



Siemplify

Quick Start Guide

Table of Contents

- 1. Siemplify Overview..... 1
- 2. Install Siemplify 2
 - 2.1. Download Siemplify 3
 - 2.2. Deployment Prerequisites 4
 - 2.3. Deploy With OVA 5
 - 2.4. Deploy With Installer 8
 - 2.5. Open Siemplify Client..... 9
- 3. Start Working in Siemplify 11
 - 3.1. Run Use Cases 12
 - 3.2. Ingest Your Data (Connectors) 18
 - 3.3. Create Entities (Mapping & Modelling) 20
 - 3.4. Configure Integrations 24
 - 3.5. Create and Run a Playbook 26
 - 3.6. Manage Cases 32

1. Siemplify Overview

Siemplify is the leader in security orchestration, automation, and incident response. Siemplify's platform is designed for security teams to manage, investigate, and automate all operations from a single pane of glass.

Used globally by Enterprise SOC teams Siemplify consolidates tools, reduces alerts by 90%, triples analyst bandwidth, and reduces the time from attack to remediation from days to minutes – becoming the de facto operating system for the next-generation SOC. Siemplify is used as the primary day-to-day application to address the needs of SOC Analysts, Managers, and Security Leaders.

2. Install Siemplify

[Download Siemplify](#)

[Deployment Prerequisites](#)

[Deploy With OVA](#)

[Deploy With Installer](#)

[Open Siemplify Client](#)

2.1. Download Simplify

- Browse to the link provided to you by the designated Support engineer.
- Download the OVA file `Siimplify.X.ova` or the installer `siimplify_installer.sh` (depending on your preferred installation mode)
- Verify the validity of the downloaded file by doing the following:
 - Run the command `md5sum <md5_filename>`
 - Compare the calculated hash values with the provided MD5 values
 - In case of mismatch try to download the file again. If the problem persists please contact Simplify support at support@siimplify.co.

2.2. Deployment Prerequisites

Integrations

To properly configure the integrations between Siemplify and your security products, please be sure to provide the credentials \ API keys required to access them.

In the Siemplify console, navigate to Marketplace to see what information is required for each integration.

In addition, network \ web access should be tested (from Siemplify machine to the security product) prior to the configuration step.

Proxy

To use a web proxy, first make sure Siemplify machine has network access to the proxy.

Then, in the Siemplify Console, navigate to Settings > Advanced > General to set up the proxy.

Web Access

Internet access from Siemplify machine is required to allow Siemplify Installer download packages from the online repository.

Shared storage access

Make sure to prepare accessible shared storage in case your mode of deployment requires that.

Time Synchronization (for version 5.3 only)

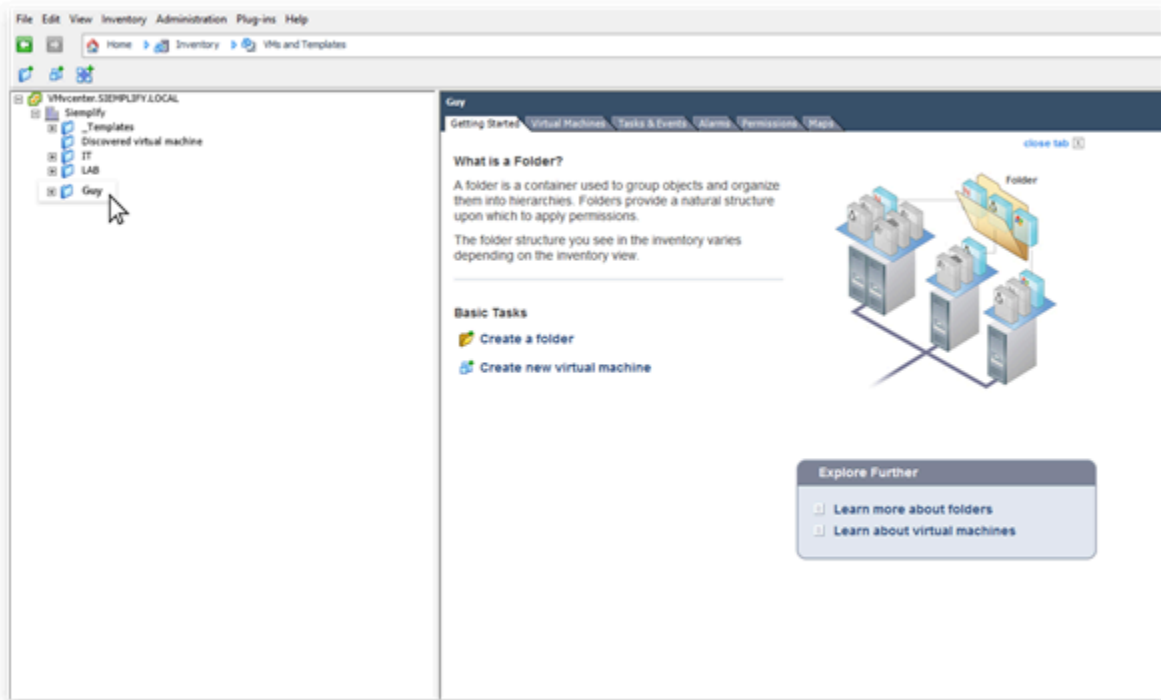
It is not recommended to perform a time synchronization of the Server after deployment.

Storage Space

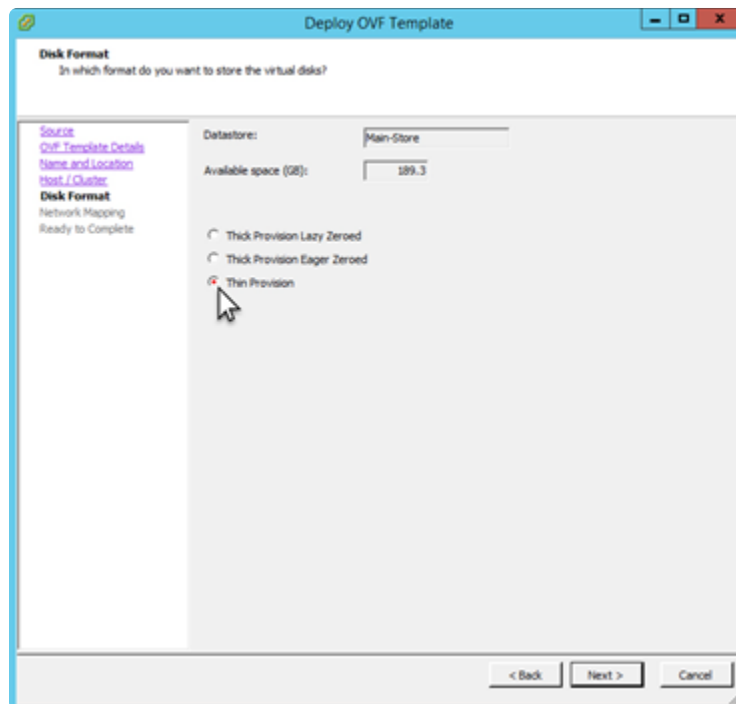
Make sure that the tmp folder has at least 10 giga of free space before both a clean install and an upgrade.

2.3. Deploy With OVA

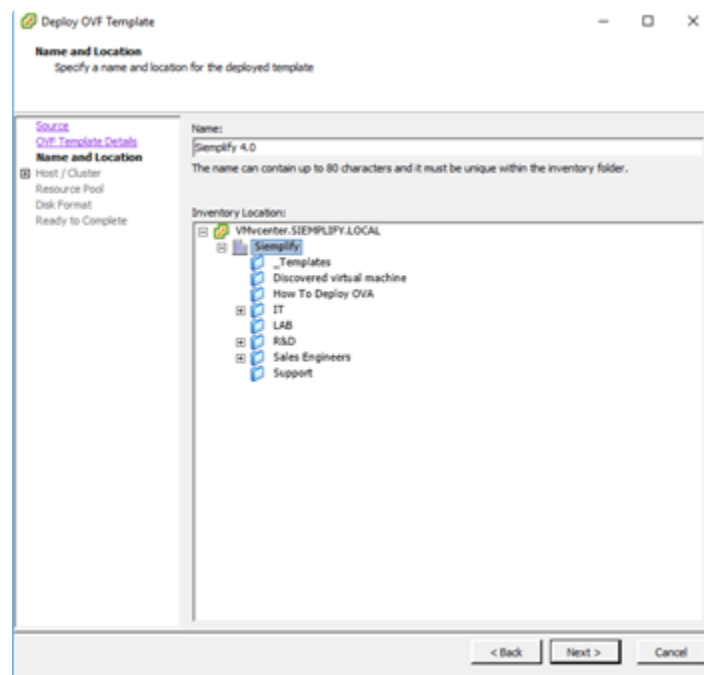
- Open the vSphere console.



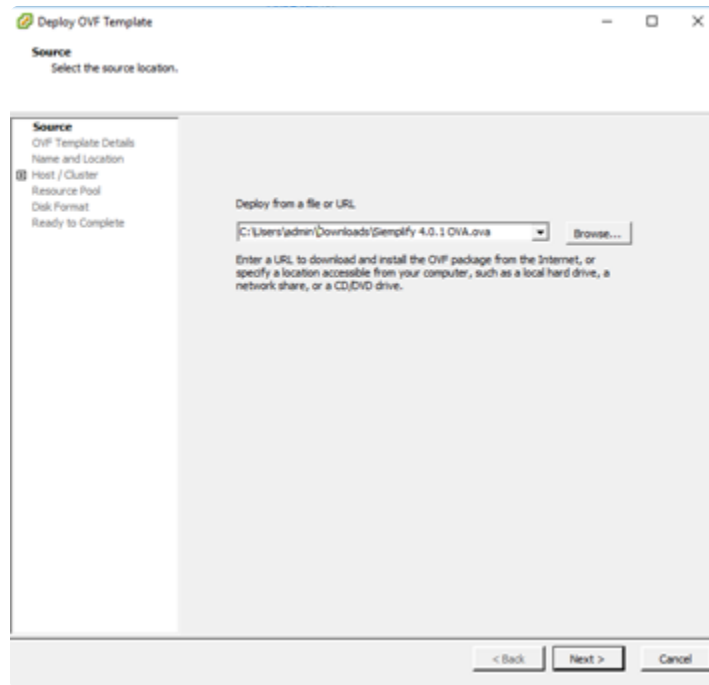
- Select the required destination folder.
- Navigate to File > Deploy OVF Template.
- In the OVF deployment wizard that opens, click Browse in the Source screen and select the Simplify OVA file. Click Next.



