DARKTRACE ACADEMY

DARKTRACE/INCIDENT READINESS & RECOVERY

Training Manual

Darktrace/Incident Readiness & Recovery

Training Manual
v1.1.2
Darktrace 6.1

Table of Contents

1. Learning Objectives

Course Agenda

Start your learning with our dedicated video 1: Course Introduction

This course provides a comprehensive understanding of Darktrace/ Incident Readiness & Recovery. It is designed for a wide audience: IT Security Managers, IT Security Architects, and Cyber Security Analysts. The following document provides an educational guide for the key elements of Darktrace/Incident Readiness & Recovery.

PDF Navigation

To navigate back to the Table of Contents page, click on the Home button.

To navigate back to the chapter's menu, click on the Menu button.

To access related videos from the Customer Portal, connect to your account and click on the Play button.

Some elements can be interacted with by clicking on options, hovering over images or typing in the reserved space.

By the end of this course, you will be able to complete the following objectives:

- **Understand basic concepts**
- **Follow a recommended workflow**
- **Implement training simulations**
- **Manage and add Playbooks**

2. Introduction

Active AI Security Platform

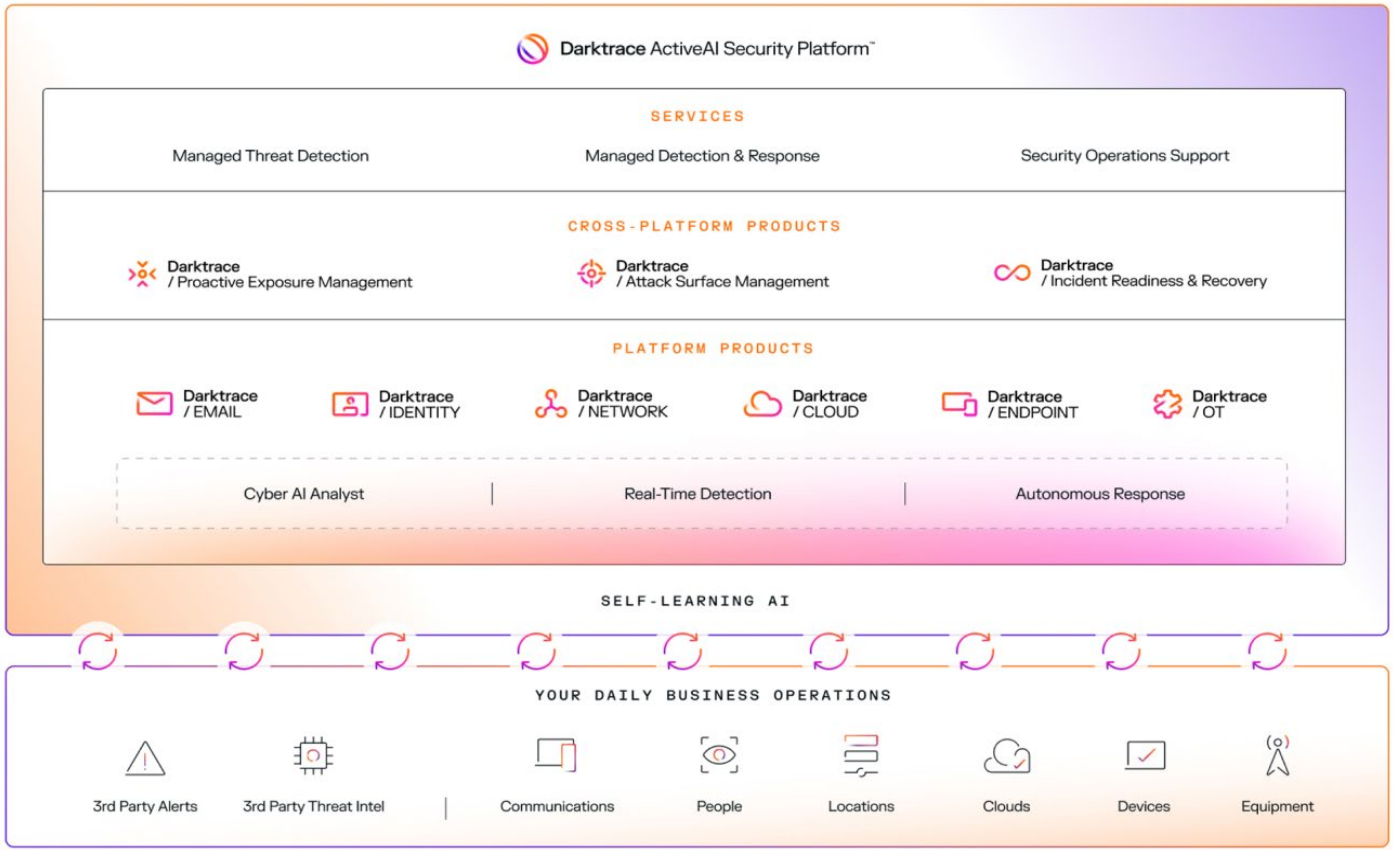
The ActiveAI Security Platform understands your enterprise data in real time to deliver preventive and live threat detection, with targeted autonomous response to shut down known and novel threats without disrupting business operations.

Proactive. Intelligent. Dynamic.

ActiveAI Security is our philosophy for the role we believe AI must play to successfully mitigate cyber risk. It embodies an intelligent, dynamic use of AI, that adapts to the environment, the threat landscape and your business. It allows defenders to remain ahead of their adversaries.

Unprecedented visibility of all threats across your enterprise

Darktrace AI ingests business data from all enterprise native and third-party sources to give you a complete view of your security posture and incidents as they occur.



Darktrace/Incident Readiness & Recovery

Get back up and Running

Darktrace Incident Readiness & Recovery uses AI to understand your business data to ensure readiness to recover from an active cyber-attack and to rapidly restore the business to an operational state. Incident Readiness & Recovery uses Darktrace's existing understanding of you – every device and communication – to establish: how ready are you for a cyber-attack? In the wake of an incident, Darktrace Incident Readiness & Recovery communicates its findings to the rest of the ecosystem, and affected assets are more closely monitored for a period of time.

Prerequisites

Before embarking on the Darktrace Incident Readiness & Recovery course, it is imperative that you have completed the appropriate prerequisites. A basic knowledge of the Threat Visualizer interface is necessary for understanding Darktrace Incident Readiness & Recovery as well as any other products licensed on your environment.

You should have already attended the relevant courses and therefore be familiar with the following topics:

Darktrace/Proactive Exposure Management

- Understanding your top critical paths
- Engaging an attack path to evaluate the risks
- Using mitigations, techniques and APTs to lower risks
- Searching for specific queries
- Applying settings suitable to your organization

Threat Visualizer Part 1 - Familiarization

- Darktrace and its available solutions
- Navigating the Threat Visualizer Interface
- Obtaining basic information about network devices
- Investigating Cyber AI Analyst incidents
- Generating reports of network activity

Threat Visualizer Part 2 - Investigation

- General analytical workflows
- AI Analyst
- Advanced Search fundamentals
- Creating Packet Captures
- Triaging alerts and assist with Security Operations

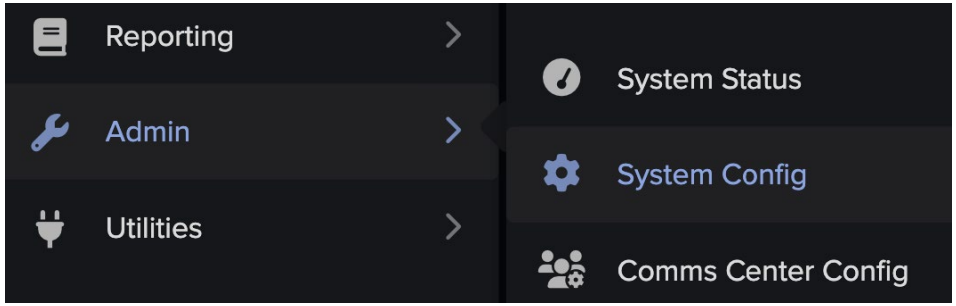
Darktrace RESPOND/Network

- Understanding the Darktrace RESPOND basic concepts
- Configuring Darktrace RESPOND options
- Handling actions raised by Darktrace
- Understanding Darktrace RESPOND/Network Models
- Tagging devices for monitoring
- Implementing recommended RESPOND quick set-up options

Licensing and Permissions

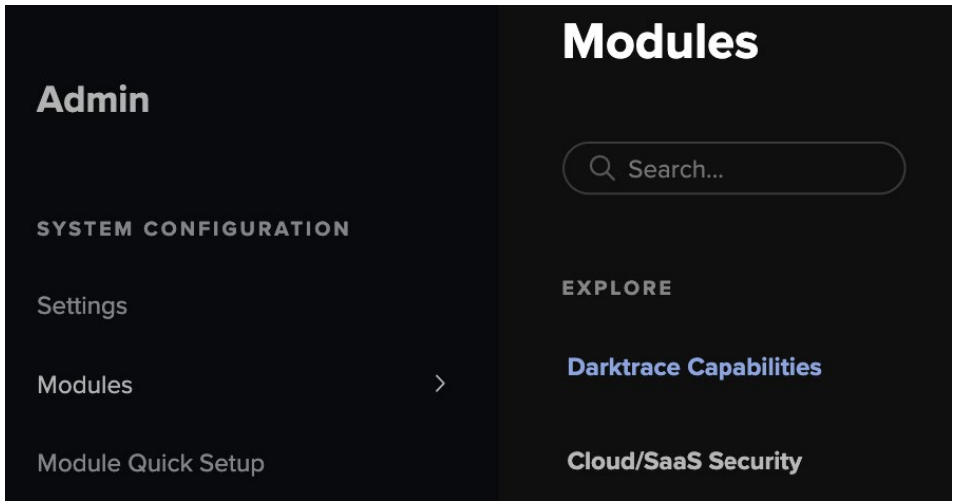
In order to enable Darktrace Incident Readiness & Recovery, make sure you are on version 6.1+ and input the appropriate license keys into the Darktrace System Config page.

1. Navigate to the **System Config** page, which is located under the Admin section of the Threat Visualizer main menu.

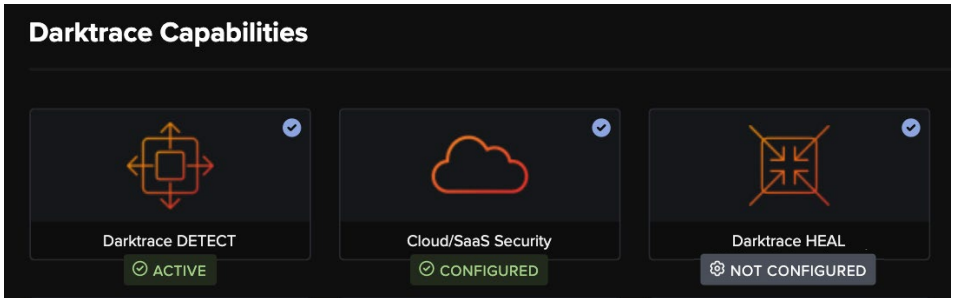


2. Once the System Config page has opened in a new tab, click on the **Modules** menu located on the left-hand side of the screen.

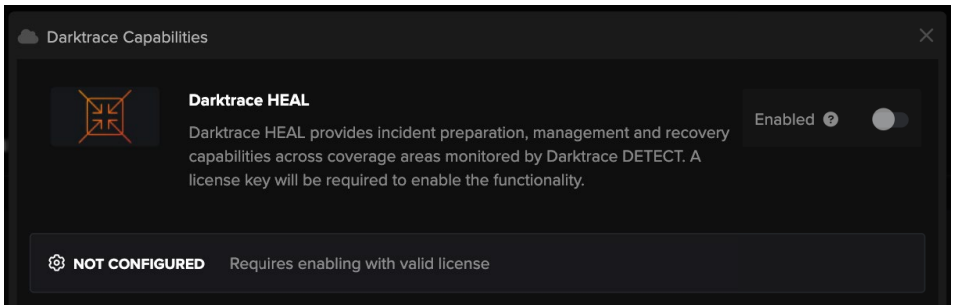
   Within the Modules page, under Explore, click on **Darktrace Capabilities**.



3. From the available applications, choose **Darktrace HEAL**.



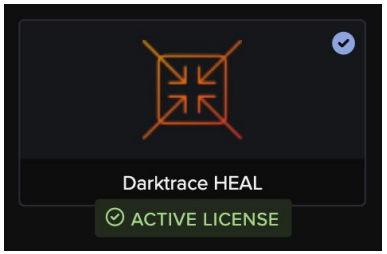
4. A new window will open. Ensure that the Darktrace HEAL **toggle is enabled**.



5. Further down this window, paste your **Heal License key**, as supplied by Darktrace Support, into the relevant text field.

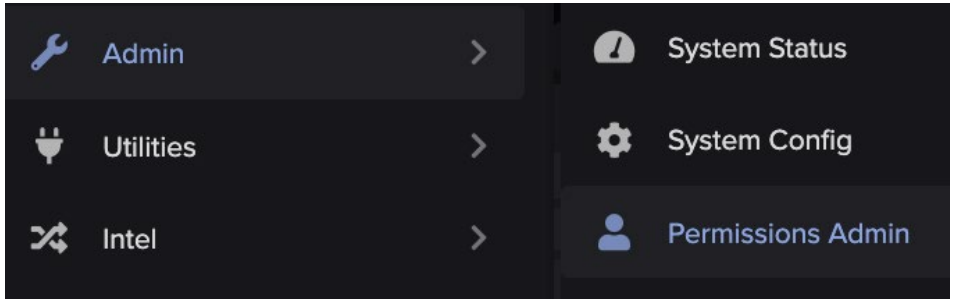
6. At this point, **save** these changes using the button that appears at the top of the window.

7. Refreshing the page, the app should now read **Active License**. Success messages are displayed within the application window and access to Darktrace Incident Readiness & Recovery granted in the Threat Visualizer main menu.

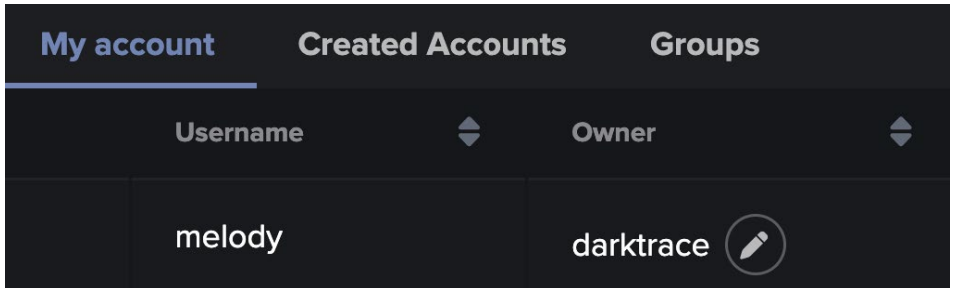


To grant access for users with the Threat Visualizer, permissions must be assigned in the Permissions Admin page.

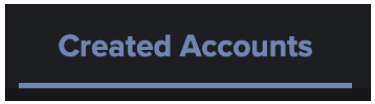
1. From the Threat Visualizer main menu, navigate to the **Admin** section of the menu and select the **Permissions Admin** option.



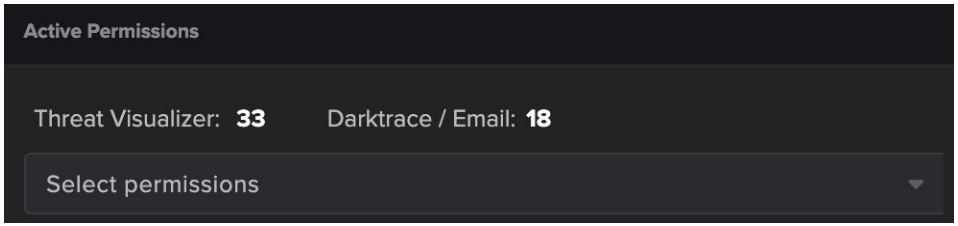
2. The Permissions Admin page will open on your account, highlighting the **My account** tab. This page displays information on your account, such as groups, permissions and restrictions.



3. The owner of the account is able to modify the user's permissions and restrictions. To do so, navigate to the **Created Accounts** tab and locate the account you wish to modify.



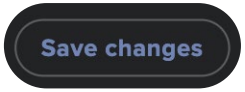
4. Clicking on the downward arrow on the **Active Permissions** column will expand a selection of permission which you can choose from. These allow access to different features of Darktrace Incident Readiness & Recovery.



5. More information about individual permission can be found in the table of **permissions** below.

NAME	DESCRIPTION	ADVISED USER LEVEL
Activate HEAL Actions	Allows the user to start automatic HEAL actions, which generally operate third-party tools affecting assets with a wide variety of active capabilities	Administrator / Analyst
Darktrace HEAL	Enables the user to view HEAL actions on devices	Administrator / Analyst
Darktrace Incident Interface	Allows the user to view and operate the Darktrace Incident Interface	Administrator / Analyst
Manage HEAL Playbooks	Allows the user to create and modify HEAL playbooks	Administrator
Manage Simulated Incidents	Allows the user to configure, schedule and delete Simulated Incidents	Administrator

6. Once you have added the desired permissions, click on **Save Changes** to save them.



3. Basic Concepts

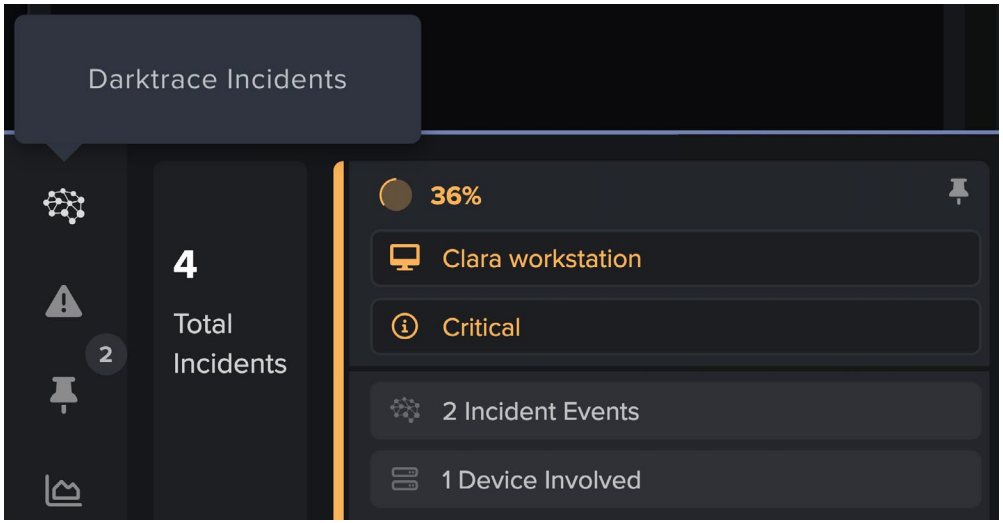
In this chapter, we will explore the various functionalities that the new Darktrace Incident tray offers, such as the Summary, Event, Interaction and Asset pages, linked to Darktrace product families: PREVENT, DETECT, RESPOND and HEAL.

Continue your learning with our dedicated video 2: Summary tab and Incident details

Darktrace Incident Tray

When logging in, Darktrace Incidents should be the first thing to be reviewed. The information it provides can be useful for quickly reviewing network anomalies or can be an excellent starting point for deep diving into activity.

From the Threat Tray, click on **Darktrace Incident** to open the incidents and use Darktrace Incident Readiness & Recovery features.

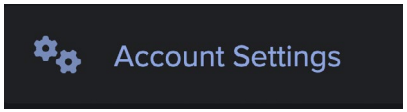


Note: The Cyber AI Incidents tray will be replaced with Darktrace Incidents which will include HEAL features.

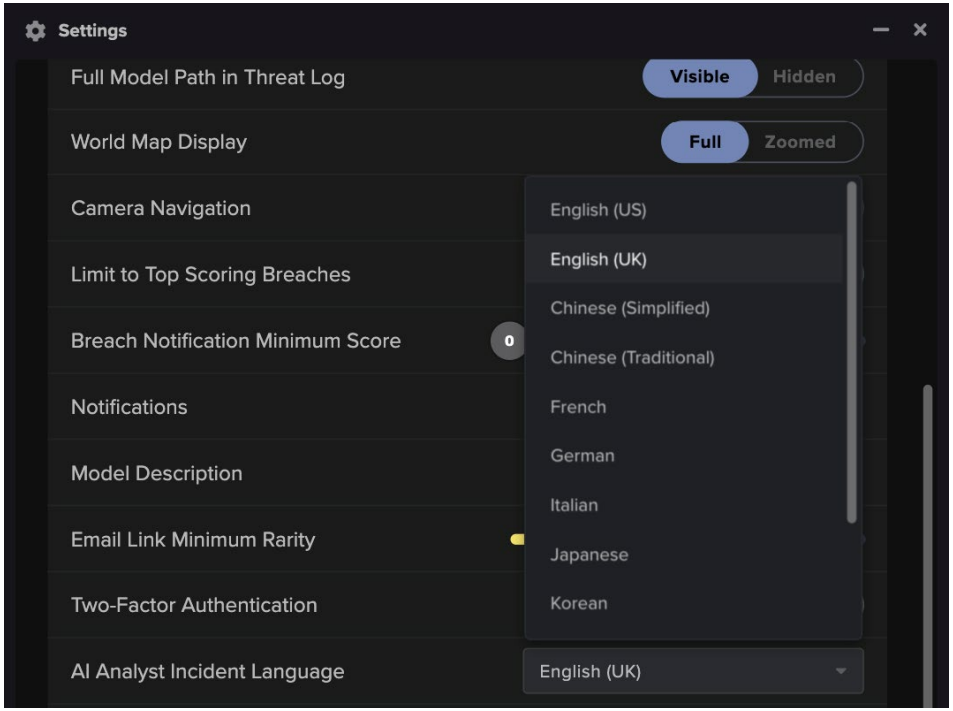
Language

Before reviewing Darktrace incidents, it is useful to return to the Account Settings and ensure that the language settings reflect the user's preferences.

1. From the Threat Visualizer main menu, open the **Account Settings** and locate the **AI Analyst Incident Language** row.



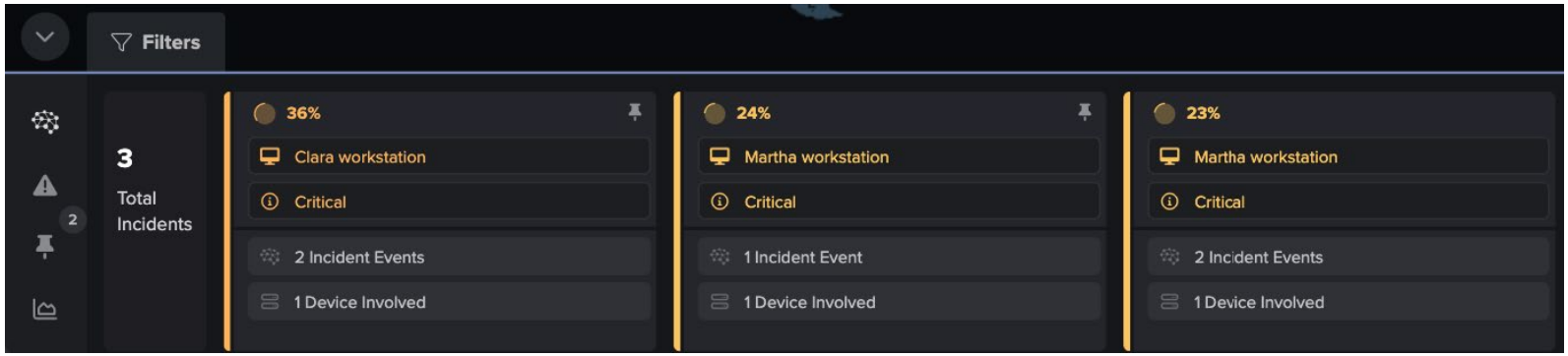
2. Click the drop-down menu to display the array of **language** options to select a **language**. *Options include: English (US), English (UK), Chinese (Simplified), Chinese (Traditional), French, German, Italian, Japanese, Korean, Portuguese (BR), Spanish (ES) and Spanish (Latin American).*



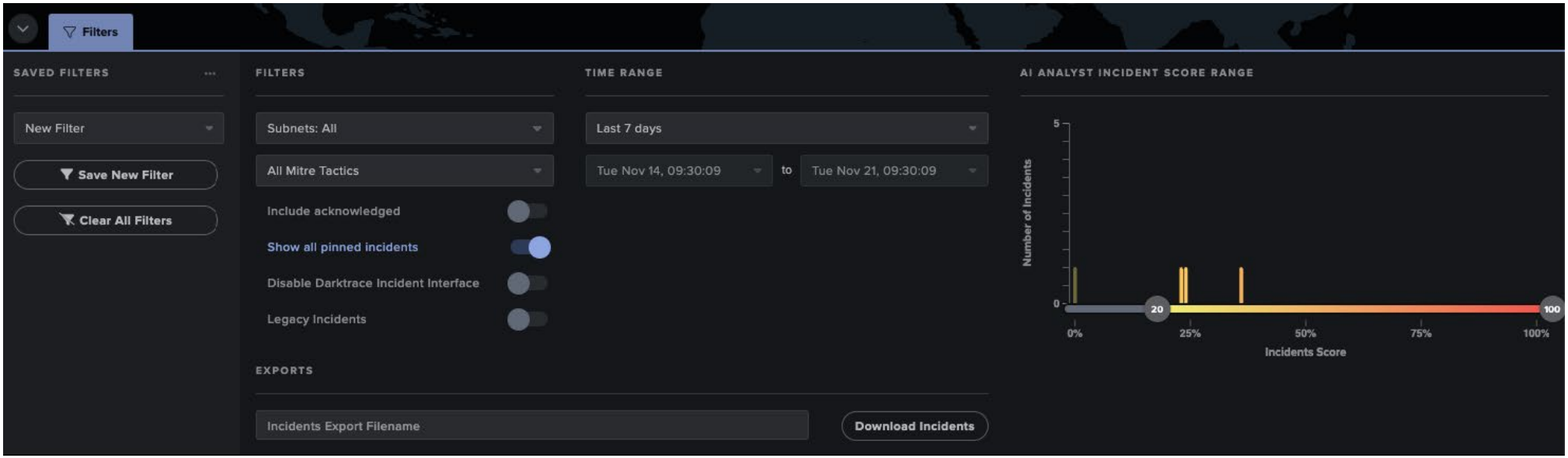
3. Open the **Darktrace Incidents Threat Tray** along the bottom of the Threat Visualizer. Incidents should now be presented in the selected language.

Filters

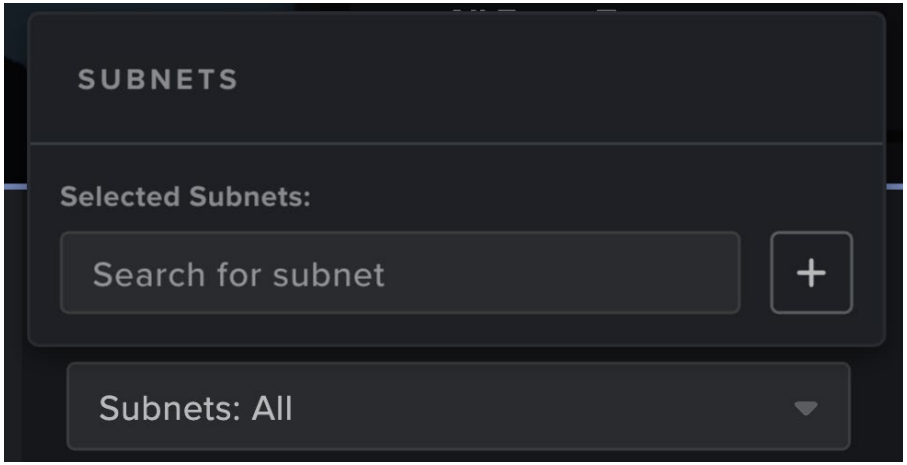
1. The **Darktrace Incident Tray** is displayed along the bottom of the Threat Visualizer interface. This can be selected by clicking on the brain icon on the left.



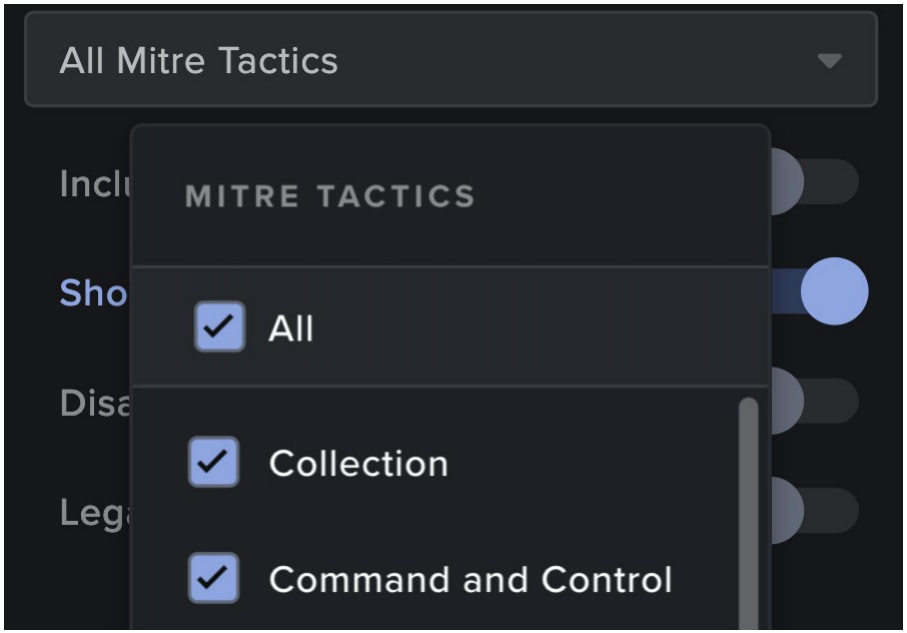
2. Before selecting any incidents, notice the Threat Tray **filters**. As a good starting point, the defaults of the **Last 7 days** and the score above **20%** should display an interesting array of incidents.



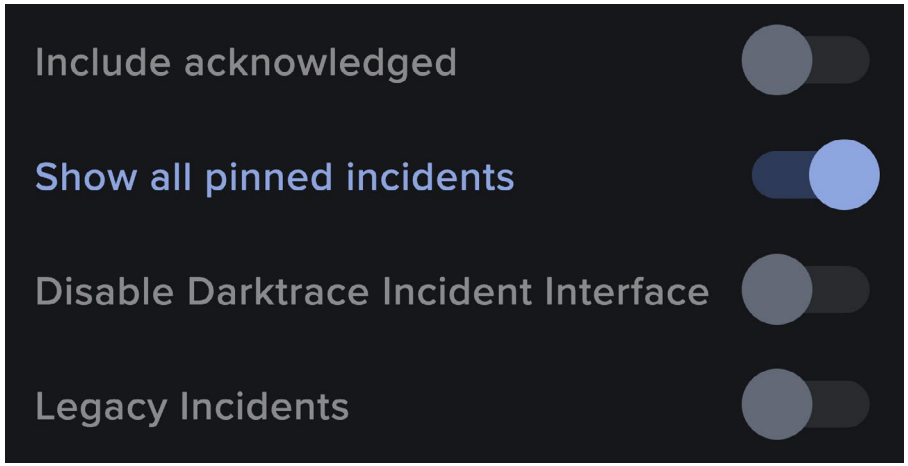
a. Under the Filters heading, notice the first drop-down - **Subnets**. This focuses the Darktrace Incidents Threat Tray on device incidents in the selected subnets.



b. Incidents can be filtered by **Mitre Att&ck Tactics**, by selecting single, multiple, or all tactics.

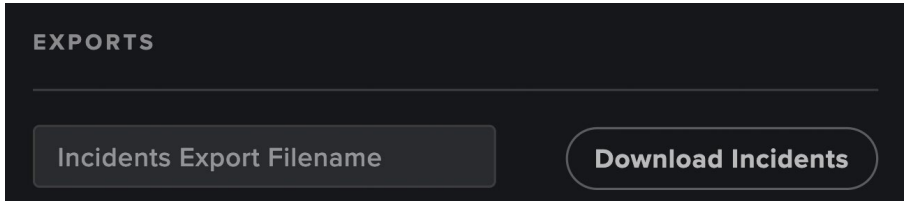


c. Next, the Darktrace Incidents Tray can be filtered using four toggles: **Include acknowledged, Show all pinned incidents**, **Disable Darktrace Incident Interface** or **Legacy Incidents**.

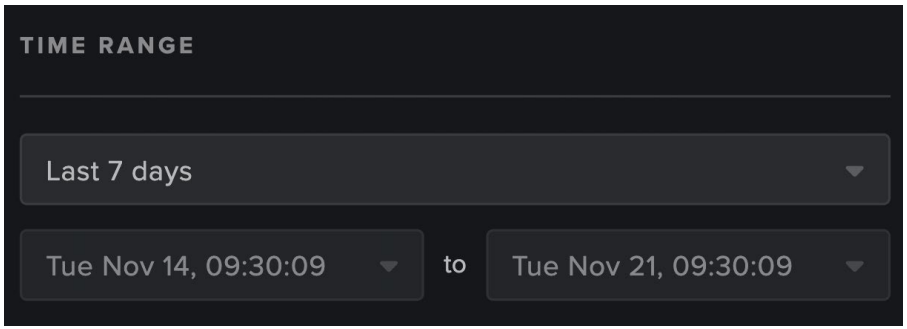


Note: Turning the Disable Darktrace Incident Interface toggle on will show the standard AI Analyst interface.

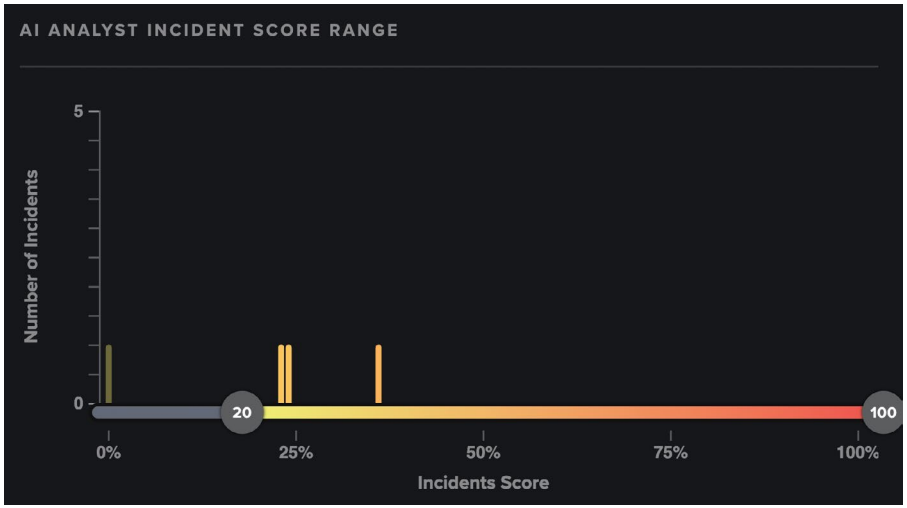
d. Incidents can also be exported as a PDF document by inputting its name in the **Exports** section and clicking on **Download Incidents**.



b. Moving across to the right, the **Time Range** section allows the Darktrace Incidents Tray to display incidents over a selected time frame.

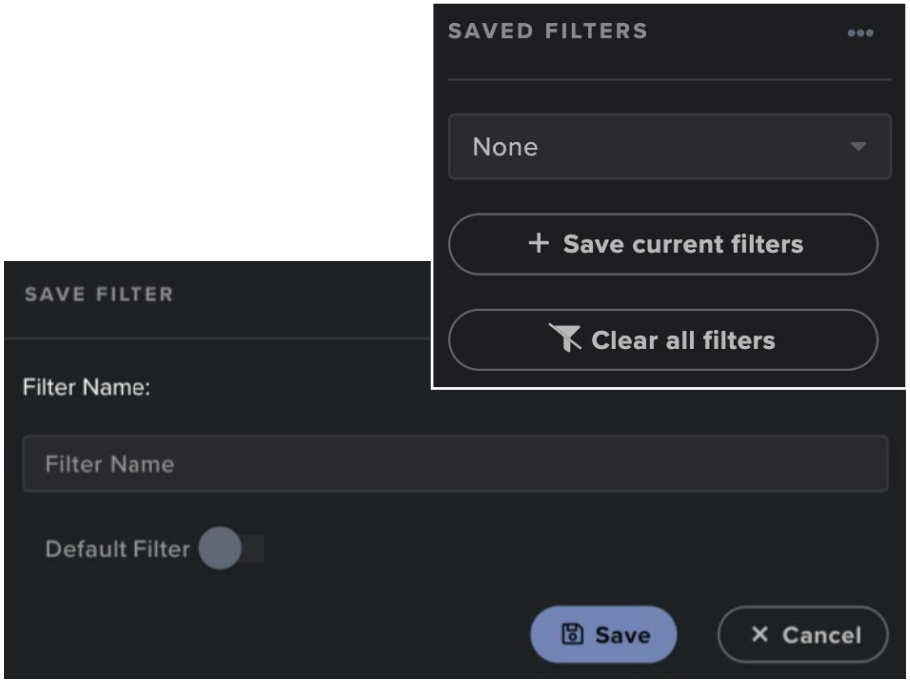


c. Finally, notice the **AI Analyst Incident Score Range**. This slider shows the number of incidents plotted against their score.



