DARKTRACE ACADEMY

THREAT VISUALIZER PART 1 - FAMILIARIZATION

Training Manual

Threat Visualizer Part 1 - Familiarization

Training Manual
v3.7.0
Darktrace 6.1

Table of Contents

DARKTRACE ACADEMY

1. Learning Objectives

Course Agenda

Start your learning with our dedicated video
1: Course Introduction

This course outlines some of the foundational elements of the Threat Visualizer interface. This course is designed for a range of Cyber Security professionals including IT Security Managers, IT Security Architects and Cyber Security Analysts. The following document serves as an educational guide for the key elements of Threat Visualizer interface.

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.

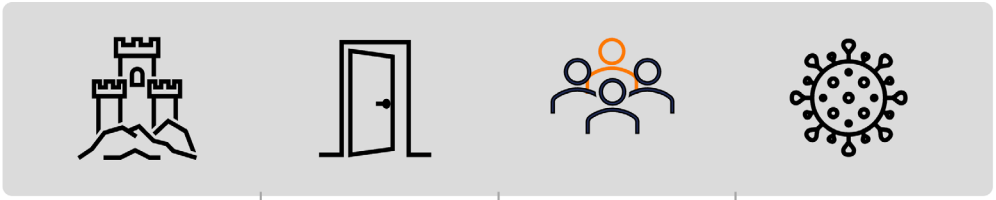
Some elements can be interacted with by clicking on options, hovering over images or typing in the reserved space.

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

- **Understand Darktrace Solutions**
- **Navigate the Threat Visualizer Interface**
- **Obtain basic information about network devices**
- **Investigate Cyber AI Analyst Incidents**
- **Generate reports of network activity**

2. Introduction to Darktrace

Security is a universal problem for everyone, for every company in the world. Attacks are becoming more sophisticated, easier to launch and yet more challenging to solve. Standard security products attempt to recognize these threats to detect signatures and rules, but they are based on having seen these attacks before. These methods no longer work as they need to be kept constantly up to date and they cannot detect new threats.



It is impossible to fully secure your enterprise network	Sophisticated threats will always find a way in	Insider threat is just as important as external threats	It is impossible to keep rules and signatures up to date 24/7

A far more intelligent, automatic, and sophisticated technology is required. A technology that can detect subtle changes and understand the normal pattern of life in a business is able to identify what is abnormal, and can highlight potential threats on the network. This is where Darktrace comes in...

Darktrace was founded in 2013 in Cambridge, UK, by government intelligence experts working with leading mathematicians at Cambridge University, with the mission to free the world of cyber disruption. Darktrace now protects over 8,100 customers from the world's most complex threats, including ransomware, cloud, and SaaS attacks.

It has complete analysis and visibility of 100% of the network traffic. Network traffic is ingested and stored for long periods of time so that it can build correlations and behavioral analysis. By iteratively monitoring network traffic all the time, Darktrace builds up a model of behavioral analysis for users, devices, and the network as a whole.

Based on important advances in Bayesian probability theory and powered by cutting-edge machine learning and artificial intelligence, Darktrace ingests communications and creates a unique behavioral understanding of "self" for each operator and device in the organization.

Self-learning AI is made up of thousands of algorithms which operate in competition with one another to deliver the best model for every user and device.

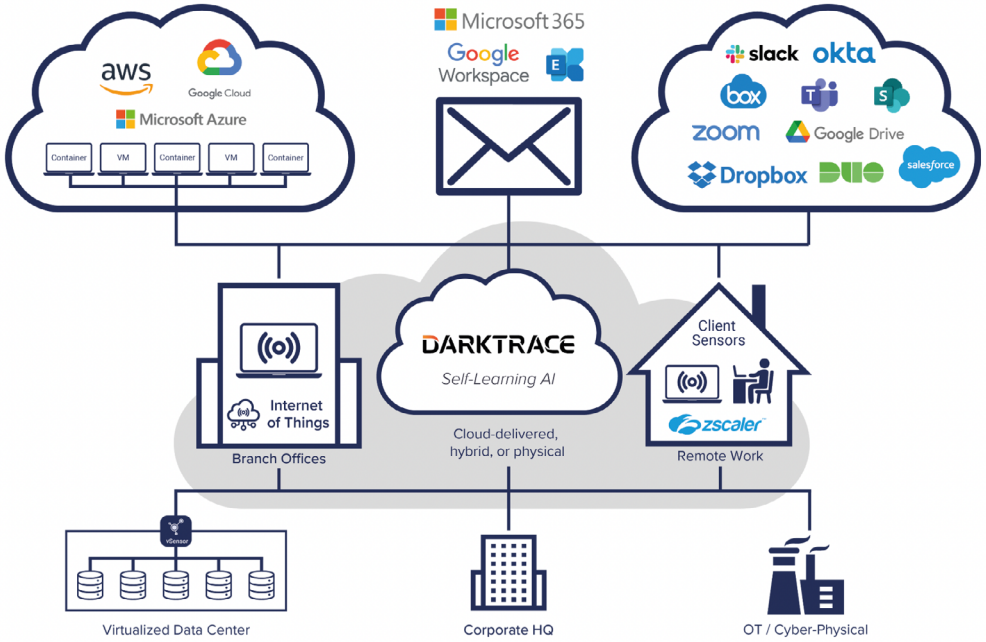
Darktrace uses a smart threshold filter that contextually weights and re-scores the outputs from all machine learning detectors in light of their previous performance. This recursive technique continually recalculates threat levels, therefore evolving its understanding of "self".

Rather than using large volumes of training data, Self-Learning AI learns on the job from real-time data. Applied to cyber security, this means that it can identify and stop zero-day attacks, because it's not learning from historical attack data.

It can do this by clustering users and devices into groups based on its understanding of how these entities behave. The majority of people and devices behave in a unique way, that differs from their peers to varying degrees, but that is significantly more predictable in comparison to their own historical behavior and rates of change. If a user of device begins to behave unusually in relation to the rest of its per group, Darktrace will detect this cyber disruption.

2. Introduction to Darktrace

In contrast to other AI approaches, which require data to be cleansed, labeled, and moved to a centralized repository, Darktrace brings AI to your data, wherever it lives. Whether it's in the cloud and email systems, across Operational Technologies or traditional networks and infrastructure, Darktrace's Self-Learning AI is installed into the heart of these systems, without requiring data migration.



It learns from scratch and constantly evolves its understanding as the data environment changes. This means that the technology is ideally suited to detecting malicious communications, even previously unknown threats that are novel or tailored, regardless of where they originate.

By identifying unexpected behavioral anomalies, defenders can investigate malware compromises and insider risks as they emerge and throughout stages of the attack life cycle. Darktrace provides the real-time visibility required to make intelligence-based decisions in live situations, while enabling in-depth investigations into historical activity.

The Threat Visualizer interface is a useful tool which offers security teams information and helps save precious time, allowing teams to focus on higher-value, strategic work.

Cyber AI Analyst discovers on its own, passively watching and listening while not interfering with existing IT network infrastructure. Instead, it surfaces incidents in the interface for review, containing all the relevant information which could take an operator hours to locate.

From here, network interactions can be played back in the Threat Visualizer to understand what factors preceded an event and what the outcomes were. Other useful pages can be opened to view information about devices and subnets or relevant logs can be pivoted on to obtain further details.

Combining this technology with other Darktrace modules, means not only can it detect, but it can also provide autonomous decision-making that is critical as an attack or incident unfolds.

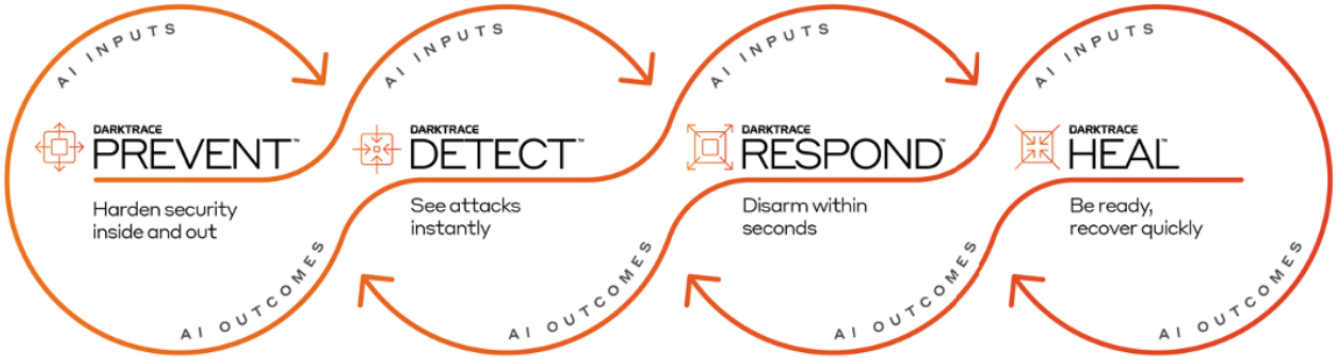
In addition, the results of the Threat Visualizer tools can be easily integrated with third-part technologies, including Security Information and Event Management (SIEM) solutions.

2. Introduction to Darktrace

Darktrace delivers the first-ever Cyber AI Loop: an interconnected set of cyber security solutions that continuously and autonomously hardens your security.

The Cyber AI Loop comprises four AI-powered product families – Darktrace PREVENT™, Darktrace DETECT™, Darktrace RESPOND™, and Darktrace HEAL™ – that work across your entire organization, including internal and external data, simultaneously. With each technology augmenting and feeding information into the others, your cyber resilience is systematically improved.

Each component of the Cyber AI Loop is powered by Self-Learning AI: proprietary Darktrace technology that learns you. By understanding your bespoke organization, your users and devices and how they interact, it can build an evolving sense of what's normal to identify what's not. This enables Darktrace to shine a light on previously unknown and unpredictable threats.



Self-Learning AI™ empowers a complete, always-on solution with autonomous feedback continuously improving the state of security.

Comprehensive Protection Wherever You Need It

Cloud · Apps · Email · Endpoint · Network · Zero Trust · OT

Dropbox · Google Cloud · slack · zscaler · CROWDSTRIKE · Microsoft 365 · box · aws · okta · DUO · Microsoft Azure · PAS · Google Workspace · cisco · SentinelOne · salesforce

DARKTRACE DETECT

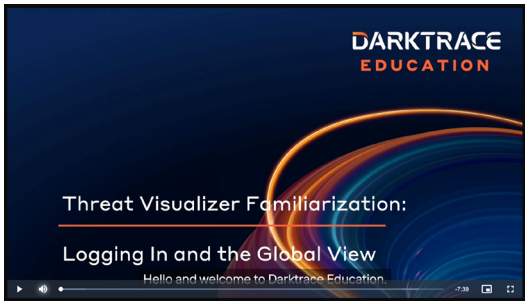
Instant visibility. Every attack, including never-before-seen emerging threats.

Darktrace DETECT analyzes thousands of metrics to reveal subtle deviations that may signal an evolving threat - even unknown techniques and novel malware. It distinguishes between malicious and benign behavior, identifying attacks that typically go unnoticed.

3. Threat Visualizer Navigation

The Threat Visualizer interface is designed to accommodate many ways of working. It provides access to individuals across an organization in varying roles. From analysts to administrators, there are many tools available in one place. In this chapter, let's learn how to log into Darktrace and navigate the interface.

Logging In



Continue your learning with our dedicated video 2: Logging in and the Global View

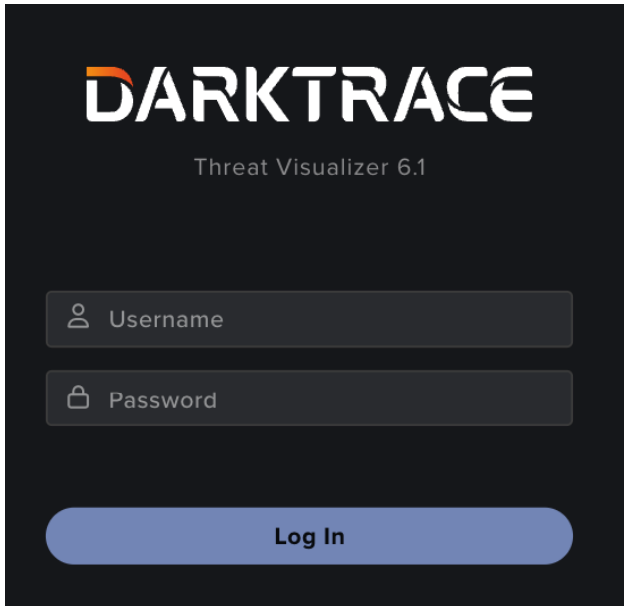
In a Chrome or Firefox web browser, navigate to the Threat Visualizer by typing in the IP or hostname of your instance:

https://<applianceIP>/

or

https://[region]-XXXX-01.cloud.darktrace.com

Enter your **username** and **password** to log in.



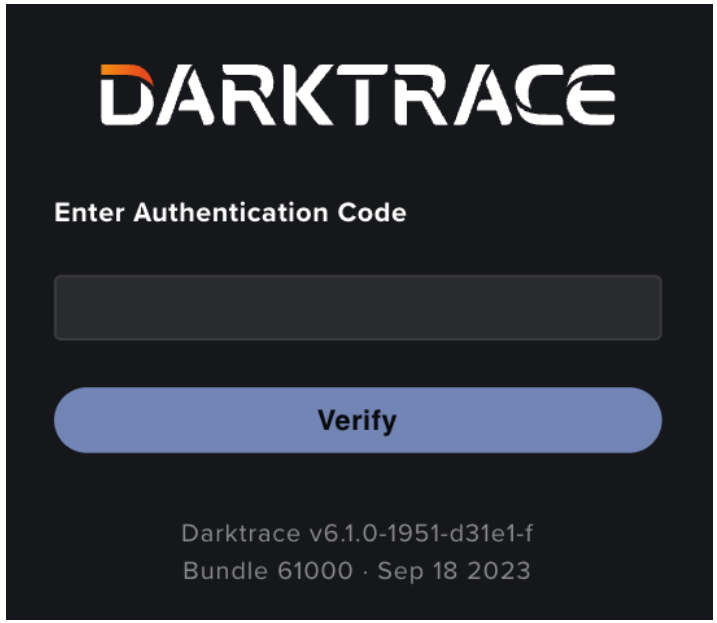
First Time Access

Your username and password will be assigned to you by your administrator. Your password can be reset at any time from the Account Settings window, or your administrator can change this for you in the User Admin page.

Alternatively, if you are accessing the Threat Visualizer via your organization's SSO system click the **Login with SSO** button as standard.

When logging in for the first time, a customer license agreement screen will be displayed. Read the terms carefully and click **Agree** to proceed.

If your environment has two-factor authentication enabled, the first time you log in, you will need to scan the QR code on screen. Going forwards, you will be able to login with your preferred multi-factor authentication app.

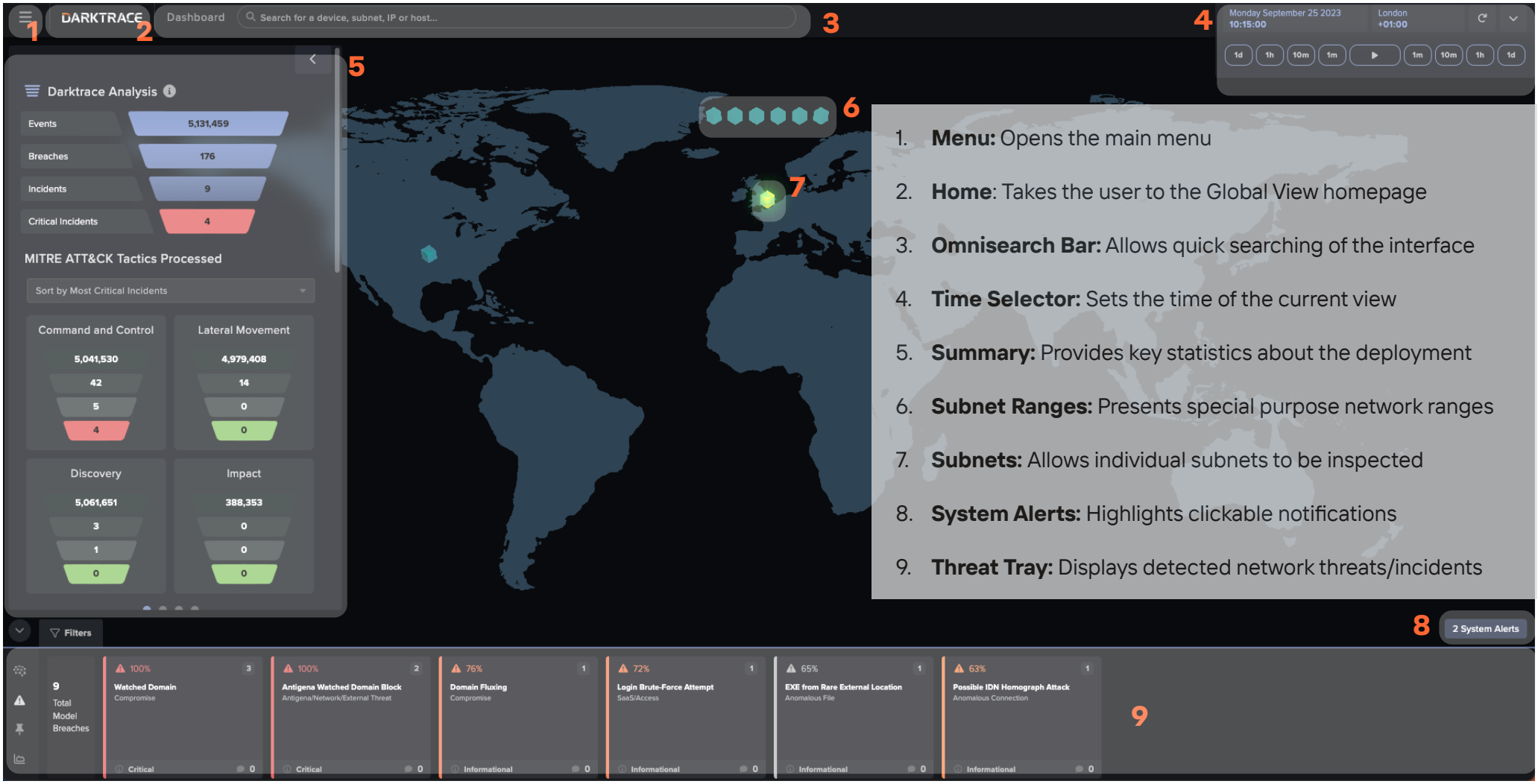


Note: Prior to accessing the interface, the Darktrace version can be seen on the login page or the two-factor authentication page. Displayed here is the bundle number and the date that the software was last updated.

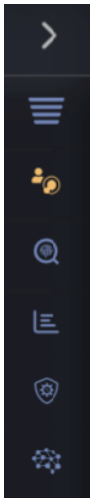
Global View

The Threat Visualizer can be broken down into the **Global**, **Subnet** and **Device** views. When logging in, the home page you are greeted with is the Global View.

Review this home page. It provides a **global snapshot** of the network, including a summary of subnets and devices on the left, a Threat Tray of anomalous behavior along the bottom, a Time Selector for controlling the view in the top right, and many more shortcuts to other useful features.



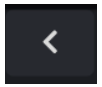
Summary Panel



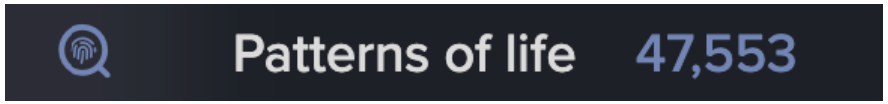
On the left of the home page, there is a column of icons, with an arrow at the top that can be clicked on to reveal the **Summary**.

This provides an overview of key information about the deployment.

The Summary, once opened, can be **collapsed** to hide it from the interface.