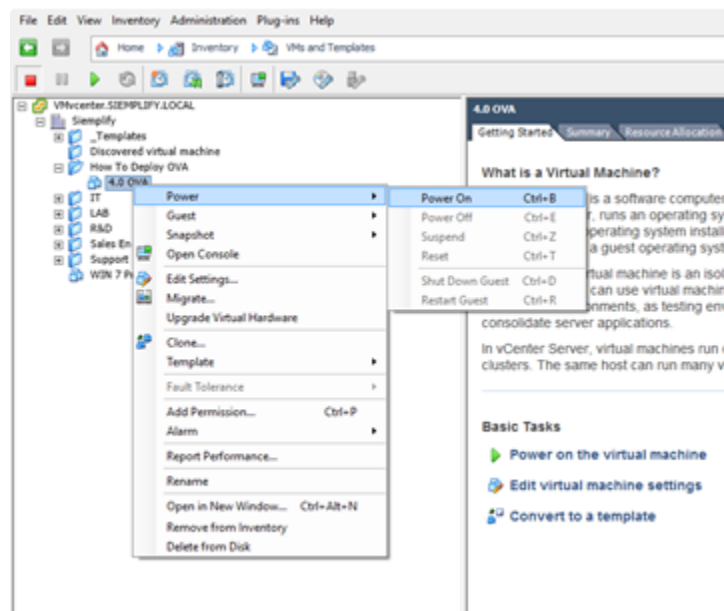
- In the Name and Location fields, provide a logical name. Click Next.



- Under Host/Cluster, select the designated cluster based on your lab architecture. Click Next.
- Under Disk Format select Thin Provision. Click Next.



- Click Finish. The machine will now take several moments to deploy.
- Once the deployment is successfully completed, select the new Simplify machine and select Power on the Virtual Machine.



Continue on with [Open Simplify Client](#).

2.4. Deploy With Installer

- Copy the installation file you downloaded to the machine where Siemplify will be installed.

- Run the installer with the following commands:

```
sudo chmod +x siemplify_installer.sh
```

```
sudo bash siemplify_installer.sh
```

```
(root@localhost ~) # sudo bash siemplify_installer.sh
#####
Welcome to the Siemplify Platform Installer <INSTALLER_VERSION>

The installer will install the Siemplify SOAR platform in a variety of modes (see --help for further information)

Supported operating systems include:
Centos: Version: 7.5.1804 and above
#####

Loaded plugins: fastestmirror
Examining /var/tmp/yum-root-SSWETS/epel-release-latest-7.noarch.rpm: epel-release-7-12.noarch
Marking /var/tmp/yum-root-SSWETS/epel-release-latest-7.noarch.rpm to be installed
Resolving Dependencies
--> Running transaction check
--> Package epel-release.noarch 0:7-12 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package           Arch      Version      Repository      Size
=====
Installing:
epel-release      noarch    7-12         /epel-release-latest-7.noarch    24 k
=====
Transaction Summary
=====
Install 1 Package

Total size: 24 k
Installed size: 24 k
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : epel-release-7-12.noarch                1/1
  Verifying  : epel-release-7-12.noarch                1/1

Installed:
  epel-release.noarch 0:7-12

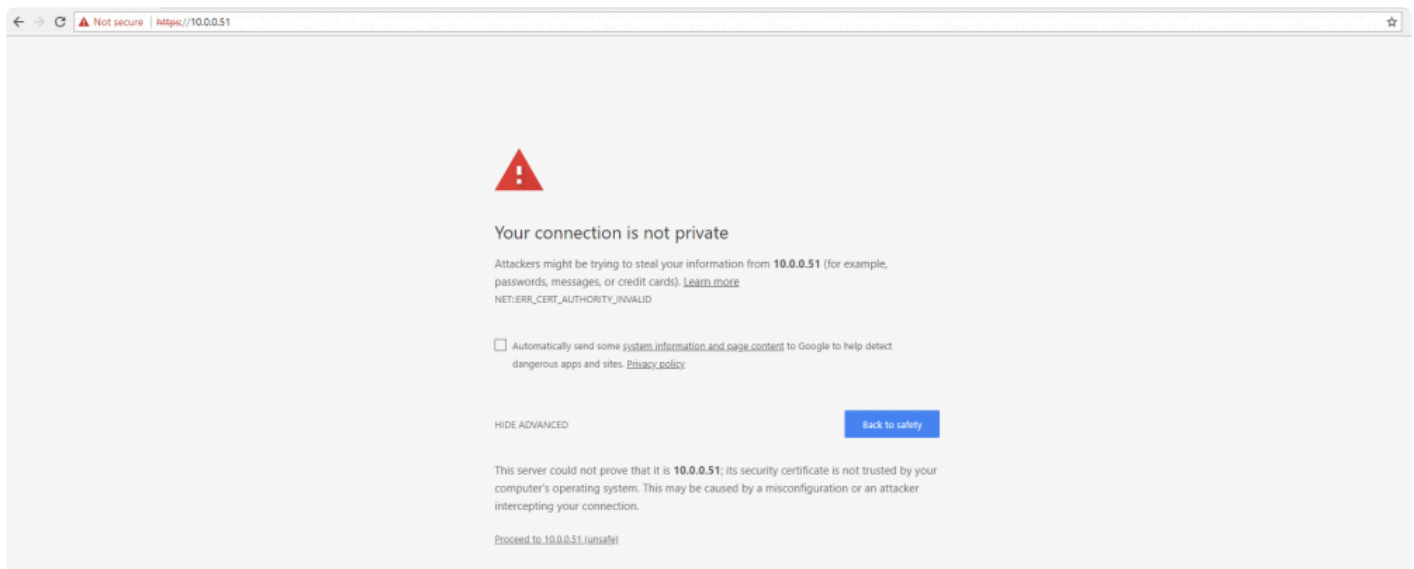
Complete!
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: centos.spd.co.il
 * epel: rep-epel-il.upress.io
 * extras: centos.spd.co.il
 * updates: centos.spd.co.il
```

- Wait for the installation to complete and access Siemplify from a client workstation.

For more information, please refer to the [Installation Guide for 5.3.0](#)

2.5. Open Siemplify Client

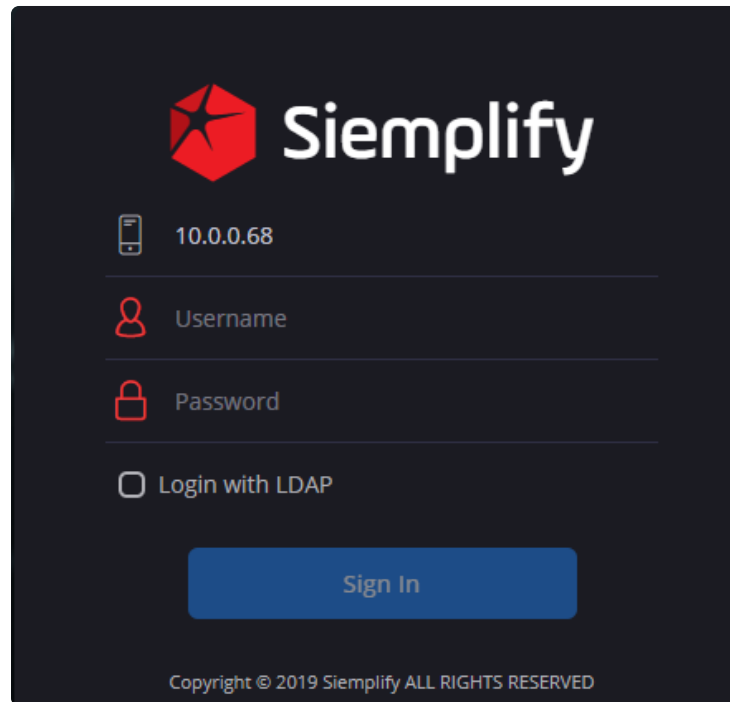
- Check the IP of Siemplify server from VSphere or with `ifconfig`.
- Login to a client workstation that has access to the Siemplify server.
- Open a Google Chrome browser and browse to the Siemplify IP `https://<siemplify_server_address>`.
- Click on Advanced and Proceed to to 10.0.0.51 (unsafe).
If you get a Resolution warning, click Proceed Anyway.



- Sign in to Siemplify with username: “admin” and password: “password”. Siemplify recommends changing your password after first login.



Siemplify customers should check first with their Customer Success Manager to make sure they have the correct username/password.

The image shows a dark-themed login interface for Siemplify. At the top, there is a red hexagonal logo with a white star-like shape inside, followed by the word "Siemplify" in a white sans-serif font. Below the logo, there is a version number "10.0.0.68" next to a small icon of a document with a checkmark. Underneath, there are two input fields: one for "Username" with a red person icon and one for "Password" with a red padlock icon. Below these fields is a checkbox labeled "Login with LDAP". At the bottom of the form is a blue button with the text "Sign In". At the very bottom, there is a small copyright notice: "Copyright © 2019 Siemplify ALL RIGHTS RESERVED".

Siemplify

10.0.0.68

Username

Password

☐ Login with LDAP

Sign In

Copyright © 2019 Siemplify ALL RIGHTS RESERVED

- If you receive a message that your license is not valid, contact your designated Customer Success Manager \ Sales Engineer and provide him with your Customer ID.
- Insert the base64 license provided by your sales engineer and click Upload.

