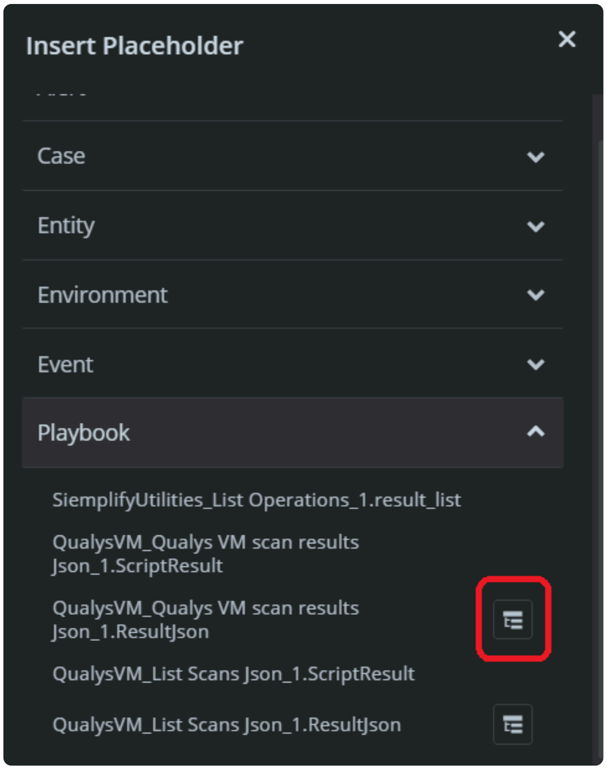
Entity

Environment

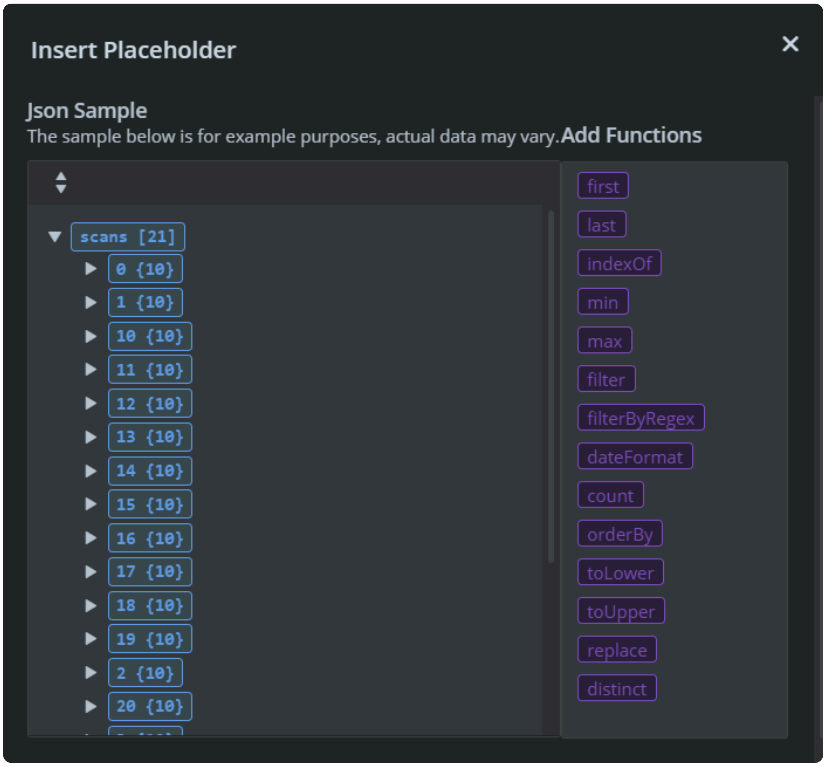
Event

Playbook

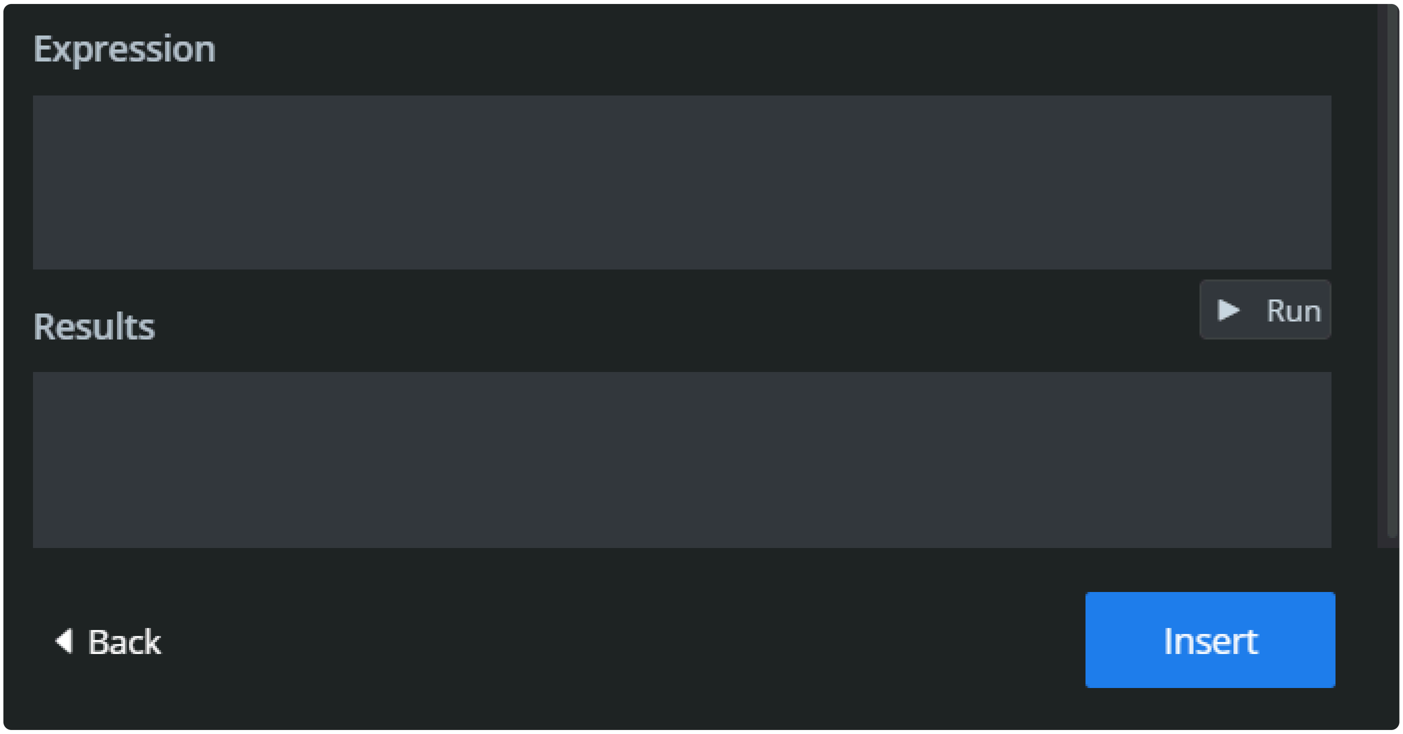
Navigate to the Playbook category, choose the required JSON Result and click the pipe builder icon.


Insert Placeholder
Case
Entity
Environment
Event
Playbook
SiemplifyUtilities_List Operations_1.result_list
QualysVM_Qualys VM scan results Json_1.ScriptResult
QualysVM_Qualys VM scan results Json_1.ResultJson
QualysVM_List Scans Json_1.ScriptResult
QualysVM_List Scans Json_1.ResultJson

The screen opens with a JSON Sample and the list of supported functions. Note that the sample appears in this window is an example. Actual data will depend on the customer's product data schemas and configuration. This screen also contains an Expressions area for you to edit the functions and pipes.



The sample below is for example purposes, actual data may vary.



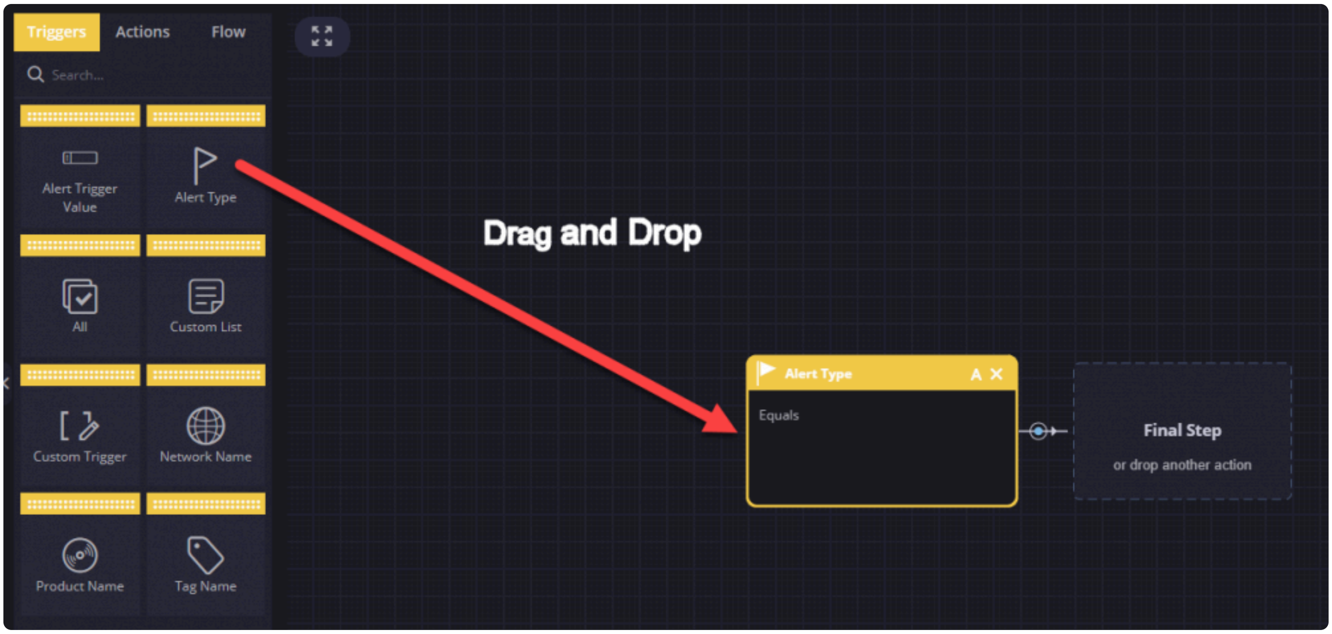
Click on Run to check the functions against the sample and see the Results.

6.1.2. Triggers

A trigger is defined during the beginning phase of creating a playbook. It specifies the instance for which a playbook must be triggered in case of an alert detection. To add the trigger to a playbook, you must drag and drop one of the triggers to the yellow Drag Trigger box in the middle pane.

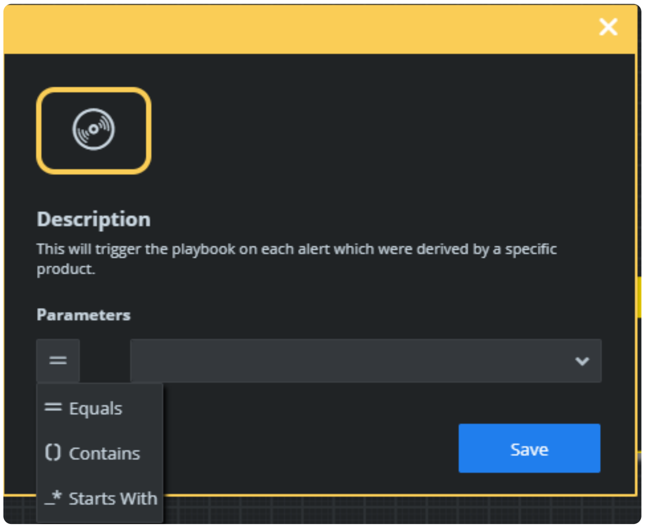
After dropping the trigger, its name and symbol appear on the Drag Trigger box.
The following Triggers are currently supported:

- Alert Trigger Value
- Alert Type
- Tag Name
- Product Name
- Network Name
- Custom List
- Custom Trigger
- All: Playbook is run on every alert that is ingested into the Siemplify platform.



To add a trigger:

1. Click on Alert Type and drag it to the trigger box.
2. Click on it to open a new Description popup window.
3. Under Parameters, click the equals sign and select either Equals, Contains or Starts With option from the signs menu.

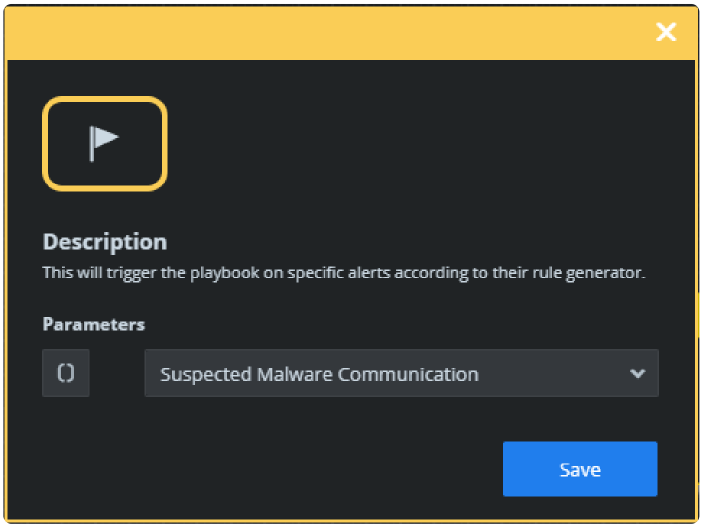


Description

This will trigger the playbook on each alert which were derived by a specific product.

Parameters

4. Select the required parameter from the drop-down menu. In this case, we have chosen an Alert Type based on any alert that contains Suspected Malware Communication.
   Note that once you specify the trigger parameter and save it, the parameter name appears as the title header of the Drag Trigger box and is non-editable.



Description

This will trigger the playbook on specific alerts according to their rule generator.

Parameters

Suspected Malware Communication

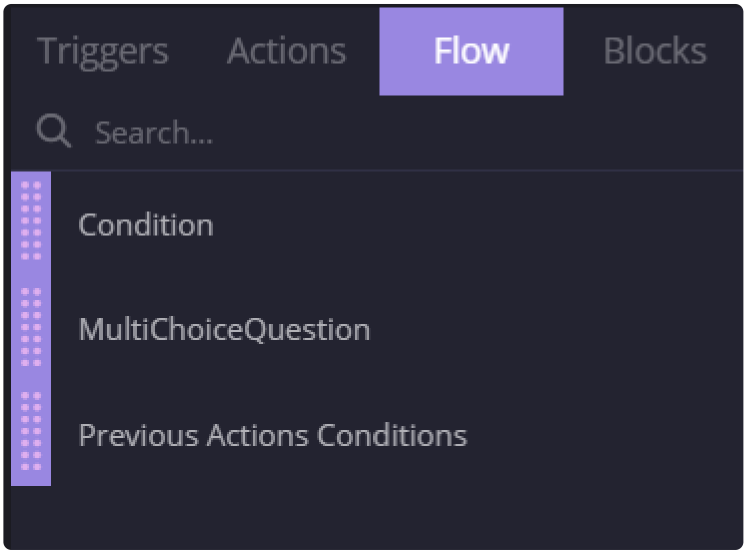
5. Click Save. The specified trigger parameter is saved and you return to the playbook page where you can define the next set of components (actions and/or flow) for the playbook.

6.1.3. Flow

The Flow component determines the next steps of a playbook by forcing the flow into decisions. This is executed by utilizing a branching system.

The following Flow options are available:

- Condition: This is based on complex conditions (based on placeholders) including existing case data and the Previous Actions flow.
- Multi Choice Question: This involves questions that must be answered by analysts manually.
- Previous Actions Conditions: This is based on data fetched by previous actions that were executed in this playbook.



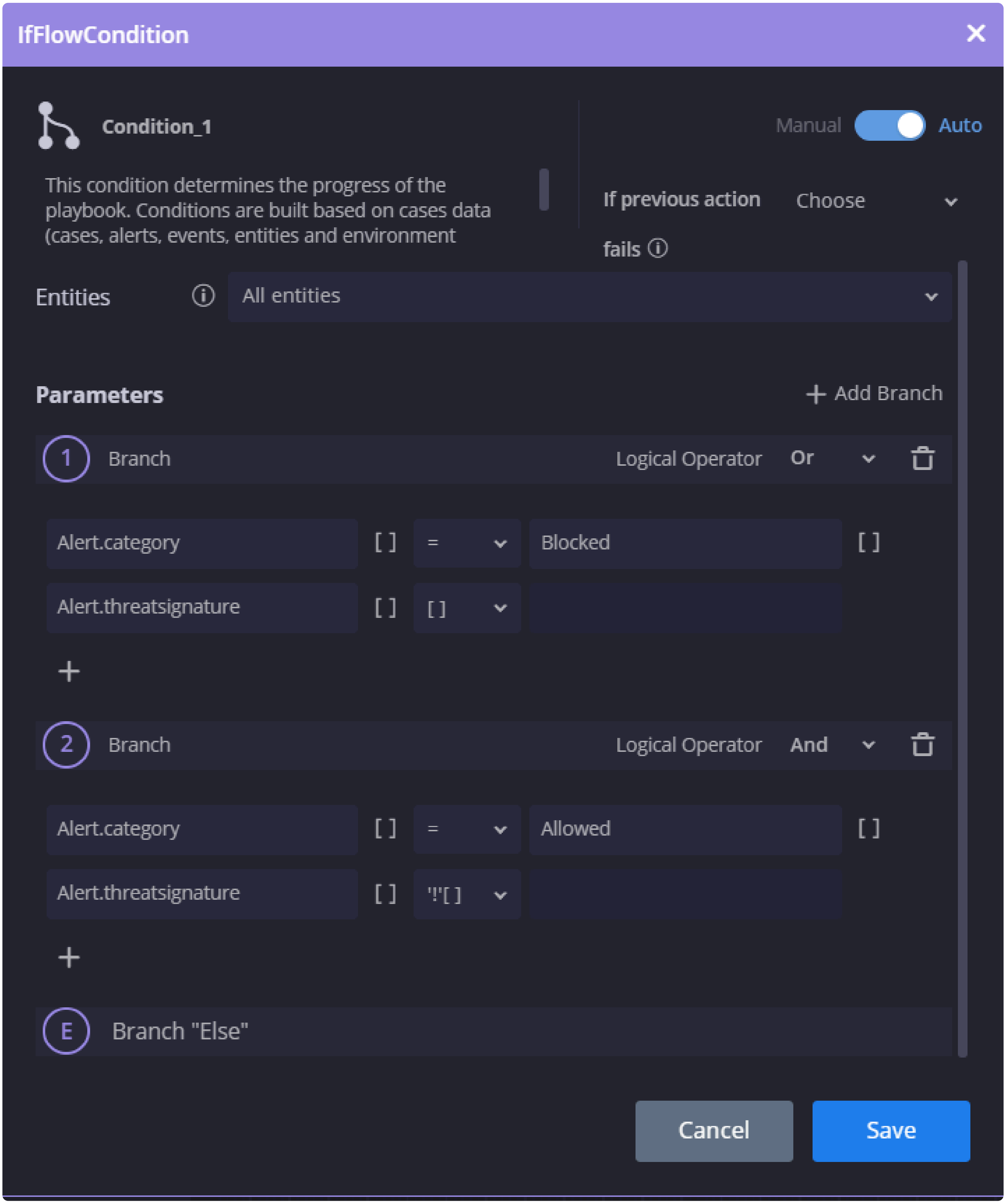
To add a Condition flow:

1. Drag and drop the Condition into the Final Step box, or between two actions depending on how you are building your Playbook.
2. Click on the Condition to open the dialog box.
3. Select the required Entities.
4. Decide how many branches you want to create. Each branch has an OR between them.
5. Select the parameter(s) for each branch.
   To add a parameter:
   a. Select the required event/case/alert parameters or enriched data that is in your Siemplify platform. (Note that for new users this will be empty if you have not ingested any alerts yet).
   b. Select the required operator: Equals to/Does not equal to. Contains/Does not contain. Starts with. Greater than/Smaller than.
   c. Choose a value.
      For this specific example, we will choose three branches (where the third branch is the Branch ‘Else’ Default Branch.)
      In Branch 1, we have blocked alerts **or** alerts without a threat signature, then do X (where X is whatever the next step of the Playbook is).
      In Branch 2, we have alerts that are allowed **and** whose threat signature is not empty.
      In Branch 3, we have the default “Else” branch.

Branch 1: Logical Operator set to **Or**.
Alert.CategoryOutcome = Blocked
Alert.ThreatSignature [] Empty

Branch 2: Logical Operator set to **And**

Alert.CategoryOutcome = Allowed
Alert. ThreatSignature ![] NotEmpty



IfFlowCondition

Condition_1

This condition determines the progress of the playbook. Conditions are built based on cases data (cases, alerts, events, entities and environment

Manual / Auto

If previous action fails: Choose

Entities: All entities

Parameters

1 Branch — Logical Operator: Or

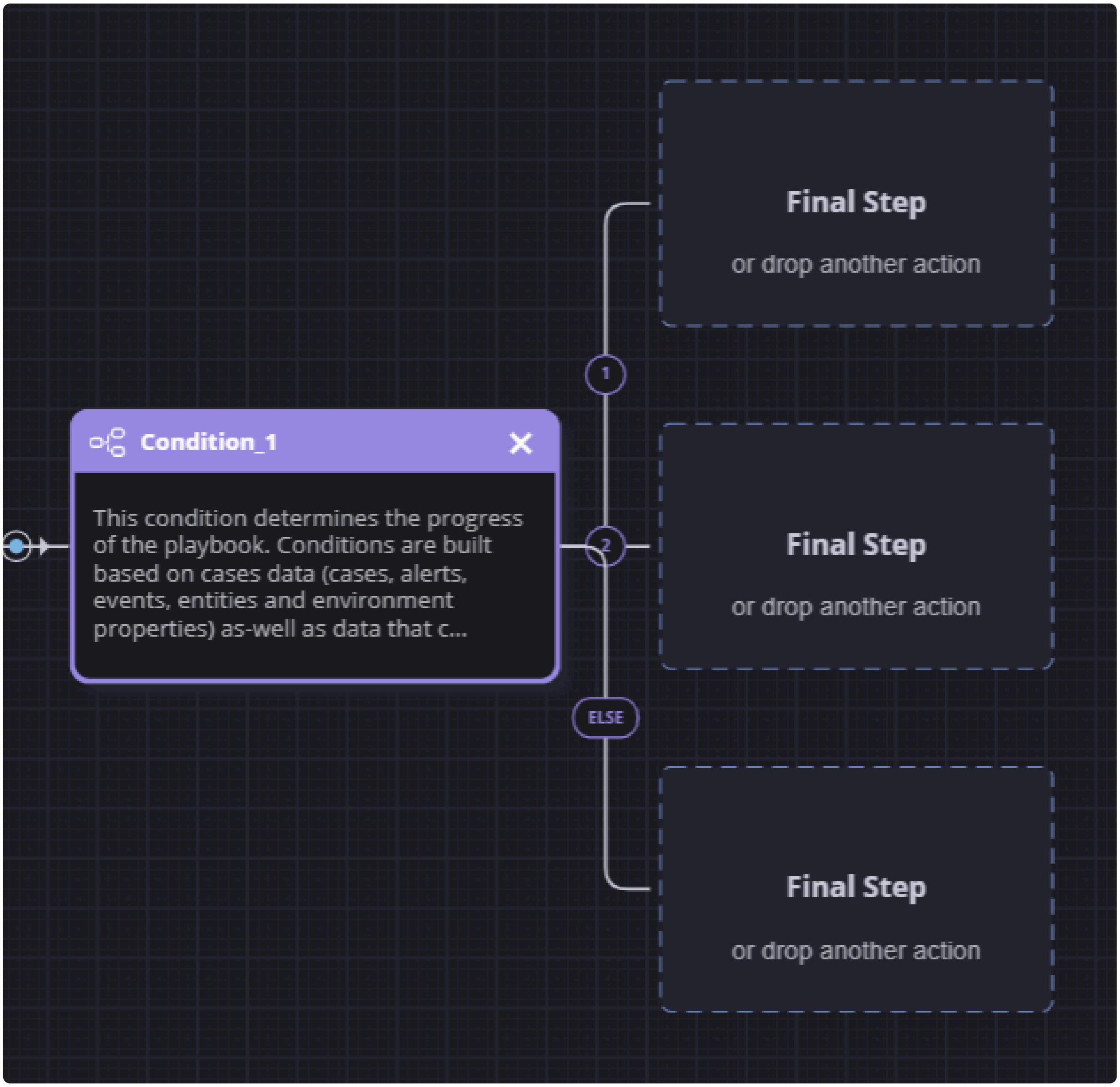
Alert.category	[ ]	=	Blocked	[ ]
Alert.threatsignature	[ ]	[ ]		

2 Branch — Logical Operator: And

Alert.category	[ ]	=	Allowed	[ ]
Alert.threatsignature	[ ]	'!'[ ]		

E Branch "Else"

6. Define a “fallback branch” to avoid failed conditions. If a condition is based on previous actions, and one of those actions failed (and skipped), the condition will continue to the fallback branch instead of stopping.
7. Click Save. The playbook now takes three branches: 1, 2 and E (Else). You would need to decide what the outcome is for at least ONE of the branches in order for the Playbook to be considered as complete. In order to choose a Fallback branch, see the procedure below.



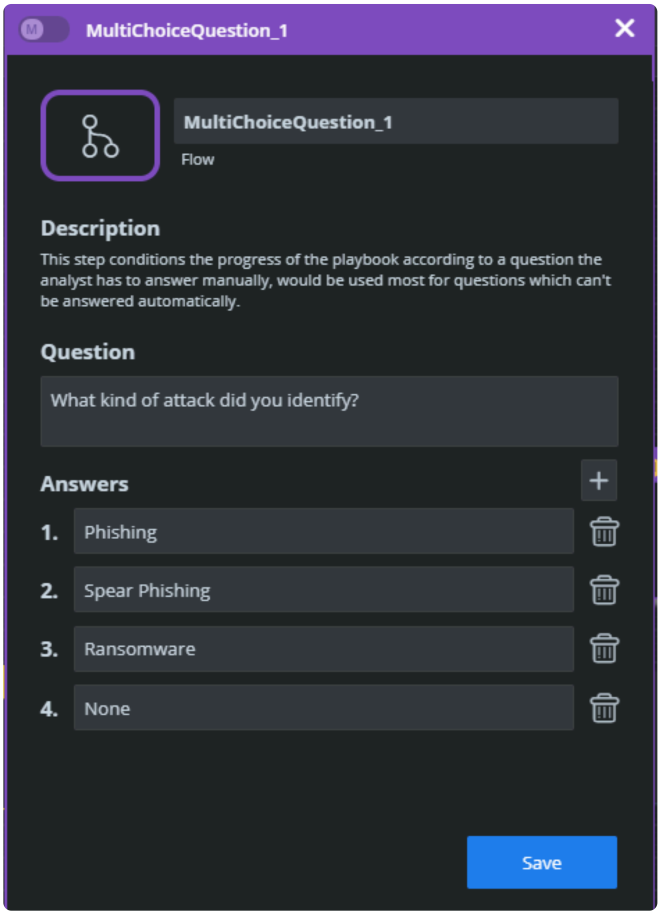
Condition_1

This condition determines the progress of the playbook. Conditions are built based on cases data (cases, alerts, events, entities and environment properties) as-well as data that c...

To add a Multi Choice Question flow:

1. Drag and drop the Multi Choice Questions into the Final Step box.

2. Click on the Multi Choice Questions to open the dialog box.
3. Add in a question and as many answers as you need. See the screenshot below for an example of the type of question and answers that might be useful for a Playbook.



MultiChoiceQuestion_1

MultiChoiceQuestion_1

Flow

Description

This step conditions the progress of the playbook according to a question the analyst has to answer manually, would be used most for questions which can't be answered automatically.

Question

What kind of attack did you identify?

Answers

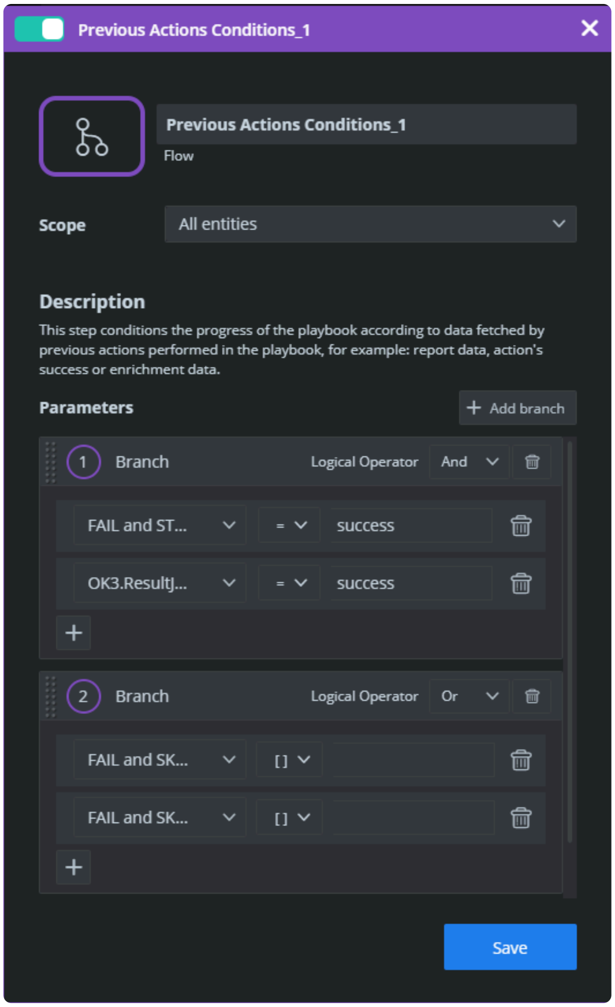
1. Phishing
2. Spear Phishing
3. Ransomware
4. None

4. Click Save. The playbooks now opens up four branches. You would need to decide what the outcome is for at least ONE of the branches in order for the Playbook to be considered as complete.

To add a Previous Actions Conditions flow:

1. Drag and drop the Previous Actions Conditions into the Final Step box.
2. Click on the Previous Actions Conditions to open the dialog box.
3. Decide how many branches you want to create. Each branch has an OR between them. To add a parameter:
   a. Select the required parameter. Note that the drop-down will only show you the Actions script results that are part of this Playbook.
   b. Select the required operator: Equals to/Does not equal to. Contains/Does not contain. Starts with. Greater than/Smaller than.
   c. Choose the value (the action result).

d. You can add more parameters to each branch and choose the Logical Operator: AND or OR.



Previous Actions Conditions_1

Previous Actions Conditions_1
Flow

Scope: All entities

Description
This step conditions the progress of the playbook according to data fetched by previous actions performed in the playbook, for example: report data, action's success or enrichment data.

Parameters

1 Branch — Logical Operator: And

FAIL and ST...	=	success
OK3.ResultJ...	=	success

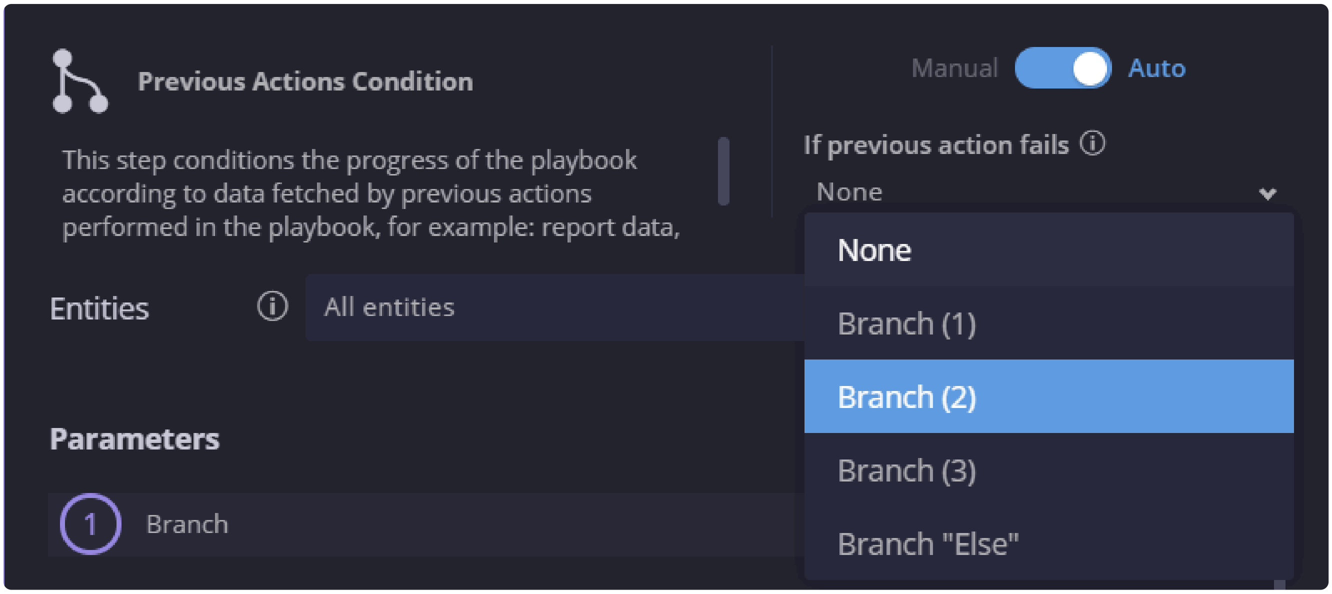
2 Branch — Logical Operator: Or

FAIL and SK...	[]	
FAIL and SK...	[]	

4. Click Save. The Playbook now opens three branches: 1, 2 and Else. You would need to decide what the outcome is for at least ONE of the branches in order for the Playbook to be considered as complete.

To define a Fallback branch:

1. In one of the Flows (Condition or Previous Actions Condition), select the branch that will be used as a fallback branch. Is this example, we have selected Branch 2.



Previous Actions Condition

This step conditions the progress of the playbook according to data fetched by previous actions performed in the playbook, for example: report data,

Manual Auto

If previous action fails ⓘ

None

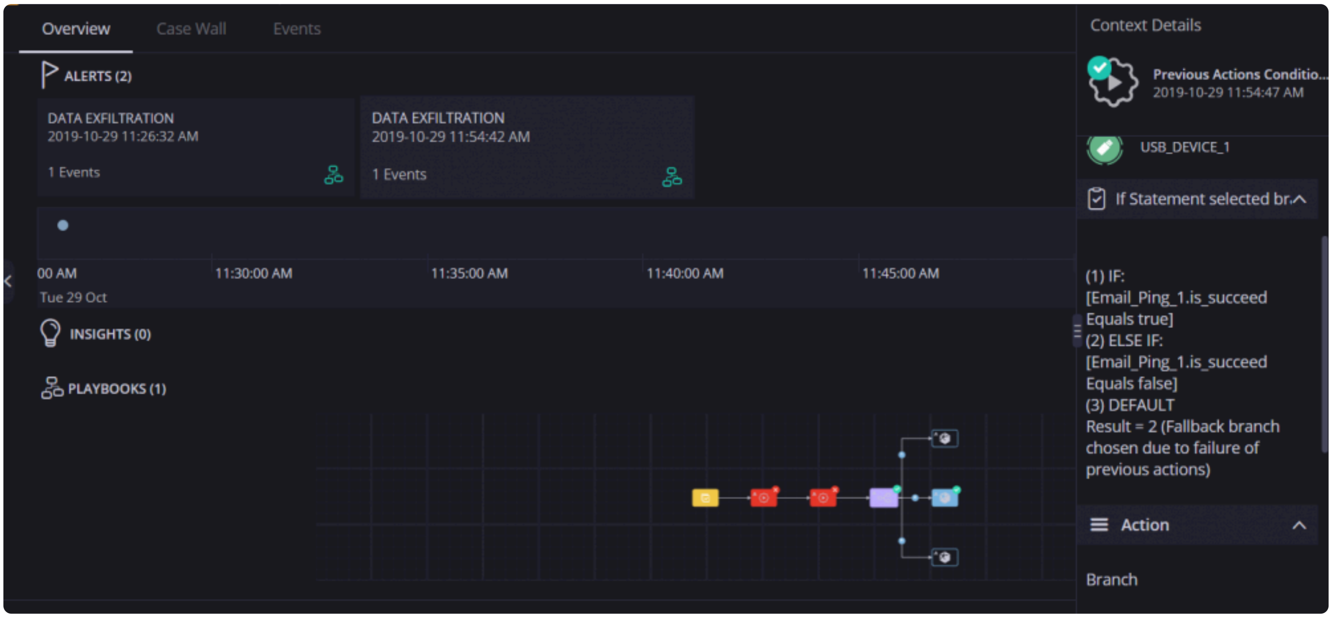
Entities ⓘ All entities

Parameters

1 Branch

Note that it is not mandatory to add a fallback branch.

2. Once the Playbook runs, and the previous actions fail, the Playbook will choose the fallback branch and continue.



(1) IF:
[Email_Ping_1.is_succeed Equals true]
(2) ELSE IF:
[Email_Ping_1.is_succeed Equals false]
(3) DEFAULT
Result = 2 (Fallback branch chosen due to failure of previous actions)

Action

Branch

Removing a Flow

When removing a flow from within a Playbook, the system will ask you whether you want to remove the entire branch or just one aspect of it.

Merge Branches

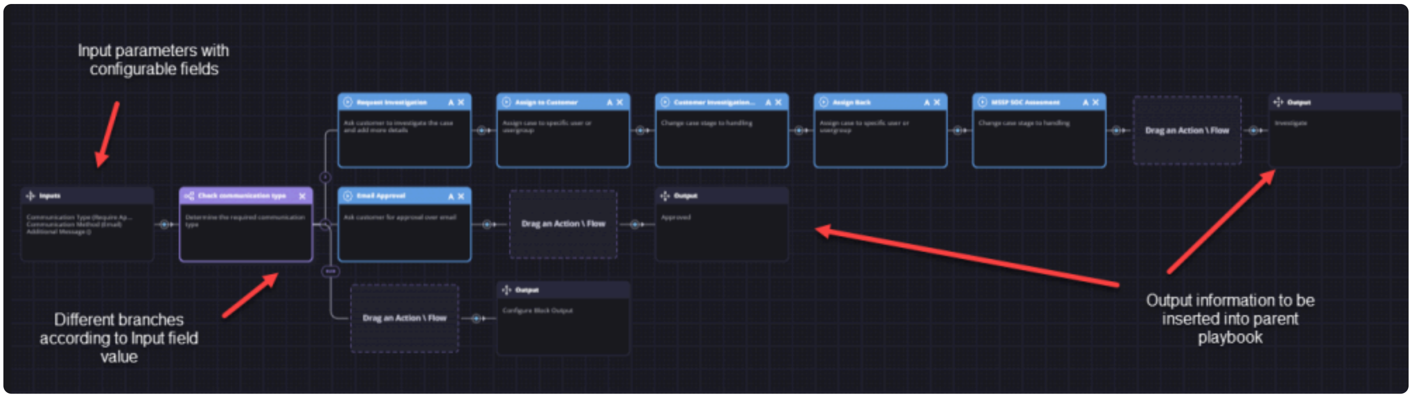
You can merge different branches of the Playbook into one branch. This is done by dragging an action from one of the branches and dropping it into the Final Step of another branch. The Playbook can continue after this or end here.

6.1.4. Playbook Blocks

Blocks are mini playbooks that users can create and reuse in other playbooks. The Blocks can implement workflows and logical decisions that might be useful in multiple playbooks. When you edit or change a Block, all playbooks using it will be affected which allows easy maintenance and playbooks improvement. When Blocks are used within other playbooks, users can configure Input parameter fields into the Block to alter its inner flow of actions.
The Block can also return an Output value into the parent playbook to allow interaction and conditioning between the two.

Before you create these blocks, it's advisable to spend time initially to map out specific processes that you can can easily reuse in parent playbooks, as well as giving thought to Input fields which can be configured per need.

Let's give below an example of a reusable Block.

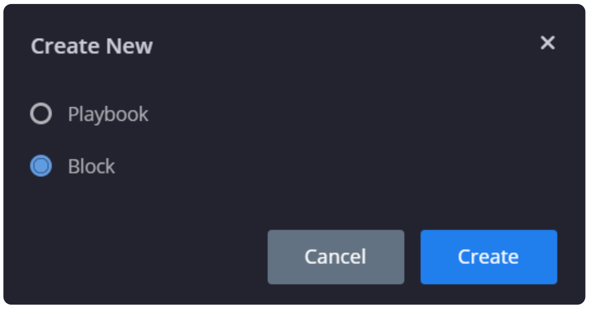

Inputs
Communication Type (Require Ap...
Communication Method (Email)
Additional Message ()
Check communication type
Determine the required communication type
Request Investigation
Ask customer to investigate the case and add more details
Assign to Customer
Assign case to specific user or usergroup
Customer Investigation...
Change case stage to handling
Assign Back
Assign case to specific user or usergroup
MSSP SOC Assessment
Change case stage to handling
Drag an Action \ Flow
Output
Investigate
Email Approval
Ask customer for approval over email
Drag an Action \ Flow
Output
Approved
Drag an Action \ Flow
Output
Configure Block Output

Input parameters with configurable fields

Different branches according to Input field value

Output information to be inserted into parent playbook

1. In the Playbook screen, click the + icon and select Block and Create.

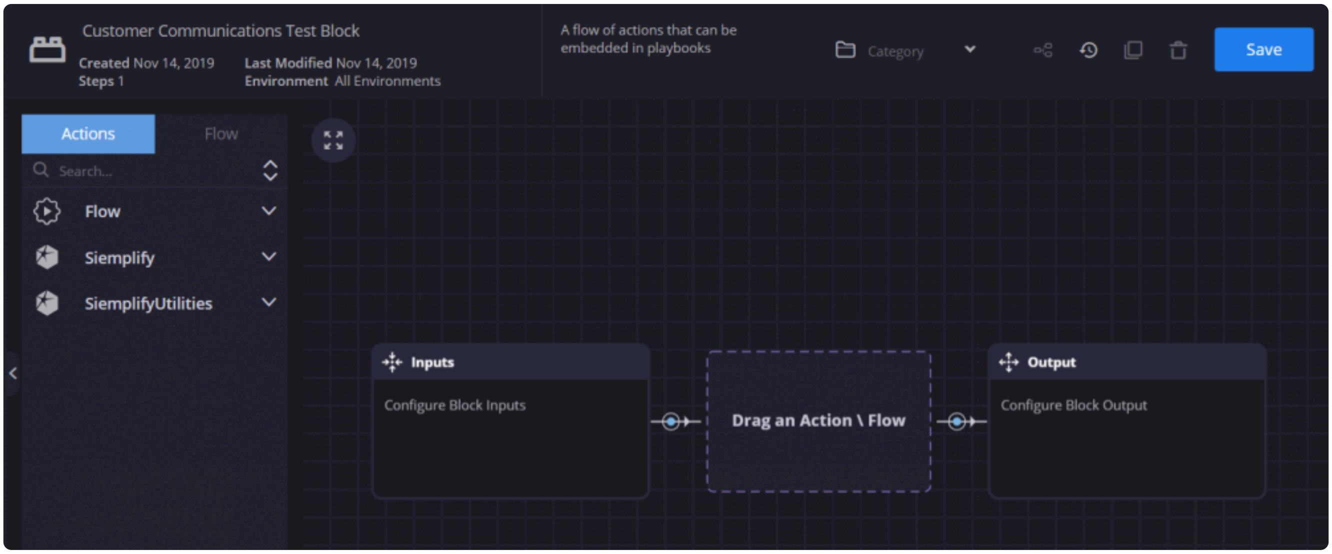


Create New

○ Playbook

● Block

2. In the screen that opens, fill out the name of the new Playbook Block at the top of the screen. For this example, we will create a Block that handles all communication between the SOC and its clients.