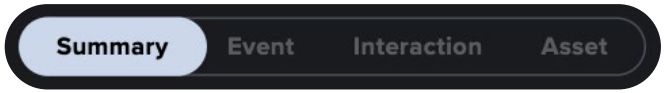
Note: The default slider will be set between 20% and 100%. This feature will be reset if the browser is refreshed.

d. When the filters are in a suitable configuration, they can be saved. Click the **Save current filters** button, give it a name and, set to default, if desired.



2. Click on any Darktrace incident to open the **Incident** window. This window will display a range of information, split into different sections.

a. The **Incident Timeline** is composed of four different tabs: Summary, Event, Interaction and Asset.



b. The **Incident Details** are composed of four different tabs, representing Darktrace product families: PREVENT, DETECT, RESPOND and HEAL.

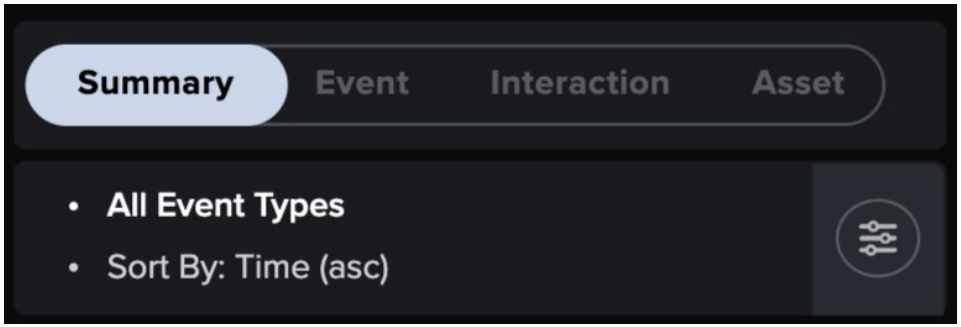
Note: Clicking on any of the Incident Timeline tabs will impact the information available from the Incident Details section.

c. The **Incident Graph** and **Further Options** sections allow more interactivity with the selected incident.

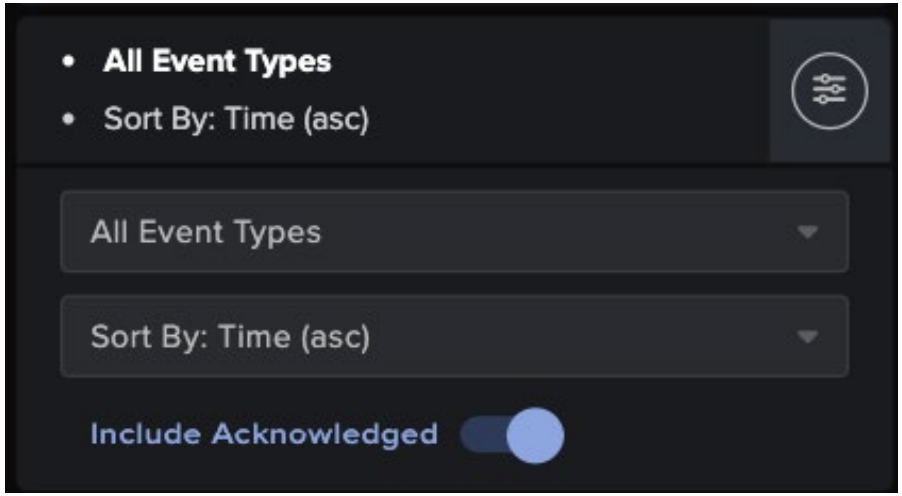
Summary

The **Summary** tab will display summarized information about the whole Darktrace incident.

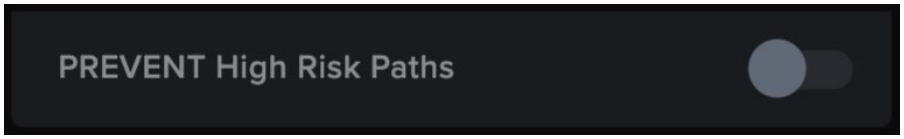
1. On the left-hand side of the Darktrace Incident window, the **Summary tab** is opened by default, dispaying a list of events related to the incident.



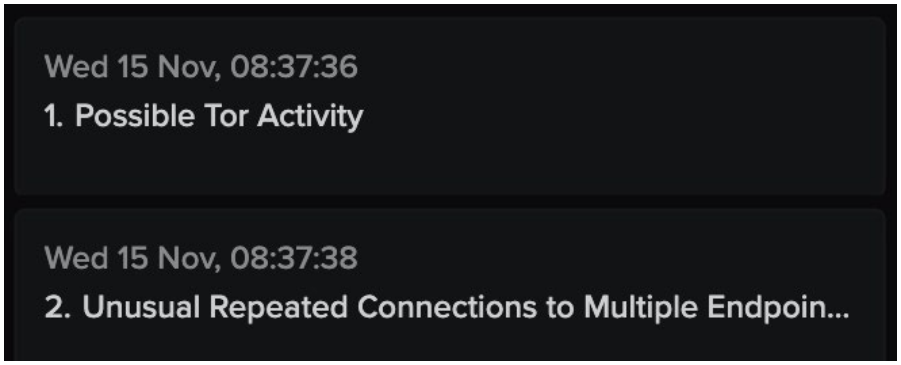
a. Click on the **filter button** to expand the filter options. Users will have the options to filter on specific **Event Types**, to **Sort by** time ascending, descending or Event Score and to **Include Acknowledged** events.



b. If any **PREVENT High Risk Paths** are part of the selected Darktrace Incident event, a toggle can be turned on to included these.

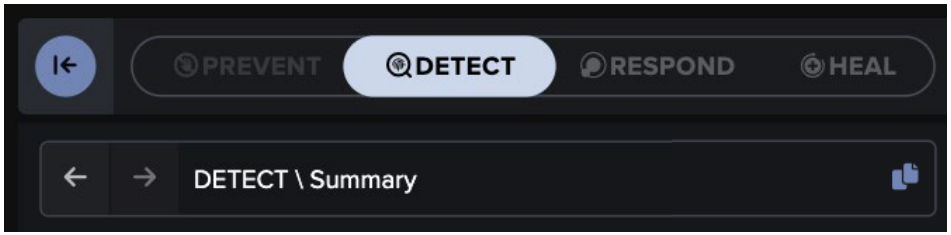


c. All **Events** will be displayed as a list underneath the filter options.



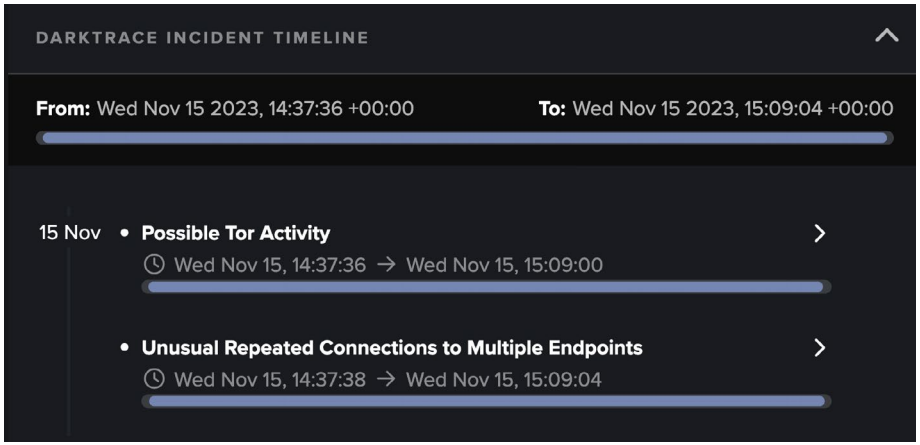
Note: Clicking on one of the event will pivot the user to the Event tab.

2. On the right-hand side of this panel, the relevant **Summary** will be available for all product families. By default, the first one to show is the **DETECT\ Summary**.



Note: The differect sections of DETECT\Summary might vary depending on the nature of the incident.

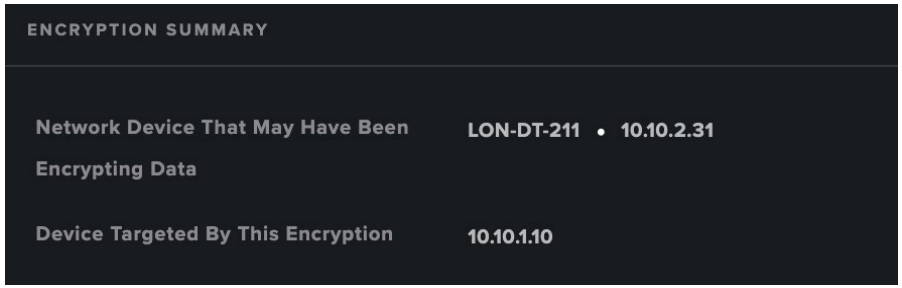
a. The first element of the DETECT\Summary section is the **Darktrace Incident Timeline** where the **duration** of each incident will be shown.



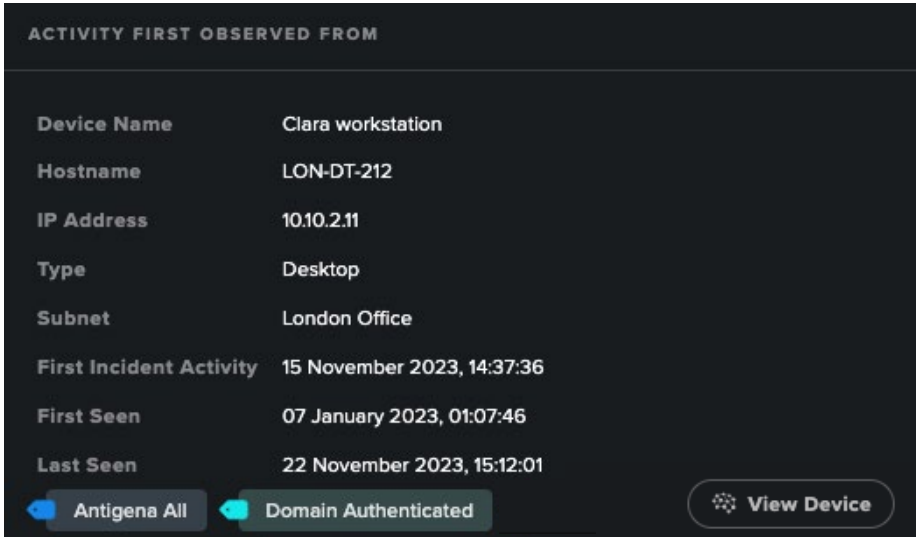
Note: Clicking on one of the activity will pivot the user to the Event tab.

b. More **technical details** of the incident will be available and can vary from one incident to another. These can be extensive and may be broken down into different relevant sections.

For example, the **Encryption Summary** can be available and will detail the device targeted by the encryption.

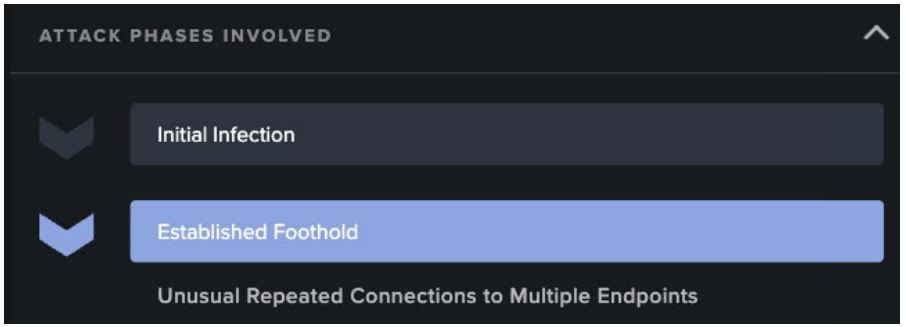


Another section which might be available is the **Activity First Observed From** section, displaying information about the offending Asset, which can be viewed in more details. Click on View Device to pivot to the Asset tab.

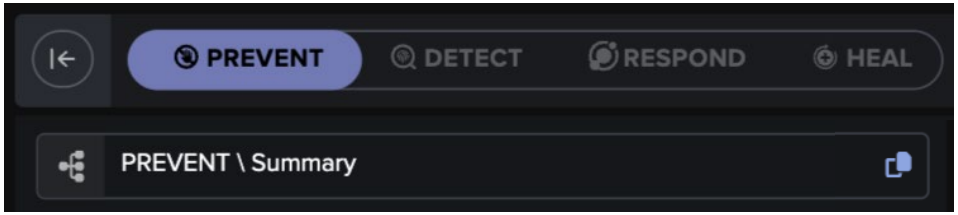


c. The **Suspicious External Communication Summary** section will detail the targeted endpoints indicating which mechanisms were used.

d. Finally, the last section will show a list of the **Attack Phases Involved**.

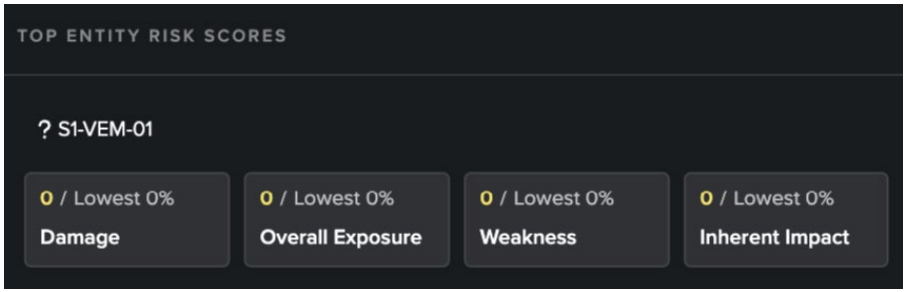


3. If Darktrace/Proactive Exposure Management is licensed, click on **PREVENT** to show the PREVENT\Summary of the selected incident.

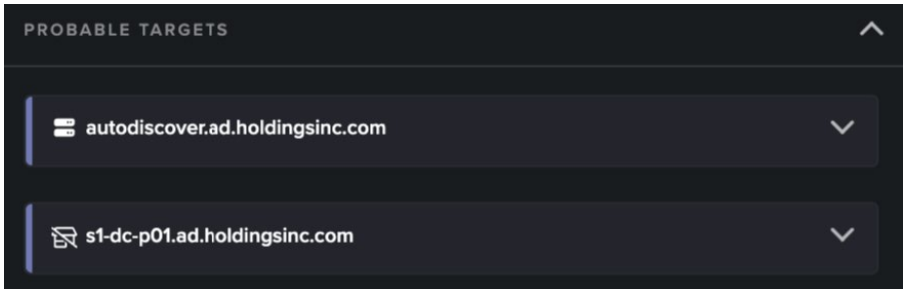


Note: The differect sections of PREVENT\Summary might vary depending on the nature of the incident.

a. The first element of the PREVENT\Summary section is the **Top Entity Risk Scores** which will display four different risk scores: Damage, Overall Exposure, Weakness and Inherent Impact.



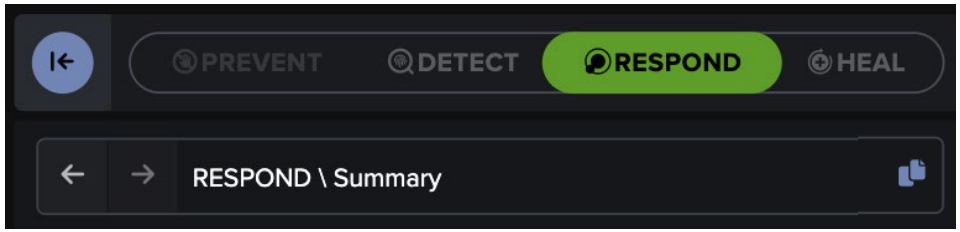
b. The **Probable Targets** section will inform users on which Assets are most likely to be targeted.



Top Tip

To learn more about Darktrace Darktrace/Proactive Exposure Management, consult our training resources and courses available on the Customer Portal.

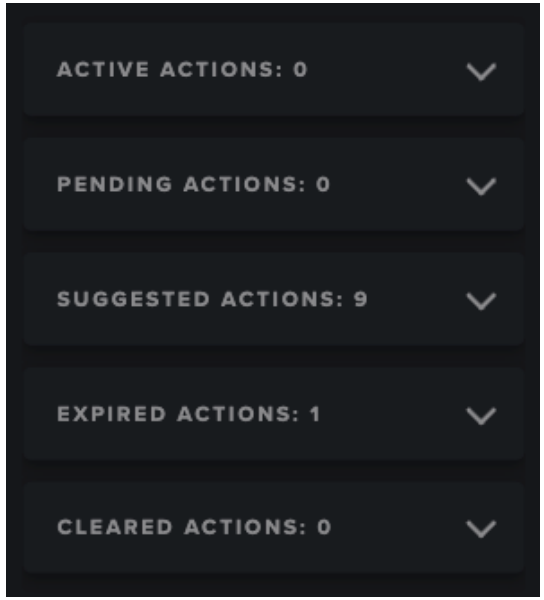
4. If licensed, click on **RESPOND** to show the RESPOND\Summary of the selected incident.



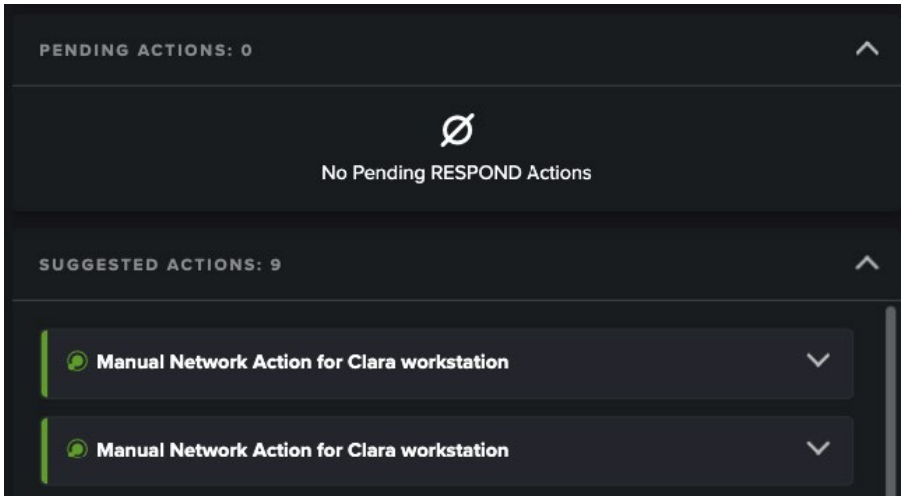
Note: The differect sections of RESPOND\Summary might vary depending on the nature of the incident.

a. There are **five tabs**, which can all be expanded for more details. The available tabs are:

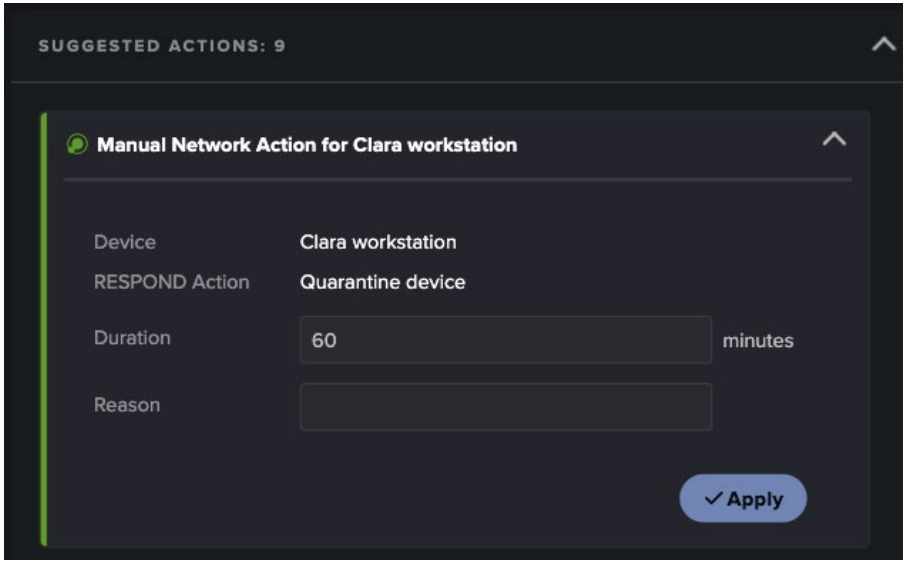
- Active Actions
- Pending Actions
- Suggested Actions
- Expired Actions
- Cleared Actions



b. Clicking on a tab **displaying a number other than 0** will display more information about the selected action.



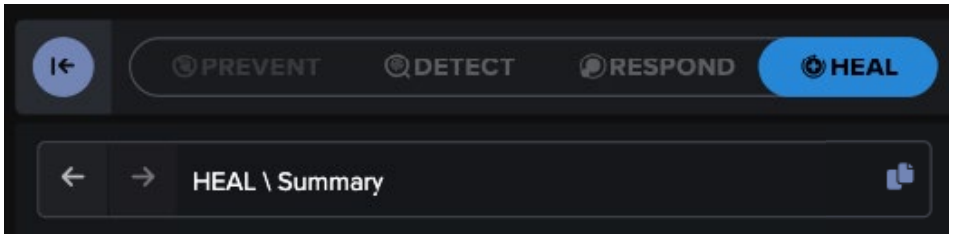
c. Actions can be interacted with by users when expanded to **Apply**, **Clear**, **Activate** or **Reactivate** the desired action. The **Duration** and **Reason** of the action can also be added.



Top Tip

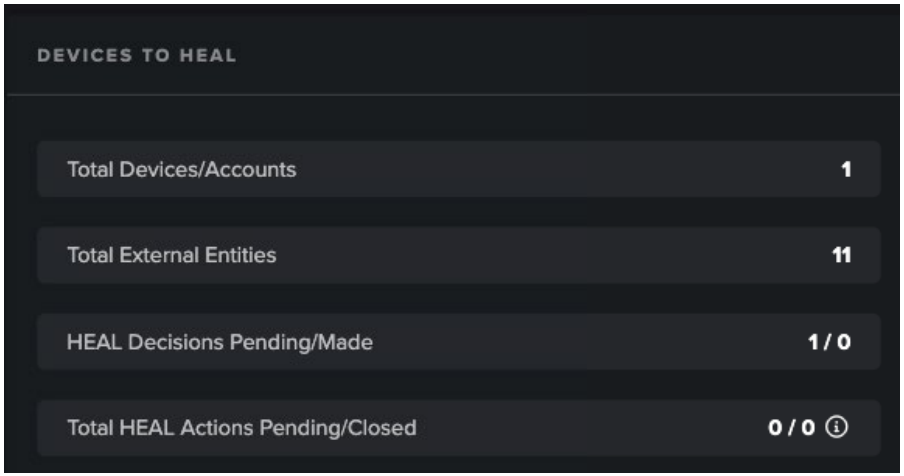
To learn more about Darktrace RESPOND/Network, consult our training resources and courses available on the Customer Portal.

5. Finally, click on **HEAL** to show the HEAL\Summary of the selected incident.

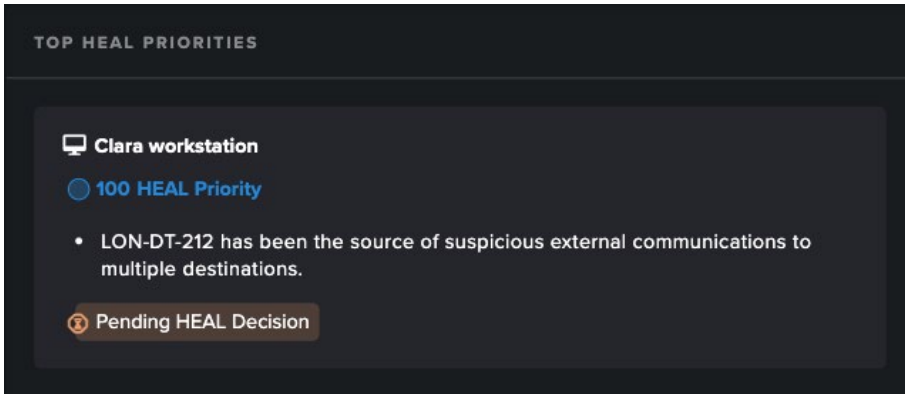


Note: The differect sections of HEAL\Summary might vary depending on the nature of the incident.

a. The **Devices to HEAL** section will display the total devices and external entities along with any pending/made decisions and pending/closed actions.



b. The **Top HEAL Priorities** section will display the devices which have a HEAL decision associated by priority, showing the Heal Priority score, a reason and a HEAL decision status.



Every device/asset involved in an Incident will have a HEAL decision associated to it.

Note: Clicking on one of the devices will pivot the user to the Asset tab.

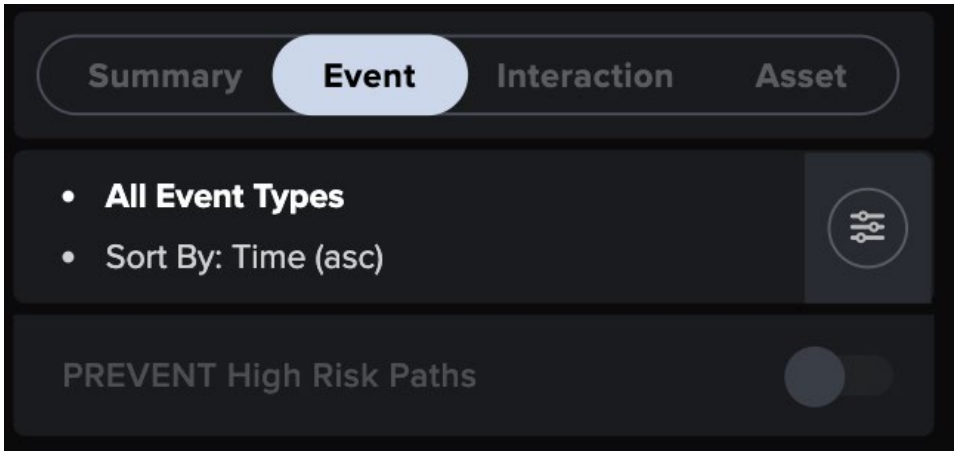
Continue your learning with our dedicated video 3: Incident Timeline Tabs

Event

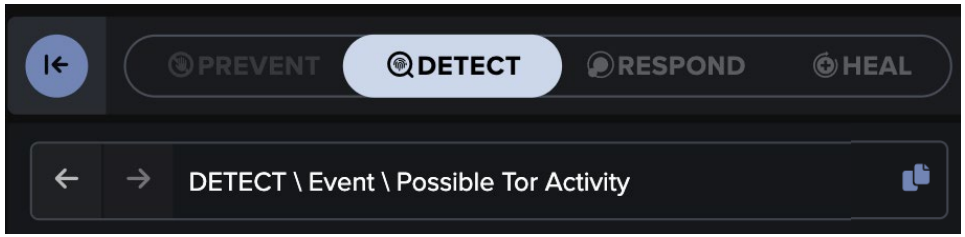
The **Event** tab will select context from high-level events described by Cyber AI Analyst.

1. Click on the **Event** tab to display a list of all events related to the incident. These can also be accessed from the Summary tab.

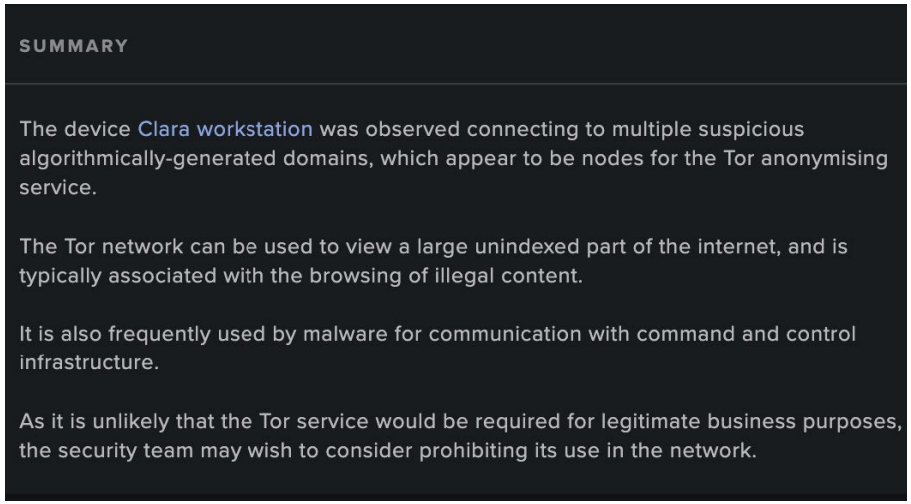
   Click on the **filter button** to expand the filter options. Users will have the options to filter on specific **Event Types**, to **Sort by** time ascending, descending or Event Score and to **Include Acknowledged** events. **PREVENT High Risk Paths** can be included vie the toggle.



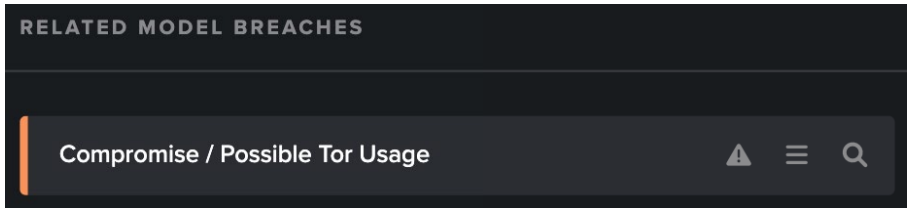
2. When selecting an event, it will be opened on the right-hand side panel, under **DETECT\Event**.



a. The first element of the DETECT\Event section is the **Summary** which is a high level event outlining the observed activity, possible implications and a suggested action which can be taken by the security team.



b. The next section is the **Related Model Breaches**, listing model breaches which are involved in the Event.

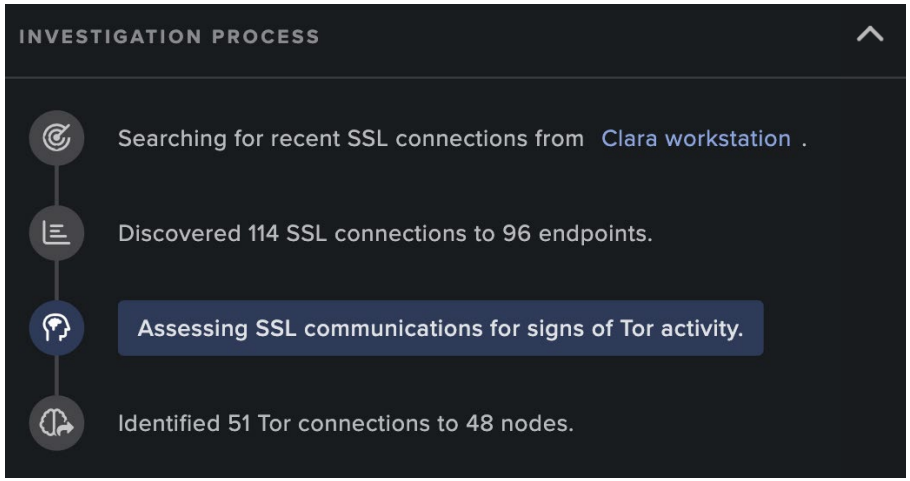


i. There are three icons on the right of each model breach, the first one being the **View Model Breach** icon, opening the corresponding Breach Log.

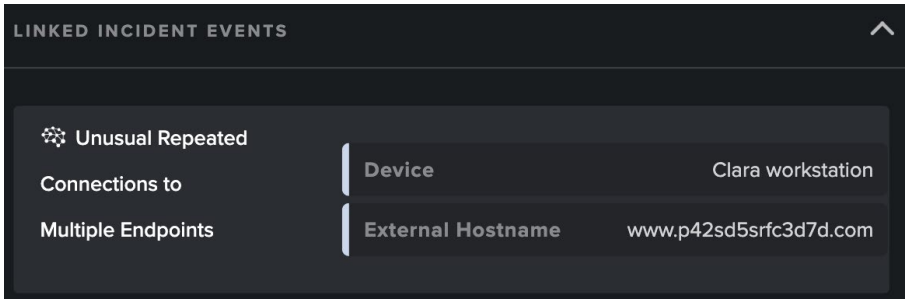
ii. The second icon is the **View Model Breach Log**, opening the corresponding Model Breach Event Log.

iii. The third icon is the **View this Model Breach** in the Visualizer, the allowing users to center the Threat Visualizer on the device at the time of the breach.

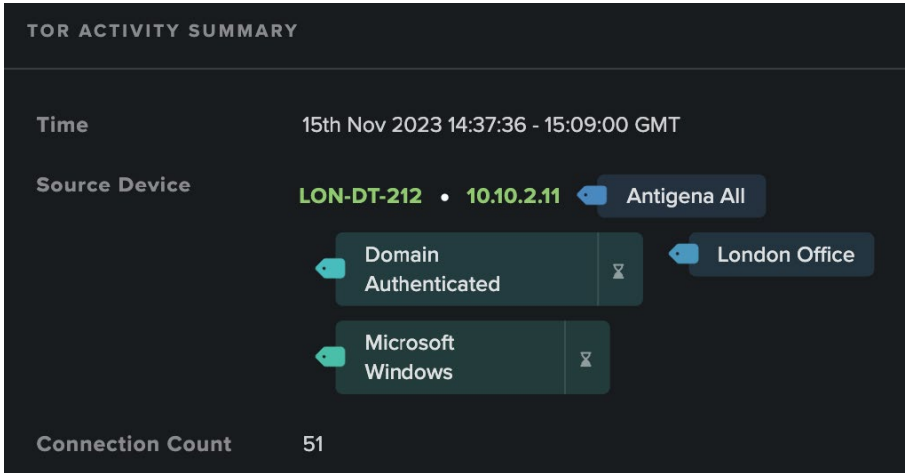
c. It can be useful to read the **Investigation Process** as an optional step. The investigation panel is collapsed by default. Upon expanding, this will display the chain of events, outlining Darktrace Incident Readiness & Recovery's thought process.



d. Any **Linked Incident Events** may be listed and can provide pivot points to other areas of an incident.



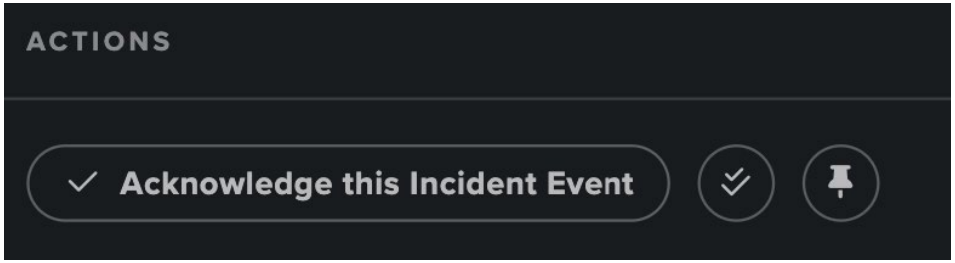
e. In order to dive into the full technical details that AI Analyst has surfaced, go to the **Incident Details** on the right of the window. These can be extensive and may be broken down into different relevant sections.



For example, if the incident includes suspicious connections, the details will outline the device in question but may also outline the application, endpoints contacted by the application and other similar endpoints.

Note: The differect sections of DETECT\Event might vary depending on the nature of the incident.

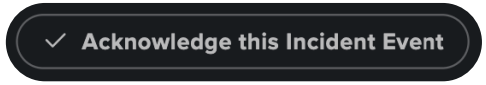
3. Once all the details have been reviewed for an individual incident event, it is possible to take **Actions** on it.



a. First, it is possible to **pin** AI Analyst incident events so they can be located at a later stage.

Note: Using this button will pin the individual tab, and not the incident as a whole.

b. The events can be **individually acknowledged**, meaning they are hidden from view.



Note: This will apply a tick at the top of the incident, indicating that this section has been acknowledged. This will not hide the whole incident.

c. Finally, after reviewing an event, **all related Model Breaches can also be acknowledged** from here in one click using the double tick icon.