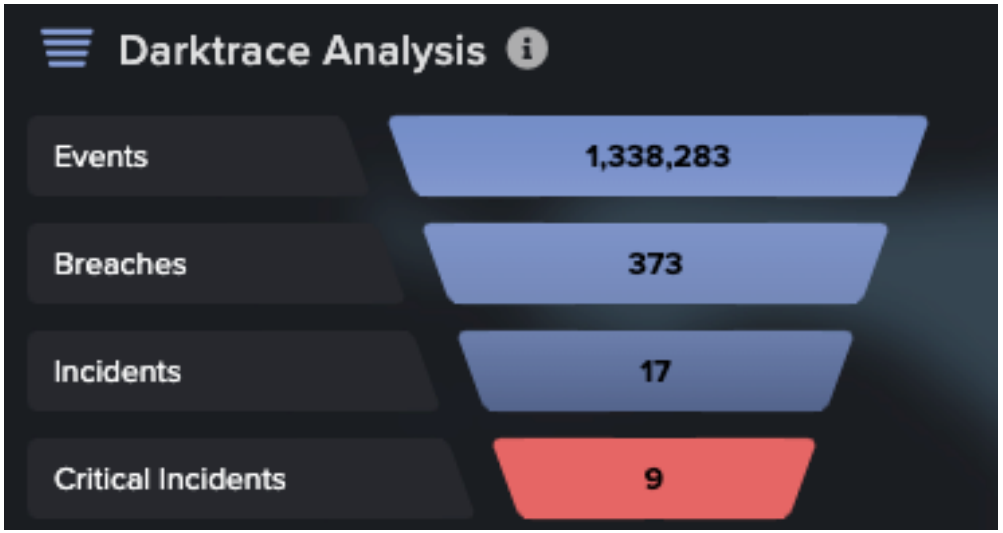


Hovering over an icon displays an **overview** of that particular section of the Summary Panel.



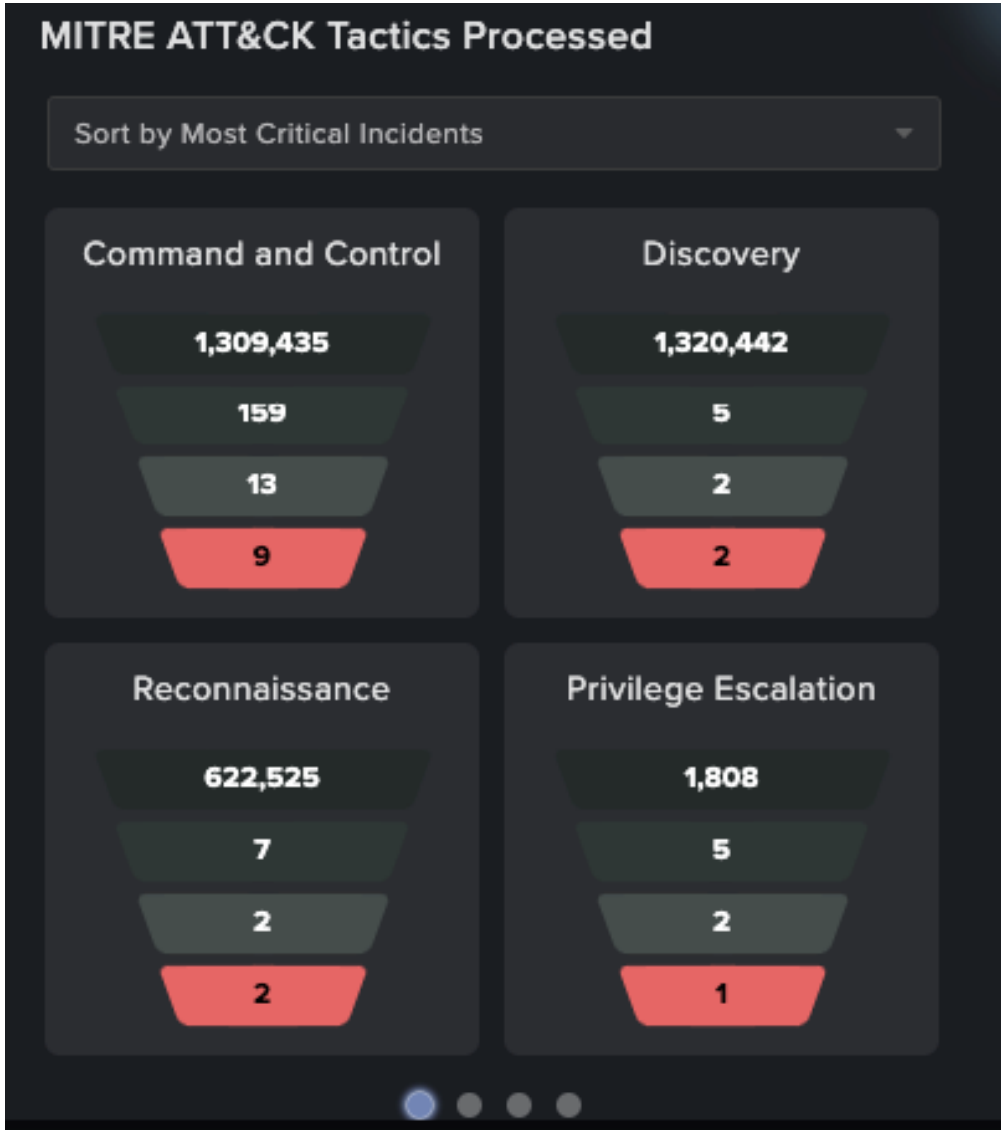
Darktrace Analysis

The **Darktrace Analysis** section displays a broad overview of pertinent network activity based on the last four weeks of analyzed data. The amount of total **Events**, **Breaches**, **Incidents**, and **Critical Incidents** will be displayed.

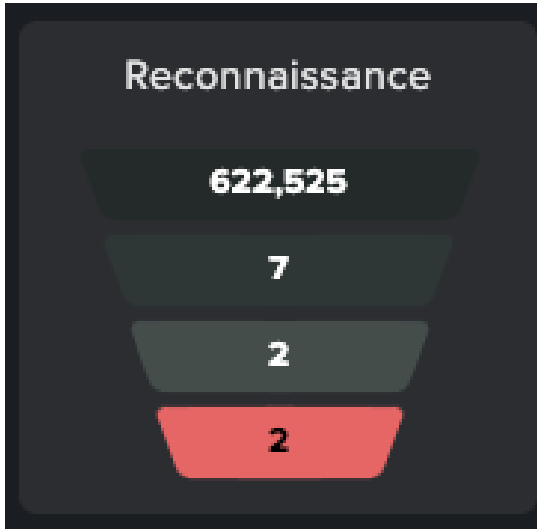


MITRE ATT&CK Tactics Processed

Next is a breakdown of the above information into respective **MITRE ATT&ACK tactics**. Within each of the 14 tactics the data is shown as **Raw Events, Model Breaches**, **Incidents**, and **Critical Incidents**. Clicking on the **grey circles** allows users to scroll to view other tactics that are not currently displayed.



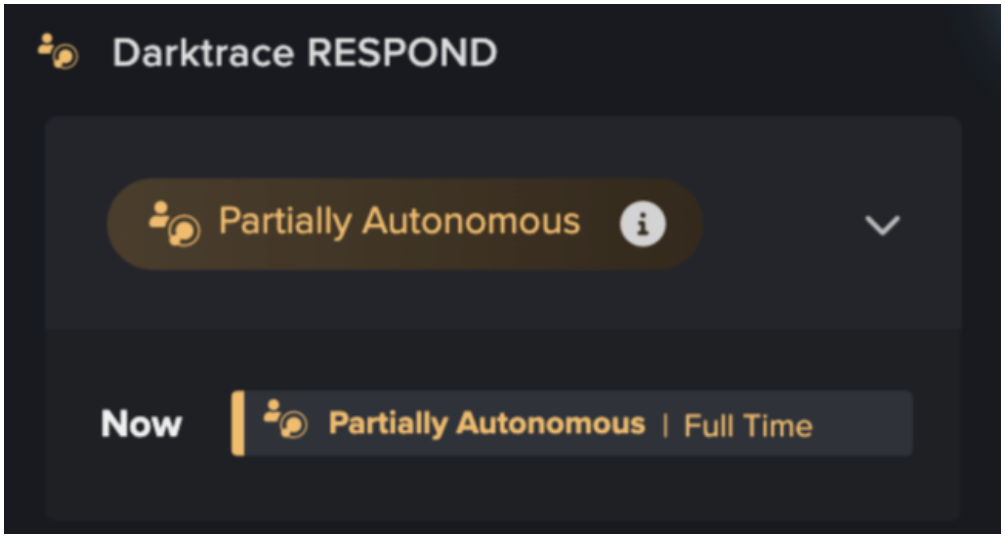
Each layer of data can each be clicked on to bring up a new window that lists all the corresponding Model Breach Logs, Incidents, and Critical Incidents.



The individual events can then be used to pivot to the specific **Model Breaches** and **AI Incidents**. The tactics, with their corresponding data, can also be sorted in the order that is most suitable for the user.

Darktrace RESPOND

If Darktrace RESPOND is enabled for the deployment, relevant RESPOND status and statistics are presented in the Summary.

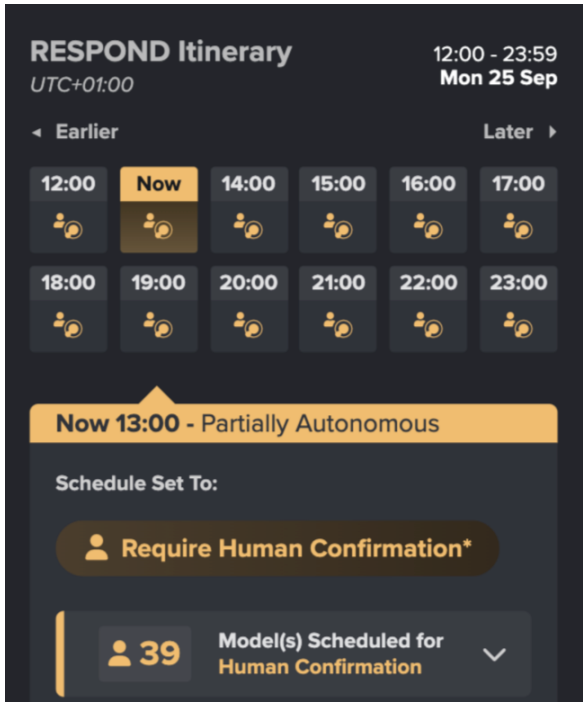


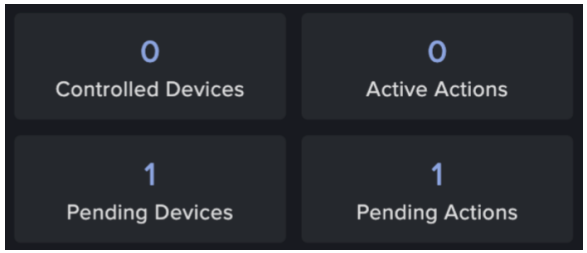
Clicking on Darktrace respond status will open the **RESPOND Itinerary** from which users can check when specific action states have been enabled.

This will also contain specific information **models** scheduled for different modes (Human Confirmation, Partially Autonomous or Autonomous) as well as **Subnets**.

The number of **Controlled Devices** is displayed, indicating how many devices have had RESPOND actions taken against them.

The number of RESPOND actions which took place over the last seven days will be displayed based on their status: **Active Actions**, **Pending Devices** and **Pending Actions**.

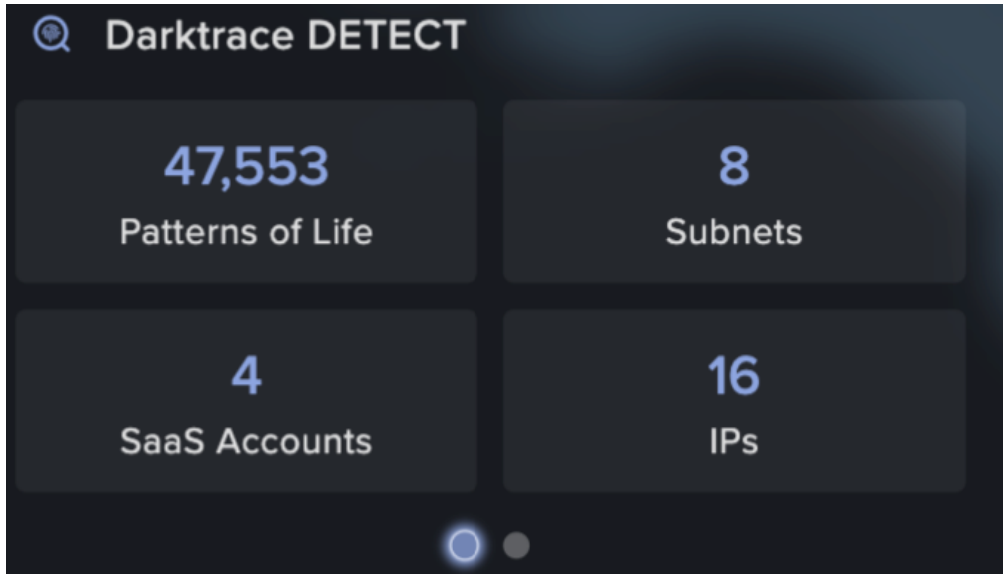




Note: Darktrace RESPOND/Network has its own dedicated course from which more information is available.

Darktrace DETECT

The **Darktrace DETECT** section outlines the scope of the deployment, including the number of subnets, IP addresses and user credentials. Clicking the dot below the four tiles will change the view to a breakdown of devices.



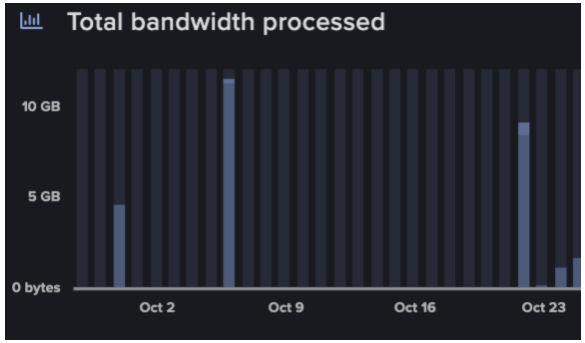
We can also see **Patterns of Life**, which represents the number of unique, active connections observed over 12 weeks in the Darktrace system, contributing to the understanding of the environment.

What is a Pattern of Life?

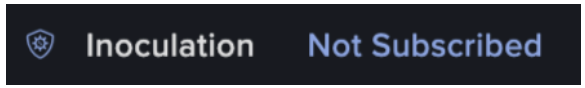
Users and devices on a network carry out a lot of regular activity, including logging into systems, accessing file shares, connecting to other devices and more. Each of these connections is a separate pattern interaction contributing to the usual activity of the device. Typically, there are around two hundred connections for every device on a network. The 'pattern of life' describes the expected behavior, which adds to Darktrace's evolving understanding of 'self'. Any deviation from this will cause Darktrace's 'pattern of life' anomaly detection to highlight instances of this.

Further Information

The **Total bandwidth processed** graph shows bytes per day for the entire network. This is the total data being captured by Darktrace. Hovering over the bars will show the date, client bytes, and total bytes observed on the network that day.



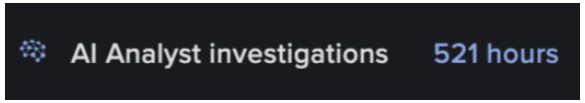
The **Inoculation** service can anonymously share IOCs observed across the Darktrace fleet. If this free service is subscribed to, the Inoculation status will reflect this.



What is Inoculation?

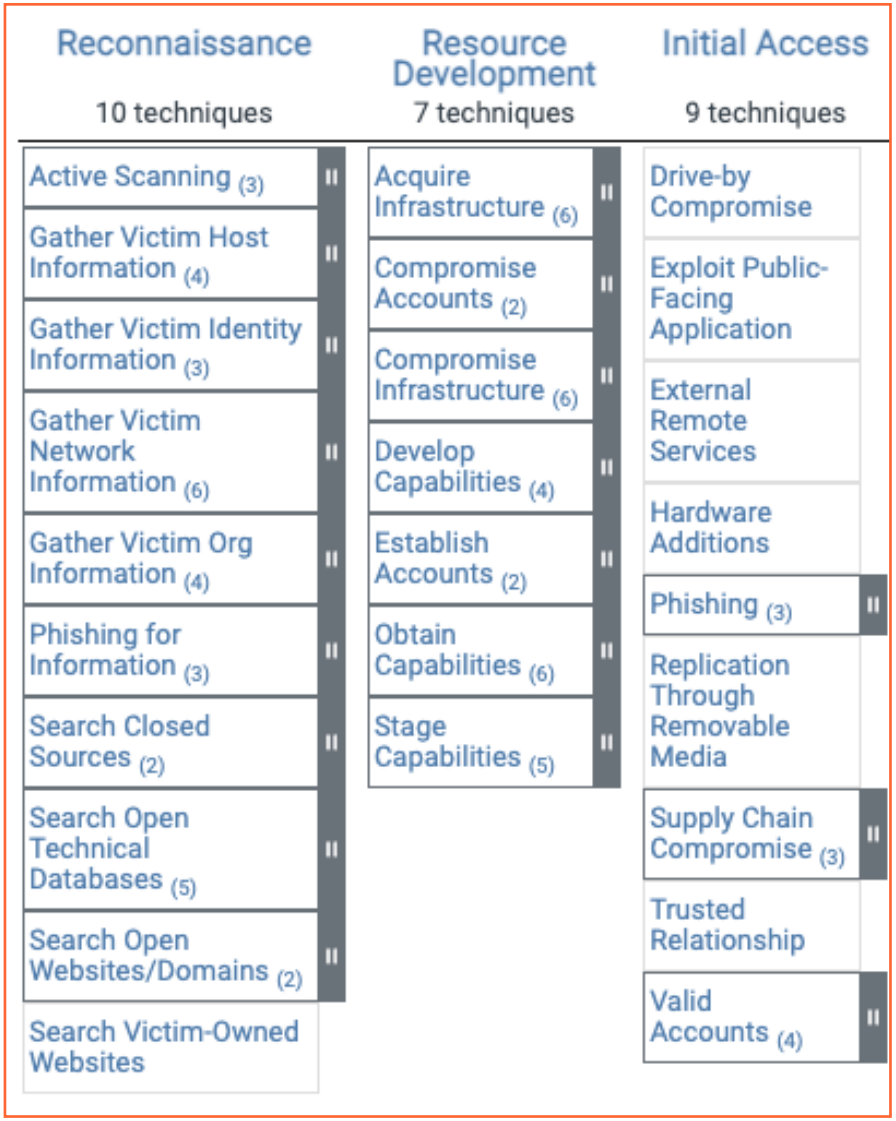
Powered by unsupervised machine learning, the Darktrace Environment detects and responds to cyber threats in real time. Like a vaccine, Darktrace Inoculation boosts your Darktrace Environment, preemptively protecting against threats that have not yet hit your systems and infrastructure. Opting in to the service allows you to anonymously share and receive intelligence about unique, high severity cyber threats discovered elsewhere across the Darktrace Community.

The **AI Analyst Investigations** metric estimates the equivalent time it would take for a human to investigate and create the incidents surfaced by AI Analyst over the last 30 days.

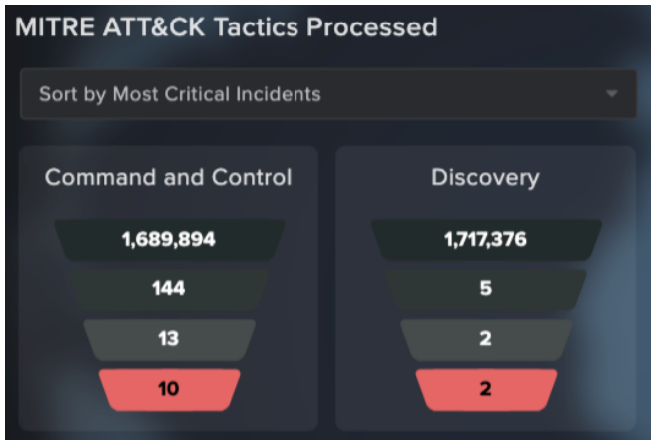


In-depth: The MITRE ATT&CK Framework

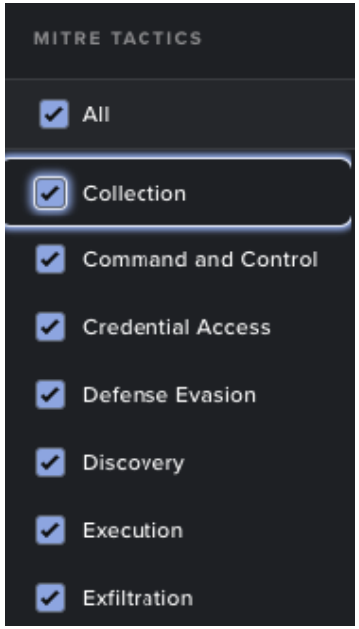
Darktrace now incorporates the MITRE ATT&CK framework into the Threat Visualizer interface, but what exactly is the MITRE ATT&CK framework and how can it enable users to detect and respond to threats?