3. Start Working in Siemplify

[Run Use Cases](#)

[Ingest Your Data](#)

[Create Entities](#)

[Configure Integrations](#)

[Create and Run a Playbook](#)

[Manage Cases](#)

3.1. Run Use Cases

Quick Summary

Simplify provides a repository for use cases developed by Simplify or by the community that can be deployed in your environment. The use cases are available for download from the Marketplace. Each use case contains the items required for an end-to-end execution of a workflow.

Overview

Use cases can be a great way for Simplify Users to share their knowledge by uploading their own use cases in the Simplify Platform. The use case contains all the items needed to implement a workflow and installs the following:

- Test case (Simulation Case)
- Mapping & modelling configuration
- Integrations
- Connectors
- Playbooks

This allows you to see how an end-to-end security workflow will look in Simplify, and even use these items as a kickstart for the actual use cases you want to implement.

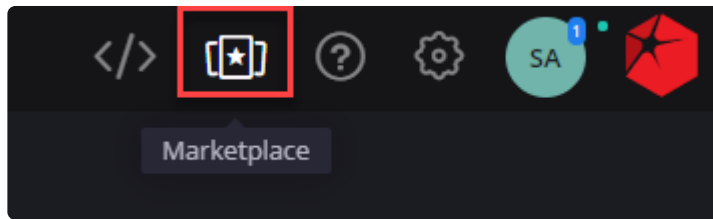
In the marketplace, you will have a fully detailed description of the items in each use case. In addition, there may be a video showing you how to deploy the use case on mock or real data. You will usually be required to configure the integrations in the use case.

When everything is set up, you will be able to run the test cases from the Cases screen.

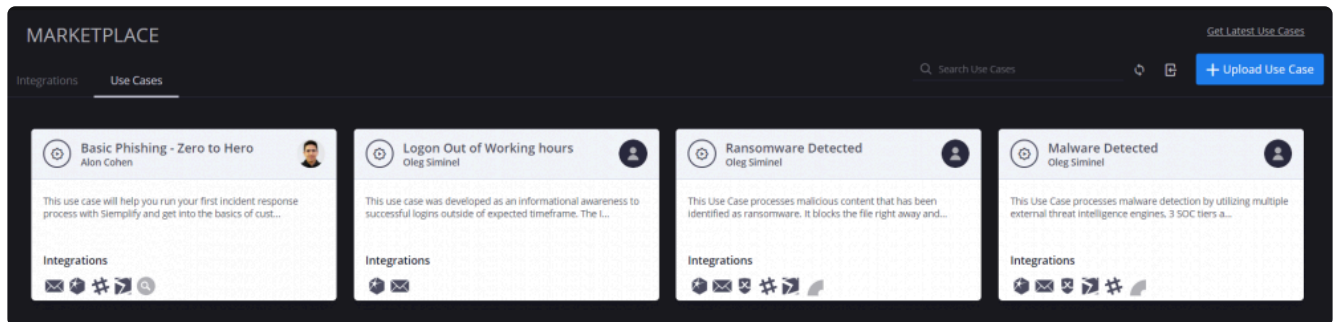
Example: Zero to Hero Use Case

Let's run the Basic Phishing (Zero to Hero) use case from the Marketplace.

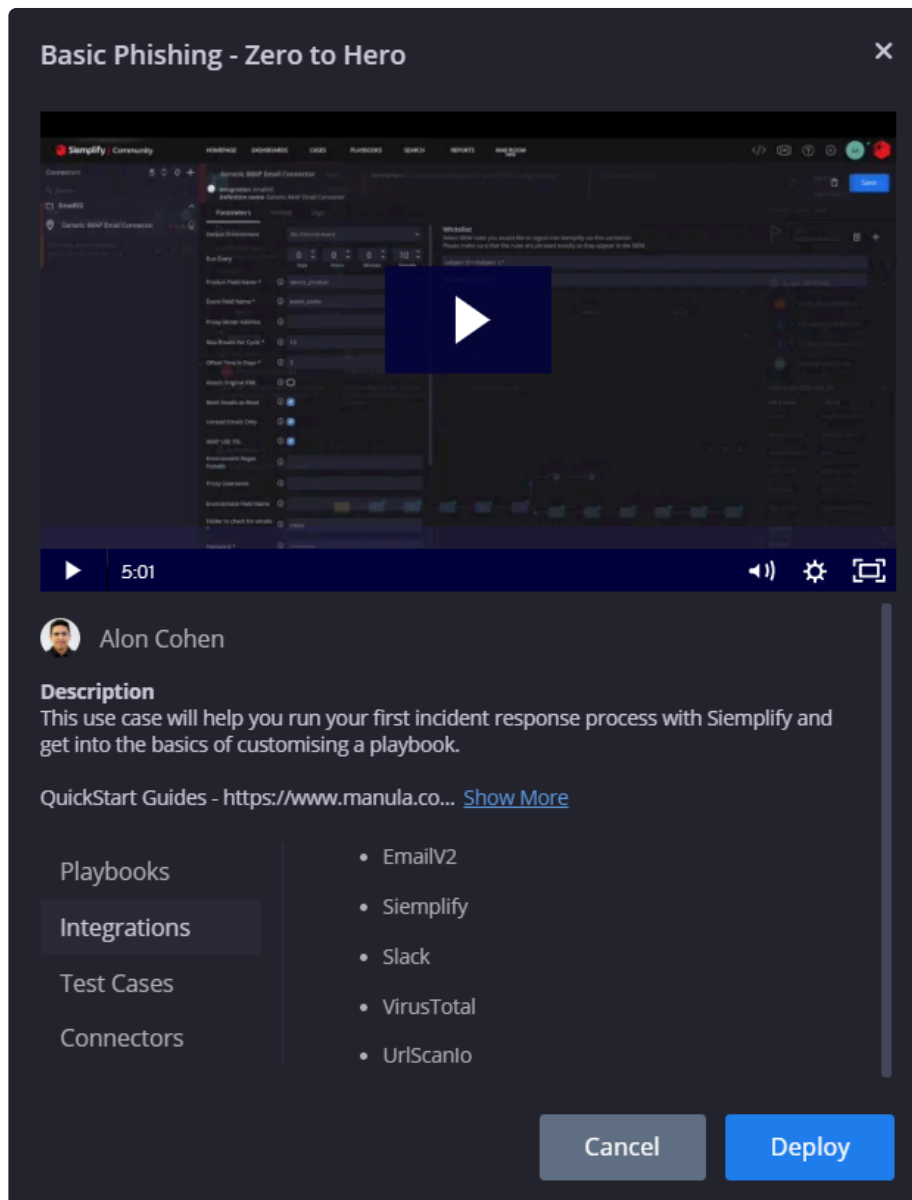
1. Navigate to the Marketplace.



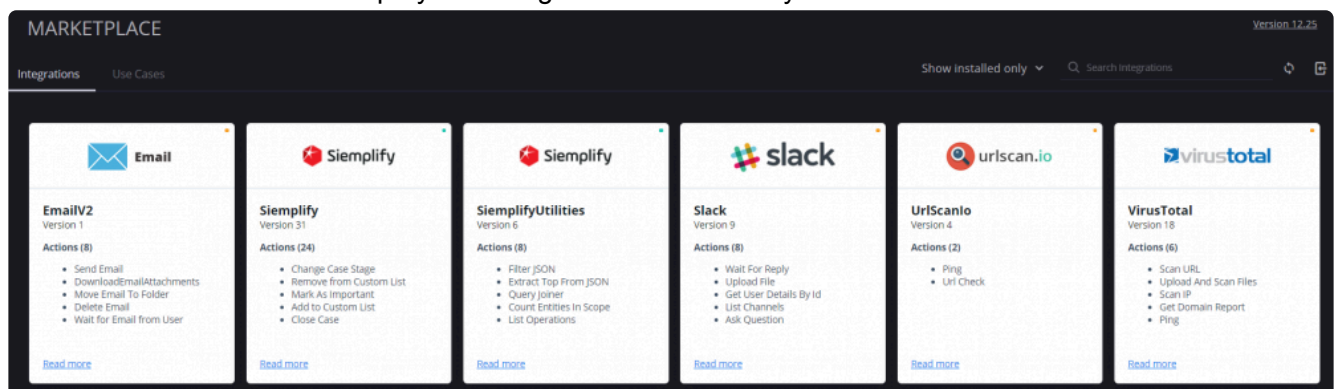
2. Click on the Use Case tab in the marketplace and select the Zero to Hero use case.