Customer Communications Test Block

Created Nov 14, 2019 Last Modified Nov 14, 2019

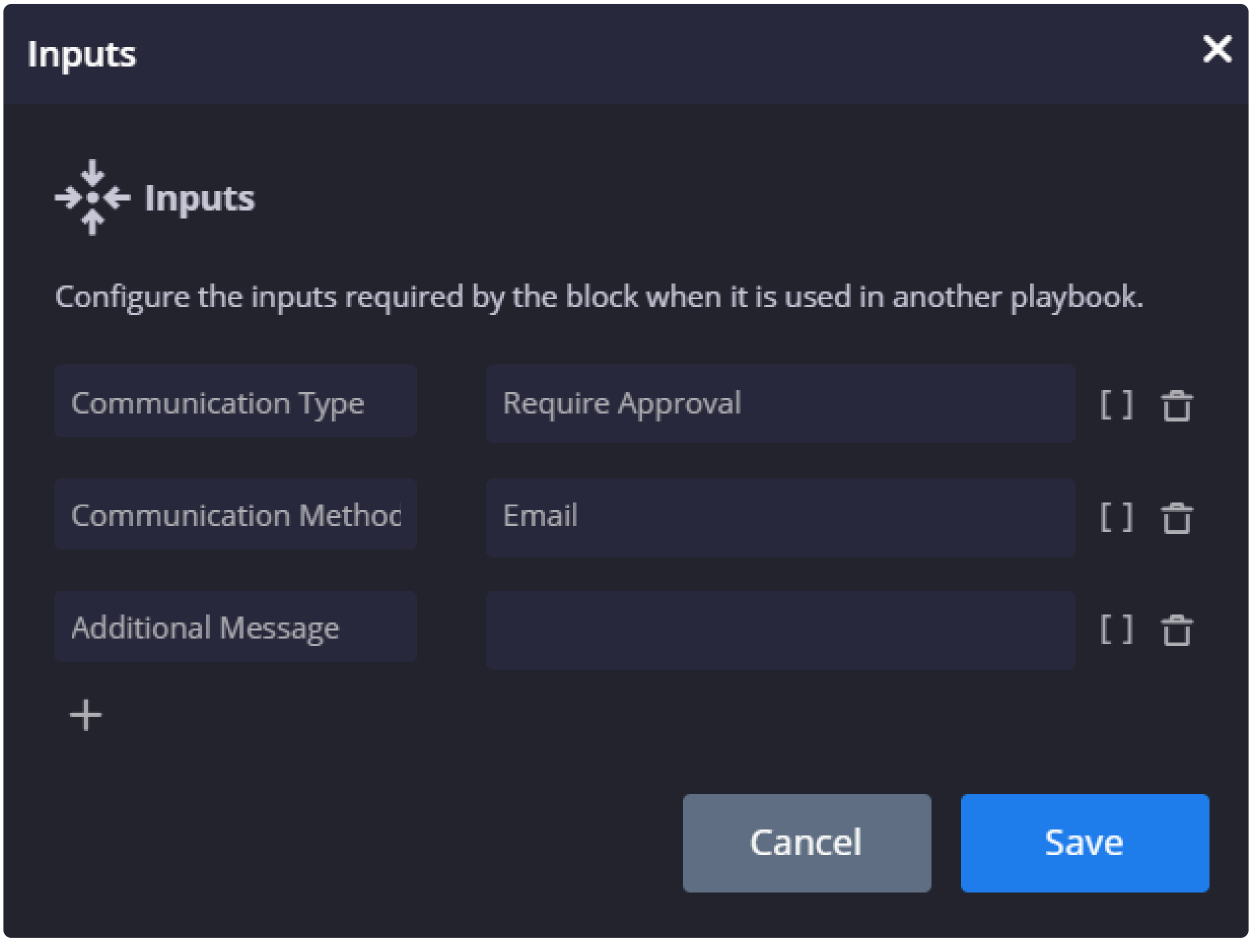
Steps 1 Environment All Environments

A flow of actions that can be embedded in playbooks

3. Let's start off by adding Input parameters. Click on the Input box and add the following fields (and default values):
   - Communication Type – Require Approval (where we have decided we will have two different communication types: Require Approval, Investigate)
   - Communication Method – Email
   - Additional Message – leave blank

     We will use these inputs to condition the flow of the Block

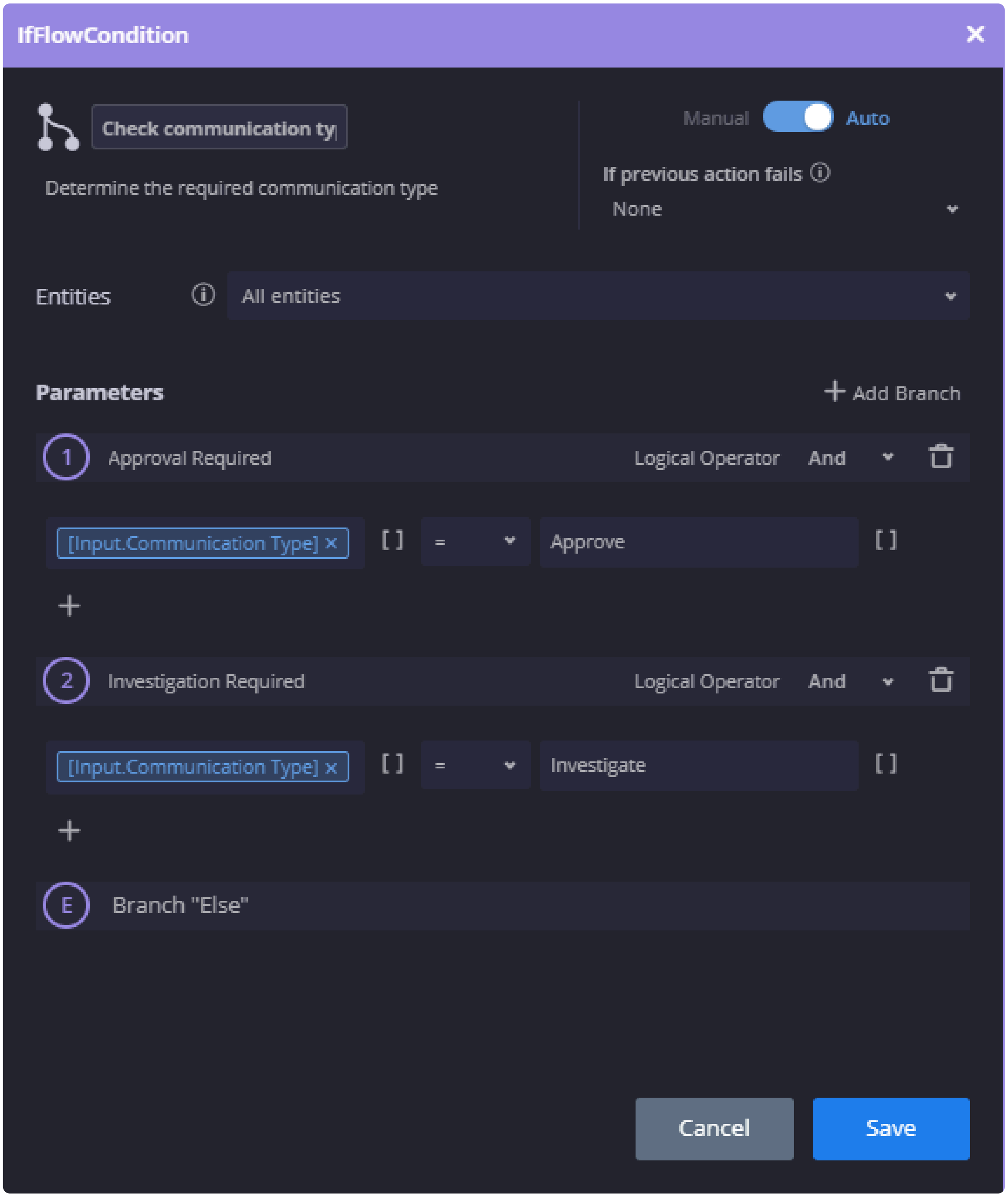
     If we add values here, they will act as default values. Note that they can be changed for each and every block after you have inserted them into the parent playbook.



Configure the inputs required by the block when it is used in another playbook.

Communication Type	Require Approval
Communication Methoc	Email
Additional Message	

- Let’s now add a Flow step which will direct the Playbook in a different direction according to which Input Type is entered.
  The types as we mentioned above are:
  Investigate
  Requires Approval
  Now let’s put these into different branches. Use the placeholders to pick up the Input types. As you can see in the following screenshot, we have two branches and an Else branch. The default branch which would go with the default Input is branch 1.



IfFlowCondition

Check communication ty

Determine the required communication type

Manual Auto

If previous action fails: None

Entities: All entities

Parameters

1 Approval Required — Logical Operator: And

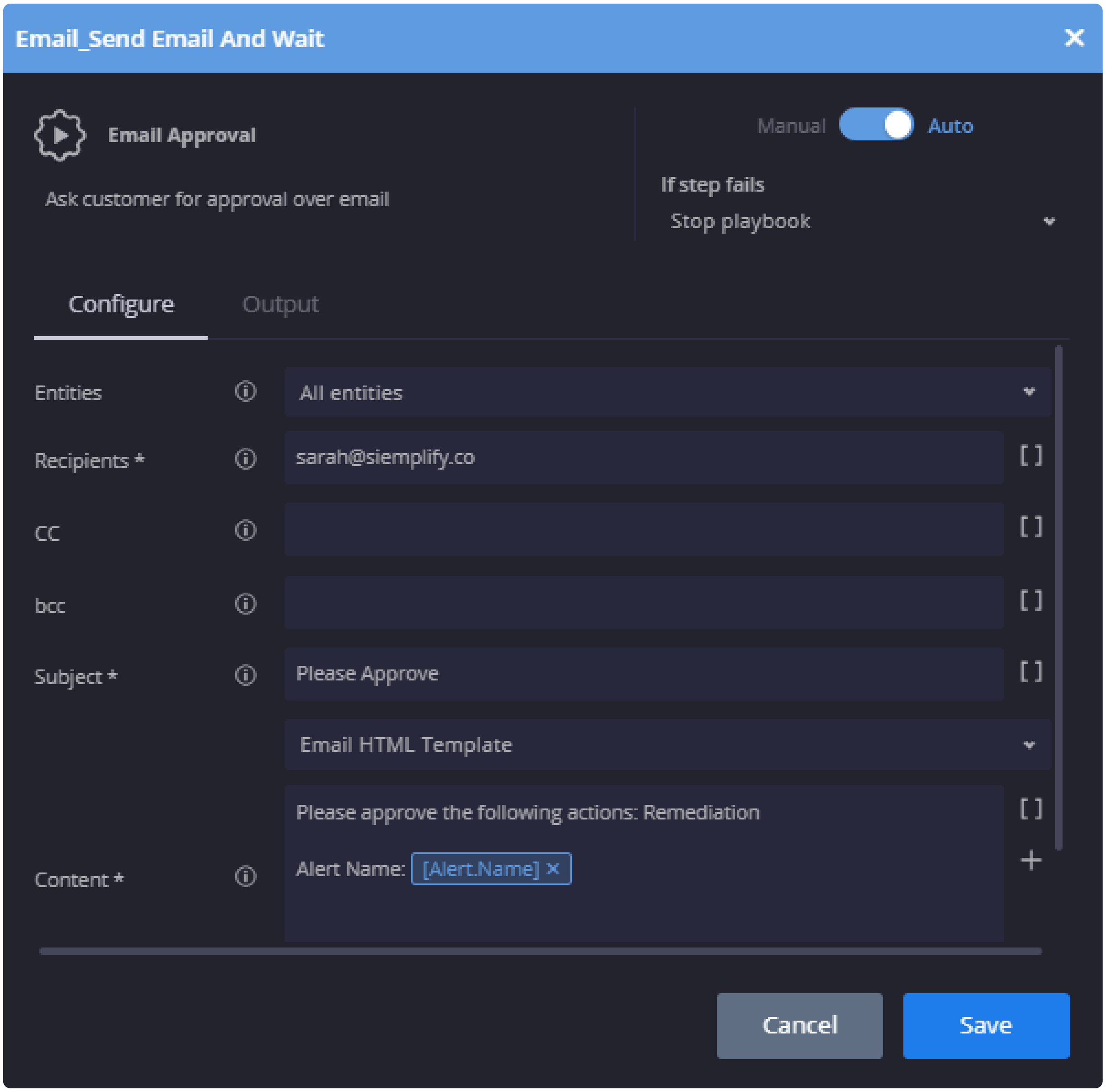
[Input.Communication Type] = Approve

2 Investigation Required — Logical Operator: And

[Input.Communication Type] = Investigate

E Branch "Else"

- The next stage would be to build action steps for each of the branches.
- Let’s start with branch 1 which is the Require Approval branch. In the Actions column, select Email > Send Email and fill in the required parameters. This step sends an email asking the user for approval for a security analyst to perform Remediation on their machine.



Email_Send Email And Wait

Email Approval

Ask customer for approval over email

Manual Auto

If step fails: Stop playbook

Configure | Output

Entities: All entities

Recipients *: sarah@siemplify.co

CC:

bcc:

Subject *: Please Approve

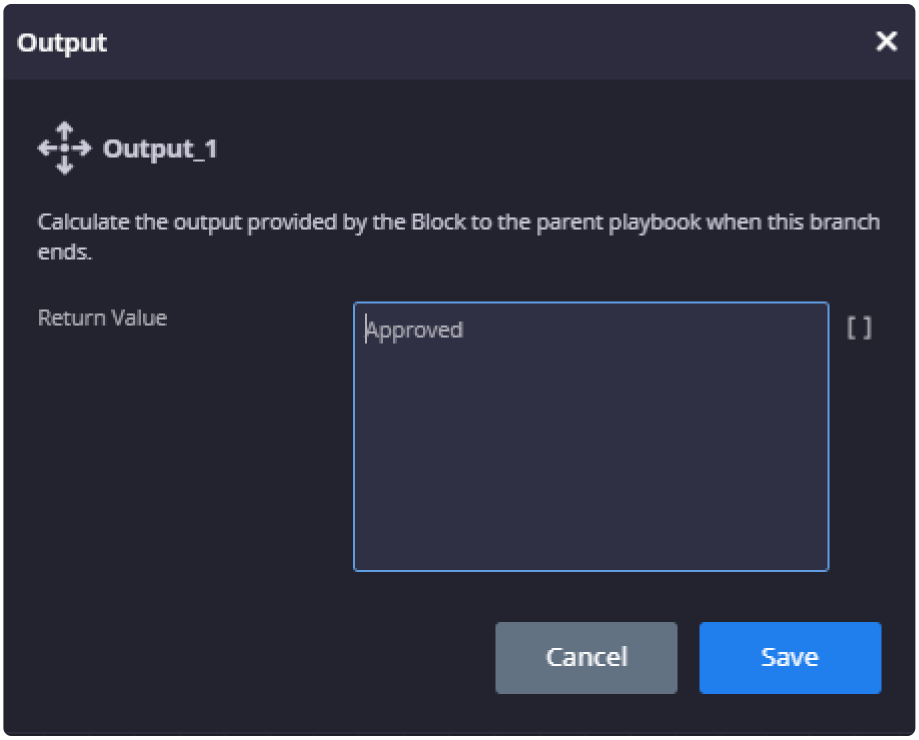
Email HTML Template

Content *: Please approve the following actions: Remediation

Alert Name: [Alert.Name]

Cancel | Save

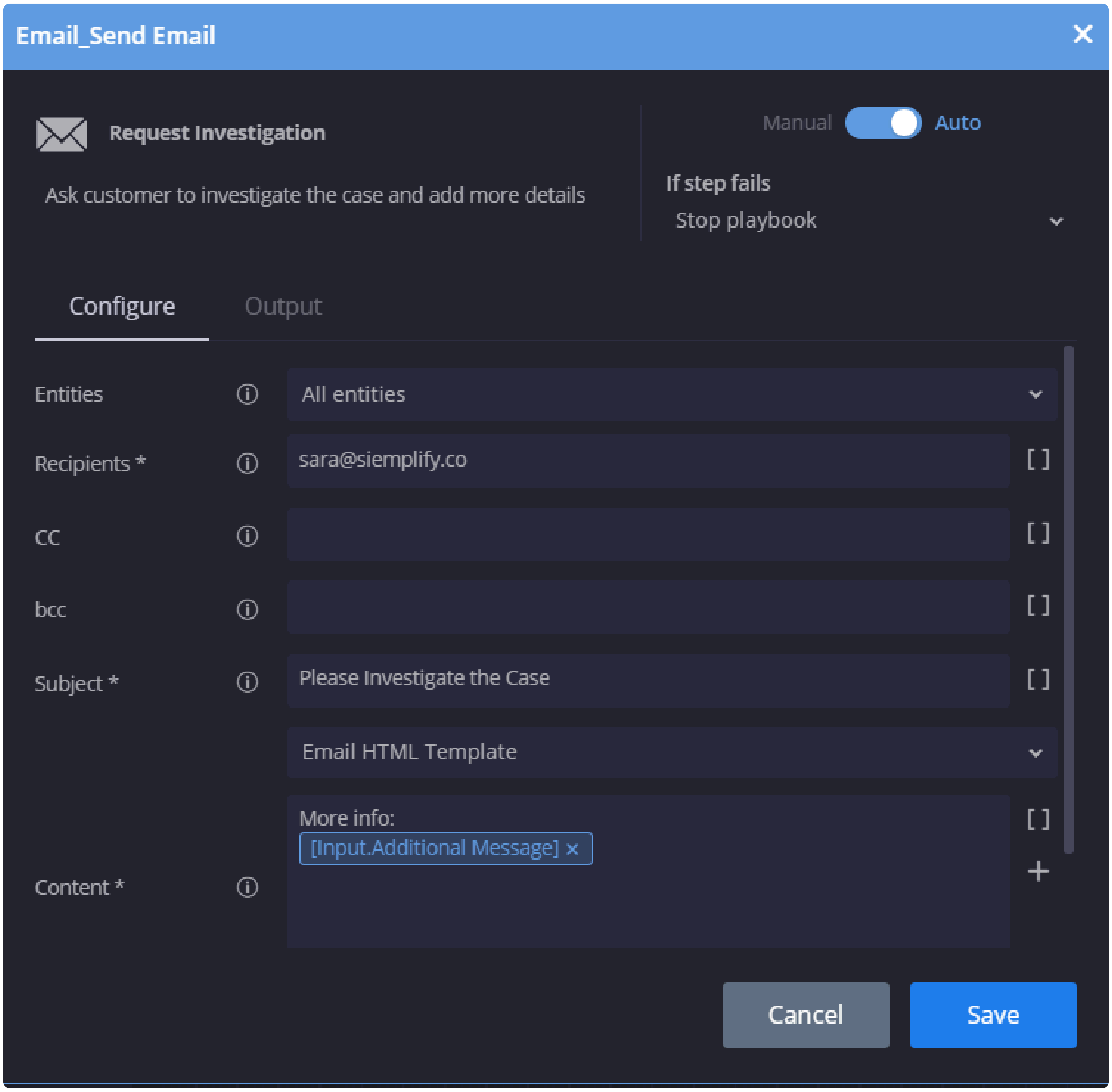
- In the next step, select Flow > Condition and fill in the required parameters. This step asks if the customer approved or not.
- In the Output step where the customer approved it, add the word Approved to be returned to the parent block.
- In the Output step of the Else branch, where the customer responded negatively, add Not Approved in the Output box.



Calculate the output provided by the Block to the parent playbook when this branch ends.

Return Value: Approved

- Let’s move onto the second branch. In this sequence we are defining what would happen if the Input Communication Type is Investigate. In the Actions column, select Email > Send Email and fill in the required parameters. In the screenshot below, you can see that we added the placeholder for the Additional Message. Make sure that you actually write a message in the Input Additional Message field if you change the Type to Investigate.



Email_Send Email

Request Investigation

Ask customer to investigate the case and add more details

Manual Auto

If step fails: Stop playbook

Entities: All entities

Recipients *: sara@siemplify.co

CC:

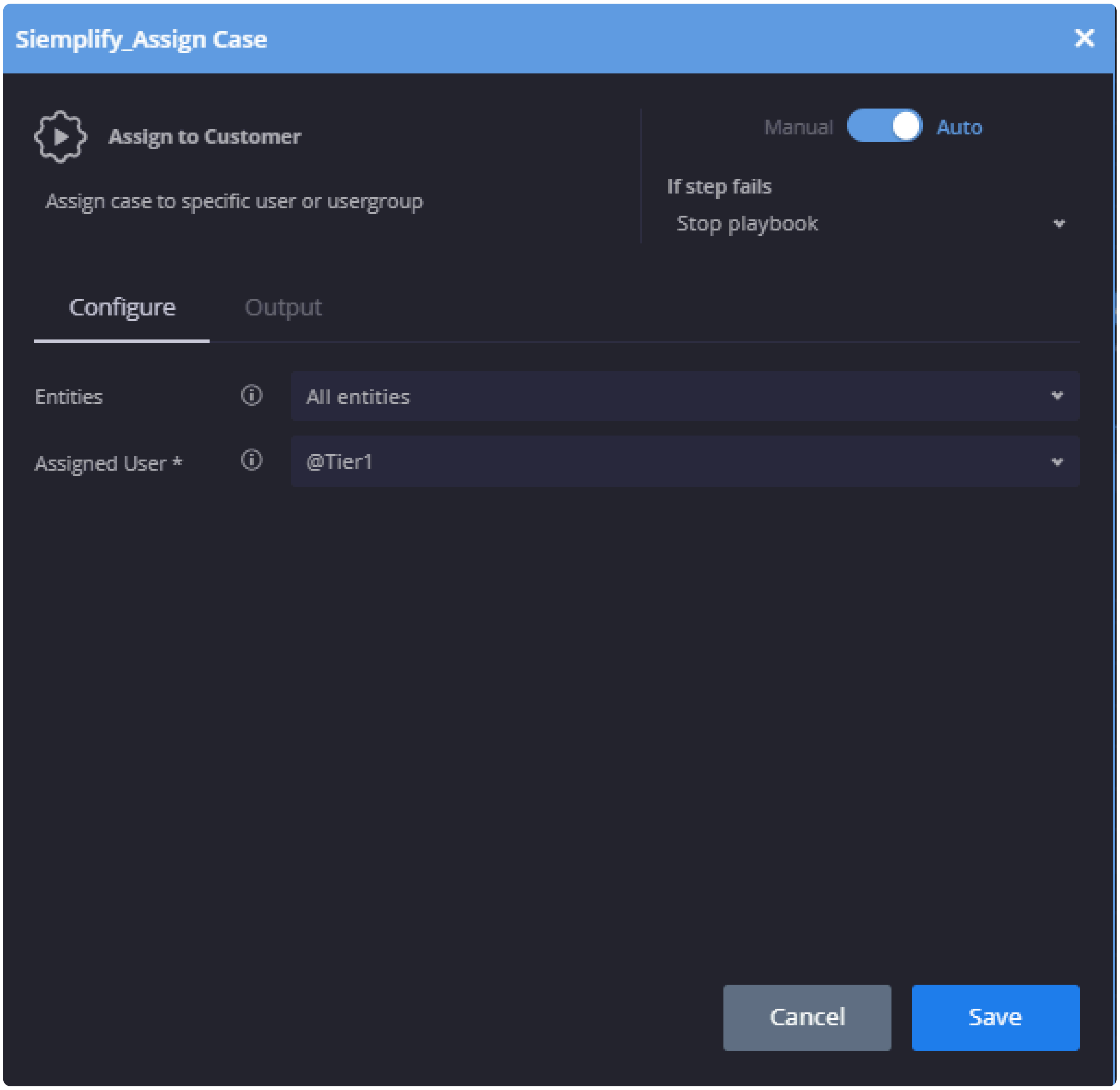
bcc:

Subject *: Please Investigate the Case

Email HTML Template

Content *: More info:
[Input.Additional Message]

- In the next step, select Siemplify > Assign Case. Here we are going to put the responsibility for investigating the case over to the Customer to get his Tier 1 analyst to look at it.



Siemplify_Assign Case

Assign to Customer

Assign case to specific user or usergroup

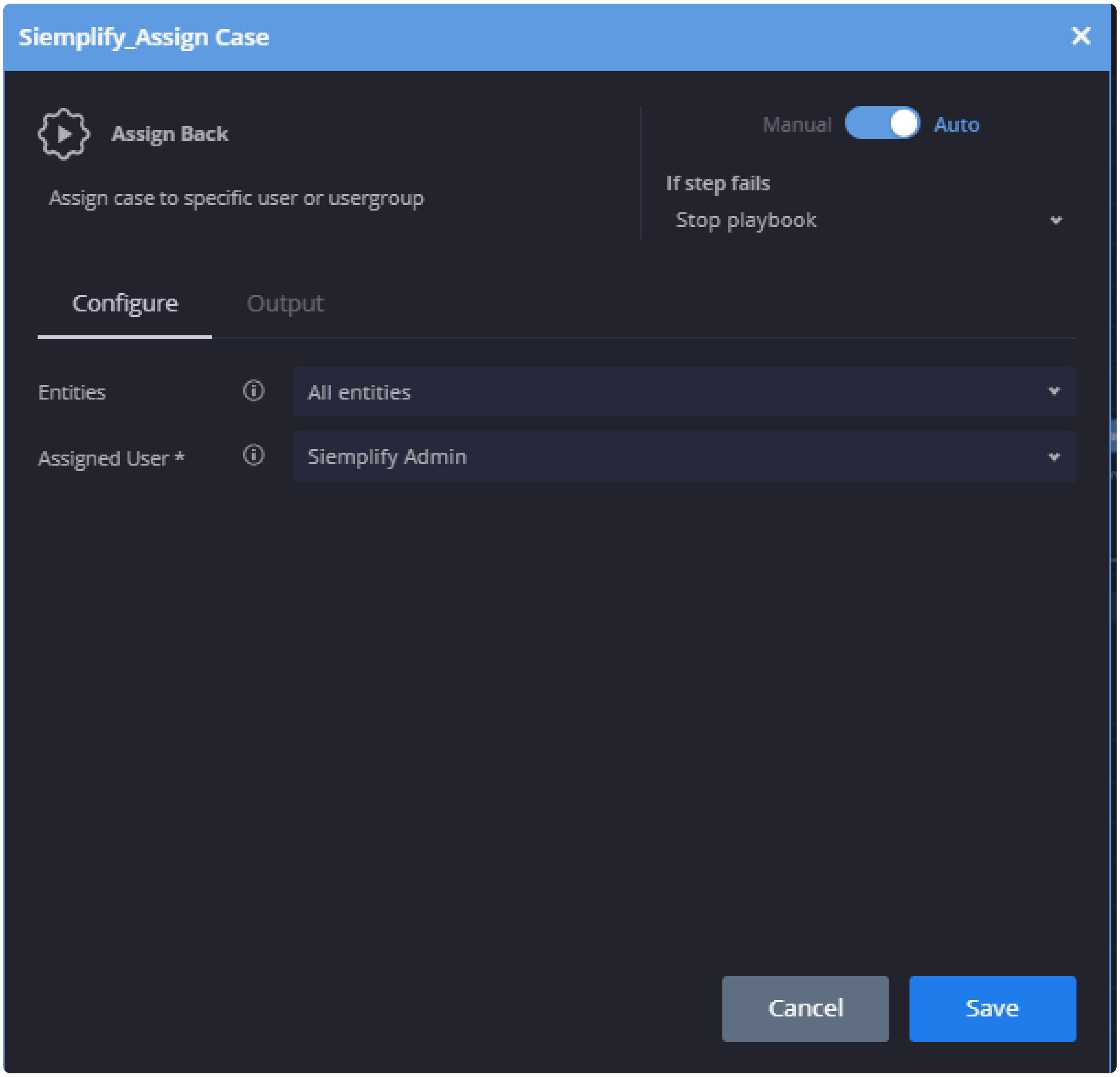
Manual / Auto: Auto

If step fails: Stop playbook

Entities: All entities

Assigned User *: @Tier1

- In the next step, select Siemplify > Change Case Stage. This step presumes that we have received confirmation that the Customer is investigating and therefore we are changing the Case stage to Investigation.
- In the next step, select Siemplify > Assign case. This step assumes that the customer has finished investigation and has asked the SOC to reclaim ownership of the case.



Siemplify_Assign Case

Assign Back

Assign case to specific user or usergroup

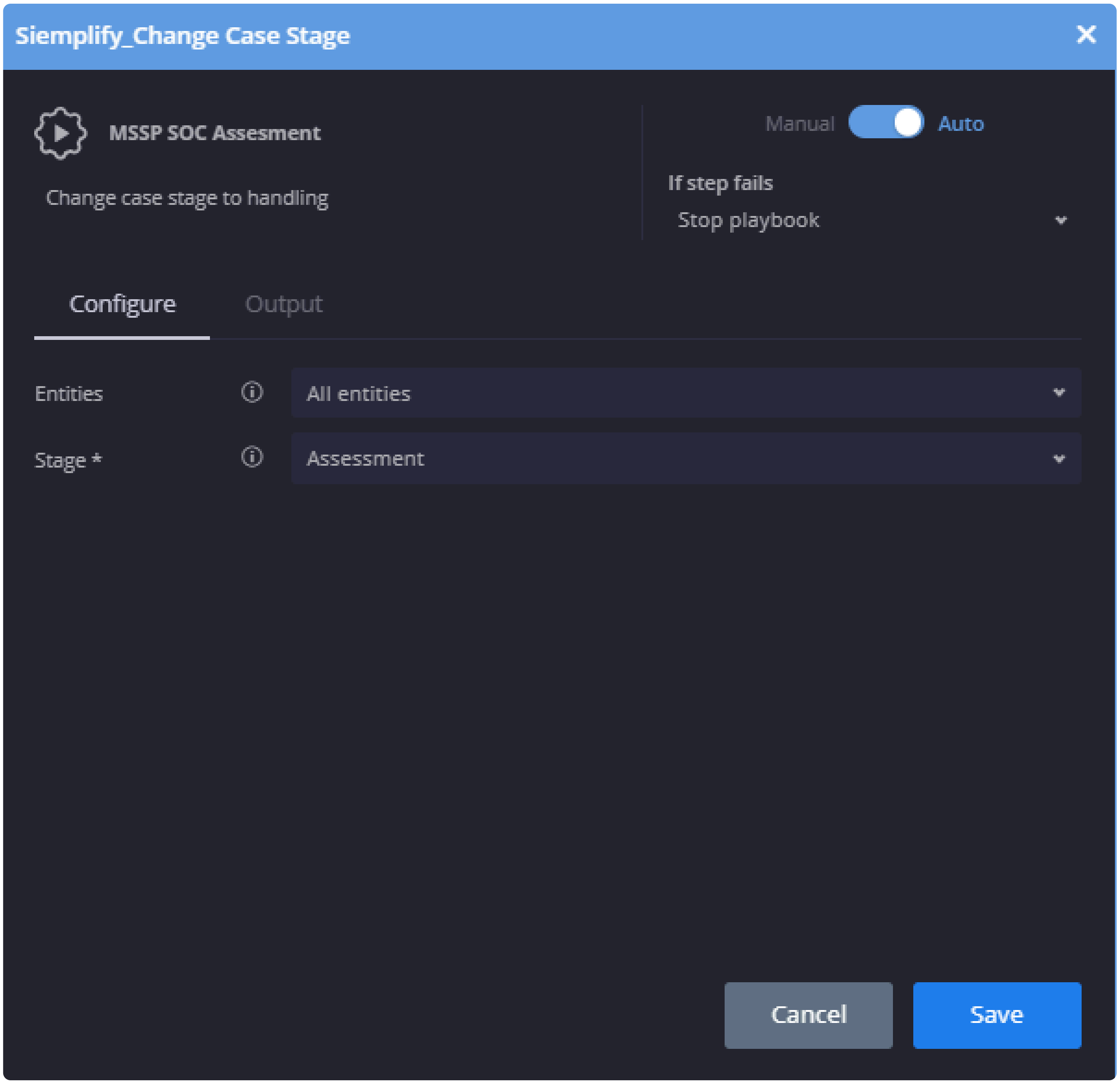
Manual Auto

If step fails: Stop playbook

Entities: All entities

Assigned User *: Siemplify Admin

- In the next step, select Siemplify > Change Case Stage. This step now changes the case stage from Investigation to Assessment so that the Soc can carry on with his handling the case.



Siemplify_Change Case Stage

MSSP SOC Assesment

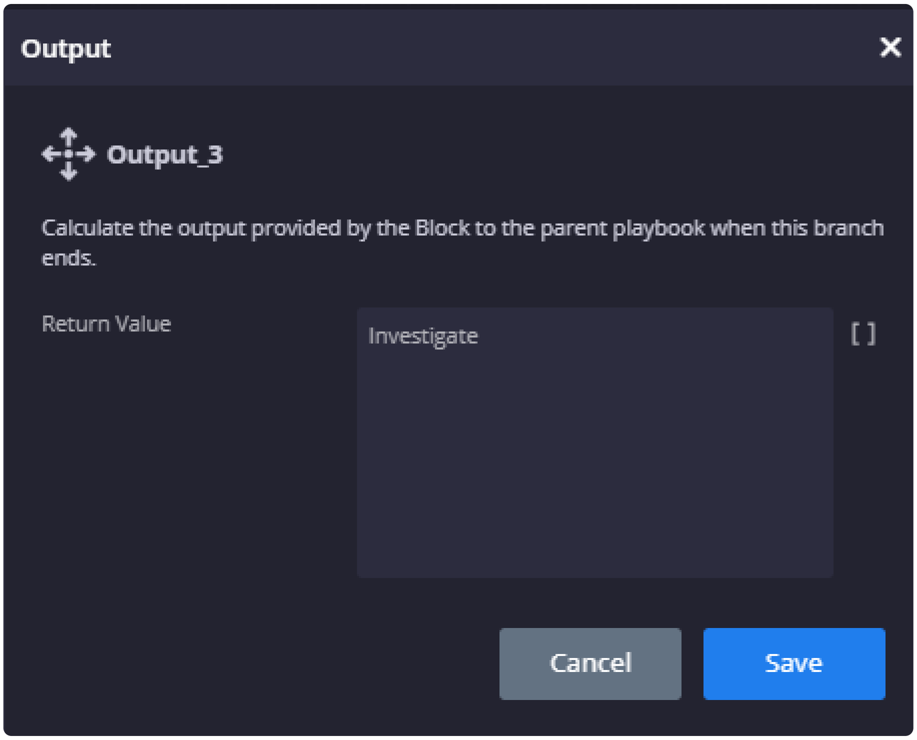
Change case stage to handling

If step fails: Stop playbook

Entities: All entities

Stage *: Assessment

- In the Output step, add the word Investigation Completed to be returned to the parent playbook.



Calculate the output provided by the Block to the parent playbook when this branch ends.

Return Value: Investigate

This block can now be inserted into various Playbooks.

6.1.5. Playbook Monitoring

Each Playbook and Block has its own Monitoring dashboard, accessed from the Playbook page by clicking

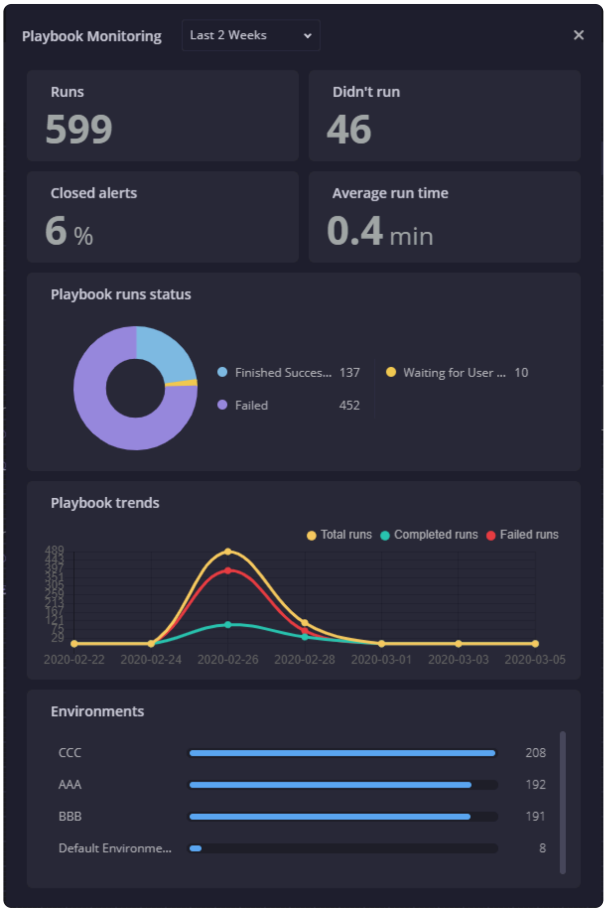
The user can define the timeframe for different resolutions of the playbooks statistics in the Monitoring dashboard.

The Monitoring dashboard contains the following information:

- Runs: How many times the Playbook/Block ran during the defined time period.
- Didn't Run: Number of times the Playbook/Block didn't run due to the three playbook limitation. (Only three playbooks can be automatically attached to an alert.)
- Closed Alerts: Percentage of alerts that were closed by this Playbook.
- Average Run Time: Average amount of time that this Playbook took to run. This can prove useful in troubleshooting Playbooks that took too long.

Playbook Status Pie Chart: Shows three options. Options are finished successfully, failed, or waiting for user action. Each option is clickable and will take you to a Search results page. This chart shows you

playbook statuses according to the defined time period and is cumulative.
Playbook Trends Line Chart: Shows completed runs, failed runs and a total of runs (both failed and successful). Hover your mouse over each dot on the line to see a pop-up showing more information. This chart can come in useful for checking trends over time. For example, let's say you you see that the Playbook didn't run twenty times over the last month, you might then tweak the trigger logic to make the Playbook more selective. You could then look at the Trends chart to check that the Playbook ran successfully from that time onwards.
Environments Bar Chart: Displays all the environments that this Playbook ran in. Each section is clickable and will take you to a Search results page.



Runs 599

Didn't run 46

Closed alerts 6 %

Average run time 0.4 min

Playbook runs status

● Finished Succes...	137	● Waiting for User ...	10
● Failed	452		

Playbook trends

Environments

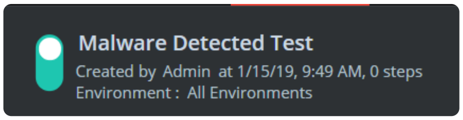
CCC	208
AAA	192
BBB	191
Default Environme...	8

6.2. Example Playbook

In this example, we will build a Playbook from scratch. This Playbook will focus on detecting Malware and making decisions based on what malware is found.

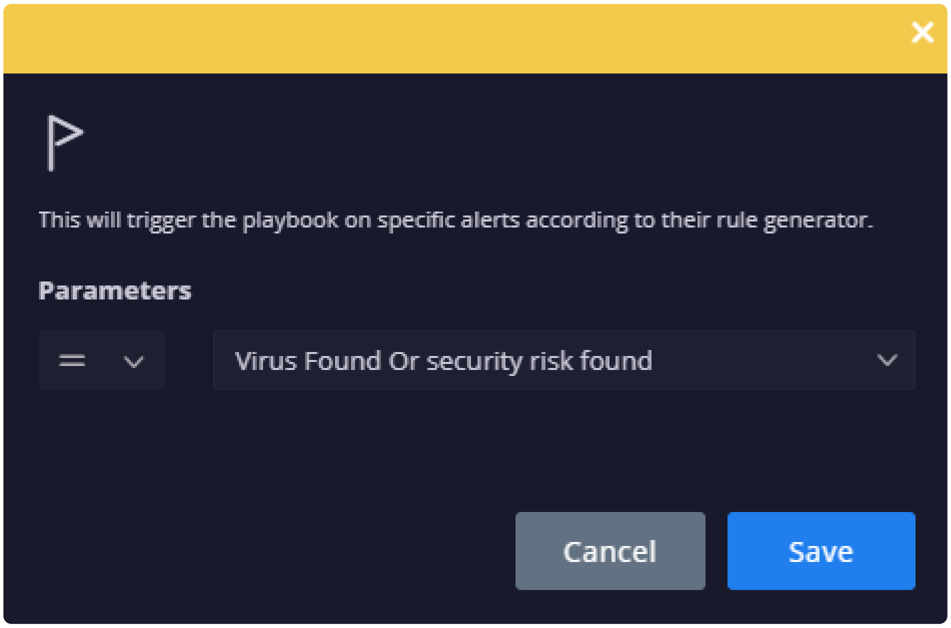
1. Let's start by setting up the new playbook. Click on the plus icon and choose the environment (or no environment) and click Create Playbook. In the top left, click the Edit icon and add a meaningful

name. For example, Malware Detected Test.