Top Tip

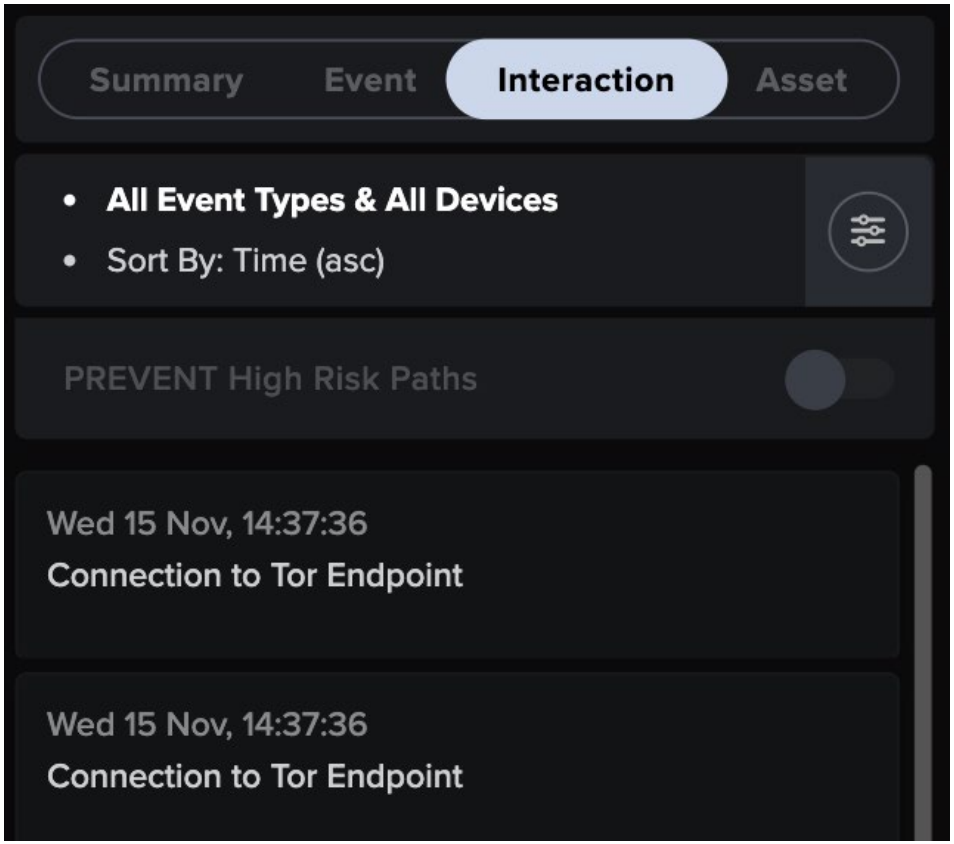
The content of the PREVENT, RESPOND and HEAL sections will not change based on the Event tab. The information from the Summary tab will still be available.

Interaction

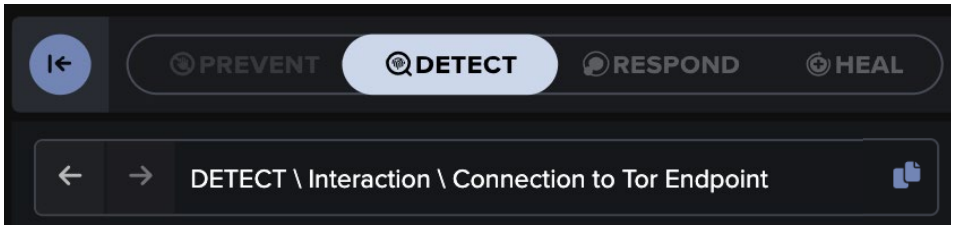
The **Interaction** tab will select context from individual interactions between assets that form part of an event.

1. Click on the **Interaction** tab to display a list of all interactions related to the incident.

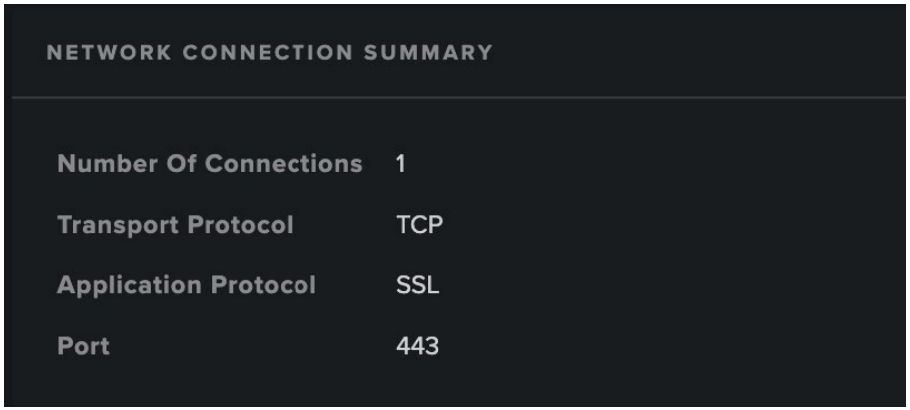
   Click on the **filter button** to expand the filter options. Users will have the options to filter on specific **Event Types** and **Devices**, and to **Sort by** time ascending, descending or Event Score.



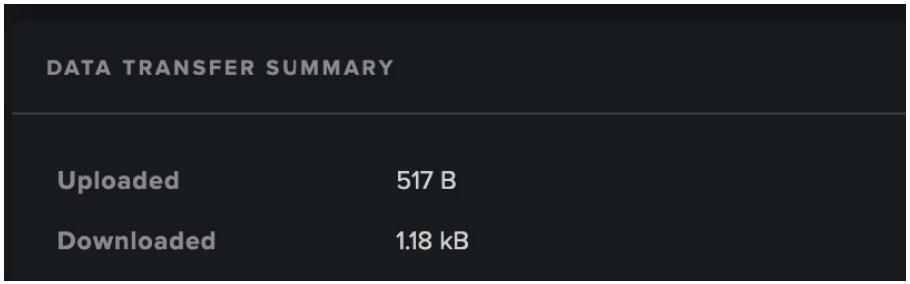
2. The selected interaction will be opened on the right-hand side panel, under **DETECT\Interaction**.



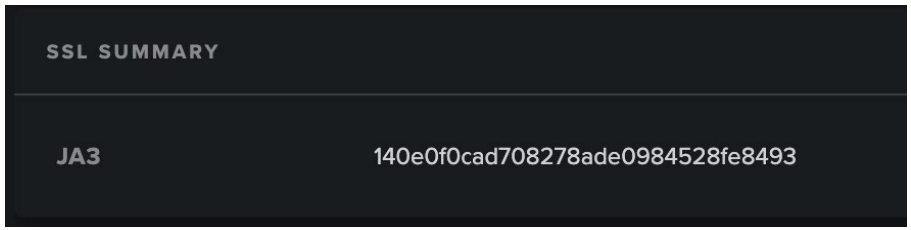
   a. The first element of the DETECT\Interaction section is the **Network Connection Summary** which outline the observed connections, including information about the protocol used.



   b. The next section is the **Data Transfer Summary**, listing uploaded and downloaded data.



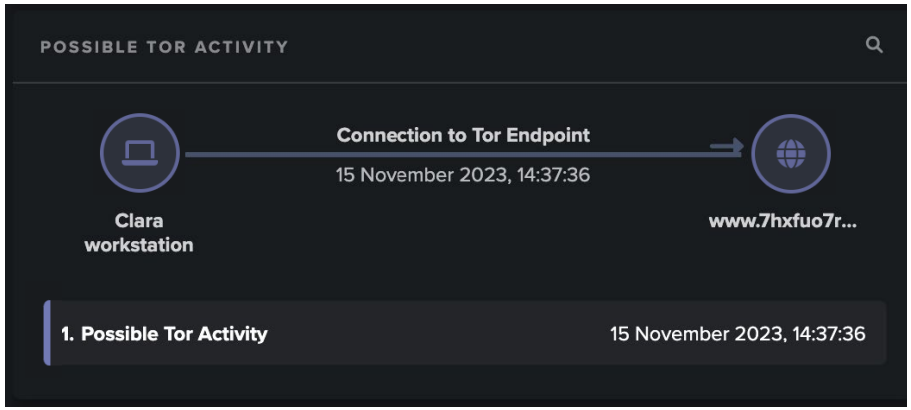
c. Next is the **SSL Summary** which will show information relating to SSL interactions.



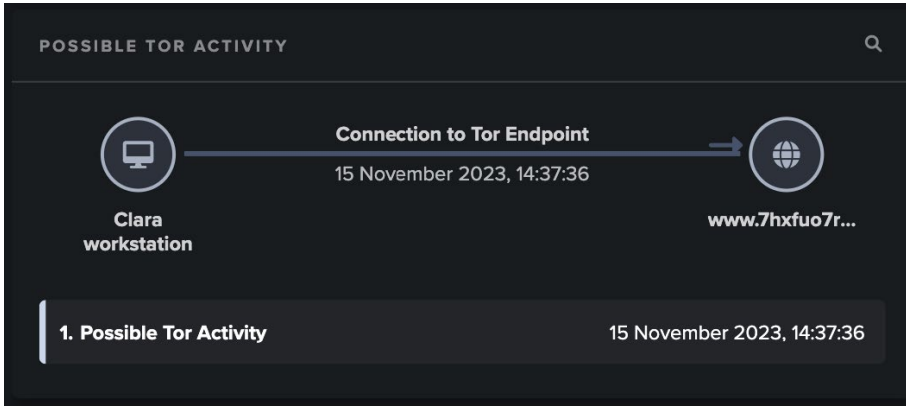
Note: The differect sections of DETECT\Interaction might vary depending on the nature of the incident.

3. The final section a **graphical representation** of the activity for the selected interaction. This section will be available for all four tabs on the right-hand side panel: PREVENT, DETECT, RESPOND and HEAL.

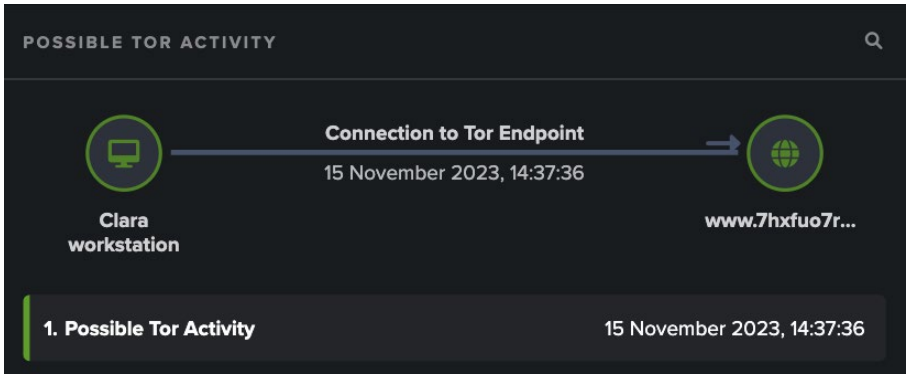
a. The graphical representation will be in **purple** within the **PREVENT** tab. Clicking on the event of this section will pivot the user to the **Event** tab, and clicking on the source device will pivot the user to the **Assets tab**.



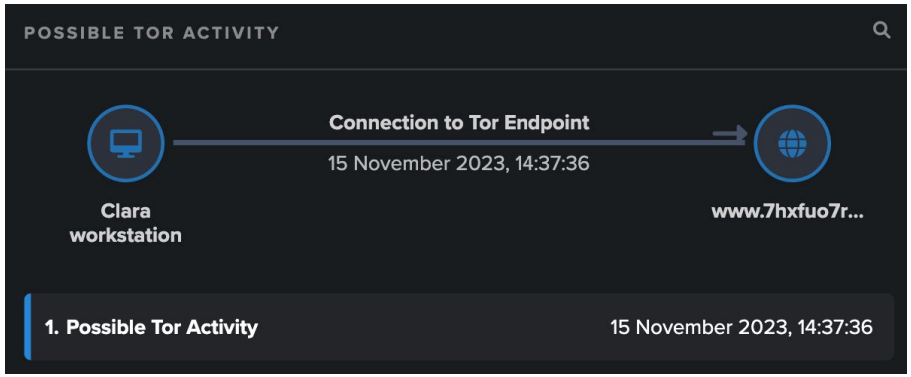
b. The graphical representation will be in **white** within the **DETECT** tab. Clicking on the event of this section will pivot the user to the **Event** tab and clicking on the source device will pivot the user to the **Assets tab**.



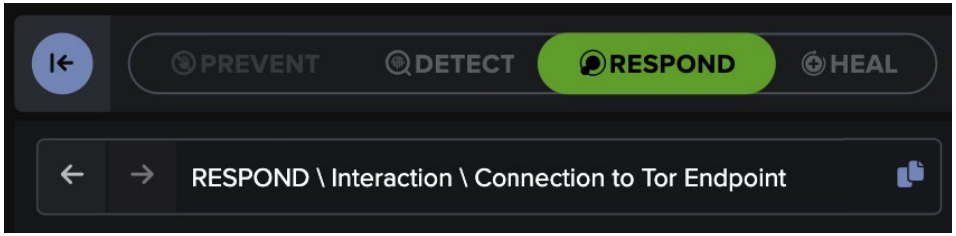
c. The graphical representation will be in **green** within the **RESPOND** tab. Clicking on the event of this section will pivot the user to the **Event** tab and clicking on the source device will pivot the user to the **Assets tab**.



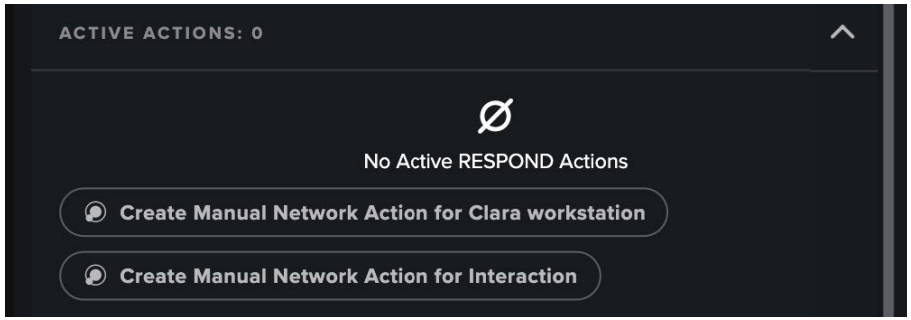
d. The graphical representation will be in **blue** within the **HEAL** tab. Clicking on the event of this section will pivot the user to the **Event** tab and clicking on the source device will pivot the user to the **Assets tab**.



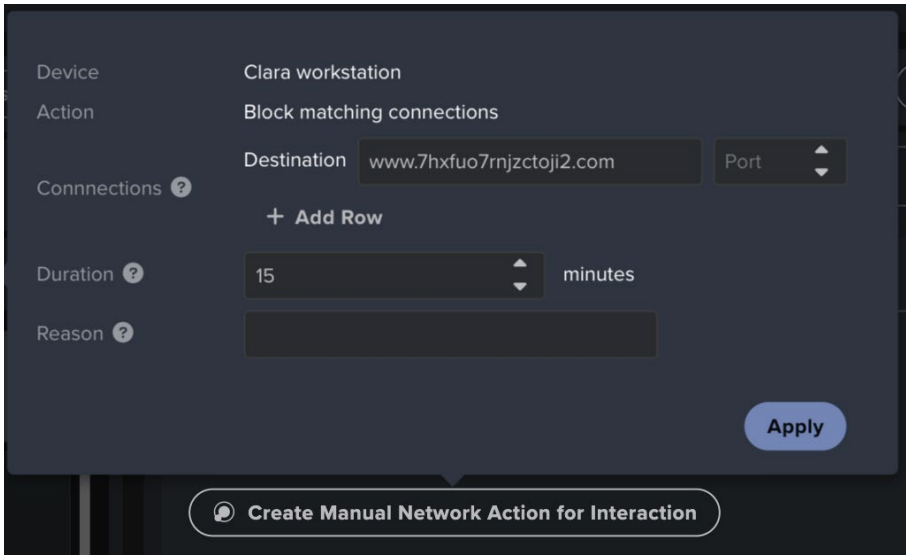
4. Finally, click on **RESPOND** to show the RESPOND\Interaction of the selected incident.



a. From the Active Actions section, users will have the additional option to click on **Create Manual Network Action for Interaction**.



b. As the RESPOND action will target the selected interaction, some fields will be pre-populated and users can choose the **Duration** as well as the **Reason** before clicking on **Apply**.



Top Tip

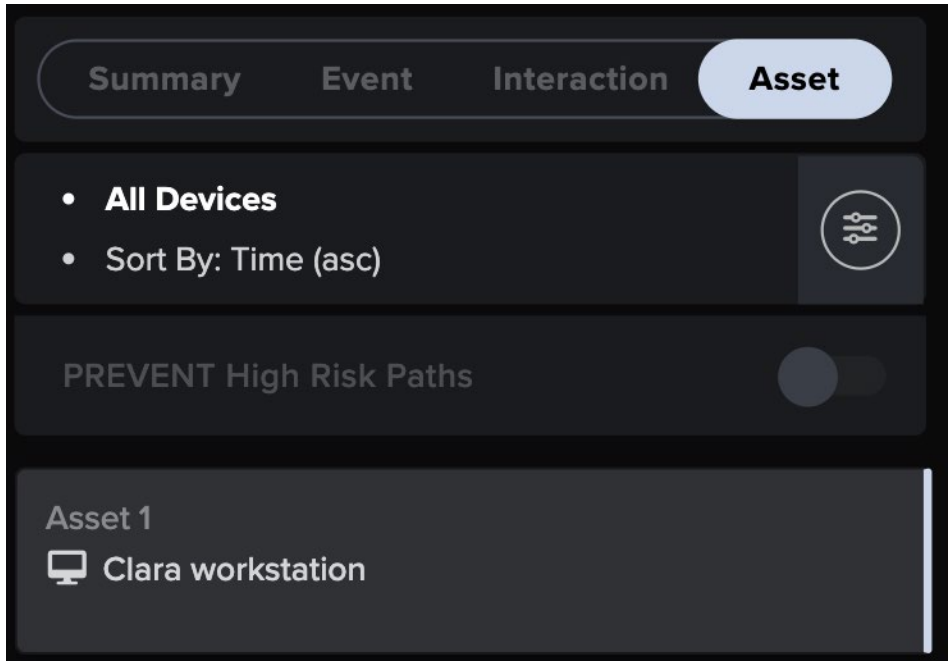
With the exception of the aforementioned options, the content of the PREVENT, RESPOND and HEAL sections will not change based on the Interaction tab. The information from the Summary tab will still be available.

Asset

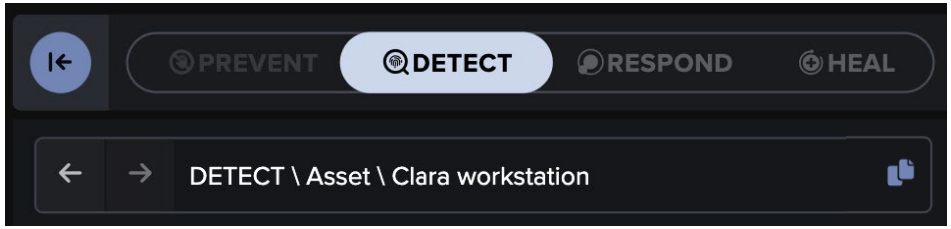
The **Asset** tab will select context from assets involved in one or more events.

1. Click on the **Asset** tab to display a list of all assets related to the incident.

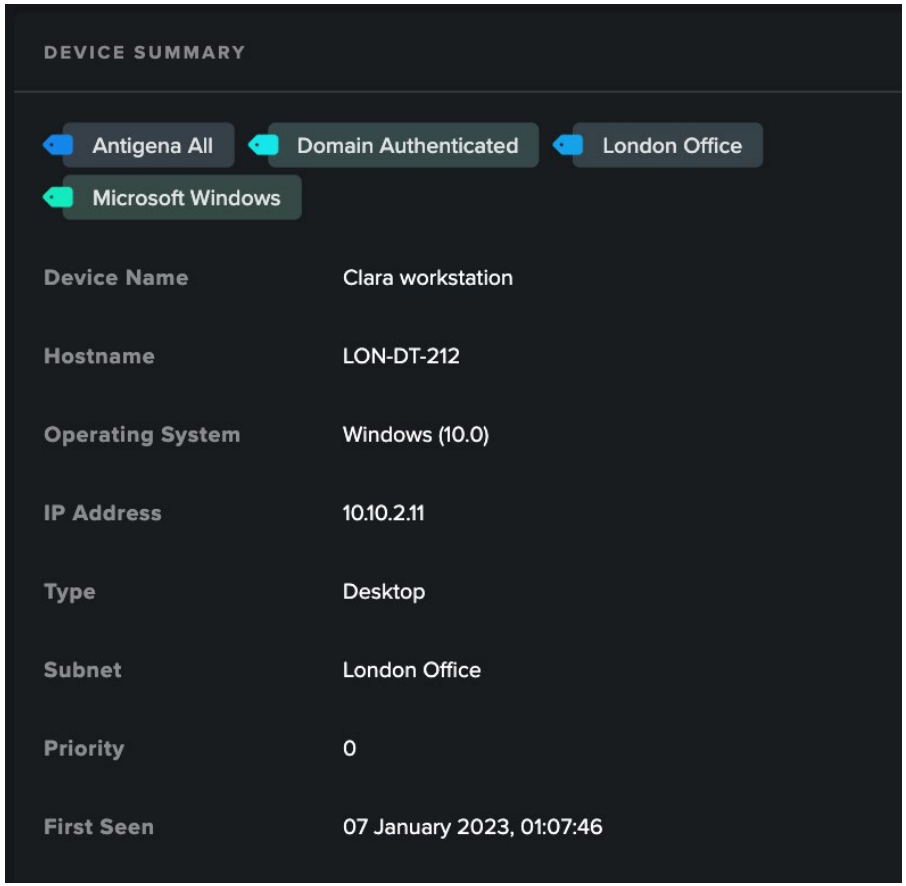
   Click on the **filter button** to expand the filter options. Users will have the options to filter on specific **Devices**, and to **Sort by** time ascending or descending.



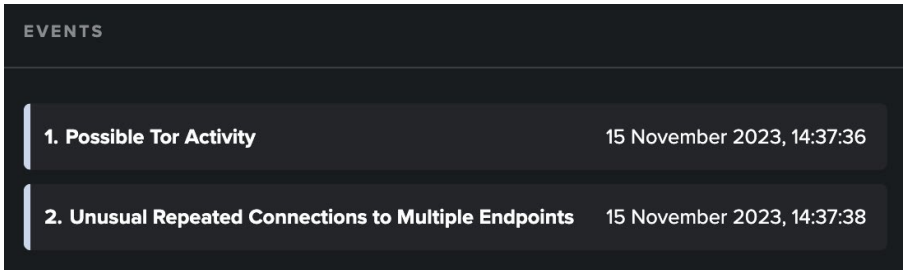
2. The selected asset will be opened on the right-hand side panel, under **DETECT\Asset**.



   a. The first element of the DETECT\Asset section is the **Device Summary** which outlines specific device information.

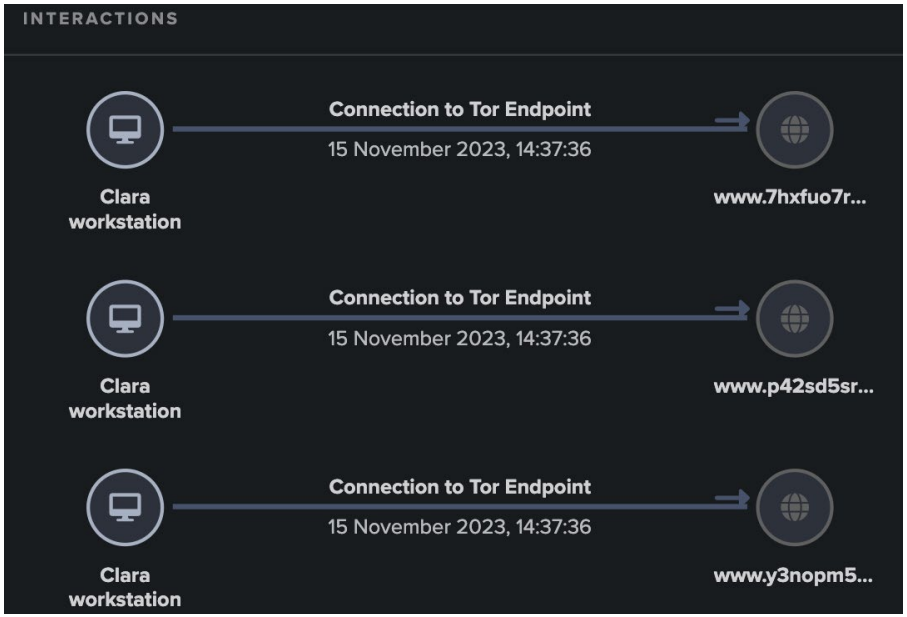


b. The next section is the **Events**, listing events related to the selected asset, including the date and time of each event.



Note: Clicking on one of the Events will pivot the user to the DETECT\ Event tab.

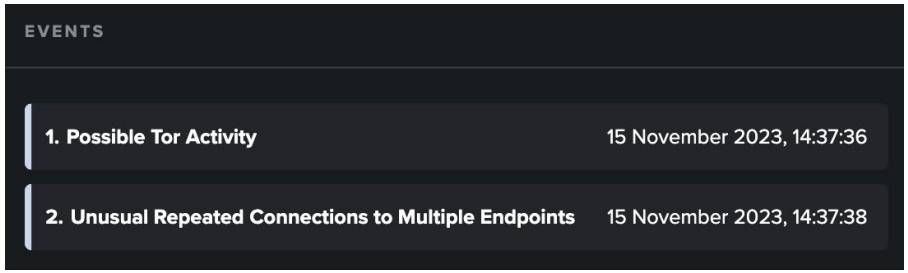
c. Next is the **Interactions** section which will show a graphical representation of all the interactions related to the selected asset.



Note: Clicking on one of the Interactions will pivot the user to the DETECT\ Interaction tab.

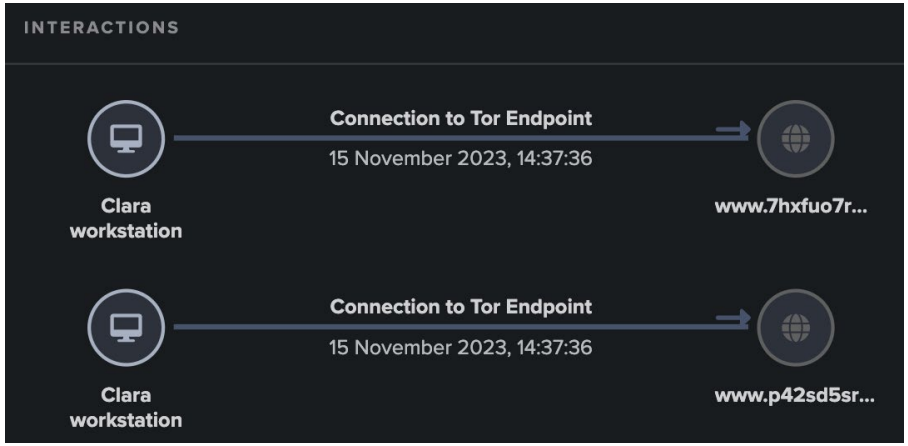
3. If Darktrace/Proactive Exposure Management is licensed, click on **PREVENT** to show the PREVENT\Asset of the selected incident.

a. There will be an additional **Events** section, listing events related to the selected asset, including the date and time of each event.



Note: Clicking on one of the Events will pivot the user to the Event tab.

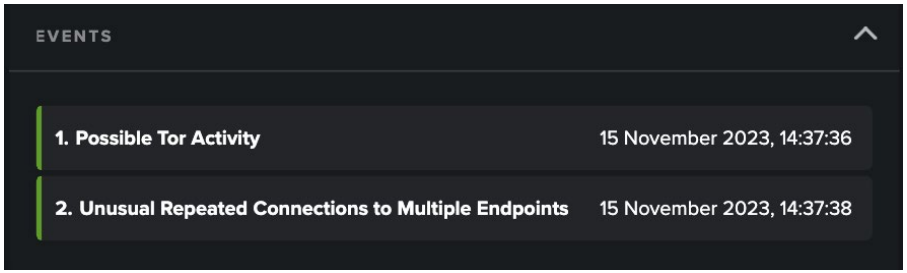
b. Next is the additional **Interactions** section which will show a graphical representation of all the interactions related to the selected asset.



Note: Clicking on one of the Interactions will pivot the user to the Interaction tab.

4. If licensed, click on **RESPOND** to show the RESPOND\Asset of the selected incident.

   a. There will be an additional **Events** section, listing events related to the selected asset, including the date and time of each event.



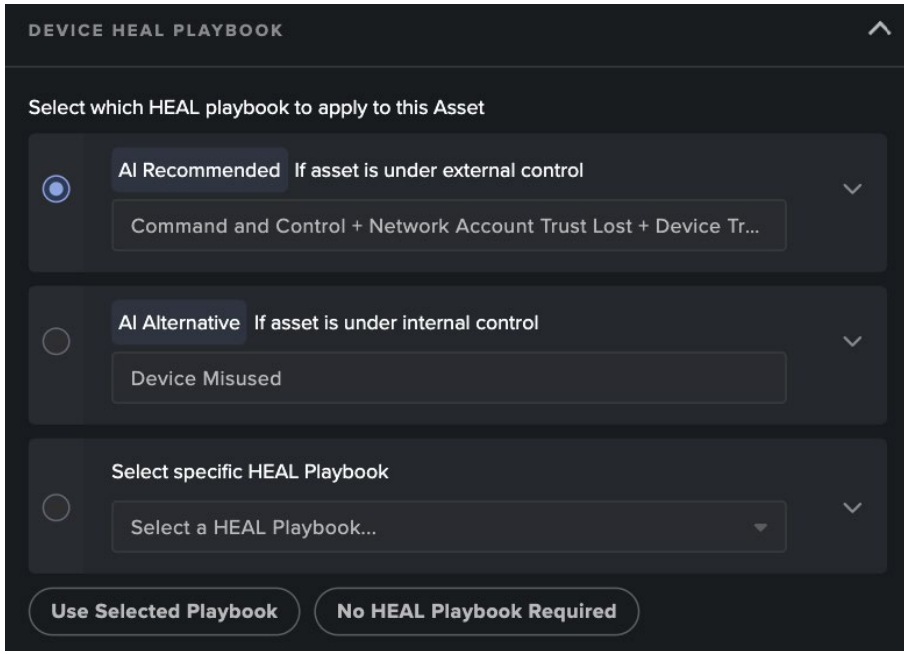
Note: Clicking on one of the Events will pivot the user to the Event tab.

   b. Next is the additional **Interactions** section which will show a graphical representation of all the interactions related to the selected asset.

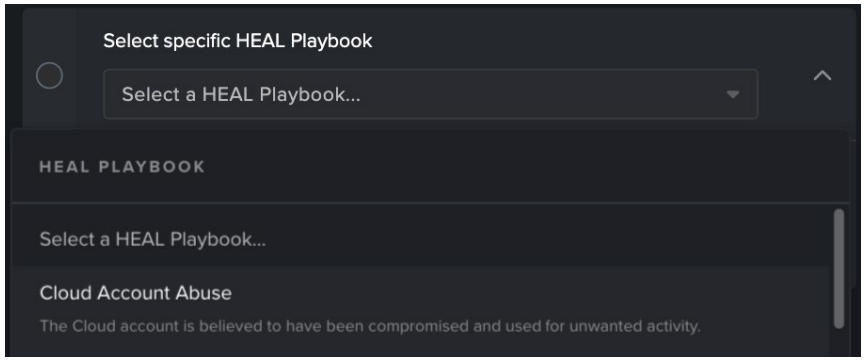
Note: Clicking on one of the Interactions will pivot the user to the Interaction tab.

5. If licensed, click on **HEAL** to show the HEAL\Asset of the selected incident.

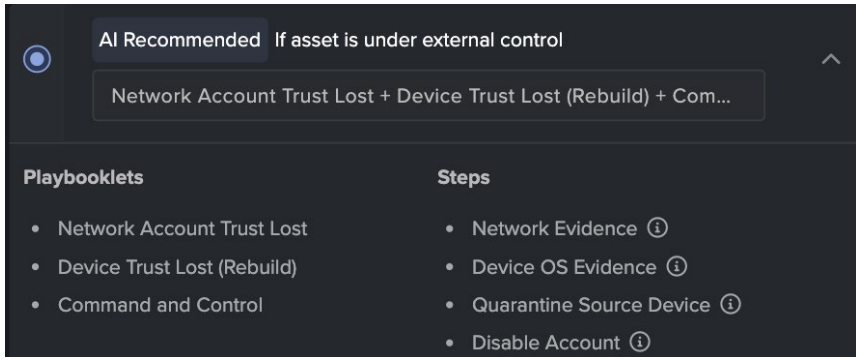
   a. There is an additional section, the **Device Heal Playbook,** from which users can select the appropriate playbook for the selected asset.



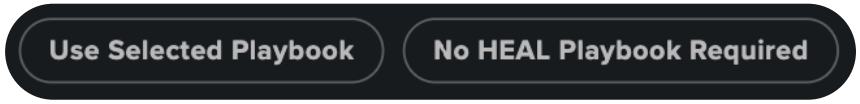
   i. Users can chose between three different options: **AI recommended**, **AI Alternative** or **select a specific Heal Playbook**. Select a specific playbook available from the drop-down menu.



ii. Click on the **downward arrow** to expand each of the options and see **playbooklets** and **detailed steps** included in the playbook.

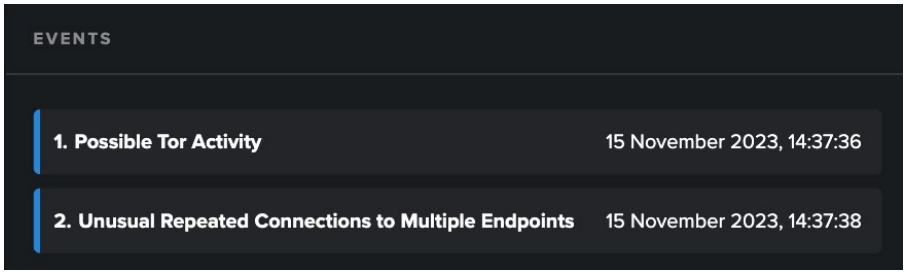


iii. Once you have chosen an appropriate playbook, click on **Use Selected Playbook**. If no playbook is required, click on **No HEAL Playbook Required** instead.



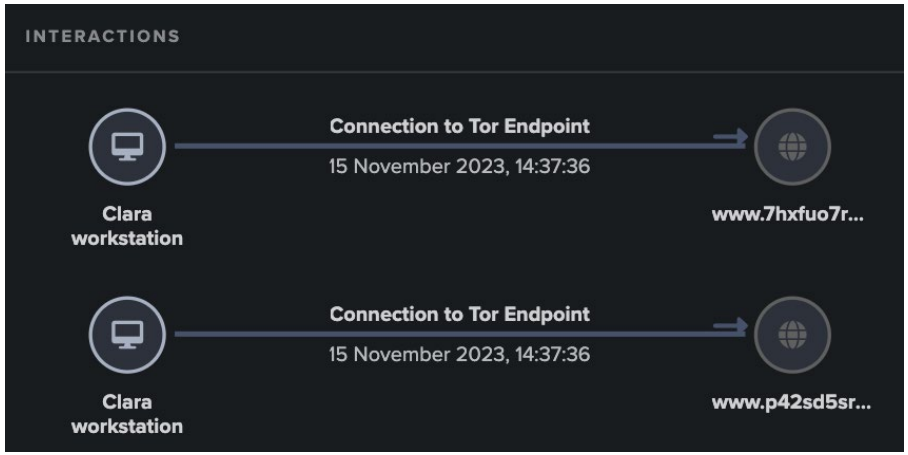
Note: Playbooks, Playbooklets and Steps will be studied further in the Recommended Workflow chapter.

b. Next is an additional **Events** section, listing events related to the selected asset, including the date and time of each event.



Note: Clicking on one of the Events will pivot the user to the Event tab.

c. Finally, there is the additional **Interactions** section which will show a graphical representation of all the interactions related to the selected asset.



Note: Clicking on one of the Interactions title will pivot the user to the Interaction tab.

Continue your learning with our dedicated video 4: Incident Graph and Further Options

1. The **play button** allows for a real time view of the data flow on your network.

2. Users can move through time using the arrows available:

   a. The **right arrow** will allow users to move to the **next event**.

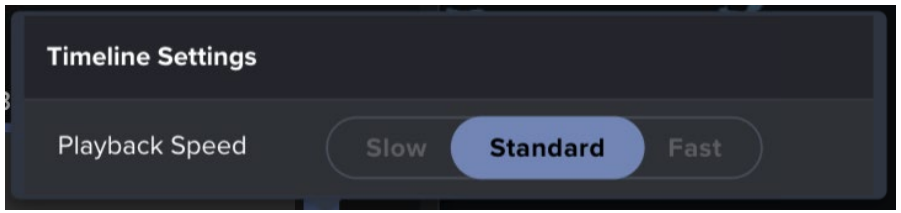
   b. The **left arrow** will allow users to move to the **previous event**.

   c. The **skip forward arrow** allow users to **skip to the end**.

   d. The **back arrow** will allow users to go back to the **first event**.

   e. The **circle arrow** will **reset** the playback graph.