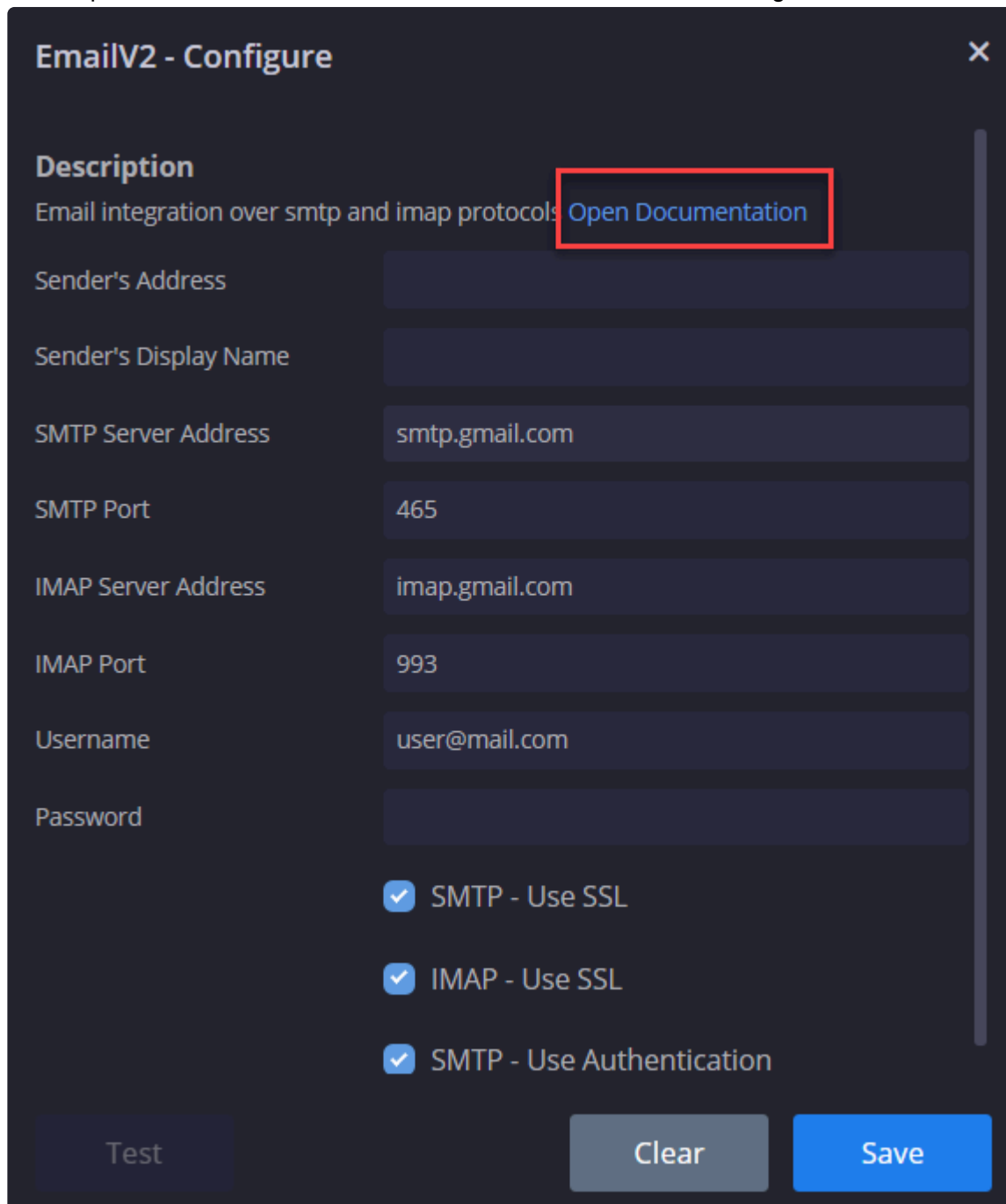
3. Before you click Deploy, we recommend you take five minutes to watch the video tutorial in this Use Case before continuing. Click Deploy and wait while the system downloads all the items. When finished, you will see a confirmation message.



4. Navigate to the Integrations section of the marketplace and click on Choose > Show Installed Only and then click Refresh to display the Integrations installed by this Use Case.



- Configure the installations that have an orange circle at the top by adding the required parameters. Click Open Documentation to see detailed information for each integration.



The image shows a configuration window titled "EmailV2 - Configure" with a close button (X) in the top right corner. The window has a dark theme. Under the "Description" section, it says "Email integration over smtp and imap protocols" and includes a link "Open Documentation" which is highlighted with a red rectangle. Below this are several input fields: "Sender's Address", "Sender's Display Name", "SMTP Server Address" (containing "smtp.gmail.com"), "SMTP Port" (containing "465"), "IMAP Server Address" (containing "imap.gmail.com"), "IMAP Port" (containing "993"), "Username" (containing "user@mail.com"), and "Password". At the bottom, there are three checked checkboxes: "SMTP - Use SSL", "IMAP - Use SSL", and "SMTP - Use Authentication". At the very bottom are three buttons: "Test", "Clear", and "Save".

EmailV2 - Configure ✕

Description
Email integration over smtp and imap protocols [Open Documentation](#)

Sender's Address

Sender's Display Name

SMTP Server Address

SMTP Port

IMAP Server Address

IMAP Port

Username

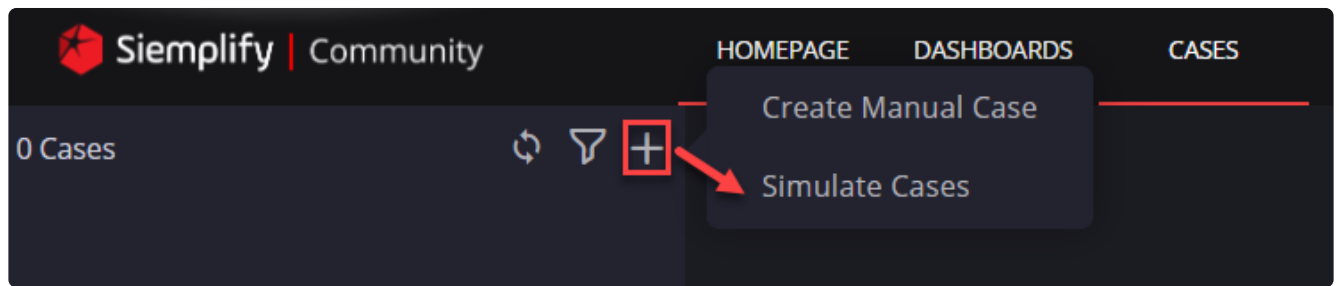
Password

☒ SMTP - Use SSL

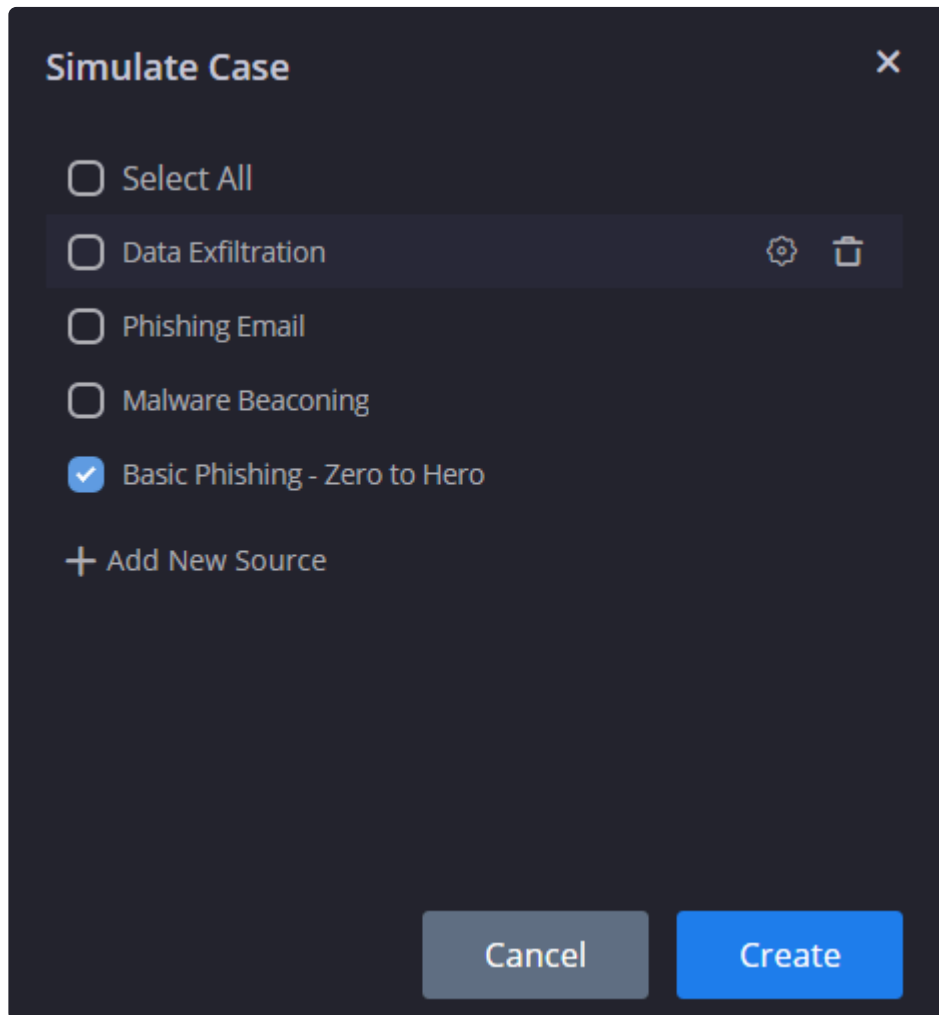
☒ IMAP - Use SSL

☒ SMTP - Use Authentication

- Click Save on the newly configured installation and then click Test. A green tick confirms that everything is configured correctly. You can close the configuration screen now.
- Refresh the page and you will see the orange circle change to a green circle on the newly configured Integration.
- Navigate to Cases, click the + sign above the cases queue and select Simulate Cases.



9. Select the Zero to Hero case and click Create.



10. Click Refresh and you will see a new Case created in Siemplify, with a playbook attached to the alert inside.

The screenshot displays the Simplify security dashboard interface. The top navigation bar includes a user profile for '@Administrator', a 'Mail' tab, and a case identifier 'ID 1 | Last modified 2020-02-09 03:40:14 PM | Stage: Triage'. A 'Click to Refresh Case' button is visible on the right.

The main content area is divided into several sections:

- Alerts (2):** Shows two 'SUSPICIOUS EMAIL' alerts from 2020-02-09 03:39:49 PM and 2020-02-09 03:40:06 PM, each with 1 event.
- Insights (4):** Displays four insights related to the alert, each with a 'Simplify' icon and a placeholder image.
- Playbooks (2):** Shows two playbooks: 'Copy of Basic Phishing PB - Zero ...' and 'Basic Phishing PB - Zero to Hero'.