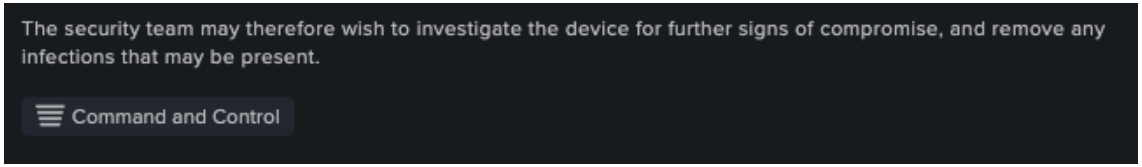
The Mitre Corporation developed the ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) framework in 2013, and it has since become a global standard as a reference of adversary tactics and techniques.



It is essentially a matrix of tactics and techniques specifically designed for threat hunters, defenders and red teams, and is seen as an alternative to the Cyber Kill Chain. It consists of 14 tactics in total, such as Reconnaisance, Resource Development, and Initial Access. Each tactic has corresponding techniques and sub-techniques; there are currently 191 techniques and 385 sub-techniques identified by MITRE ATT&CK.

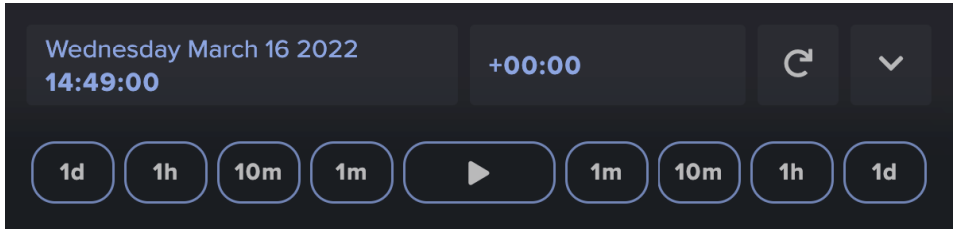


Within the Threat Visualizer, breaches and incidents are broken down into MITRE ATT&ACK tactics, enabling users to interrogate their data and critical incidents on a MITRE ATT&ACK basis by filtering breaches and incidents by specific tactics. For example, if a user is interested in Command and Control incidents, they can instantly display all Command and Control events on their network.



Time Selector

1. In the top right corner, the **Time Selector** specifies the time window for events displayed in the event log, as well as the time window for network activity playback.

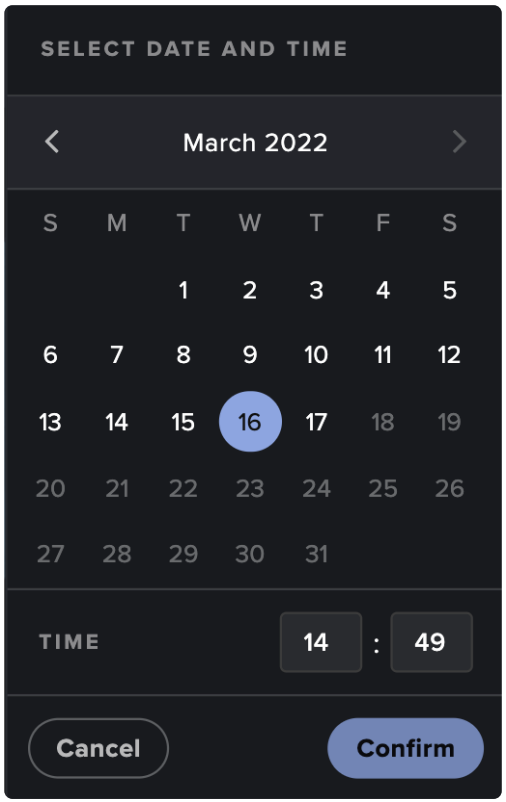


By default, the Time Selector is set to the timezone specified by the NTP server at the time of installation.

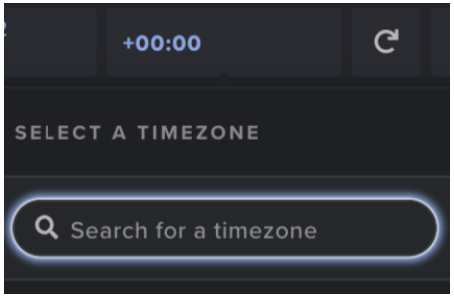
Note: This Time Selector is distinct from the time period defined in the Threat Tray.

a. Click on the **date**.

b. Select a date and time and click **Confirm**.



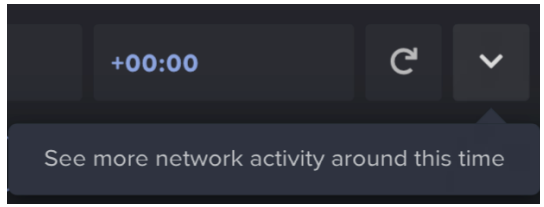
c. Click the +00:00 field and enter a relevant timezone in the **Search for timezone** bar.



Enter a minimum of three characters of your desired timezone or city, such as GMT or Los Angeles.

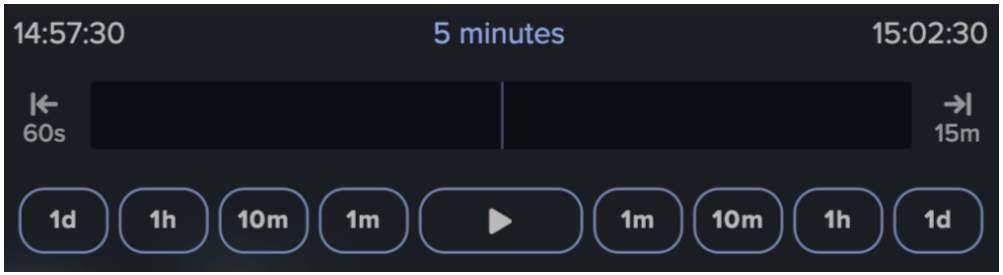
Note: Once a timezone has been selected, this will remain tied to the user unless modified again.

2. To make use of the playback features in the visualizer, click the **downwards facing arrow** to reveal further options for expanding, constricting and moving through time.



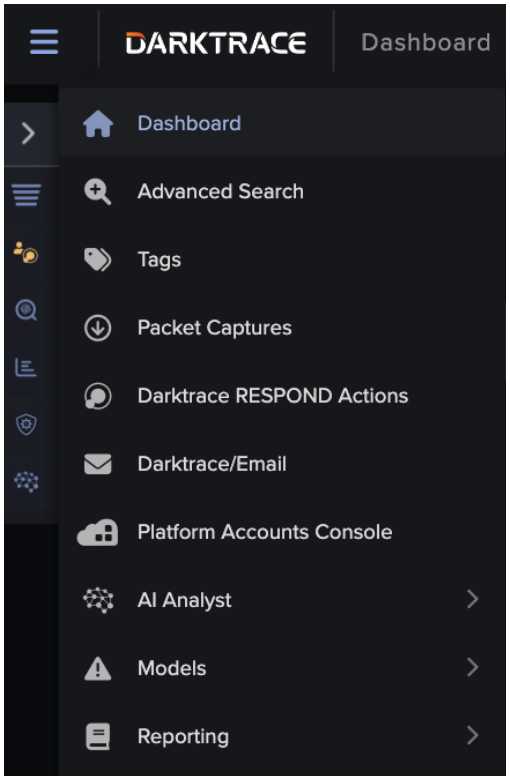
Top Tip:

The resulting playback features depicted below can be useful for exploring the subnet and device views.



3. At any time, the visualizer can be recentered to the **current time** using the refresh icon.

Continue your learning with our dedicated video
3: Main Menu Navigation



Menu Navigation

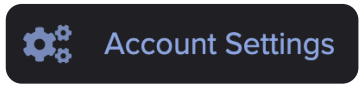
The Main Menu, found in the top left-hand corner of the interface, contains shortcuts to key functions of the Threat Visualizer. Some functionalities can only be accessed with appropriate user/group role permissions.

Advanced Search	Opens a new browser tab for Advanced Search.
Tags	Add or review tags in the Tags Manager window.
Packet Capture	Download PCAPs from a list of files which have been created on the appliance.
Darktrace Respond Actions	Schedule and configure Darktrace RESPOND and review and export actions.
Darktrace Respond/ Network Quick Setup	View and configure Darktrace RESPOND/Network actions and settings.
Darktrace/Email	Pivots to the Darktrace/Email interface where mailflow can be reviewed.
Platform Accounts Console	Pivots to the Platform Accounts Console to investigate anomalous SaaS events.
AI Analyst	Manually launch or view existing AI Analyst investigations.
Models	View and edit the underlying Model Logic which triggers Model Breaches.
Reporting	Create and download high level reports based on system activity.
Admin	Administer devices, subnets, permissions and check the health of the system.
Utilities	Use the tools to facilitate additional investigation based on Darktrace findings.
Intel	Configure TAXII feeds and add to trusted and watched domains lists.
Dynamic Threat Dashboard	Review breaches in a left-to-right formatted dashboard.
Explore	Dynamically explore device connectivity based on subnets and tags.
Help	Ask Darktrace experts questions or be redirected to useful documentation.
Account Settings	Change settings for your own account, including accessibility options.
Customer Portal	Opens the Customer Portal, providing access to a plethora of information.
Explore New Features	For large interface updates, windows highlighting new features can be opened.
Logout	Logs out the current user from Darktrace interfaces.

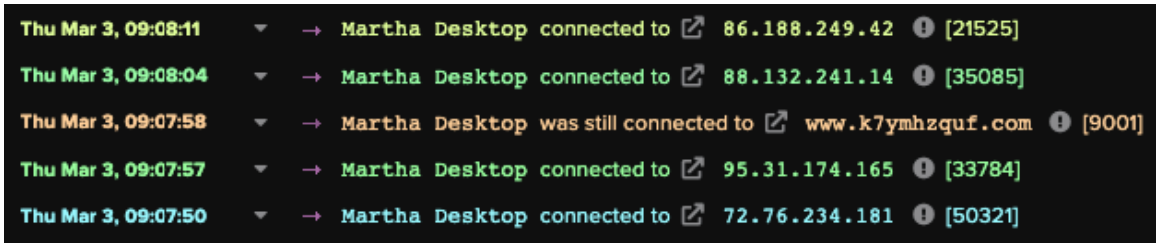
Account Settings and Accessibility

Before using the Threat Visualizer, it is recommended to set it up to best reflect your way of working. Within the Account Settings, there are multiple options aimed at making the Threat Visualizer interface more accessible.

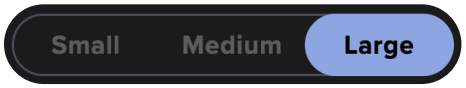
1. Within the menu options, select **Account Settings** to open the Settings window.



2. It is a popular choice to set the **Default Color-Coding in the Event log** to **Destination port**. The Application protocol and External hostname rarity are also useful considerations.

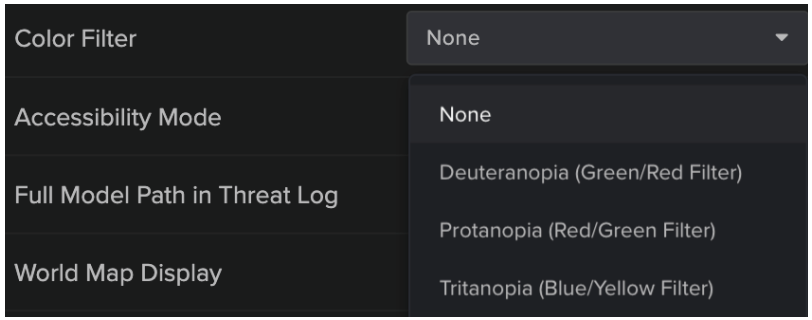


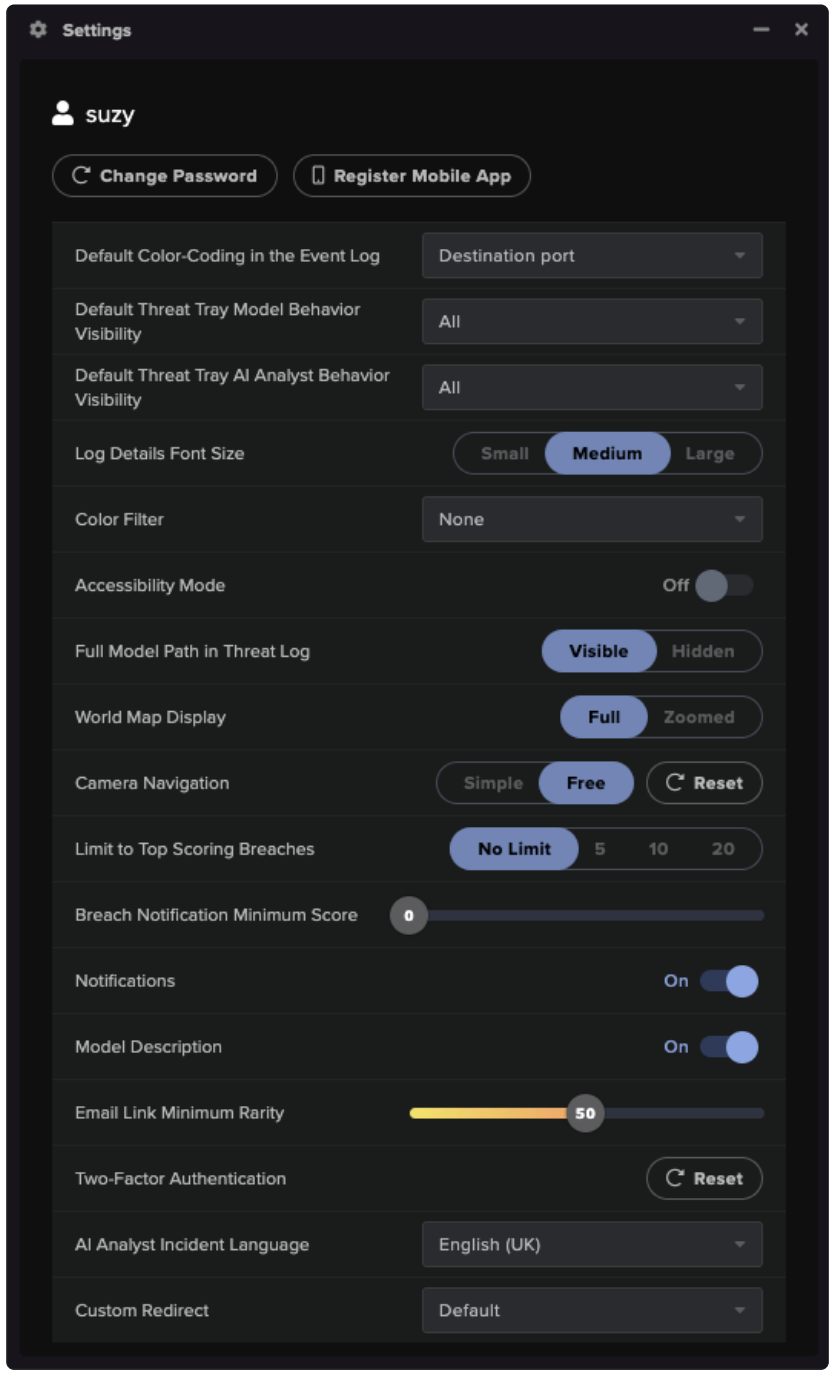
3. Depending on your screen resolution, you may wish to change the **Log Details Font Size**. Setting this to **Large** will also increase the readability of text in the Breach and Event Logs.



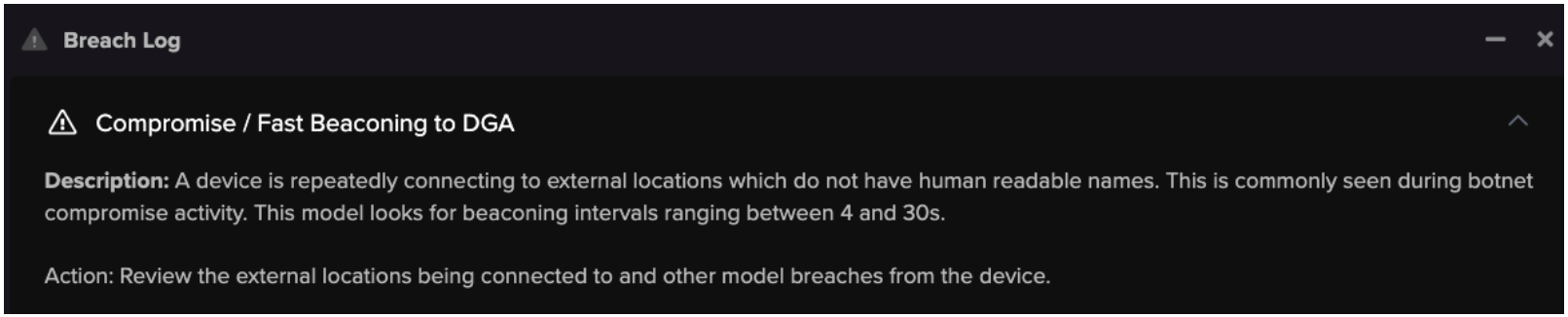
4. Moving down the Account Settings, notice the **Color Filter** drop-down. There are color filters for three varieties of color blindness: **Deuteranopia** (Green/Red), **Protanopia** (Red/Green), and **Tritanopia** (Blue/Yellow).

Selecting one of the available option has a visual impact on the interface.





5. For extra information to be displayed when becoming familiar with the Threat Visualizer, the **Full Model Path in Threat Log** and **Model Description** may be useful features to have visible/enabled.



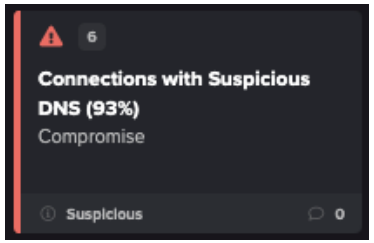
   a. Enabling the Full Model Path in Threat Log will **display the folder names** for where the Model is located in the Model Editor. This can help with understand what category a Model falls under.

   b. Turning on the Model Description displays a short **description** of what activity the Model is looking for and provides a suggested **action** for the user.

Note: If this option is toggled on, the Model Description can be hidden on a Breach Log basis by clicking the upwards arrow in the top right.

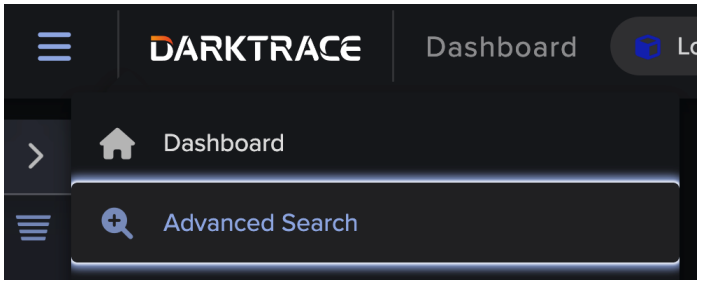
6. Furthermore, **Accessibility Mode** is another feature which can be enabled from the Account Settings. This mode enhances the interface by providing alt text elements to make the Threat Visualizer screen-reader compatible, amongst other more visible features, as outlined below.

   a. The first feature is in the **Threat Tray** where the top scoring breach has its **percentage** highlighted beside the name of the Model, Device or User, depending on the sorting method. Hovering over a breach in the Threat Tray will also show the scores for each individual breach of that type.



   b. Next, Accessibility Mode has **keyboard focusable elements** of the page which can be navigated between using the **tab** key. This highlights individual elements with a high contrast outline and displays text which provide a short description of the buttons' functions.

   c. Furthermore, notice the **increased contrast for menu items** when highlighted.



Top Tips:

- To move forwards through the interface, use the tab key.
- To move backwards through the interface, use shift + tab.
- To interact with a highlighted element, hit the enter key on the keyboard.

Navigation Chapter Test

This page will test your knowledge and check your understanding of the Navigation section. This is the perfect way to work towards your **Threat Visualizer Essentials Certification**! *Select an answer by clicking on it. Wrong answers are denoted by a red cross and right answers are denoted by a green tick.*

DARKTRACE
Essentials Certification

1. What is the name of the Darktrace AI understanding of everyday activity?

- [ ] Behavioral norms
- [ ] Habitual actions
- [ ] Patterns of life

2. Which Framework does Darktrace integrate into the Threat Visualizer?

- [ ] Cyber KIll Chain
- [ ] MITRE ATT&CK
- [ ] NIST Cybersecurity Framework

3. True or False: The keyboard can be used to navigate the interface.

- [ ] True
- [ ] False

4. Which menu option enables you to change the font size?

- [ ] Admin
- [ ] Account Settings
- [ ] Utilities

5. On the home page, which option allows quick searching of the interface?

- [ ] The Threat Tray
- [ ] The Summary
- [ ] The Omnisearch bar

6. Which statement about the Time Selector is true?

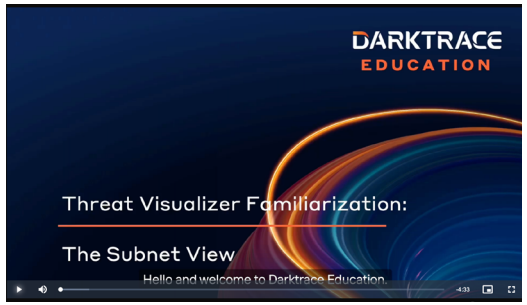
- [ ] It is distinct from the time period defined in the Threat Tray.
- [ ] It cannot be modified after installation.
- [ ] It is automatically set to GMT.