Malware Detected Test
Created by Admin at 1/15/19, 9:49 AM, 0 steps
Environment : All Environments

2. Create a Trigger which will cause the Playbook to run if an Alert for a virus or security risk pops up. Note: In this specific trigger type, the alert type options will appear in the drop-down as possible options only if the alerts were already ingested.
   Trigger > Alert Type
   Parameters: Virus Found or Security Risk found

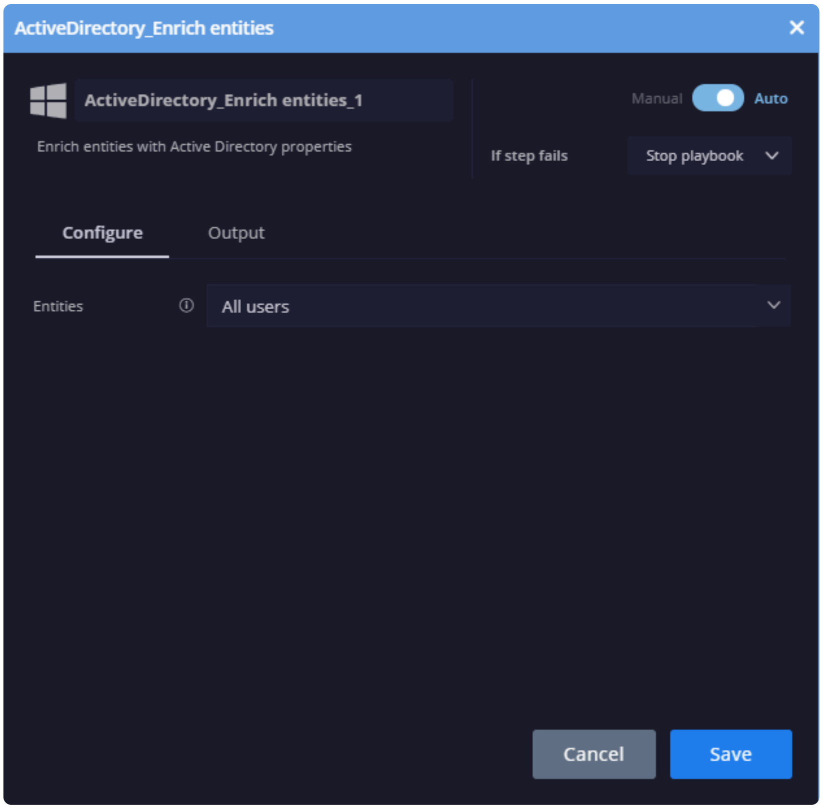


This will trigger the playbook on specific alerts according to their rule generator.

Parameters

= Virus Found Or security risk found

3. Add an Enrichment action to find out all attributes of the Active Directory Users so we can see who is involved with the suspicious risk.
   ActiveDirectory > Enrich Entities
   Entities: All Users



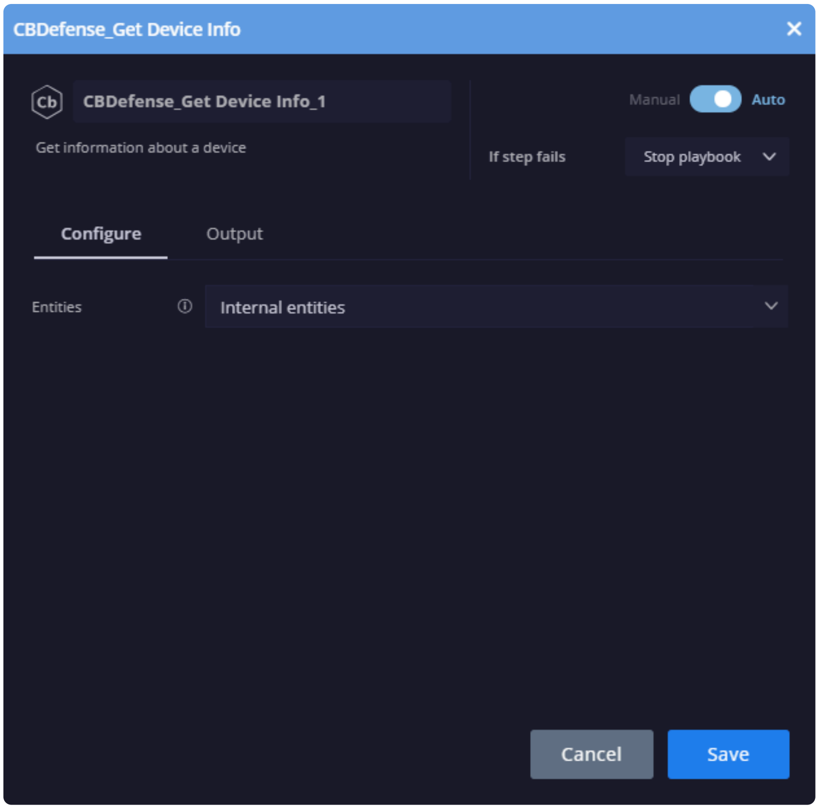
ActiveDirectory_Enrich entities_1

Enrich entities with Active Directory properties

If step fails: Stop playbook

Entities: All users

4. Add an action to get more information on the device.
   CBDefense > Get Device Info
   Entities: Internal Entities

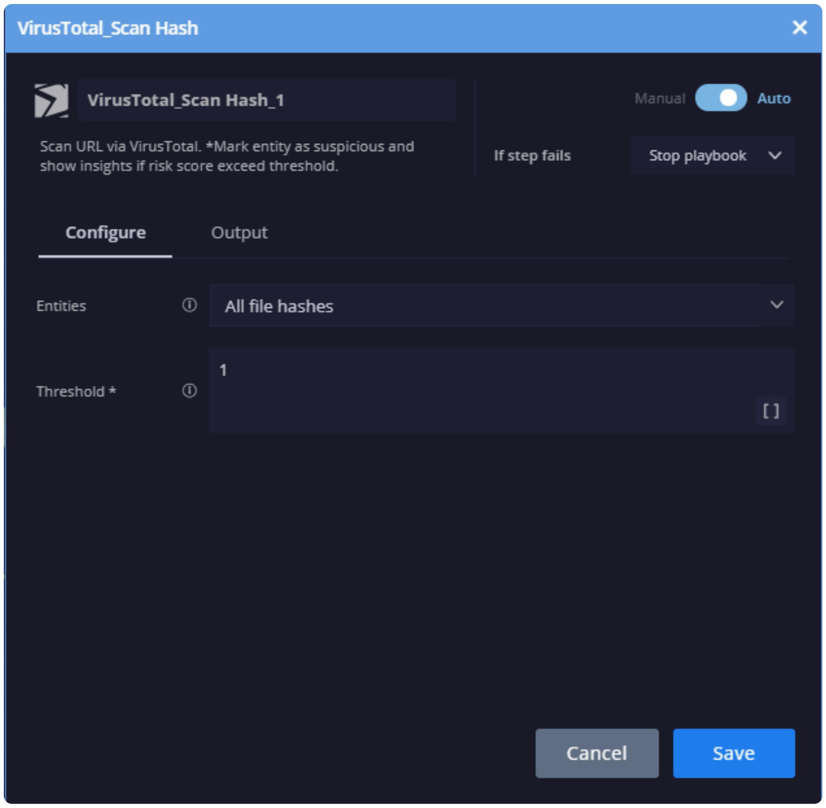


Get information about a device

If step fails: Stop playbook

Entities: Internal entities

5. Add an action to scan all the files to see if any are known to be malicious.
   VirusTotal > Scan Files
   Entities: All File Hashes
   Threshold: **1**



VirusTotal_Scan Hash

VirusTotal_Scan Hash_1

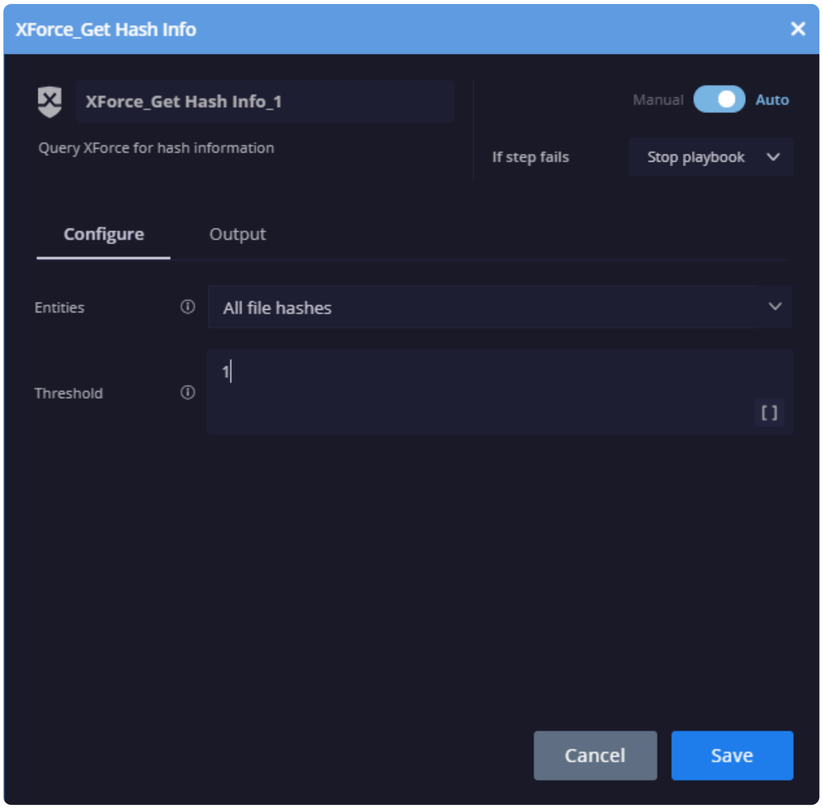
Scan URL via VirusTotal. *Mark entity as suspicious and show insights if risk score exceed threshold.

If step fails: Stop playbook

Entities: All file hashes

Threshold *: 1

6. Add an action to get more information on the files using hash info.
   XForce > Get Hash Info
   Entities: All File Hashes
   Threshold: 1



XForce_Get Hash Info

XForce_Get Hash Info_1

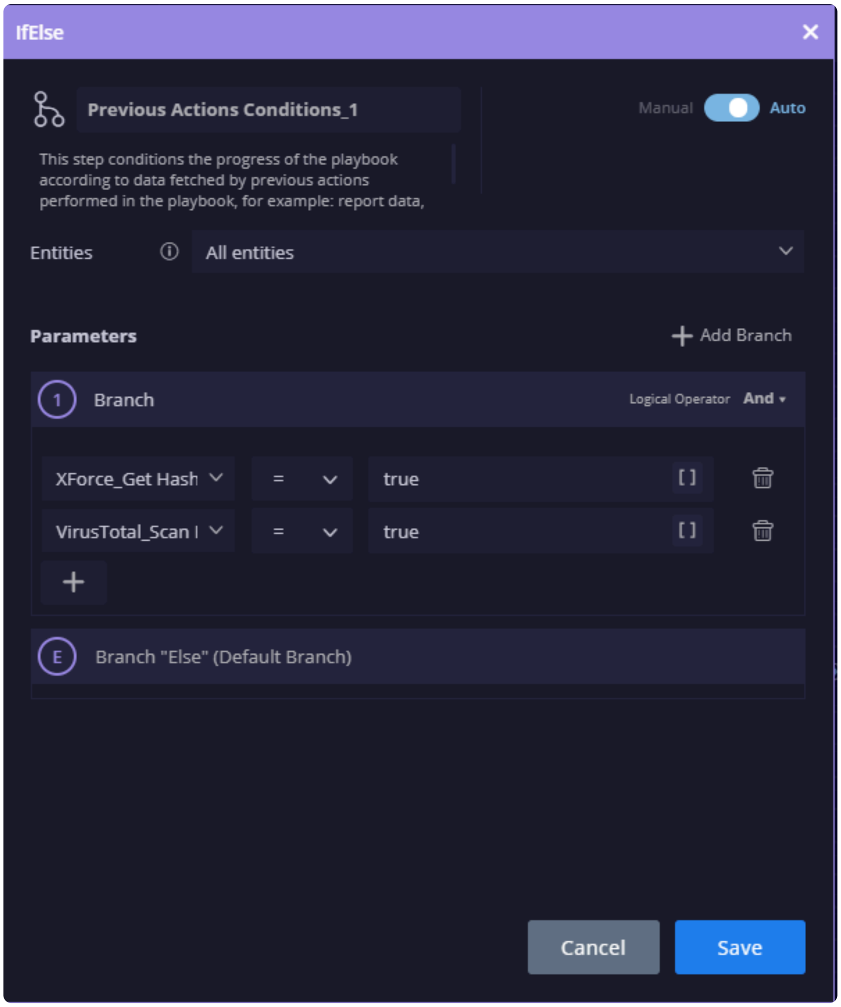
Query XForce for hash information

If step fails: Stop playbook

Entities: All file hashes

Threshold: 1

7. Now is the time to branch off the playbook by creating one path if the XForce and Virus Total have found viruses and another if they haven’t.
   Flow > Previous Actions Conditions
   Parameters: XForce_Get Hash Info = true
   VirusTotal_Scan Files = true
   Logical Operator: And



IfElse

Previous Actions Conditions_1

Manual Auto

This step conditions the progress of the playbook according to data fetched by previous actions performed in the playbook, for example: report data,

Entities: All entities

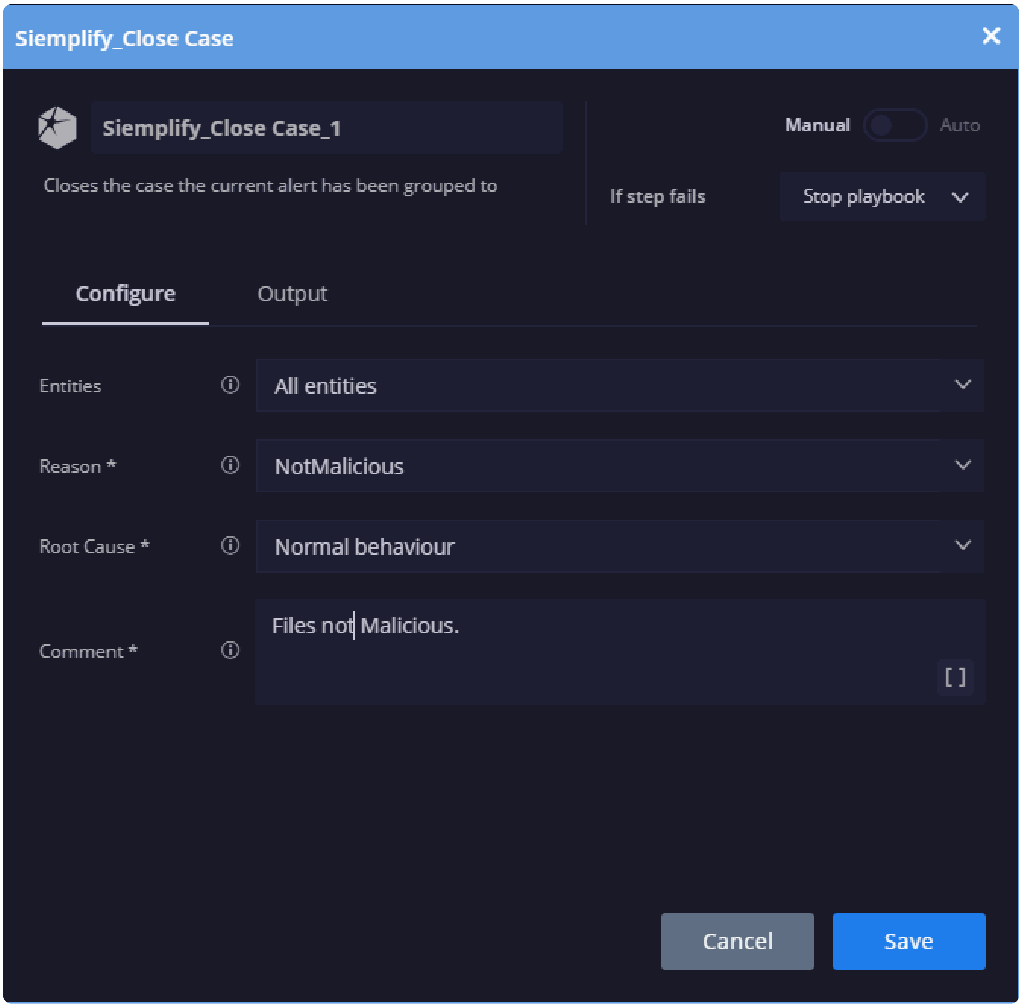
Parameters

1 Branch — Logical Operator: And

XForce_Get Hash	=	true
VirusTotal_Scan I	=	true

E Branch "Else" (Default Branch)

8. Now we are going to add a manual Close Case action to the False branch. This means that no malicious viruses have been found and we want to close the case.
   Siemplify > Close Case
   Parameters: Reason > NotMalicious. Root Cause > Normal Behavior. Comments: free text.
   Make sure to toggle the top to M for Manual intervention by Analyst.



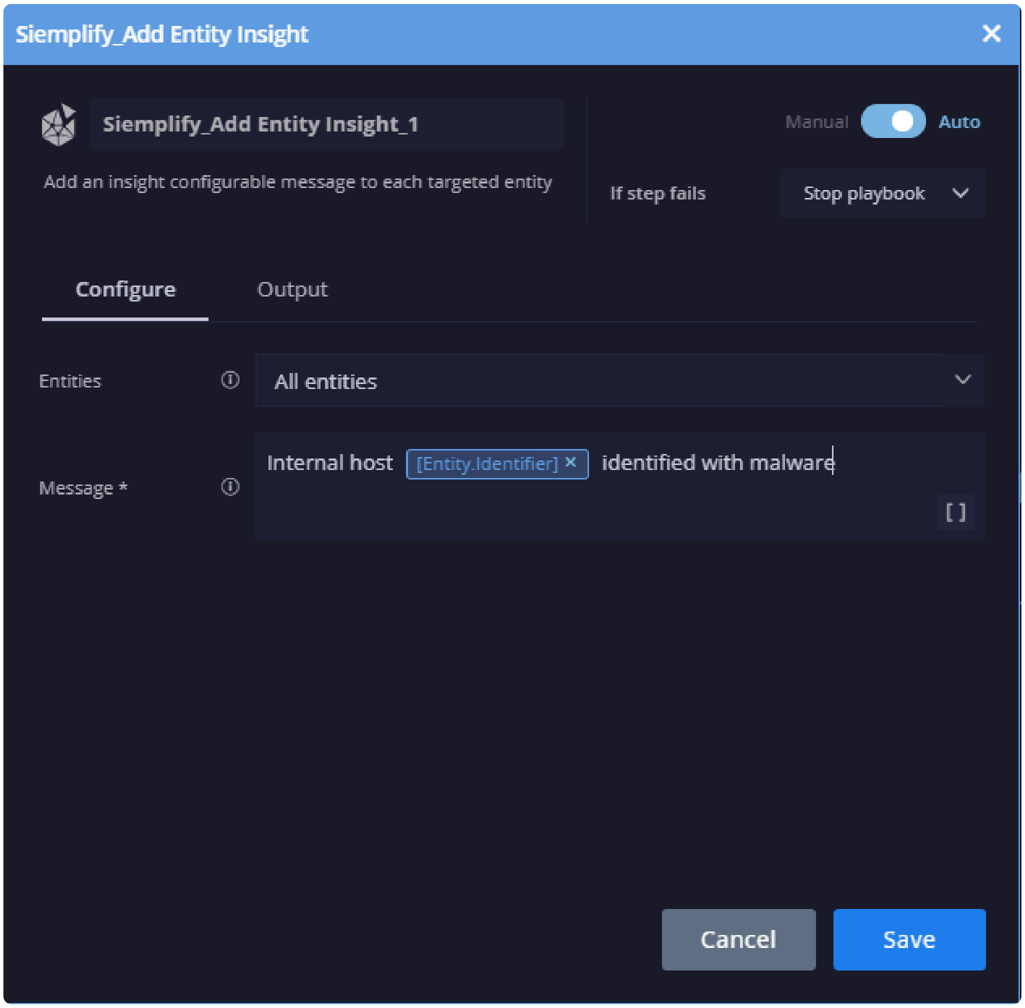
Entities: All entities

Reason *: NotMalicious

Root Cause *: Normal behaviour

Comment *: Files not Malicious.

9. Add an Entity Insight to the True branch which will be displayed in the Insight panel of the Cases screen to show the Analyst that a virus has been found.
   Siemplify > Add Entity Insight
   Entities: Source Entities
   Parameters: Internal host “Entity_Identifier” identified with malware



Siemplify_Add Entity Insight

Siemplify_Add Entity Insight_1

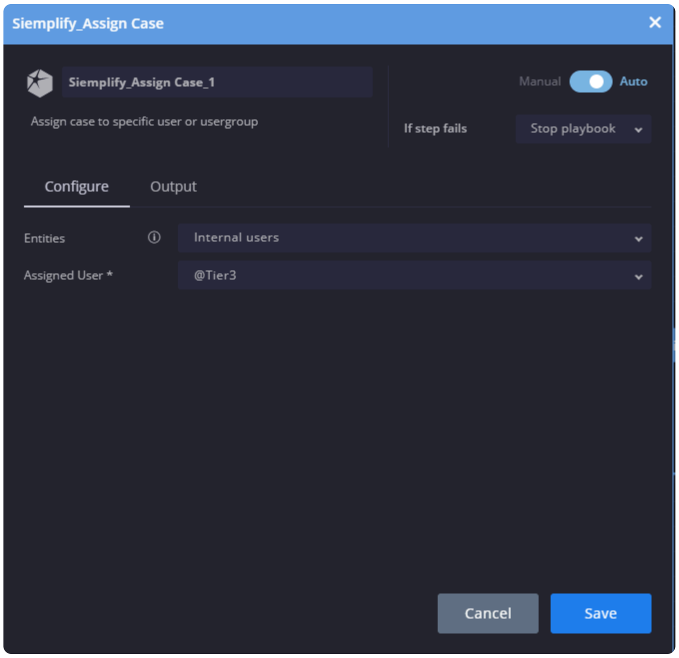
Add an insight configurable message to each targeted entity

If step fails: Stop playbook

Entities: All entities

Message *: Internal host [Entity.Identifier] identified with malware

10. In this step, we are going to select a Siemplify Assign Case action for the True branch. This means that the Playbook has identified viruses that need to be dealt with and the case will be assigned to a higher tier (usually Tier 2)
    Siemplify > Assign Case
    Entities: Internal Users
    Assigned User: Tier3



Siemplify_Assign Case

Siemplify_Assign Case_1

Assign case to specific user or usergroup

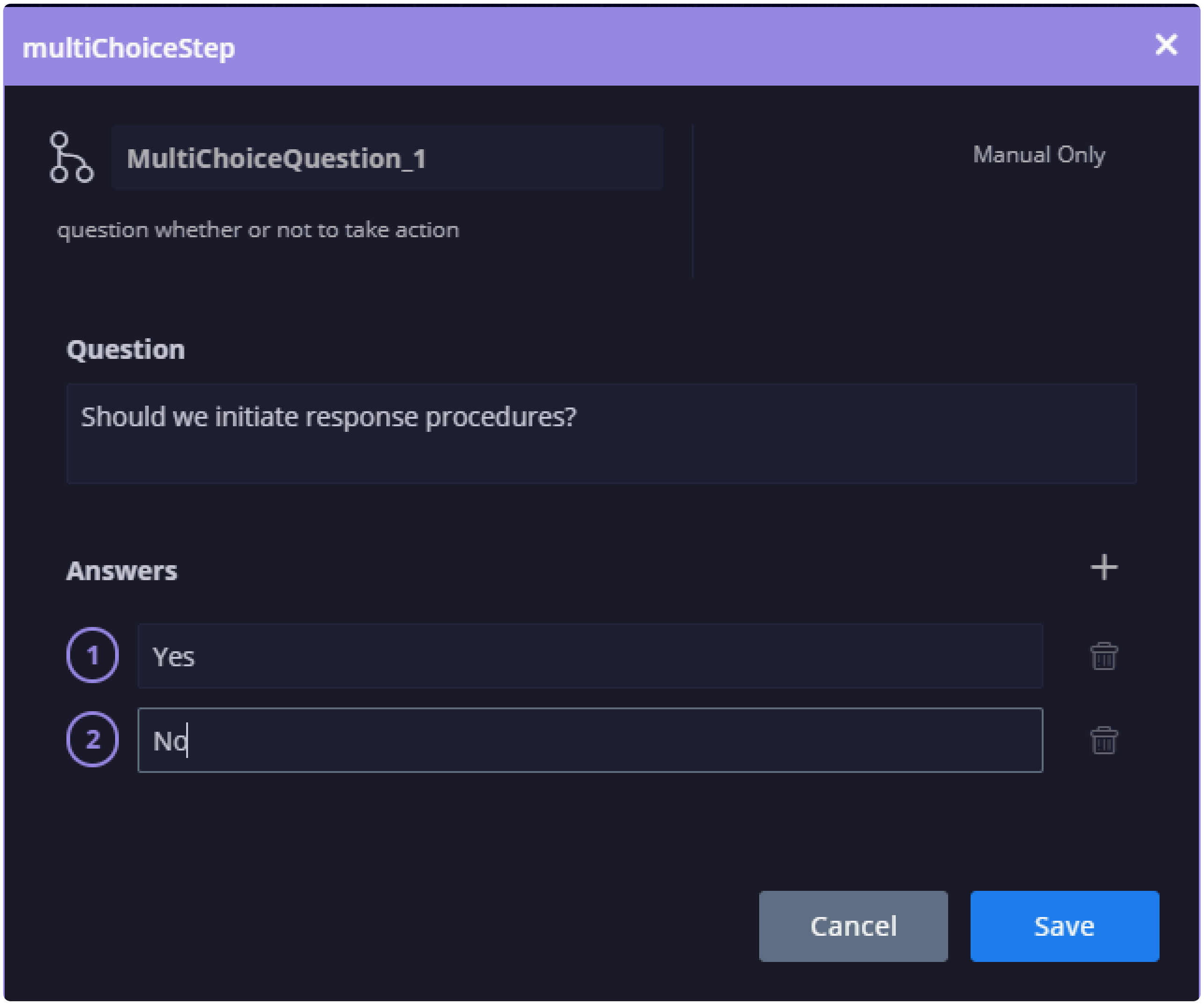
Manual / Auto

If step fails: Stop playbook

Entities: Internal users

Assigned User *: @Tier3

11. We are going to add in some questions so that in run time, the higher level analyst will be asked to make a decision whether to initiate a response procedure.
    Flow > MultiChoiceQuestion
    Question: Should we initiate response procedures?
    1. Yes
    2. No



multiChoiceStep

MultiChoiceQuestion_1

question whether or not to take action

Question

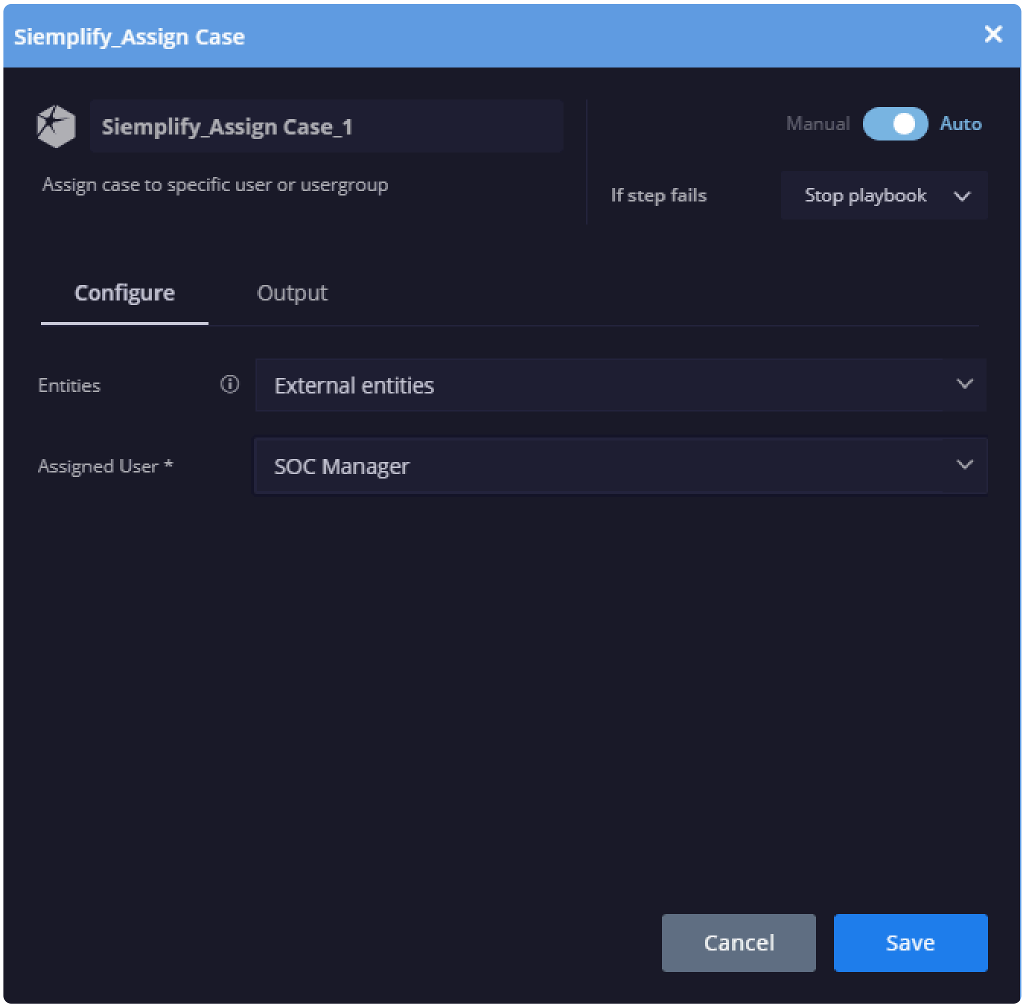
Should we initiate response procedures?

Answers

1 Yes

2 No

12. In this step we will add an Assign Case so that if the Analyst has answered Yes to the question above, then the case is assigned to the SOC Manager.
    Siemplify > Assign Case
    Assigned User: SOC Manager



Siemplify_Assign Case

Siemplify_Assign Case_1

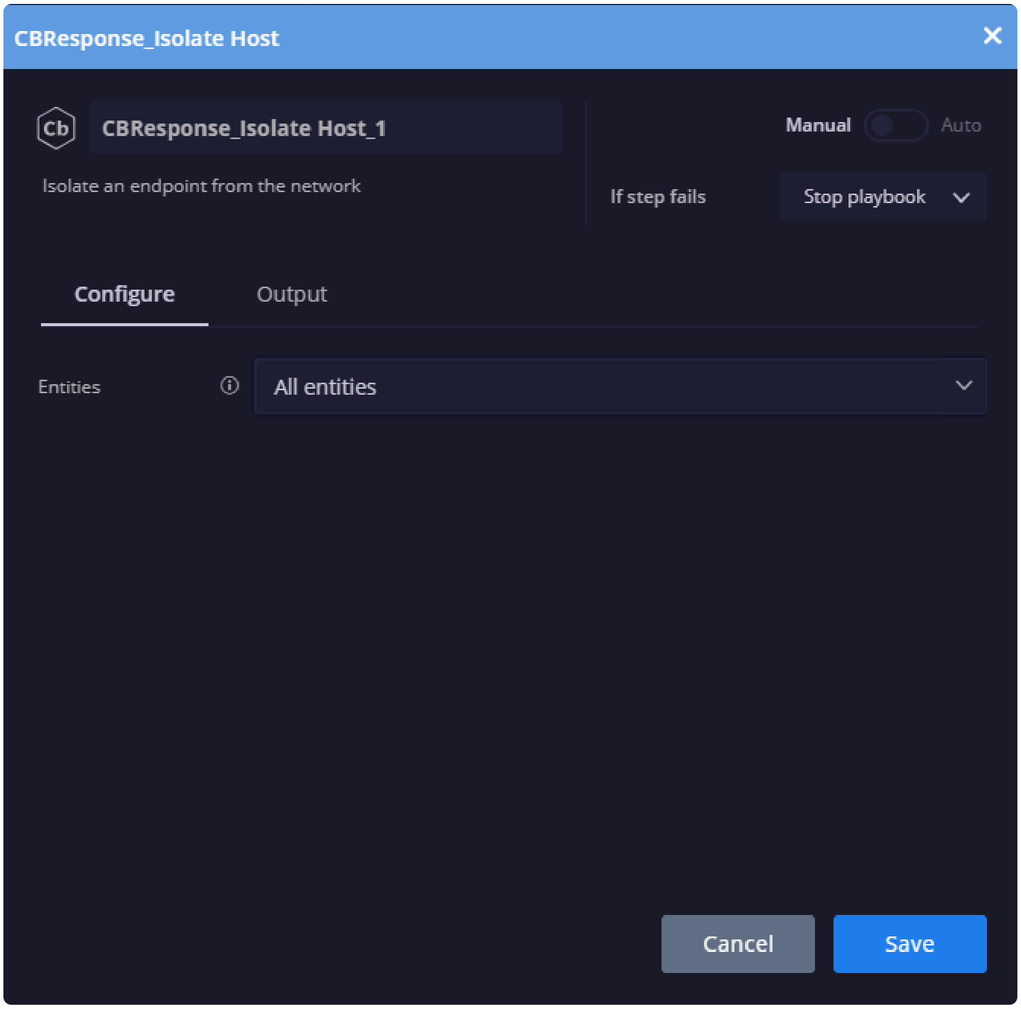
Assign case to specific user or usergroup

If step fails: Stop playbook

Entities: External entities

Assigned User *: SOC Manager

13. Finally, we will add an Isolate Host action for the SOC Manager to manually perform.
    CBResponse > Isolate Host
    Toggle the top button to M for Manual.



CBResponse_Isolate Host

CBResponse_Isolate Host_1

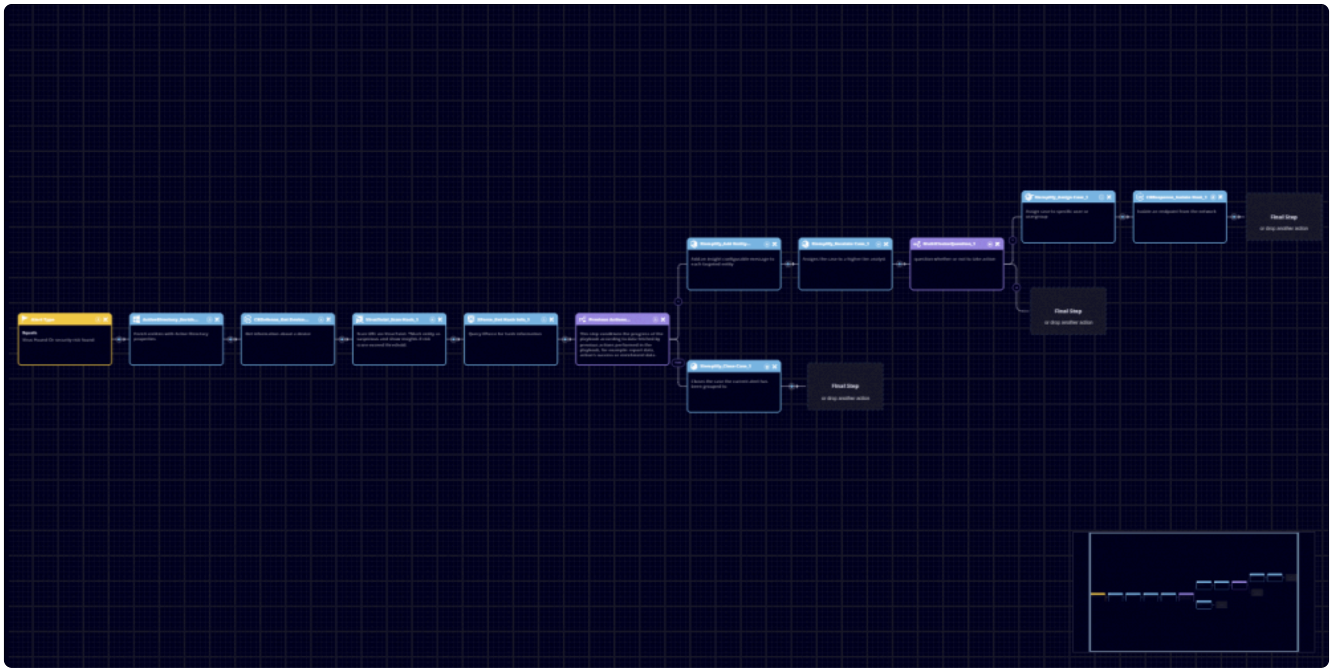
Isolate an endpoint from the network

Manual / Auto

If step fails: Stop playbook

Entities: All entities

14. Make sure to click the large blue Save button on the top right. Congratulations! You have built a Playbook. Once an alert of the type ‘Virus found…’ is ingested, the playbook will be automatically attached to it, and act accordingly to the set of actions and flows that was set in the playbook


Alert Type
Equals
Final Step
or drag another action
Final Step
or drag another action
Final Step
or drag another action

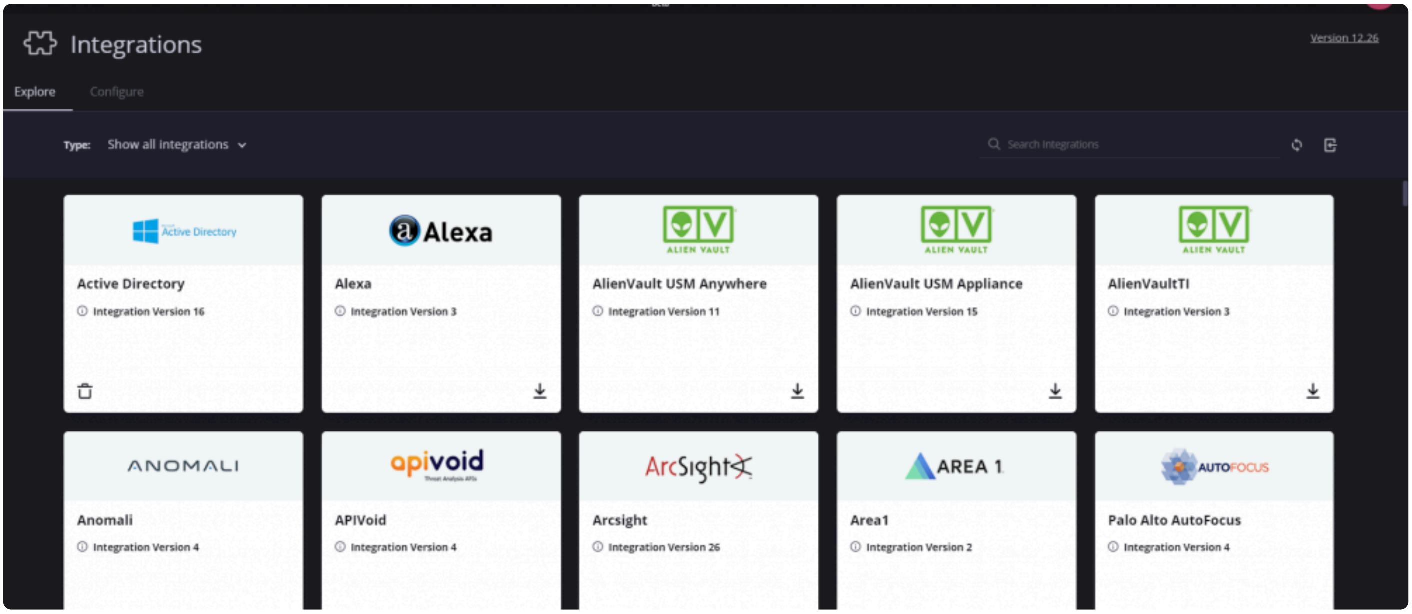
7. Marketplace

The Siemplify Marketplace allows you to find and install an integration of third party applications, custom integrations that you have built in the IDE, and pre-built playbook workflows to integrate into the organizational security products for automated IR process and optimize your Siemplify installation. The Marketplace also contains a repository for use cases – including predefined use cases from Siemplify and customer uploaded use cases.

Clicking on the Marketplace icon on the top right of the screen allows you to choose between Integrations and Use Cases.

Integrations

Clicking on Integrations displays the following screen.



Integrations Explore

You can display the Integrations according to the type of integrations you want to show (for example, show installed only, all uninstalled, custom integrations)
Integrations that have not been installed yet will have a downwards arrow on the bottom right of the box. Click on this to successfully install the integration. Custom Integrations will not show the downwards arrow as they are installed via the IDE. All integrations need to be configured and saved. For detailed information

on installing and configuring an Integration, see here.
Note that for each supported Integration in the Marketplace, there will be a link to an Integrations and Connectors Portal page with detailed information on that specific Integration.

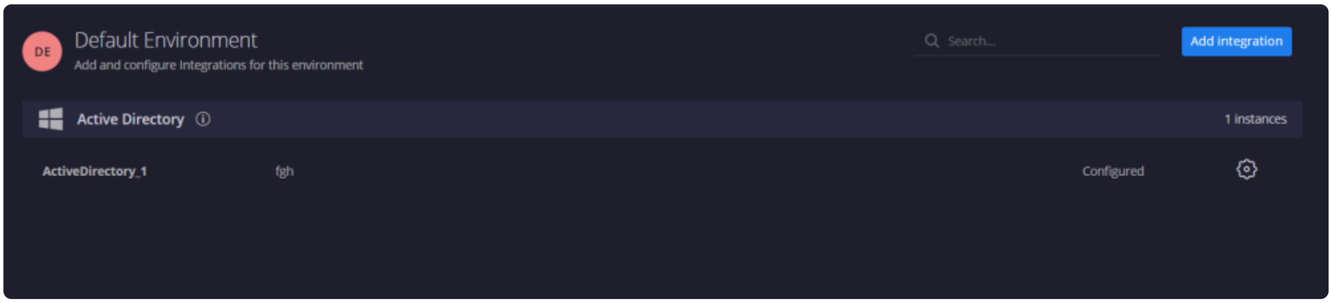
Integrations Configure

In the Configure screen you can configure an Integration in several different ways and use them per Environment. Each configuration is called an “instance” and once configured, can be selected within a Playbook step. For example, when building a Playbook which caters to a customer site using two Active Directories, it will now be possible to choose a different configured instance of the Active Directory integration within the Playbook step.

On the left of this screen are the Environments in which you can configure an Instance. The Shared Instances provides a container where you can configure Instances that can be used in all environments. Note that the default environment is the predefined environment that Siemplify provides. (In previous Releases – this was referred to as “no” environment.)

To configure an Instance:

1. In the Environments list on the left, click on the Environment you want to create an Instance for.
2. On the right of the screen, click Add Integration.