The right sidebar contains 'Context Details' for the alert, including a search bar and a list of related entities:

- CRAG@TEXTSPEER.DE
- STEVEN.B@SIMPLIFY.CO
- HTTPS://TEXTSPEER.DE
- YOUR DROPBOX FILE


Below the entity list is a 'HIGHLIGHTED FIELDS' table:

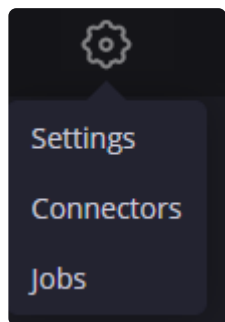
FIELD NAME	VALUE
Name	Suspicious Email
Device/Vendor	Phishing Email B...
Device/Product	Mail
Start Time	2020-02-09 03:4...
End Time	2020-02-09 03:4...
Alert Name	SUSPICIOUS EM...
Default	
Threat	

3.2. Ingest Your Data (Connectors)

Quick Summary

Siemplify uses connectors to ingest alerts from a variety of data sources into the Siemplify platform. A connector is one of the items in an integration package – which can be downloaded via the Marketplace.

Connectors are configured via  > Connectors.




Overview

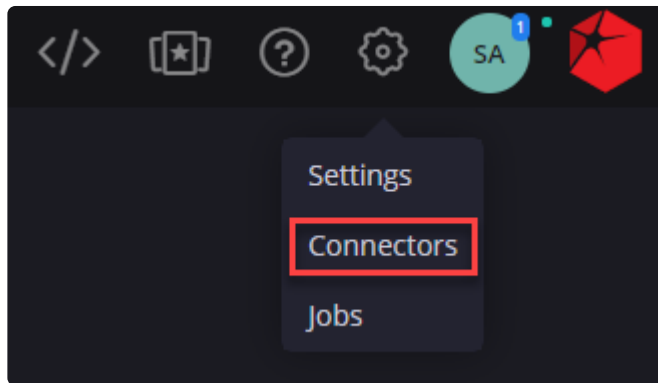
Connectors are Python based applications that allow users to pull alerts from 3rd party products into Siemplify. Connectors also parse and normalize the raw data (alerts, events) into a Siemplify format which will then be presented as a Case in the Case Queue.

If you are running a SIEM (a central place for all your alerts), one connector will be enough. It is also possible to pull data from multiple sources with several connectors. Each connector will have a dedicated documentation link for additional help.

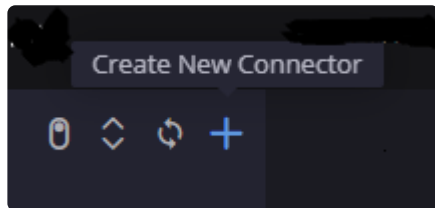
Example – Email Connector

Let's set up an email connector.

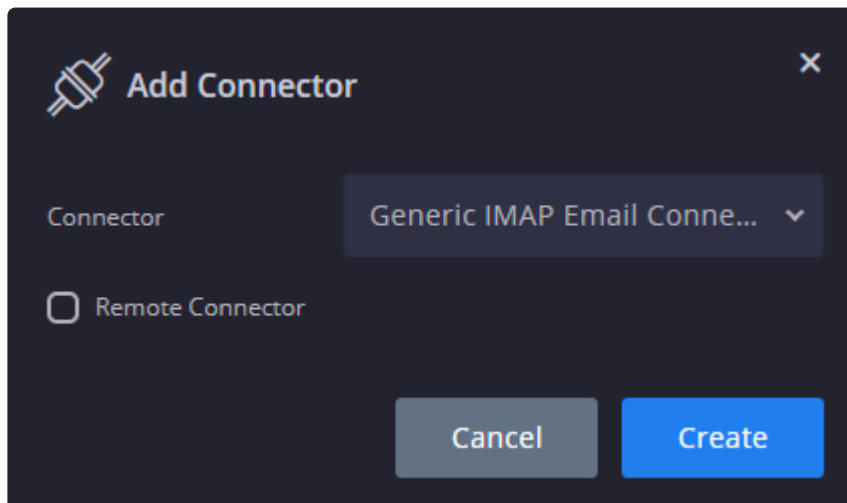
1. Navigate to Marketplace > Integrations and install the EmailV2 integration. Refer to information in [Run Use Cases](#) on how to complete this step.
2. Navigate to  > Connectors.



3. Click on the plus icon on the left side of the screen.



4. Select the IMAP Email connector and click Create.



5. Fill in the empty mandatory fields and save the connector. Click Yes on the confirmation message.
6. Enable the connector and save it again. This will make it run periodically to pull any new emails according to the configuration.

3.3. Create Entities (Mapping & Modelling)

Quick Summary

Simplify uses an automated system (Ontology) to extract the main objects of interest from the raw alerts to create Entities. Each Entity will be represented by an object that can track its own history for future reference.

Overview

Entities are objects that represent points of interest extracted from alerts (IOCs, artifacts etc.). Entities allow you to automatically track their history, group alerts without human intervention and hunt for malicious activity based on the relationship between the different entities.

Entities can also help security analysts to read cases faster and build playbooks more seamlessly.

Part of configuring the Ontology involves a process called Mapping and Modelling. In this process you select the visual representation of alerts and the Entities that should be extracted from it.

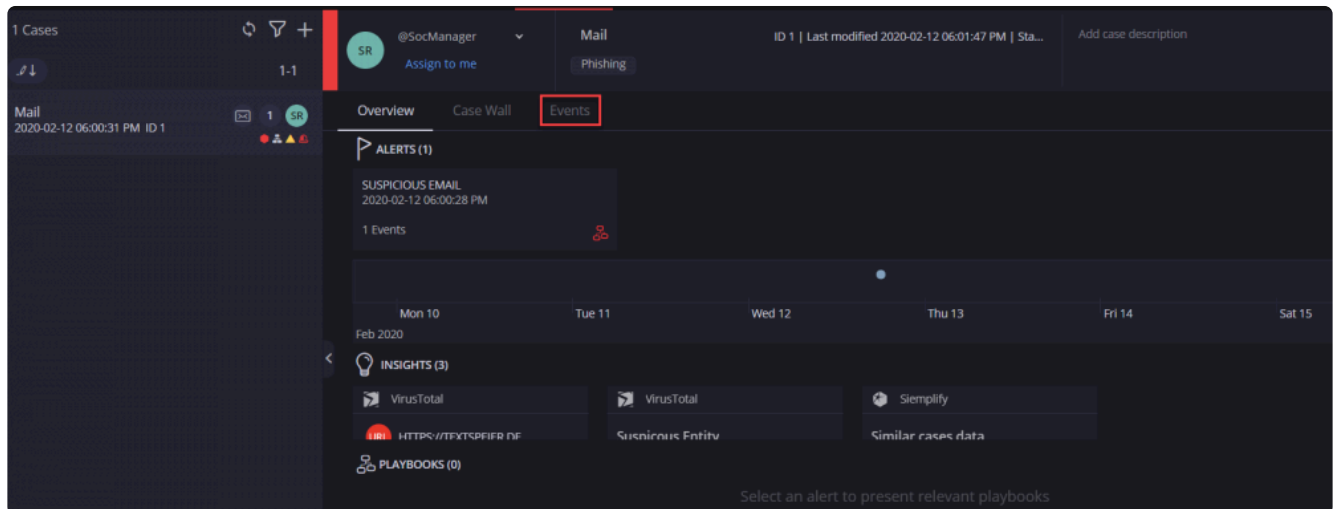
Simplify provides basic Ontology rules for most popular SIEM products out-of-the-box.


The best time to start customizing the Ontology is when you already have a Connector that pulls data into Simplify. When configuring Ontology, the user is first required to choose the visualization type for the data (select the model \ visual family) and then map the fields to support the selected model and extract the entities (mapping).

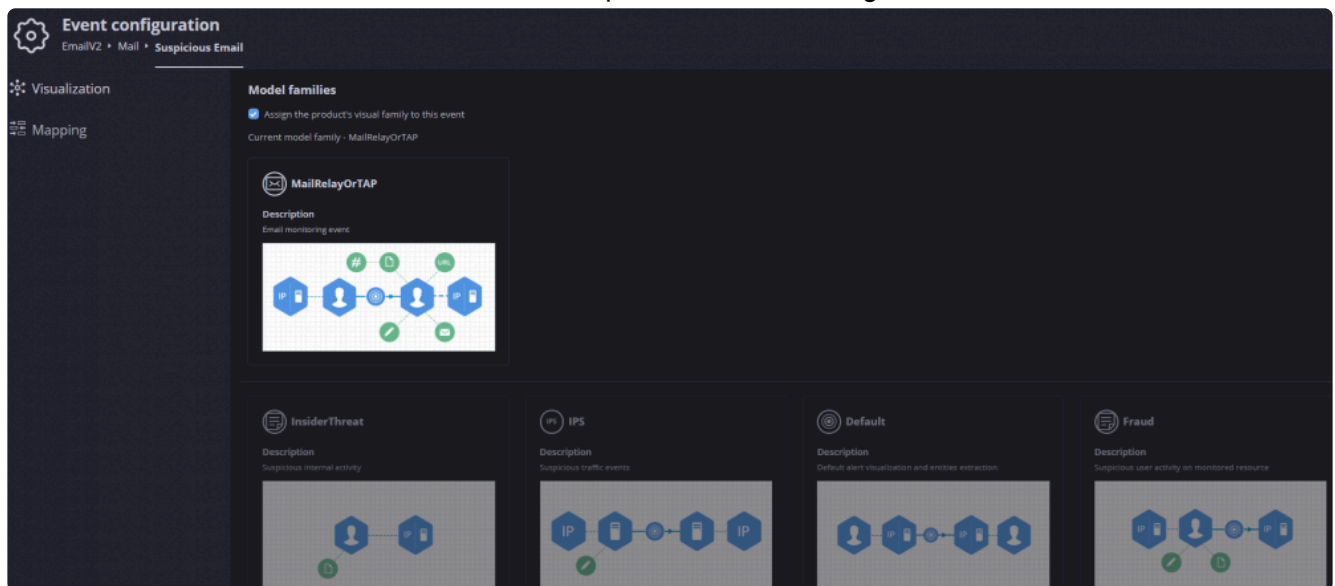
Example – Ingested Email

Let's map and model new data of an ingested email.