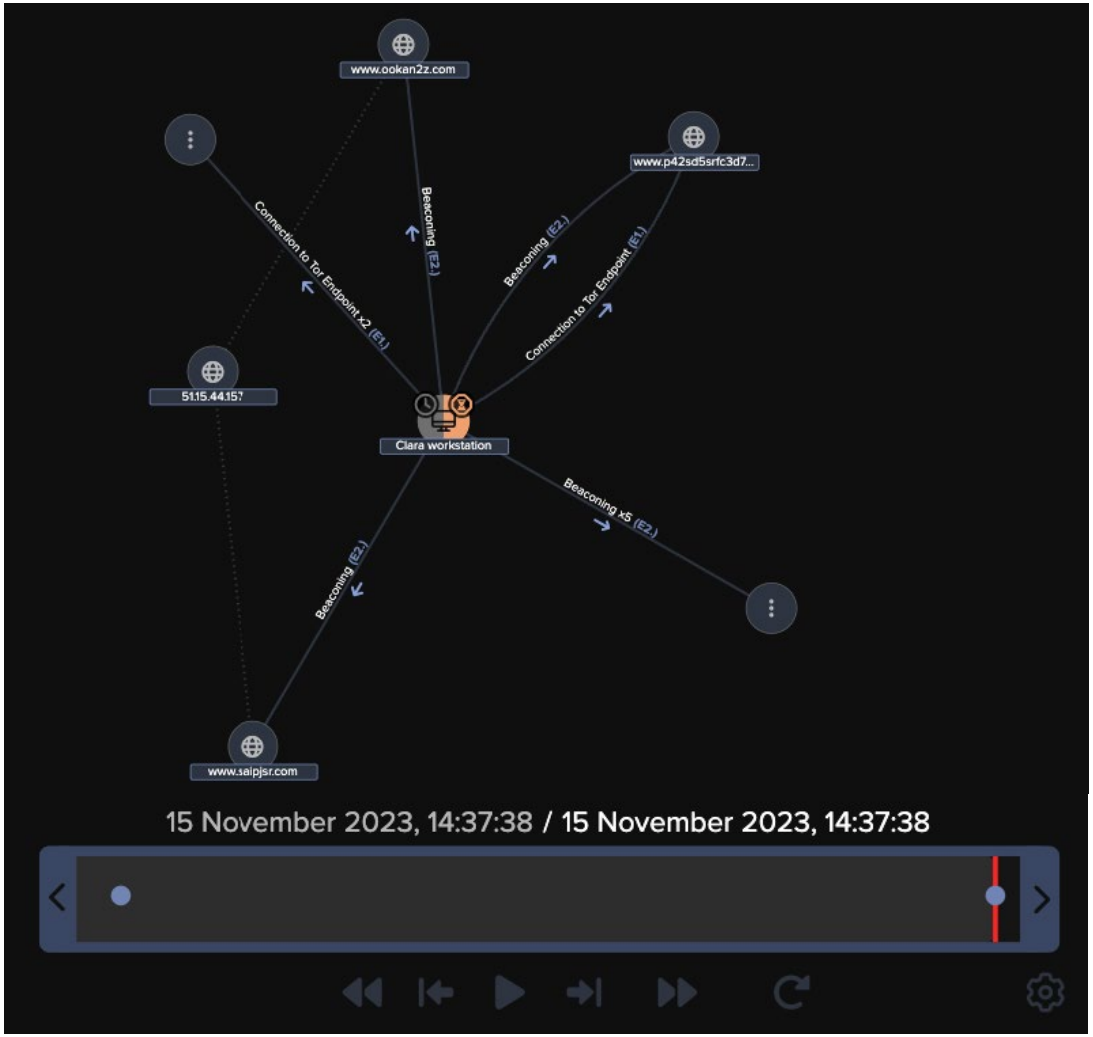
3. Click on the **cog icon** to open **timeline settings**, choosing between Slow, Standard or Fast.



Incident Graph

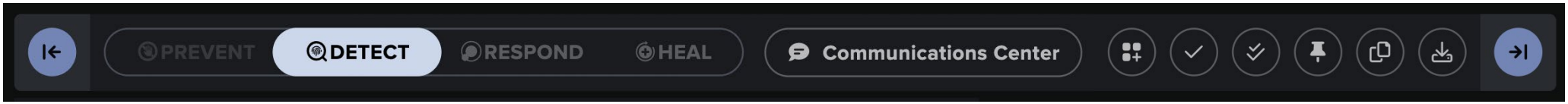
On the right-hand side of the Darktrace Incident window, an **incident graph** is always available. This allows for a playback of events showing how the real-time connections played out.

The incident graph can be interacted with by using the buttons available at the bottom of this section.



Further Options

Several options are available along the top of the **Darktrace Incident** window.



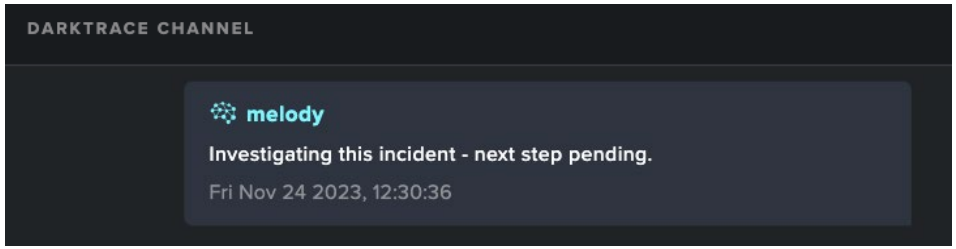
1. The first options are the **blue arrows** on each sides of the panel.

   a. Click on the **left-hand side arrow** to **expand the Incident Graph** section. This allows users to focus on the playback features of the incident graph, hiding the textual information.

   b. Click on the **right-hand side arrow** to **expand the Incident Details** section. This allows users to focus on the textual information of the incident details, hiding the incident graph.

   c. Depending on which view you are focused on, **click on the opposite arrow** to come back to the **original view**, with both the Incident Details and the Incident Graph available.

2. Click on **Communications Center** to participate in the internal Darktrace Incident chat.



Note: Teams and Slack can be integrated and used with the Communications Center.

3. There are six additional buttons available at the top of the incident window:

   a. The first button available is the **Add Another Asset to the Incident**, which allows users to add another device to the selected incident.

   b. Once reviewed, incidents can be acknowledged using the **Acknowledge Incident** tick icon. They will then be hidden unless the **Include acknowledged** toggle is on in the filters.

   c. Alternatively, click the double tick icon to **Acknowledge Incident and all related Model Breaches**.

   d. To pin the incident and save it for later, click the **Pin Incident** icon. The incident in the Darktrace Incident Tray will also have a pin icon displayed to demonstrate it has been pinned.

   e. Notice the **Copy Incident URL to clipboard** icon. This can be clicked to copy the URL of the selected incident to the device clipboard to be shared with colleagues or saved locally.

   f. To create a **report** of this particular incident, click on the **Download Incident Report (PDF)** icon. Give the report a name and click **Generate Report**.

Basic Concepts Chapter Test

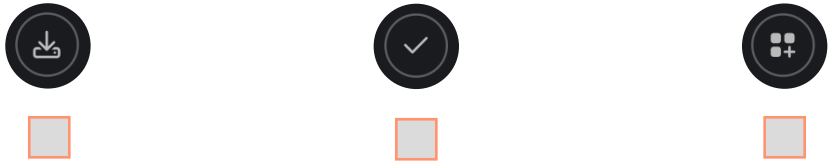
This page will test your knowledge and check your understanding of the Basic Concepts section.
Select an answer by clicking on it. Wrong answers are denoted by a red cross and right answers are denoted by a green tick.
You can clear all the answers and try again at any time by clicking the button to the right.

Clear All Answers

1. Which permission will allow you to view Incident Readiness & Recovery actions on devices?

- [ ] Activate Incident Readiness & Recovery Actions
- [ ] Manage Incident Readiness & Recovery Playbooks
- [ ] Darktrace Incident Readiness & Recovery

2. Which icon allows you to download an incident report as a PDF document?



- [ ]
- [ ]
- [ ]

3. Which filter option will allow you to see the standard AI Incident interface?

- [ ] Include acknowledged
- [ ] Disable Darktrace Incident Interface
- [ ] Legacy Incidents

4. The Darktrace Incident interface is available in several languages.

- [ ] True
- [ ] False

5. From which section would you be able to read the Network Connection Summary?

- [ ] PREVENT\Summary
- [ ] DETECT\Incident
- [ ] HEAL\Asset

6. From which section would you be able to read the Top Entity Score?

- [ ] PREVENT\Summary
- [ ] DETECT\Incident
- [ ] HEAL\Asset

4. Recommended Workflow

The recommended workflow in this chapter shows the user how to practically use Darktrace Incident Readiness & Recovery to prevent damage to your assets, investigate detected incidents, respond to potential threat and, ultimately, heal your environment.

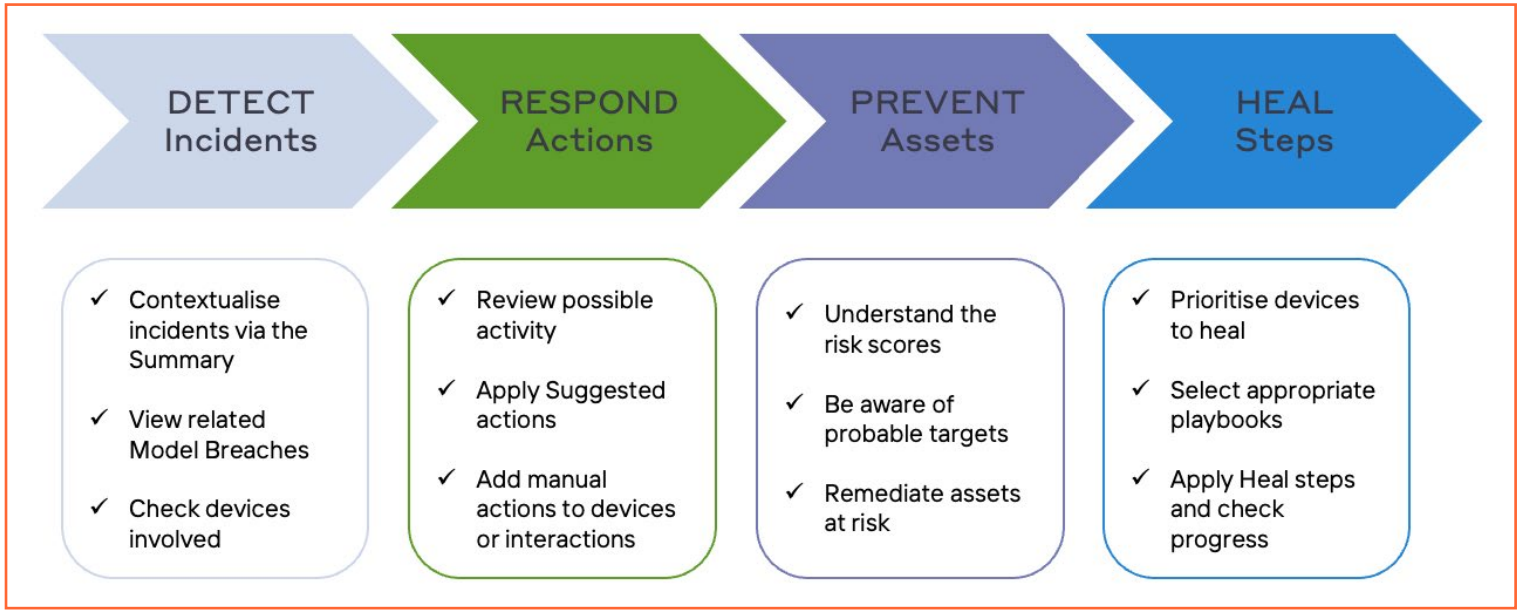
4. Recommended Workflow

When using Darktrace Incident Readiness & Recovery, there are several steps to follow in order to **Prevent, Respond, Detect** and **Heal** incidents related to your environment.

The workflow will vary among users, however, it is preferable to follow a systematic process of **detecting incidents,** activating **Respond actions, Prevent further assets** being involved and going through **Heal steps**.

These steps will include important stages to assist you with contextualising the incident, reviewing possible activity before applying necessary actions, understand risk score and probable next targets to prevent further compromise and finally prioritise devices to heal and select the appropriate playbook.

Use all appropriate information present on the incidents, such as the **Summary** to have an overview of the whole chain of Event, the **Event** tab to see Events one by one, the **Interaction** to allow you to see the link between involved devices and finally the **Assets** which will show you the data being targeted.



Each of the step above answers questions which the security team can ask themselves when dealing with an incident:

- **DETECT**: *What have we seen on our environment?*
- **RESPOND**: *What actions can we take to stop the compromise?*
- **PREVENT**: *What more could happen to our environment?*
- **HEAL**: *What are the appropriate next steps and what can we learn from this?*

DETECT Events

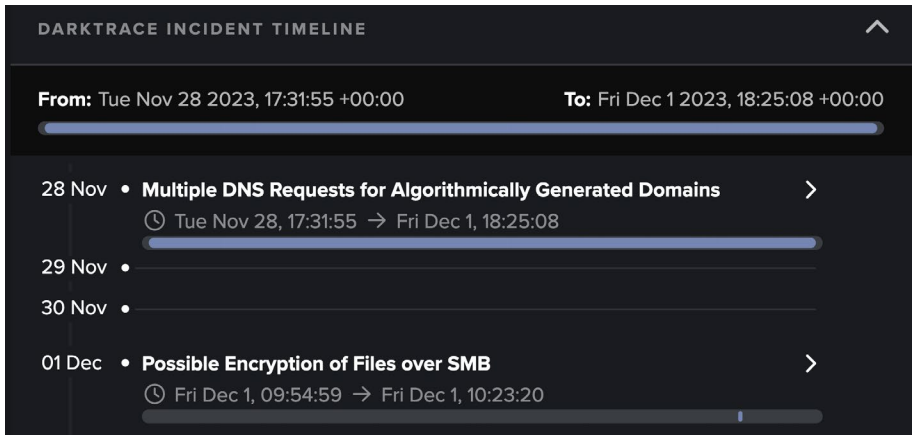
Continue your learning with our dedicated video 5: DETECT Events

The first step when investigating a Darktrace Incident will be to go through the information available in the DETECT tab. This will include the following steps:

- Contextualise incidents via the Summary
- View related Model Breaches
- Check devices involved

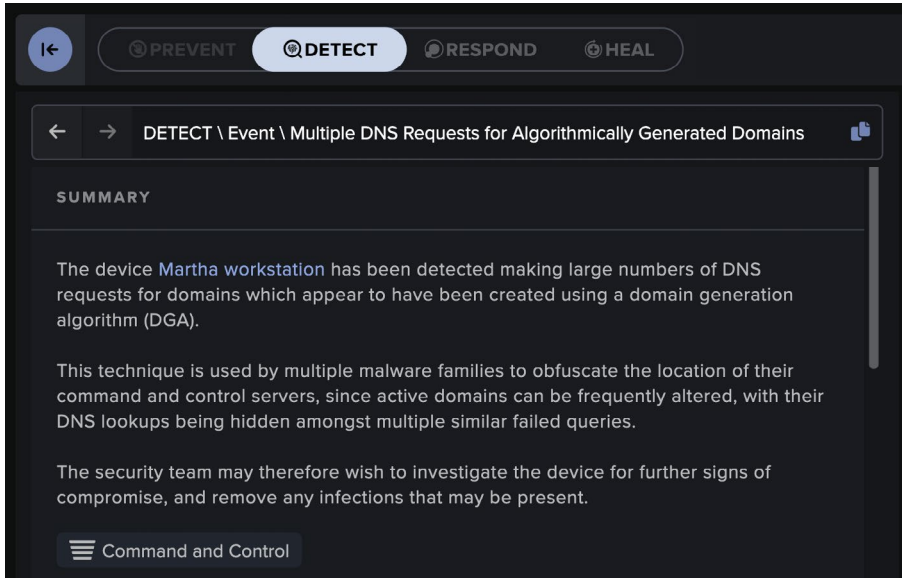
1. The **Summary** here shows you different events that a Darktrace incident consists of, giving more context to various aspects of the incident.

   a. Start by looking at the **Incident Timeline** and check if these behaviors are expected for the devices involved.



   Notice how in this example, the device has made **Multiple DNS Requests for Algorithmically Generated Domains** over several days. This leads to another step in the potential attack, with a **Possible Encryption of Files over SMB** event.

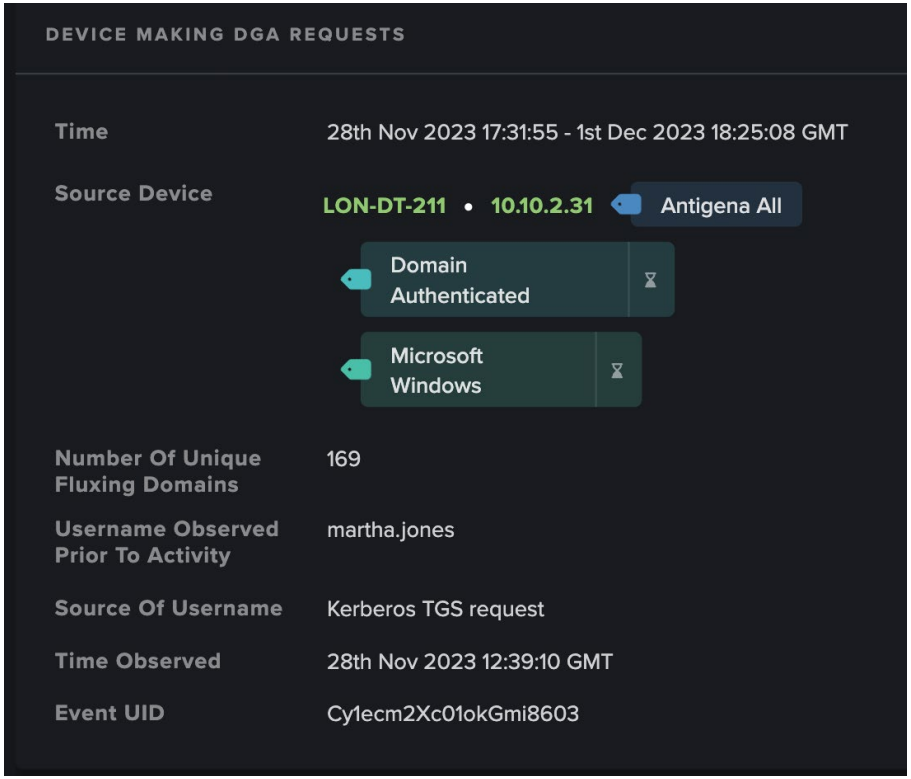
   b. Each of the events from the timeline can be clicked on, leading you to the **Event Detect summary page**, with a textual summary including the device and the technique involved and steps for a resolution.



From the Summary above, we learn more about the device involved, and potential user.

It is also useful to note the description of this technique, **DGA requests**, and the fact that it is often used in the **Command and Control attack phase**, as indicated at the end of the Summary. As a next step, it is advised to check for any other signs of compromise.

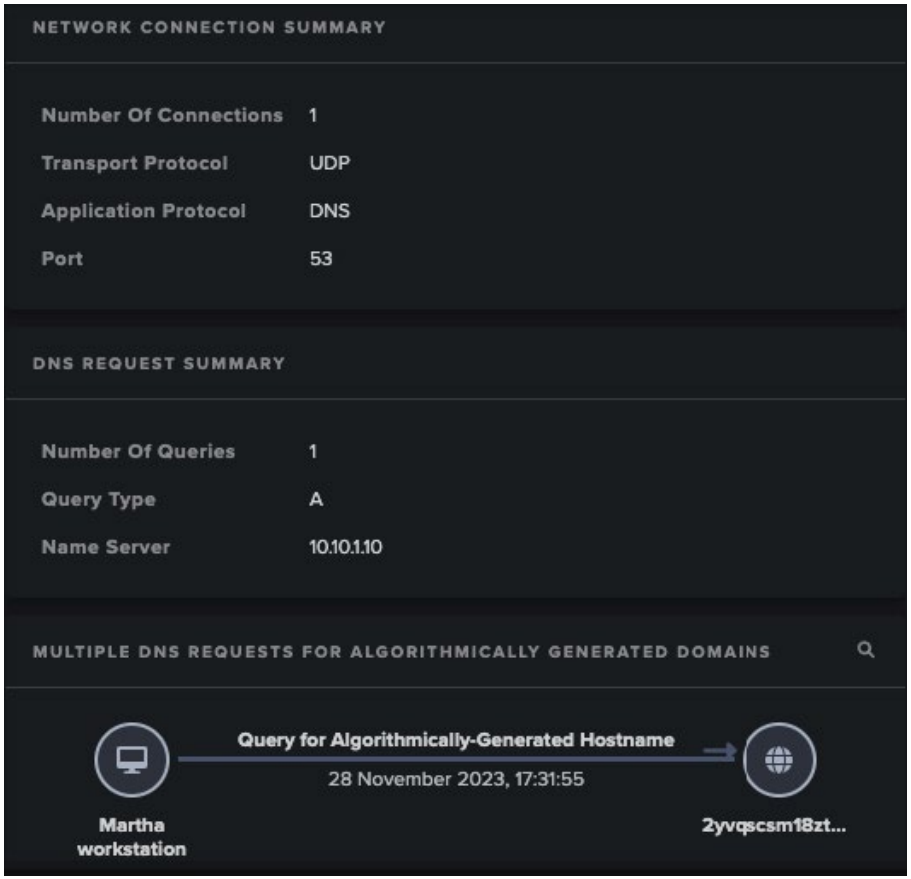
c. Access more **technical details** by scrolling down on this page, including older and different types of events.



This section helps us understand more about the source device such as which **tags** are attached to this device and if they show if this device is particularly at risk.

It is also interesting to note the high number of **Unique Fluxing Domains**, 169, as well as the **Source of Username** which is a Kerberos TGS request in this instance.

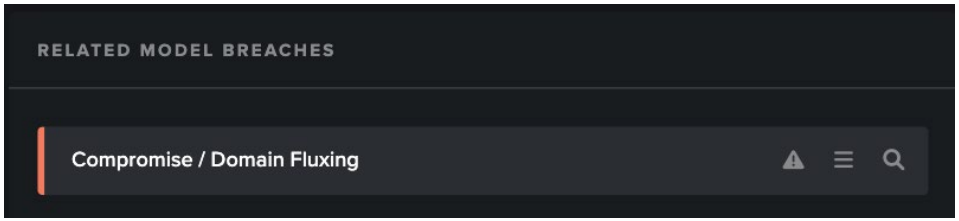
d. Moving on to the **Interactions** tab, you can see the overlapping sort of events and how they have interacted with one another.



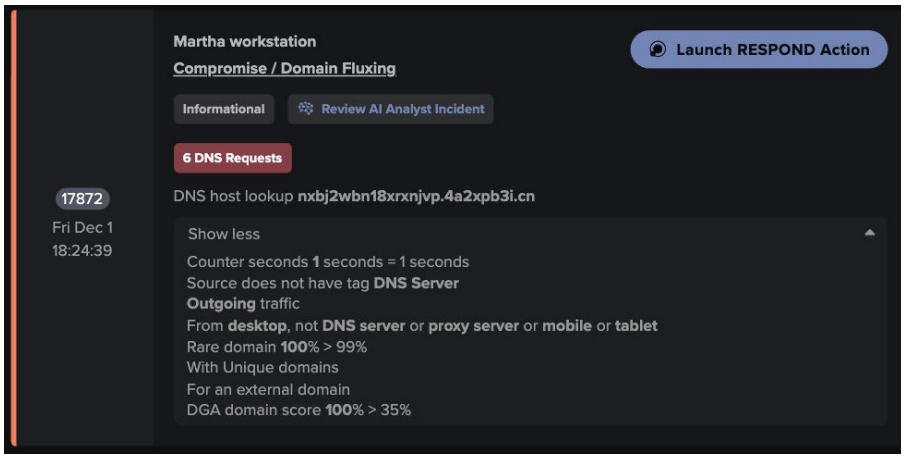
For example, we can gather more information about this specific event, such as the **number and type of connections**, one UDP connection using Port 53 in this instance.

It is also useful to know the name of the server and have a **visual representation** of the same event, including the source device, type of event, data and time, and detected DGA query.

2. It can be useful to have a better look at the **Related Model Breaches**, accessible from the Event page, to gather more information on the steps



a. Click on the model breach icon to load the **Breach Log** and its relevant information. In this example, a device sent multiple DNS requests to rare domains.

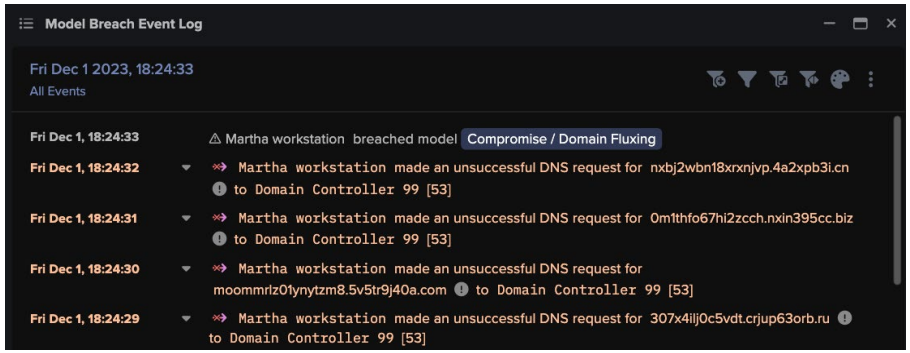


In its default view, some details will be hidden behind the **Show more** expandable sections - these have already been expanded.

Notice the rare domain score achieved 100% > 99%. This means it exceeded the Model target of 99% and so triggered the breach. Similarly, the DGA domain score reached 100%, exceeding the Model target of 35%.

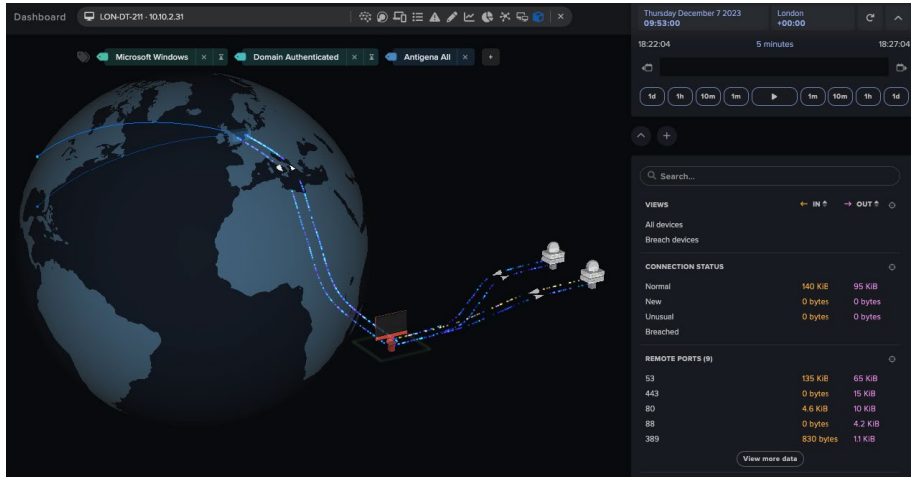
Hovering over the vertical colored bar for any breach will reveal the overall Threat score, which in this case was 80%.

b. Review all the **connection and event information** relevant to a breach by opening the **Model Breach Event Log**.



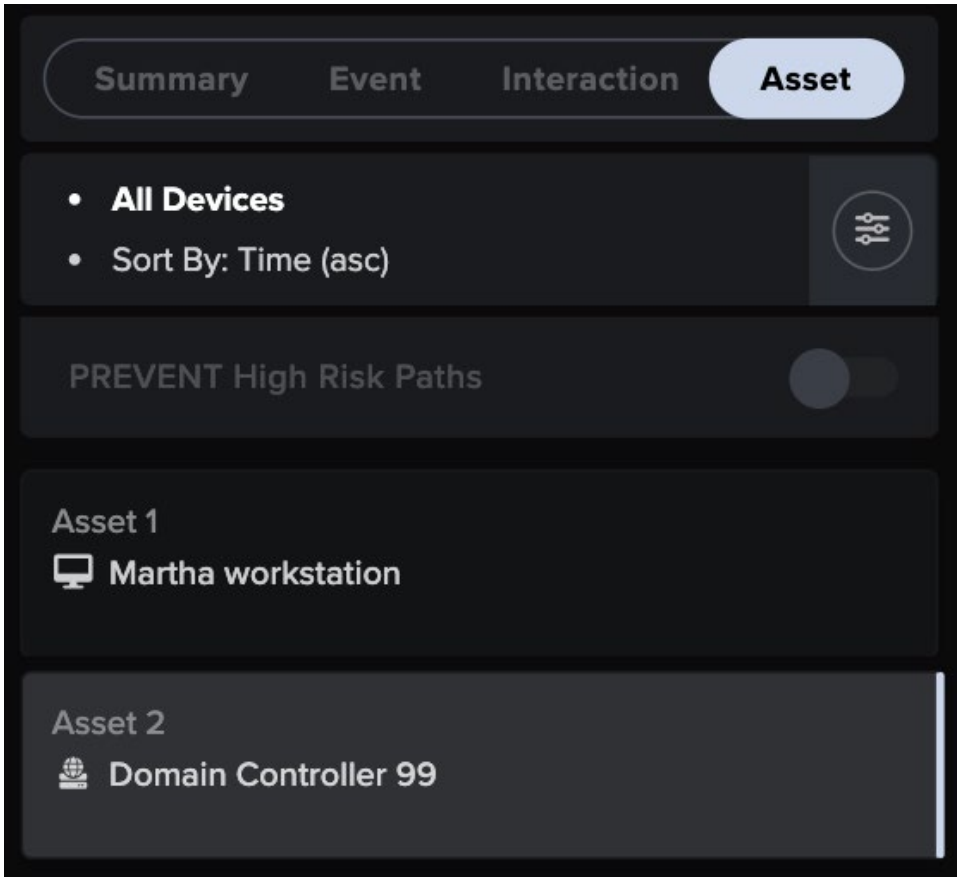
In this example, the device has been seen making unsuccessful DNS request for several domains within a short period of time.

c. Clicking on the **magnifying glass** will open the Device view in the background. If centered around the time of a **Model Breach**, the **interactions** taking place at that moment can be **visualized**.

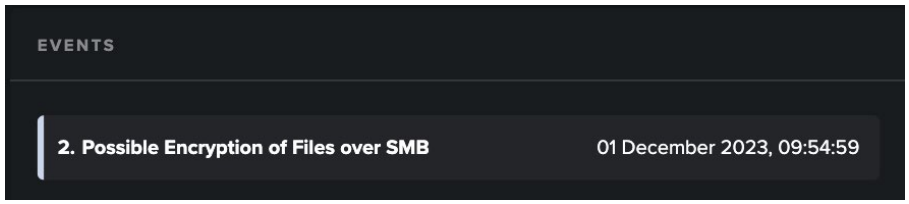


In this example, the device at fault is clearly marked in red while the connections to Domain Controllers can be investigated further.

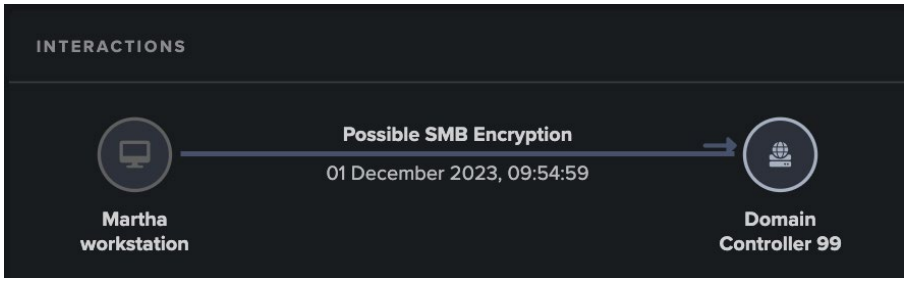
3. Users can investigate all assets that are involved, or alternatively focus on a specific asset by accessing the **Asset** section of the Detect Summary.



a. The information on the side will show **what activity** is observed on this asset and in what **types of events** was this asset involved in. This gives a different angle of which you can look at this incident.



b. Users can see the **different interactions** of this particular asset and what connections it has made. In this example, Martha workstation has made a possible SMB encryption to the Domain Controller 99.



c. From the graph, use third-party resources such as **Lookup in WHOIS** or **Lookup in VirusTotal** to investigate domains interacting with assets.

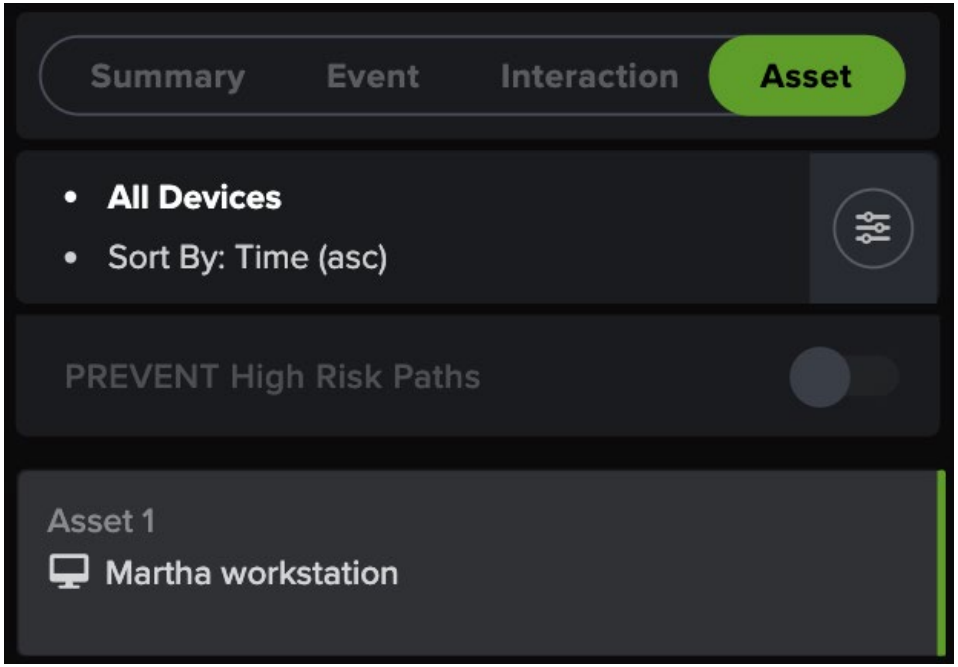
RESPOND Actions

The second step when investigating a Darktrace Incident will be to go through the actions available in the RESPOND tab. This will include the following steps:

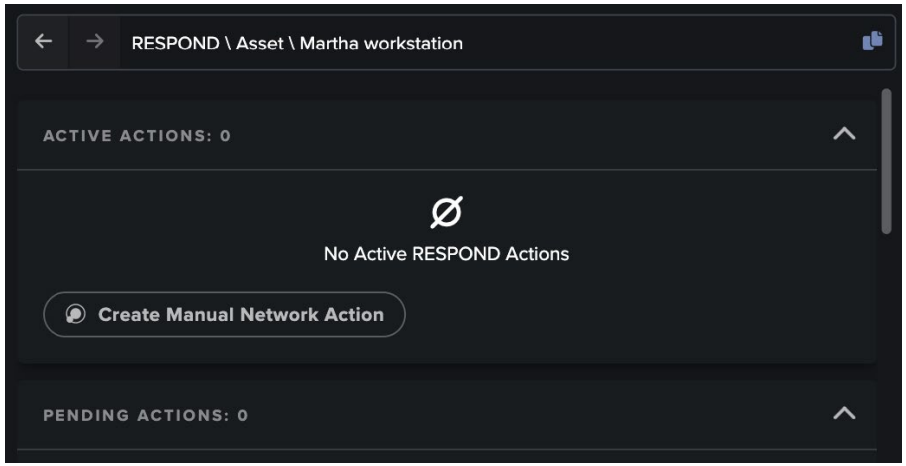
- Review possible activity
- Apply Suggested actions
- Add manual actions to devices or interactions

Continue your learning with our dedicated video 6: RESPOND Actions

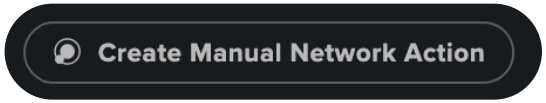
1. Users can access the **RESPOND Asset** section to look at different assets by selecting them from the left-hand side.