Clear All Answers

4. Visualization Options

The Subnet View is a useful way to quickly review subnets and identify their size, whilst the Device View focuses on one device and displays all the network communication between it and other devices. In this chapter, we will begin exploring the subnet and device visualizations.

Subnet View



Continue your learning with our dedicated video
4: The Subnet View

The Subnet View works best for smaller networks. The Subnet View can be opened directly from the Global View or via a shortcut in the Omnisearch bar when in the Device View. Alternatively, the Subnet View can be glanced at before navigating directly to the Device View.

1. The global map displays the **location** of your networks. Hovering over a group reveals the number of subnets in that location. Click on a cube icon to display subnets for the selected location.

Note: This investigative step is not necessary in all cases and can be more useful for some deployments than others. We recommend spending a short time viewing the subnet view.

2. Each **colored cube** represents a subnet.

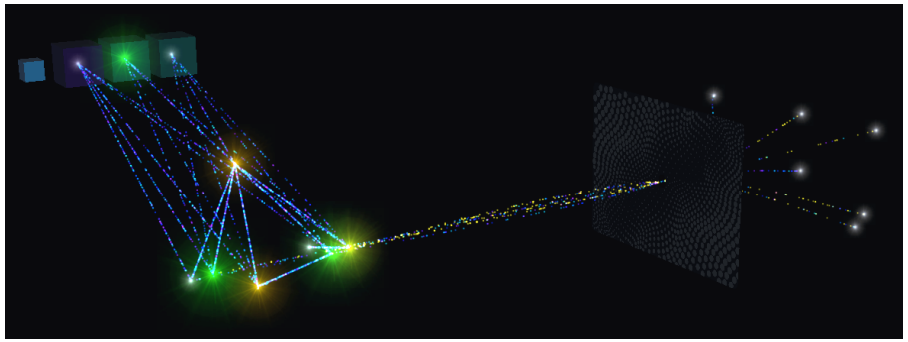
   a. Subnet cubes in shades of **yellow**/**orange**/**red** indicate that Darktrace has detected anomalies on those subnets.

   b. Cubes are **green** if there has recently been a Darktrace RESPOND action on at least one device in that subnet.

   c. Subnets depicted in **blue**/**purple** suggest that no anomalies have been detected in those ranges.

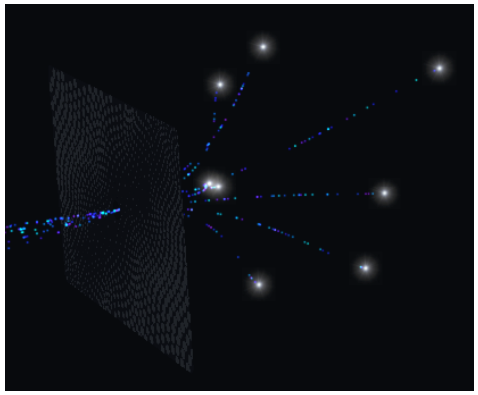
3. The Subnet View displays all the subnets' **active connections** and **traffic flows** between subnets and devices, both internal and external.

   a. The data protruding from the subnet represents the **network traffic** seen in the selected time duration.

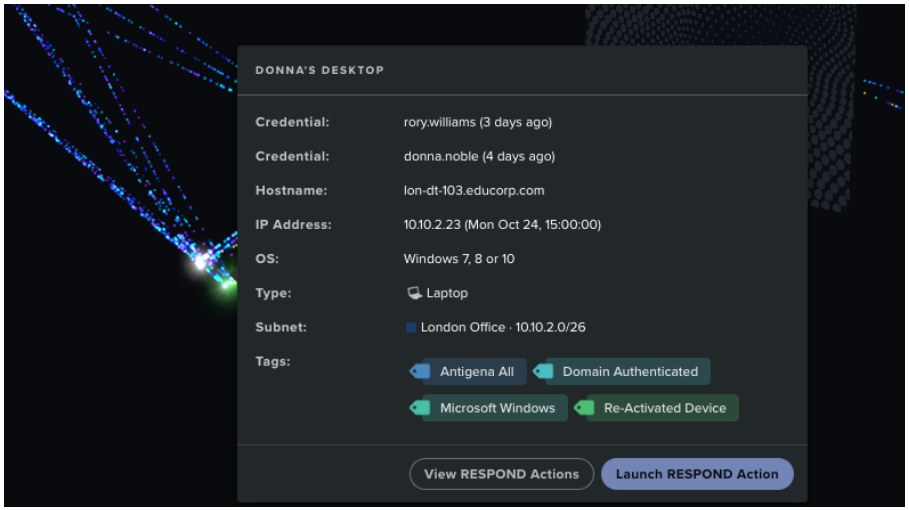


Note: The thicker the line, the greater the volume of data flow between devices. Yellow lines represent what Darktrace believes to be unusual activity that deviates from a device's normal pattern of life.

b. The **wall** represents the external perimeter of the network and data leaving it points to different destinations.



c. Inside the network perimeter, each **star** represents a device. Brighter stars represent more anomalous devices. Hovering over these provides device details.

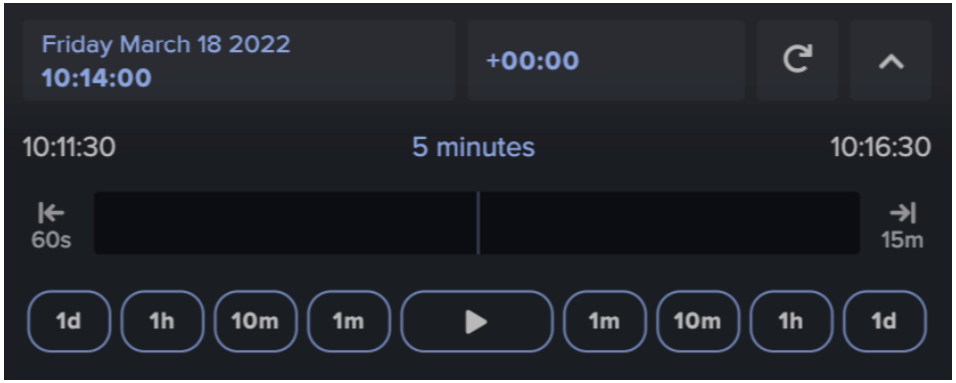


Note: Clicking on a star/device opens the Device View so devices can be individually inspected.

Top Tip:

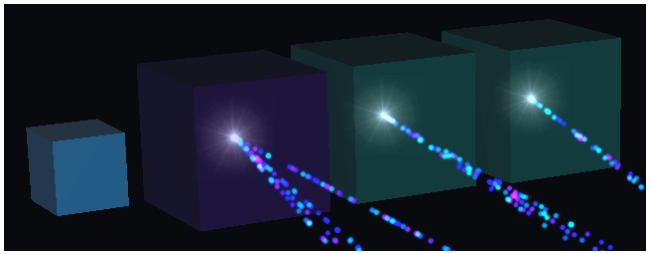
Move the view around to gain a better view of the endpoints. Left-click and hold to rotate the view of the subnets. Right-click and hold to drag the view horizontally or vertically.

4. Upon opening of the Subnet View, the **Time Selector** in the top-right hand corner will expand to display 5 minutes of analyzed data by default.



Use the **arrows** to change the duration to 15 minutes and watch the data flow increase or try the minute/hour/day shortcuts to move through time. The play button allows for a real time view of the data flow on your network. By clicking the refresh on the far right, you can return to the current time.

5. Notice that there are multiple subnet cubes in this view:

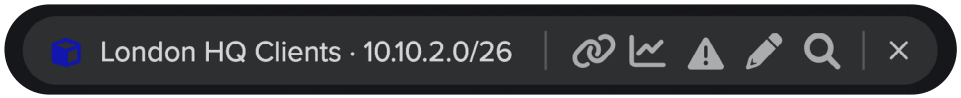


a. To navigate to different subnets, click on the **different cubes** of the same size.

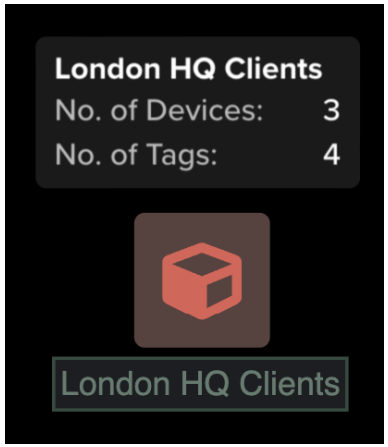
The network data flow will update. This will simultaneously update the Omnisearch bar in the top left corner to display the currently selected subnet.

b. Clicking the smallest cube, labeled **Full Network**, will return the view to the Global View.

6. With the subnet populated in the Omnisearch bar, **additional options** are available to the right. These can be useful to deep-dive into the subnet's connectivity and devices.



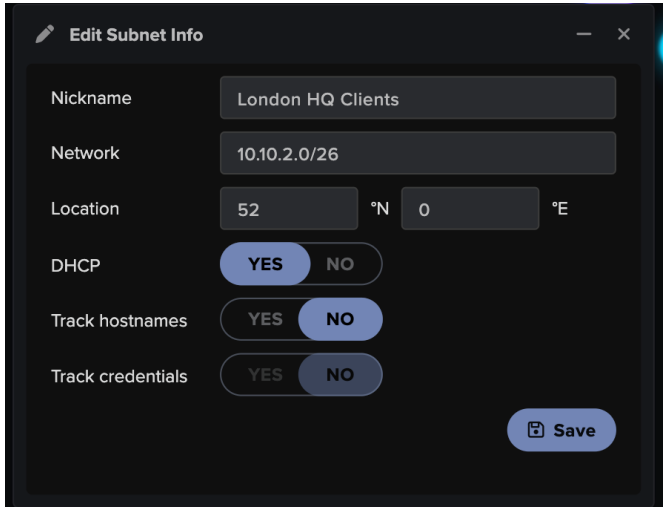
   a. The first option, denoted by a **link icon**, will open the subnet connectivity in Darktrace's **Explore** function in a separate browser tab. This provides an alternative interface to the Threat Visualizer.

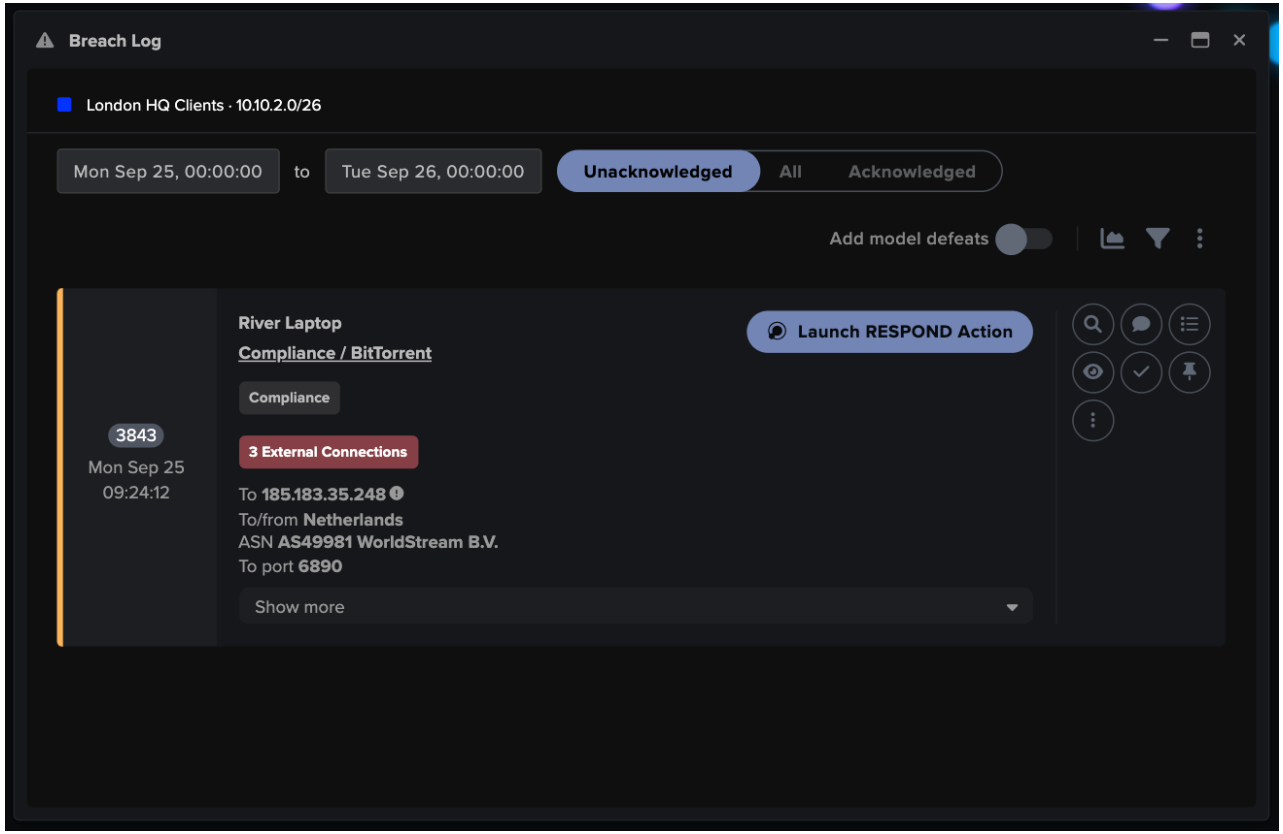


   b. The second button represented by a **graph** will open a **graph of all connections observed** on the subnet.

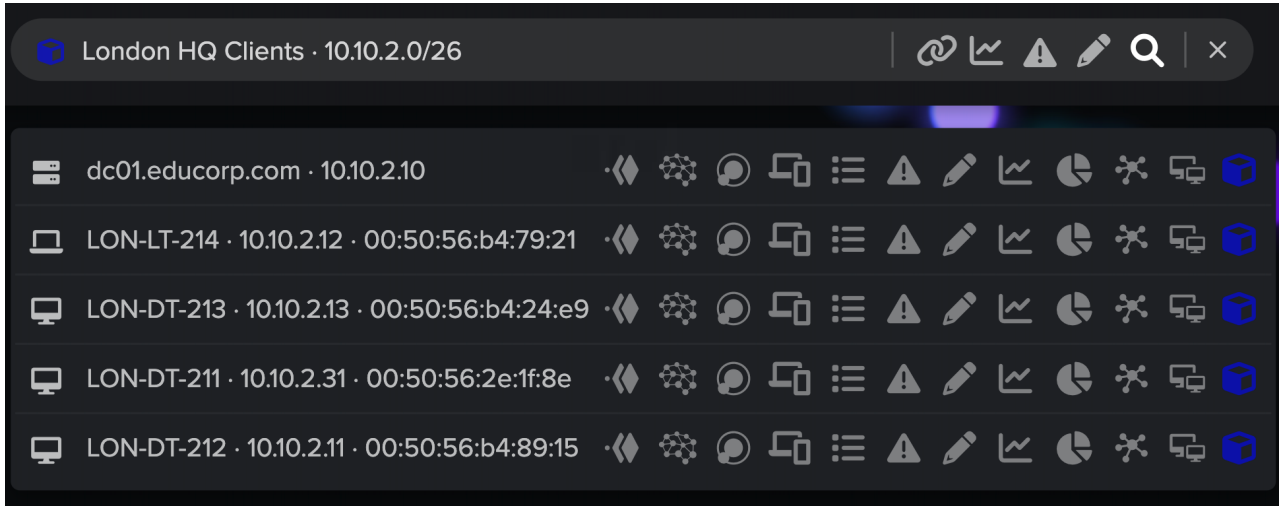
c. Next, the **warning triangle** will open the **Breach Log** which lists all Model Breaches triggered by devices on the selected subnet.

d. Subnet information can be directly edited by clicking the **Pencil icon**. Editing subnet details here has the same impact as modifying them in the Subnet Admin page.



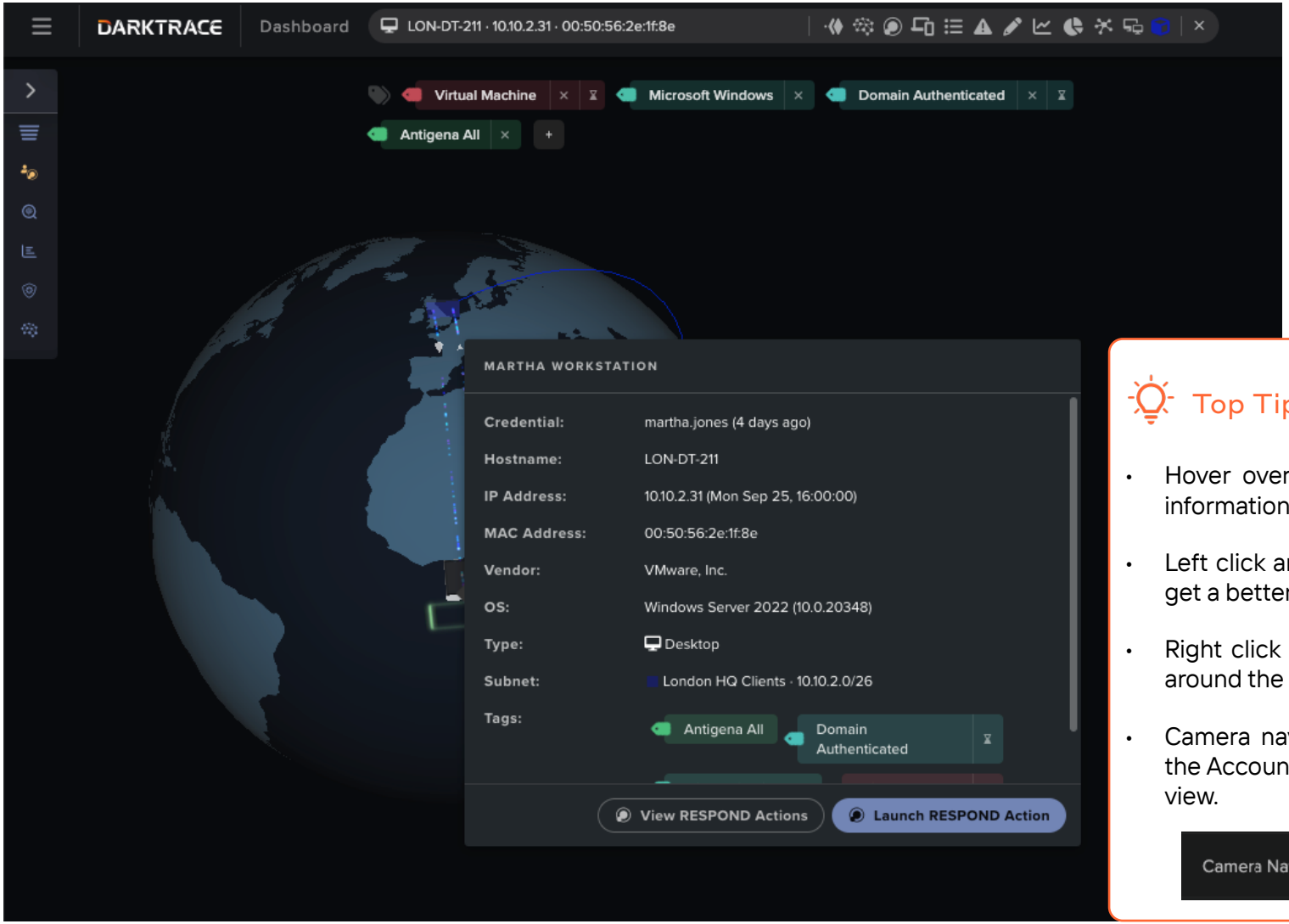


e. The **Magnifying Glass** allows the operator to focus on the subnet's devices, which can be clicked to open the Device View.



Device View

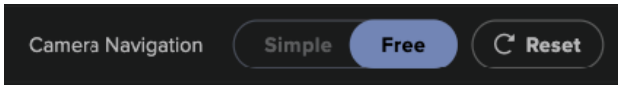
This view may be navigated to in a variety of ways: through the Omnisearch bar, from the Subnet View, via an AI Analyst Incident or Model Breach, pivoting between devices and many more.