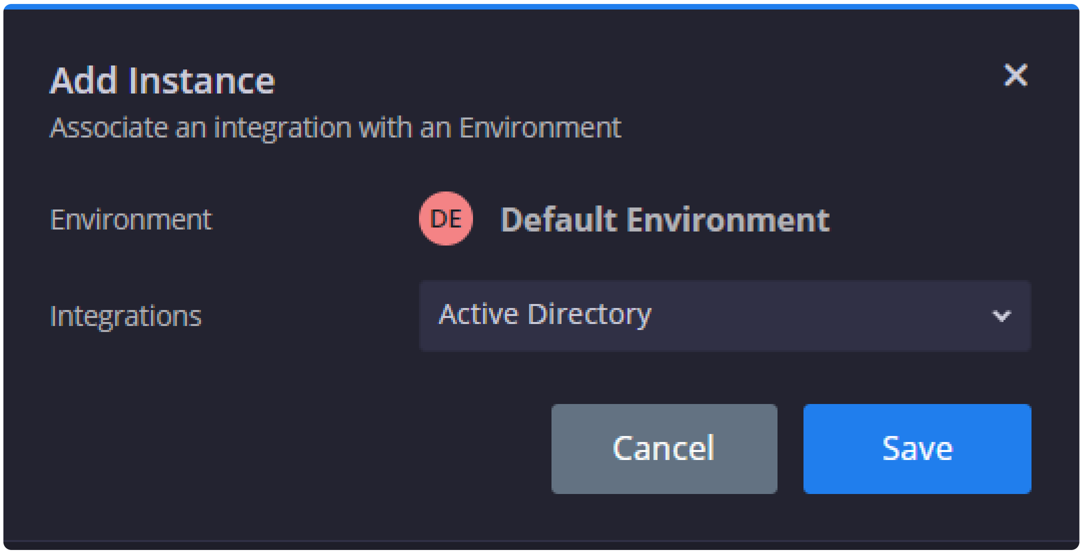


DE Default Environment
Add and configure Integrations for this environment

Active Directory 1 instances

ActiveDirectory_1 fgh Configured

3. Select the required Integration and click Save. In this example, we have selected Active Directory.



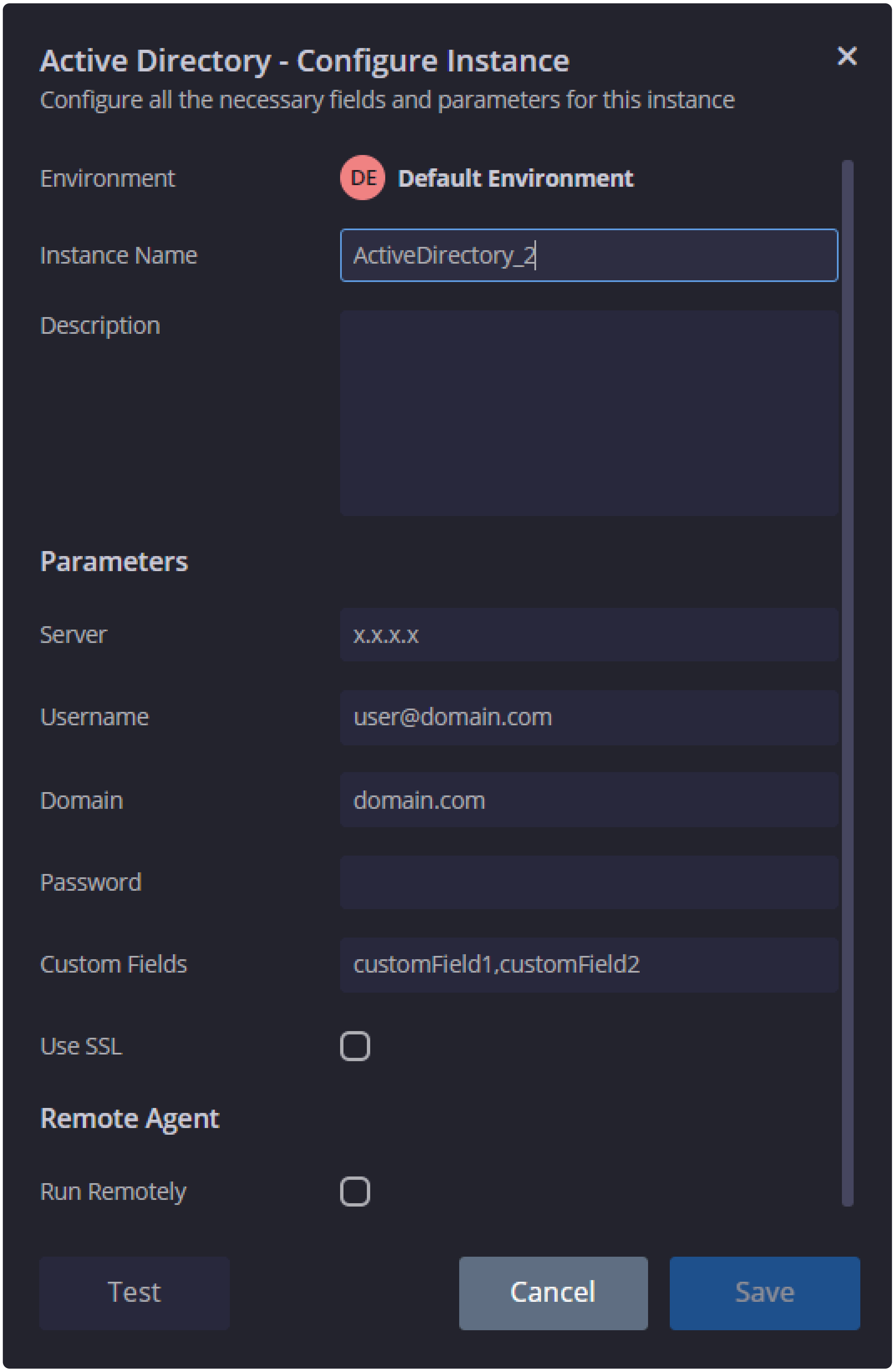
Add Instance

Associate an integration with an Environment

Environment: DE Default Environment

Integrations: Active Directory

4. In the Configuration screen that displays, add in all the relevant information and parameters. When finished, click Save.



Active Directory - Configure Instance

Configure all the necessary fields and parameters for this instance

Environment: DE Default Environment

Instance Name: ActiveDirectory_2

Description:

Parameters

Server: x.x.x.x

Username: user@domain.com

Domain: domain.com

Password:

Custom Fields: customField1,customField2

Use SSL: □

Remote Agent

Run Remotely: □

5. Note that you can make changes at a later stage if needed. Once configured, the Instances can be

used in Playbooks.

Use Cases

Select Use Cases from the Marketplace tab to display the Use Cases screen.
Each Use Case contains relevant items such as integrations, Playbooks etc in order to simulate an entire workflow from end-to-end. After deploying one of these use cases, you can choose to Simulate it in the Cases tab. In addition, you can configure the Connector, and/or edit the Playbook, of a predefined Use Cases and run it on real data.

Upload: Click Upload to create your own Use Case with playbook/s, test case/s and connector/s and upload it. Once it's uploaded, it's sent to a dedicated Siemplify team who will analyze it and if relevant, will add it to the Use Case repository for all Siemplify customers and community members to use. For this reason, it's important to think carefully about what type of information you are uploading. The goal of the Upload Use Case option is to encourage all customers to share playbooks and use cases that can help others out with their Siemplify journey.
Optionally, you can choose to create your own use case via the Upload feature, BUT instead of submitting it to the repository, you can export it as a zip file and then import it. That way, you will have it just on your Marketplace! Note that any imported cases will be deleted when you choose to Get Latest Cases. (Although as soon as the latest cases are uploaded, you can simply import them again!)

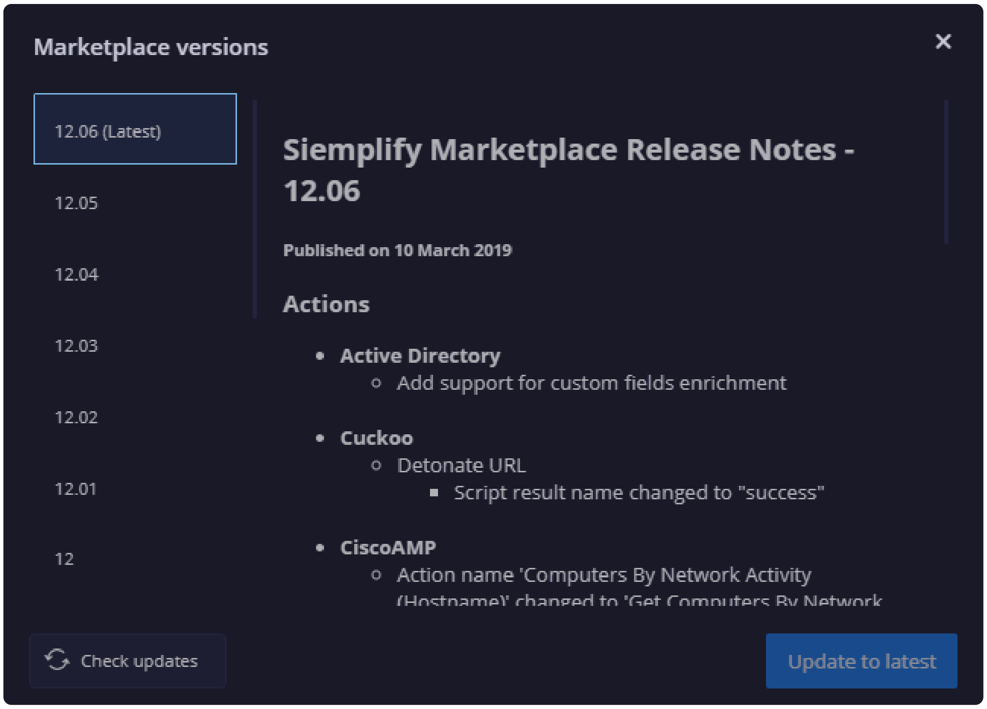
Get Latest Use Case: Click this button in the Repository to download new Use Cases that Siemplify have added to the repository. These could also include customer-uploaded Use Cases.

Update Marketplace Version

To update the Marketplace version:

> ✻ The system automatically notifies you of pending versions to be updated.

1. Click on the new version available notification to be redirected to the Marketplace Versions screen.
2. Click on Update to latest.



Siemplify Marketplace Release Notes - 12.06

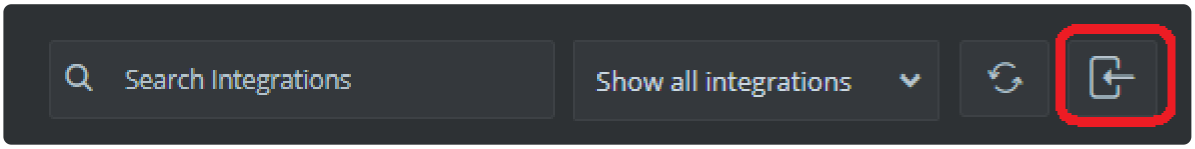
Published on 10 March 2019

Actions

- Active Directory
  - Add support for custom fields enrichment
- Cuckoo
  - Detonate URL
    - Script result name changed to "success"
- CiscoAMP
  - Action name 'Computers By Network Activity (Hostname)' changed to 'Get Computers By Network

For customers without external Internet access:

1. Request a zip file with the latest update from your Support manager and download it to your desktop.
2. Click the Import Marketplace icon.



3. Select the zip file and click Open.
4. Click Yes on the confirmation message. The Marketplace is updated with the latest version.

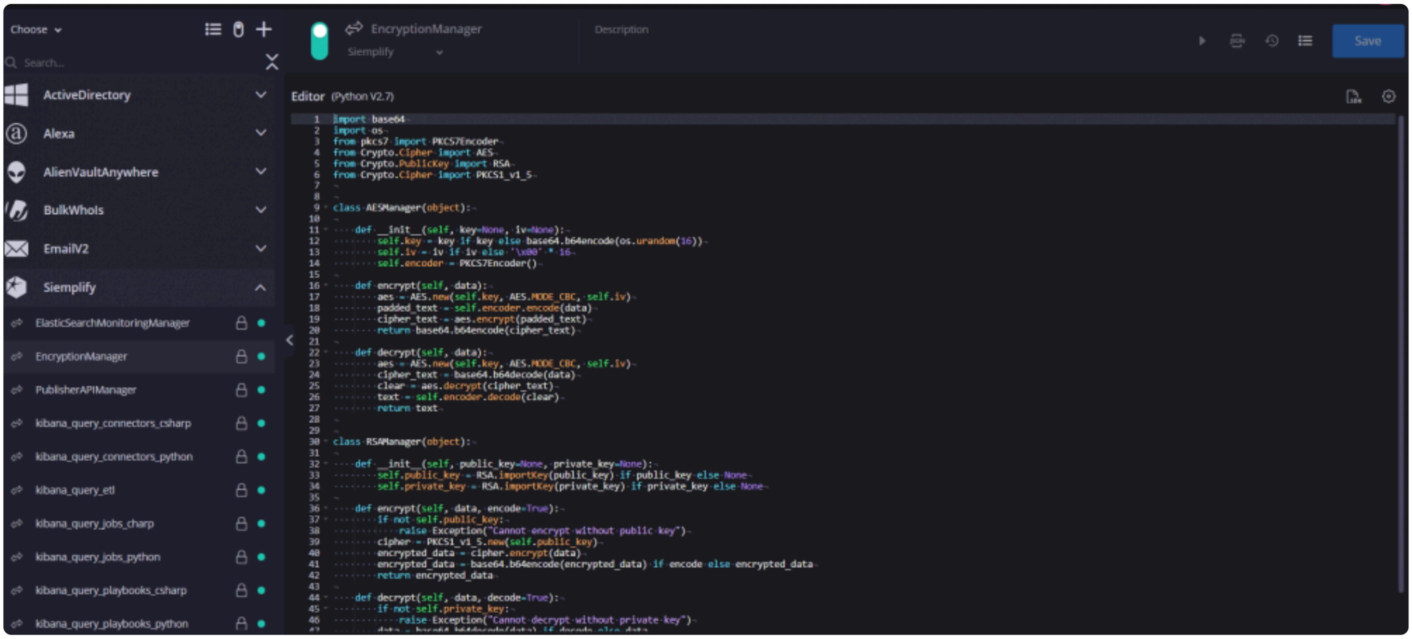
Updating Marketplace: In order to update the Marketplace with integrations, navigate to Settings > Advanced > General > Source Repository. Click Update Marketplace. Note that the Marketplace version needs to be compatible with the Siemplify platform version. In addition, custom actions will not be updated.

8. IDE

The Integrated Development Environment (IDE) is a framework for viewing, editing, and testing code. It allows you to view the code of commercial integrations and to create custom integrations from scratch or by duplicating commercial integrations code.

In addition – this is the place to manage, import and export custom integrations.

To open the IDE, click the IDE code icon </> on the top right menu. The IDE screen displays.



```
import base64
import os
from pkcs7 import PKCS7Encoder
from Crypto.Cipher import AES
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_v1_5


class AESManager(object):

    def __init__(self, key=None, iv=None):
        self.key = key if key else base64.b64encode(os.urandom(16))
        self.iv = iv if iv else '\x00' * 16
        self.encoder = PKCS7Encoder()

    def encrypt(self, data):
        aes = AES.new(self.key, AES.MODE_CBC, self.iv)
        padded_text = self.encoder.encode(data)
        cipher_text = aes.encrypt(padded_text)
        return base64.b64encode(cipher_text)

    def decrypt(self, data):
        aes = AES.new(self.key, AES.MODE_CBC, self.iv)
        cipher_text = base64.b64decode(data)
        clear = aes.decrypt(cipher_text)
        text = self.encoder.decode(clear)
        return text


class RSAManager(object):

    def __init__(self, public_key=None, private_key=None):
        self.public_key = RSA.importKey(public_key) if public_key else None
        self.private_key = RSA.importKey(private_key) if private_key else None

    def encrypt(self, data, encode=True):
        if not self.public_key:
            raise Exception("Cannot encrypt without public key")
        cipher = PKCS1_v1_5.new(self.public_key)
        encrypted_data = cipher.encrypt(data)
        encrypted_data = base64.b64encode(encrypted_data) if encode else encrypted_data
        return encrypted_data

    def decrypt(self, data, decode=True):
        if not self.private_key:
            raise Exception("Cannot decrypt without private key")
        data = base64.b64decode(data) if decode else data
```

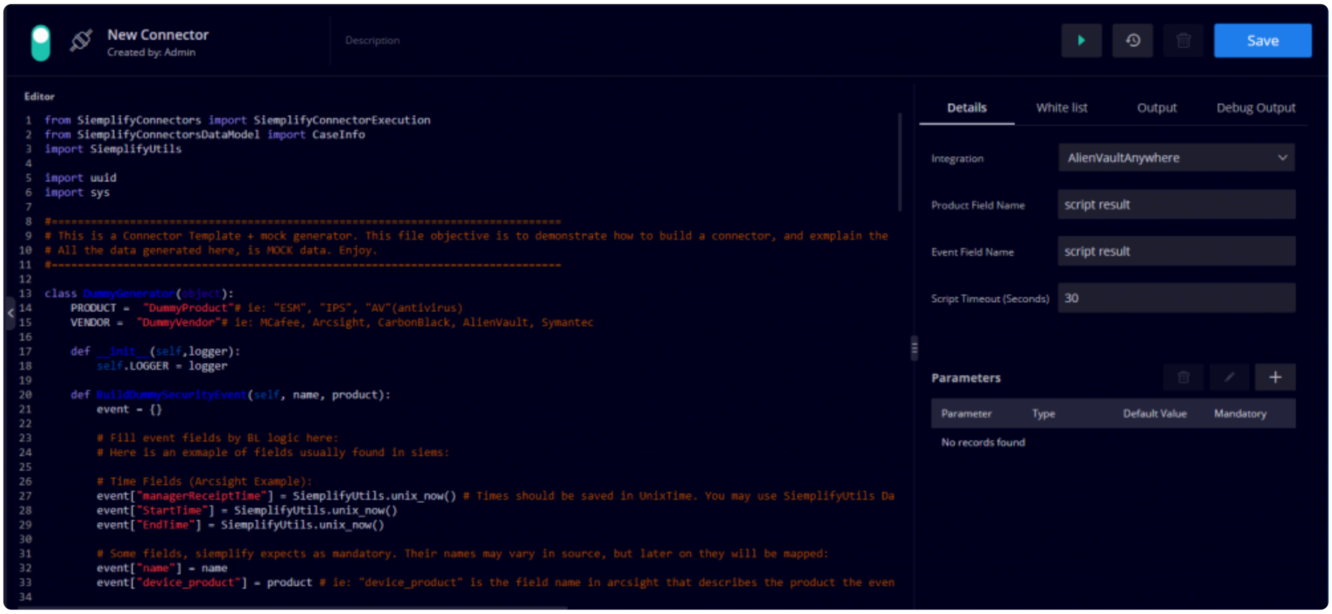
The following options are available from the top left of the screen:

Option	Description
Integrations ⌄ Integrations Types	Choose between Integrations or Types (Connectors, Actions, Jobs and Managers)
⇤ ⇥	Import or Export Packages (zip files only)
○	Show or Hide disabled items (actions, connectors)

+	Can add a new custom Integration, connector, action, job or manager to the list.

To add a connector

1. Click plus icon and give a name to the new connector.
2. In the right of the screen, add Integration details.
3. Add the required parameters.
4. Toggle the button at the top to the green position to enable the job.
5. Click Save when done, or click Ctrl + S.



```
from SiemplifyConnectors import SiemplifyConnectorExecution
from SiemplifyConnectorsDataModel import CaseInfo
import SiemplifyUtils

import uuid
import sys

#==============================================================================
# This is a Connector Template + mock generator. This file objective is to demonstrate how to build a connector, and exmplain the
# All the data generated here, is MOCK data. Enjoy.
#------------------------------------------------------------------------------

class DummyGenerator(object):
    PRODUCT =  "DummyProduct"# ie: "ESM", "IPS", "AV"(antivirus)
    VENDOR =  "DummyVendor"# ie: MCafee, Arcsight, CarbonBlack, AlienVault, Symantec

    def __init__(self,logger):
        self.LOGGER = logger

    def BuildDummySecurityEvent(self, name, product):
        event = {}

        # Fill event fields by BL logic here:
        # Here is an exmaple of fields usually found in siems:

        # Time Fields (Arcsight Example):
        event["managerReceiptTime"] = SiemplifyUtils.unix_now() # Times should be saved in UnixTime. You may use SiemplifyUtils Da
        event["StartTime"] = SiemplifyUtils.unix_now()
        event["EndTime"] = SiemplifyUtils.unix_now()

        # Some fields, siemplify expects as mandatory. Their names may vary in source, but later on they will be mapped:
        event["name"] = name
        event["device_product"] = product # ie: "device_product" is the field name in arcsight that describes the product the even

```

Integration: AlienVaultAnywhere

Product Field Name: script result

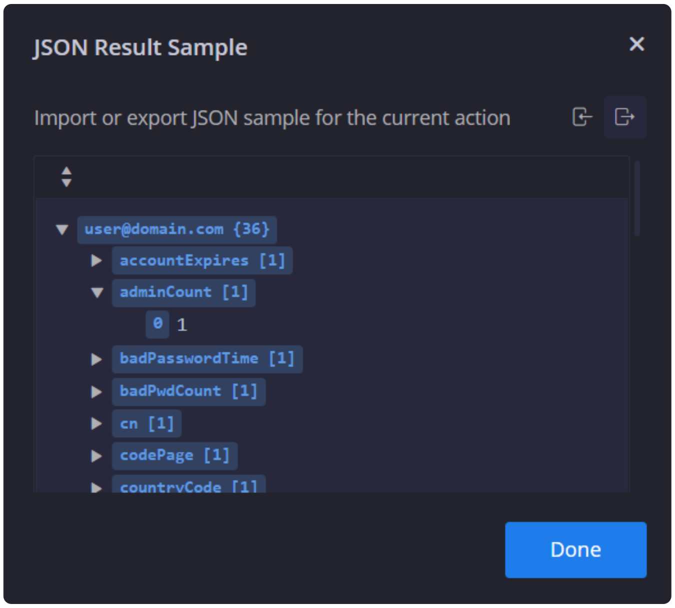
Event Field Name: script result

Script Timeout (Seconds): 30

Parameter	Type	Default Value	Mandatory
No records found			

The following options are available from the right of the screen:

Option	Description
🗑	The delete option is available for IDE items added to Custom Integrations only.
▶	Runs the Test method of the script, which runs the selected script (action \ job \ connector). The result of the script is shown in the Testing tab and the debug information (Python prints) is shown in Debug Output for debugging purposes.
JSON	This is the JSON Sample import/export dialog. Note that you need to enable “Include JSON Result” and then when using an action which returns JSON result, you can click on this icon and choose whether to import your own JSON sample, or export the current one in order to edit it.

	 JSON Result Sample Import or export JSON sample for the current action user@domain.com {36} accountExpires [1] adminCount [1] 0 1 badPasswordTime [1] badPwdCount [1] cn [1] codePage [1] countryCode [1]
Details	In the details tab, you can provide the user supplied input as well as other parameters such as Integration name.
⟲	Version Control - Select an action/job/connector and click to see the following options: **Save as New Version** - Click to save the object as a new version, add your comments, then click Save as. **View Version History** - Click to see the version history of the object in a tabular form. Click Restore to revert to any of the previous versions anytime. This is only available if you have clicked Save as New Version on an action/job/connector/manager previously.
⧉	Select a job/action/connector/manager and click the duplicate icon to create a copy of the job/action/manager. You can then edit this according to your needs. You will notice that after pressing Save this now appears in the list without the lock icon.

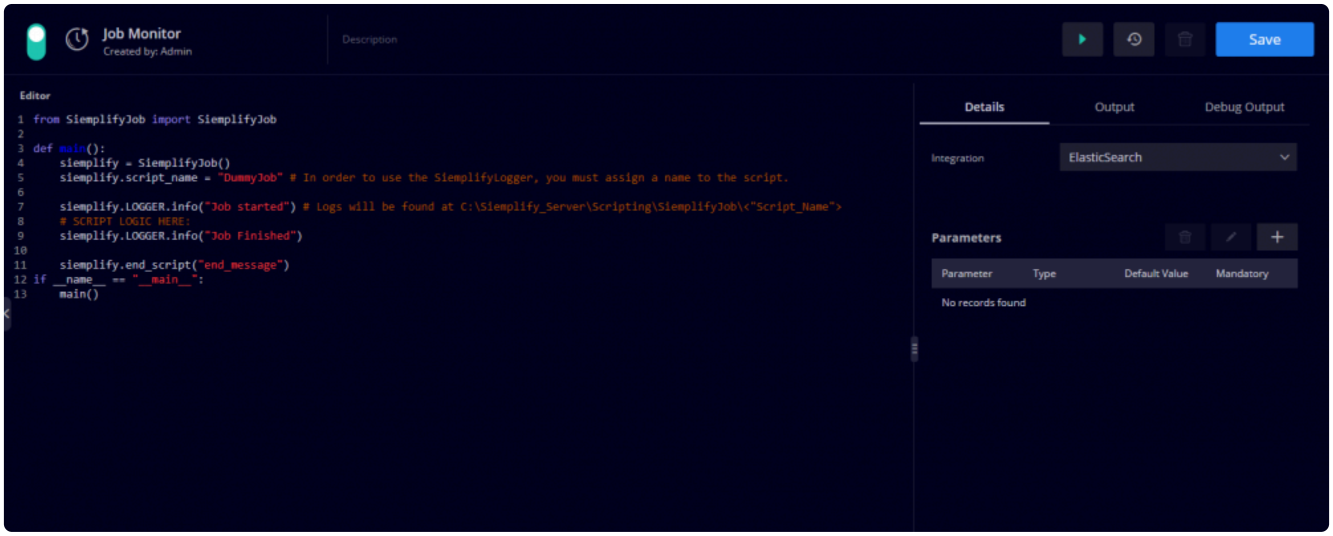
To create a custom integration:

1. Click the plus icon and select Integration. Enter a name and click Create.
2. Click the wheel icon and add in the relevant information:
    a. Description of your Integration. Note that this description will appear in the Marketplace and will be visible to all Siemplify users.
    b. Image of your integration. Note that this picture will appear in the Marketplace and will be visible to all Siemplify users.
    c. Script dependencies – you can add scripts written in whl, py, tar, gz formats. These scripts will add more functionality to your integration.
    d. Parameters – you can add parameters or fields to your Integration which need to be configured in the Marketplace. You can choose type of parameter, default value and whether or not to make it a mandatory field.
3. Click Save when done.

> ✻ Note that you can add jobs, actions, managers and connectors to your custom integration and use them to push or collect information according to your needs. Simply create a new action and then choose the custom Integration. It is also recommended to create a Ping action so that you can test it in the Marketplace.
> For more detailed information on Custom Integrations, please refer here.

To create a job:

1. Click the plus icon and select Job. Enter a name and click Create.
2. Toggle the button at the top to the green position to enable the job.
3. In the Details tab at the right, select an Integration.



```
from SiemplifyJob import SiemplifyJob

def main():
    siemplify = SiemplifyJob()
    siemplify.script_name = "DummyJob" # In order to use the SiemplifyLogger, you must assign a name to the script.

    siemplify.LOGGER.info("Job started") # Logs will be found at C:\Siemplify_Server\Scripting\SiemplifyJob\<"Script_Name">
    # SCRIPT LOGIC HERE:
    siemplify.LOGGER.info("Job Finished")

    siemplify.end_script("end_message")
if __name__ == "__main__":
    main()
```

Integration: ElasticSearch

Parameters

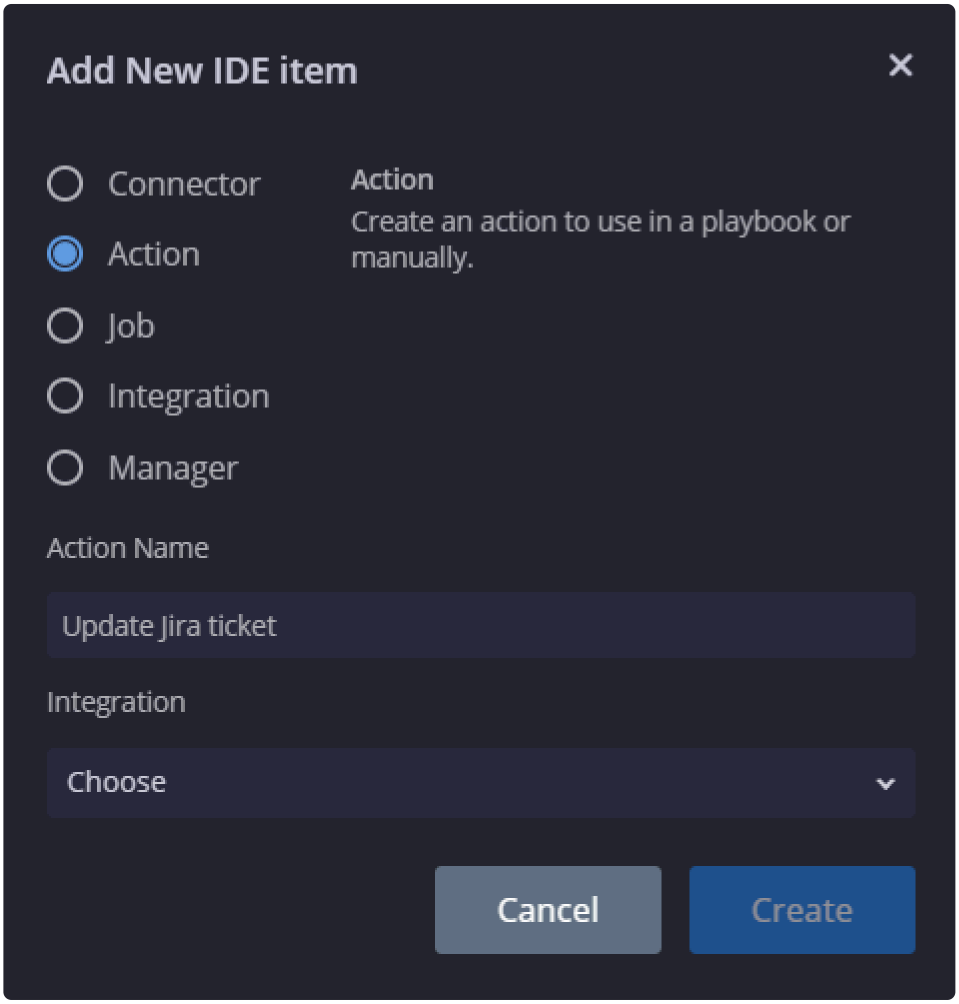
Parameter	Type	Default Value	Mandatory
No records found			

You can also add parameters which enables you to configure jobs to receive input from users or another script.

4. Make sure to click the Save icon on the top right of the screen, or click Ctrl + S.
5. Click the green arrow (Play Item) in order to run the script.
6. Next, navigate to Settings > Jobs.
7. Click the plus icon and select the Job that you just created.
8. Choose the required time in the Scheduler to run the Job (script) that you created.

To create a new action to be used in a Playbook:

1. Click the plus icon and select Actions. Enter a name and click Create.



Add New IDE item

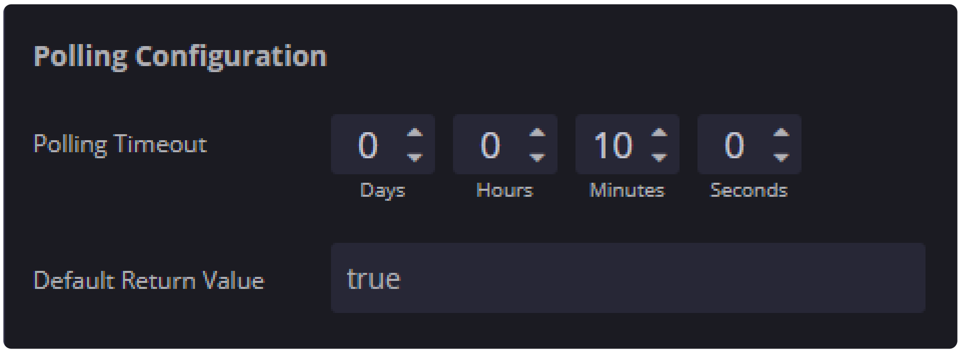
○ Connector
● Action
○ Job
○ Integration
○ Manager

Action
Create an action to use in a playbook or manually.

Action Name: Update Jira ticket

Integration: Choose

2. Edit the code as required.
3. Make sure to enable the "Include JSON Result" if you want the Action to return JSON results in the Playbook.
4. If necessary, add parameters to be displayed as a drop down list.
5. Make sure to enable the action and click Save at the top right of the screen.
6. In the right side of the screen, under the heading Polling Configuration, you can choose to define the amount of time after which if the Action has not returned a result it times out. You can add a default value to be returned in the event of a timeout.



Polling Configuration

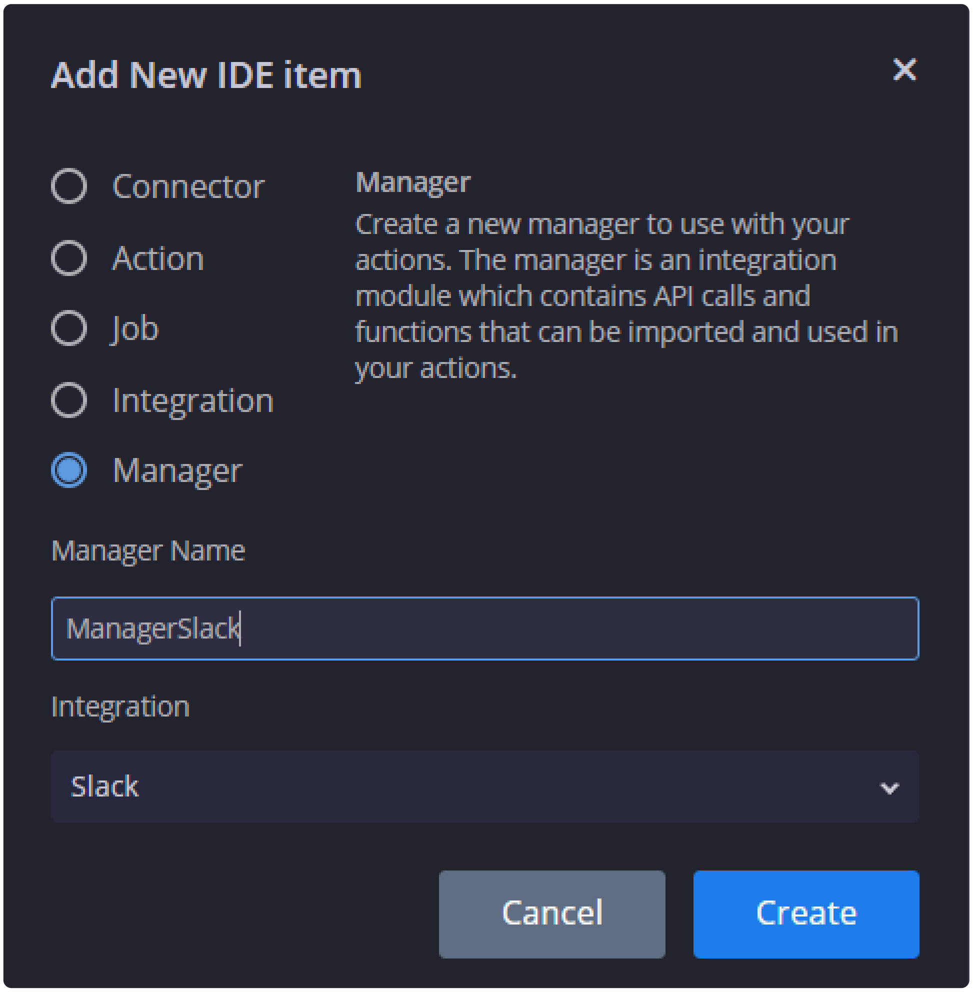
Polling Timeout: 0 Days, 0 Hours, 10 Minutes, 0 Seconds

Default Return Value: true

The Action is now available for use in the Playbook > Actions.

To create a custom manager:

1. Click the plus icon and select Manager. Enter a name and the required Integration and click Create.



Add New IDE item

○ Connector
○ Action
○ Job
○ Integration
● Manager

Manager
Create a new manager to use with your actions. The manager is an integration module which contains API calls and functions that can be imported and used in your actions.

Manager Name: ManagerSlack

Integration: Slack

2. Edit the code as required.
3. Click Save.

> For more help with this page, click on the link to the SDK Guide in the screen or alternatively, click here.

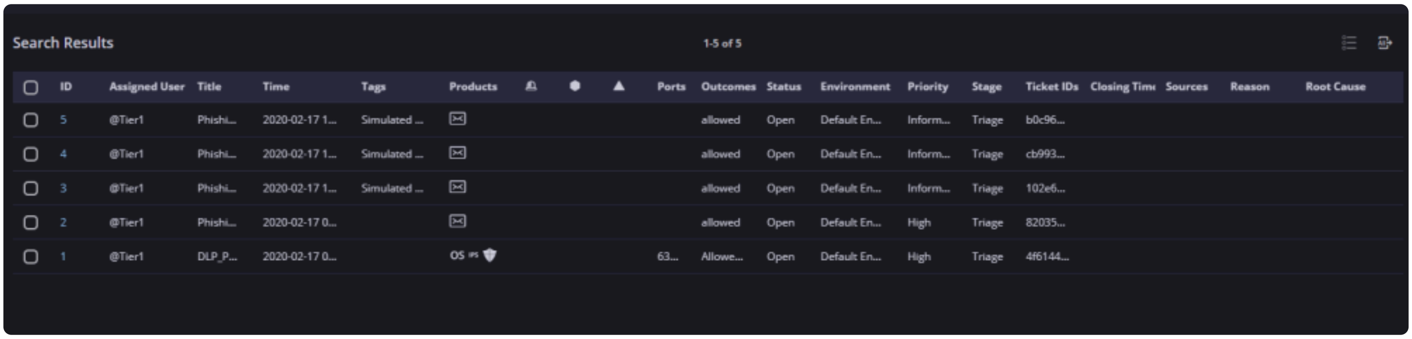
9. Search

The Search page allows you to find specific cases or entities indexed by Siemplify. Siemplify stores all case and entity information from cases, giving you the ability to retrieve information that may be relevant for what you are investigating. The search field will accept free text searching on all data that is indexed by Siemplify within the last year, which includes cases metadata, alerts, events, ports, case wall, etc. In Siemplify you can search either cases or entities.

Case Search:
When searching cases, you can have free text as well as field-based searches. Case searches also allow you to narrow down the time period of the records being searched. This returns the cases that have information related to your search. The fields that can be searched are: CaseIds, TicketIds, Ports, AlertName and Entity. Each case can be clicked giving you the ability to generate a report and review all the information associate with the case (Alerts, Entities, Insights, Case Wall, etc.) as well as perform actions on a case.

Entity Search:
When searching entities, you will see the Name of the Entity, Risk, Location, Environment and Case Count. Entities can be involved in more than one case. Each entity can be clicked so you can review the context details, previous cases and entity log.

Once you have your Search results, you can use the filters on the left hand side to further refine your Search.



Search Results

1-5 of 5

□	ID	Assigned User	Title	Time	Tags	Products	🔔	●	▲	Ports	Outcomes	Status	Environment	Priority	Stage	Ticket IDs	Closing Tim	Sources	Reason	Root Cause
□	5	@Tier1	Phishi...	2020-02-17 1...	Simulated ...	✉					allowed	Open	Default En...	Inform...	Triage	b0c96...				
□	4	@Tier1	Phishi...	2020-02-17 1...	Simulated ...	✉					allowed	Open	Default En...	Inform...	Triage	cb993...				
□	3	@Tier1	Phishi...	2020-02-17 1...	Simulated ...	✉					allowed	Open	Default En...	Inform...	Triage	102e6...				
□	2	@Tier1	Phishi...	2020-02-17 0...		✉					allowed	Open	Default En...	High	Triage	82035...				
□	1	@Tier1	DLP_P...	2020-02-17 0...		OS IPS				63...	Allowe...	Open	Default En...	High	Triage	4f6144...				

Filters

You can select all the filters (and then deselect individual filters). You can also search within each Filter category.

CASE: Specify any of the following filters and click Apply to view the basic details of the returned cases on the right pane.

- Status – Select the Open and/or Closed options as required. This selection returns cases that are either opened or closed or both, based on your selection.
- Environments (Top 20) – Select the required environments related to the cases.
- Tags (Top 20) – Select the required tags assigned to the cases.
- Assigned Users – Select the required system users to whom the cases are assigned.
- Category Outcomes (Top 20) – Select the required outcomes that are imposed on the cases.
- Ports (Top 20) – Select the required source and destination ports that are involved in the cases.
- Products (Top 20) – Select the integrated products of the cases.
- Case Source – Select the required options that are the source of the cases.
- Case Stage (Top 20) – Select the required case stages that are used for managing cases according to SOC methodology.
- Alert Types (Top 20) – Select the required alert types associated with the cases.
- Priorities – Select the required priorities assigned to the cases.
- Importance – Select True and/or False to display cases are marked or not marked as important respectively.

Entity: Specify any of the following filters and click Apply to view the basic details of the returned entities on the right pane.

- Networks (TOP 20) – Select the required organizational networks of the entities.
- Environments (TOP 20) – Select the required environments related to the entities.
- Type – Select the types of the entities you are searching.
- Is Suspicious – Select True and/or False to display entities marked as suspicious or not.
- Is Internal Asset – Select True and/or False to display entities you are searching from within the organization or if they are external entities.
- Is Enriched – Select True and/or False to display entities you are searching are enriched by the system's action or not.

Note: Click Clear to reset case or entity filters to default values anytime.

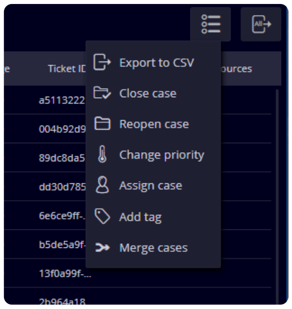
Single or Batch Actions on Cases

The following Actions can be taken on one or more selected Cases:

- **Export to CSV** – Exports the selected case results to your local system in .CSV file format.
- **Export All** – Exports all the cases to your local system in .CSV file format. The system can export up

to 1000 cases.

- **Close case** – Closes the selected cases that are open.
- **Reopen case** – Reopens the selected cases that were closed.
- **Change priority** – Enables you to change the priority of the selected cases that are open.
- **Assign case** – Enables you to assign the selected open cases to a different user.
- **Add tag** – Enables you to add tags to the selected open cases.
- **Merge cases** – Merges two or more of the selected cases that are open.
- **Change status** – Can change status of selected cases.

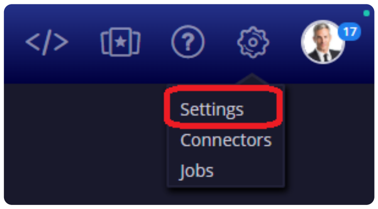


10. Settings

The Settings page allows you to set up various parameters that help maximize the features of Siemplify and customize according to your dynamic needs.

To open the Settings page:

1. From the top menu bar on the right hand side, click the Configuration gear icon and select Settings.



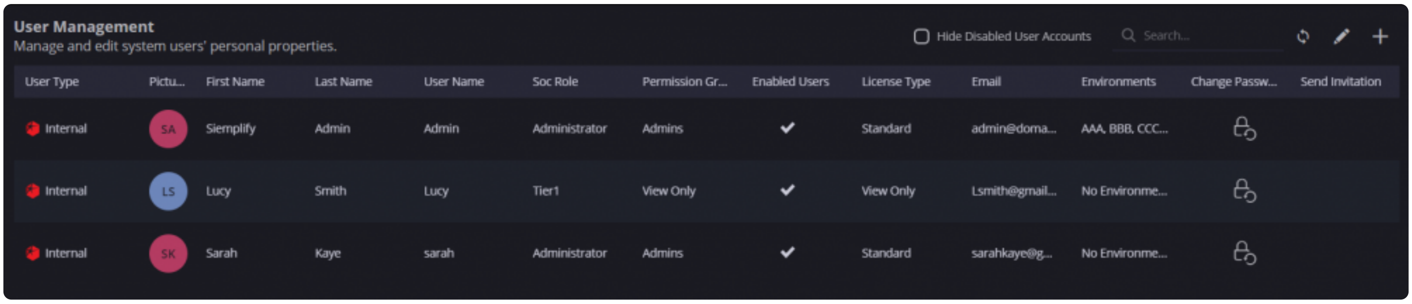
2. The Settings page opens.