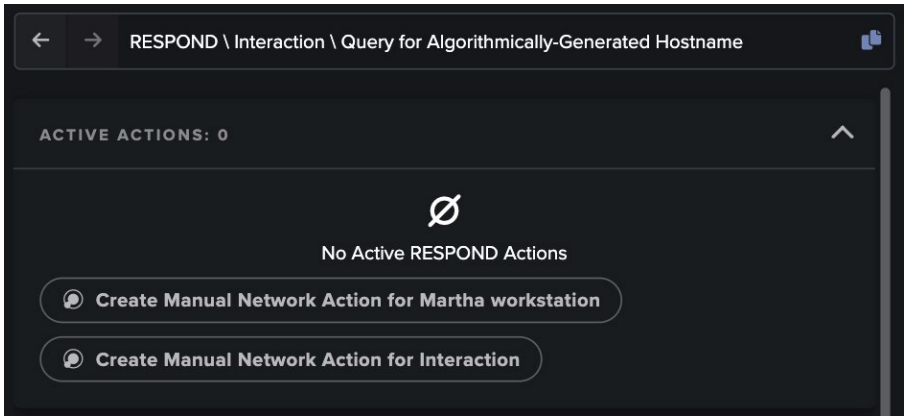
a. Check whether the asset currently has any **active or pending RESPOND actions** on the right-hand side.



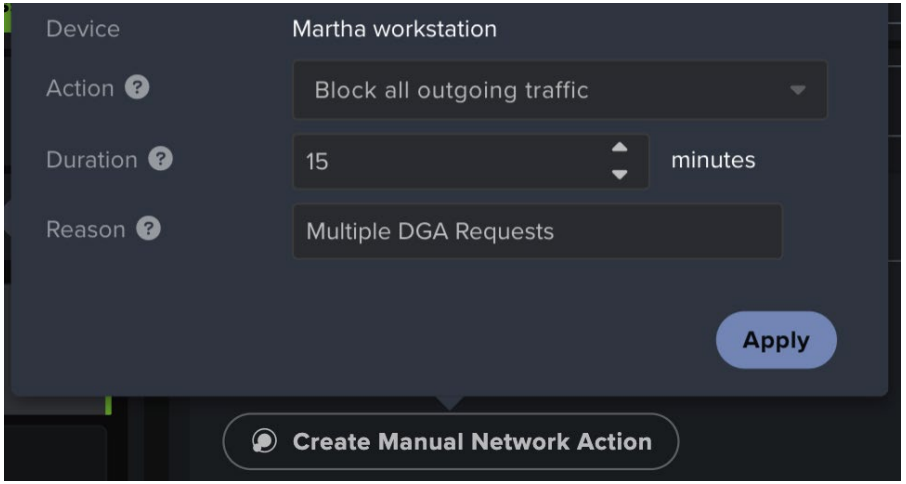
b. If no actions are currently active, you can create an appropriate action by clicking on **Create Manual Network Action**.



c. Alternatively, access the **RESPOND Interaction** section from the left panel and select **Create a Manual Network Action for Interaction** rather than the whole asset.

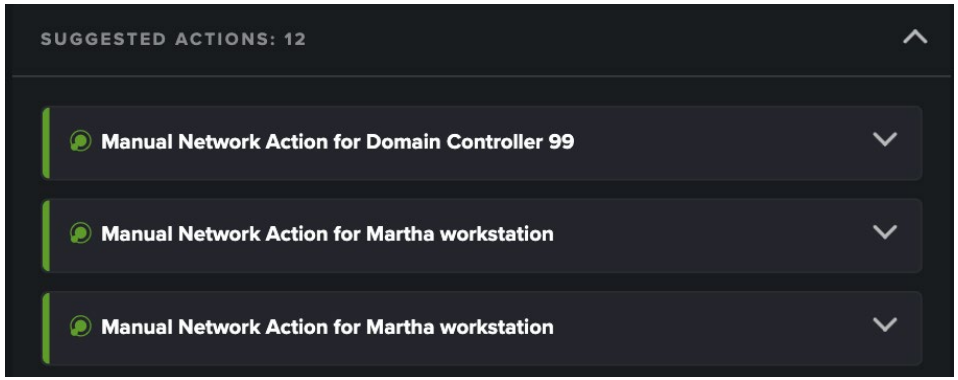


d. In this instance, we might decide to **block all outgoing traffic** from the device, rather than action a specific interaction. This will allow us time to move on to other steps and actions.

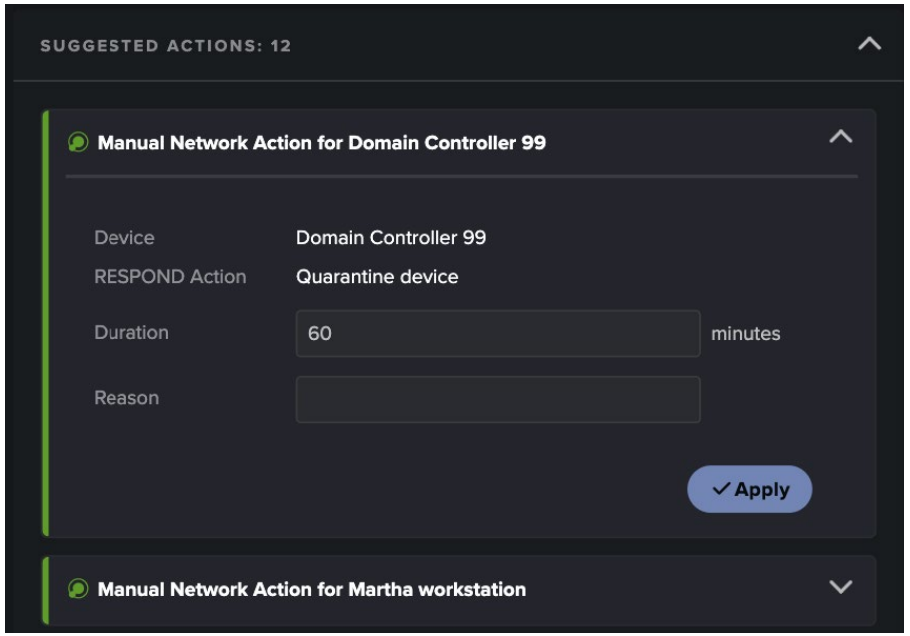


Note: If the RESPOND Action is one of the Heal steps, you can mark it as complete from the HEAL page, which will be explored further in its dedicated section.

2. Another interesting feature on the RESPOND page is the **Suggested Actions**. These can be viewed from all RESPOND sections but the Summary page will show all available actions for this incident.

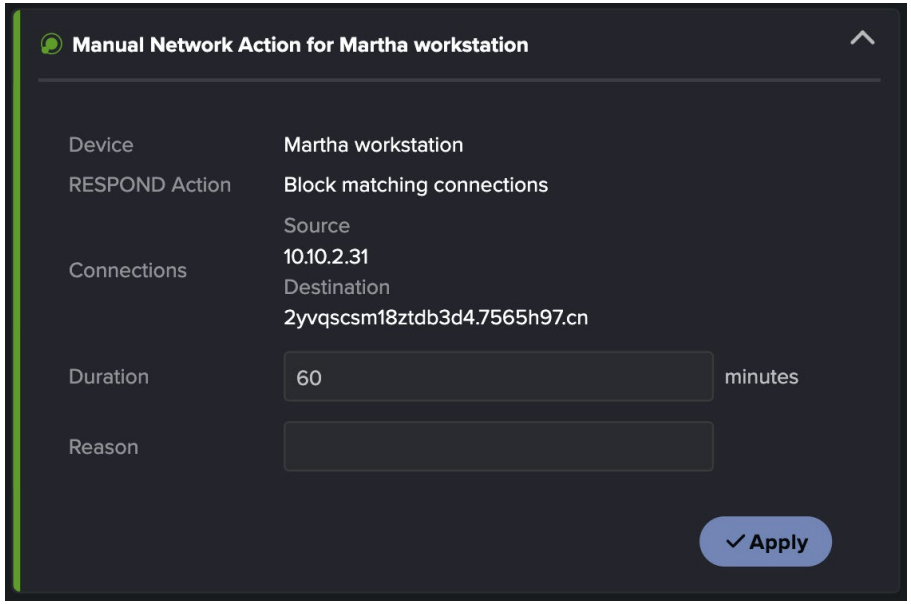


a. Click on the downward arrow to open a suggested action. Once you have reviewed the action, you can add a **Reason** and then click **Apply**.



Based on the knowledge you have gained from previous sections, such as if this compromise is highly likely to spread further into other directions, Darktrace Incident Readiness & Recovery might suggest you to actually quarantine the device for an hour.

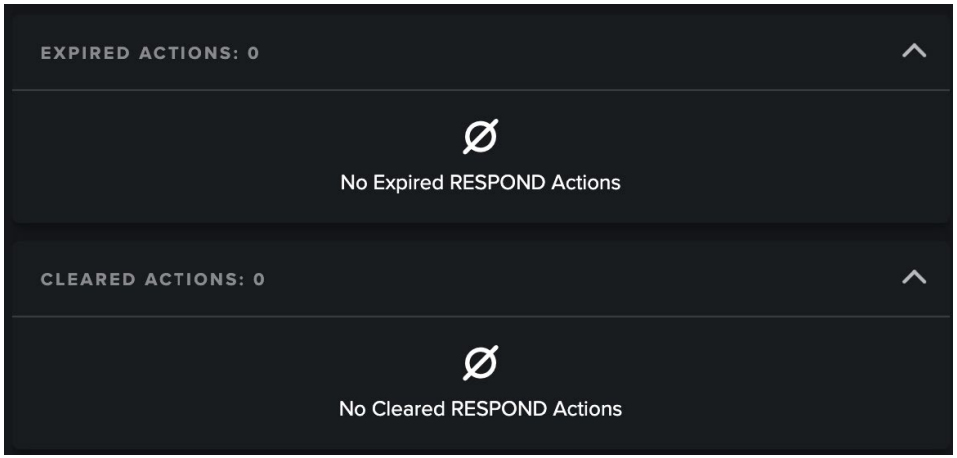
b. Other manual actions might be available such as **Block matching connections** to a specific destination. Once you have reviewed the action, you can add a **Reason** and then click **Apply**.



For example, because we may have seen connections to a certain end point or certain other device, we would block this specific connection to try and contain the spread of this incident further.

Rather than having to think about it yourself and do a manual action, an action might be suggested to you, helping you further in your investigation process.

3. Finally, it might be interesting to check if there are any **Expired** or **Cleared Actions** which you might want to reapply.

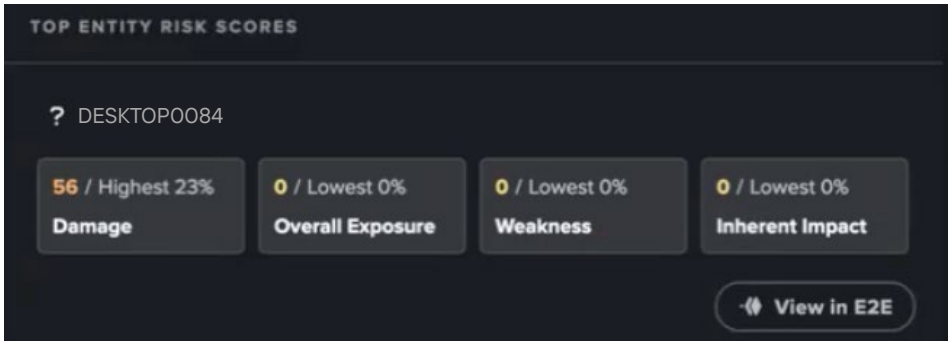


PREVENT Assets

The third step when investigating a Darktrace Incident will be to go through the assets available in the PREVENT tab. This will include the following steps:

- Understand the risk scores
- Be aware of probable targets
- Remediate assets at risk

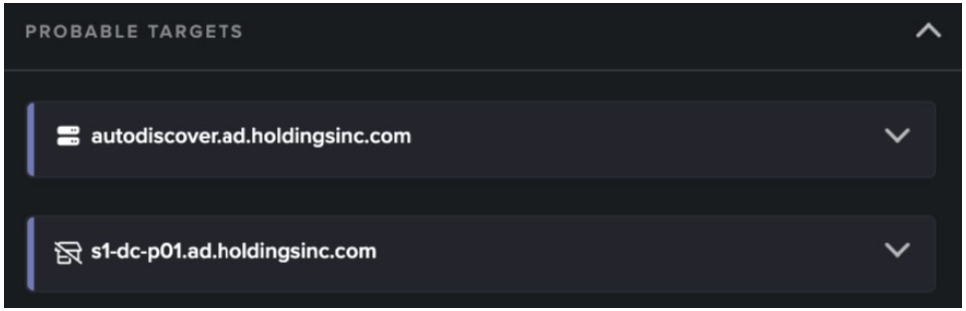
1. Let's think about whether the asset in this example is **compromised**.



Although the Overall Exposure, Weakness and Inherent Impact scores are low, this device has a high **Damage score**, 56, which makes it in the **highest 23%** out of all the device part of this environment.

Click on **View in E2E** to see if it sits on a critical attack path and gather more information concerning this device.

2. Based on the information provided, if the compromise were to spread further the assets listed below are likely next **Probable Targets**.



3. This information really helps security teams to make decisions concerning the assets at risk, such as:

   a. Preventing further risks to this device by **mitigating high priority CVEs** from the Proactive Exposure Management interface.

   b. From the Threat Visualizer, add a **different tag** on this device so it can be categorized appropriately.

   c. Apply a **RESPOND action** on this device so that the compromise cannot go further.

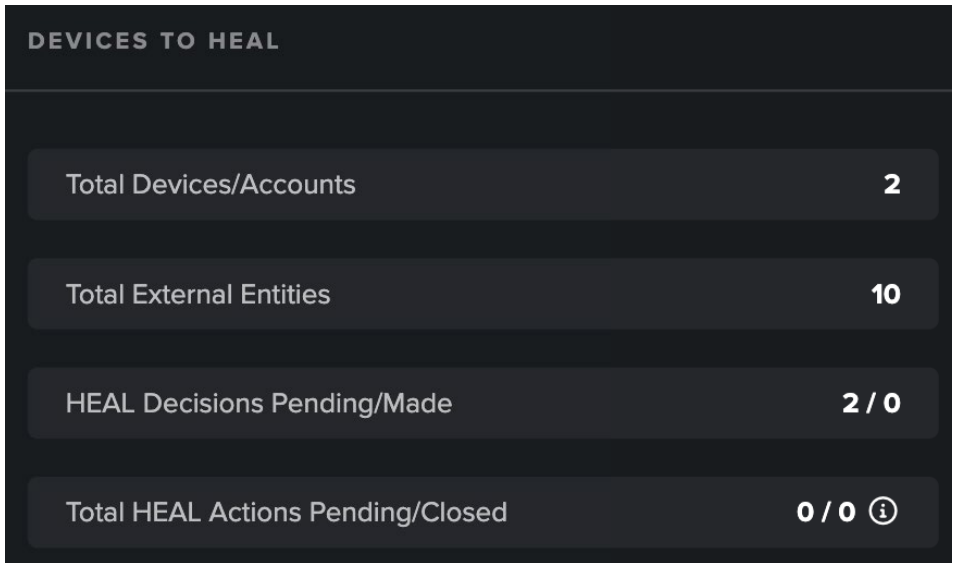
HEAL Steps

Continue your learning with our dedicated video 7: HEAL Steps

The fourth, and last, step when investigating a Darktrace Incident will be to go through the Playbooks available in the HEAL tab. This will include the following steps:

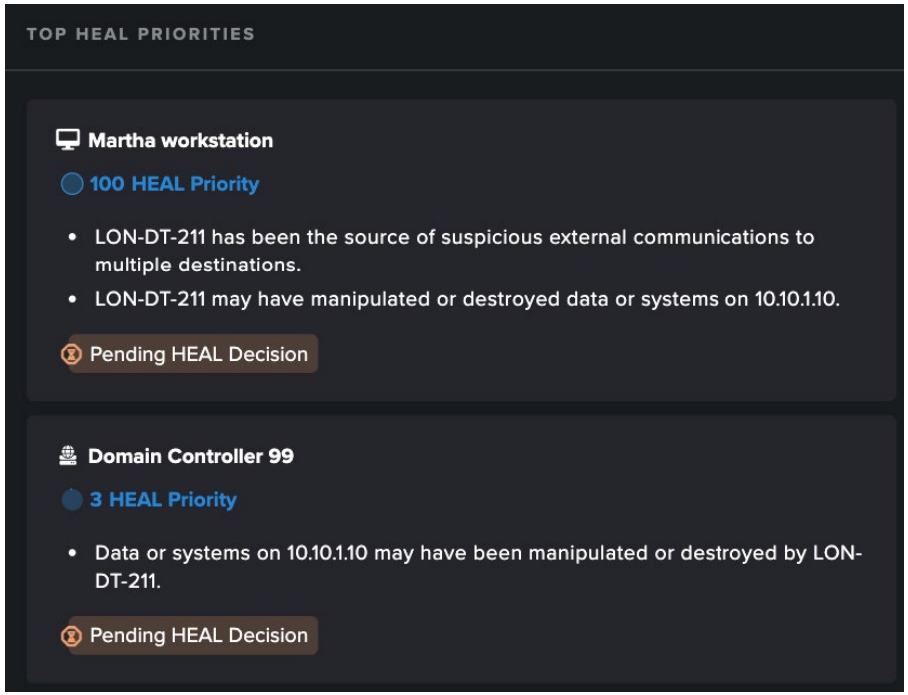
- Prioritize devices to heal
- Select appropriate playbooks
- Apply Heal steps and check progress

1. From the **Summary** page, check the **Devices to HEAL** section.



In this instance, two **Total Devices** need to be healed, we can see here that 10 different external domains have been visited in the **Total External Entities** section, and there are two **HEAL Decisions Pending** but zero have already been **Made**, and there are no **Pending** or **Closed Actions**.

a. From the information we have gathered from DETECT, PREVENT and RESPOND, this will give you a **prioritisation of the assets** that need to be healed in the Top HEAL Priorities underneath.



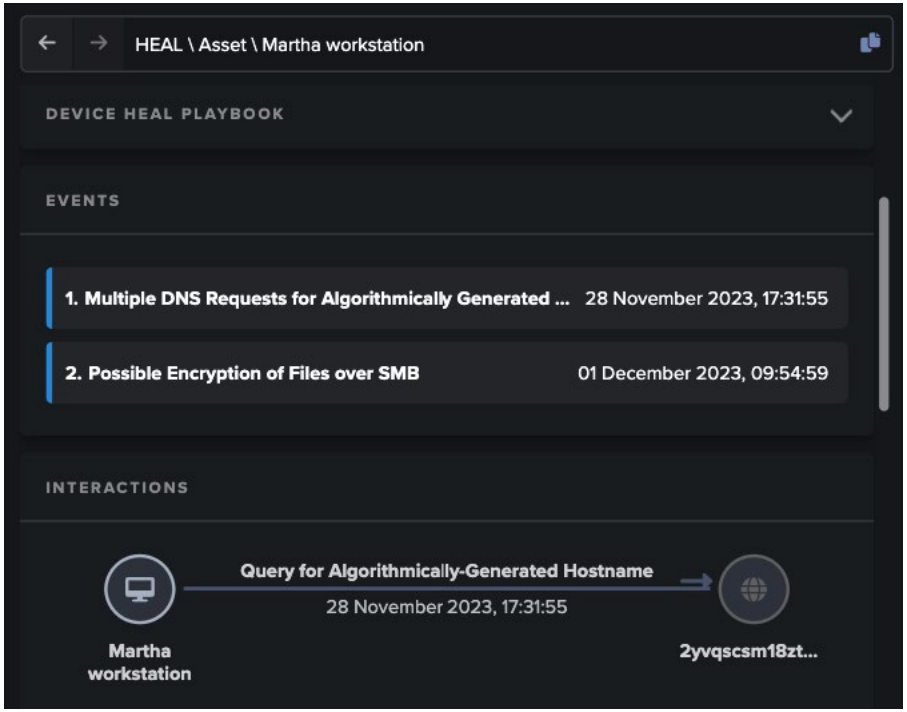
From the example above, notice the **HEAL Priority Scores**, which is only 3 for the Domain Controller 99 but 100 for Martha workstation.

This is explained underneath by the type of activities we have seen on these different devices: not only has Martha Workstation had **data or systems manipulated or destroyed**, it is also the **source of suspicious external communications to multiple destinations**.

Martha Workstation is therefore more critical for recovery and Darktrace will give you that priority based on a technical score.

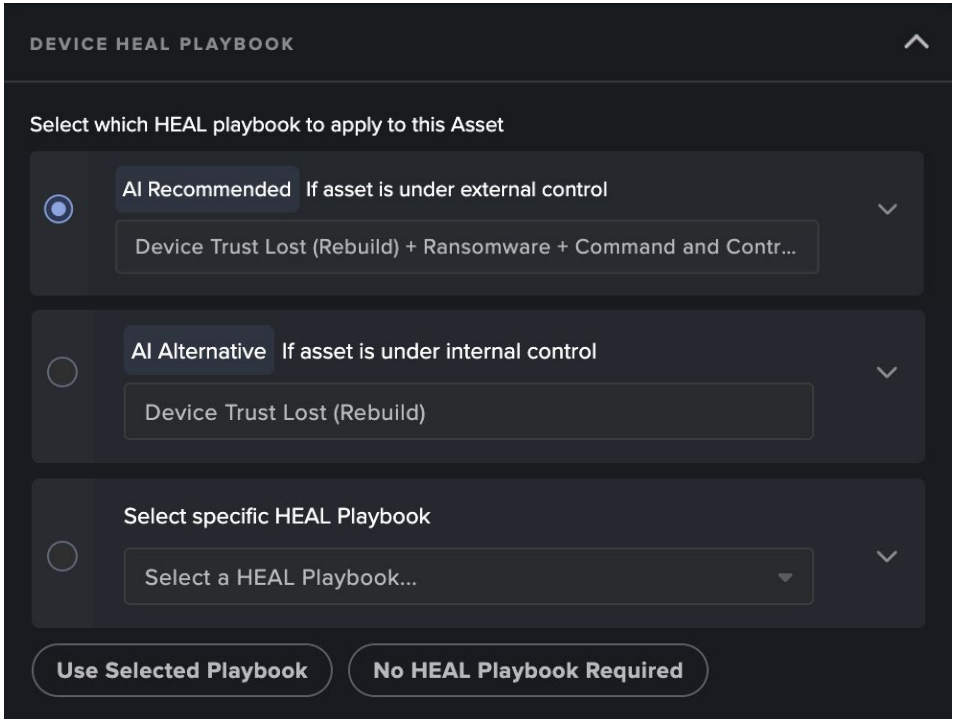
Note: HEAL Priority scores are based on technical information gathered from Detect, Prevent, Respond and possible integrations. The priority of an asset may change based on other factors such as human input.

b. Click on the asset you have chosen to heal as a priority to view a summary of **Events** and **Interactions**.



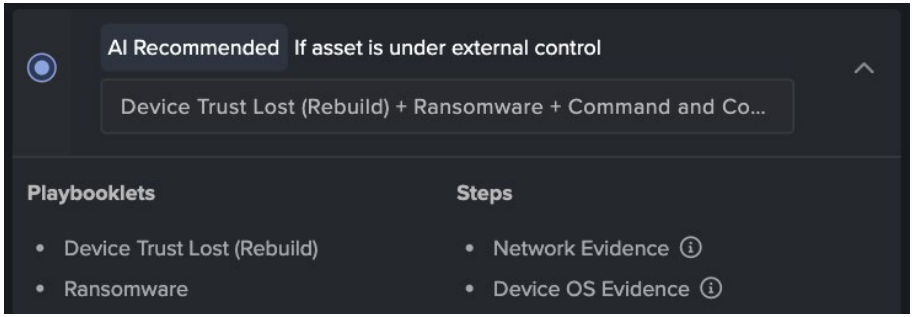
What has happened in this case is that this device is the source of **Multiple DNS request for Algorithmically Generated Domains**, informing us that this is where it all started from, and there has been a **Possible Encryption of Files over SMB** a few days later.

2. The next section is the **Device HEAL Playbook** which will give you four options to choose from: an **AI Recommended** Playbook, an **AI Alternative, Select specific HEAL Playbook** or **No HEAL Playbook Required**.

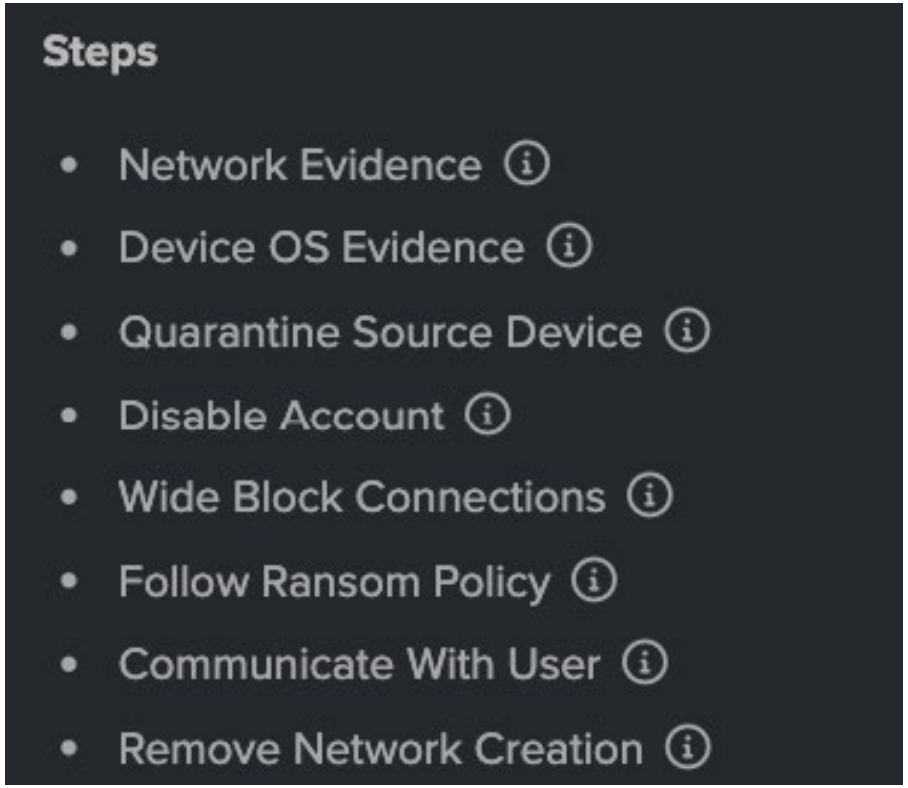


a. The AI will recommend a Playbook which fits best, such as if the **asset is under external control**. Click on the **downward arrow to expand** the Playbook and read more about the playbooklets and steps included.

In this instance, the AI is recommending using the **Device Trust Lost (Rebuild) + Ransomware + Command and Control + Network Account Trust Lost Playbook**, which will include the Playbooklets.

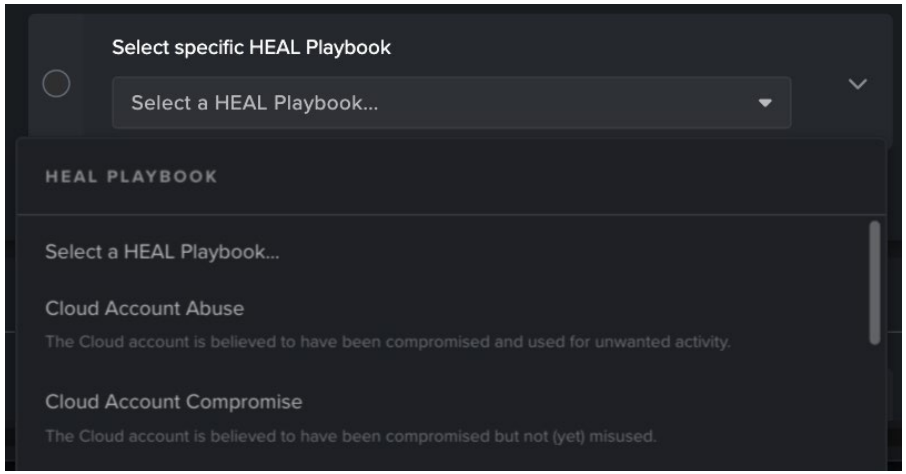


The **Steps** included in this Playbook will be displayed on the right-hand side.



Browsing the steps will help you determine if you would like to use the AI recommended Playbook or, alternatively, choose another Playbook.

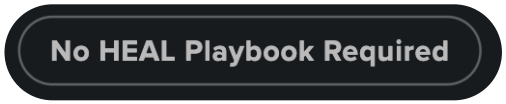
b. Alternatively, choose another playbook that you think is more fitting based on the additional business context that you have by using the drop-down menu in the **Select Specific HEAL Playbook** option.



Once the Playbook has been selected, click on the **downward arrow** to review the **Playbooklets** and **Steps** included.

c. After having choosen either a playbook recommended by the AI or a playbook that you think is more fitting, click on **Use Selected Playbook**.

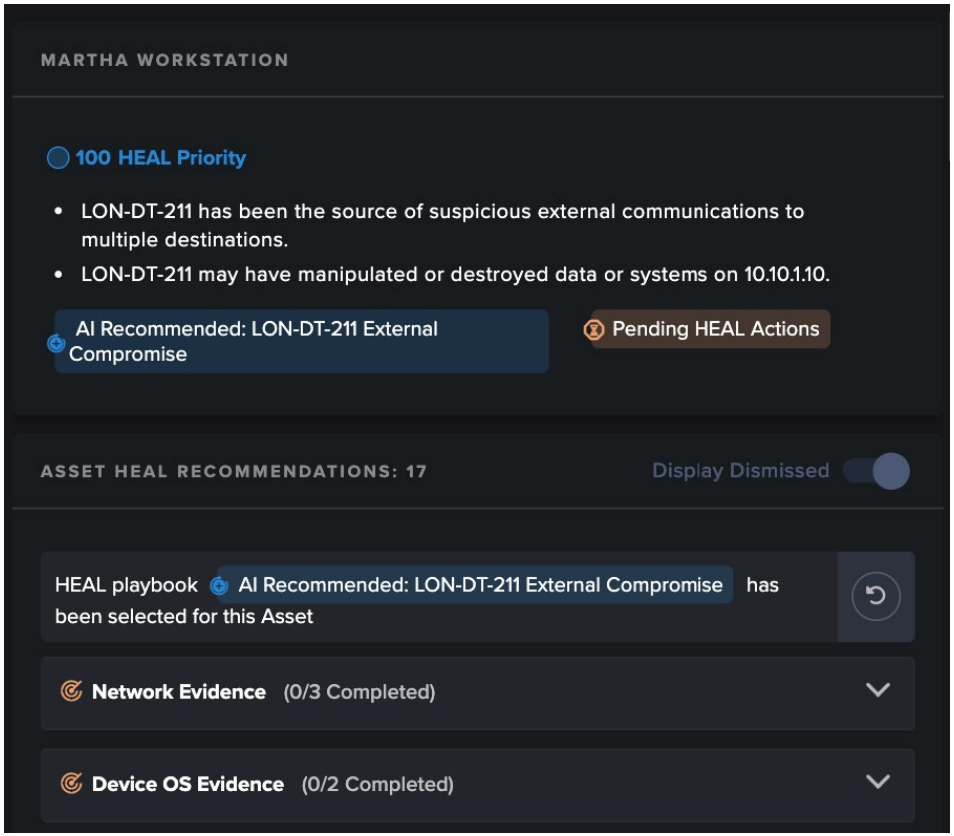
If you believe HEAL actions are required, click on **No HEAL Playbook Required** instead.



Note: HEAL Playbooks, Playbooklets and Steps will be further explored in their dedicated section, chapter 5.

HEAL Steps

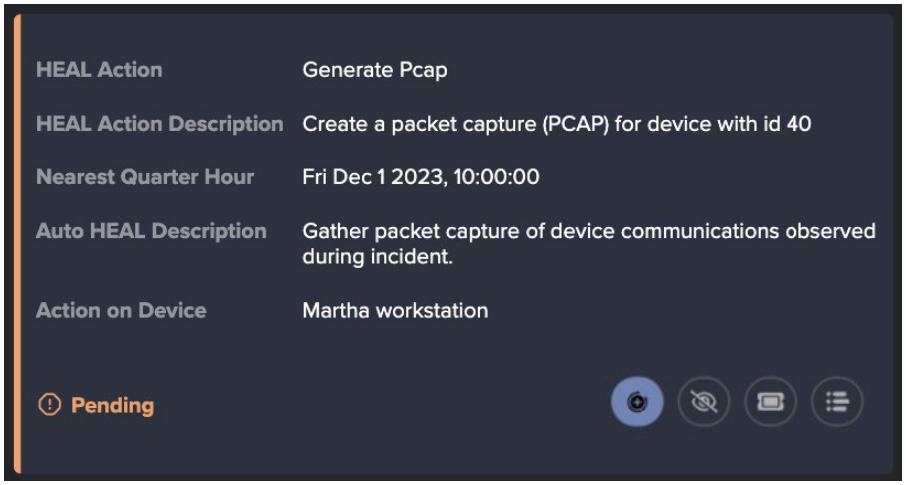
3. Once you have applied the selected Playbook, you can start going through the different HEAL steps. The Asset to be healed will be displayed at the top, along with information on the **priority score**, choosen **Playbook** and **Heal actions status**.



Underneath the information concerning the device, the **Asset HEAL Recommendations** will be displayed. The selected Playbook will be indicated, as well as all of the steps and actions to take in order for the incident to be remediated.

In our example, there are 17 HEAL recommended actions, three of which are part of the **Network Evidence** step, and two of which are part of the **Device OS Evidence** one.

a. The first step here is to gather **Network Evidence** and the security team can start going through these step by step. Clicking on the **downward arrow** will expand the step and show the first HEAL action: **Generate PCAP**.



b. Depending on the type of HEAL action, you can **interact** in different ways via the **buttons** available in the right-hand corner:

i. Click on the **plus icon** to **Activate auto HEAL**. This will automatically activate the HEAL action, which will be running on your interface.

ii. If the HEAL action is a manual one, the plus icon will be replaced by a **person icon**. Click to **Mark as Applied**, confirming you have completed this action outside of the interface, such as speaking to the user directly.

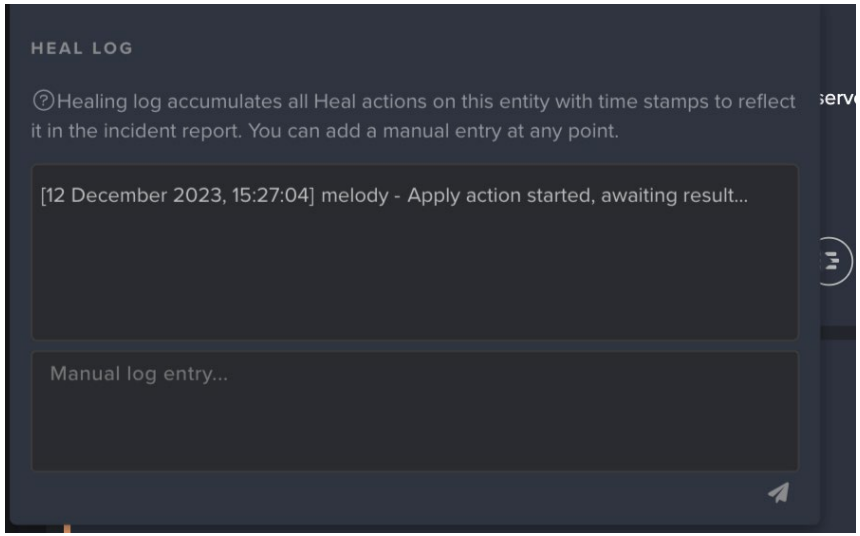
iii. Click on the **crossed-out eye icon** to **Dismiss Action**, if you believe that this specific action is not relevant to your environment. This action will prompt you for a reason before being able to dismiss.

iv. If the ServiceNow Ticketing module has been configured, the **External Ticketing** button will appear on the HEAL action section. This enables you to link this action to your external ticketing service.

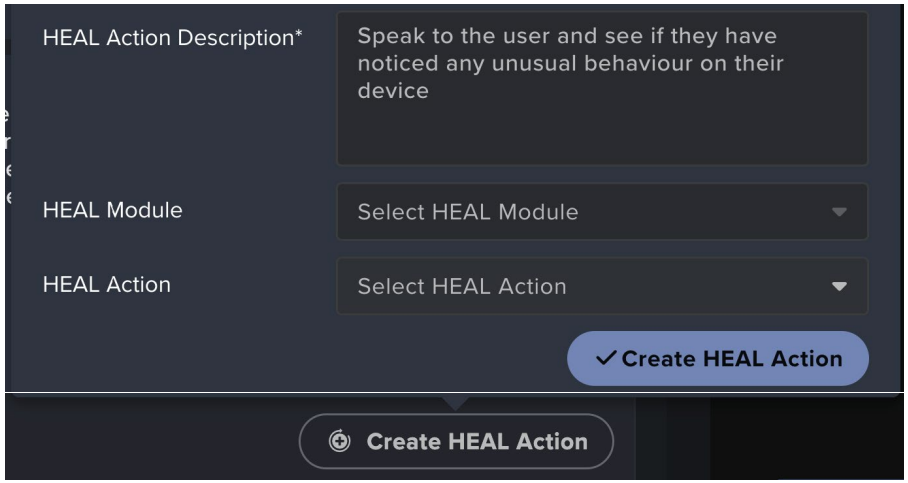
Note: Integrations will be further explored in their dedicated section in the next chapter.

v. Finally, click on the **menu icon** to **View HEAL Log**, which is a pop-up window for the **HEAL Log**.