Continue your learning with our dedicated video
5: Device View - Part 1

Top Tips:

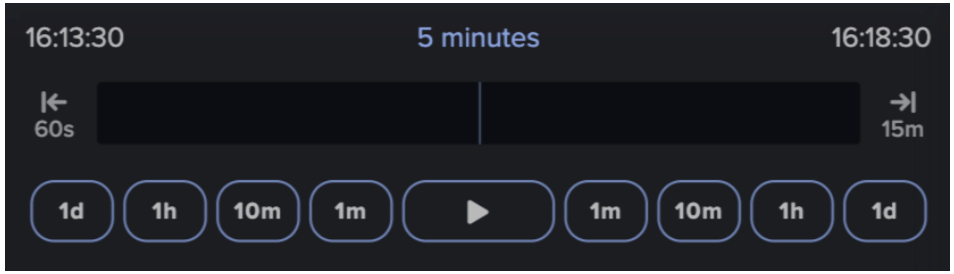
- Hover over the device to display device specific information.
- Left click and drag the space around the device to get a better view of network interactions.
- Right click and hold the mouse to move the icons around the screen.
- Camera navigation can be reset at any time from the Account Settings to return to the default device view.



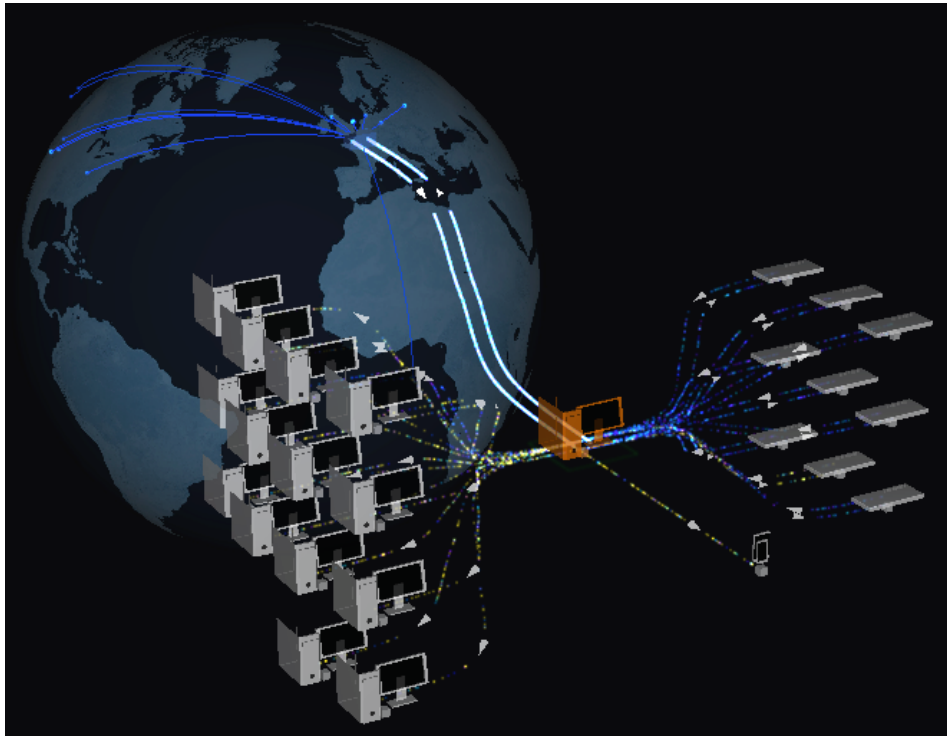
4. Visualization Options

Device View

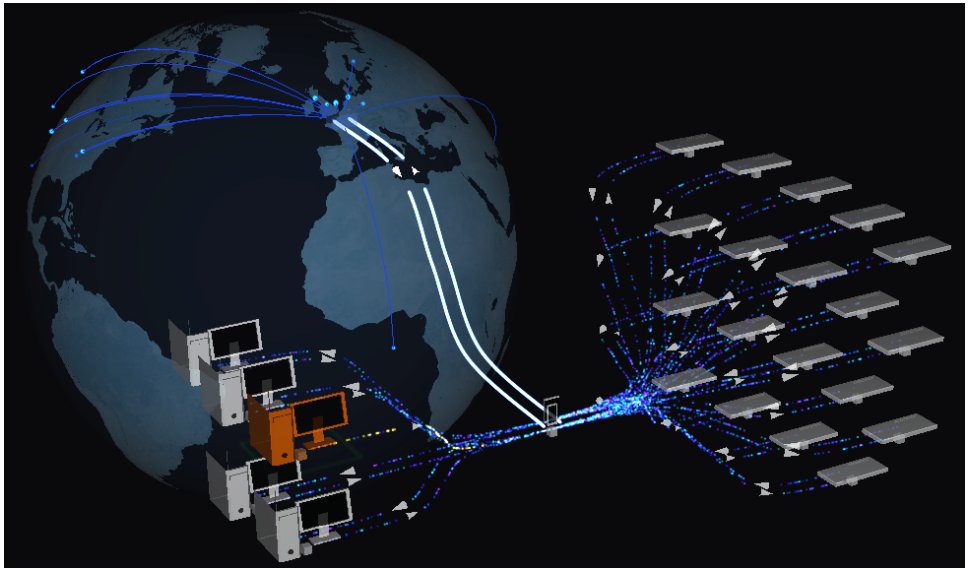
1. Upon entering the Device View and clicking on the device, notice that the **Time Selector** may automatically expand.



2. Try **increasing the duration** using the right facing arrow in Time Selector to view more network communication. **New devices** may appear in the interface.

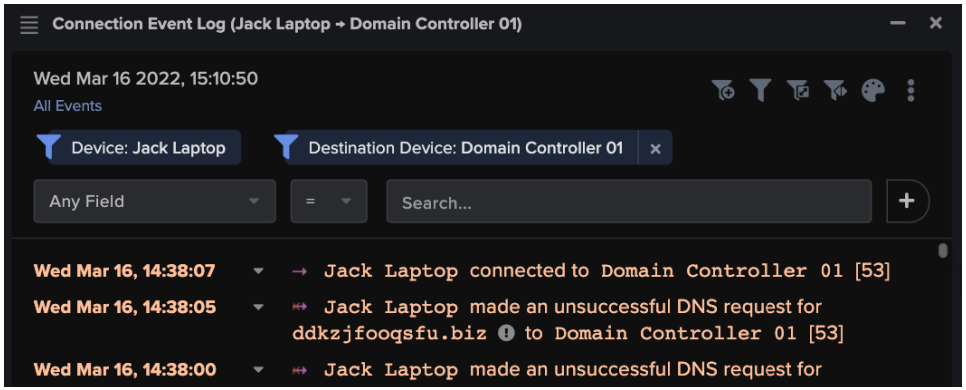


3. Clicking on **another device** will **refocus** the Threat Visualizer on to it.

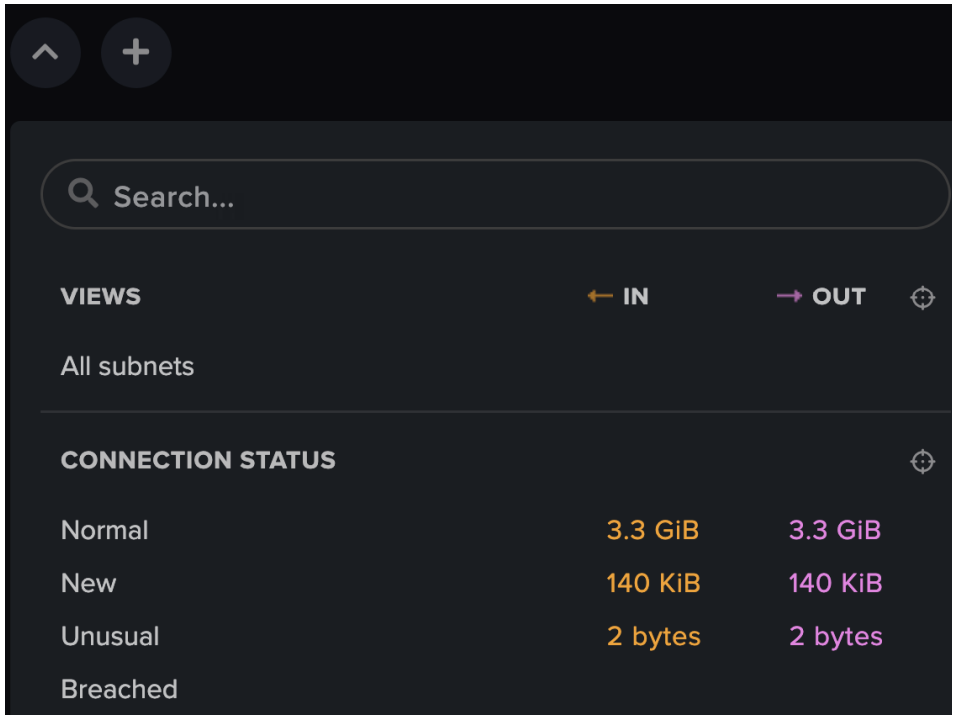


Note: The color of the connectivity indicates how anomalous it is. Connections containing yellow indicate anomalous activity. Furthermore, the thicker/brighter the lines, the more data transfer is occurring.

4. To find out more information about the connectivity between two particular devices, hover over the arrows between them or click the arrows to open up a filtered **Connection Event Log**.

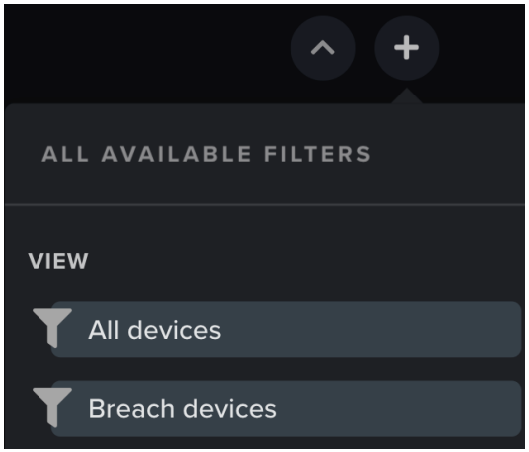


5. On the right-hand side of the device view, an interactive summary of all communication within the selected time period is displayed. The information in **orange** is the received data (IN) for the device and the information in **pink/purple** represents the data sent (OUT). This information can be used to filter the device view.

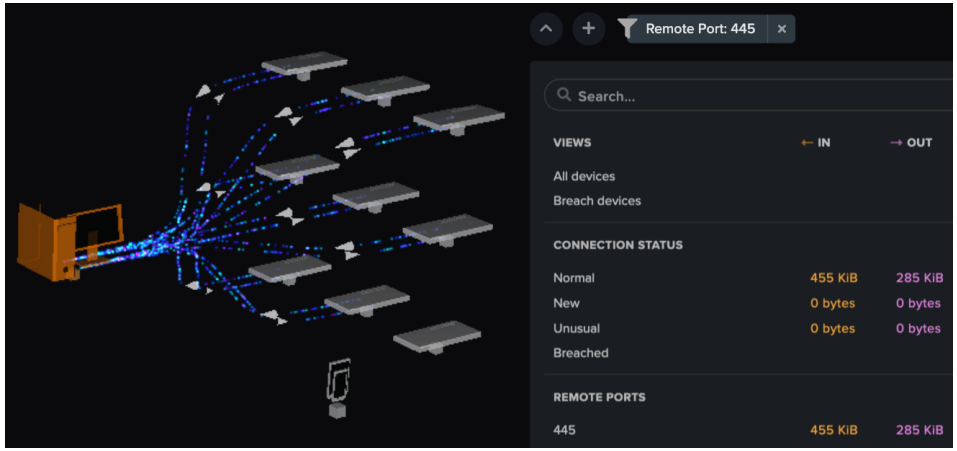


6. When reviewing the summary, sometimes there are more results than displayed. To inspect these options, click the **view more data** button.

7. There are many filtering options to narrow down the results and to restrict the visualizer data. Click the plus icon at the top of the summary to **view all available filters**.



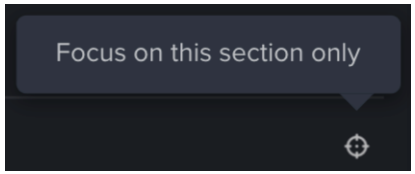
8. Alternatively, **click a row to restrict results**. This is a useful way to quickly understand how much data has been sent/received and which protocols and ports were used, for example. Look out for unusual data on specific ports. Large volumes may be of particular interest and require further investigation.



Top Tip:

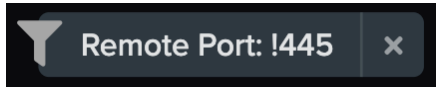
The summary is split into different sections: Views, Connection Status, Remote Ports, Local Ports, Devices, Subnets, Networks, Protocol and Application Protocols.

To focus the summary on one of these categories and view the most common results, click the cross hairs.



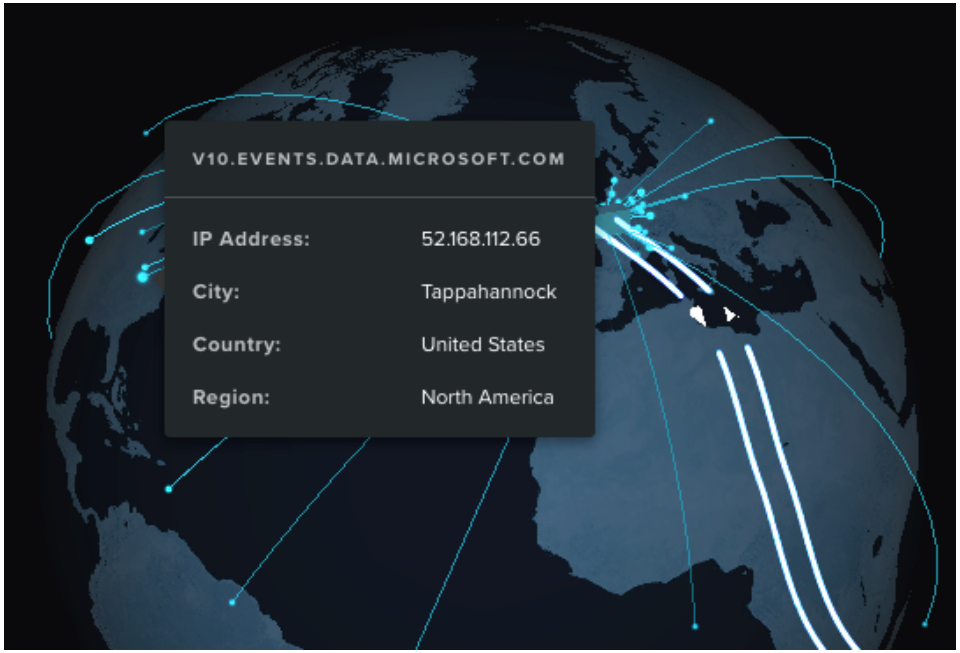
4. Visualization Options

Note: Hold shift and click on a different entry from the summary to create an exclude filter.



9. Once applied, click the **cross** beside a filter to remove and reset your selection.

10. If a device has made **external connections**, the locations will appear on the globe. Hover over the dots to view the IP address as well as domain and country information.



Device View

11. Clicking on any of the dots will open an **alternative view** in the Threat Visualizer, showing all external connections made by the device around the globe.

Note: This removes the device view and allows you to focus on external locations only.

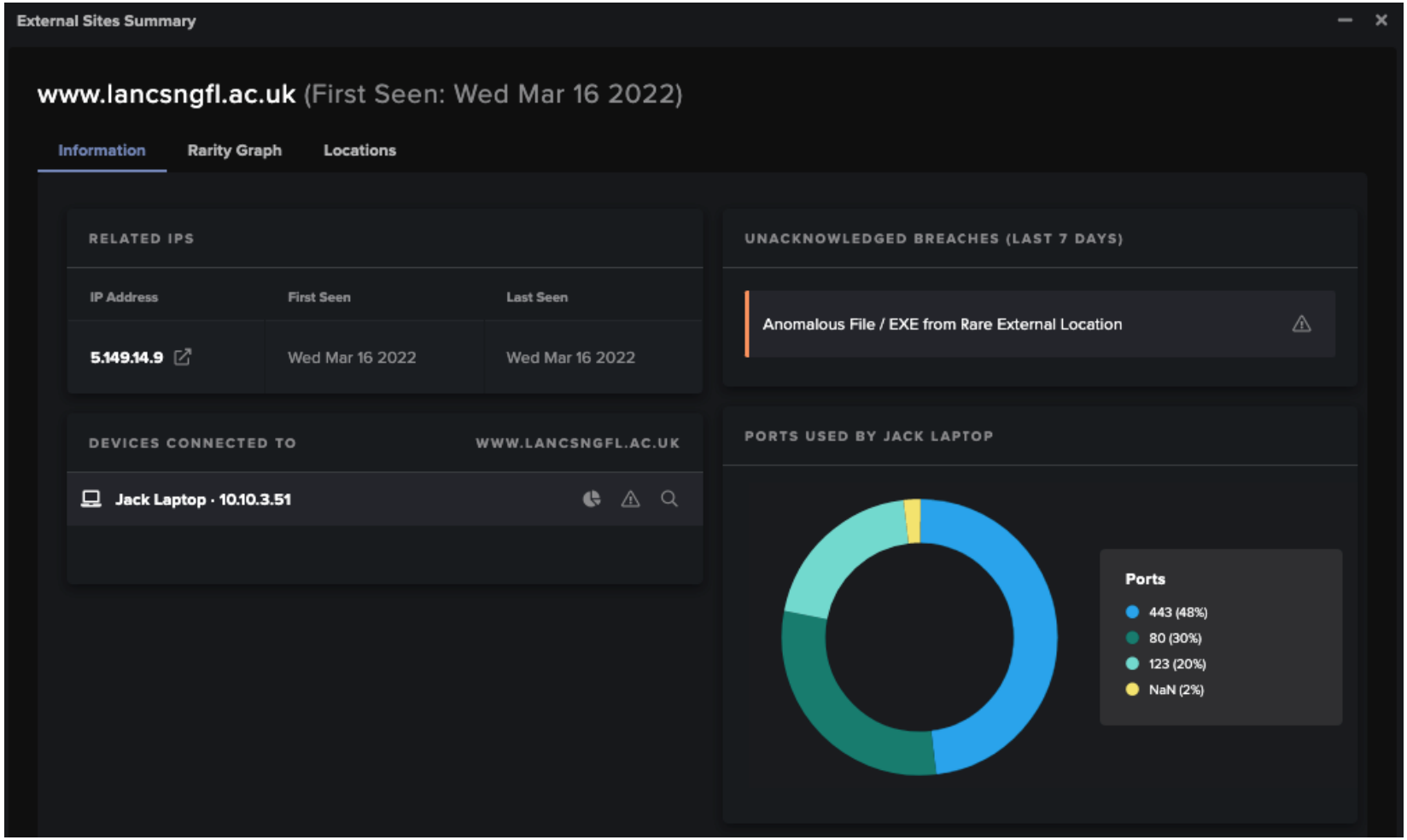
Top Tip:

The External Sites Summary may be accessed in multiple ways. It can be opened by searching for an external domain in the Omnisearch bar and selecting the **globe icon** at the end of the row.

Furthermore, any time an external domain is presented in event logs, an **arrow icon** can be clicked on to open the summary.

12. Clicking on a dot will open an **External Sites Summary**.

a. **Information**: This produces a list of all hostnames/IPs associated with the selected IP address/hostname. If the destination has appeared in any unacknowledged breaches in the last 7 days, the model breach names will be presented in the top right of the window.



This view provides a convenient shortcut for analysts to quickly check which devices have contacted an external domain. For each connecting device, multiple options are available.

i. Clicking the **pie chart** icon will display the **ports** used by the device to connect to the destination in graph format.

ii. The **Breach Log** for each device can be opened by clicking the **warning triangle** icon.

iii. Finally, clicking the **magnifying glass** from a device row will center the visualizer around the selected device.

b. **Rarity Graph**: This changes the view in the External Sites Summary to show the changes in rarity of the endpoint over time.