10.1. Organization

User Management
Environments
Permissions
License Management
System Logo

10.1.1. User Management

The User Management screen allows you to add, modify and hide inactive users – both Standard Users and View Only Users – in the Siemplify platform. Standard Users can be put into various permission groups and have read/write access to as much or as little of the Platform as you decide. View-Only users require a different license and can only read (view) parts of the Platform. View-Only users can come in useful for MSSPs to allow certain customers to view dashboards or reports specifically aimed at them.



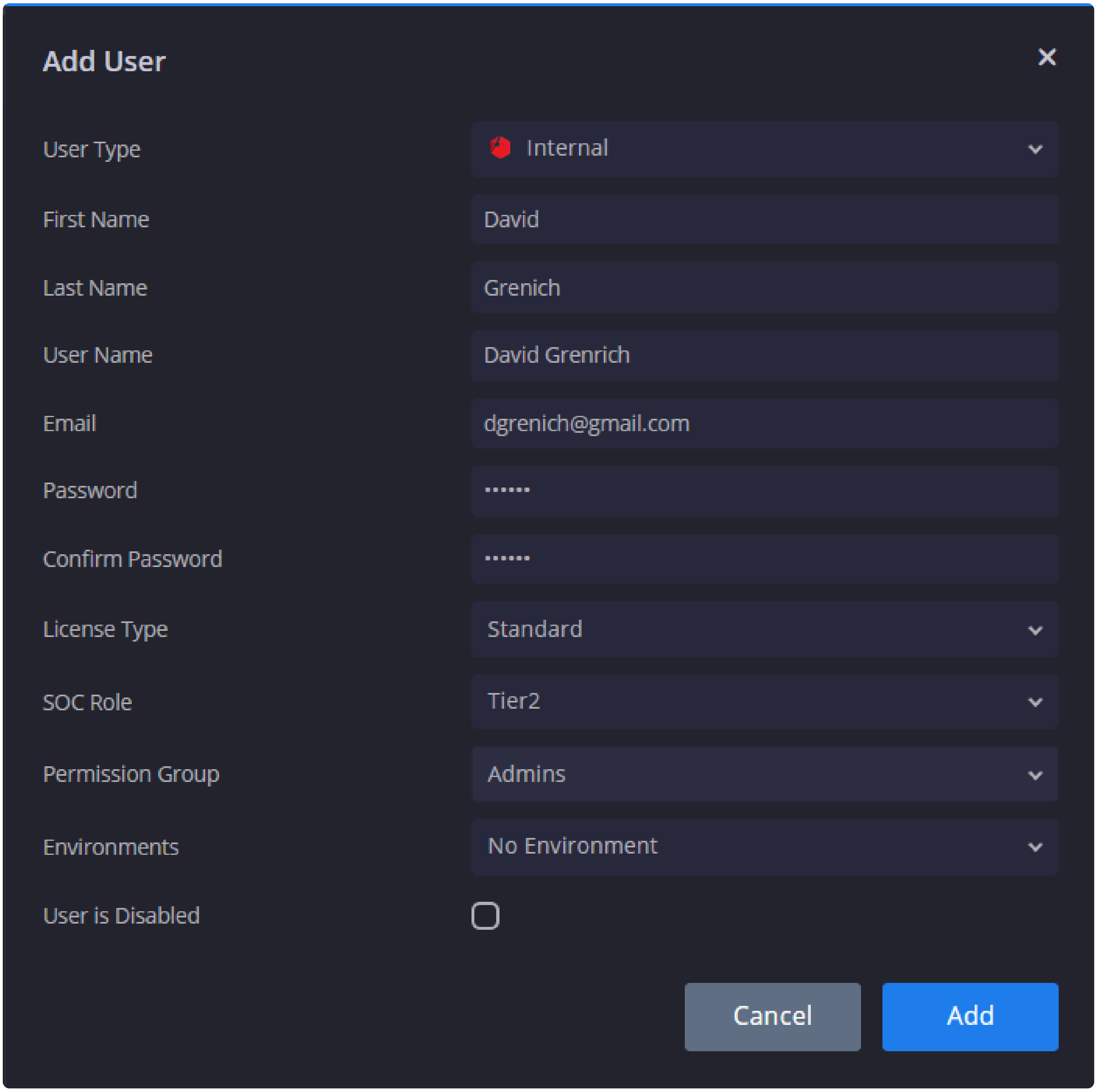
User Management
Manage and edit system users' personal properties.

□ Hide Disabled User Accounts   Search...

User Type	Pictu...	First Name	Last Name	User Name	Soc Role	Permission Gr...	Enabled Users	License Type	Email	Environments	Change Passw...	Send Invitation
Internal	SA	Siemplify	Admin	Admin	Administrator	Admins	✓	Standard	admin@doma...	AAA, BBB, CCC...		
Internal	LS	Lucy	Smith	Lucy	Tier1	View Only	✓	View Only	Lsmith@gmail...	No Environme...		
Internal	SK	Sarah	Kaye	sarah	Administrator	Admins	✓	Standard	sarahkaye@g...	No Environme...		

To add a new user to the Siemplify platform:

1. Click the plus icon on the top right of the screen. The new user screen opens.
2. Fill out the relevant information. If you are configuring new users for SAML authentication, make sure to select the required SAML provider in the User Type field. If you are adding a View-Only user, make sure to select the View-Only option in the License Type field.



Add User

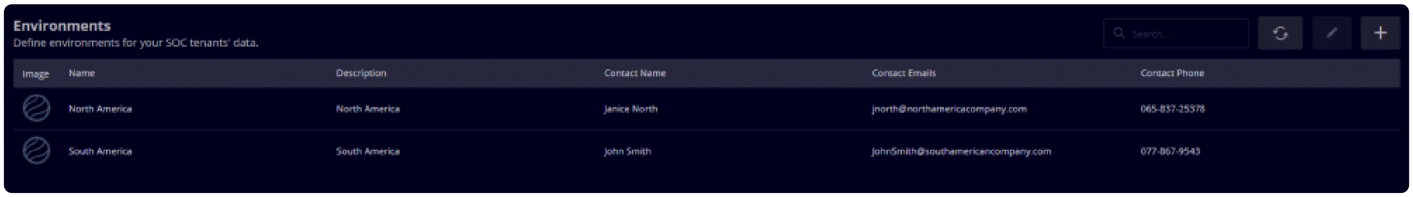
User Type	Internal
First Name	David
Last Name	Grenich
User Name	David Grenrich
Email	dgrenich@gmail.com
Password	••••••
Confirm Password	••••••
License Type	Standard
SOC Role	Tier2
Permission Group	Admins
Environments	No Environment
User is Disabled	□

Note that if you selected a Permission group which has edit permissions to All Environments this will appear here. To change this at Permission group level, select None for All Environment in the Permissions screen. Once you do that, you can select one to several environments for the user to have access to.

3. Click Add. The new user appears in the list of Users.
4. Click on the picture icon to upload a PNG file up to 400kb for this new User. If you are configuring new users for SAML authentication, make sure to click on the Send Invitation icon.

10.1.2. Environments

The Environments screen enables you to add, modify or delete environments, or group them into different categories. An environment is simply another word for your different networks or customers that are managed by the SOC. This is useful for SOCs who provide services to several different networks, customers or business units within the organization. You can search for a specific environment in the Search field, and click on that environment and then Edit details using ✎
The Platform comes with a predefined environment named Default Environment.

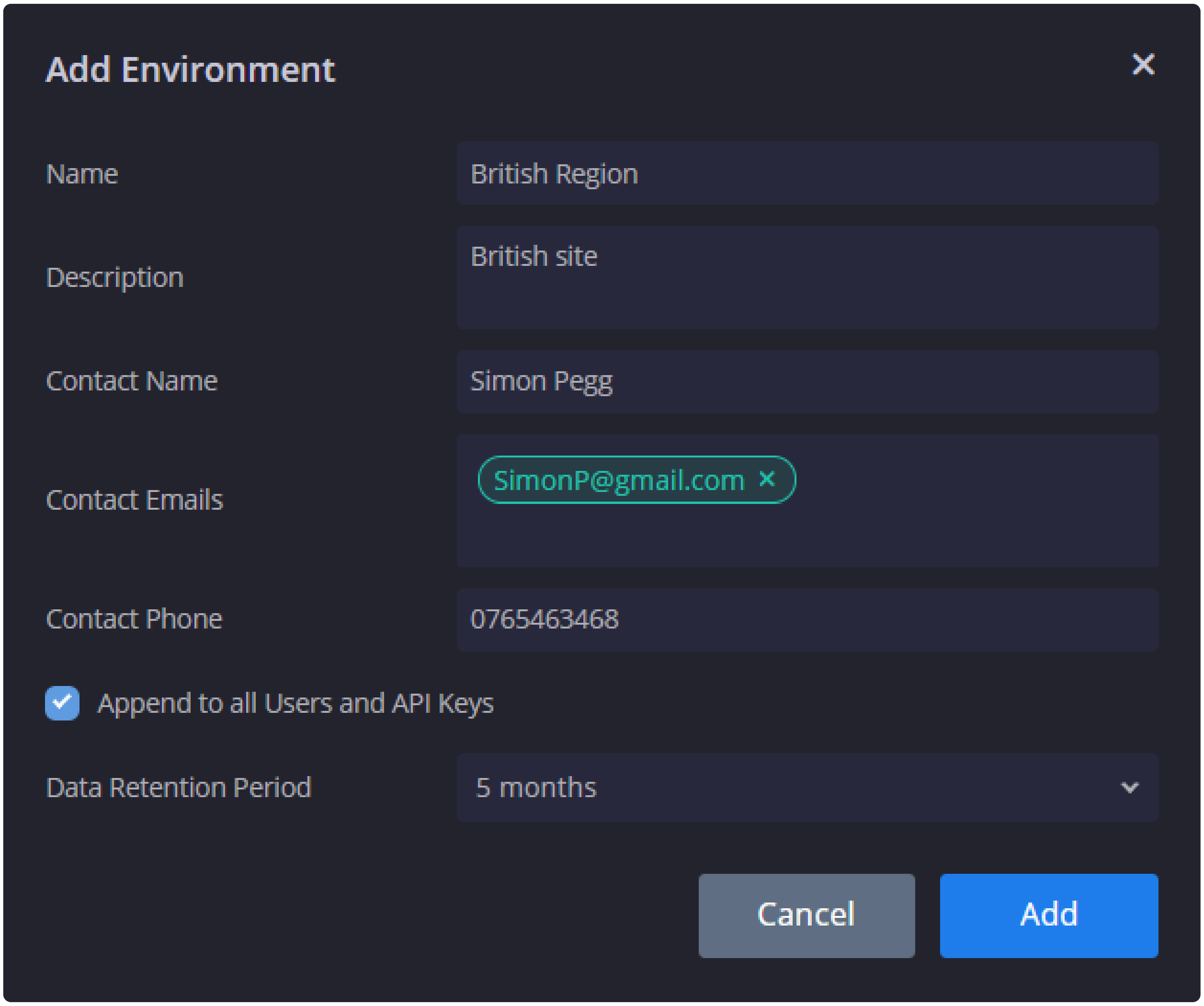


Environments
Define environments for your SOC tenants' data.

Image	Name	Description	Contact Name	Contact Emails	Contact Phone
	North America	North America	Janice North	jnorth@northamericacompany.com	065-837-25378
	South America	South America	John Smith	JohnSmith@southamericancompany.com	077-867-9543

To add a new environment:

1. Click the plus icon on the top right of the screen. The new environment screen opens.
2. Fill out the relevant information. Make sure to click Add to Users and API Keys if you want to add this new environment directly to existing users and API keys.
3. If you have deselected the “Set Default Retention period of all environments” in the General screen, then define here the time period after which all information on closed cases for this environment is deleted.



Add Environment

Name	British Region
Description	British site
Contact Name	Simon Pegg
Contact Emails	SimonP@gmail.com ×
Contact Phone	0765463468

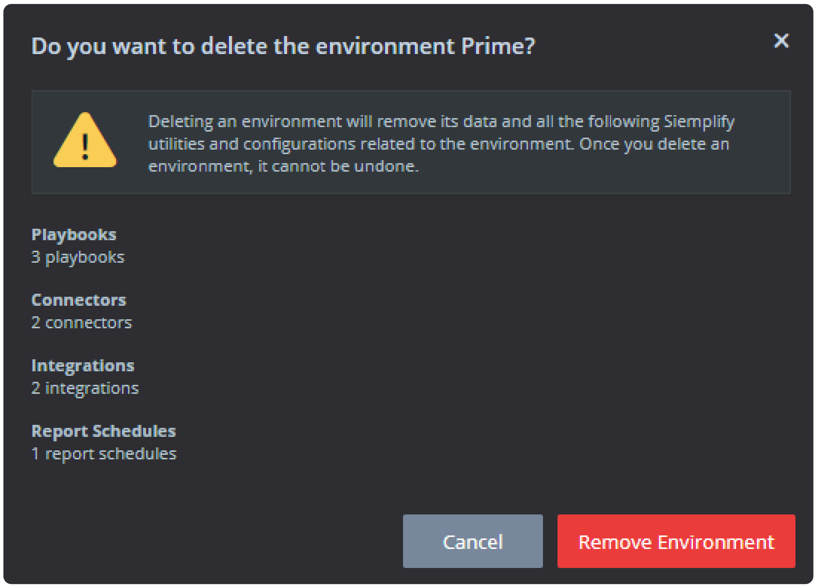
☑ Append to all Users and API Keys

Data Retention Period: 5 months

4. Click Create. The new environment appears in the list of Environments.

To delete an environment:

1. Select the required environment.
2. Click the Edit icon.
3. Click the Delete button in the bottom left of the Edit window.
4. In the Delete screen, you will see all the configurations and utilities related to this environment. Note that once you delete this environment, you cannot undo this action.



Do you want to delete the environment Prime?

Deleting an environment will remove its data and all the following Siemplify utilities and configurations related to the environment. Once you delete an environment, it cannot be undone.

Playbooks
3 playbooks

Connectors
2 connectors

Integrations
2 integrations

Report Schedules
1 report schedules

5. Click Remove Environment.

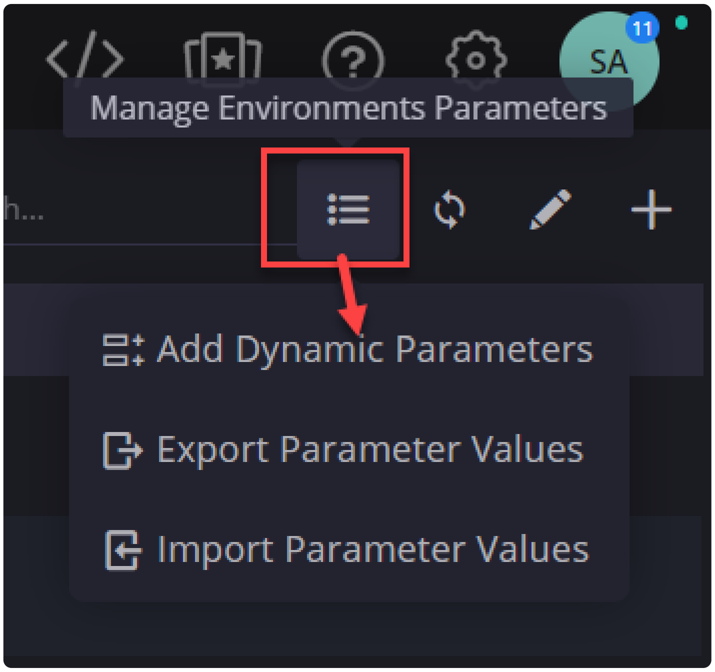
Dynamic Parameters

✻ This feature was added in 5.3.2

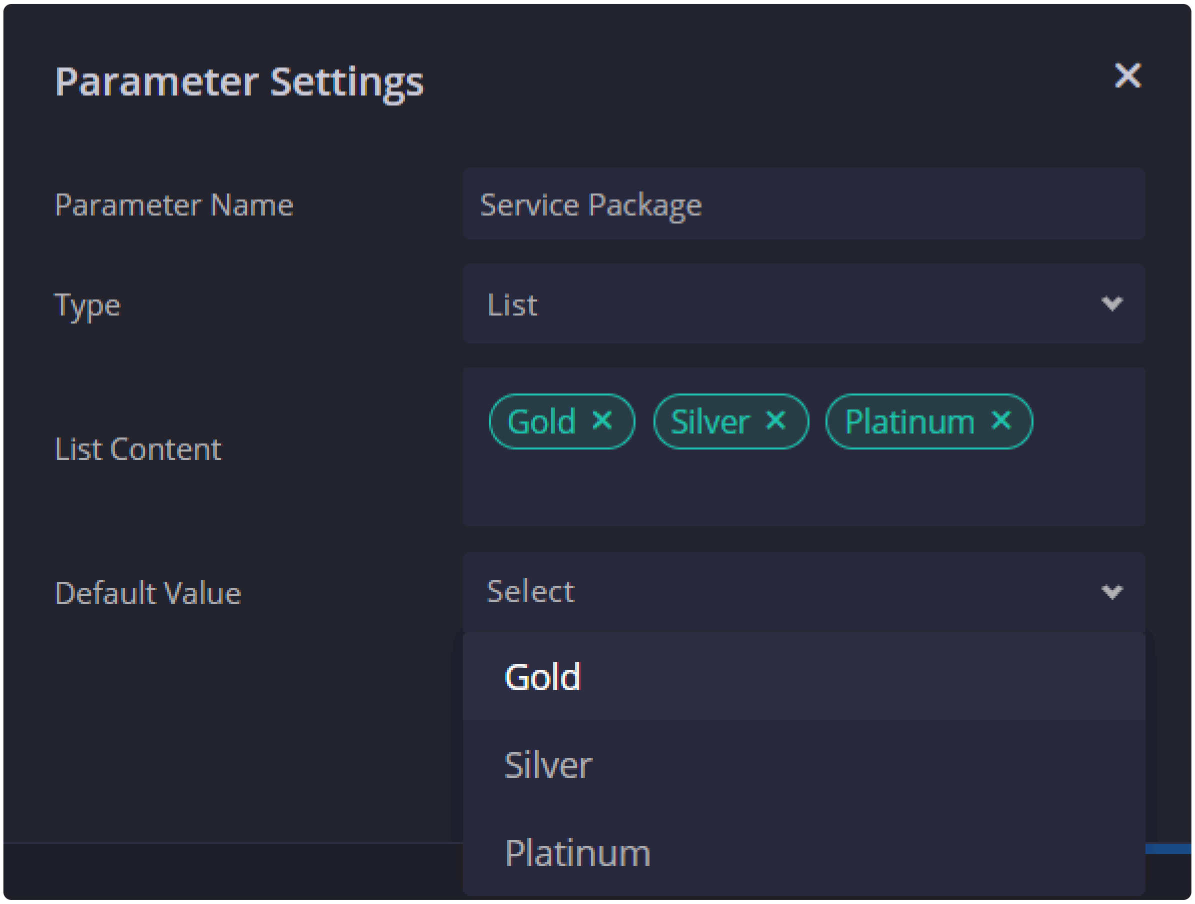
Dynamic Parameters allows you to create “groups” or “categories” of environments to further help categorize and define environments. This can come in particularly useful when running Playbooks as you can use Custom Trigger/Actions or Conditions based on one of these new environment parameters. This provides greater customization for Playbooks and is useful for Enterprises or MSSPs with lots of tenants.

To add a dynamic parameter:

1. In the Environments screen, click on the Manage Environment Parameters button and select Add Dynamic Parameters.



2. In the Dynamic Parameters dialog box, click the plus icon to add a new parameter.
3. Choose a name for the parameter. For this example, let's choose Service package.
4. You can choose to add a string and a default value. Note that the default value will be propagated to all existing environments.
5. Or you can choose to add a list with list content and the default value. In this example, we will choose List, and add values into the List Content. To add a value to the list content, enter the value and click Enter. Repeat till you have the list you need.



Parameter Settings

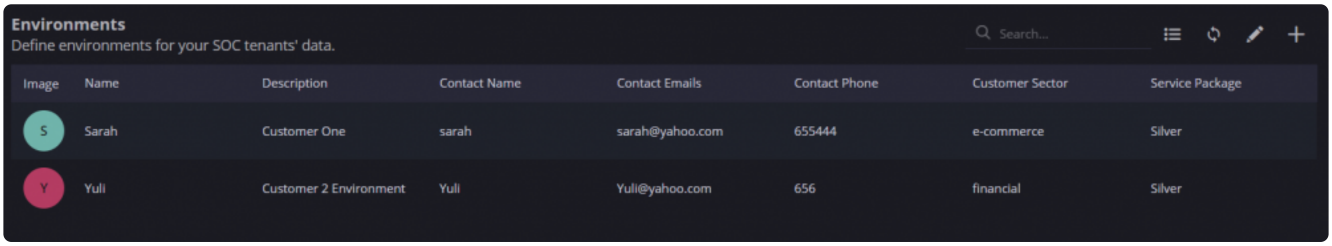
Parameter Name: Service Package

Type: List

List Content: Gold, Silver, Platinum

Default Value: Select

6. Choose the default value that you want from the drop down and save. The dynamic parameter with this default value are now passed on to all existing environments.
   Note that everything can be edited at a later date either one at a time, or as a bulk action using the Export/Import procedure described below.
7. The dynamic parameter is added to the main screen as shown in the screenshot below.



Environments
Define environments for your SOC tenants' data.

Image	Name	Description	Contact Name	Contact Emails	Contact Phone	Customer Sector	Service Package
S	Sarah	Customer One	sarah	sarah@yahoo.com	655444	e-commerce	Silver
Y	Yuli	Customer 2 Environment	Yuli	Yuli@yahoo.com	656	financial	Silver

Editing in Bulk using Export / Import

In order to perform editing actions in bulk, it is recommended to edit in an exported Excel chart.

To edit parameters in bulk:

1. Click on the Manage Environment Parameters button and select Export Dynamic Parameters.

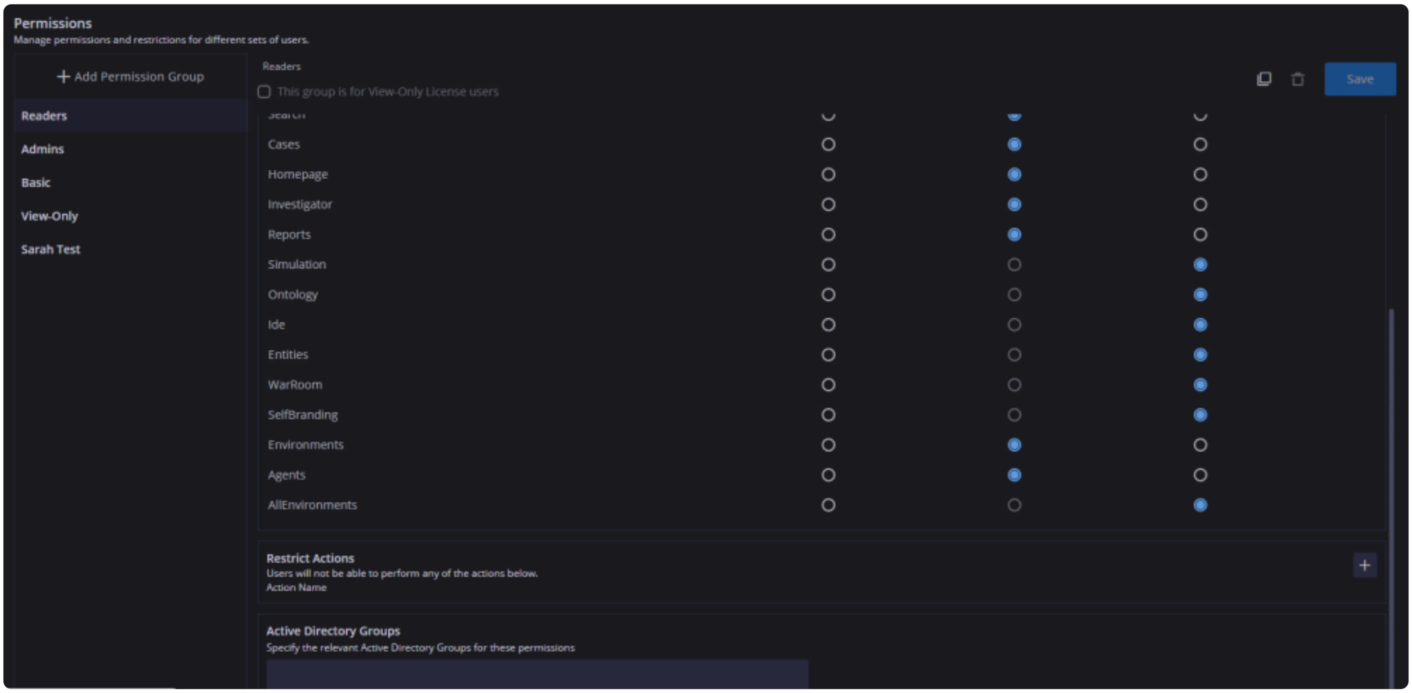
2. In the excel chart, perform bulk editing on the values. Note that you cannot change the Parameter Names or Environment names.
3. When done, click on Manage Environment Parameters button and select Import Dynamic Parameters.

10.1.3. Permissions

In the Permissions screen you can manage permissions and restrictions for different types of users, user groups and actions.
For example, if the user is in a group that has Edit permissions for the Playbooks module then the user can both view and edit that Playbook. However, if you then add a restricted Action to this group such as Download Email Attachments, then this User will no longer be able to view or edit any Playbook that contains this action.

Note that the following predefined permission groups are in the Siemplify Platform:

- Readers
- Admin
- Basic
- View Only – these are for users with a View Only License


Permissions
Manage permissions and restrictions for different sets of users.

Readers
□ This group is for View-Only License users

Search	○	●	○
Cases	○	●	○
Homepage	○	●	○
Investigator	○	●	○
Reports	○	●	○
Simulation	○	○	●
Ontology	○	○	●
Ide	○	○	●
Entities	○	○	●
WarRoom	○	○	●
SelfBranding	○	○	●
Environments	○	●	○
Agents	○	●	○
AllEnvironments	○	○	●

Restrict Actions
Users will not be able to perform any of the actions below.
Action Name

Active Directory Groups
Specify the relevant Active Directory Groups for these permissions

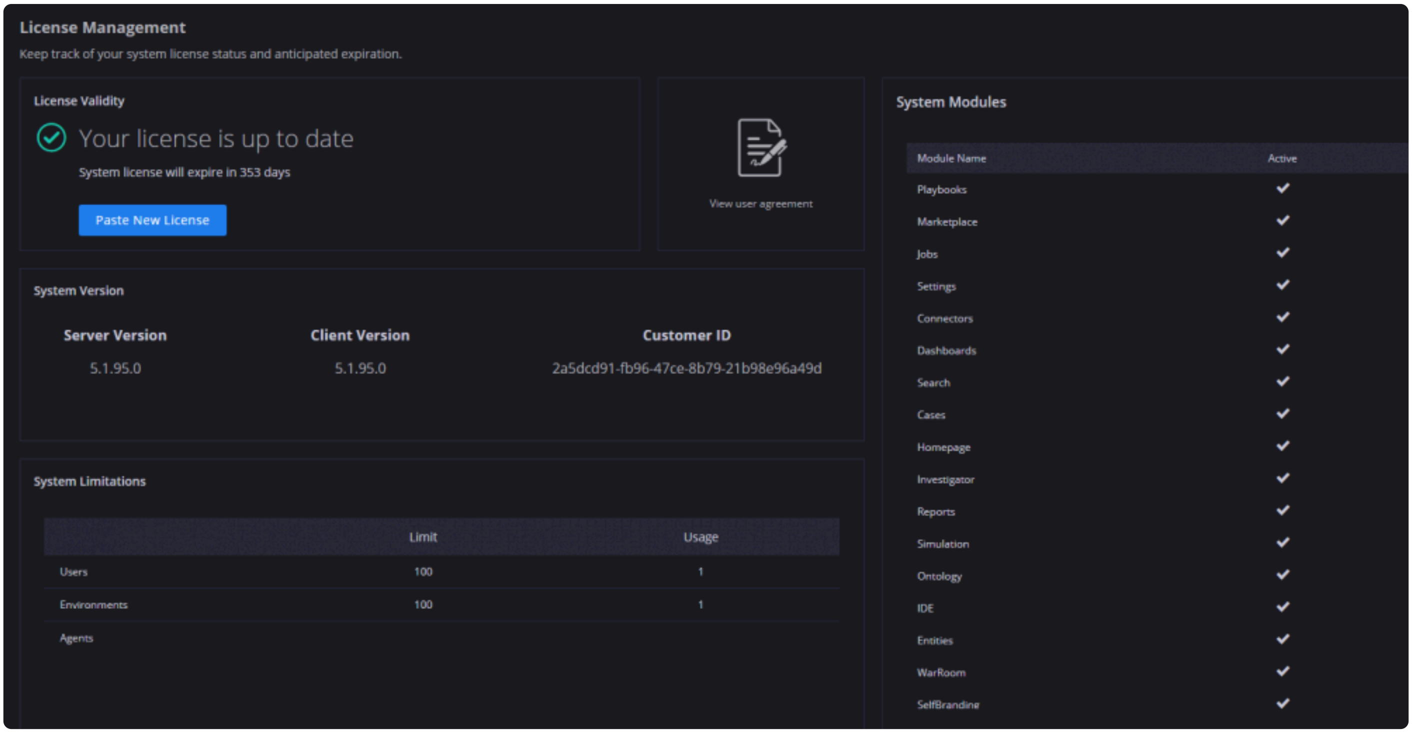
The predefined Admin group has predefined Edit rights to the All Environments thereby allowing them to view data from all environments in the system. When creating a new permissions group, it is recommended to think carefully before allowing edit rights to All Environments.

To add a new permissions group:

1. Click the Add Permissions group. A New Group is added to the list on the left.
2. Fill out the following areas on the screen:
    a. Your cursor will automatically be placed next to the title of New Group. Delete the words New Group and add in your own name for the new Group. For example, Tier One.
    b. If you are creating a View Only user group, then tick the required checkbox.
    c. Decide what type of permissions you want to give this group for each module – Edit, View or None.
    d. Add Active Directory groups to be assigned to this permission group. This is useful if you are using Active Directory to authenticate Siemplify users.
    e. If required, you can restrict specific Actions for this new group. Click on the plus sign in the Restrict Actions area and choose the action from the drop down. For multiple actions, you will need to add one at a time. So for example, you might want to restrict Delete Cases Action. Note that if an analyst in this user group tries to run a playbook with this action, they will be denied permission to run this playbook.
3. When finished, make sure to click Save. Note that at any time, you can make changes and then re-Save. You can also duplicate permission groups for easier editing.

10.1.4. License Management

In the License Management screen, you can add or modify licensing details as well as view license version details and the user agreement.



License Management

Keep track of your system license status and anticipated expiration.

License Validity

Your license is up to date

System license will expire in 353 days

System Version

Server Version	Client Version	Customer ID
5.1.95.0	5.1.95.0	2a5dcd91-fb96-47ce-8b79-21b98e96a49d

System Limitations

	Limit	Usage
Users	100	1
Environments	100	1
Agents		

System Modules

Module Name	Active
Playbooks	✓
Marketplace	✓
Jobs	✓
Settings	✓
Connectors	✓
Dashboards	✓
Search	✓
Cases	✓
Homepage	✓
Investigator	✓
Reports	✓
Simulation	✓
Ontology	✓
IDE	✓
Entities	✓
WarRoom	✓
SelfBranding	✓

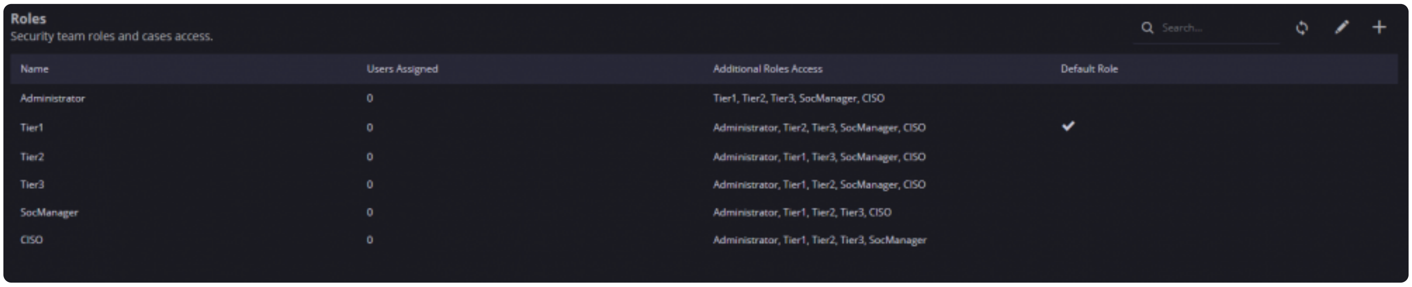
To upload a new license:

1. Copy the license key from the email you received from Siemplify.
2. Click Paste new licence . The Upload new license dialog displays.
3. Paste in the license key and click Update. Your license is updated.

10.1.5. Roles

The Security Analyst can add up to 20 customized roles in this screen. In addition, the predefined SOC roles can be modified here as well.

New roles can be created for various purposes including routing tasks to specific SOC teams, managing their daily workload, controlling view permissions and managing cases access permissions.



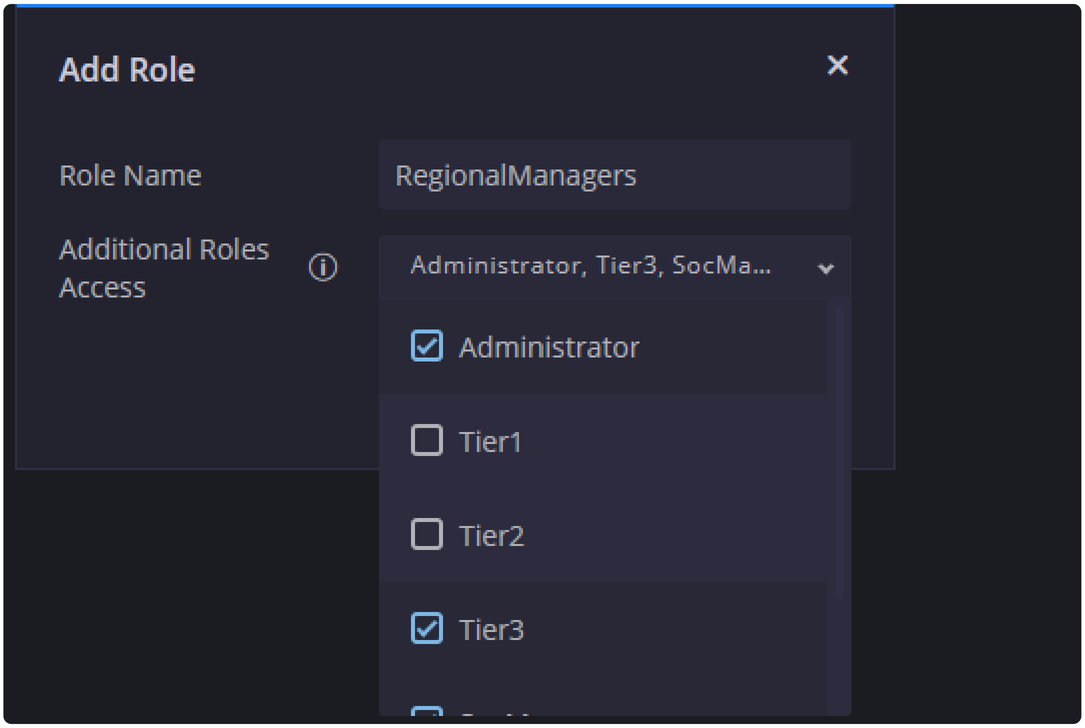
Roles

Security team roles and cases access.

Name	Users Assigned	Additional Roles Access	Default Role
Administrator	0	Tier1, Tier2, Tier3, SocManager, CISO	
Tier1	0	Administrator, Tier2, Tier3, SocManager, CISO	✓
Tier2	0	Administrator, Tier1, Tier3, SocManager, CISO	
Tier3	0	Administrator, Tier1, Tier2, SocManager, CISO	
SocManager	0	Administrator, Tier1, Tier2, Tier3, CISO	
CISO	0	Administrator, Tier1, Tier2, Tier3, SocManager	

To create a new role:

1. Click the plus icon on the top right of the screen.
2. In the Add Role dialog box, enter a name for the new Role, and select which additional roles they should have access to. (This will affect which cases they can see in the Siemplify platform.)



Add Role

Role Name: RegionalManagers

Additional Roles Access: Administrator, Tier3, SocMa...

☑ Administrator

□ Tier1

□ Tier2

☑ Tier3

3. Click Add. The Role is added to the table in the screen.

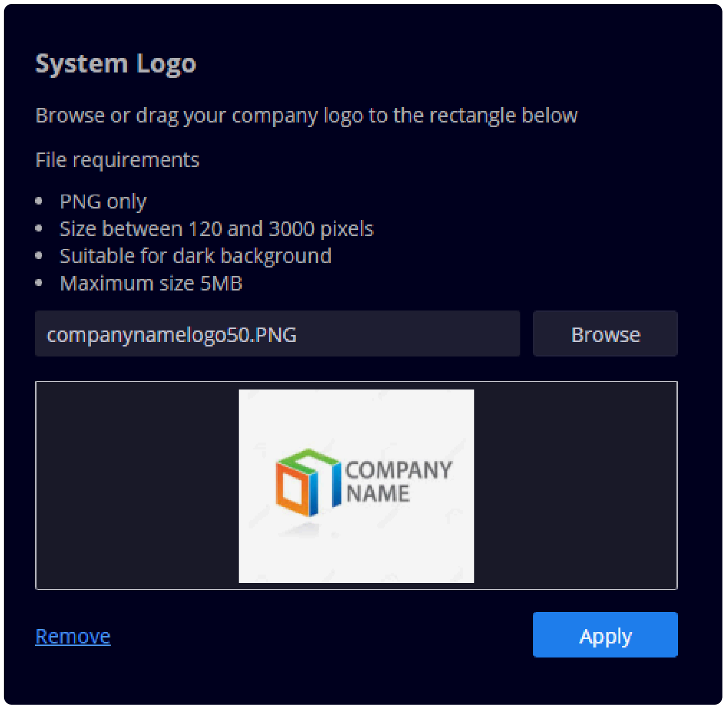
One of the Roles can be set as Default using the Edit button. The default role will have all new cases automatically assigned to it. Note that this default role cannot be deleted.

10.1.6. System Logo

In the System Logo screen, you can brand the Siemplify platform by adding your company logo.

To add a logo:

1. Browse and attach your logo.



System Logo

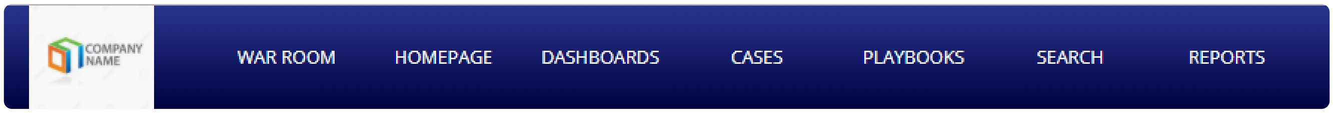
Browse or drag your company logo to the rectangle below

File requirements

- PNG only
- Size between 120 and 3000 pixels
- Suitable for dark background
- Maximum size 5MB

companynamelogo50.PNG

2. Click Apply. The top menu bar refreshes to display your company logo.



10.2. Case Data

10.2.1. Tags

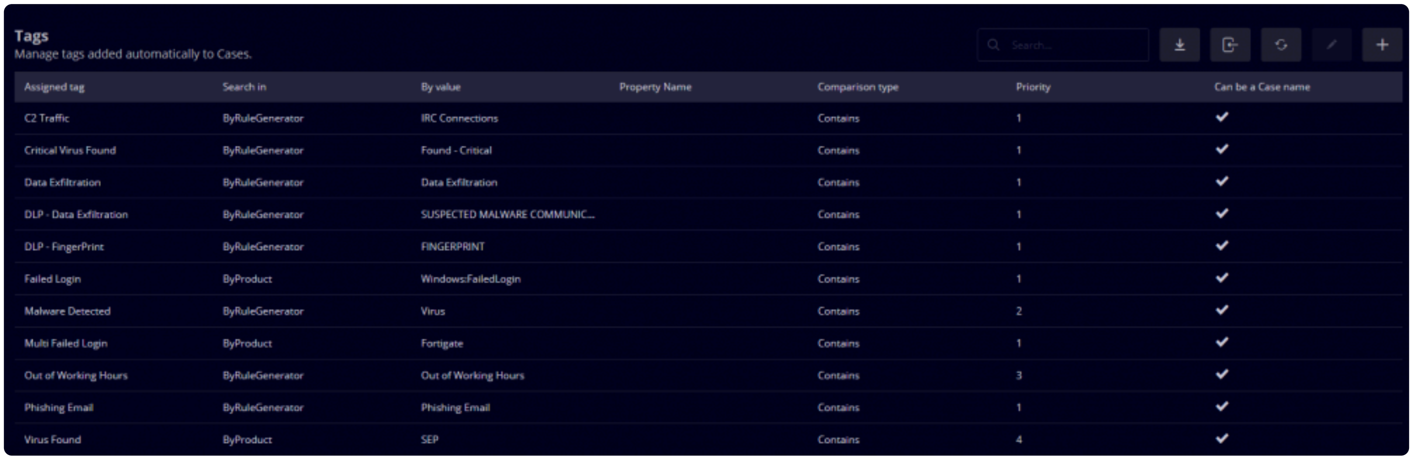
In the Tags screen, you have the option to add, modify and delete tags. Tags are assigned to cases by Siemplify based on predefined rules and can be used to classify cases or find specific cases faster. Note that you can manually add tags to a case from the Case screen. These tags can be removed from the case, but NOT removed entirely from the system.

You might want to import tags in the following situations. For example, moving from staging to production environment or for backup purposes.

To import tags:

1. Click on the Download template icon. The excel chart shows the exact structure of how the imported tags should be layed out.
2. Enter in the tag information.
3. Click the Import icon and import in the filled excel chart.

> The relationship between Assigned Tag and Search Name is many-to-many. That is, more than one Assigned Tag can be associated with one Search Name, and more than one Search Name can be associated with one Assigned Tag. For example, Siemplify assigns the same tag “DLP” to alerts the SIEM tags as “Data Exfiltration” or “Symantec DLP – Financial Information – Network”.