The log accumulates all HEAL actions on the selected entity with time stamps to reflect it in the incident report. **Manual log entries** can be added at any point.

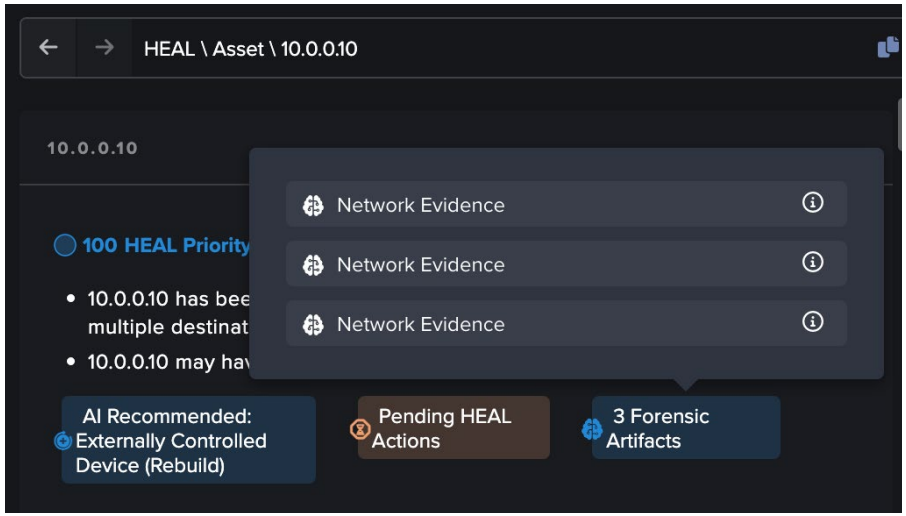


c. If a HEAL integration has been set up, scroll down and click on **Create HEAL Action** to add a personalised action.

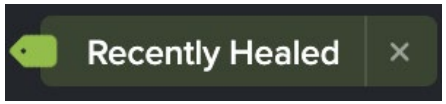


Note: Integrations will be further explored in their dedicated section in the next chapter.

d. Once HEAL steps have been carried out you can see **further options**. In this example PCAPs were taken as part of **gathering forensic evidence** and clicking on it allows you to **download** the PCAP.



e. Once an asset has been involved in a HEAL activity, it will get a **Recently Healed** tag added, which will expire after 1 week.



Top Tip

Once you have gone through all the available steps, your incident has been resolved and you can move on to the next Darktrace Incident.

Note that not all Darktrace Incidents will require HEAL actions to be taken, in this case, the HEAL section of the incident will not be available.

Recommended Workflow Chapter Test

This page will test your knowledge and check your understanding of the Recommended Workflow section.
Select an answer by clicking on it. Wrong answers are denoted by a red cross and right answers are denoted by a green tick.
You can clear all the answers and try again at any time by clicking the button to the right.

Clear All Answers

1. During which step would you apply suggested actions?

- [ ] DETECT Incidents
- [ ] RESPOND Actions
- [ ] PREVENT Assets

2. Where would you find more information about specific connections and events?

- [ ] DETECT Summary text
- [ ] The Model Breach Event Log
- [ ] Darktrace Incident Timeline

3. RESPOND Actions can be applied to specific connections and interactions.

- [ ] True
- [ ] False

4. HEAL actions are always available for all Darktrace incidents.

- [ ] True
- [ ] False

5. Which icon will you use to dismiss a HEAL action?

6. Where can you view high priority risks which need to be mitigated?

- [ ] Darktrace/Proactive Exposure Management
- [ ] Threat Visualizer
- [ ] Darktrace Incident

5. Key Features

In this chapter, we will show how to test a variety of plans and processes, and build staff experience based on detailed, bespoke scenarios to ensure the team can act instinctively when an incident occurs. Additionally, reports can be pulled at any time to give an understanding of tech stack readiness.

Training Simulations

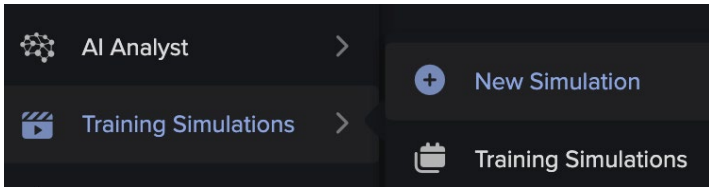
From the Threat Visualizer main menu, navigate to **Training Simulations** to access the two available pages:

- **New Simulation**, which allows you to create or schedule a new training incident, and
- **Training Simulations** displaying a history of all past, current and future simulations.

Continue your learning with our dedicated video 8: Training Simulations

New Simulation

Schedule a simulated incident for training purposes. Simulated incidents are clearly marked as such to all viewers and any RESPOND and HEAL actions relating to them are also simulated instead of taken.



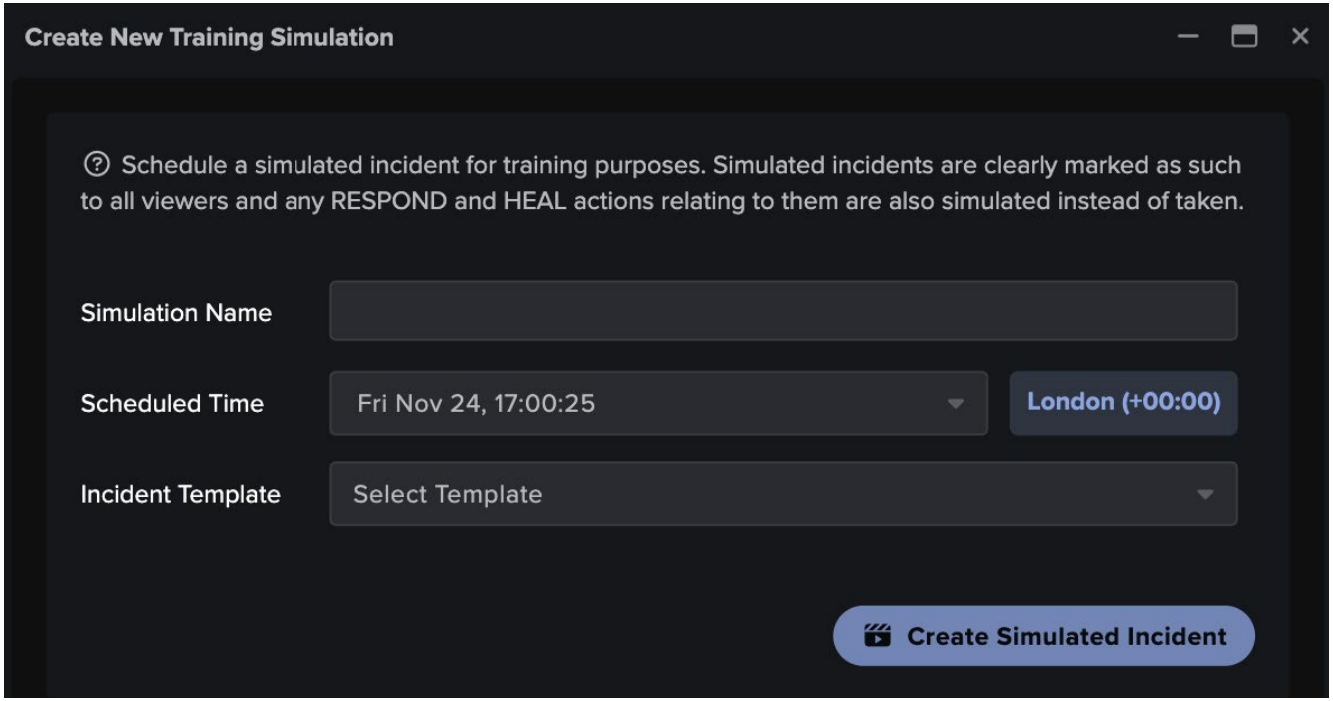
1. To create a new simulation, navigate to **New Simulation** from the Threat Visualizer's main menu.

2. This will open a new window titled **Create New Training Simulation**.

   a. Start with entering a unique **Simulation Name**.

   b. Decide when you would like this simulation to start by inputting the **Scheduled Time**, including the timezone.

   c. Select one of the available templates from the **Incident Template** drop-down menu.



3. Once you have chosen an Incident Template, **details** of this template will be available with the following sections:

   a. Complete **Template Details** with contextualised information will help users with determining if this simulation is the best option for the intended purpose.

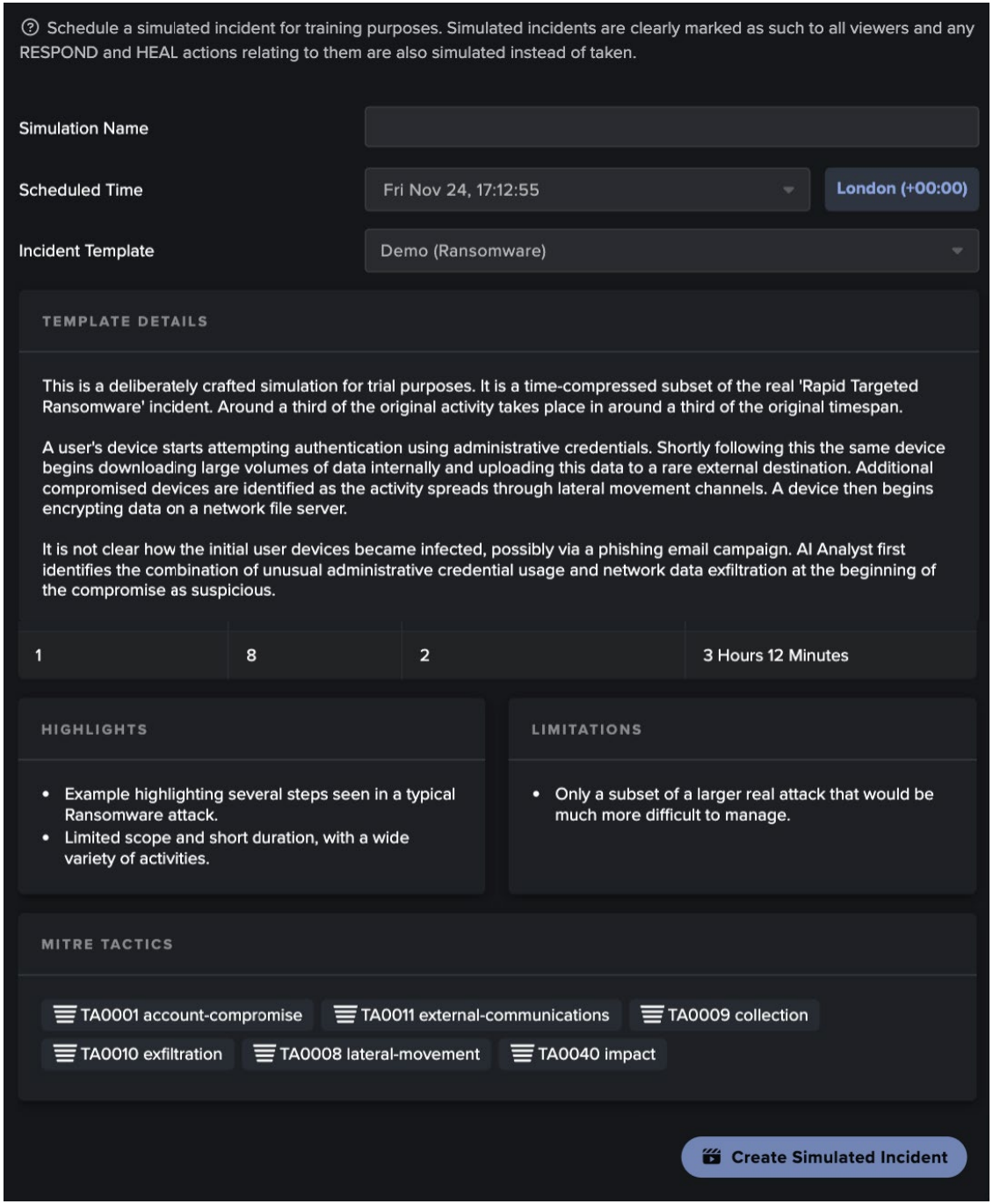
   b. Data on the **Total Incidents**, **Total Devices**, **Total External Endpoints** involved and the **Simulation Duration** will be displayed.

   Note: Simulations might run over several hours or days with the length being determined once the first incident event occurs.

   c. **Highlights** and **Limitations** of the simulation will reflect real-life examples.

   d. The **Mitre Tactics** involved will also be listed.

4. Finally, click on **Create Simulation Incident**, which will now appear on the Training Simulations page, in the planning tab.

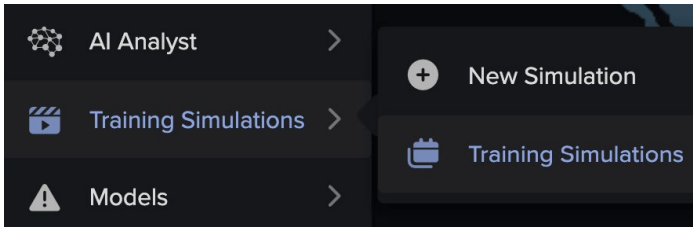


Top Tip

These theoretical simulations can help checking for IT Security gaps while testing your processes and teams.

Users and devices are not impacted by training simulations.

Training Simulations

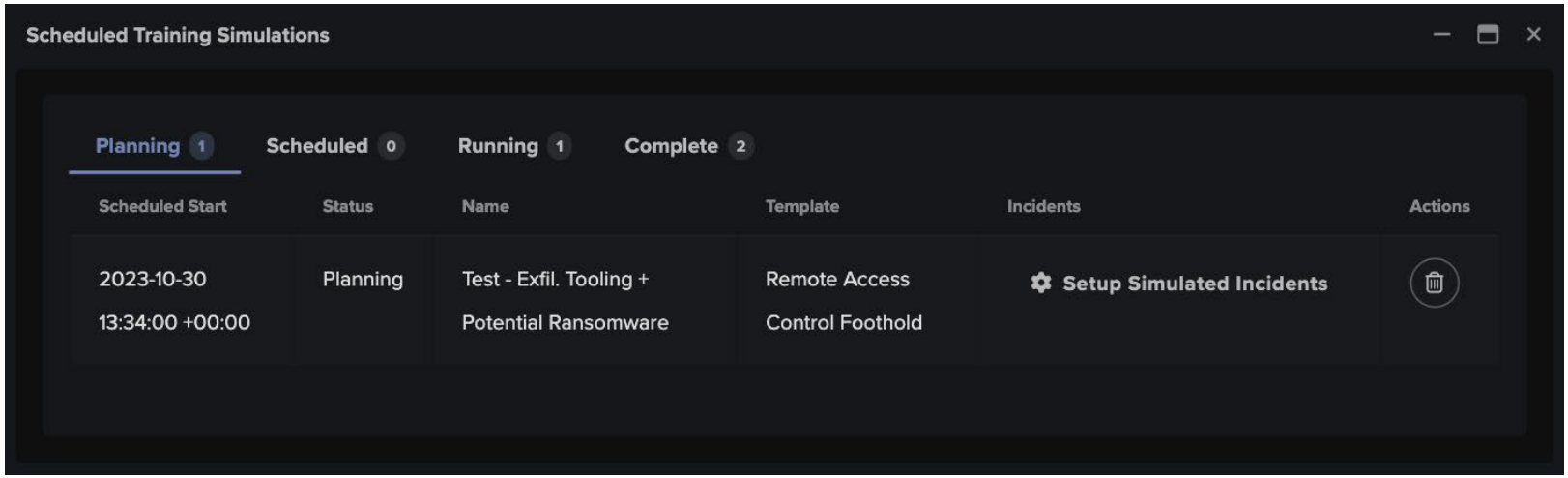


All simulated incidents can be seen from the Training Simulations page to check on their status.

1. To view simulations, navigate to the **Training Simulation** page from the Threat Visualizer's main menu.

2. The **Schedule Training Simulations** window will open, where four different tabs are available:

   - **Planning**, for incidents which are currently being planned.
   - **Scheduled**, for incidents which have been planned to run at a later date.
   - **Running**, for incident which are currently active.
   - **Complete**, for incidents which are now over.



3. The four tabs will show similar information, displaying the **Scheduled Start**, **Status**, **Name**, **Template**, **Incidents** and **Actions**.

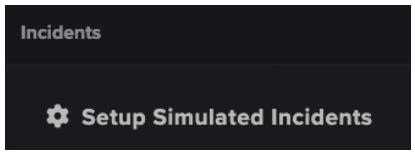
   a. The **Scheduled Start** can show future dates (Planning and Scheduled) or past dates (Running and Complete) to indicate when the simulation will start or has started.

   b. The **Status** column will inform users if a simulation has been planned, scheduled, is running or complete.

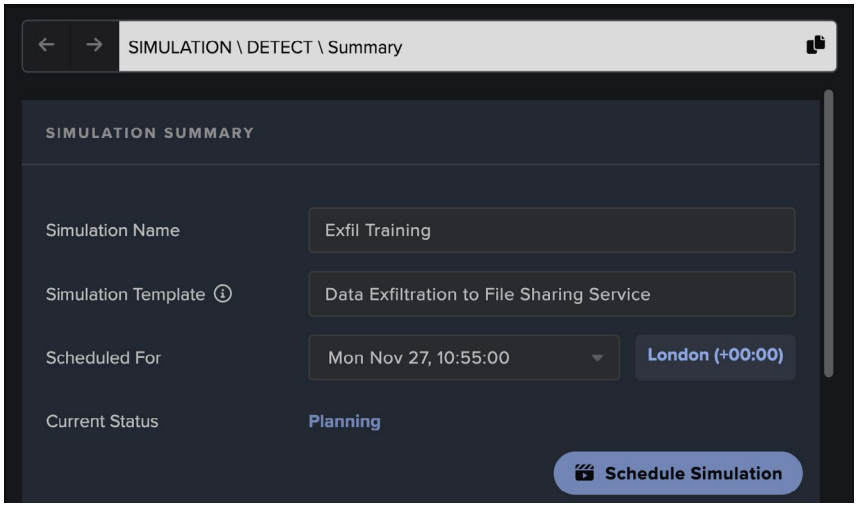
   c. The **Name** of the simulation can be set up by users during the simulation creation step to make each simulation unique and easily recognizable.

   d. The simulation's **Template** will also be reflected so users can easily know the focus of this simulation.

e. The **Incidents** column will allow user to modify the simulation's parameters. Click on the **cog icon** to open the simulation's parameters.



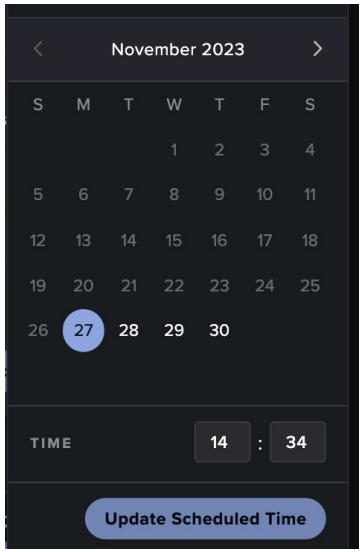
i. The **Simulation\DETECT\Summary** will open, with the **Simulation Summary** available at the top.



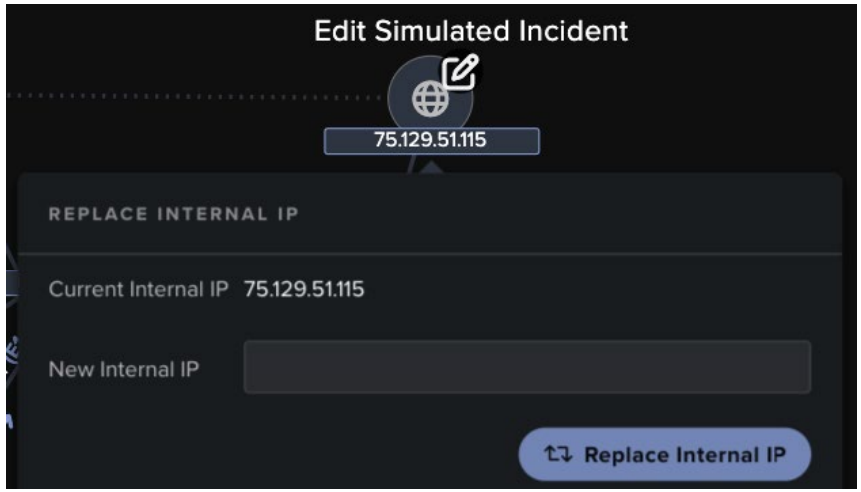
ii. The **Scheduled For** section can be changed by clicking on the drop-down menu and using the calendar available.

Click on **Update Scheduled Time** to save the changes.

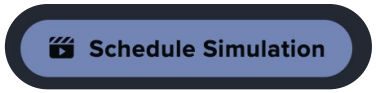
Note: The Simulation Name and Template cannot be changed.



iii. To make the simulation as realistic as possible, it is highly encouraged to edit assets involved. If available, click on the **edit icon** to replace the **Internal IP**, **device** or **hostname** and click on the **Replace** button to confirm.

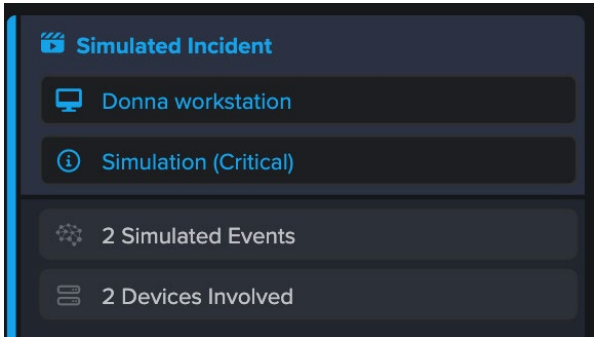


iv. Click on **Schedule Simulation** to confirm it. The simulation will be moved to the Scheduled column until it is Running or Unscheduled.



f. The final column is **Actions**, where planned and scheduled simulations can be deleted by clicking on the **bin icon**.

4. Once active, **Simulated Incidents** will appear in **blue** in the Threat Tray.



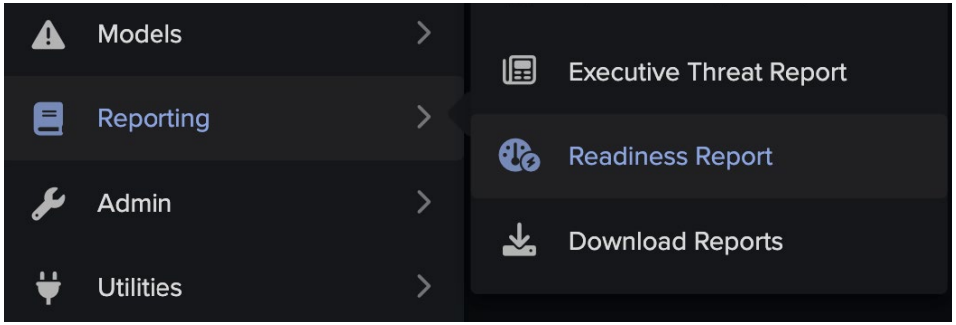
Continue your learning with our dedicated video 9: Readiness Report and Playbook Manager

Readiness Report

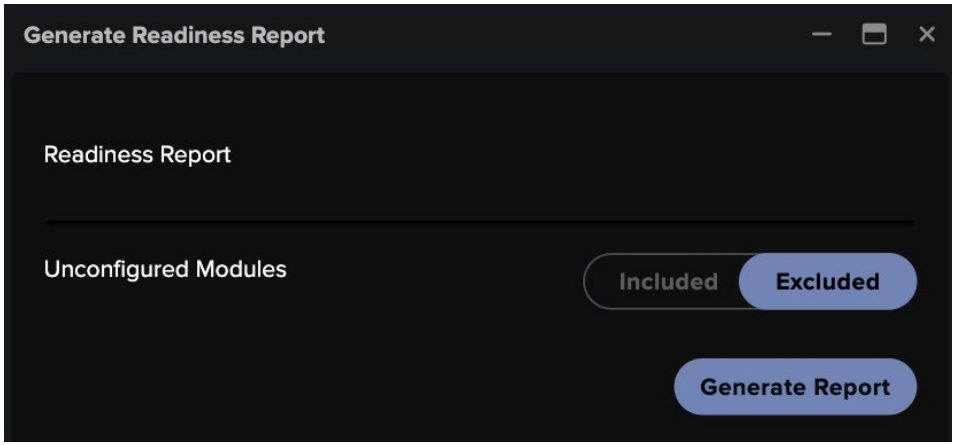
Readiness reports can be pulled at any time to give an understanding of tech stack readiness. The report displays currently deployed capabilities, security and workflow integrations, telemetry modules and vulnerability scanning.

The data contained in each report is specific to your organization and includes specific information such as the configuration status of each element, when it was last active along with its readiness (Ready, Check or Warning).

1. From the Threat Visualizer main menu, go to **Reporting** and select the **Readiness Report** option.



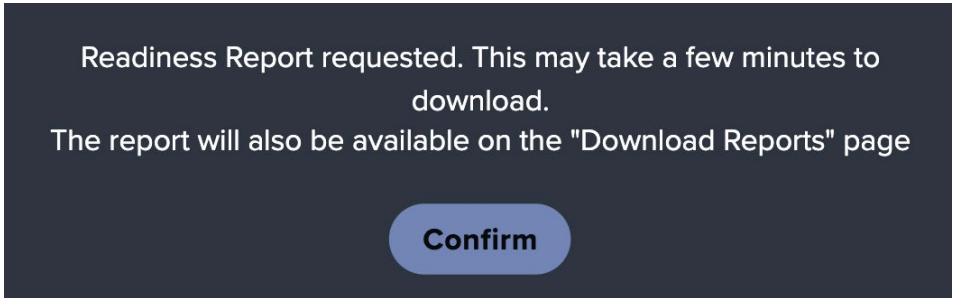
2. This opens the **Generate Readiness Report** window allowing for the generation of a Readiness Report.



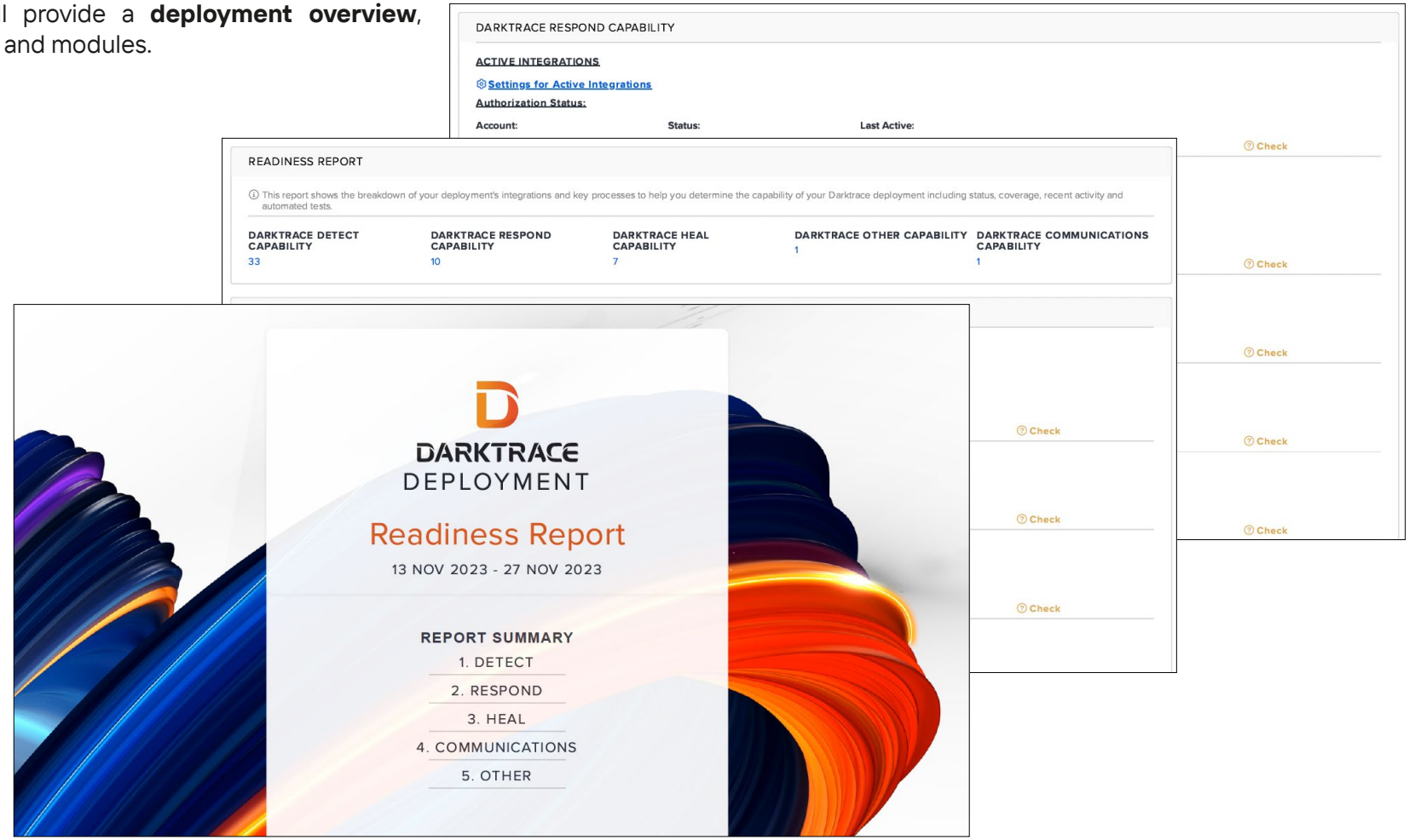
3. Select whether or not you wish to include **Unconfigured Modules** by using the available toggle.

4. Click the **Generate Report** button at the bottom of the window.

5. A **confirmation** will appear before the report is **downloaded**.



6. The Readiness Report will provide a **deployment overview**, including security coverage and modules.



Top Tip

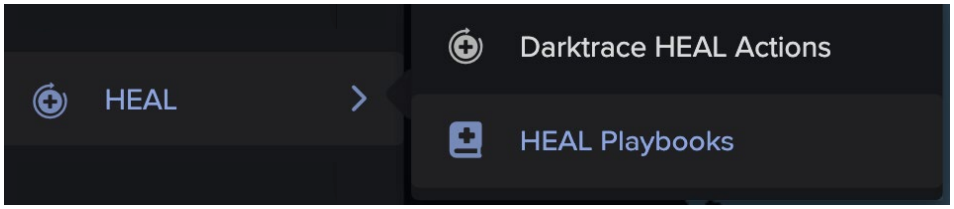
The Readiness Report will show how ready your deployment is by including a status next to each element:

- **Ready**, in green, means that this element has been fully deployed and is running as expected.
- **Check**, in orange, means that this element should be checked as it might not be running as expected.
- **Warning** , in red, means that this element has not yet been fully deployed or is not available on your deployment.

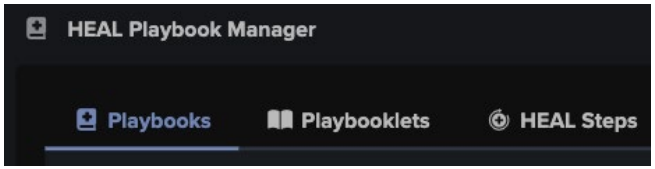
Playbook Manager

When incidents occur, Darktrace's dynamic playbooks adapt responses automatically to precise incident details. You can also create and edit HEAL Playbooks to include your organisation's IT remediation protocol steps.

1. From the Threat Visualizer main menu, go to **HEAL** and select the **HEAL Playbooks** option.



2. This will open the **HEAL Playbook Manager** window which is comprised of three distinct tabs:



   a. **Playbooks**: Each Playbook is made of a set of Playbooklets that are made of a set of specific HEAL Steps. You can edit a Playbook's strategy and description by managing its constituent Playbooklets

   b. **Playbooklets**: Each Playbooklet is made of a set of specific HEAL Steps. You can edit a Playbooklet's strategy and description by managing its constituent HEAL Steps.

   c. **HEAL Steps**: Individual HEAL Steps are the building blocks for Playbooklets, instructions for a unique step in a recovery process. They can be customised from the defaults or new ones created. HEAL Steps are first organised into five types and have a secondary ordering within each type. Playbooklets that use multiple HEAL Steps retain this organisation.

HEAL Steps

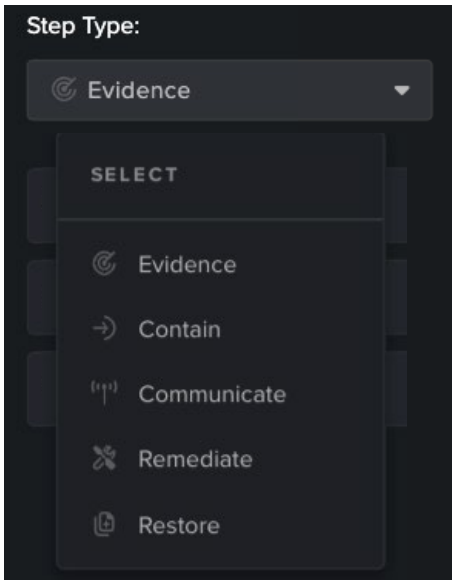
1. Click on the **HEAL Steps** tab to start editing existing steps or creating new ones.

Note: Modifying or creating Steps will impact the existing Playbooklets and Playbooks.

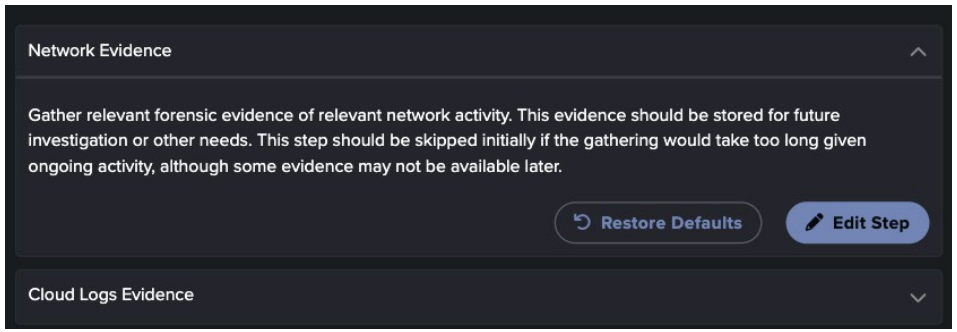
2. First, select the desired **Step Type** using the drop-down menu. There are five step types available:

   - Evidence
   - Contain
   - Communicate
   - Remediate
   - Restore

Note: The order of these steps follow the healing process of a device.



3. The list of **specific steps** will be available for each step type. Click on the **downward arrow** to open the full step's description.

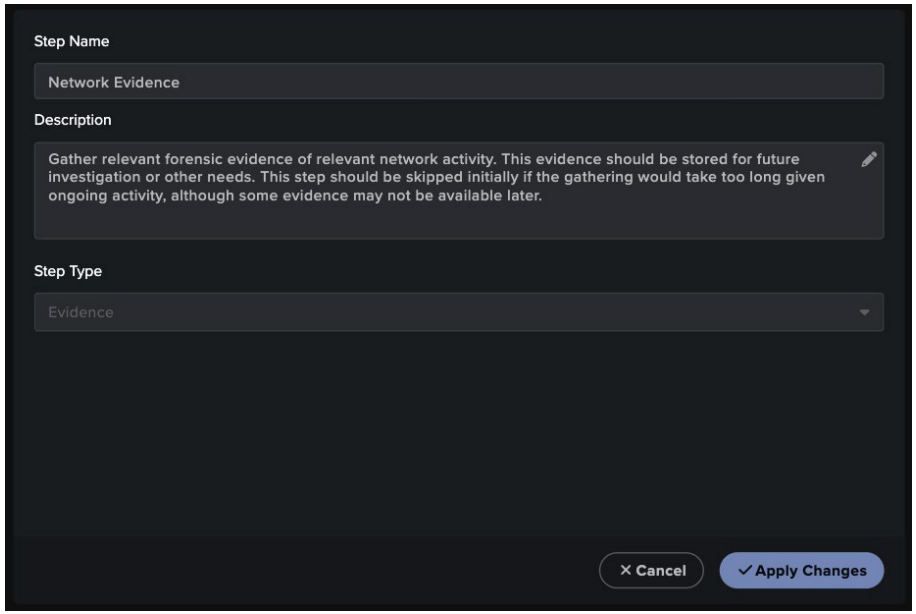


a. If a steps has been modified in the past, click on the **Restore Defaults** button to restore the selected steps to its original settings.

Note: Any edits made will not be overwritten by System updates to Playbooks, Playboooklets or steps.

b. Clicking on **Edit Step** will allow user to modify the description of the step.

c. Once the **Description** of the step has been edited, you can **Apply Changes** or alternatively **Cancel**.