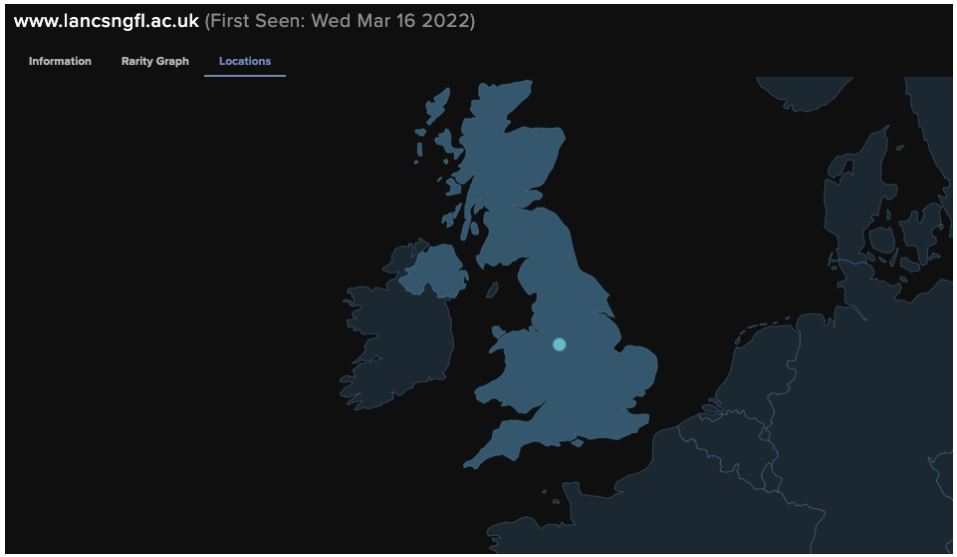
This rarity may increase or decrease over time based on how often it is seen in network traffic. This means the graph's profile may be flat, could have a gradient or may contain peaks or troughs.

For example, if no devices connect or only one device occasionally connects to a domain, it will remain consistently rare (close to 100%).

However, if multiple devices connect to the same domain on a regular basis, such as a company-approved search engine, the rarity will decrease over time.

If external destinations are connected to by many devices at once and then not connected to again on a regular basis, this could impact the graph and cause a dip in rarity.

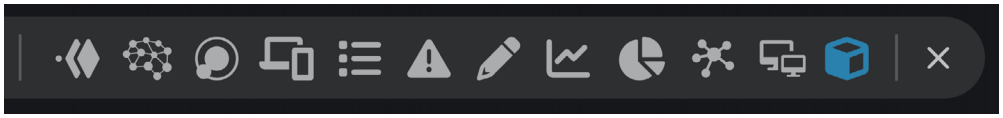
c. **Locations**: The final view in the External Sites summary shows the location of the IP address. It will zoom in to the country and the location is marked by a pulsating, blue circle.



Device Details

Continue your learning with our dedicated video 6: Device View - Part 2

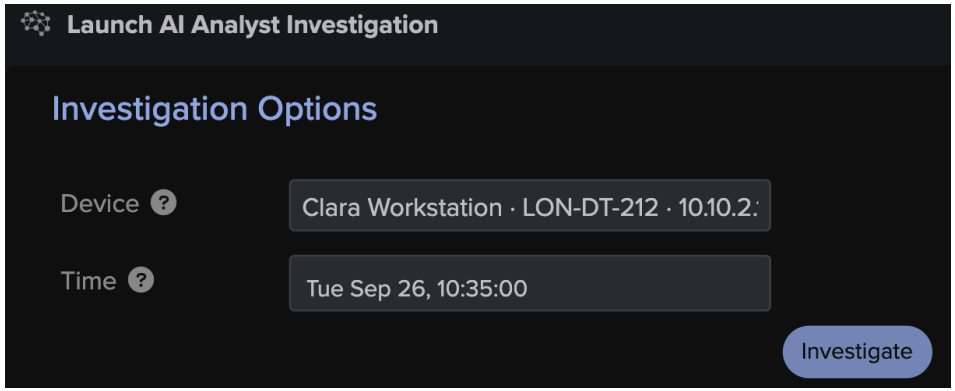
As Darktrace analyses a network, it automatically discovers and records all devices including servers, desktops, phones, printers, and other devices. From this data, the Threat Visualizer generates a collection of summaries, graphs, and logs for each device, which are all easily accessible.



1. Within the Device View, notice a **series of icons** displayed on the right of the Omnisearch bar. What is displayed is permission dependent, but from left to right using the image above, the icons are as follows:

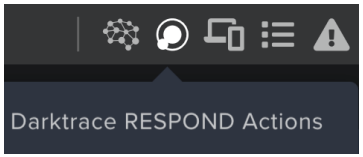
E2E	Opens the device in E2E (if available)
AI ANALYST	Triggers AI Analyst on demand for the device
DARKTRACE RESPOND ACTIONS	Shows Darktrace RESPOND actions taken on the device
DEVICE SUMMARY	Summarizes key device details
DEVICE EVENT LOG	Shows all connections/events for a device
DEVICE BREACH LOG	Displays device specific model breaches
EDIT DEVICE	Allows device specific details to be modified
GRAPH	Opens a graph of all connectivity
CONNECTIONS DATA	Shows port usage and connections
SIMILAR DEVICE MAP	Visualizes similar peer devices
SIMILAR DEVICES	Lists similar devices on the network
SUBNET VIEW	Opens the Subnet View

2. The brain icon allows the user to instigate an **on-demand AI Analyst** investigation. This option allows the user to select a time to focus the investigation around.



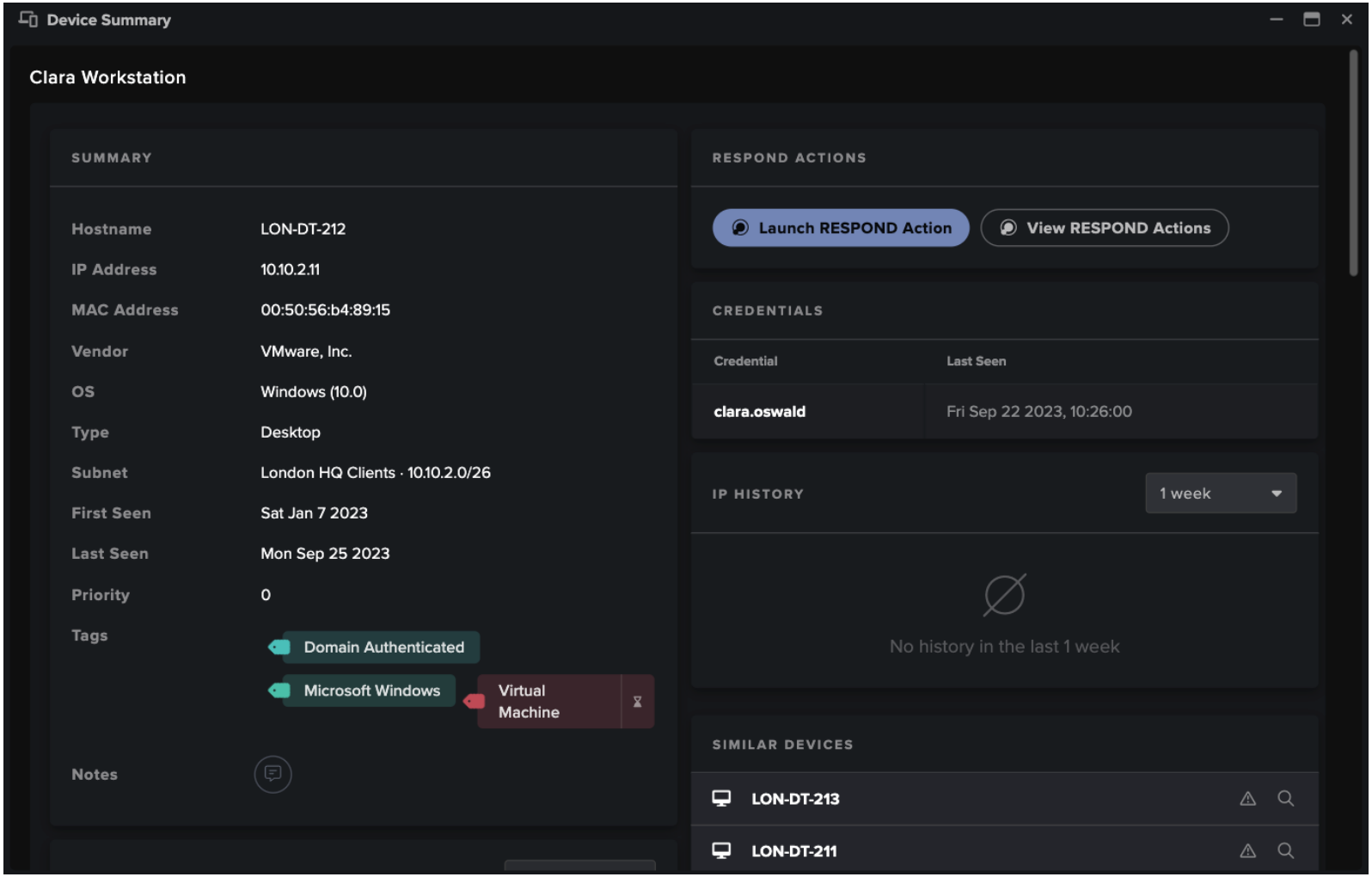
Note: This functionality is discussed in the AI Analyst chapter.

3. One icon in the Omnisearch bar is only relevant for deployments with the **Darktrace RESPOND** module. This icon allows the user to review and confirm actions performed by Darktrace RESPOND on the device.



Note: This functionality is discussed in the Darktrace RESPOND/Network course.

4. Click the **Device Summary** icon.



   a. **Key information** that has been captured by Darktrace is displayed at the top of the window, including specific device information, as well as **credentials** observed on the device, a seven-day **IP history** and list of **similar devices**. Specific **notes** can be added by users.

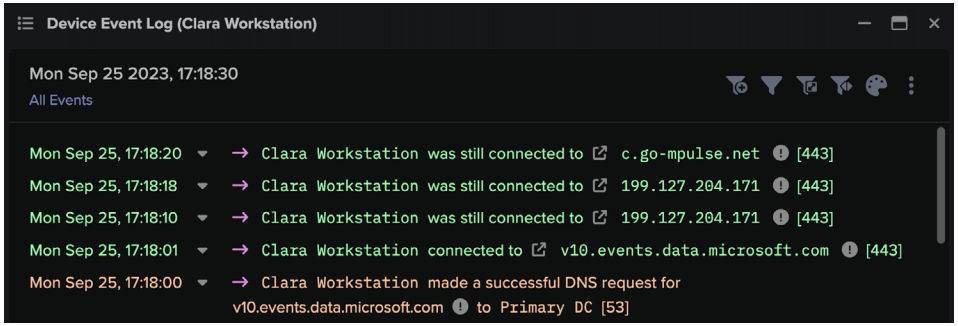
   b. Down the left, the Device Summary also provides a quick and easy way to understand **what activity has occurred** on the device in the form of historical model breaches and AI Analyst incidents. This activity can be displayed for different time frames between the last week up to the past six months.

      This **Model Breach** and **AI Analyst Incident Event** activity is broken down into two further categories - **Unacknowledged** and **Acknowledged**. This can be useful to see what activity might be expected from a device by viewing the historical trends, depending on the time frame selected, or what activity is particularly anomalous and should be investigated further.

   c. Scroll down the Device Summary window. Displayed here are the **ports** that are most commonly used and served, as well as the devices it most commonly communicates with. This is a useful way to quickly understand what roles the device has on the network.

Device View

5. The **Device Event Log** is similar to the Model Breach Log, except it shows all connection data in the given time frame. It includes filter options along the top row.



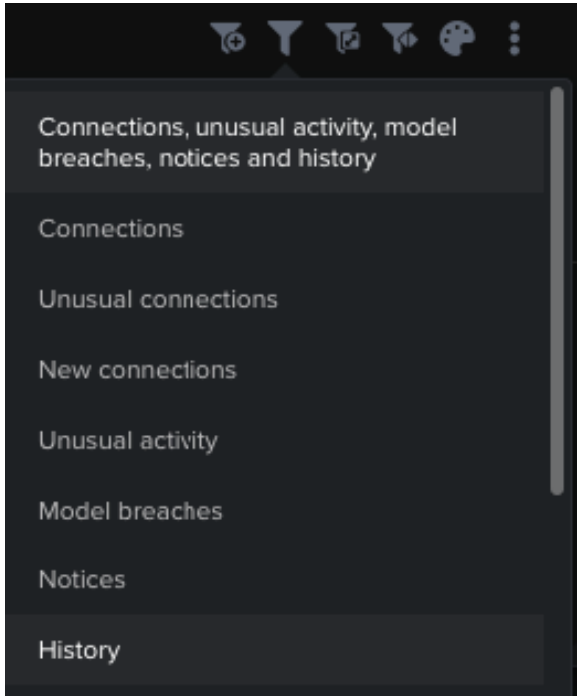
a. The history of a device is easy to recall within the Device Event Log. Select which type of events to show in the log. Click the **History** option to reveal a range of key events in the Event Logs, including:

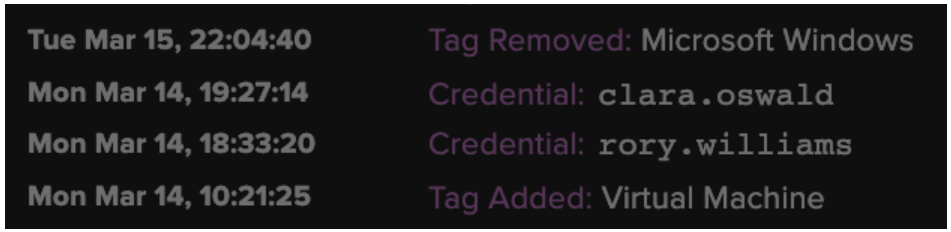
i. Kerberos, RADIUS and POP3 authentications

ii. Changes in IP, MAC, hostname, and subnet

iii. Application, removal, or expiration of tags

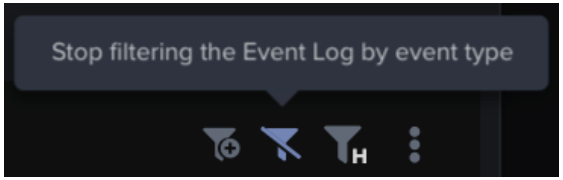
iv. Observed user agents



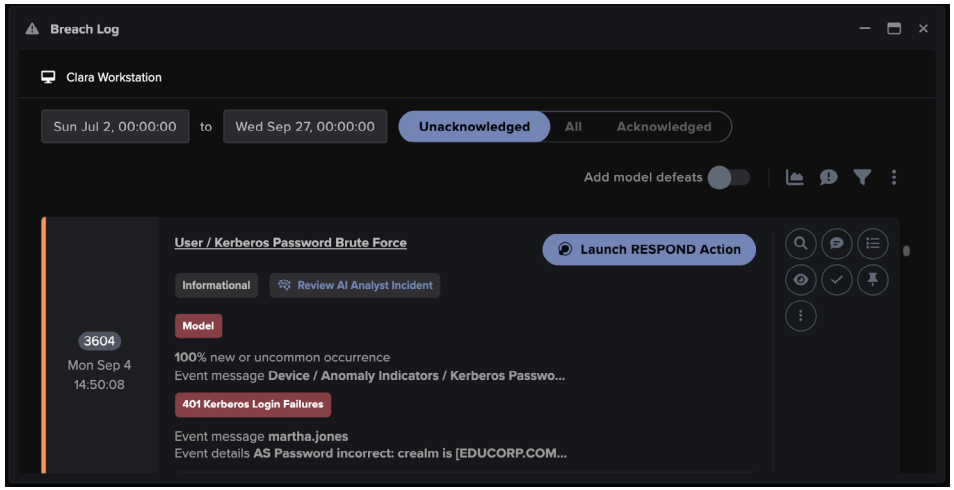


These events can help with understanding how a device is being tracked over time or which user authenticated prior to an event of interest. For example, viewing the credentials can be useful when investigating lateral movement. The entries displayed represent two weeks leading up to the current Threat Visualizer time, as set in the time selector.

b. If filters have been applied, click the **crossed out filter** icon to remove them and return to the full Device Event Log.

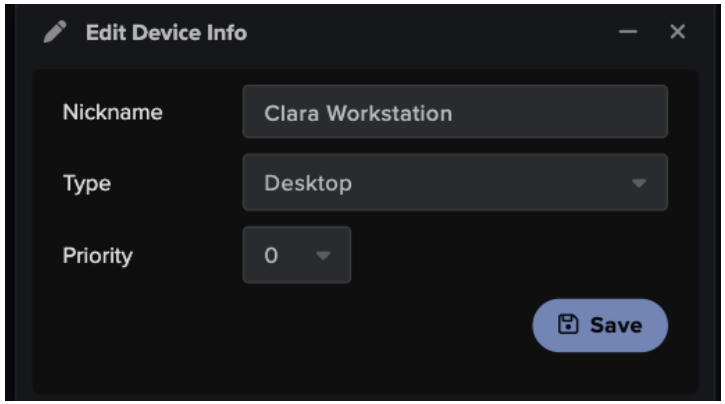


6. The **Device Breach Log** button reveals all breaches for the device over the selected time frame.



Device View

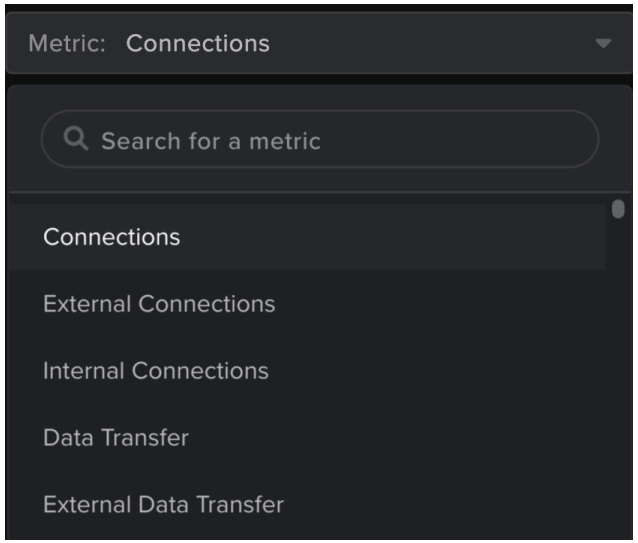
7. The **Edit Device Info** can be used to update the Device label (nickname) and type. This information is useful to assist analysts in understanding devices.



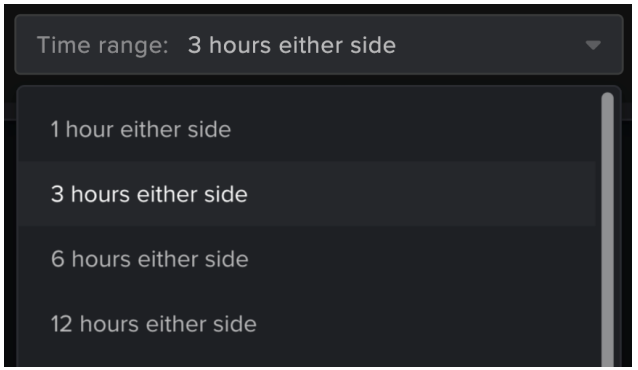
Note: Such details can be edited in the Device Admin page. This and Priority are covered in other classes.

8. The **Open Graph** function can display a broad range of metrics.

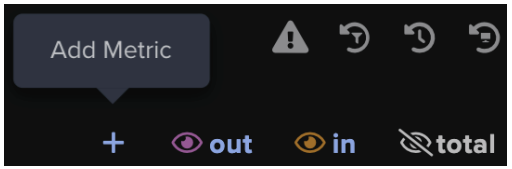
a. Select the **Metric** drop-down menu to review the options available. Remember that historical data can be viewed by clicking on the graph. This is particularly useful to track peaks of traffic flow at different times of the day and week.



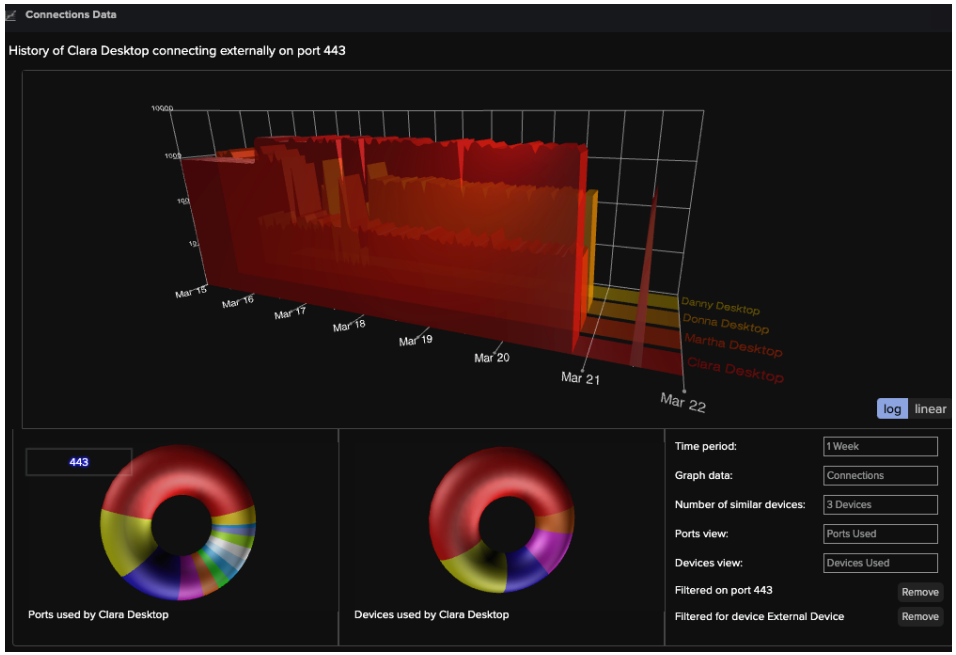
b. Click the **Time Range** under the x-axis to reveal additional time filters in a drop-down menu.



c. Additional metrics can be added to the graph to provide a better understanding of network events using the **plus** button.