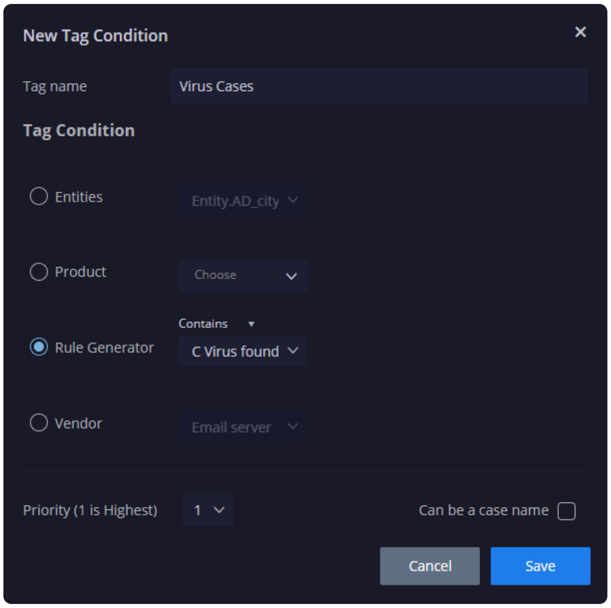
Tags

Manage tags added automatically to Cases.

Assigned tag	Search in	By value	Property Name	Comparison type	Priority	Can be a Case name
C2 Traffic	ByRuleGenerator	IRC Connections		Contains	1	✓
Critical Virus Found	ByRuleGenerator	Found - Critical		Contains	1	✓
Data Exfiltration	ByRuleGenerator	Data Exfiltration		Contains	1	✓
DLP - Data Exfiltration	ByRuleGenerator	SUSPECTED MALWARE COMMUNIC...		Contains	1	✓
DLP - FingerPrint	ByRuleGenerator	FINGERPRINT		Contains	1	✓
Failed Login	ByProduct	Windows:FailedLogin		Contains	1	✓
Malware Detected	ByRuleGenerator	Virus		Contains	2	✓
Multi Failed Login	ByProduct	Fortigate		Contains	1	✓
Out of Working Hours	ByRuleGenerator	Out of Working Hours		Contains	3	✓
Phishing Email	ByRuleGenerator	Phishing Email		Contains	1	✓
Virus Found	ByProduct	SEP		Contains	4	✓

To add a new tag:

1. Click on the plus icon on the top right of the screen.
2. In Tag Condition, choose between Entities, Product, Rule Generator or Vendor. Note that you can select Other and add in your own option thereby creating a new tag.
3. Where required, add in the value of the above.
4. After selecting one of the options, you will see a drop down with the following qualifiers, contains, exact, starts with, ends with. Choose the qualifier that best fits your needs.
5. Select the priority for the tag. Note that Siemplify merges priority with other alerts and entities and events so that the priority here is not an absolute.
6. Select the **Can be a case name** if required. When checked, the tag will be assigned as the title of the Case if it meets the conditions.



New Tag Condition

Tag name Virus Cases

Tag Condition

○ Entities Entity.AD_city

○ Product Choose

● Rule Generator Contains C Virus found

○ Vendor Email server

Priority (1 is Highest) 1

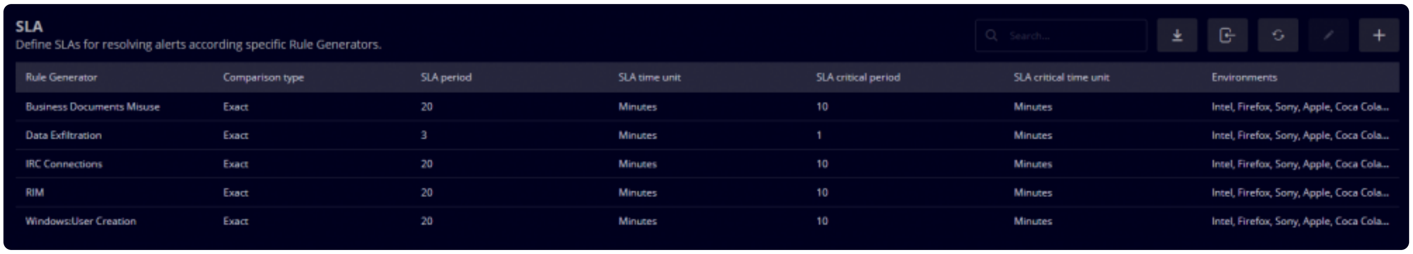
Can be a case name □

7. Click Save.

10.2.2. SLA

A Service Level Agreement (SLA) represents a commitment by the SOC to resolve certain types of cases within a specified duration of time. For example, you can specify that cases with a specific tag must be resolved within 30 minutes. When several SLAs are attached to a case (i.e.when several alerts in the case contain SLA) then the case SLA will be assigned with the SLA of the shortest time, as defined in the SLA period field.

The SLA screen tab enables you to add, modify, and delete SLA definitions.



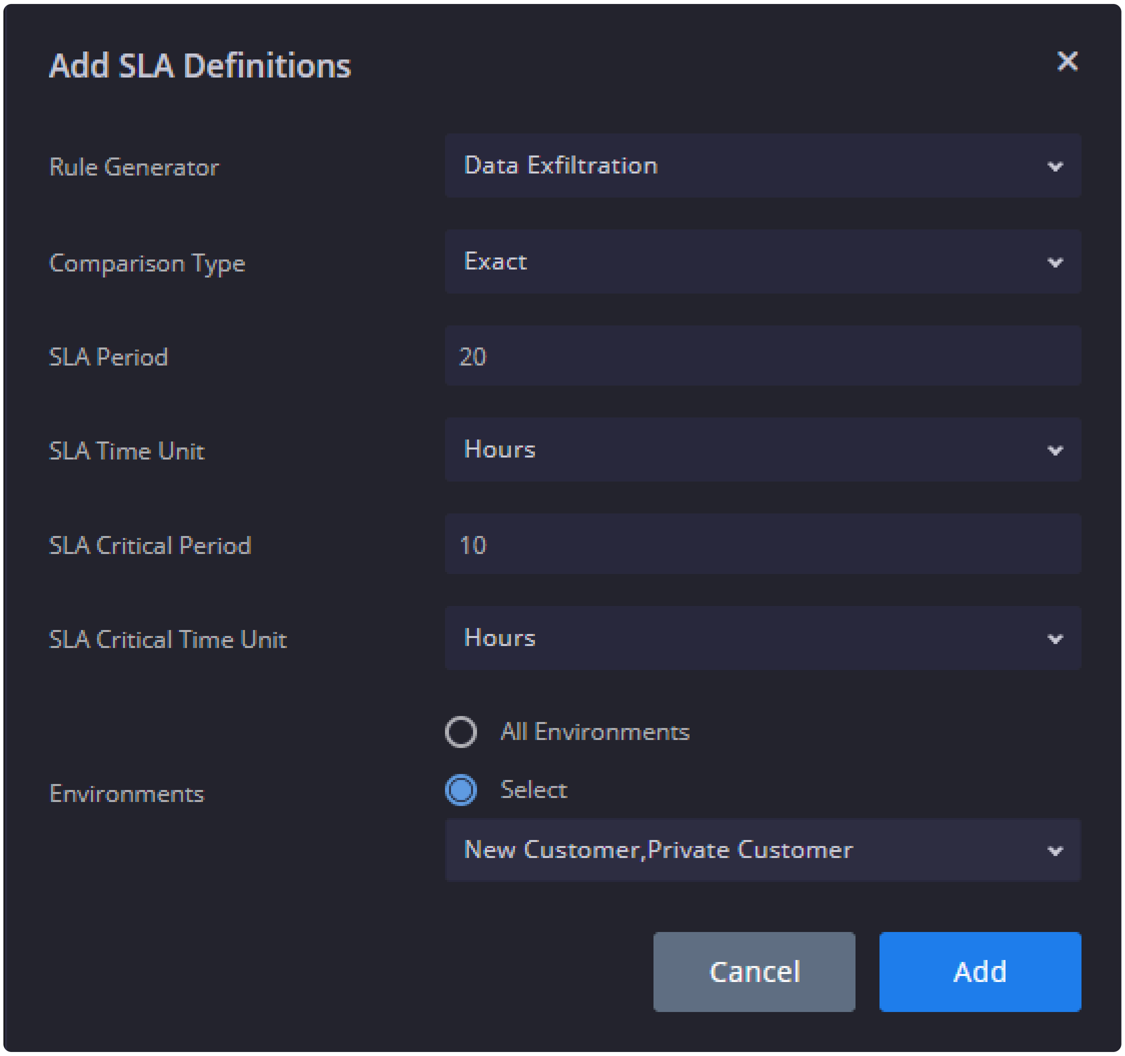
SLA

Define SLAs for resolving alerts according specific Rule Generators.

Rule Generator	Comparison type	SLA period	SLA time unit	SLA critical period	SLA critical time unit	Environments
Business Documents Misuse	Exact	20	Minutes	10	Minutes	Intel, Firefox, Sony, Apple, Coca Cola...
Data Exfiltration	Exact	3	Minutes	1	Minutes	Intel, Firefox, Sony, Apple, Coca Cola...
IRC Connections	Exact	20	Minutes	10	Minutes	Intel, Firefox, Sony, Apple, Coca Cola...
RIM	Exact	20	Minutes	10	Minutes	Intel, Firefox, Sony, Apple, Coca Cola...
Windows:User Creation	Exact	20	Minutes	10	Minutes	Intel, Firefox, Sony, Apple, Coca Cola...

To add an SLA:

1. Click the plus icon on the top right of the screen.
2. Add in the relevant information to the New SLA Definitions box.
   Note that the SLA period is counted from when an alert enters the system.



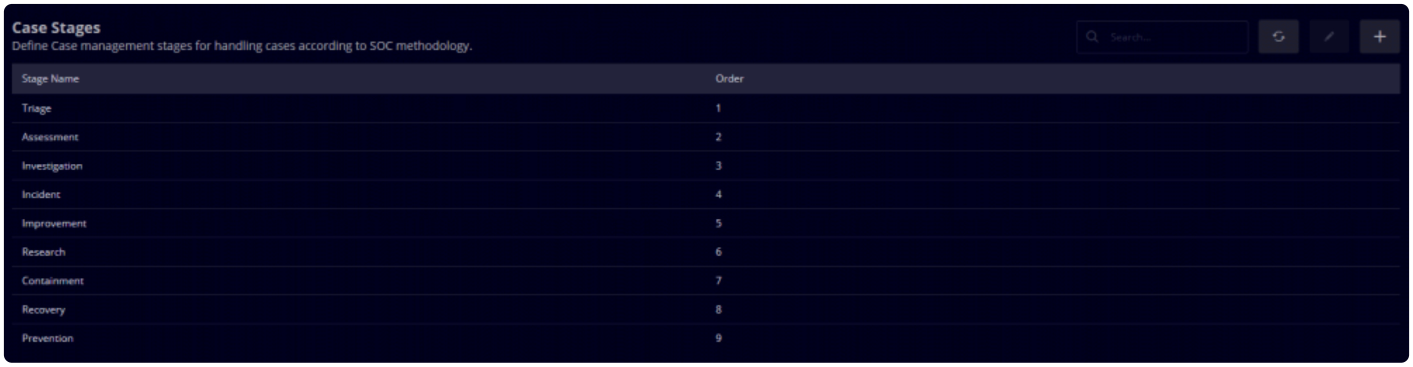
Add SLA Definitions

Rule Generator	Data Exfiltration
Comparison Type	Exact
SLA Period	20
SLA Time Unit	Hours
SLA Critical Period	10
SLA Critical Time Unit	Hours
Environments	○ All Environments ● Select New Customer,Private Customer

3. Click Create.

10.2.3. Case Stages

In the Case Stages screen, you can add, modify, and delete case stages. You can customize the stages to match your organization’s case management stages so as to be in alignment with your company strategy.



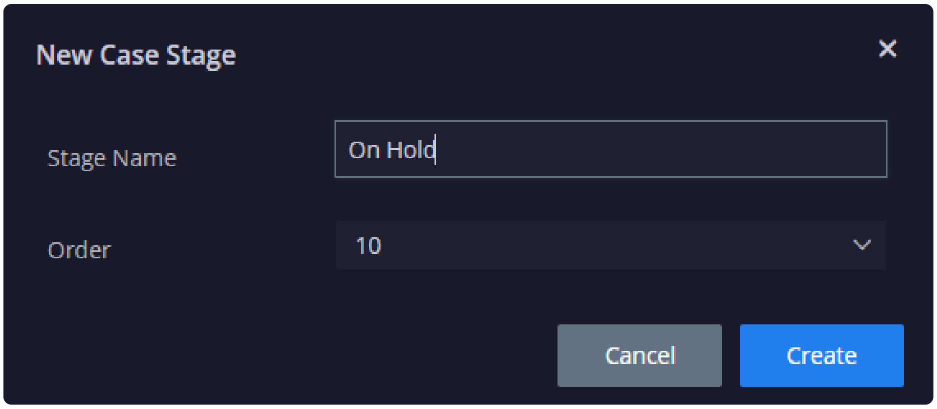
Case Stages

Define Case management stages for handling cases according to SOC methodology.

Stage Name	Order
Triage	1
Assessment	2
Investigation	3
Incident	4
Improvement	5
Research	6
Containment	7
Recovery	8
Prevention	9

To add a new stage:

1. Click the plus icon on the top right of the screen.
2. Add the relevant information.



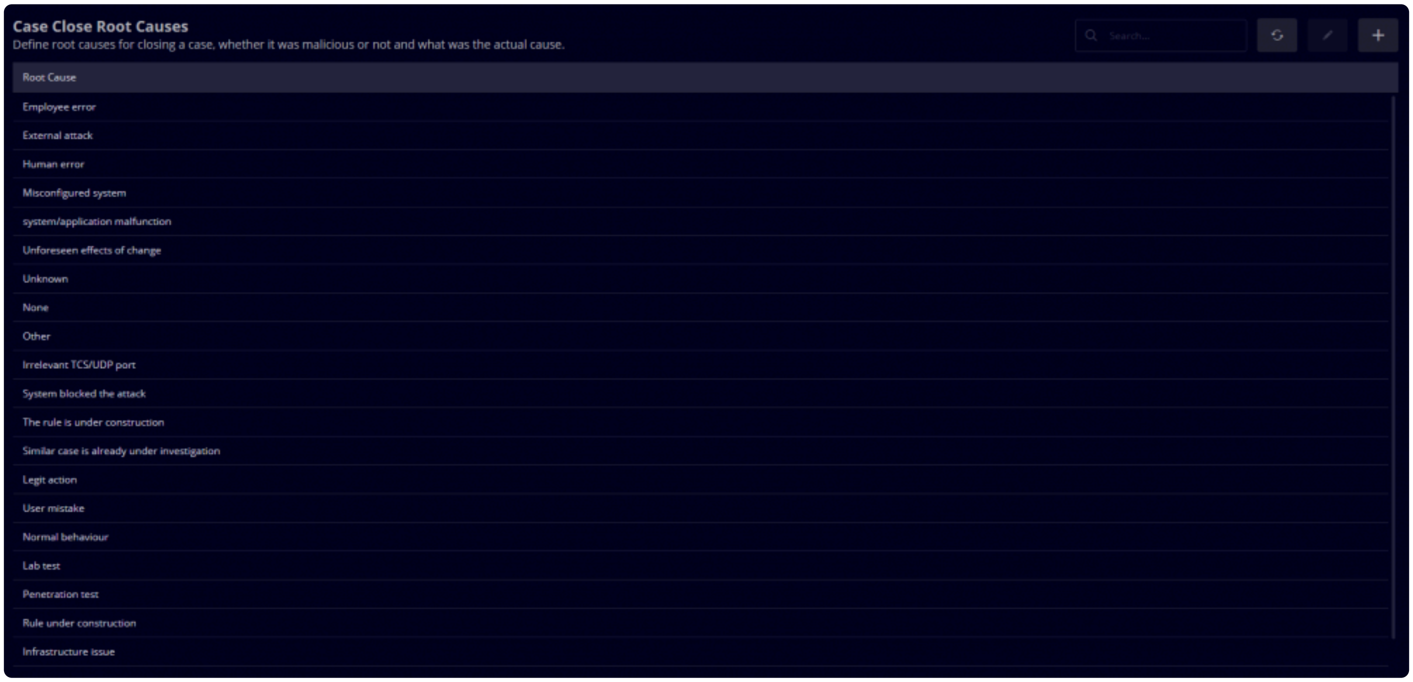
New Case Stage

Stage Name	On Hold
Order	10

3. Click Create.

10.2.4. Case Close Root Cause

In the Case Close Root Cause screen, you can define root causes for closing a case. These will be used by the analyst when closing a case.



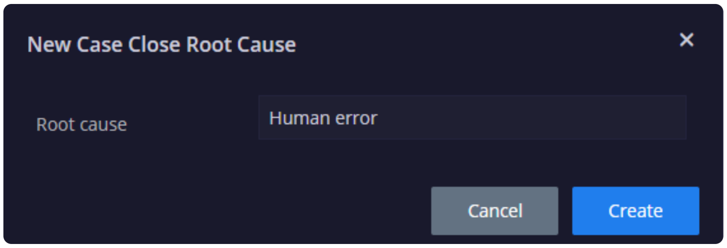
Case Close Root Causes

Define root causes for closing a case, whether it was malicious or not and what was the actual cause.

Root Cause
Employee error
External attack
Human error
Misconfigured system
system/application malfunction
Unforeseen effects of change
Unknown
None
Other
Irrelevant TCS/UDP port
System blocked the attack
The rule is under construction
Similar case is already under investigation
Legit action
User mistake
Normal behaviour
Lab test
Penetration test
Rule under construction
Infrastructure issue

To add a new root cause:

1. Click the plus icon on the top right of the screen.
2. Add in the relevant information.



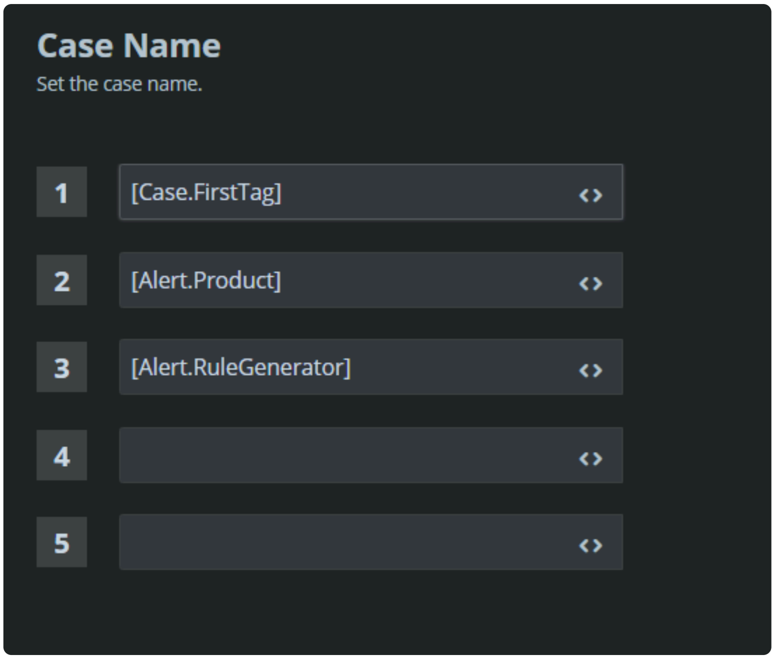
New Case Close Root Cause

Root cause: Human error

3. Click Create.

10.2.5. Case Name

In the Case Name screen you can set the conditions by which Siemplify will know what name to give a case. In this screen are five fields – Siemplify matches each case with the first field name. If there is no match, Siemplify moves to the next field.



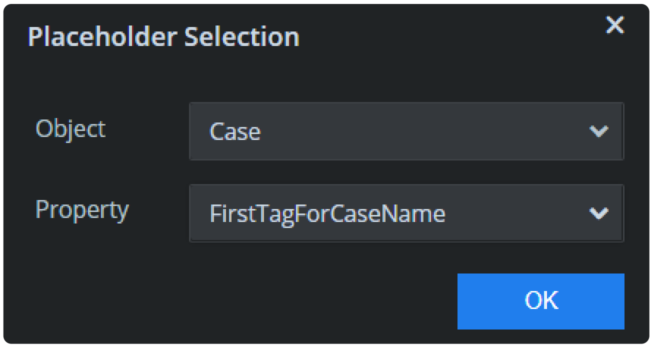
Case Name

Set the case name.

1 [Case.FirstTag]
2 [Alert.Product]
3 [Alert.RuleGenerator]
4
5

To add a Case Name:

1. Place your cursor in the first field.
2. You can choose to enter fixed text or alternately, click <> on the right of the field.
   a. In the Object field, choose from Alert, Case or Event.
   b. Choose the required property. For example, choose First Tag for Case Name for the Case Object. This means, that the Case will be called by the first Tag Name.



c. Click OK.

3. Repeat as required.

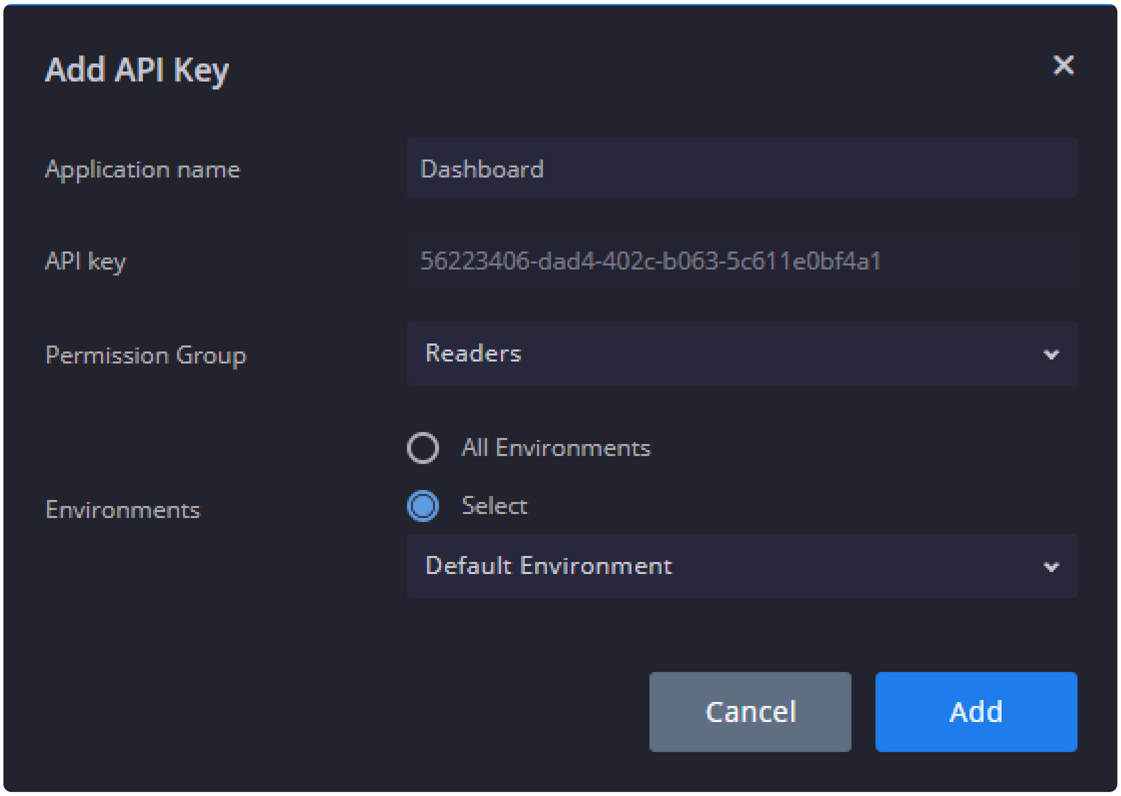
10.3. Advanced

10.3.1. API Keys

In the API keys screen you can specify new API keys that provide authentication to connect via Siemplify API.
For a detailed list of Siemplify API commands, refer to https://[hostname]:443/swagger

To create a new API key:

1. Click the plus icon on the top right of the screen.
2. In the new API screen, add the name of the application that you need to access Siemplify via API.
3. Select the required permission group for this API key. Note that the groups that appear in this dropdown are defined in the Organizations > Permissions screen.
4. Select the required environments: All Environments or Multi-Select.



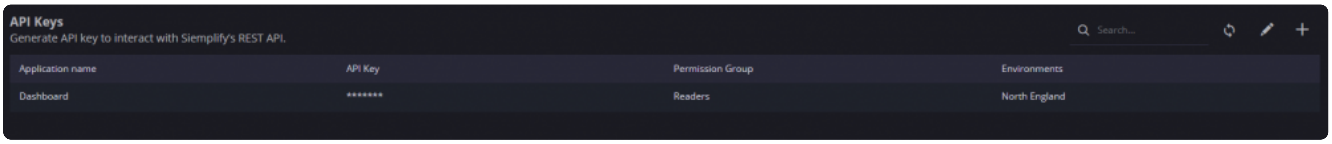
Application name: Dashboard

API key: 56223406-dad4-402c-b063-5c611e0bf4a1

Permission Group: Readers

Environments:
○ All Environments
● Select
Default Environment

5. Click Create. The new key now appears in the API keys screen.

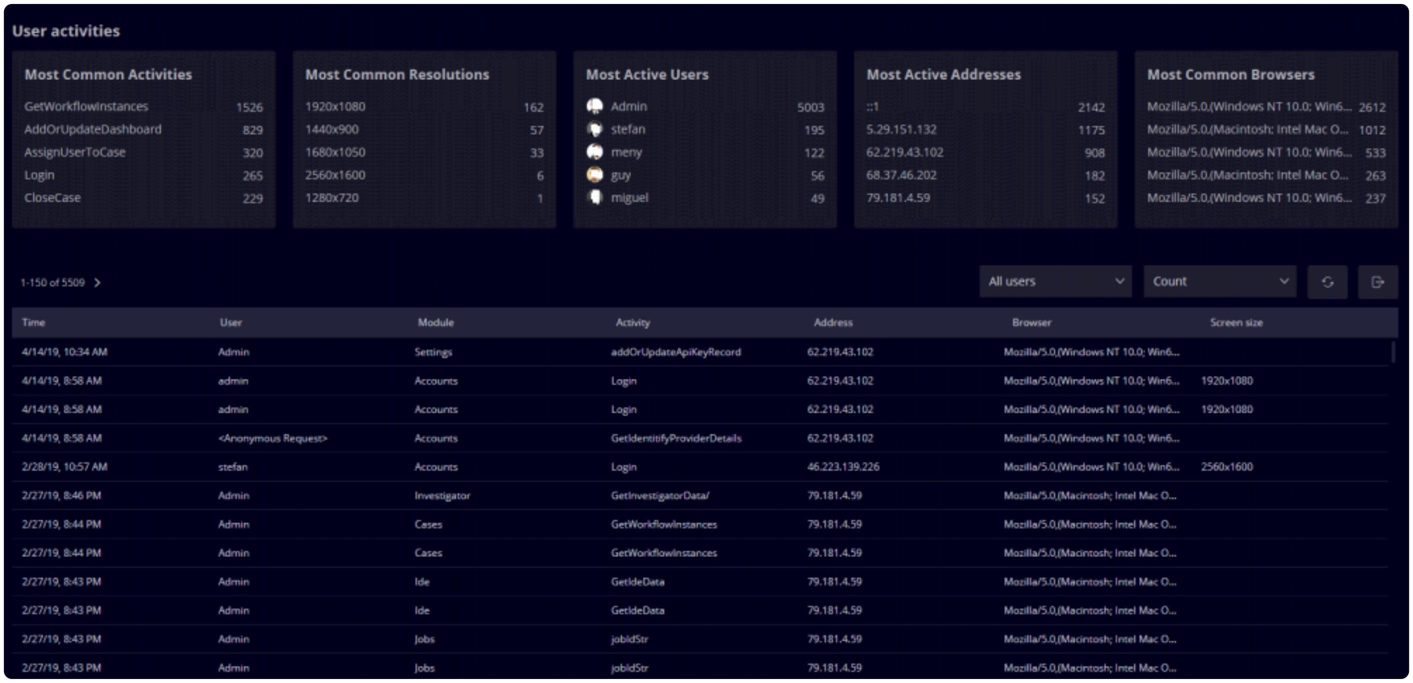


API Keys
Generate API key to interact with Siemplify's REST API.

Application name	API Key	Permission Group	Environments
Dashboard	*******	Readers	North England

10.3.2. Audit

In the Audit screen you can see at a glance the most common activities and other topics of interest. In addition, you can filter results according to User Name, Activities Group, or Number (Count). You can also export the results to a CSV file for further analysis.



User activities

Most Common Activities	
GetWorkflowInstances	1526
AddOrUpdateDashboard	829
AssignUserToCase	320
Login	265
CloseCase	229

Most Common Resolutions	
1920x1080	162
1440x900	57
1680x1050	33
2560x1600	6
1280x720	1

Most Active Users	
Admin	5003
stefan	195
meny	122
guy	56
miguel	49

Most Active Addresses	
::1	2142
5.29.151.132	1175
62.219.43.102	908
68.37.46.202	182
79.181.4.59	152

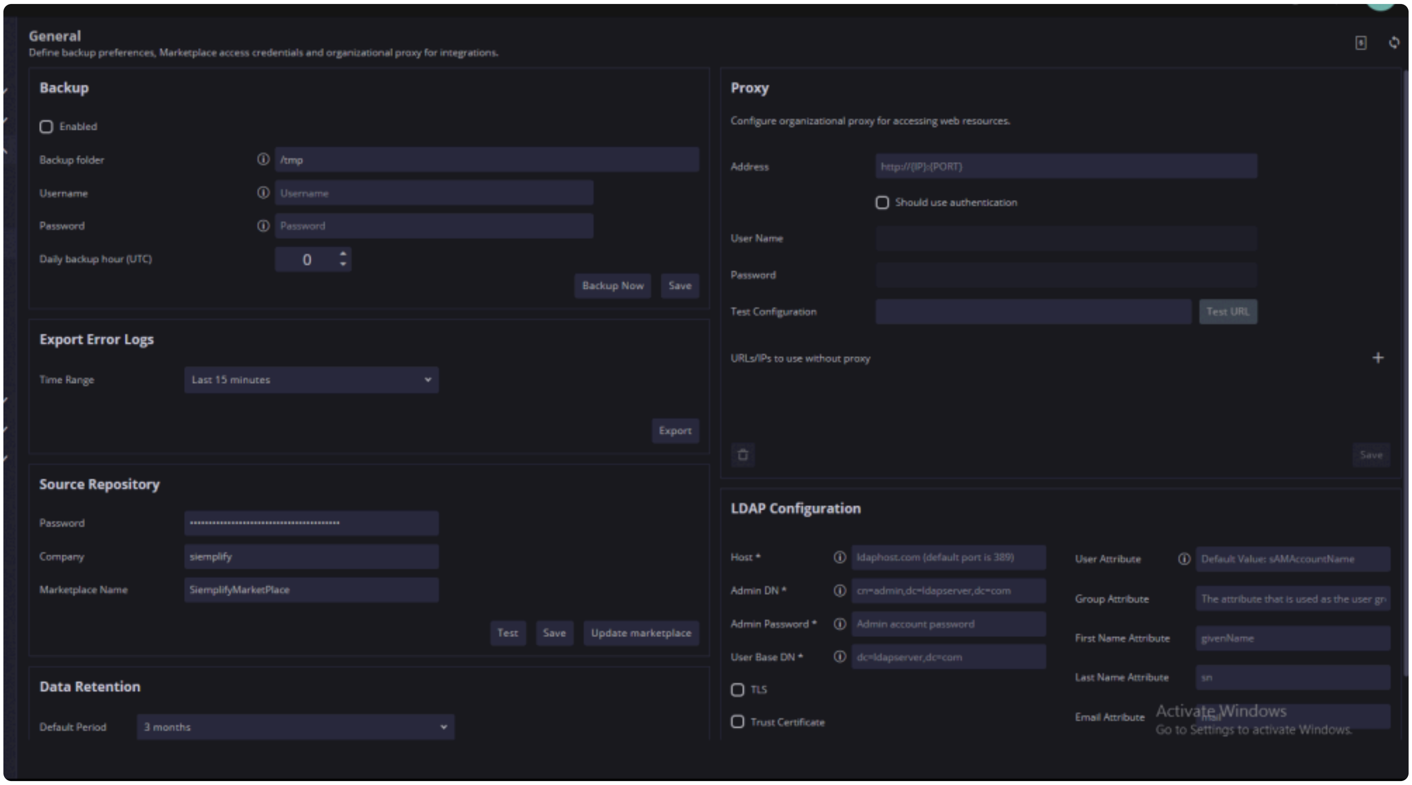
Most Common Browsers	
Mozilla/5.0,(Windows NT 10.0; Win6...	2612
Mozilla/5.0,(Macintosh; Intel Mac O...	1012
Mozilla/5.0,(Windows NT 10.0; Win6...	533
Mozilla/5.0,(Macintosh; Intel Mac O...	263
Mozilla/5.0,(Windows NT 10.0; Win6...	237

Time	User	Module	Activity	Address	Browser	Screen size
4/14/19, 10:34 AM	Admin	Settings	addOrUpdateApiKeyRecord	62.219.43.102	Mozilla/5.0,(Windows NT 10.0; Win6...	
4/14/19, 8:58 AM	admin	Accounts	Login	62.219.43.102	Mozilla/5.0,(Windows NT 10.0; Win6...	1920x1080
4/14/19, 8:58 AM	admin	Accounts	Login	62.219.43.102	Mozilla/5.0,(Windows NT 10.0; Win6...	1920x1080
4/14/19, 8:58 AM	<Anonymous Request>	Accounts	GetIdentitifyProviderDetails	62.219.43.102	Mozilla/5.0,(Windows NT 10.0; Win6...	
2/28/19, 10:57 AM	stefan	Accounts	Login	46.223.139.226	Mozilla/5.0,(Windows NT 10.0; Win6...	2560x1600
2/27/19, 8:46 PM	Admin	Investigator	GetInvestigatorData/	79.181.4.59	Mozilla/5.0,(Macintosh; Intel Mac O...	
2/27/19, 8:44 PM	Admin	Cases	GetWorkflowInstances	79.181.4.59	Mozilla/5.0,(Macintosh; Intel Mac O...	
2/27/19, 8:44 PM	Admin	Cases	GetWorkflowInstances	79.181.4.59	Mozilla/5.0,(Macintosh; Intel Mac O...	
2/27/19, 8:43 PM	Admin	Ide	GetIdeData	79.181.4.59	Mozilla/5.0,(Macintosh; Intel Mac O...	
2/27/19, 8:43 PM	Admin	Ide	GetIdeData	79.181.4.59	Mozilla/5.0,(Macintosh; Intel Mac O...	
2/27/19, 8:43 PM	Admin	Jobs	jobIdStr	79.181.4.59	Mozilla/5.0,(Macintosh; Intel Mac O...	
2/27/19, 8:43 PM	Admin	Jobs	jobIdStr	79.181.4.59	Mozilla/5.0,(Macintosh; Intel Mac O...	

10.3.3. General

In the General screen, you can define back up preferences, marketplace access credentials and organizational proxy for integrations.

- Generate ROI Report (SOC Managers only)
- Perform Backup
- Export Error Logs
- Configure Source Repository
- Define data retention
- Proxy
- LDAP Configuration



General

Define backup preferences, Marketplace access credentials and organizational proxy for integrations.

Backup

□ Enabled

Backup folder: /tmp

Username: Username

Password: Password

Daily backup hour (UTC): 0

Export Error Logs

Time Range: Last 15 minutes

Source Repository

Password: ••

Company: siemplify

Marketplace Name: SiemplifyMarketPlace

Data Retention

Default Period: 3 months

Proxy

Configure organizational proxy for accessing web resources.

Address: http://{IP}:{PORT}

□ Should use authentication

User Name

Password

Test Configuration

URLs/IPs to use without proxy

LDAP Configuration

Host *: ldaphost.com (default port is 389)

Admin DN *: cn=admin,dc=ldapserver,dc=com

Admin Password *: Admin account password

User Base DN *: dc=ldapserver,dc=com

□ TLS

□ Trust Certificate

User Attribute: Default Value: sAMAccountName

Group Attribute: The attribute that is used as the user gr

First Name Attribute: givenName

Last Name Attribute: sn

Email Attribute: mail

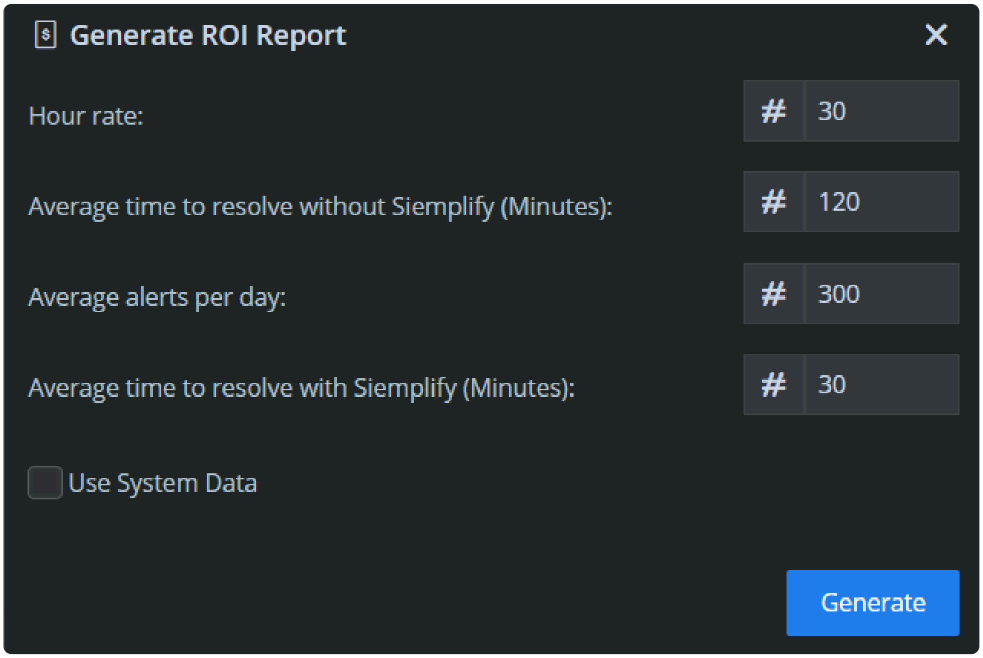
Activate Windows
Go to Settings to activate Windows.

Generate ROI Report

In this screen, you can calculate a report which shows the return on investment on using Siemplify.

Click on $.

Fill out the relevant information. Note that the hour rate refers to US dollars.



Generate ROI Report

Hour rate: # 30

Average time to resolve without Siemplify (Minutes): # 120

Average alerts per day: # 300

Average time to resolve with Siemplify (Minutes): # 30

□ Use System Data

Click Generate. A Word document showing the estimated savings when using Siemplify is downloaded to your desktop.

Perform Backup

You can perform the following options:

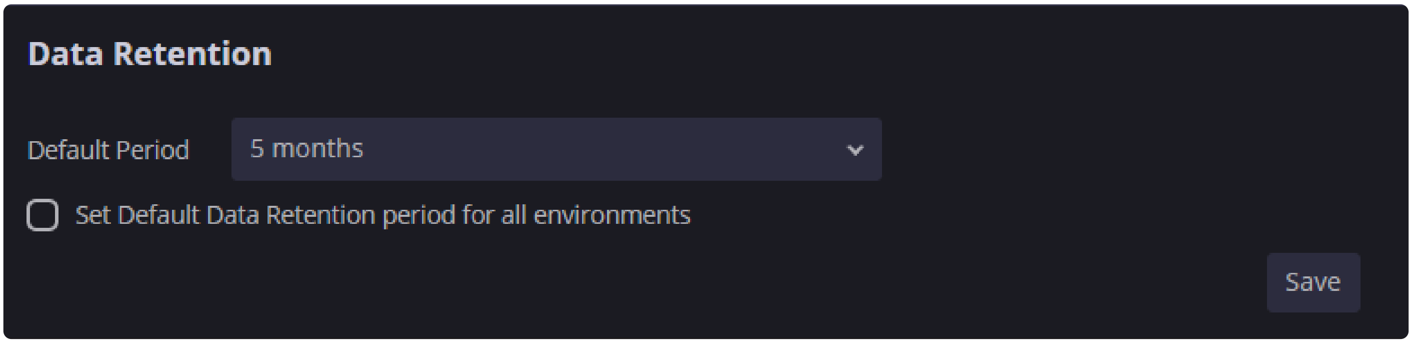
- Enable/Disable backup
- Specify Backup Folder (network pathway and folder name)
- Add username and password
- Specify the hour when backup should be performed
- Backup immediately instead of waiting for configured backup time.

Configure Source Repository

The source repository obtains the integration data, the actions, playbooks, and the rest of the items an analyst can download in Siemplify.
Add the password, company name and Marketplace name. You can test to check the source repository is valid. You can also update the Marketplace with new information.

Data Retention

In this section, you can define how long the system retains all information related to closed cases before deleting it. You can either choose to set this system-wide (i.e., for all environments) or per environment. If you select the per environment checkbox, make sure to navigate to the required environment/environments in the Organization > Environments screen, click Edit and select the required time frame. The maximum time frame is defined within the customer license. Customers who wish to extend the time frame should contact their Siemplify Account Manager. The minimum time frame is 3 months.



Data Retention

Default Period: 5 months

□ Set Default Data Retention period for all environments

Proxy

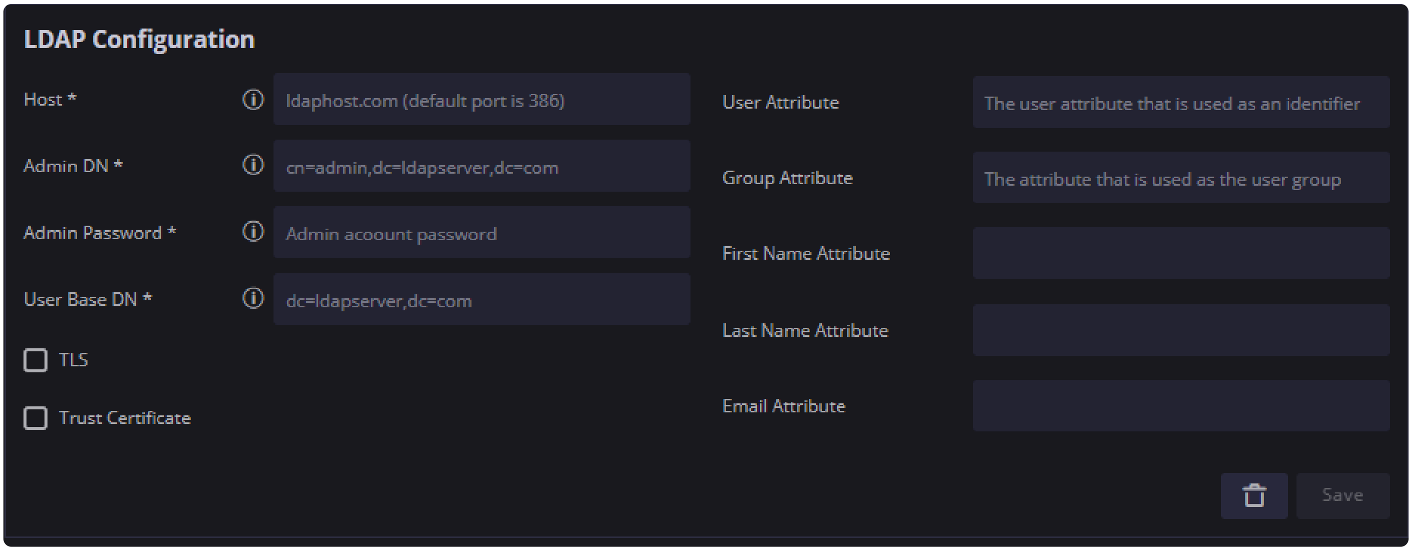
A Proxy is used for integrations that need information from outside the network or DMZ and want the security of a proxy.