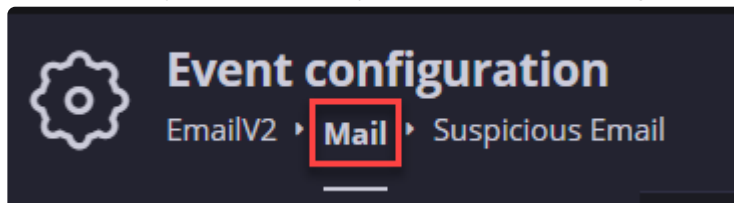
1. Run the Zero to Hero test case. Refer to [Run Use Cases](#) for full details on how to do this.
2. In the Cases tab, click to open the Mail case from the Cases Queue and select the Events tab.



- Click on  on the left of the Alert name, to open the Event Configuration screen.

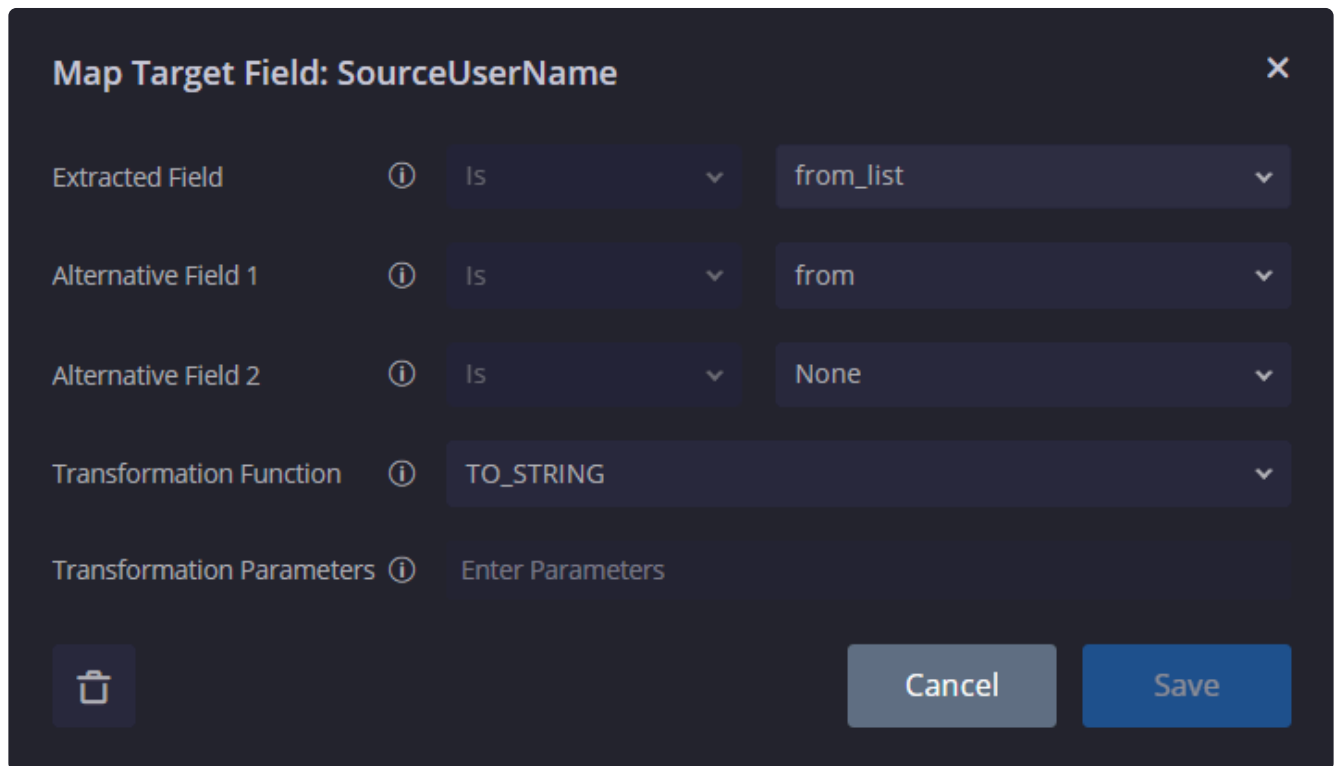


- On the top left corner, click on the word Mail in the hierarchy. That ensures that your configuration will automatically work for every piece of data coming from this product (Email box).




- Assign the Visual Family that most represents the data – in our example we can skip this step as 'MailRelayOrTAP' has already been selected following the deployment of the Zero to Hero use case.
- Switch to Mapping and map the following Entity Fields:
SourceUserName, DestinationUserName, DestinationURL, EmailSubject.
This can be done by double clicking each and selecting the raw data field for that entity in the

Extracted Field. As you can see in the screenshot below, you can provide alternative fields from which to extract the information from.



Map Target Field: SourceUserName ✕

Extracted Field	ⓘ	Is	from_list
Alternative Field 1	ⓘ	Is	from
Alternative Field 2	ⓘ	Is	None
Transformation Function	ⓘ	TO_STRING	
Transformation Parameters	ⓘ	Enter Parameters	

 Cancel Save

7. In order to see what the original fields are in the email, click on the Raw Event Properties table in the top right corner.

Event Fields

Q Search...

Key	Value
Name	Suspicious Email
CategoryOutcome	allowed
DeviceProduct	Mail
startTime	1581523228284
endTime	1581523228284
from	craig@textspeier.deo
to	steven.b@siemplify.co
url_1	https://textspeier.de
sourcetype	Email
.....

Close

3.4. Configure Integrations

Quick Summary

Integrations are packages that can be installed from the Marketplace. When you install an integration, you are adding Connectors, Playbook Actions and Scheduled Jobs. These are all able to connect Siemplify with third party products in order to perform tasks. Each of these items can be configured from the relevant screen (Connectors, Playbooks, Jobs).

Overview


Each integration has multiple types of items that are relevant for different use cases.

The Connectors help you ingest alerts into Siemplify.

The Actions are used to enrich existing data and perform proactive actions (e.g. block IP, send email).

The Jobs help users perform scheduled tasks on the 3rd party product directly from Siemplify.

To use an Integration the user has to locate it in the Marketplace, download it and then configure and test it. In addition, users should configure the specific Connector, Action or Job from the integration they would like to run.

The Connectors are configured from  > Connectors.

The Jobs are configured from  > Jobs.

Actions can be either used in playbooks (dragging Actions to playbooks) or directly on Alerts.

Example

Let's configure an Email integration.

1. First, navigate to Marketplace > Integrations, locate the Email integration and click the arrow to install it.



Email

EmailV2

Version 1

Actions (8)

- Send Email
- DownloadEmailAttachments
- Move Email To Folder
- Delete Email
- Wait for Email from User

[Read more](#)



- Next, move to the Marketplace > Configure. Select the default environment on the left and click the plus icon on the right.



- Select the required Integration and then fill in with the required parameters.
- Click on Test (after saving it) which will query back and tell you whether the integration is able to communicate successfully with the product or not.

3.5. Create and Run a Playbook

Quick Summary

Playbooks are step by step workflows that can run automatically or guide Siemplify users through a process. Playbooks are used for SOC, NOC and Incident Response use cases (e.g. gather enrichment, complete tasks etc.) and can be triggered manually or automatically.

Overview

Playbooks allow Siemplify users to create workflows based on SOC, NOC and Incident Response use cases to standardize and automate security tasks.

Playbooks are triggered by different types of alerts – these Triggers are logical conditions that tell the playbook when to run.

The workflow is created with Actions that are able to perform tasks in Siemplify and integrated 3rd party products.

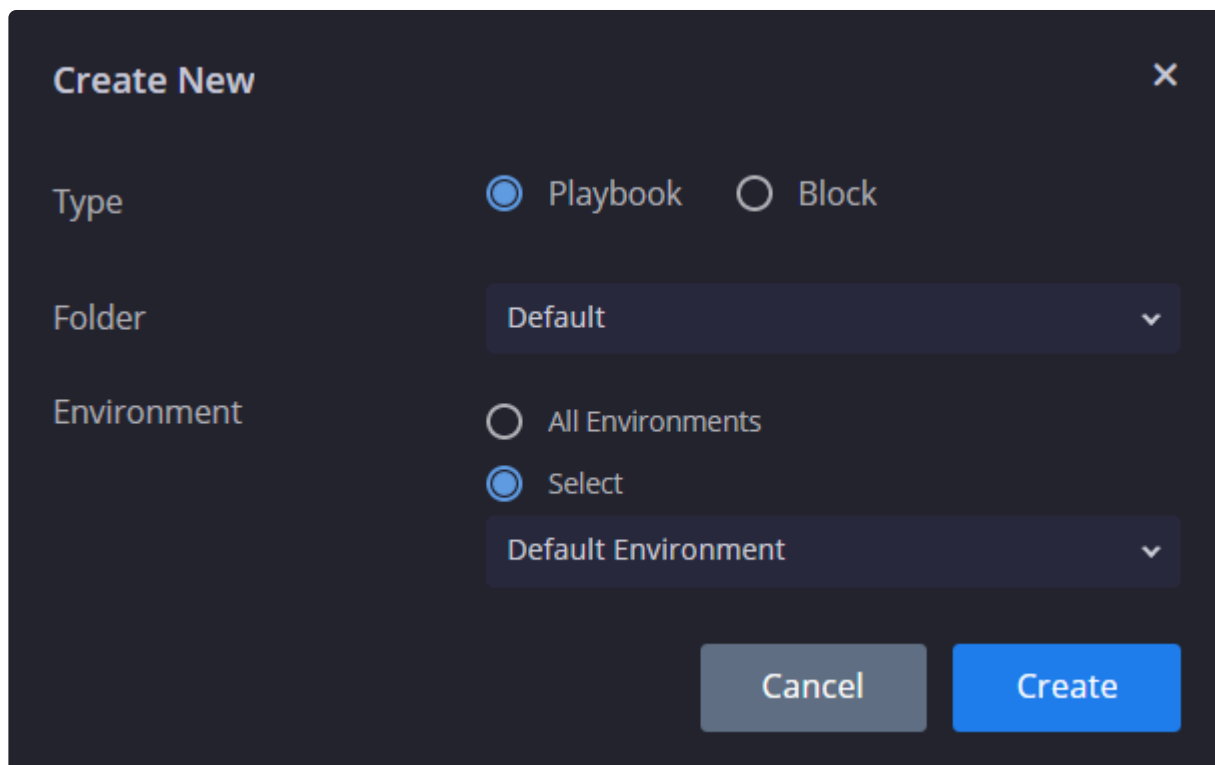
In addition, Siemplify provides multiple Flow components to help with making decisions during the workflow (with or without human intervention).