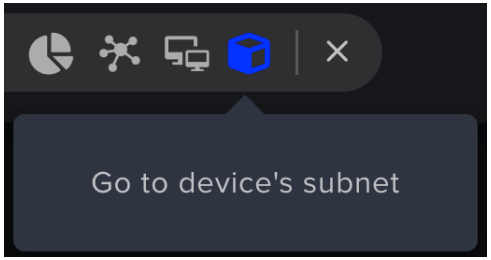
9. Select the **View Connections Data** icon to display additional graphics and summaries.



Through these graphics, it is easy to understand the ports and devices used by each device. Simply hover over the different colors in the donut charts to highlight the port or device.

It is also possible to click the menu options in the bottom right to filter or expand the data.

10. Finally, the **Go to Device's Subnet** button is a handy shortcut to open the Subnet View to easily visualize device connectivity on the subnet.

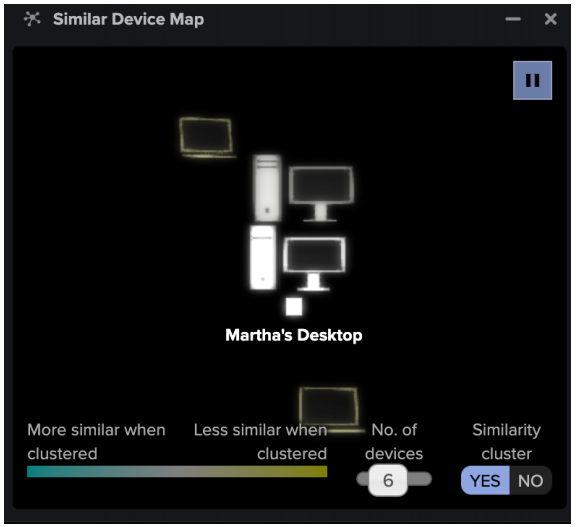


Similar Devices

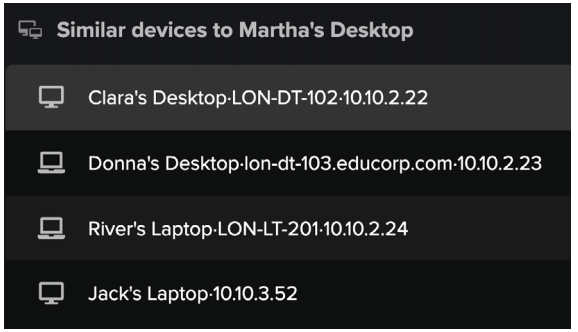
Darktrace can group devices together based on their similarity. This is automatically calculated in real time and uses machine learning and mathematical clustering values to calculate how similar one device is to another. At a basic level, it includes a combination of connecting devices on the network or devices which share the same port usage.

When in the **Device View**, there are two options for viewing similar devices from the Omnisearch bar.

The first option is the **Similar Device Map** which is a three-dimensional view that displays similar devices. Hover over a device icon to obtain its information. This view automatically rotates. Utilize the pause function in the top right of the window to stop the animation and view any of the devices.



Alternatively, the **View Similar Devices** icon provides a list of similar devices which can be easily clicked to explore each device in its own view.



Visualization Chapter Test

This page will test your knowledge and check your understanding of the Visualization section. This is the perfect way to work towards your **Threat Visualizer Essentials Certification**! *Select an answer by clicking on it. Wrong answers are denoted by a red cross and right answers are denoted by a green tick.*

DARKTRACE
Essentials Certification

1. Which colour(s) will indicate anomalies on the subnets?

- [ ] Blue / Purple
- [ ] Gray / Black
- [ ] Yellow / Orange

2. Which icon will open a representation of all connections observed on the subnet?



3. True or False: There is only one way to access the External Sites Summary.

- [ ] True
- [ ] False

4. Which option will display a three-dimensional view of similar devices?

- [ ] View Similar Devices
- [ ] Similar Device Map
- [ ] Device View

5. Which option from the Device View will show port usage?

- [ ] AI Analyst
- [ ] Edit Device Info
- [ ] Connections Data

6. Which information CANNOT be changed from the Edit Device Info page?

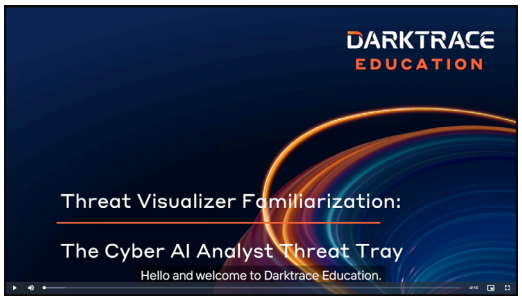
- [ ] The Device's Tags
- [ ] The Device's Type
- [ ] The Device's Priority

Clear All Answers

5. Cyber AI Analyst

The Darktrace Cyber AI Analyst (AIA) investigates, analyzes and triages threats seen within your Darktrace environment and forms potentially interesting and unusual incidents, often centered around a device. Incidents involving multiple devices are classified as 'cross-network' incidents. By learning from the millions of interactions between Darktrace's expert analysts and Darktrace DETECT, the Cyber AI Analyst combines human expertise with the consistency, speed, and scalability of AI. With its global network awareness and machine-speed investigation time, it performs the heavy-lifting of the analysis process. Not only does AIA perform autonomous, unprompted investigations, it is also available on demand for a selected device. Let's discover how to interpret and instigate AI Analyst incidents.

AI Analyst Workflow



Continue your learning with our dedicated video 7: Cyber AI Analyst - Part 1

When logging into Darktrace, Cyber AI Analyst 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. The workflow below outlines Darktrace's recommendation for reviewing incidents in the Threat Visualizer.

- Open the Threat Visualizer to review AI Analyst Incidents
- Select a severe or interesting Incident from the Threat Log
- Read the summaries to understand the order of events
- Review the detailed event information
- Dive into the related Model Breaches
- Using AI Analyst's recommendations, taking any remediating actions
- Create a PDF report which describes the events
- Acknowledge individual events or the entire incident

Note: This best practice can also be applied to the Cyber AI Analyst tab in the Mobile App.

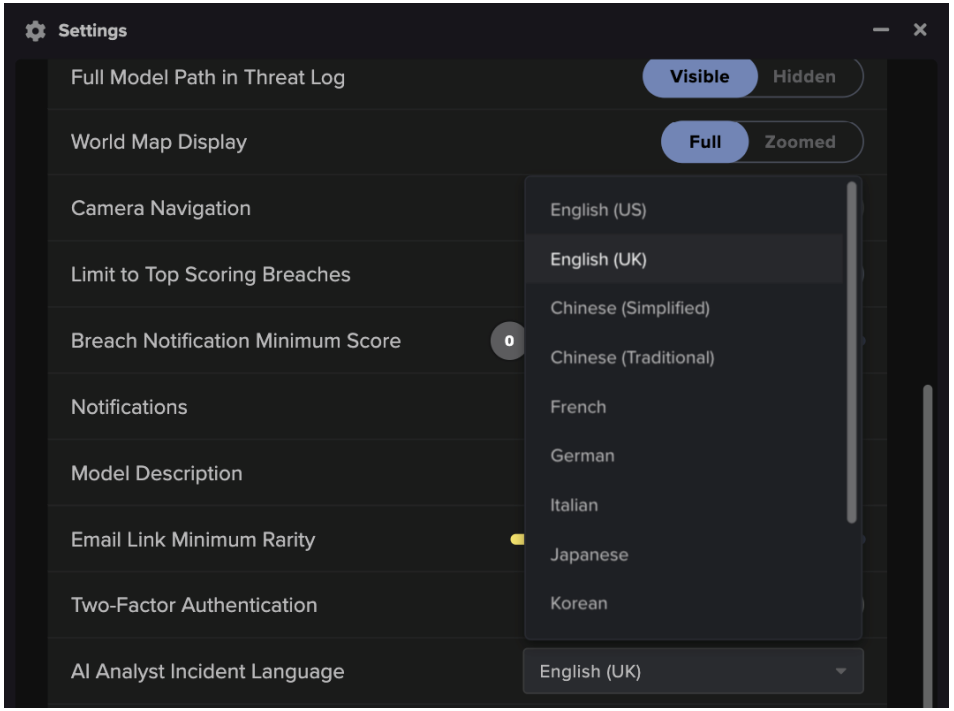
AI Analyst Incident Language

Before reviewing AI Analyst incidents in the Threat Tray or creating AI Analyst reports, 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).*

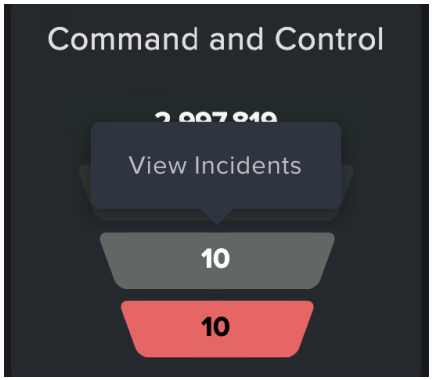
3. Open the **AI Analyst Threat Tray** along the bottom of the Threat Visualizer. Incidents should now be presented in the selected language.



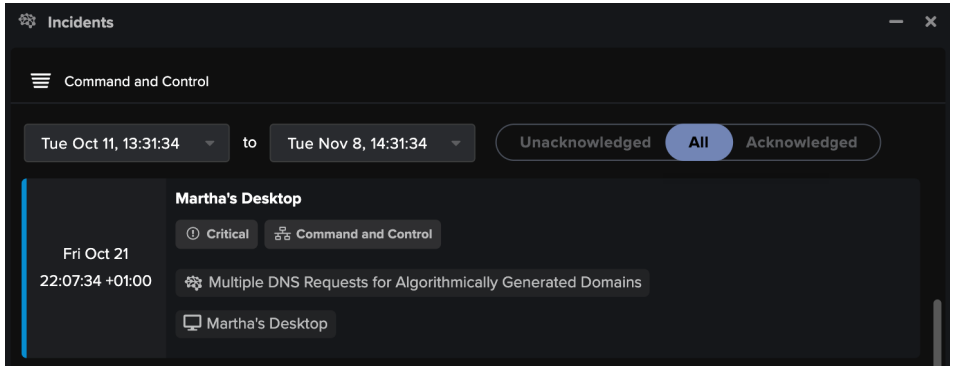
AI Analyst Incident Log

Cyber AI Analyst incidents can be viewed in an AI Analyst incident log.

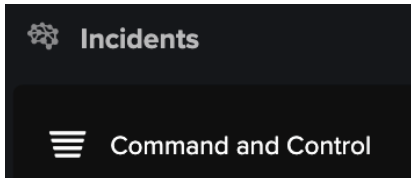
1. From the "MITRE ATT&CK Tactics Processed" statistics on the Threat Visualizer homepage summary, click on **View Incidents** or **View Critical Incidents** to open the incident log.



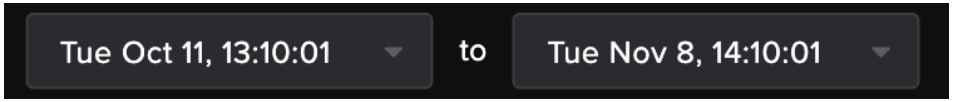
2. The panel displays a count of **events and alerts** that are relevant to "tactics" from the MITRE ATT&CK Framework



3. The **MITRE tactic** filtered upon is displayed in the top left of the window.

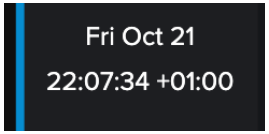


4. Underneath is the **time range** for AI Analyst incidents to be included in the log. The default range is taken from the 28 day summary panel range but can be altered using the time selectors.



5. The log can also be filtered to show **Unacknowledged**, **Acknowledged** or **All** states of AI Analyst incidents. By default, acknowledged alerts are removed from the returned results.

6. Each incident appears as a separate entry and lists the initial device at the top. The **time** that the incident was first created appears on the left.



7. Important information is displayed such as the **incident priority**, **involved devices**, **types of activity detected** and the **associated MITRE tactics**

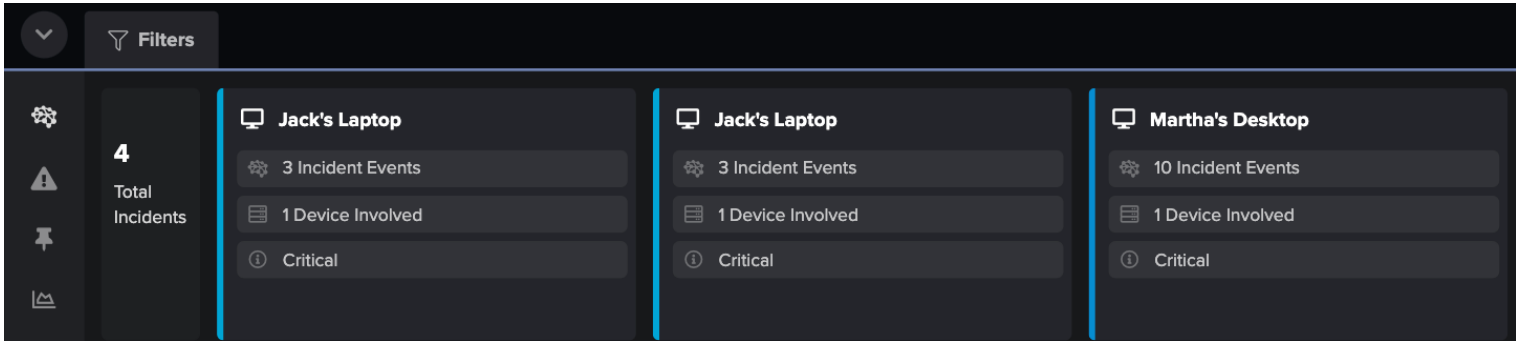
Example incident Information	Meaning
Critical	The incident behavior category - in this case, "Critical".
Command and Control	A MITRE tactic associated with the incident.
Multiple DNS Requests	The title of an event that is part of the AI Analyst incident.
Martha's Desktop	A device that was involved in the incident.

8. Click anywhere on the log entry to open the **incident information** event.

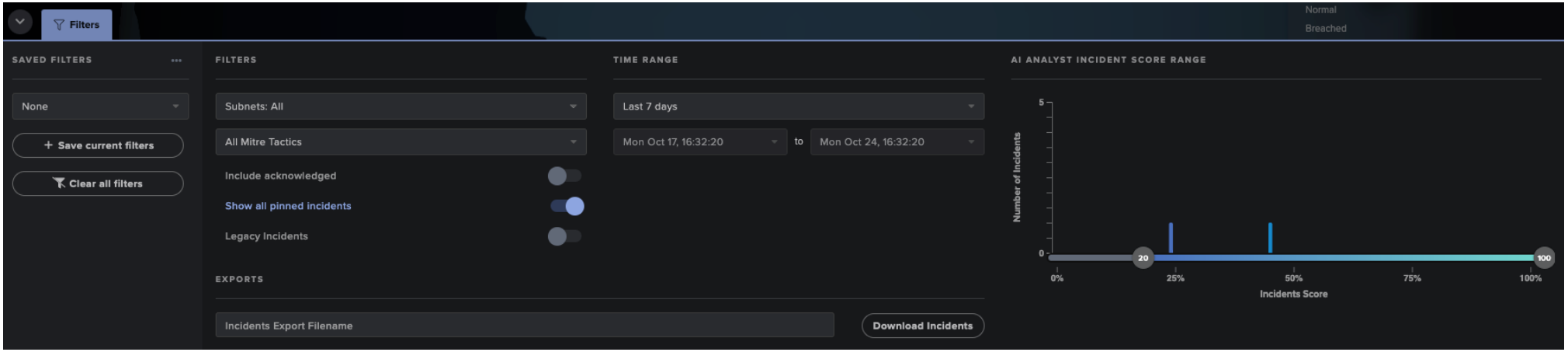
AI Analyst Incidents

Continue your learning with our dedicated video
8: Cyber AI Analyst - Part 2

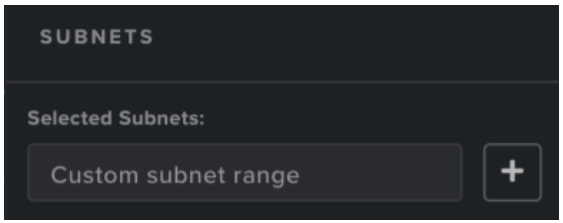
1. The **AI Analyst Incident Tray** is the default view for the Threat Tray displayed along the bottom of the Threat Visualizer interface. This can be selected by clicking on the brain icon on the left.



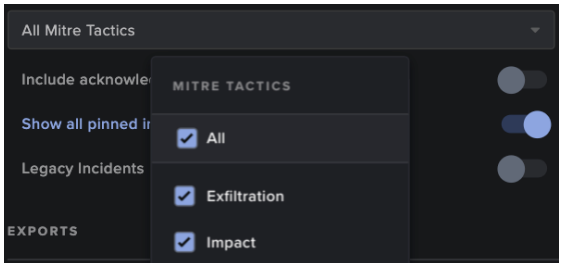
2. Before selecting any incidents, notice the Threat Tray **filters**. As a good starting point, the defaults of the **Last 7 days** and the score above **20%** should display an interesting array of incidents.



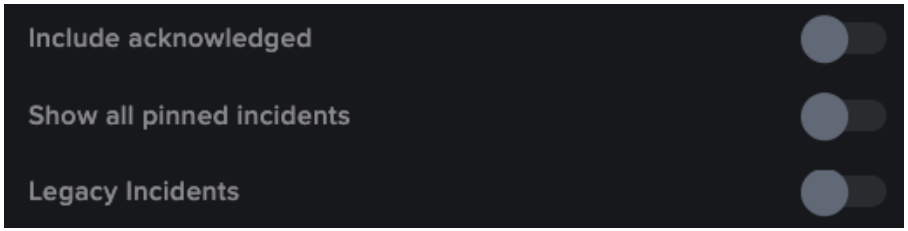
a. Under the filters heading, notice the first drop-down - **Subnets**. This focuses the Cyber AI Analyst Threat Tray on device incidents in the selected subnets.



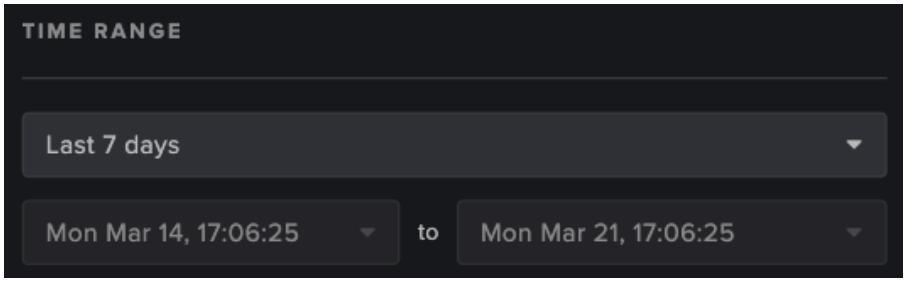
b. Incidents can be filtered by **Mitre Att&ck Tactics**, by selecting single, multiple, or all tactics.



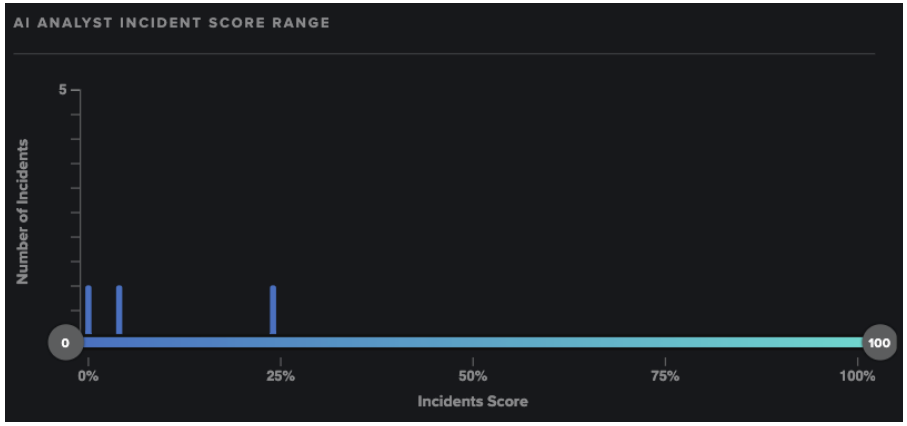
c. Next, the Threat Tray can be filtered using three toggles: **Include acknowledged, Show all pinned incidents**, or **Legacy Incidents**.