In this section you can configure the proxy address, whether or not it should use authentication – as well as a valid user name and password.

You can add URLs or IP addresses that can be accessed without needing a proxy. Make sure to save all entered settings.

LDAP Configuration

Enter the parameters to enable you to authenticate LDAP users. For more information on LDAP, please refer to How To Configure LDAP



LDAP Configuration

Host * ⓘ ldaphost.com (default port is 386)

Admin DN * ⓘ cn=admin,dc=ldapserver,dc=com

Admin Password * ⓘ Admin acoount password

User Base DN * ⓘ dc=ldapserver,dc=com

□ TLS

□ Trust Certificate

User Attribute: The user attribute that is used as an identifier

Group Attribute: The attribute that is used as the user group

First Name Attribute

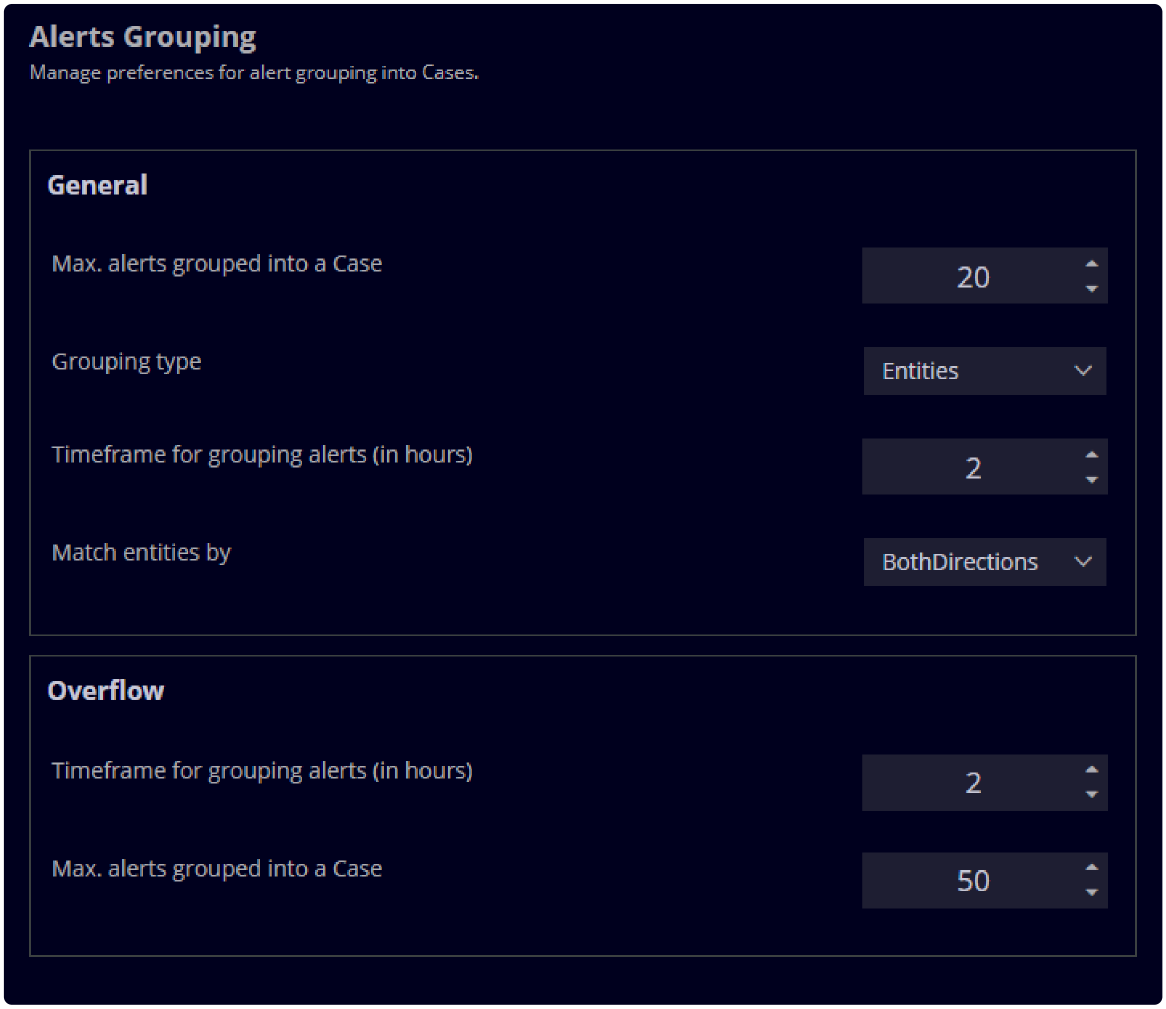
Last Name Attribute

Email Attribute

10.3.4. Alerts Grouping

In the Alerts Grouping screen, you can configure how alerts are grouped into cases.
This screen also allows you to define the Alerts Overflow configuration. The default configuration is more than 50 alerts in 10 minutes. Alerts Overflow mechanism was designed to prevent system overflow, when lots of alerts from the same environment, product and rule are occurring in a short period of time.
Once triggered, an Overflow case will be added to the case queue, with one alert indicating the environment, product and rule of the overflowing alert, and an Overflow tag.

Field	Description
General	
Max. alerts grouped into a Case	Define the maximum number of alerts to group together into one Case.
Grouping Type	Choose between Entities or SourceGroupingIdentifier (relevant for alerts coming from QRadar Connector – identifier called "offense".)
Timeframe for grouping alerts (in hours)	Choose the number of preceding hours with which to group the alerts for the Case.
Match Entities	Source Only, Destination Only or Both directions.
Overflow	
Timeframe for grouping alerts (in hours)	Choose the number of preceding hours with which to group the overflow alerts for the Case.
Max. alerts grouped into a Case	Define the maximum number of overflow alerts to group together into one Case.



Alerts Grouping

Manage preferences for alert grouping into Cases.

General

Max. alerts grouped into a Case: 20

Grouping type: Entities

Timeframe for grouping alerts (in hours): 2

Match entities by: BothDirections

Overflow

Timeframe for grouping alerts (in hours): 2

Max. alerts grouped into a Case: 50

10.3.5. External Authentication

> ✻ For customers with 5.1, this screen is viewable only and cannot be edited.

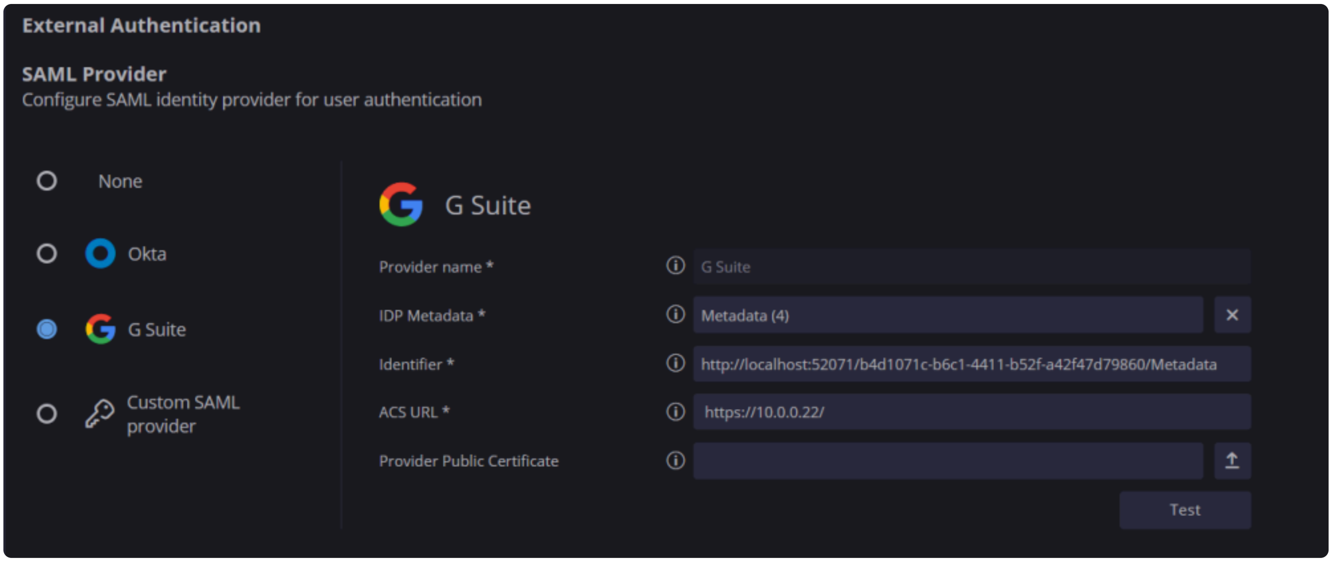
For more information, refer to SAML Configuration for G Suite
or SAML Configuration for Okta
or contact your Account Manager.

> ✻ For customers with 5.11 and higher, this screen is now configurable. See below for further details.

The External Authentication screen allows you to choose and configure the SAML provider that external users can access Siemplify with. Currently, the options are G-Suite, Okta or a Custom SAML provider.

To configure a SAML provider on the Siemplify platform:

1. Navigate to Settings > Advanced > External Authentication.
2. Select the required provider. For example, G Suite.
3. Fill out the following fields.
   a. Provider Name: G Suite (will be automatically populated)
   b. IDP Metadata: Upload file which defines the connection between Siemplify and the Custom provider.
   c. Identifier: URL of G Suite provider.
   d. ACS URL: Siemplify server name. Can be either an IP URL, Host Name URL or Local Host URL. Note that users have to connect to Siemplify with the same URL pattern configured in this field in order to log in with SAML.
   e. Provider public certificate: This is not needed for G Suite.
4. Click Save in the top right corner.
5. Restart the Server.
6. Click Test in order to make sure the connection is working as expected.



External Authentication

SAML Provider

Configure SAML identity provider for user authentication

○ None
○ Okta
● G Suite
○ Custom SAML provider

G Suite

Provider name *: G Suite
IDP Metadata *: Metadata (4)
Identifier *: http://localhost:52071/b4d1071c-b6c1-4411-b52f-a42f47d79860/Metadata
ACS URL *: https://10.0.0.22/
Provider Public Certificate:

The next stage is to add Users and assign them with this SAML provider. Note that if you are trying to change SAML providers, you need to disable each individual user first and then create new ones with the changed SAML provider.

10.3.6. Remote Agents

The Remote Agent is a lightweight agent installed at the end customer site which connects the customer

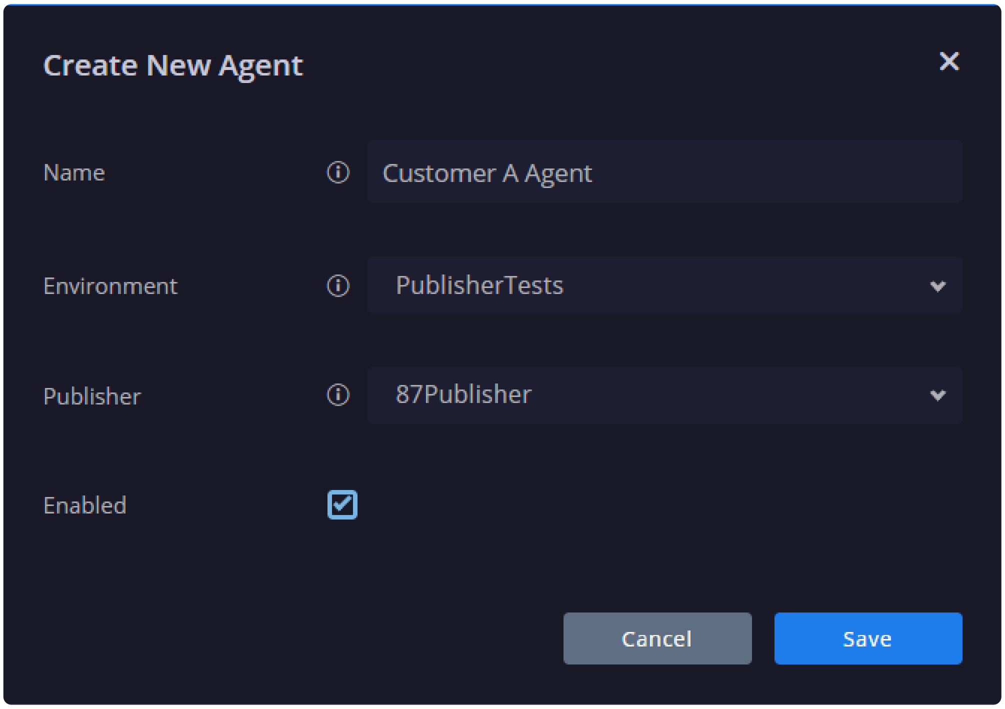
environment to the Siemplify platform.
The Agent enables the analyst to run actions, playbooks and connectors on remote customer sites directly from Siemplify.
In order for Siemplify to connect with the Agent, it pushes information to the Publisher which is a Proxy Server which usually resides in the Cloud. The Publisher has the information pulled from it by the Agent.

The following steps need to be taken in the correct order to set up the Remote Agent.

1. Deploy the Publisher. For full information refer to Siemplify Agent and Publisher Guide.
2. Pair the Publisher. In order to see this information, refer to the Publisher screen.
3. Create and Deploy New Agent. See below.
4. Set up Integration. Refer to Marketplace.
5. Set up Connectors. Refer to Marketplace.

To create a new agent:

1. In Settings > Advanced > Remote Agents, click the plus icon on the top right of the screen.
2. Fill out the relevant information: Name, Environment, Publisher and check **Is Enabled**.
3. A unique identifier is generated automatically for each customer.
4. A download link to install the Agent on the remote site will be created for each customer.
5. Click Save.



Create New Agent

Name: Customer A Agent

Environment: PublisherTests

Publisher: 87Publisher

Enabled ☑

6. Click **Send Now** in the main screen for the platform to send the defined user the link for them to install

the Agent.

Possible Agent Status Options:
Waiting for Agent: Only displays if it is a new agent and it is enabled. Status means it's waiting for the agent to be installed and perform initial communication with Siemplify.
Live: There is full communication from Agent to Publisher or from Siemplify to Publisher in last X minutes (where X is taken from Publisher pairing configuration)
Error: There was a problem with the communication from Agent to Publisher or from Siemplify to Publisher in last X minutes (where X is taken from Publisher pairing configuration)
Disabled: Will display if the agent is disabled
Stopped: Will display if the agent was stopped

Disable an Agent

To disable an agent:

1. Navigate to Settings > Advanced > Remote Agents.
2. Click Edit on the required agent.
3. Deselect the Enabled checkbox.
4. Click Save.
   Note that disabling an agent will stop any assigned integrations and connectors from running.

Stop an Agent

> ✻ Once you stop an agent, you cannot restart it.

To stop an agent:

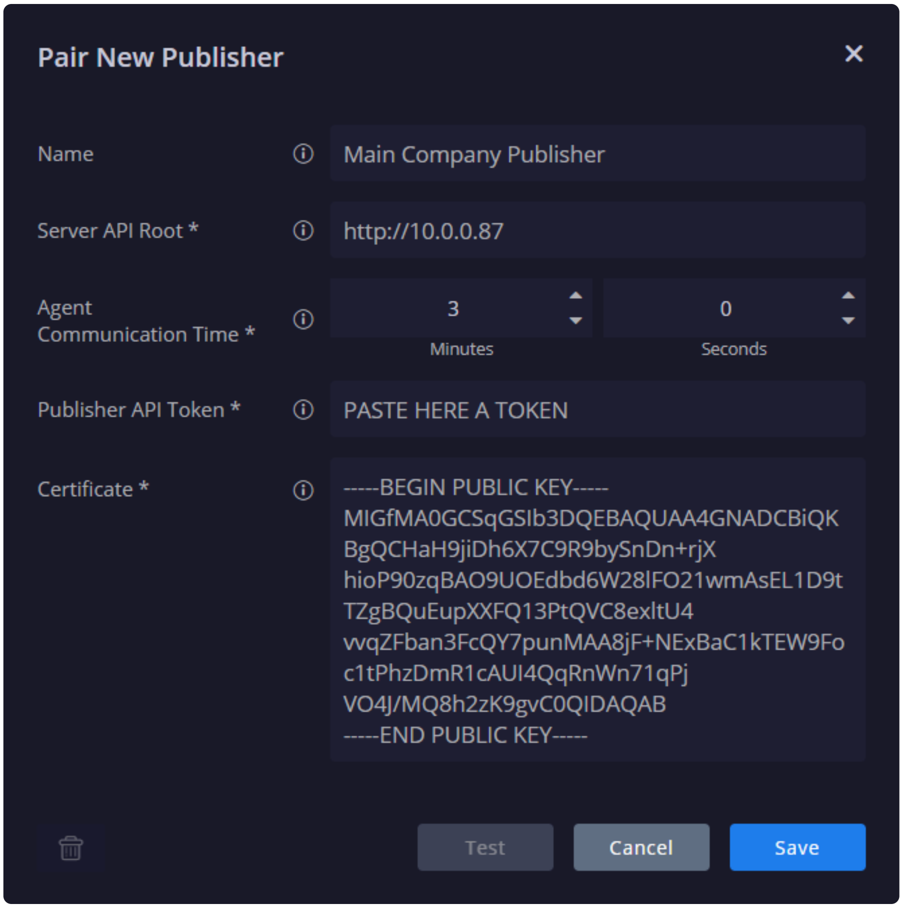
1. Navigate to Settings > Advanced > Remote Agents.
2. Click Edit on the required agent.
3. Click the red Stop Agent button.
4. Click Save.

10.3.7. Publisher

In the Publisher screen, you will pair a Publisher with the Siemplify instance.

To pair a publisher:

1. Click the plus icon on the top right of the screen.
2. Fill in the following information
   a. Name of Publisher
   b. Server API Root (Publisher Public Address)
   c. Agent Communication Time: This is the time threshold for receiving a ping from the Agents. Once this time is up, then the Status of the Agents will show as Error.
   d. Publisher API token: Created at deployment time.
   e. Certificate for encryption (Supplied by Siemplify)



Pair New Publisher

Name: Main Company Publisher

Server API Root *: http://10.0.0.87

Agent Communication Time *: 3 Minutes 0 Seconds

Publisher API Token *: PASTE HERE A TOKEN

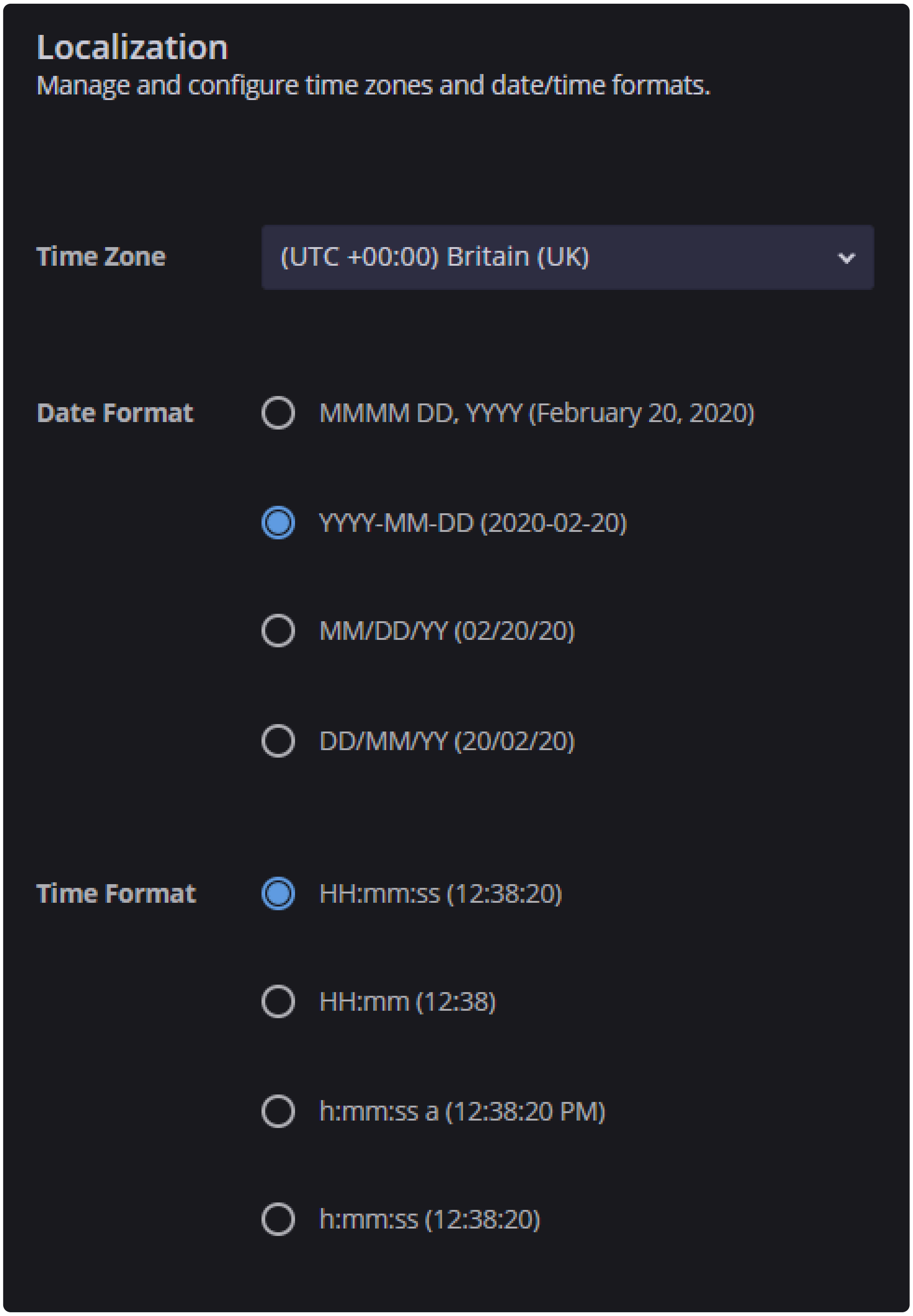
Certificate *:

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQK
BgQCHaH9jiDh6X7C9R9bySnDn+rjX
hioP90zqBAO9UOEdbd6W28lFO21wmAsEL1D9t
TZgBQuEupXXFQ13PtQVC8exltU4
vvqZFban3FcQY7punMAA8jF+NExBaC1kTEW9Fo
c1tPhzDmR1cAUI4QqRnWn71qPj
VO4J/MQ8h2zK9gvC0QIDAQAB
-----END PUBLIC KEY-----
```

Note that you can click on **View Publisher Logs** in the main Publishers management screen to view the logs in ElasticSearch. This can be useful if there is a Status error.
The next step is to create a Remote Agent. Refer to previous topic.

10.3.8. Localization

In this screen, you can set the time zone for your Platform, as well as how you want the date and time format to be displayed. The configuration is per user. Once saved, the changes take place immediately.



Localization

Manage and configure time zones and date/time formats.

Time Zone: (UTC +00:00) Britain (UK)

Date Format:

○ MMMM DD, YYYY (February 20, 2020)

● YYYY-MM-DD (2020-02-20)

○ MM/DD/YY (02/20/20)

○ DD/MM/YY (20/02/20)

Time Format:

● HH:mm:ss (12:38:20)

○ HH:mm (12:38)

○ h:mm:ss a (12:38:20 PM)

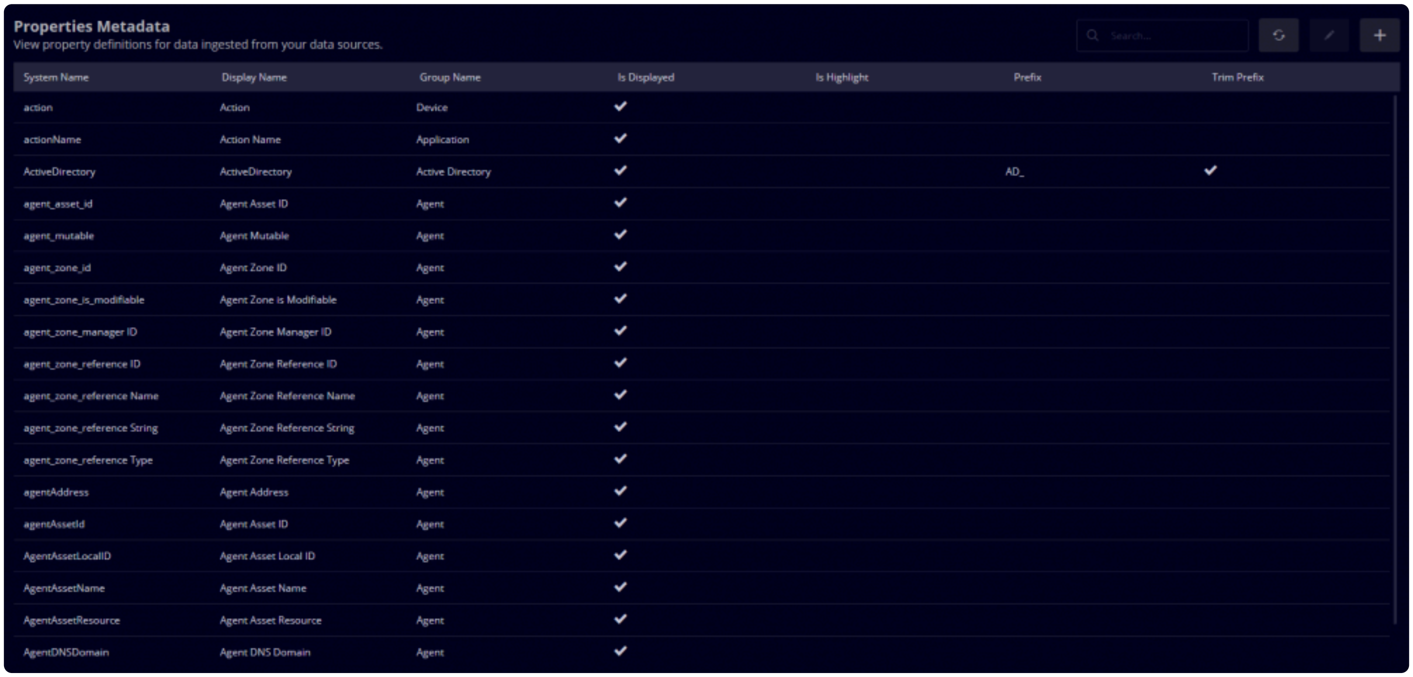
○ h:mm:ss (12:38:20)

10.4. Data Configuration

Properties Metadata
Statistics

10.4.1. Properties Metadata

In this screen you can add, modify, and delete metadata properties. The properties metadata map which event fields are located under which headings in the Context Details screen.

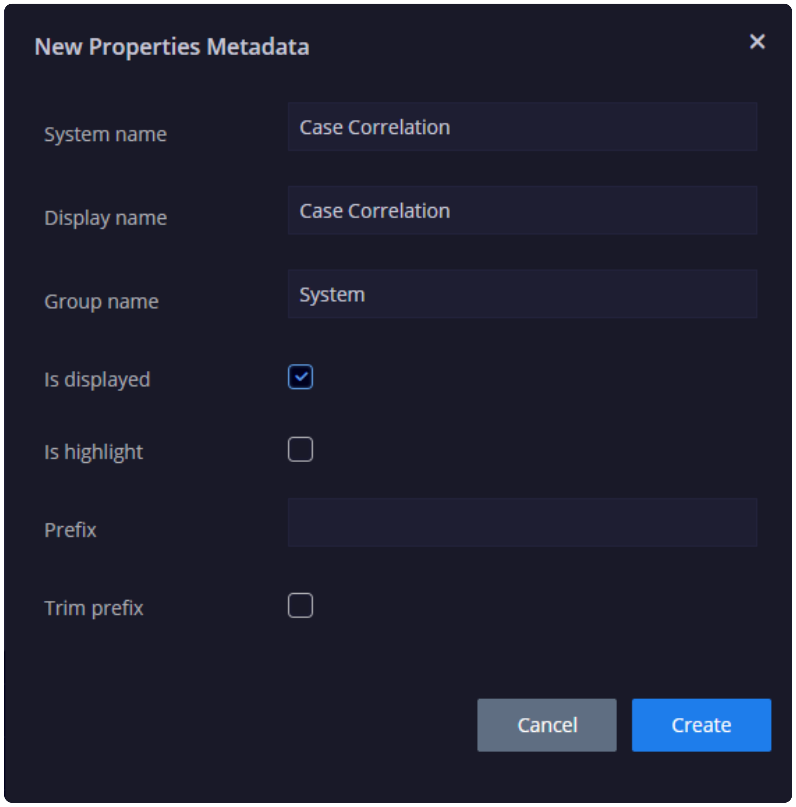


Properties Metadata
View property definitions for data ingested from your data sources.

System Name	Display Name	Group Name	Is Displayed	Is Highlight	Prefix	Trim Prefix
action	Action	Device	✓			
actionName	Action Name	Application	✓			
ActiveDirectory	ActiveDirectory	Active Directory	✓		AD_	✓
agent_asset_id	Agent Asset ID	Agent	✓			
agent_mutable	Agent Mutable	Agent	✓			
agent_zone_id	Agent Zone ID	Agent	✓			
agent_zone_is_modifiable	Agent Zone is Modifiable	Agent	✓			
agent_zone_manager ID	Agent Zone Manager ID	Agent	✓			
agent_zone_reference ID	Agent Zone Reference ID	Agent	✓			
agent_zone_reference Name	Agent Zone Reference Name	Agent	✓			
agent_zone_reference String	Agent Zone Reference String	Agent	✓			
agent_zone_reference Type	Agent Zone Reference Type	Agent	✓			
agentAddress	Agent Address	Agent	✓			
agentAssetId	Agent Asset ID	Agent	✓			
AgentAssetLocalID	Agent Asset Local ID	Agent	✓			
AgentAssetName	Agent Asset Name	Agent	✓			
AgentAssetResource	Agent Asset Resource	Agent	✓			
AgentDNSDomain	Agent DNS Domain	Agent	✓			

To add a property:

1. Click the plus icon on the top right of the screen.
2. Add in the relevant information.



New Properties Metadata

System name: Case Correlation

Display name: Case Correlation

Group name: System

Is displayed ☑

Is highlight □

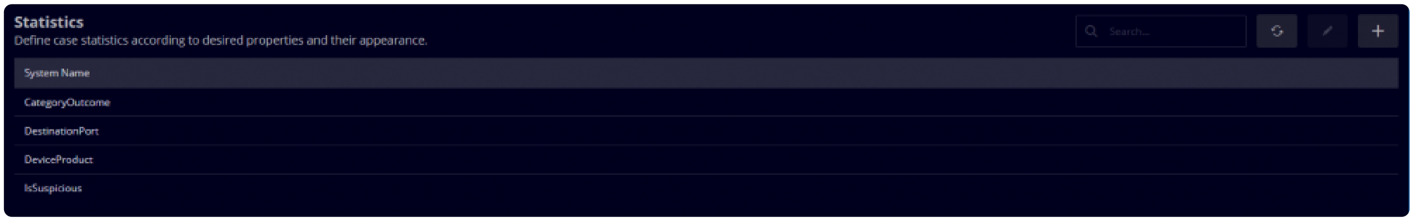
Prefix:

Trim prefix □

3. Click Create.

10.4.2. Statistics

In the Statistics screen, you can define the statistics that you want to display in the case Context Details pane in the case management screen.



Statistics

Define case statistics according to desired properties and their appearance.

System Name
CategoryOutcome
DestinationPort
DeviceProduct
IsSuspicious

10.5. Ontology

[Ontology Overview](#)
[Ontology Status](#)
[Visual Family](#)

10.5.1. Ontology Overview

Siemplify ontology provides a formal specification that provides a shareable and reusable knowledgeable representation of alerts and events that will be consumed. The ontology allows Siemplify to build entities out of events and define relationships between them. This enables the user to see the full “picture” and gives them the ability to explore potential threats via the Explore Cases screen. Once entities have been defined using the ontology, you can run actions on them based on their role in the attack or event.

After you have established an initial data connection, you will need to complete the following procedures to ensure that the data is ingested into the Siemplify data model. You will also need to map and model new events and alerts according to your requirements and as your connectors pick up new events.

Set up Model families:

Step One: Define family in Settings > Ontology > Visual Families.

Step Two: Assign the family to the Event (or Product/Source) in the Event Configuration > Visualization screen. This screen can be reached by clicking the Configure icon either on the Events tab or on the Ontology Status screen.

Map Data Fields:

Step One: Using the Case Management and/or Explore screen, identify missing or incorrect field information.

Step Two: Check if this can be solved by attaching a new Visual Family.

Step Three: Otherwise, edit and configure the rules that make up both the Family and the general System fields in the Event Configuration > Mapping screen.

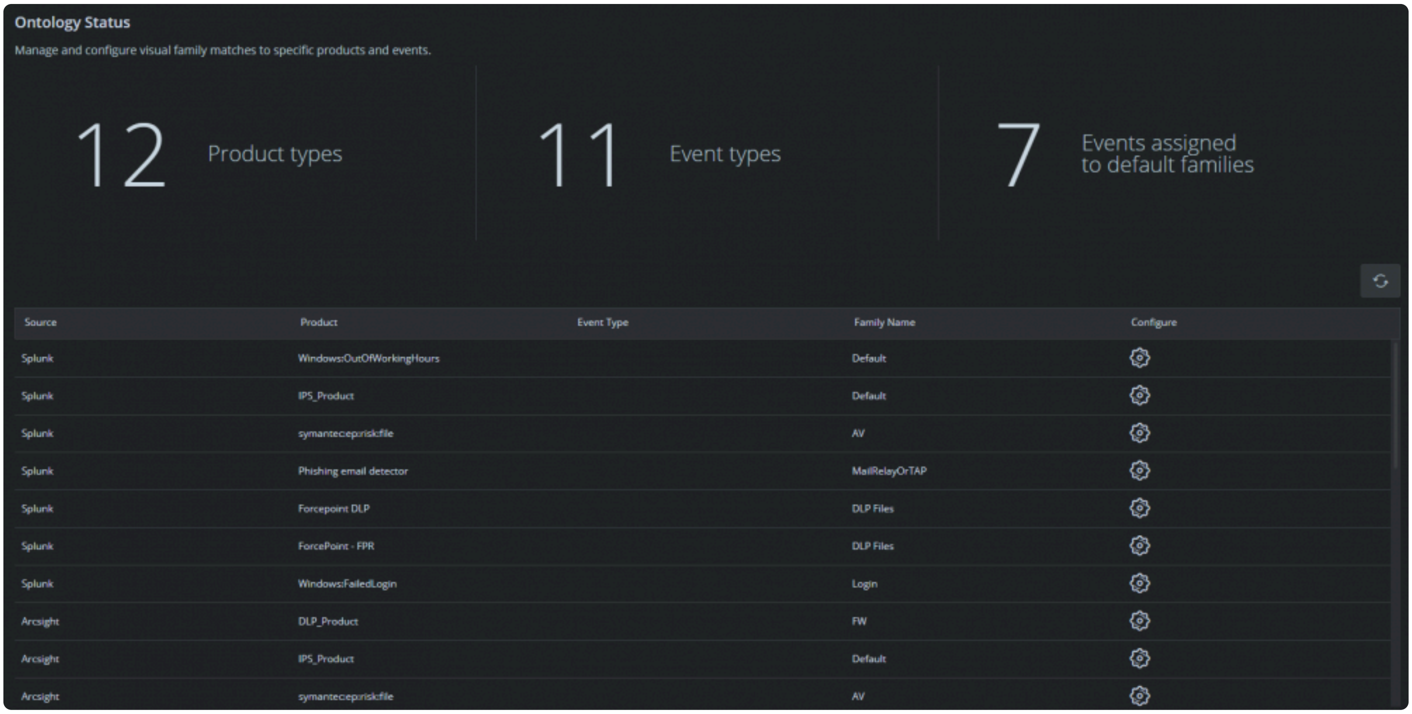
10.5.2. Ontology Status

The Ontology status screen displays the following information:

Number of Product Types: This is the number of products that are captured by Siemplify from your environment. This number is in flux as more products are added to your environments.
Number of Events Types: This is the number of events that are captured by Siemplify from your environment.

Number of Events assigned to Default Families: This is the number of events that have been automatically assigned by Siemplify to default families. At any stage, you can look in the Family Name column for Default, click the Configure icon and assign them to a different model family.

To change the Model family or the field Mapping, click on the Configure icon. Refer to Event Configuration for full details.



Ontology Status

Manage and configure visual family matches to specific products and events.

12 Product types

11 Event types

7 Events assigned to default families

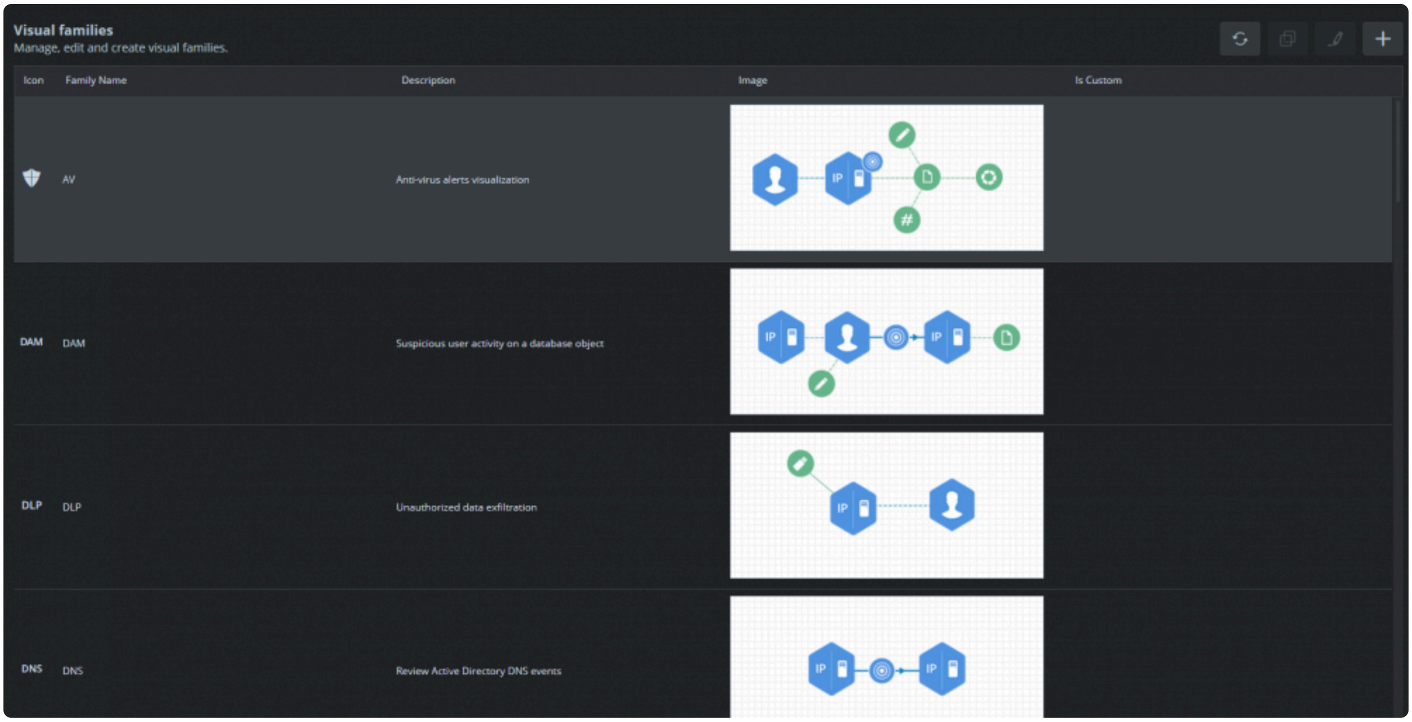
Source	Product	Event Type	Family Name	Configure
Splunk	Windows:OutOfWorkingHours		Default	⚙
Splunk	IPS_Product		Default	⚙
Splunk	symantec:ep:risk:file		AV	⚙
Splunk	Phishing email detector		MailRelayOrTAP	⚙
Splunk	Forcepoint DLP		DLP Files	⚙
Splunk	ForcePoint - FPR		DLP Files	⚙
Splunk	Windows:FailedLogin		Login	⚙
Arcsight	DLP_Product		FW	⚙
Arcsight	IPS_Product		Default	⚙
Arcsight	symantec:ep:risk:file		AV	⚙

10.5.3. Visual Families

Visual families specify the relationship between the entities and protagonists from the third-party applications.

The family is attached to a specific event / product in the Event Configuration > Visualization screen. The family is then displayed in the Explore Cases screen for each event, product or source so that the analyst can see who did what and when.

The Visual Families screen is where you can configure the family's fields and relationships.



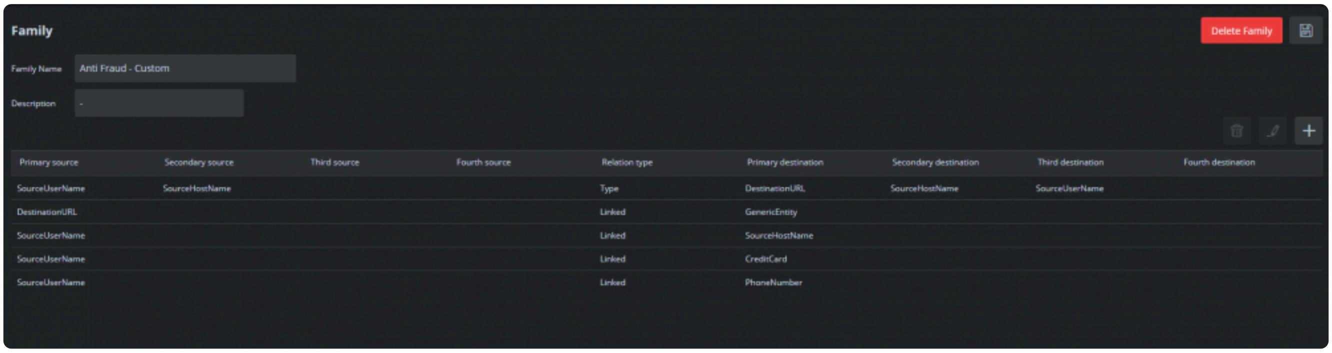
Visual families

Manage, edit and create visual families.

Icon	Family Name	Description	Image	Is Custom
	AV	Anti-virus alerts visualization		
DAM	DAM	Suspicious user activity on a database object		
DLP	DLP	Unauthorized data exfiltration		
DNS	DNS	Review Active Directory DNS events		

To clone or create a visual family:

1. Navigate to Settings > Ontology > Visual Families.
2. Either select one of the existing visual families and click the Duplicate icon on the top right. (Or select the plus icon and create a new family from scratch).



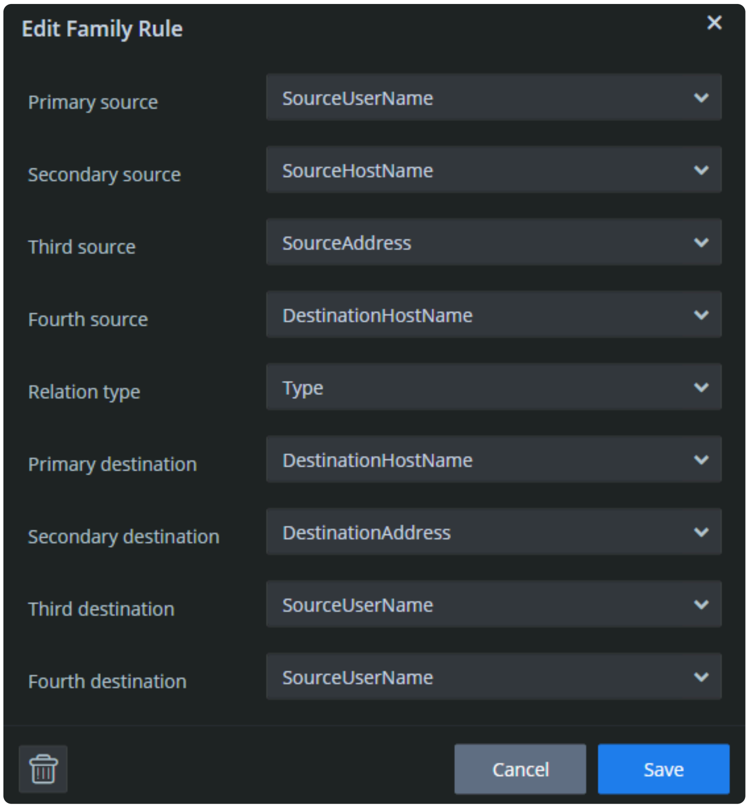
Family

Family Name: Anti Fraud - Custom

Description: -

Primary source	Secondary source	Third source	Fourth source	Relation type	Primary destination	Secondary destination	Third destination	Fourth destination
SourceUserName	SourceHostName			Type	DestinationURL	SourceHostName	SourceUserName	
DestinationURL				Linked	GenericEntity			
SourceUserName				Linked	SourceHostName			
SourceUserName				Linked	CreditCard			
SourceUserName				Linked	PhoneNumber			

3. In the Family Rules screen that opens, edit the relevant information by either selecting a row and clicking on Edit icon. Or click on the plus icon to add a new family rule.
4. Enter the relevant information. Primary to Fourth Source of where to take the Information and the Primary to Fourth Destination in Siemplify to send it to. Relation Type: Type (action) or Linked (connection). An action is when one entity does something to another entity (user sends an email). A connection simply means the two entities are related (user and the machine's host name). In the Explore screen, the Type (action) is denoted by an arrow and Linked (connection) is denoted by a dotted line.



Edit Family Rule

Primary source: SourceUserName

Secondary source: SourceHostName

Third source: SourceAddress

Fourth source: DestinationHostName

Relation type: Type

Primary destination: DestinationHostName

Secondary destination: DestinationAddress

Third destination: SourceUserName

Fourth destination: SourceUserName

5. Click Save.
6. Make sure to click the Save icon the top right of the screen before exiting this screen!

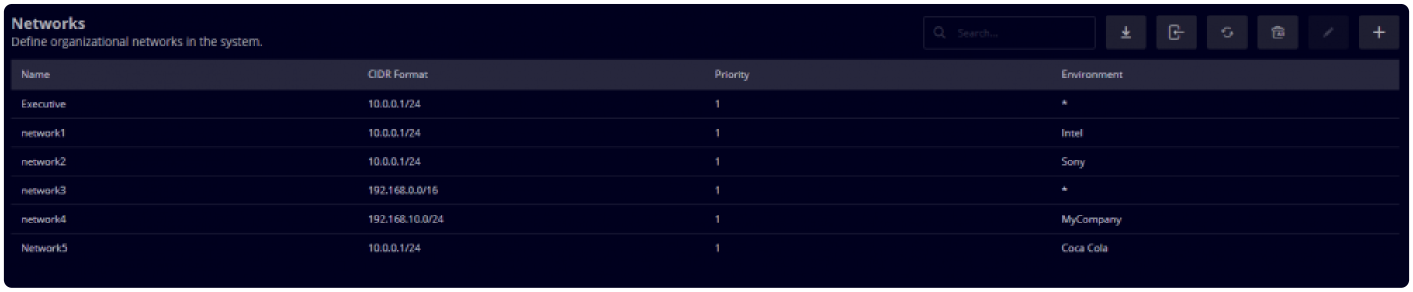
10.6. Environments

Networks
Domains
Custom Lists
Email Templates
Email HTML Templates
Black items

10.6.1. Networks

In the Networks screen, you can add, modify and delete networks in a CIDR format. The system supports identification of network subnets. The network names will be displayed in Cases and Reports for readability. For example, an entity with an IP address that was set, will appear as an Internal Entity in the Cases screen, and will have the ‘isInternal:True’ field in its context details. The option to export and import multiple networks is supported using the Export/Import buttons.

You can also choose to download a template, use this format to add networks and then import the information back in. This can be useful if you are a new Siemplify customer and want to import existing information into the platform.



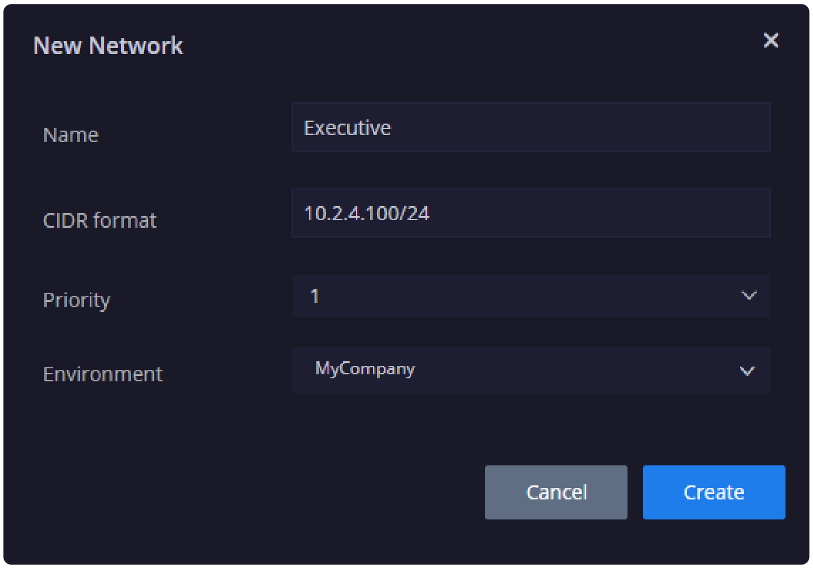
Networks

Define organizational networks in the system.

Name	CIDR Format	Priority	Environment
Executive	10.0.0.1/24	1	*
network1	10.0.0.1/24	1	Intel
network2	10.0.0.1/24	1	Sony
network3	192.168.0.0/16	1	*
network4	192.168.10.0/24	1	MyCompany
Network5	10.0.0.1/24	1	Coca Cola

To add a new network:

1. Click the plus icon on the top right of the screen.
2. In the New Network dialog box add in the relevant information. The Priority decides the order of the networks. If an entity fits several ranges, it will select the top priority one.



New Network

Name: Executive

CIDR format: 10.2.4.100/24

Priority: 1

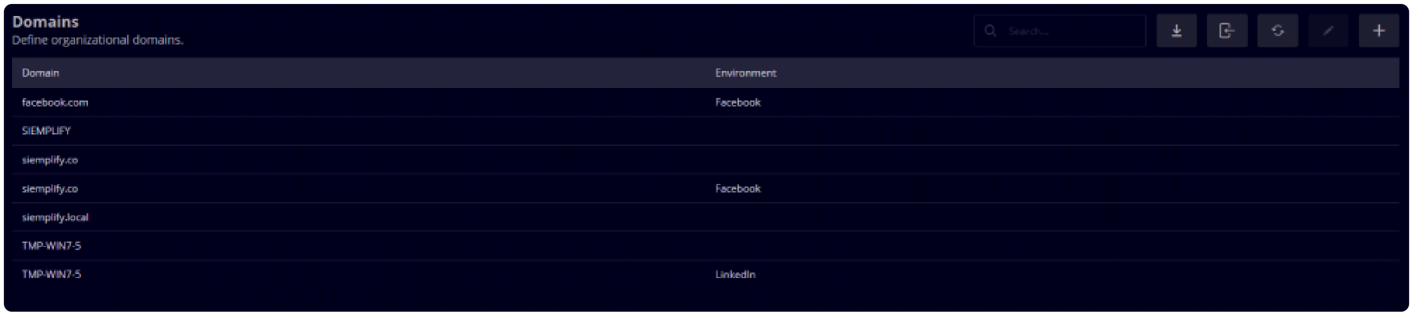
Environment: MyCompany

3. Click Create.

Users can add sub-networks with smaller ranges. The entity will match against the smallest network that fits.

10.6.2. Domains

In the Domain screen, you can define internal domains for your customers which then enables agents to identify the internal entities that are users.
This is especially relevant for MSSPs and their customers. The option to export and import multiple networks is supported using the Export/Import buttons. In this screen, you can also choose to download a template, use this format to add domains and then import the information back in. This can be useful if you are a new Siemplify customer and want to import existing information into the platform.

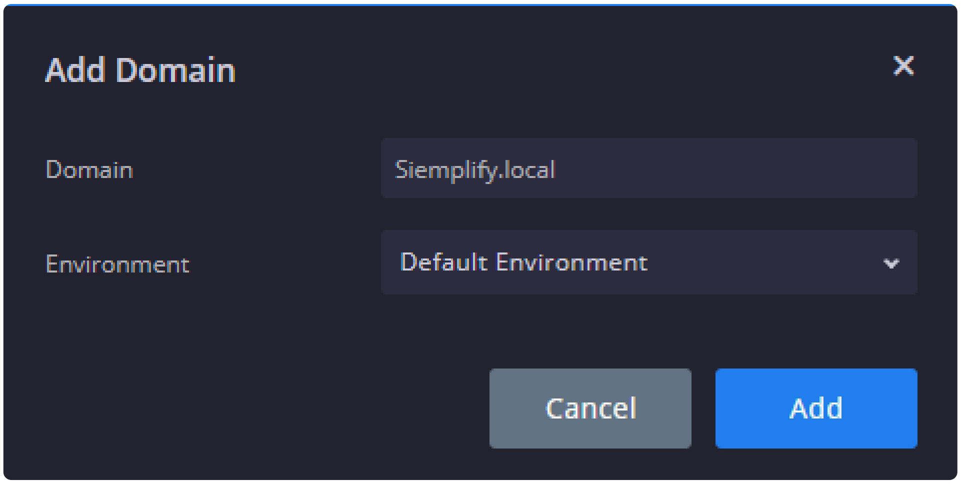


Domains
Define organizational domains.

Domain	Environment
facebook.com	Facebook
SIEMPLIFY	
siemplify.co	
siemplify.co	Facebook
siemplify.local	
TMP-WIN7-5	
TMP-WIN7-5	LinkedIn

To add a new domain:

1. Click the plus icon on the top right of the screen.
2. Enter the relevant information into the the New Internal Domain dialog box.



Add Domain

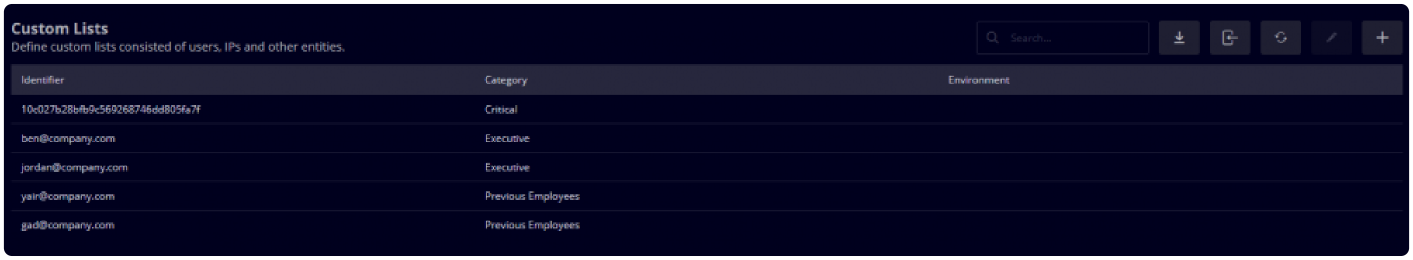
Domain: Siemplify.local

Environment: Default Environment

3. Click Create.

10.6.3. Custom Lists

In the Custom Lists screen you can define lists of special interest, for example, hosts holding confidential information or users who have come under suspicion. These custom lists can be selected as triggers for Playbooks. The option to export and import multiple networks is supported using the Export/Import buttons. You can also choose to download a template, use this format to add lists (categories) and then import the information back in. This can be useful if you are a new Siemplify customer and want to import existing information into the platform.



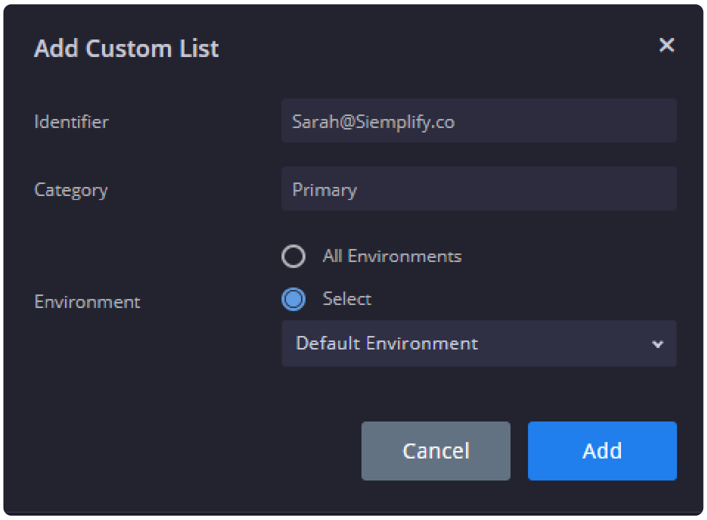
Custom Lists

Define custom lists consisted of users, IPs and other entities.

Identifier	Category	Environment
10c027b28bfb9c569268746dd805fa7f	Critical	
ben@company.com	Executive	
jordan@company.com	Executive	
yair@company.com	Previous Employees	
gad@company.com	Previous Employees	

To add a new custom list:

1. Click the plus icon on the top right of the screen.
2. Enter the relevant information into the New Custom List dialog box. Note that Category has a fixed search result but can be modified in the template.



Add Custom List

Identifier: Sarah@Siemplify.co

Category: Primary

Environment: ○ All Environments ● Select

Default Environment

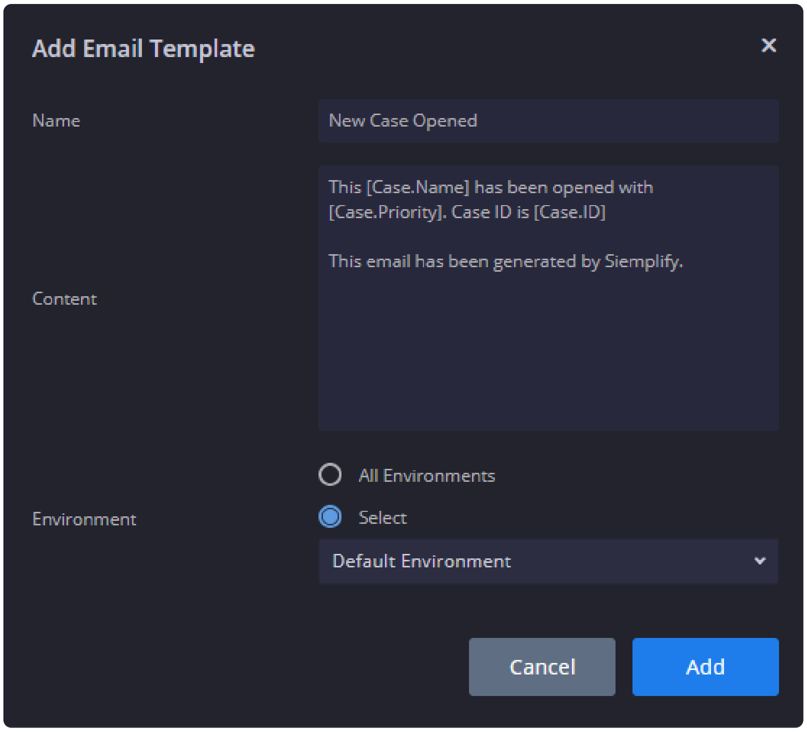
3. Click Create.

10.6.4. Email Templates

In the Email Templates screen, you can define templates for recurring emails, so that they can be sent by scripts and can be also sent automatically with playbooks.

To create a new email template:

1. Click the plus icon on the top right of the screen.
2. Enter in the Email message as well as name and environment. Note that this email template is capable of extracting information from cases/events/insights/entities and more that are available in the Siemplify case using the Placeholder. In this picture, you can see “Case.Name” inside square brackets, which will get the name of the case in which the email action is taken.



Add Email Template

Name: New Case Opened

Content:

This [Case.Name] has been opened with [Case.Priority]. Case ID is [Case.ID]

This email has been generated by Siemplify.

Environment:
○ All Environments
● Select
Default Environment

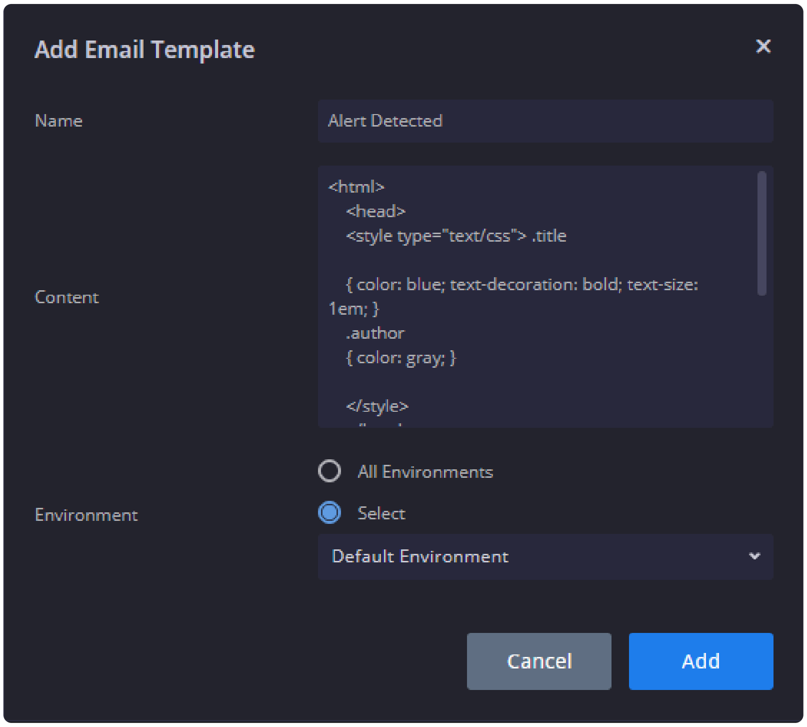
3. Click Create.

10.6.5. Email HTML Templates

In the Email HTML Templates screen, you can define HTML templates for recurring emails, so that they can be sent by scripts.

To create a new HTML email template:

1. Click the plus icon on the top right of the screen.
2. Edit the HTML information making sure to add in the required body text.



Add Email Template

Name: Alert Detected

Content:

```
<html>
   <head>
   <style type="text/css"> .title

   { color: blue; text-decoration: bold; text-size:
1em; }
   .author
   { color: gray; }

   </style>
```

Environment: ○ All Environments ● Select

Default Environment

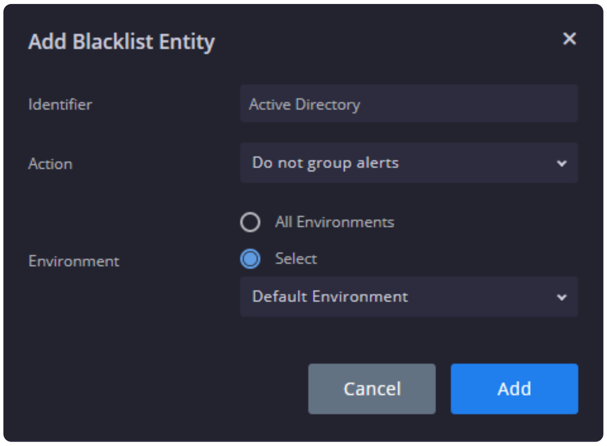
3. Click Create.

10.6.6. Blacklist

In the Blacklist screen you can create a black list of items. These are composed of entities that the system will not group alerts by or entitles which should not be displayed in the system.

To add a new blacklist item:

1. Click the plus icon on the top right of the screen.
2. Enter in the relevant information.



Add Blacklist Entity

Identifier: Active Directory

Action: Do not group alerts

Environment: ○ All Environments ● Select

Default Environment

3. Click Create.

11. Connectors

For detailed information on adding specific Connectors please refer to Integrations and Connector Guides Portal

12. Jobs

The Jobs screen contains default Siemplify jobs, as well as jobs that are created in the IDE screen and are essentially scripts that can be scheduled to run periodically.

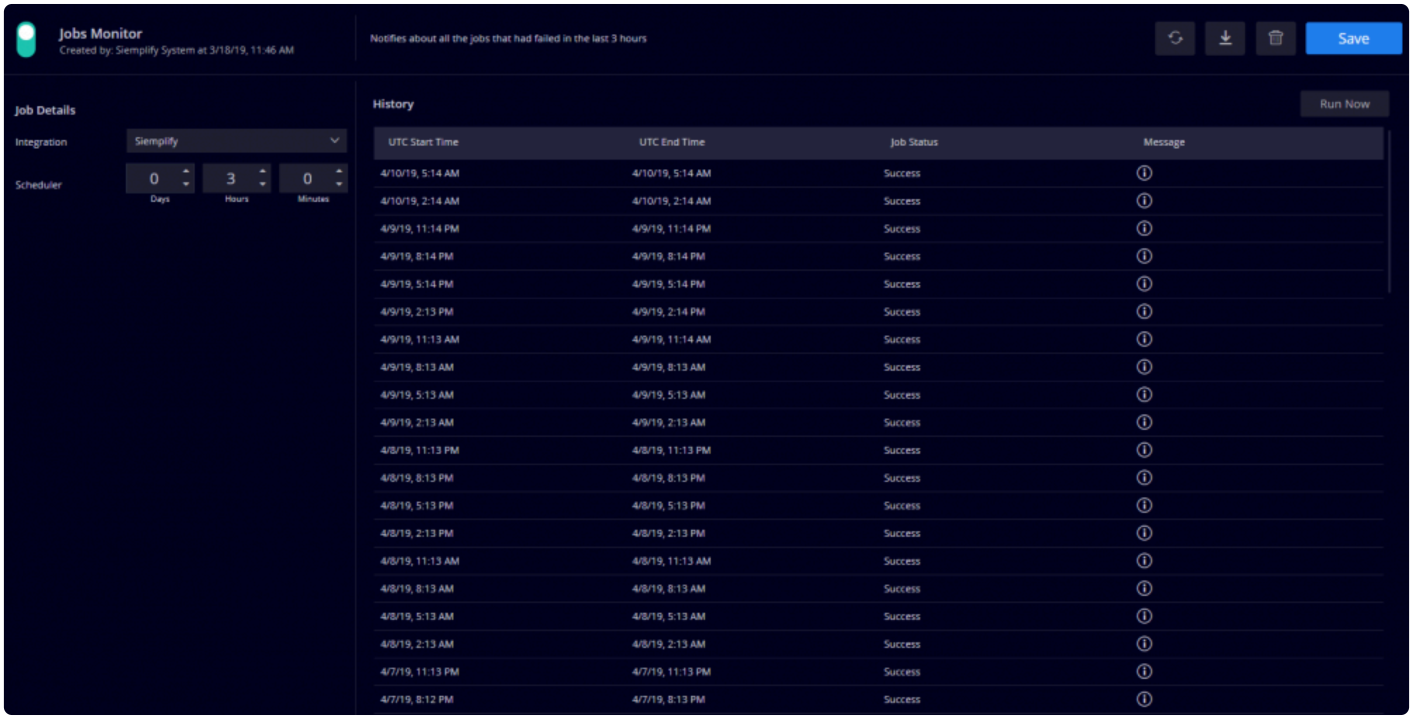
The following predefined jobs are available:

✻ These Jobs will work only after configuring the Siemplify integration in the Marketplace!

Option	Description
Actions Monitor	Notifies if a specific action has failed at least 3 times, across all cases it was performed in (to a predefined email, as set in the Siemplify integration configuration in Marketplace.)
Connectors Monitor	Notifies regarding any Connectors error in the alert ingestion process
Machine Resource Utilization	Notifies if the machine resource utilization is close to full usage, according to the following default rules: CPU – over 90% MEM – over 85% Drive – over 80%
ETL	Notifies regarding any error in the ETL alert ingestion process
Jobs Monitor	Notifies if a specific job has failed at least 3 times (sends a notification for each specific job once every 3 hours)

To configure a new job:

1. First, create the Job in the IDE screen. Refer to the IDE screen for more details.
2. Navigate to Settings > Jobs.
3. Select the plus icon.
4. Select the job you created in the IDE screen and click Create.
5. Enter the Scheduler information for when the script should run.
6. Make sure to click Save.
7. You can also choose to run the script immediately by clicking Run Now.



Jobs Monitor
Created by: Siemplify System at 3/18/19, 11:46 AM

Notifies about all the jobs that had failed in the last 3 hours

Job Details

Integration: Siemplify

Scheduler: 0 Days, 3 Hours, 0 Minutes

History

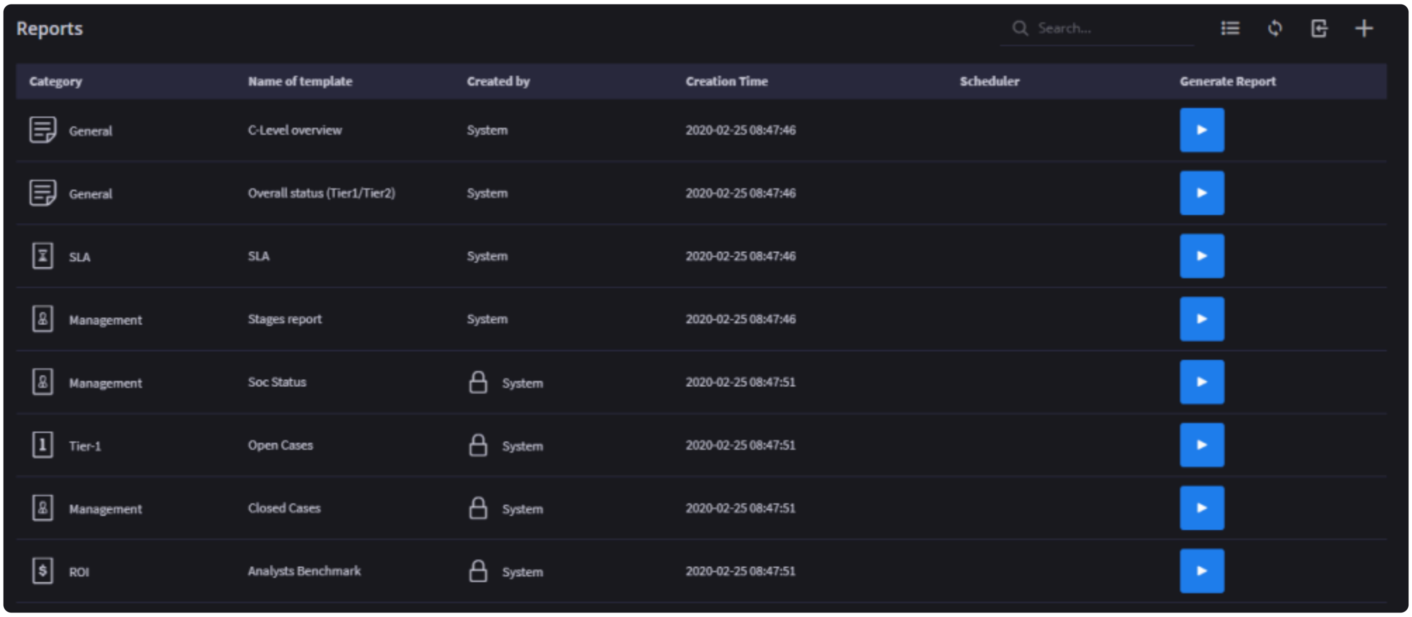
UTC Start Time	UTC End Time	Job Status	Message
4/10/19, 5:14 AM	4/10/19, 5:14 AM	Success	ⓘ
4/10/19, 2:14 AM	4/10/19, 2:14 AM	Success	ⓘ
4/9/19, 11:14 PM	4/9/19, 11:14 PM	Success	ⓘ
4/9/19, 8:14 PM	4/9/19, 8:14 PM	Success	ⓘ
4/9/19, 5:14 PM	4/9/19, 5:14 PM	Success	ⓘ
4/9/19, 2:13 PM	4/9/19, 2:14 PM	Success	ⓘ
4/9/19, 11:13 AM	4/9/19, 11:14 AM	Success	ⓘ
4/9/19, 8:13 AM	4/9/19, 8:13 AM	Success	ⓘ
4/9/19, 5:13 AM	4/9/19, 5:13 AM	Success	ⓘ
4/9/19, 2:13 AM	4/9/19, 2:13 AM	Success	ⓘ
4/8/19, 11:13 PM	4/8/19, 11:13 PM	Success	ⓘ
4/8/19, 8:13 PM	4/8/19, 8:13 PM	Success	ⓘ
4/8/19, 5:13 PM	4/8/19, 5:13 PM	Success	ⓘ
4/8/19, 2:13 PM	4/8/19, 2:13 PM	Success	ⓘ
4/8/19, 11:13 AM	4/8/19, 11:13 AM	Success	ⓘ
4/8/19, 8:13 AM	4/8/19, 8:13 AM	Success	ⓘ
4/8/19, 5:13 AM	4/8/19, 5:13 AM	Success	ⓘ
4/8/19, 2:13 AM	4/8/19, 2:13 AM	Success	ⓘ
4/7/19, 11:13 PM	4/7/19, 11:13 PM	Success	ⓘ
4/7/19, 8:12 PM	4/7/19, 8:13 PM	Success	ⓘ

13. Reports

Reports come in useful to justify Return on Investment (ROI) to upper management and to achieve transparency and accountability to customers and fellow colleagues. Siemplify provides analysts with four predefined Reports and the option to create new ones. You can export and import Reports to other platforms.

The predefined Reports are:

- Management – SOC status
- Management – Closed Cases
- Tier 1 – Open Cases
- ROI – Analysts Benchmark

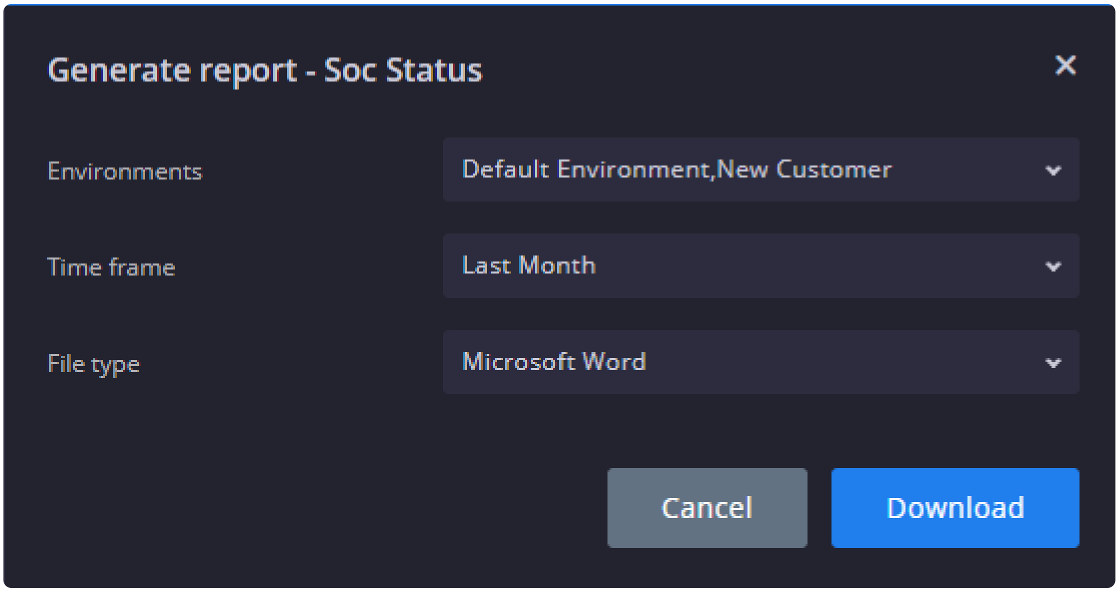


Reports

Category	Name of template	Created by	Creation Time	Scheduler	Generate Report
General	C-Level overview	System	2020-02-25 08:47:46		▶
General	Overall status (Tier1/Tier2)	System	2020-02-25 08:47:46		▶
SLA	SLA	System	2020-02-25 08:47:46		▶
Management	Stages report	System	2020-02-25 08:47:46		▶
Management	Soc Status	🔒 System	2020-02-25 08:47:51		▶
Tier-1	Open Cases	🔒 System	2020-02-25 08:47:51		▶
Management	Closed Cases	🔒 System	2020-02-25 08:47:51		▶
ROI	Analysts Benchmark	🔒 System	2020-02-25 08:47:51		▶

To generate a Report:

1. Click the play button under the Generate Report column.
2. In the dialog box, select the required environments to be included in the Report, Time Frame and the document type (Word or PDF).
3. Click Download.



Generate report - Soc Status

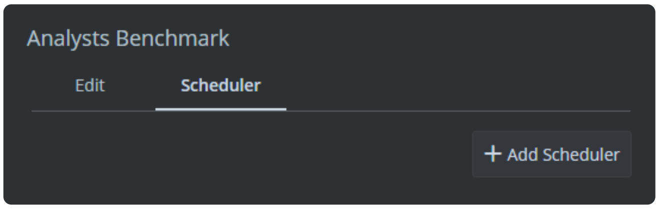
Environments: Default Environment,New Customer

Time frame: Last Month

File type: Microsoft Word

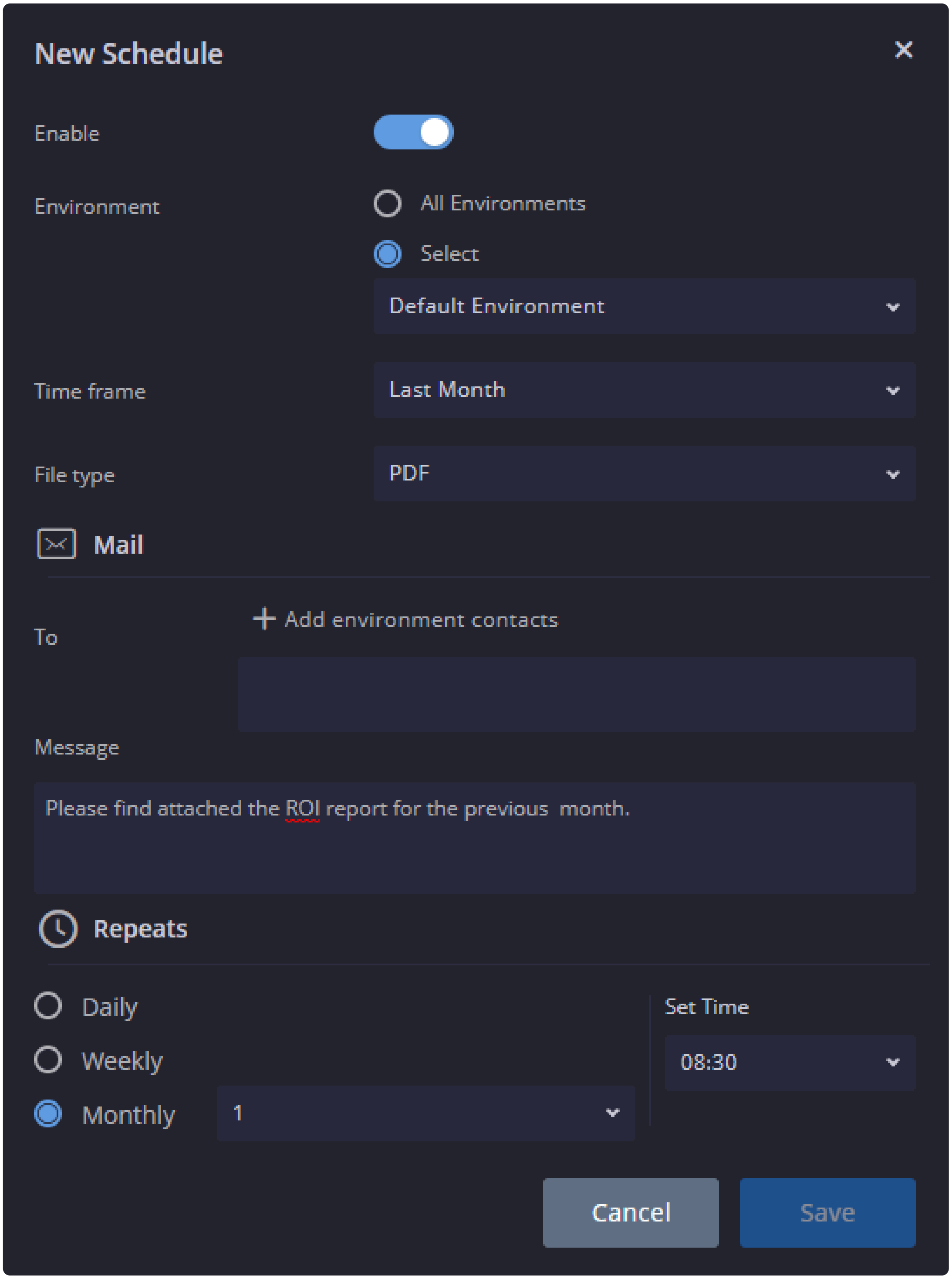
To schedule a Report:

1. Select the required report.
2. In the right of the screen, select the Scheduler.



Analysts Benchmark

3. Click on Add Scheduler.
4. Enter the relevant information.



New Schedule

Enable: On

Environment: ○ All Environments ● Select

Default Environment

Time frame: Last Month

File type: PDF

Mail

To

Message: Please find attached the ROI report for the previous month.

Repeats

○ Daily

○ Weekly

● Monthly 1

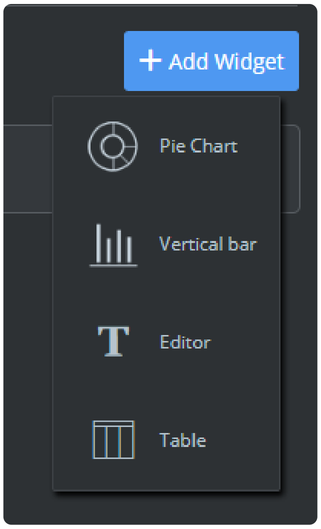
Set Time: 08:30

5. Click Save.

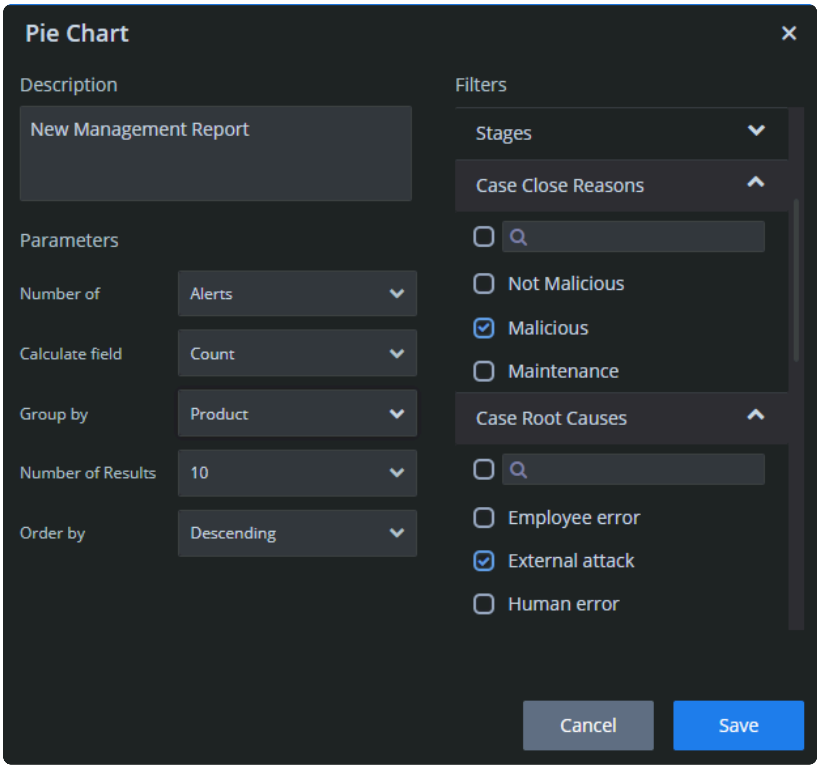
To add a new Report:

1. Click the plus icon on the top of the screen and add name of the new Report.

2. Note that you can also duplicate an existing Report and edit as required.
3. Click Create. The Report appears in the list of Reports.
4. Select this Report and in the right pane in the screen, click Edit.
5. Click Add Widget and choose one of the following formats: Pie Chart, Vertical Bar, Editor or Table.



6. Depending on what format you choose, a different dialog box will open. For this procedure, let's choose a Pie Chart.
7. Enter the relevant information. Note that whether you choose Alert or Cases will affect the options in the other fields.
8. In this procedure, we have created a Report based on Alerts coming from Products whereby the case was closed as malicious and the root cause was an External Attack.



Pie Chart

Description

New Management Report

Parameters

Number of	Alerts
Calculate field	Count
Group by	Product
Number of Results	10
Order by	Descending

Filters

Stages

Case Close Reasons

□ Not Malicious

☑ Malicious

□ Maintenance

Case Root Causes

□ Employee error

☑ External attack

□ Human error

9. Click Save.