Siemplify also provides Playbook Blocks which are reusable playbooks that can be embedded in other playbooks. Playbooks Blocks can change their behavior based on execution context.

Example – Email Playbook

Let's create a playbook for the Email case.

1. Navigate to the Playbooks tab and click + to choose a Playbook.
2. Select the required folder and environment and click on Create.



The 'Create New' dialog box is shown with a dark theme. It has a title bar with 'Create New' and a close button. The 'Type' section has two radio buttons: 'Playbook' (selected) and 'Block'. The 'Folder' section has a dropdown menu set to 'Default'. The 'Environment' section has two radio buttons: 'All Environments' and 'Select' (selected). Below the 'Select' radio button is another dropdown menu set to 'Default Environment'. At the bottom are 'Cancel' and 'Create' buttons.

Create New

Type ☒ Playbook ☐ Block

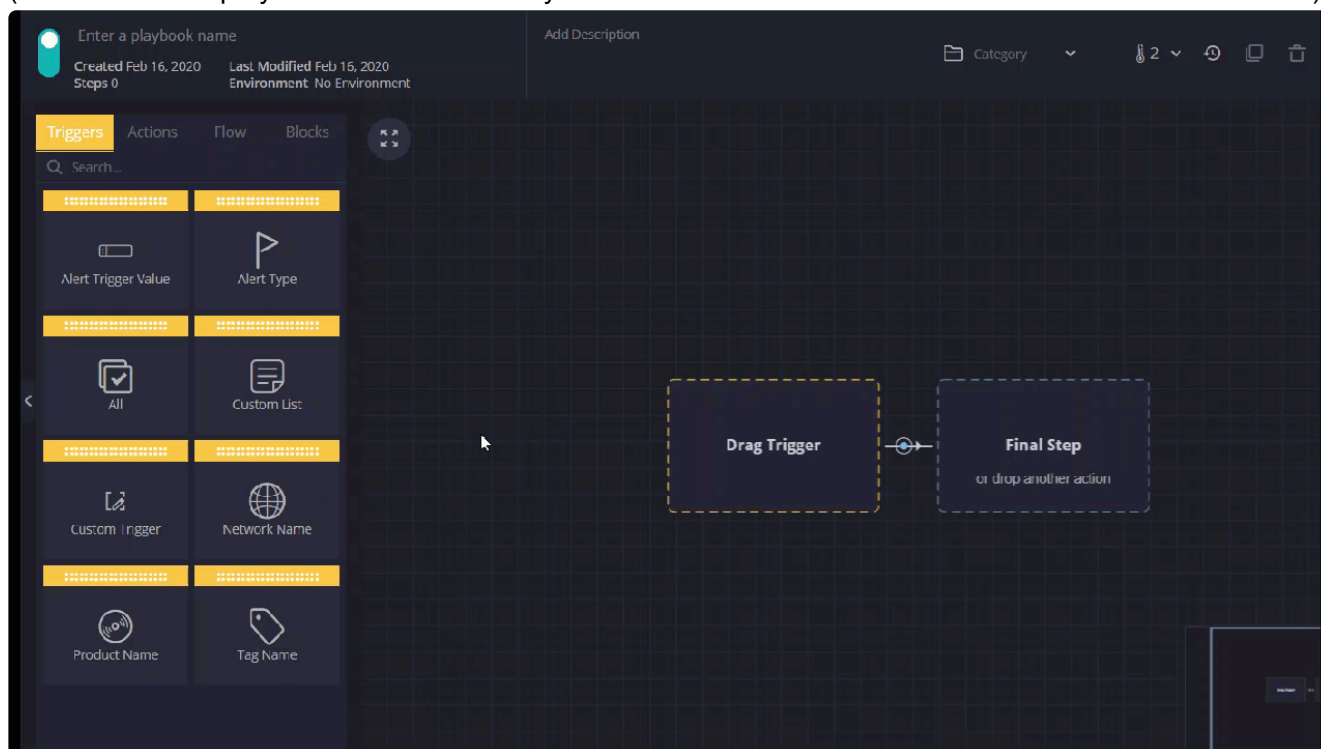
Folder Default

Environment ☐ All Environments ☒ Select

Default Environment

Cancel Create

3. Drag a Trigger into the trigger box. For this example we will use the 'Product Name' trigger.
4. Click on the trigger you added to configure it.
5. Change the operator in the dropdown to "Contains" and put Mail as the parameter (that means the playbook will run on every alert that contains the word Mail in its DeviceProduct field).



The screenshot shows the 'Create New' dialog box in the background, with the 'Product Name' trigger selected. In the foreground, the 'Triggers' tab of the playbook editor is active. The left sidebar shows a list of triggers: Alert Trigger Value, Alert Type, All, Custom List, Custom Trigger, Network Name, Product Name, and Tag Name. The main canvas shows a flow diagram with a 'Drag Trigger' box and a 'Final Step' box. The 'Drag Trigger' box is highlighted with a dashed orange border, and the 'Final Step' box is highlighted with a dashed blue border. A mouse cursor is hovering over the 'Drag Trigger' box.

Enter a playbook name Add Description

Created Feb 16, 2020 Steps 0 Last Modified Feb 16, 2020 Environment No Environment

Category

Triggers Actions Flow Blocks

Search...

Alert Trigger Value Alert Type

All Custom List

Custom Trigger Network Name

Product Name Tag Name

Drag Trigger

Final Step
or drop another action

- Switch to the Actions tab and drag the Get Similar Cases action under the Siemplify integration.
- Click the action to configure the parameters. These will be considered when the playbook looks for similar cases during run time.

Siemplify - Get Similar Cases

Siemplify_Get Similar Case

Search for similar cases and return their Ids

Manual ☐ Auto ☒

If step fails
Stop playbook ▼

Choose Instance ⓘ Shared_Siemplify_1 ▼

Configure Output

Entities ⓘ All entities ▼

Rule Generator ⓘ ☒

Port ⓘ ☒

Category Outcome ⓘ ☒

Entity Identifier ⓘ ☒


Days Back * ⓘ 4 []

Cancel Save

- Switch to the Flow tab and drag a Previous Action Condition to the last step.
- Set the condition to go to branch 1 by selecting 'Siemplify_Get Similar Cases_1.SimilarCasesIds' on the left side and select the 'Not Empty' operator. Click Save.<https://manula.r.sizr.io/large/user/14758/img/previousactionsconditionsstep.png>

10. Switch to the Actions tab, select and drag the Siemplify > Assign Case to branch number 1 and select yourself.

Siemplify - Assign Case

 **Siemplify_Assign Case_1**

Assign case to specific user or usergroup

Manual ☒ Auto

If step fails

Stop playbook ▼

Choose Instance ⓘ

Shared_Siemplify_1 ▼

Configure

Output

Entities ⓘ

All entities ▼

Assigned User * ⓘ


@Administrator ▼

Cancel

Save

11. Drag the Siemplify > Close Alert action to the Else branch.

Siemplify - Close Alert

**Siemplify_Close Alert_1**

Closes the current alert

Manual ☒ Auto

If step fails
Stop playbook ▼

Choose Instance ⓘ Shared_Siemplify_1 ▼

Configure

Output

Entities ⓘ All entities ▼

Reason * ⓘ Not malicious ▼

Root Cause * ⓘ Employee error ▼

Comment * ⓘ

Not malicious - can close []

Assign To User ⓘ OTier1

Cancel

Save

12. Enable the playbook, name it and save it.
13. Simulate the Zero to Hero case to see this playbook running.

The screenshot displays the Simplify SOC Manager interface for a case titled "Mail" (ID 2). The interface is divided into several sections:

- Header:** Shows the user "@SocManager", the case title "Mail", and the ID "ID 2 | Last modified 2020-02-13 05:21:58 AM | Stage: Incident". There is an "Add case description" field and an "Explore" button.
- Overview Tab:** The active tab, showing a timeline of events. A "SUSPICIOUS EMAIL" alert is listed with the timestamp "2020-02-12 06:00:28 PM". Below this is a calendar view for February 2020, with a blue dot indicating an event on Thursday, Feb 13.
- INSIGHTS (3):** A section with three cards:
 - VirusTotal:** Shows a URL "HTTPS://TEXTSPEIER.DE" marked as malicious by 4 of 72 engines.
 - Suspicious Entity:** States "Found 4 engines that marked HTTPS://TEXTSPEIER.DE as a real malicious".
 - Similar cases data:** Shows "found similar cases : []".
- PLAYBOOKS (2):** Lists two playbooks: "Basic Phishing PB - Zero to Hero" and "Test Playbook Quick Start".
- Context Details Panel (Right):** Displays details for the "Alert: Suspicious Email". It includes a search bar and a list of related entities:
 - URL: HTTPS://TEXTSPEIER.DE
 - DeviceVendor: CRAIG@TEXTSPEIER.DE
 - DeviceProduct: STEVEN.B@SIMPLIFY.CO
 - YOUR DROPBOX FILE
- HIGHLIGHTED FIELDS:** A table showing key-value pairs for the alert:

FIELD NAME	VALUE
Name	Suspicious Email
DeviceVendor	Phishing Email B...
DeviceProduct	Mail
Start Time	2020-02-13 05:2...
End Time	2020-02-13 05:2...
Alert Name	SUSPICIOUS EM...
Default	
Threat	

3.6. Manage Cases

Quick Summary

Cases are the management unit for security threats in Siemplify. Cases have all the required ticketing capabilities and much more to support management use cases in the SOC.