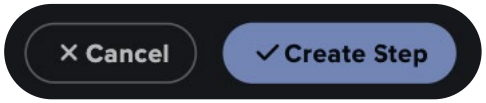


Note: The Step Name and the Step Type cannot be modified.

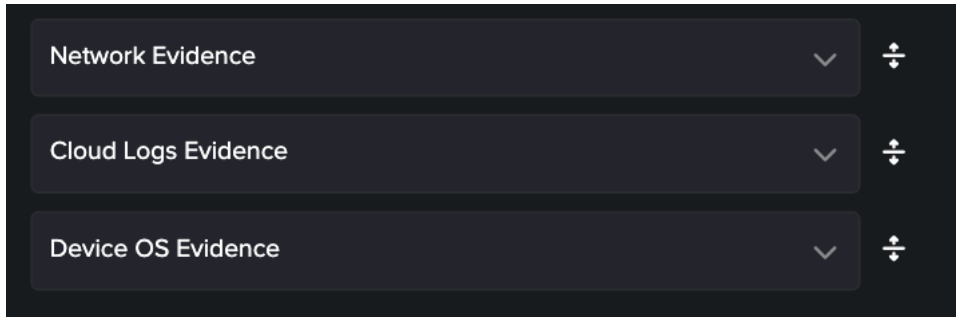
4. New steps can also be created by clicking on **Create Step**.

a. All fields can be completed, starting by the **Step Name** and then the **Description**. Users are also able to choose the **Step Type** amongst the five previously mentioned.

b. Once all fields have been completed, you can **Create Step** or alternatively **Cancel**.

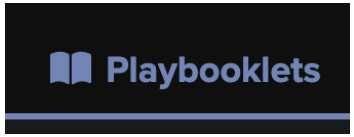


5. Finally, all steps of a specific Step Type can be **reordered** by clicking and dragging the **arrows** at the end of each step's row.



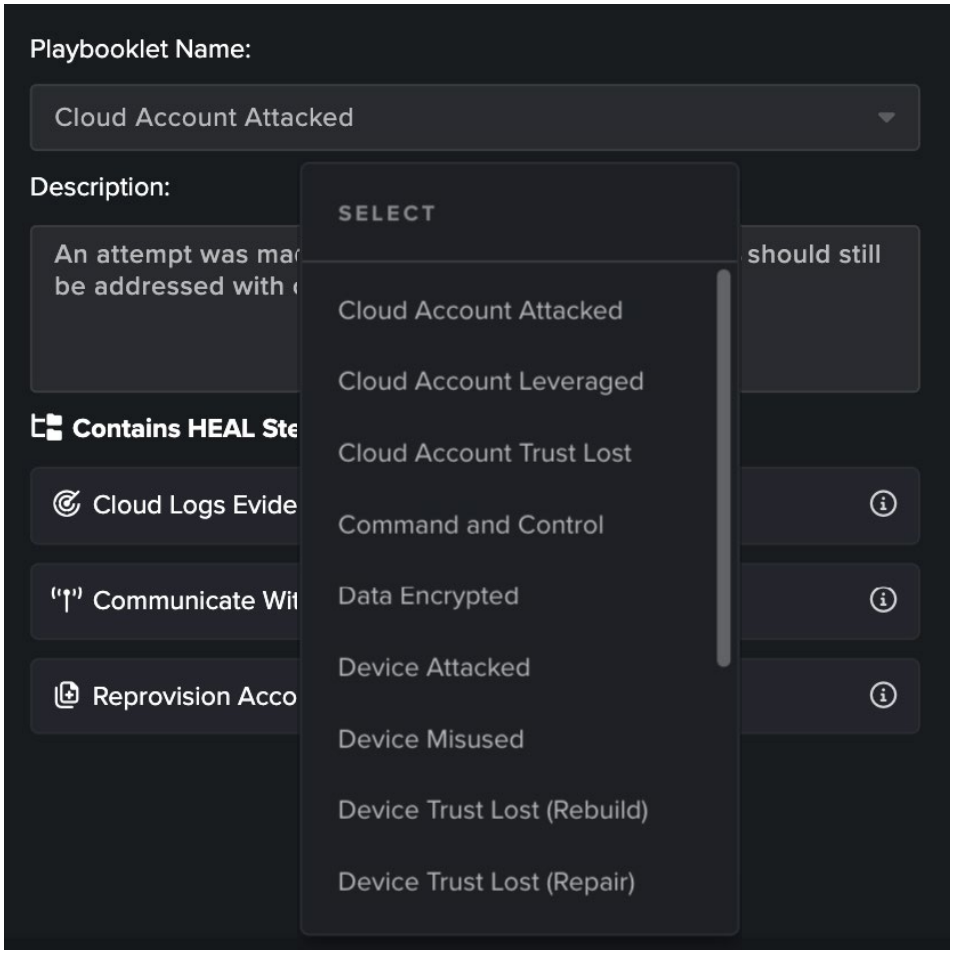
Playbooklets

1. Click on the **Playbooklets** tab to start editing existing playbooklets or creating new ones.

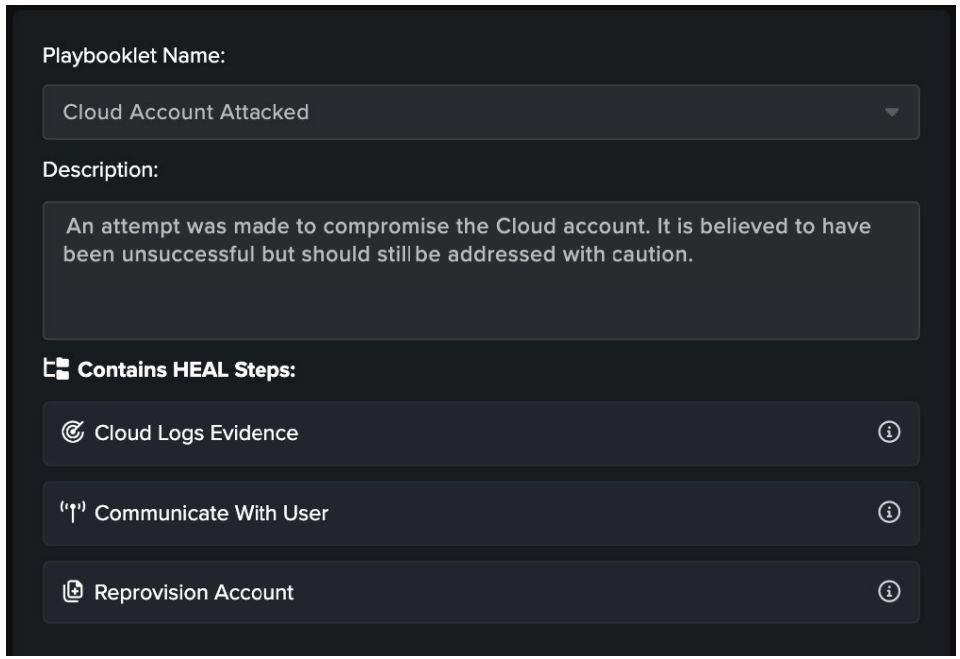


Note: Modifying or creating Playbooklets will impact the existing Playbooks but not the Steps.

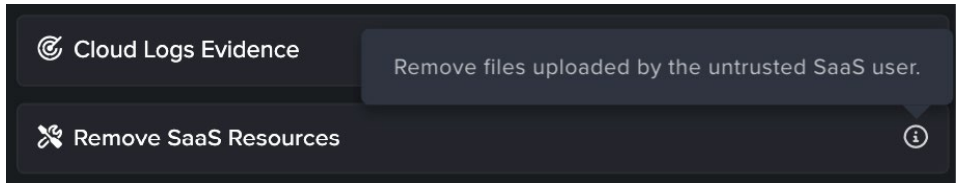
2. First, select the desired **Playbooklet** using the drop-down menu, where all existing playbooklets will be available.



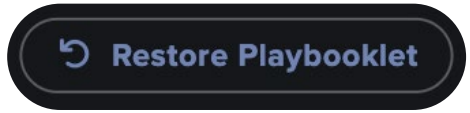
3. Once selected, detailed information about the Playbooklet will be available such as the **Description** and the **HEAL Steps** involved.



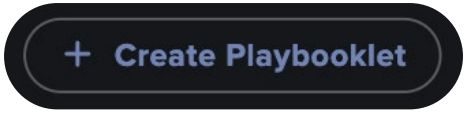
4. Hovering over the **info icon** of one of the HEAL Steps will provide a full **description**.



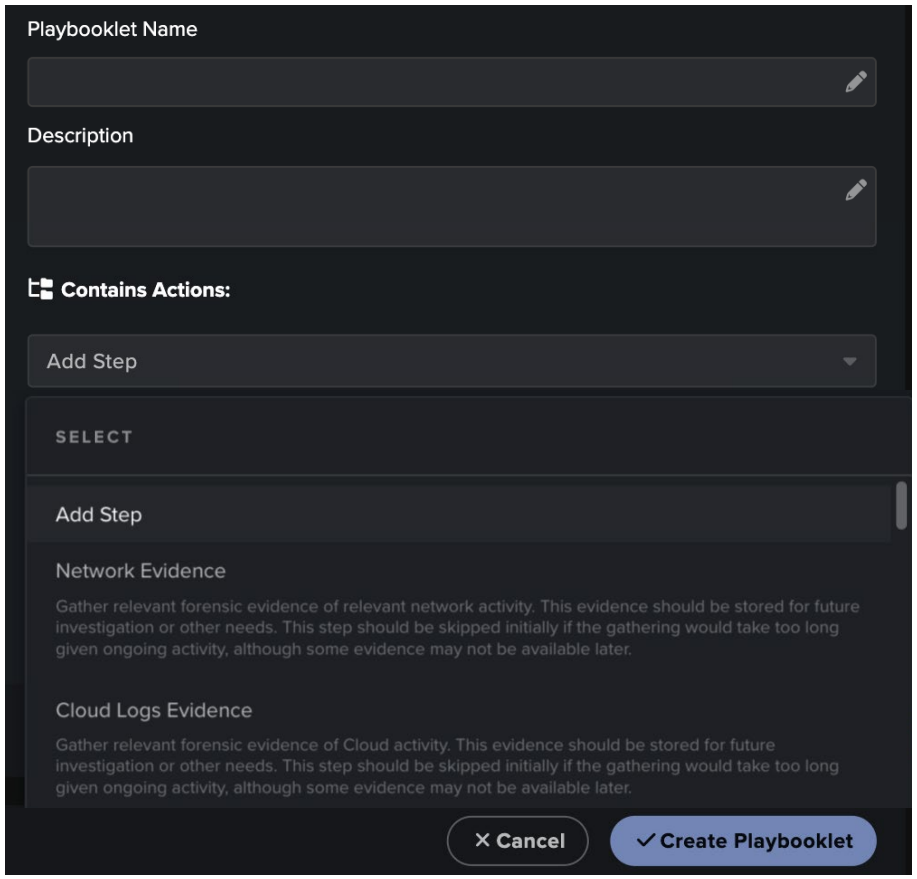
5. If a playbooklet has been modified in the past, click on the **Restore Playbooklet** button to restore it to its original settings.



6. Clicking on **Create Playbooklet** will allow the user to create a new playbooklet.



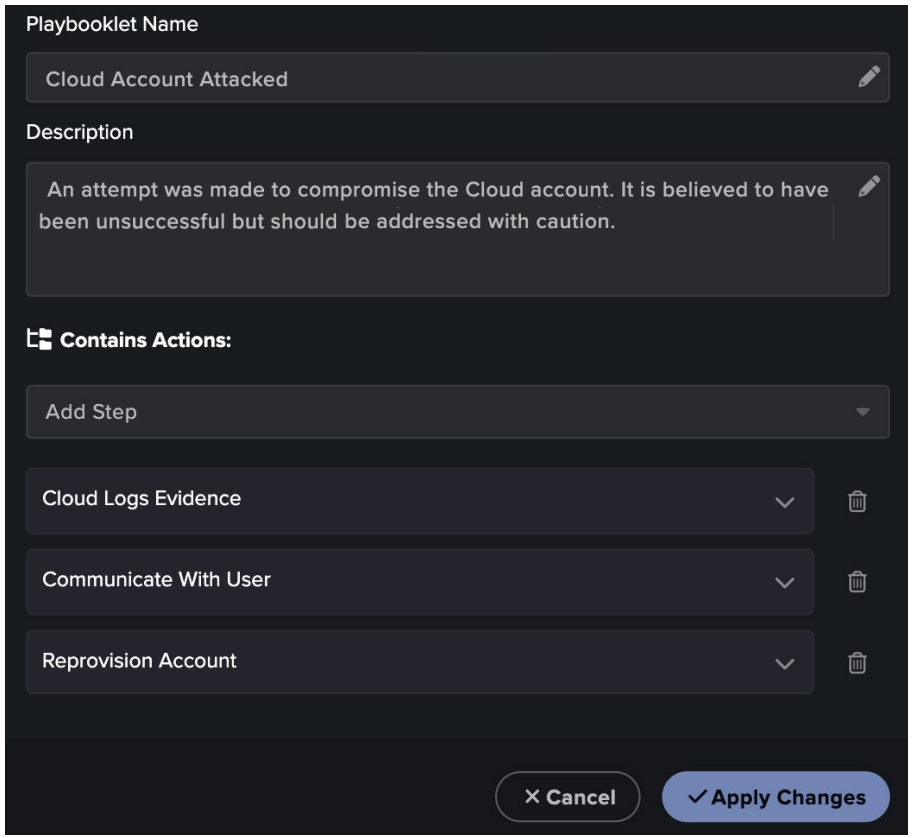
   a. All fields can be completed, starting by the **Playbooklet Name** and then the **Description**. Users are also able to add different existing steps by choosing them from the **Add Step** drop-down menu.



   b. Once all fields have been completed, you can **Create Playbooklet** or alternatively **Cancel**.

7. Clicking on **Edit Playbooklet** will allow the user to edit the selected playbooklet.

   a. Start by editing the **Playbooklet Name** and **Description**.



   b. The Steps available in the Playbooklet can be edited in the **Contains Actions** section. Click on the drop-down menu to **Add Steps**.

   c. Alternatively, click on the **bin icon** to **delete** steps.

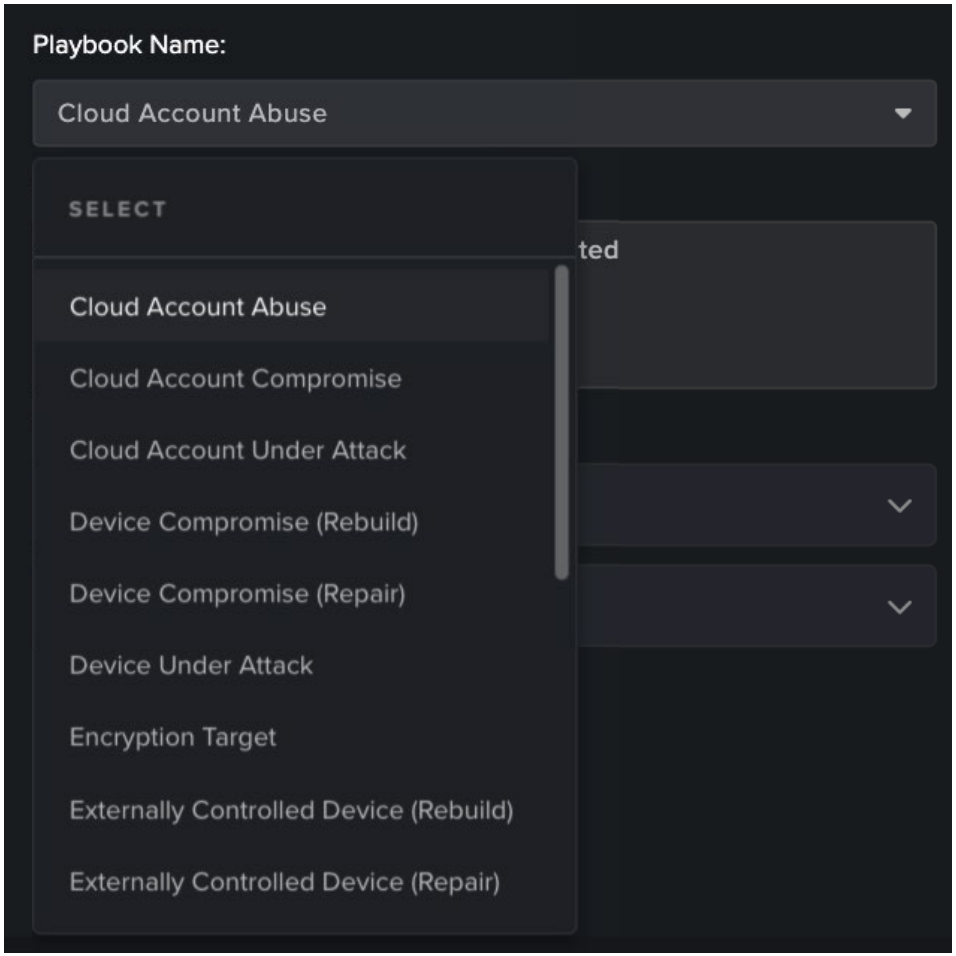
   d. Once the playbooklet has been edited, you can **Apply Changes** or alternatively **Cancel**.

Playbooks

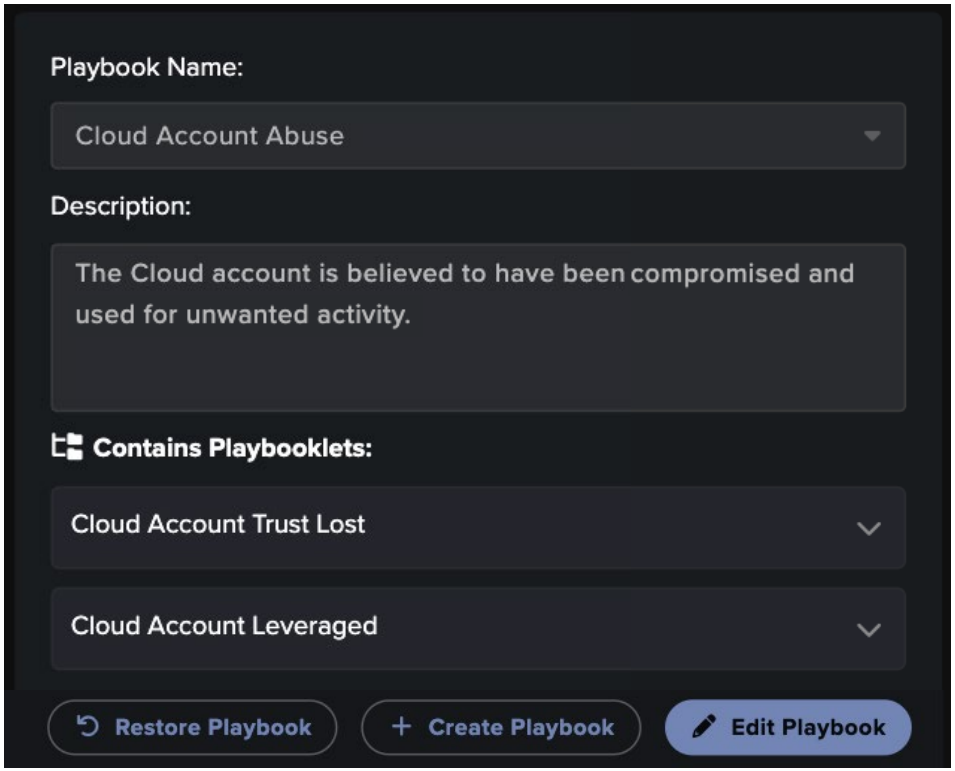
1. Click on the **Playbooks** tab to start editing existing playbooks or creating new ones.

   Note: Modifying or creating Playbooks will not impact the existing Playbooklets or Steps.

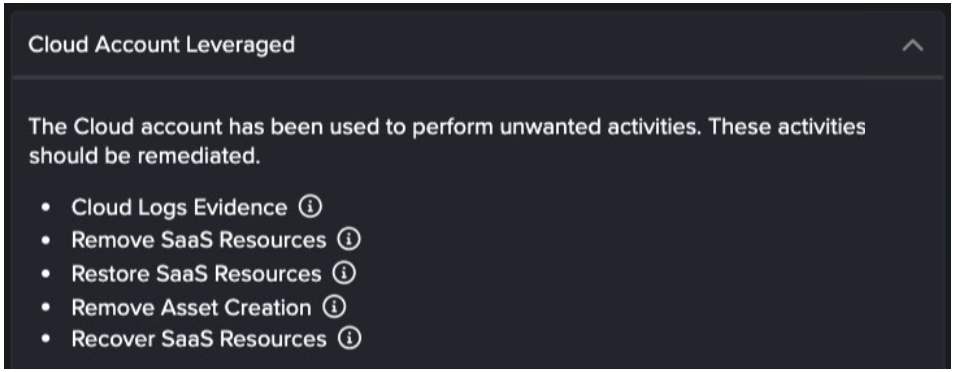
2. First, select the desired **Playbook** using the drop-down menu, where all existing playbooks will be available.



3. Once selected, detailed information about the Playbook will be available such as the **Description** and the **Playbooklets** involved.



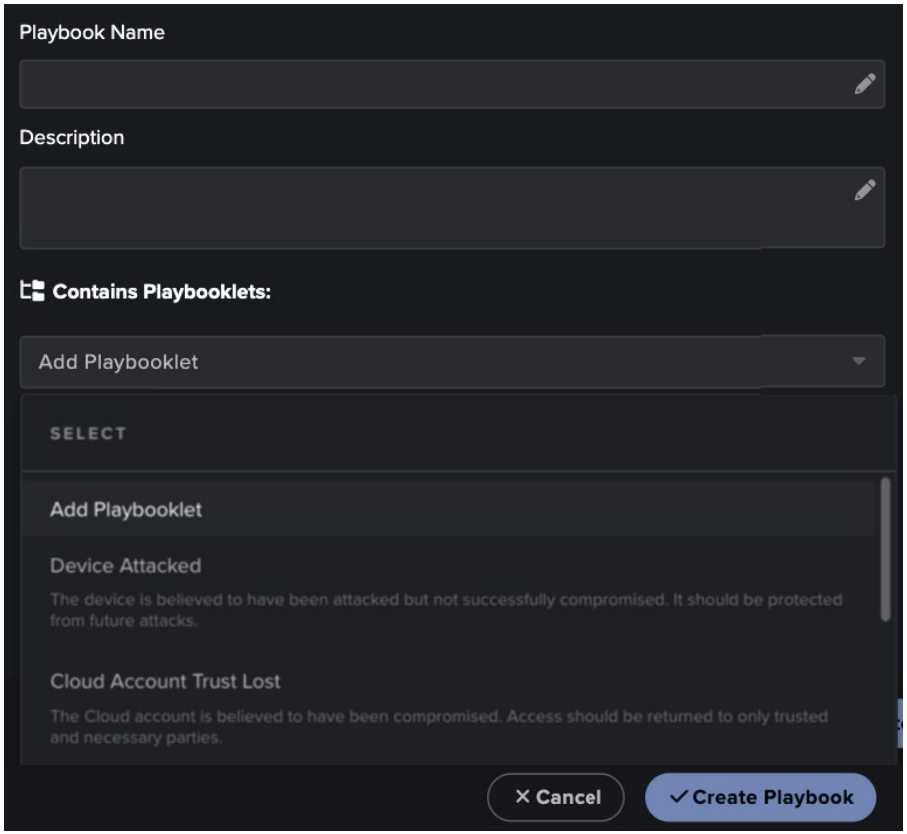
4. Clicking on the **downward arrrow** of one of the Playbooklets will provide a full **description**, including **Steps** involved.



5. If a playbook has been modified in the past, click on the **Restore Playbook** button to restore it to its original settings.

6. Clicking on **Create Playbook** will allow the user to create a new playbook.

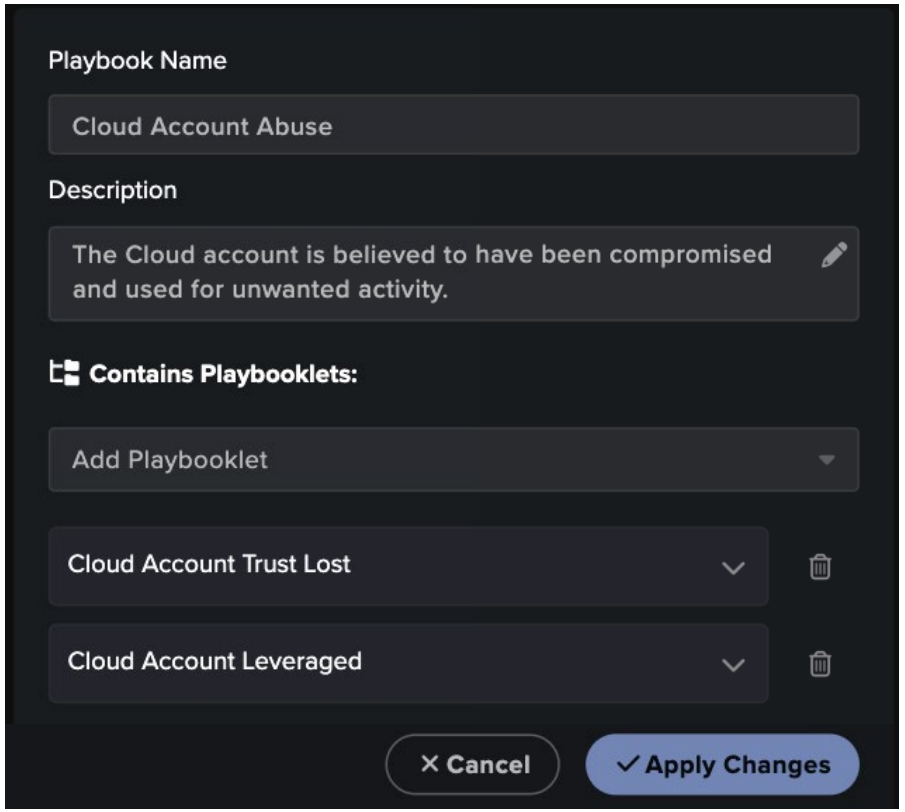
   a. All fields can be completed, starting by the **Playbook Name** and then the **Description**. Users can add different existing playbooklets by choosing them from the **Add Playbooklet** drop-down menu.



   b. Once all fields have been completed, you can **Create Playbook** or alternatively **Cancel**.

7. Clicking on **Edit Playbook** will allow the user to edit the selected playbook.

   a. Start by editing the **Playbook Name** and **Description**.



   b. The Playbooklets available in the Playbook can be edited in the **Contains Playbooklets** section. Click on the drop-down menu to **Add Playbooklet**.

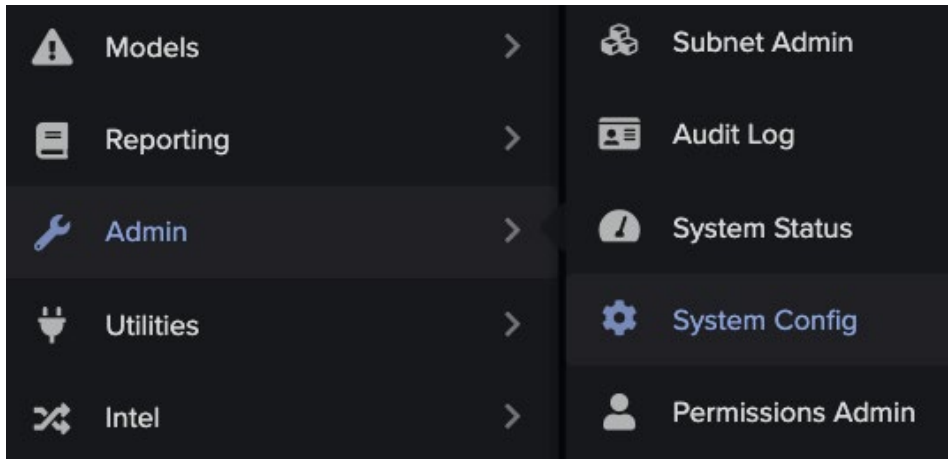
   c. Alternatively, click on the **bin icon** to **delete** playbooklets.

   d. Once the the playbook has been edited, you can **Apply Changes** or alternatively **Cancel**.

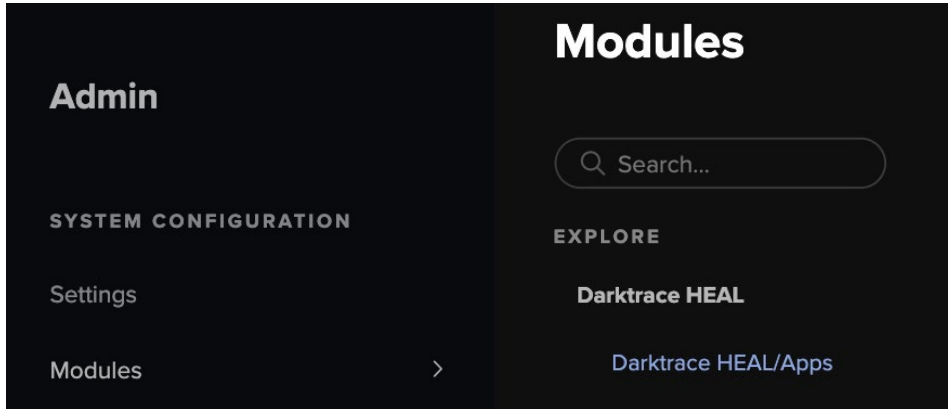
Integrations

Darktrace offers a variety of Darktrace Incident Readiness & Recovery integrations, which can all be authorized within the Darktrace System Config, including Acronis, Duo, Google, Jamf, Microsoft and Veeam. There is also a ServiceNow Ticketing module which can be configured to facilitate ticketing systems. To enable any of these modules, a license is required.

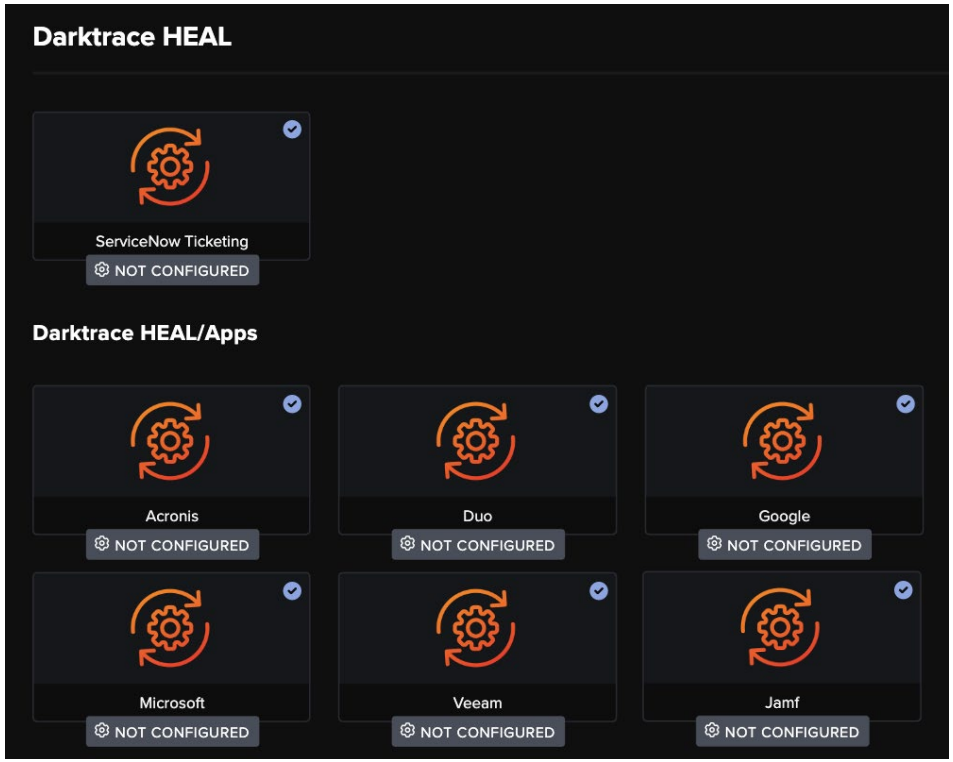
1. Navigate to the **System Config** page from the main menu.



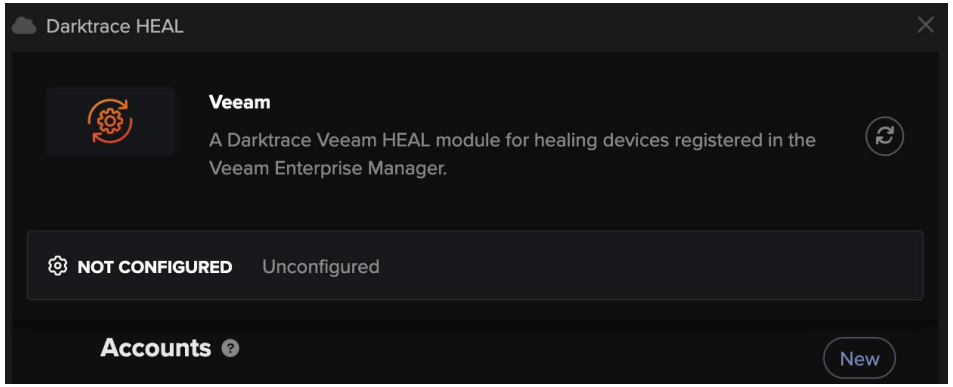
2. Within the Modules menu, navigate to the **Darktrace HEAL** subsection which will show modules for Darktrace Incident Readiness & Recovery.



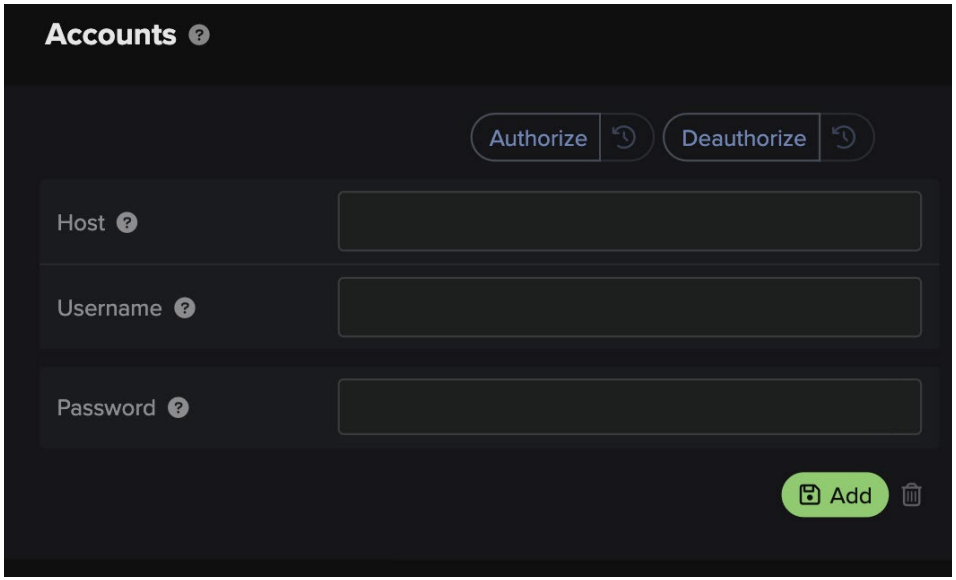
3. Modules in the **Darktrace HEAL** section can have different status depending whether or not they are in use.



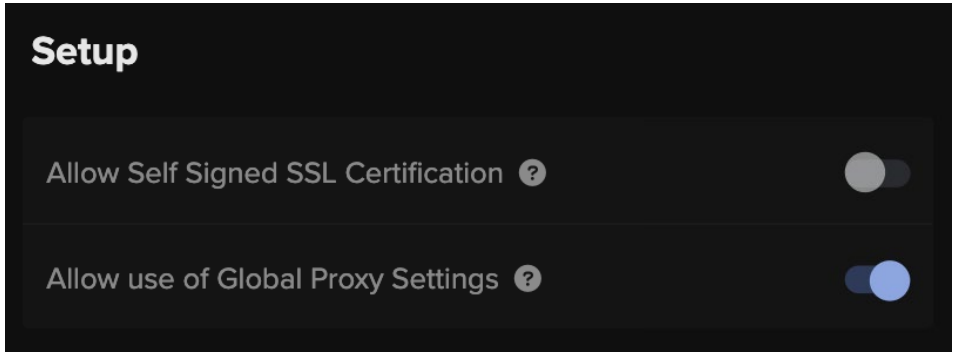
4. Within the Darktrace module window, click the **New** button to add a new account.



5. Clicking on the New Account button will open up more **fields**. Fill these out using the **tooltips** for assistance. Once completed, click the **Authorize** button above these fields.