Cases can be viewed and managed from the Cases Queue. It is also possible to search for Cases in the Search screen.

Overview

When data is ingested into Siemplify (usually in a form of security alerts or events) it is wrapped inside a Case for management purposes (tracking activity, incident response etc).

A Case will always include at least one alert (or more if Siemplify applies grouping). Each alert contains both the original raw data coming from the data source and the objects Siemplify extracted based on it (Entities, enrichment etc).

The grouping of alerts is performed automatically by Siemplify regardless of the source of each alert to allow better contextual understanding of a threat.

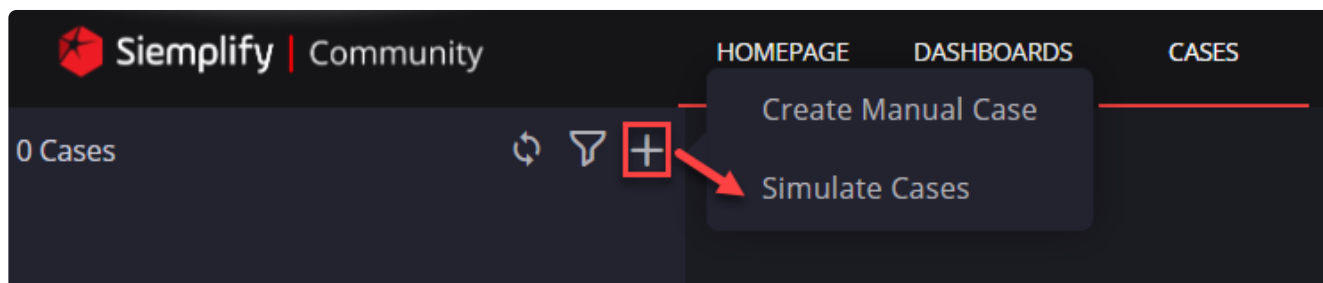
Security analysts then can:

- Understand the threat presented by the case
- Review the case graph for more context (via the Explore button)
- Review enrichment collected manually or with automation
- Review the tasks performed on the case (with Case Wall)
- Manage the case as a ticket (close, re-open, merge, tag, track history, report and more)
- Run actions and playbooks on the alerts in the case

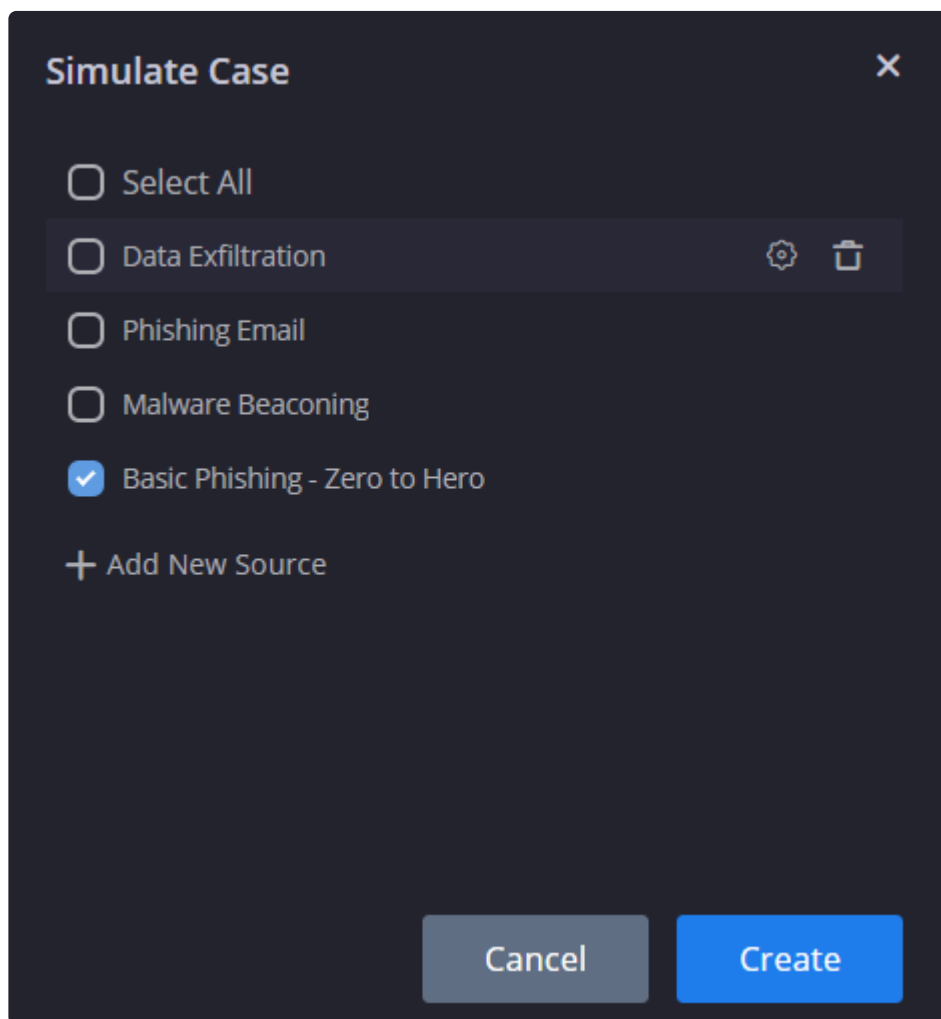
Example

Let's read a case and close it.

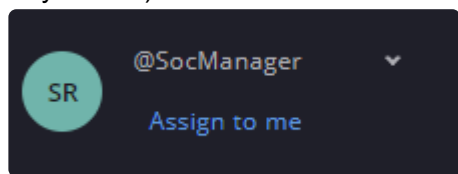
1. Navigate to Cases, click the + sign above the cases queue and select Simulate Cases.



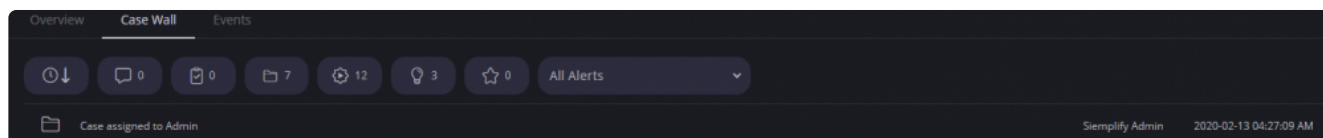
2. Select the Zero to Hero case and click Create.



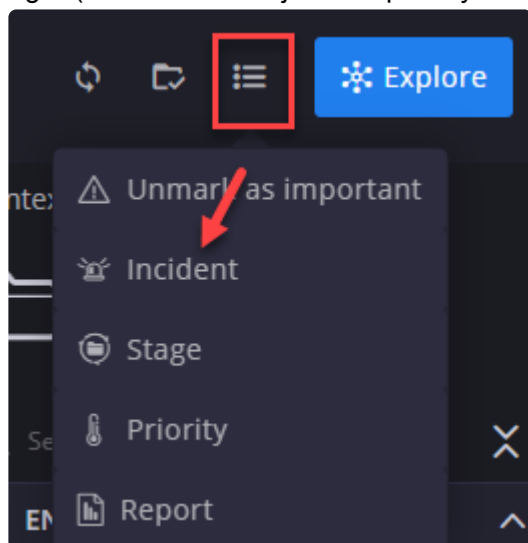
3. Click on the Email case in your queue.
4. To assign the case – select a team or a user from the dropdown on the top bar (in this case, assign it to yourself).



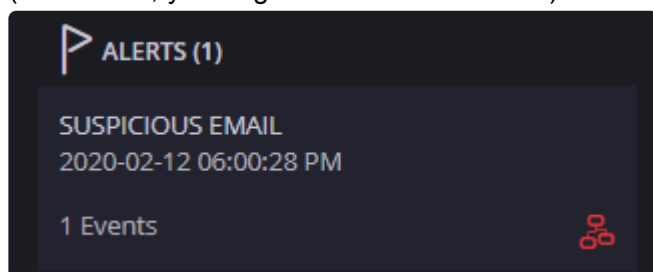
5. The Case Wall tab has now a new entry that shows that the case was reassigned.



6. Go back to the Overview and check out the:
 - a. Name and time of the alert
 - b. Any Insights collected on the case
 - c. The Entities extracted are on the right side (if an entity is red, it is malicious)
7. We found malicious activity in the case – let's mark it as an incident from the hamburger menu on the right (this will also adjust the priority of the case).



8. Playbooks are attached to alerts. To view a playbook, click on one of the alert cards in the case (remember, you might have several alerts).



9. Click on the steps of the playbook to see more info about the actions.

The screenshot displays the Simplify SOC Manager interface for a case titled "Mail" (ID 2). The interface is divided into several sections:

- Header:** Shows the user "@SocManager", the case title "Mail", and the stage "Incident". It also includes a "Close Case" button and an "Explore" button.
- Overview Tab:** The active tab, showing a timeline of events. A "SUSPICIOUS EMAIL" alert is visible on Feb 10, 2020, at 06:00:28 PM. The timeline spans from Mon 10 to Sat 15.
- Alerts (1):** A list of alerts, including the "SUSPICIOUS EMAIL" alert.
- Insights (3):** A section showing insights from VirusTotal and Simplify. It includes a "Suspicious Entity" insight for "HTTPS://TEXTSPEIER.DE" and a "Similar cases data" insight.
- Playbooks (2):** A section showing playbooks, including "Basic Phishing PB - Zero to Hero" and "Test Playbook Quick Start".
- Context Details:** A sidebar on the right showing details for the selected entity "HTTPS://TEXTSPEIER.DE". It includes target entities (CRAIG@TEXTSPEIER.DE, STEVEN.B@SIMPLIFY.CO), parameters, and an action result showing "The case priority was set to High."

- Assuming you handled the threat with success, close the case by clicking Close Case button on top and then filling out the reasons in the dialog box.