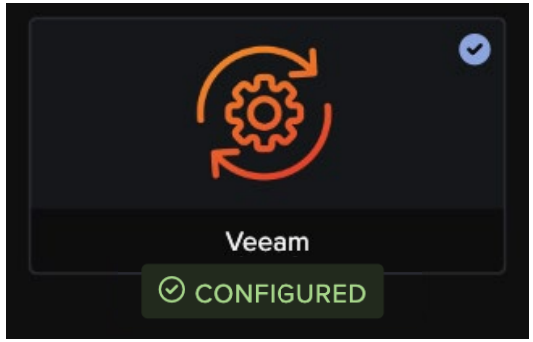


6. Optionally, scroll down the window and configure the **proxy server** details and **additional settings**.



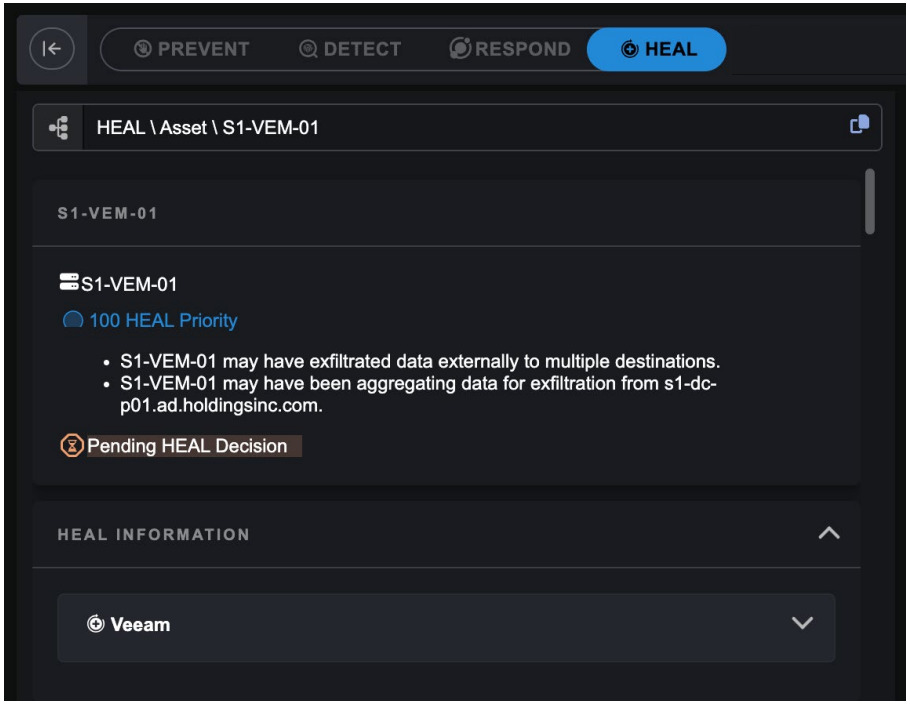
7. Click **Save** at the top of the window to confirm the configurations of the module.

8. When the module has been successfully configured, a message will appear within the **Status** section of the window.

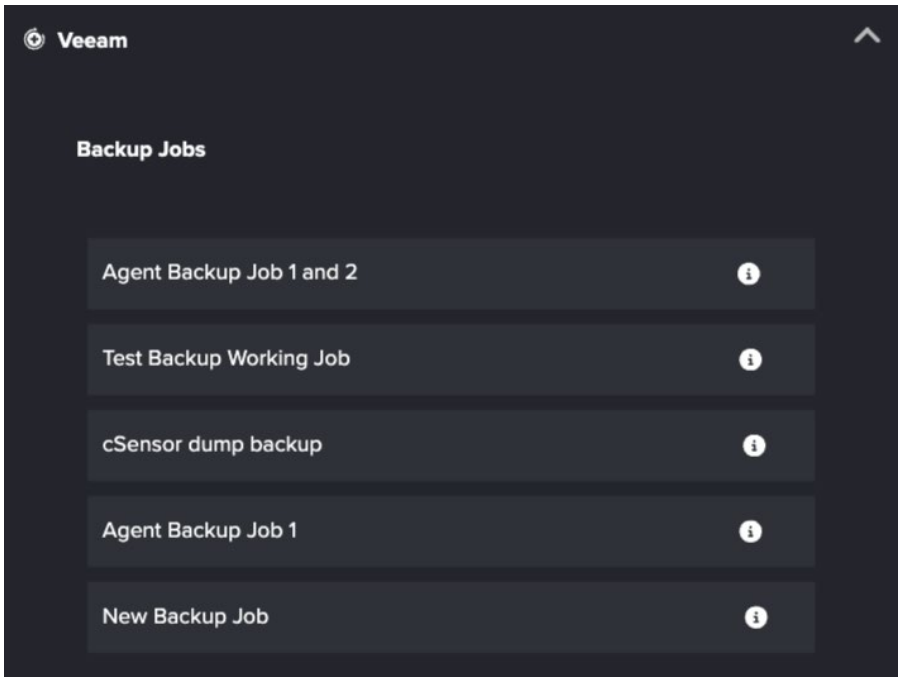


9. Depending on which module has been configured, there might be **extra features** available in Darktrace/Incident Readiness & Recovery.

   a. For example, **Veeam** integration will be available under the **HEAL\ Asset** tab.



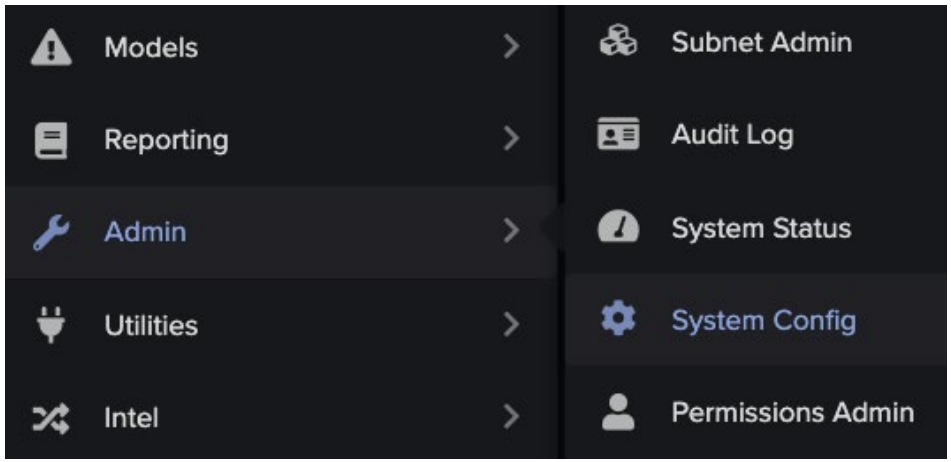
b. Click on the **drop-down menu** available to see more information and options.



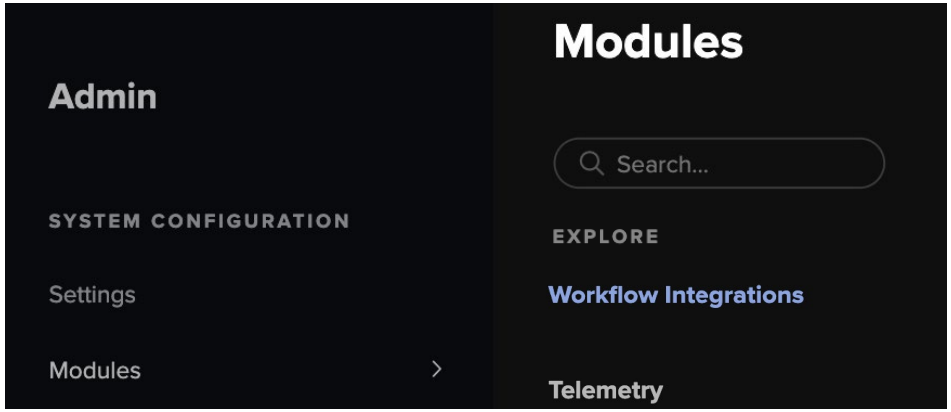
Darktrace Communicator

Darktrace Communicator is a module for configuring third party communications and alerting people of detected incidents and issues.

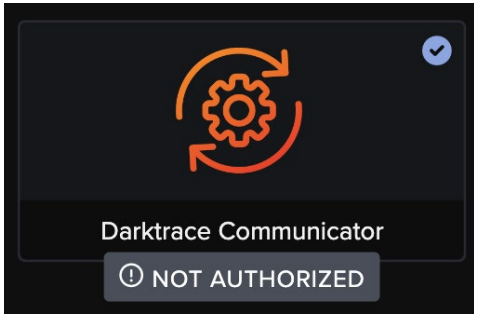
1. Navigate to the **System Config** page from the main menu.



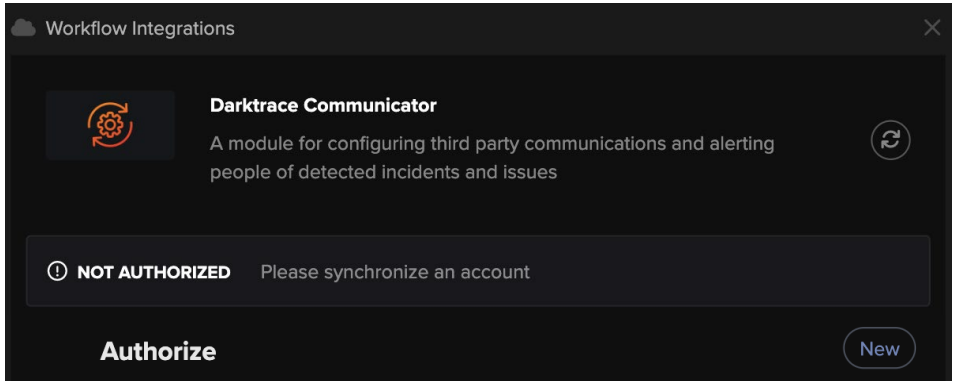
2. Within the Modules menu, navigate to the **Workflow Integrations** subsection which is where the Darktrace Communicator module is.



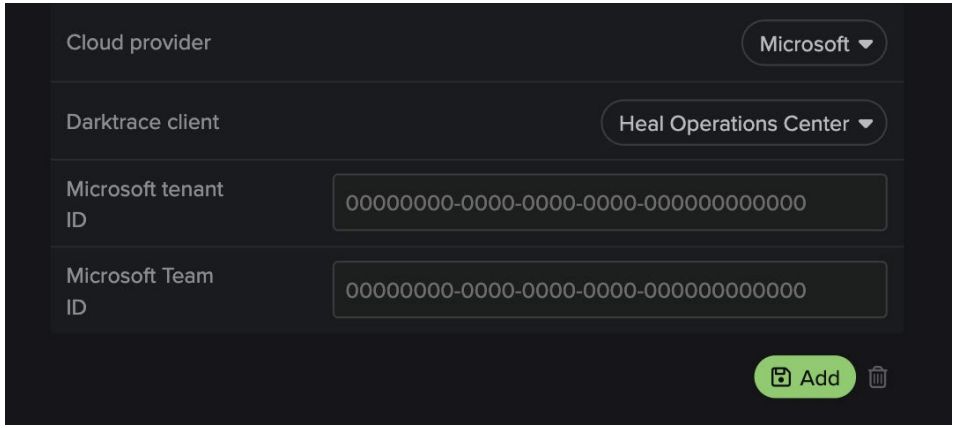
3. If not authorized, click on the **Darktrace Communicator** module to open the settings window.



4. Clicking on the New Account button will open up more **fields**.

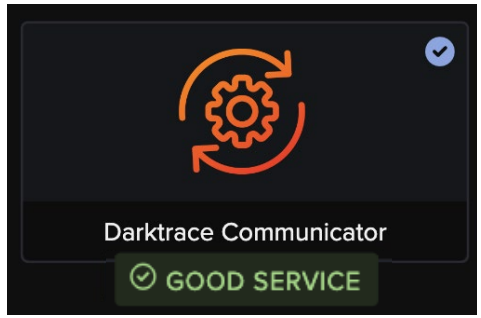


5. Choose between Microsoft or Slack and fill out the information requested. Once completed, click the **Add** button.



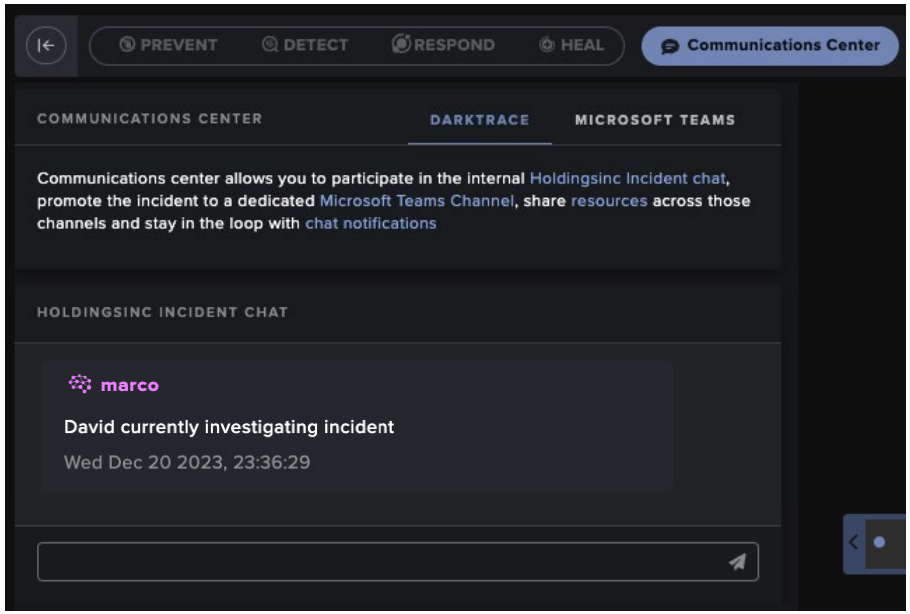
6. Click **Save** at the top of the window to confirm the configurations of the module.

7. When the module has been successfully configured, a message will appear within the **Status** section of the window.



8. Once the Communication Centre has been authorized and synchronized, an extra option will be available when clicking on the **Communication Centre** button available within a Darktrace Incident.

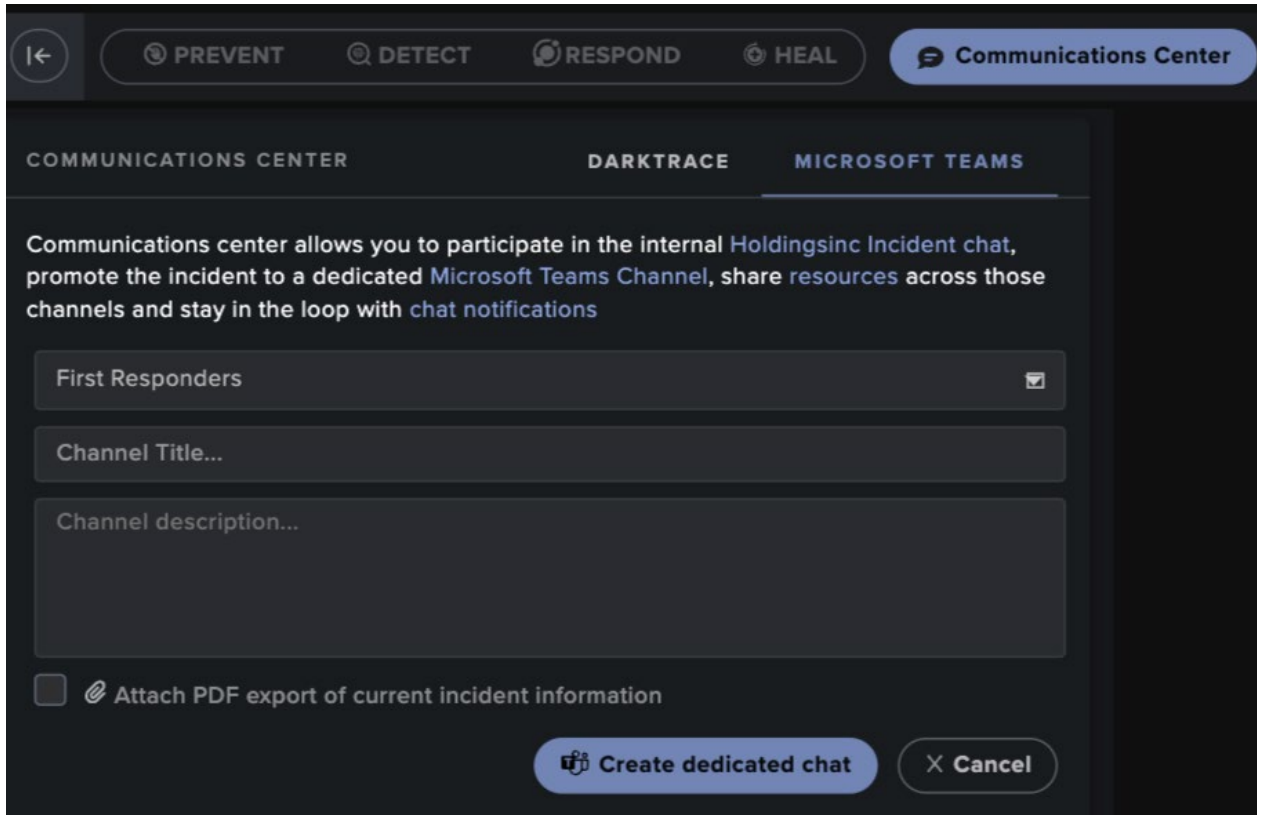
   a. The internal chat available by default within the interface will still be accessible under the **Darktrace** tab.



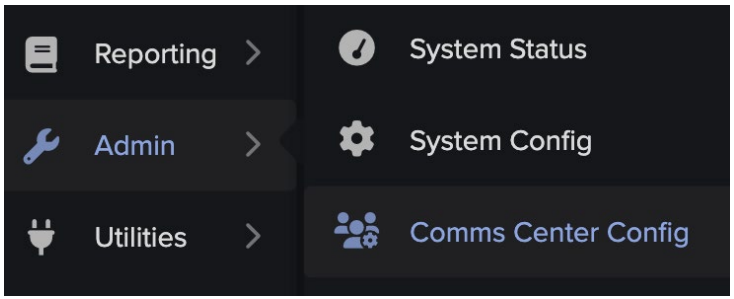
b. An extra tab will also be available so you can create an external chat linked to either **Microsoft Teams** or **Slack**, available from its dedicated tab.

You can configure the chat from the Darktrace Incident by choosing from the list of configured **Responders**, adding a **Channel Title** and a **Channel Description** and tick the **Attach PDF export of current Incident information** option.

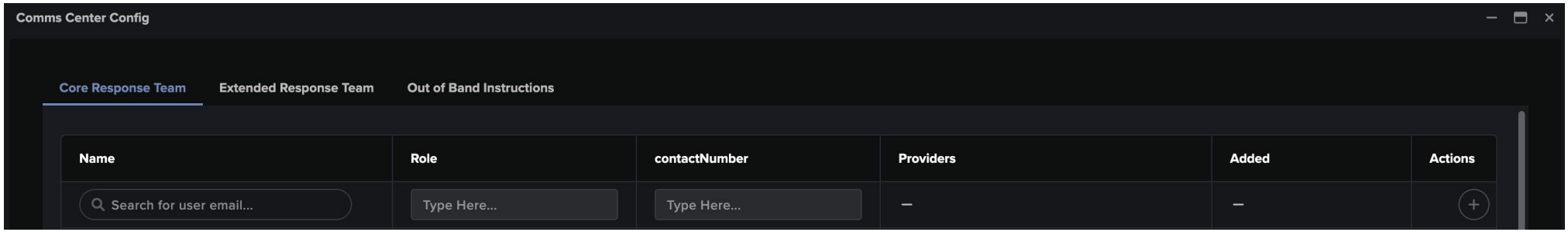
Once you have configured the chat, click on the **Create dedicated chat** button to take this conversation to your choosen app.



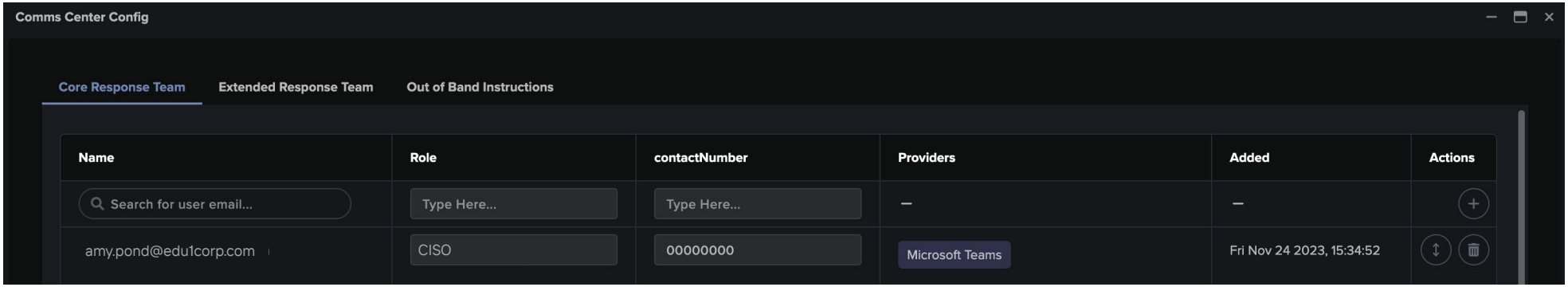
9. To determine your list of Responders, navigate to the main menu and click on **Comms Center Config** under the Admin menu.



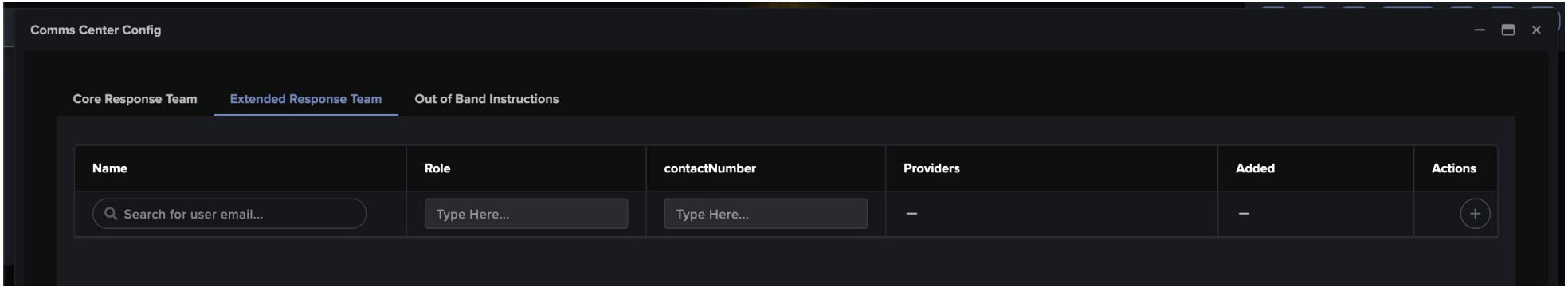
10. This will open a new window from which you can configure your **Core Response Team**, **Extended Response Team** and **Out of Band Instructions**.



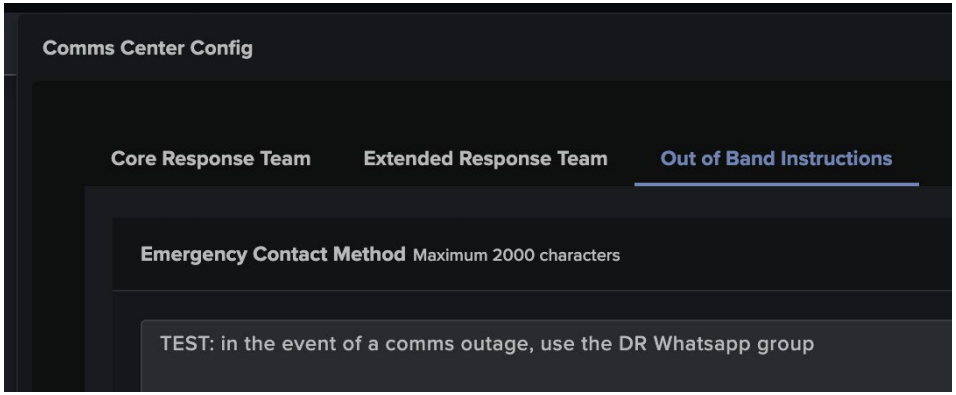
a. Under the **Core Response Team** tab, include who will be your First Responders by inputting their details: Name, Role, Contact Number and Providers (Microsoft Teams or Slack). The date and time of when they have been added will be available along with some Actions such as adding a responder, moving responders within the list or deleting them.



b. Under the **Extended Response Team** tab, include who will be your next responders by inputting the same details as for the Core Response Team.



c. Under the **Out of Band Instructions** tab, include any protocols to follow when neither the Core Response nor the Extented Response Teams are available.



Darktrace HEAL Actions

The different HEAL modules can also be used to create specific HEAL actions and manually add them to the selected HEAL Playbook of an incident.

1. Under Heal\Asset, access a step of an active Playbook and scroll down to the **Create HEAL Action** button.

   a. The first mandatory field is the **HEAL Action Description**. If the action is outside of Darktrace environment, there is no need to choose a Module or an Action.

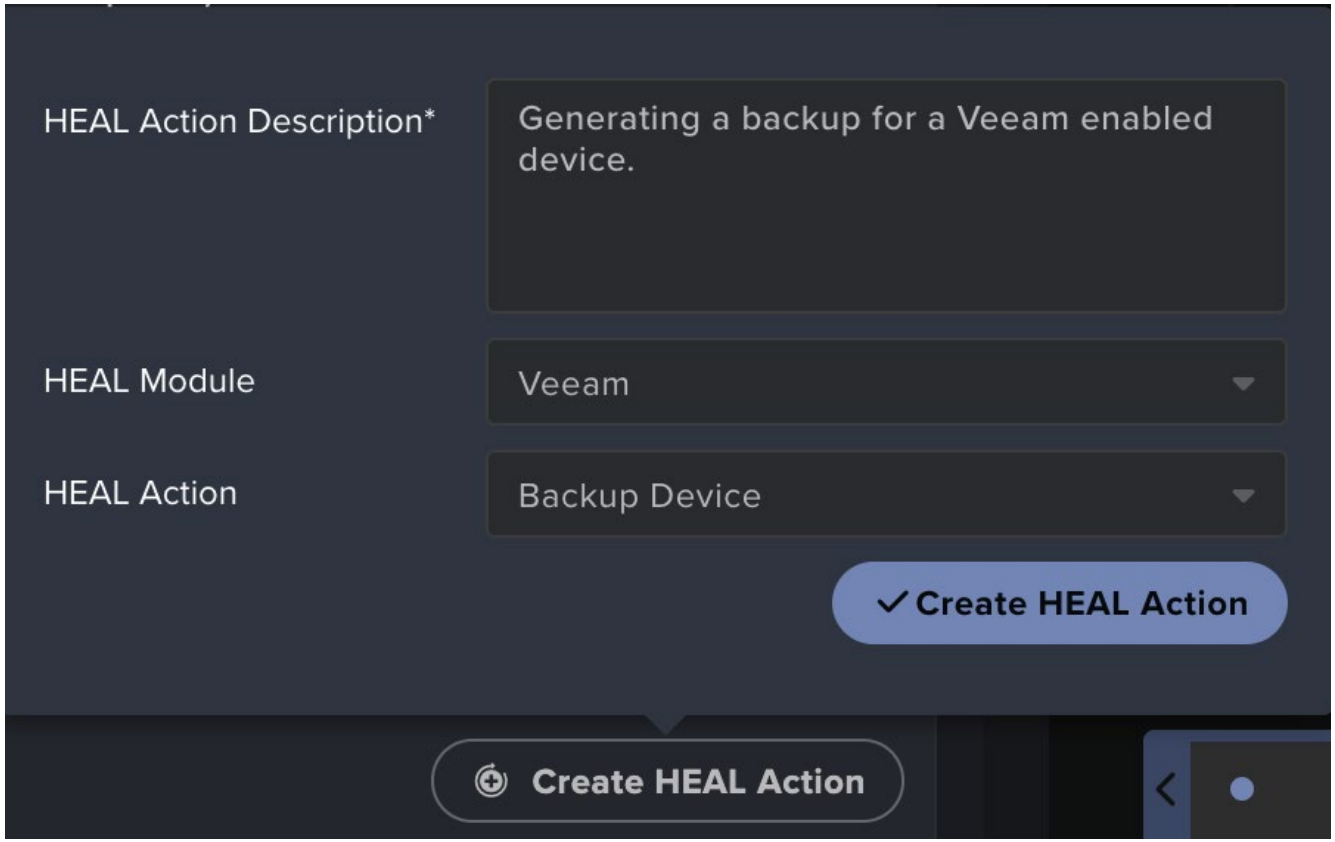
      This is for example the case should you need to speak with the user directly.

   b. If using one of your active integrations, click on the **Select HEAL Module** drop-down menu to access the modules available on your environment.

      Note: The desired HEAL Modules will need to have been authorized from the System Config page, as previously described.

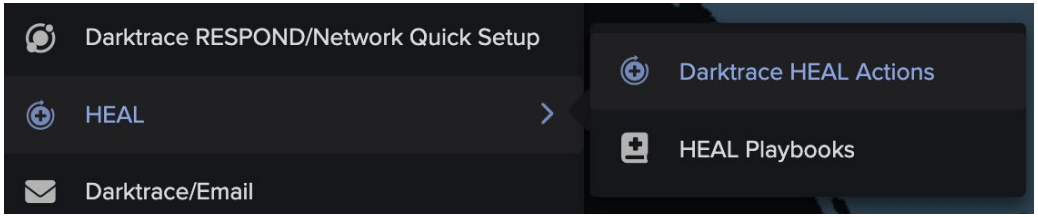
   c. Next, click on the **Select HEAL Action** drop-down menu to access the actions available for the selected Module.

      Each module will have specific actions available, for example, Veeam will enable you to back up the device or remove users from groups.

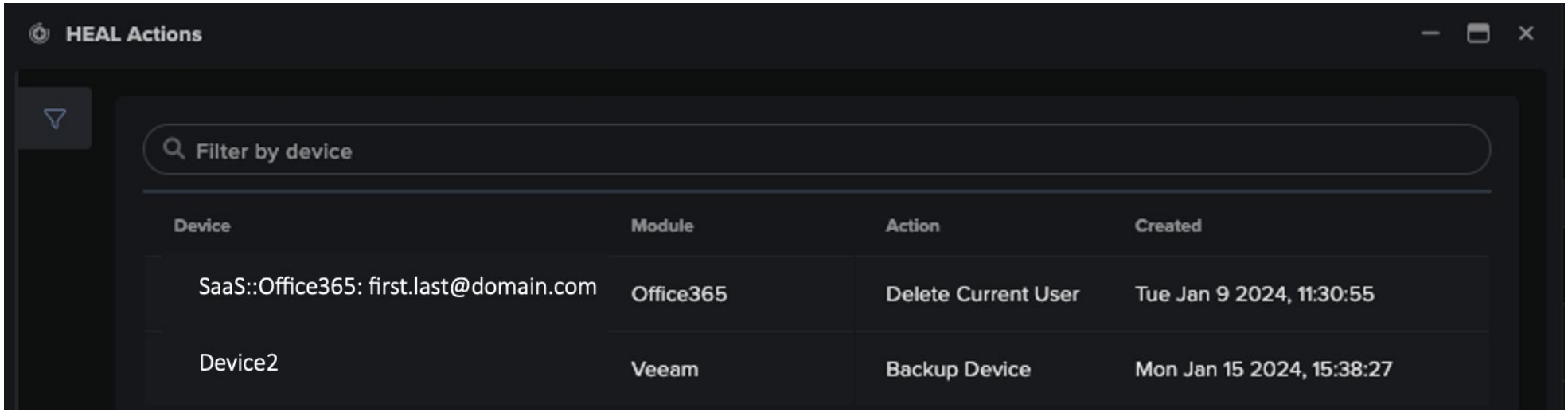


   d. Finally, click on **Create HEAL Action** to add the action to the HEAL Playbook steps of the selected incident. The action will now be available from the HEAL\Asset tab and can be interacted with the same way as with other steps.

2. Once a HEAL Action has been manually added, navigate to **Darktrace HEAL Actions**, accessible under the HEAL section of the main menu.

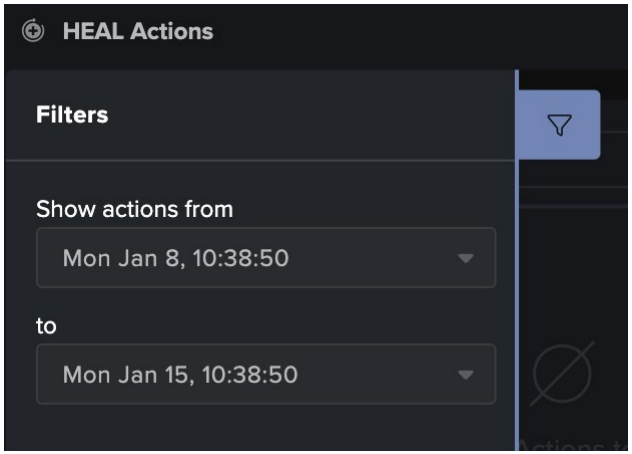


   a. This window will list all **HEAL Actions** which have been manually added to a Darktrace Incident. Each action will reference which **Device** it has been added on as well as the **Module** and **Action** used and when it was **Created**.



Note: Hovering over the device name in the Heal Actions tab will show device details.

   b. Clicking on the **funnel icon** will open the filter panel where user can **show actions from** and **to** specific dates, selecting them from the calendars available.



Key Features Chapter Test

This page will test your knowledge and check your understanding of the Key Features section.
Select an answer by clicking on it. Wrong answers are denoted by a red cross and right answers are denoted by a green tick.
You can clear all the answers and try again at any time by clicking the button to the right.

Clear All Answers

1. Training Simulations can last several days.

- [ ] True
- [ ] False

2. Which colour represents a Training Simulation?

- [ ] Red
- [ ] Green
- [ ] Blue

3. What additional report is available with Darktrace Incident Readiness & Recovery?

- [ ] Healing Report
- [ ] Training Report
- [ ] Readiness Report

4. Users can create Microsoft Teams channel for a specific Darktrace incident.

- [ ] True
- [ ] False

5. Users CANNOT create Playbooks, Playbooklets or Steps.

- [ ] True
- [ ] False

6. Which option enables users to reset a playbook to its default settings?

- [ ] Restore Playbook
- [ ] Create Playbook
- [ ] Edit Playbook

6. Learning Outcomes

Course Agenda Checklist

Continue your learning with our dedicated video
10: Course Summary

Thank you for completing this Darktrace Incident Readiness & Recovery course.

We hope this have given you the confidence to tackle a variety of investigative processes within your deployment.

Contact Us

For all further education inquiries, contact:

EMEA: training-emea@darktrace.com
APAC: training-apac@darktrace.com
AMERICAS: training-amer@darktrace.com

For technical support with your installation, go to https://customerportal.darktrace.com

When contacting support, please make sure you provide as much detail as possible.

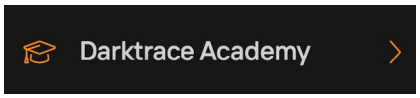
Complete the learning outcomes checklist below:

- **Understand basic concepts** ☐
- **Follow a recommended workflow** ☐
- **Implement training simulations** ☐
- **Manage and add Playbooks** ☐

7. Additional Educational Material

Darktrace Academy Training Resources are designed to maximize your practical skills, understanding, and confidence using Darktrace products. They are available on the Customer Portal at: https://customerportal.darktrace.com/

To access the Training Videos, Courses, and Certification, navigate to Darktrace Academy, and to the resources you require.



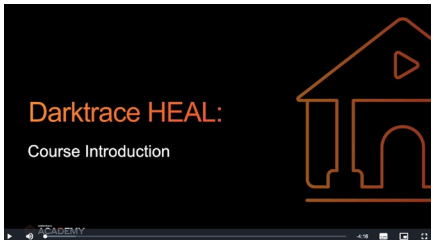
Training Courses

We have a wide range of Training Courses available, in multiple languages, all of which are complimentary for our Customers and Partners.

COURSE	AUDIENCE
Darktrace/Attack Surface Management	All end users
Darktrace/Proactive Exposure Management	All end users
Threat Visualizer Part 1 - Familiarization	All end users
Threat Visualizer Part 2 - Investigation	All end users
Darktrace RESPOND/Network	Administrators and Analysts
Darktrace/Incident Readiness & Recovery	All end users
Cyber Analyst Part 1 – Advanced Analysis	Super Users (Tier 2 Analysts)
Cyber Analyst Part 2 – Model Optimization	Super Users (Tier 2 Analysts)
Cyber Engineer	Partners / Installers
Threat Visualizer Administration	Administrators
Darktrace/Email Part 1 - Familiarization	Administrators and Analysts
Darktrace/Email Part 2 - Customization	Email Administrators
Darktrace/Identity	All end users

Training Videos

Our new self-access Training Videos can be accessed at any time to support your learning.



Darktrace Certification

Darktrace offers Customers and Partners who have attended the appropriate webinars and passed the attendance tests, the opportunity to become officially Darktrace certified through multiple certification paths, as shown below.