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

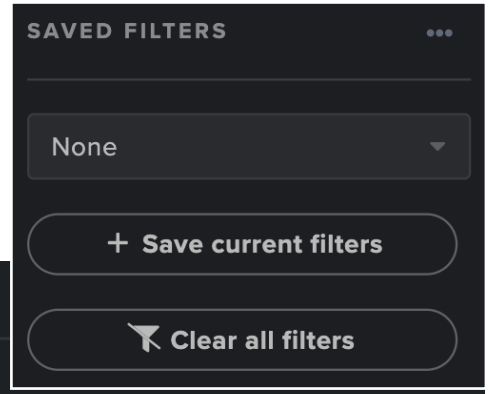


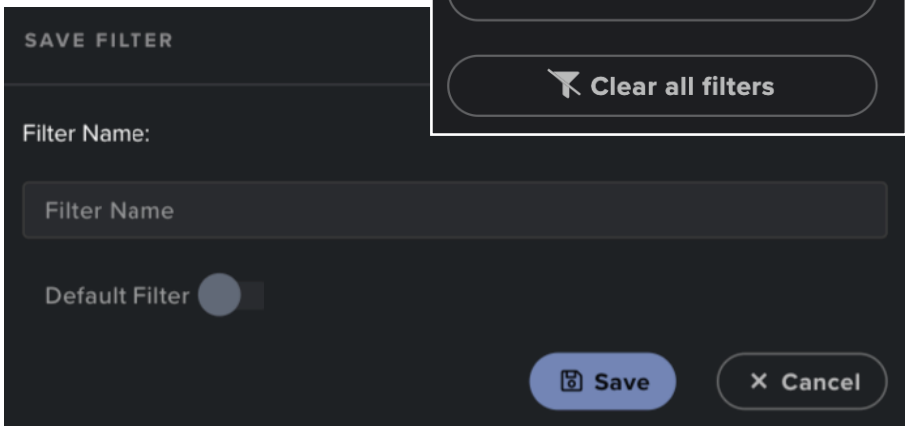
e. Finally, notice the **AI Analyst Incident Score Range**. This slider shows the number of incidents plotted against their score.



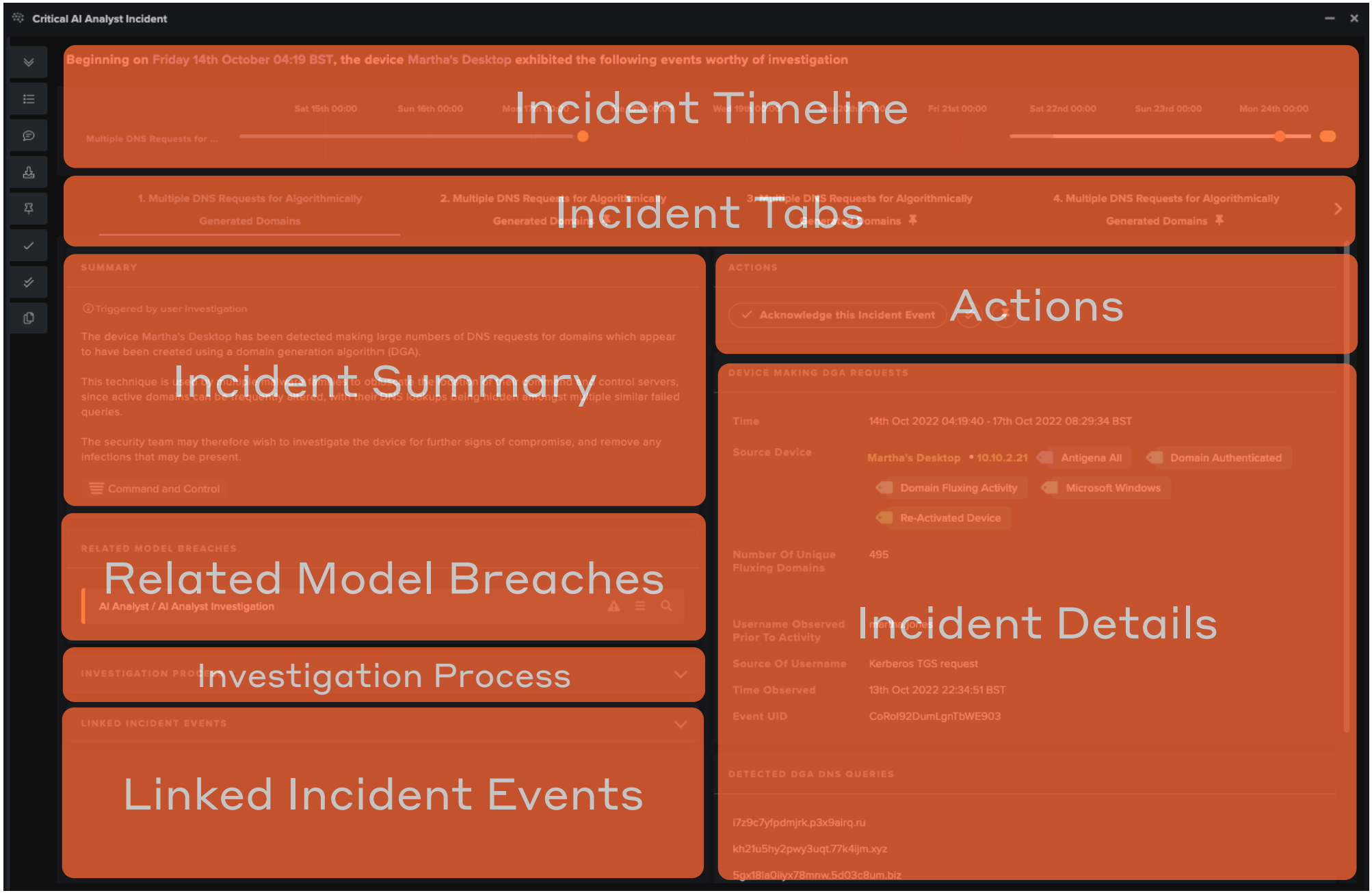
Note: The default slider will be set between 20% and 100%. This feature will be reset if the browser is refreshed.

f. 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.



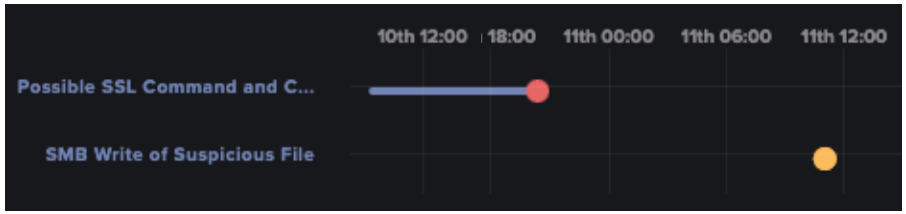


3. Click on any Cyber AI Analyst incident to open the **AI Analyst Incident** window. This window will display a range of information, split into different sections.



4. First, it is useful to understand the incident. This can be done by looking at how long the activity lasted, what the activity consisted of, reading the summaries and diving into the details.

   a. Along the top of the window is the **Incident Timeline**.

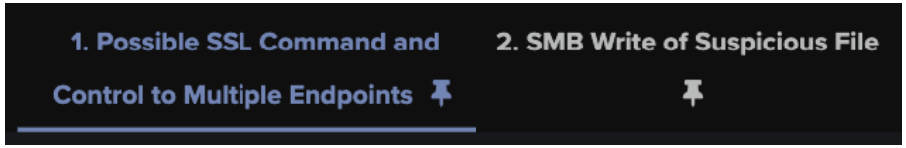


   Model Breaches relating to the Incident Tabs are displayed as dots, where their color indicates severity.

   The currently selected event will be highlighted in blue. A bar in the same row as an incident represents associated activity.

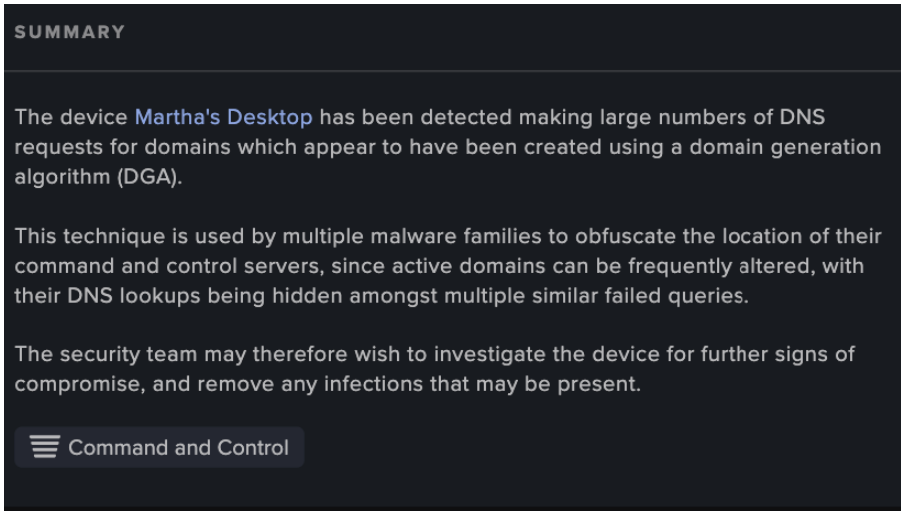
   Note: If there is a green bar present on the timeline, this represents a Darktrace RESPOND activity.

   b. Below the timeline, the **Incident Tabs** can be found.

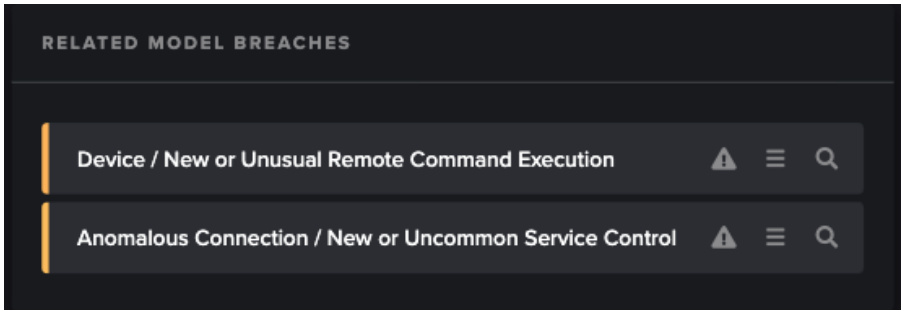


   Each event appears as a tab. Directly select them to view the incident details or click the event in the incident time period graph.

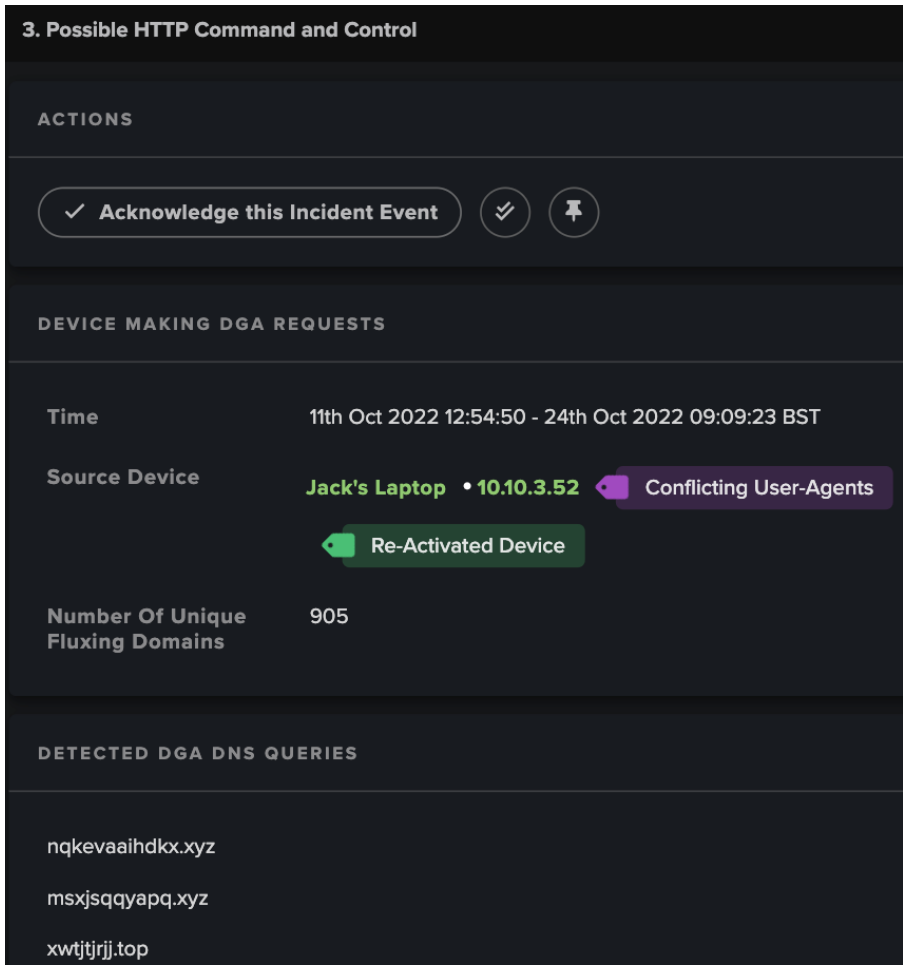
   c. Moving down the page, the **Incident Summary** for the current tab can be read. This high level event outline is given in the left panel explaining the observed activity, possible implications and a suggested action which can be taken by the security team. It also features the corresponding Mitre Att&ck tactic.



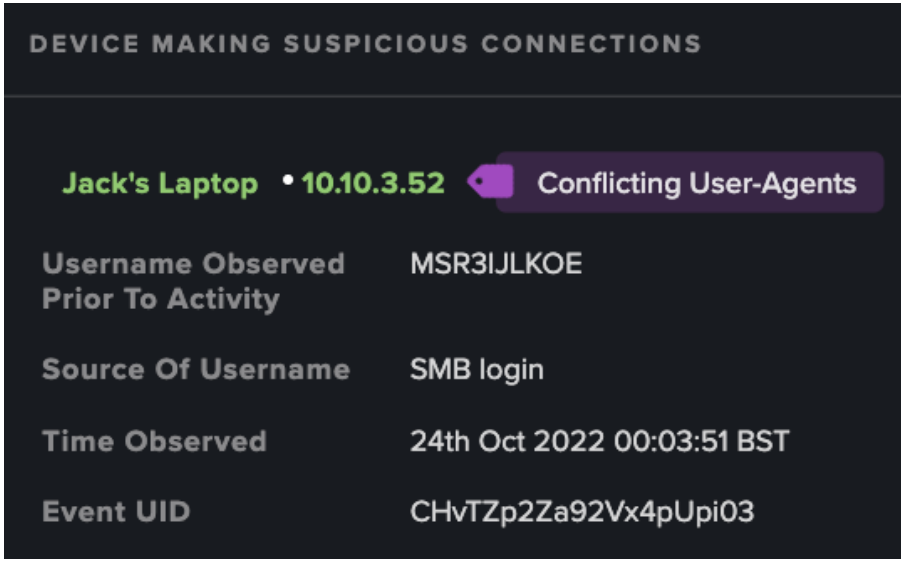
   d. Often, the activity will have **Related Model Breaches**. The associated Breach Log and Model Breach Event Log can be viewed using the first two symbols respectively. Furthermore, the Threat Visualizer can be centered on the device at the time of the breach using the magnifying glass.



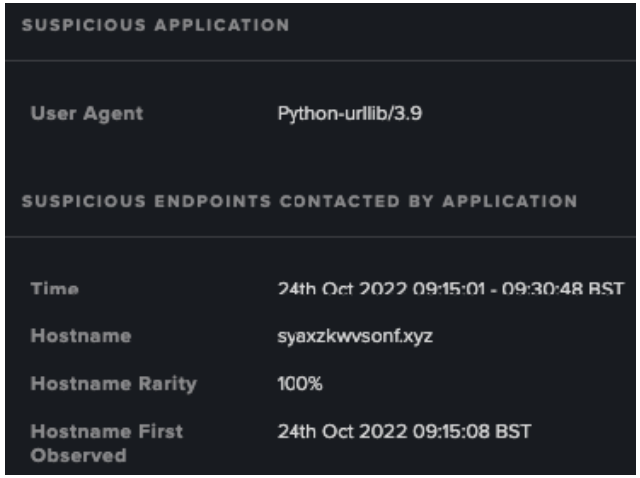
e. In order to dive into the full technical details that AI Analyst has surfaced, go to the **Incident Details** on the right of the window.



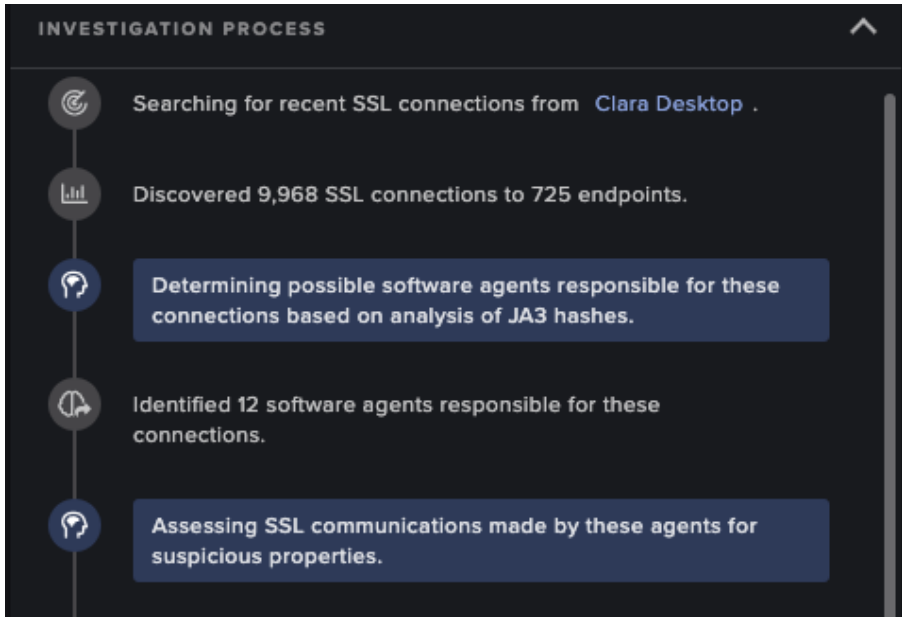
These can be extensive and may be broken down into different relevant sections.



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.



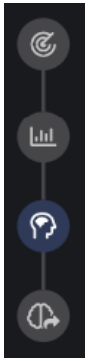
f. It can be useful to read the **Investigation Process** as an optional step. The investigation panel is collapsed by default. Upon expanding, this will display the chain of events, outlining the AI Analyst's thought process.



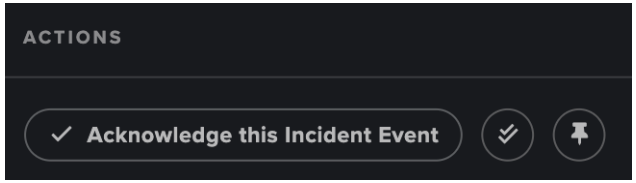
Top Tip:

Hover over the different icons to identify Cyber AI Analyst's investigation stages.

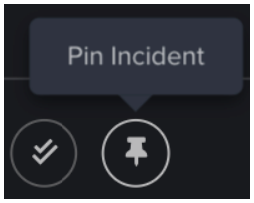
From top to bottom, the icons to the right indicate a targeted search for data, reporting the results of a targeted search, carrying out intelligent data analysis and reporting the results of intelligent data analysis.



5. Once all the details have been reviewed for an individual incident event (tab), 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.

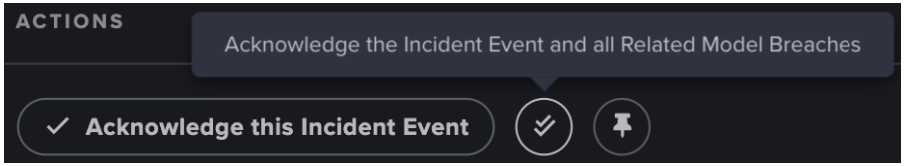


Note: Using this button will pin the individual tab, and not the incident as a whole.

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

Note: This will apply a tick beside the event tab, indicating that just 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.



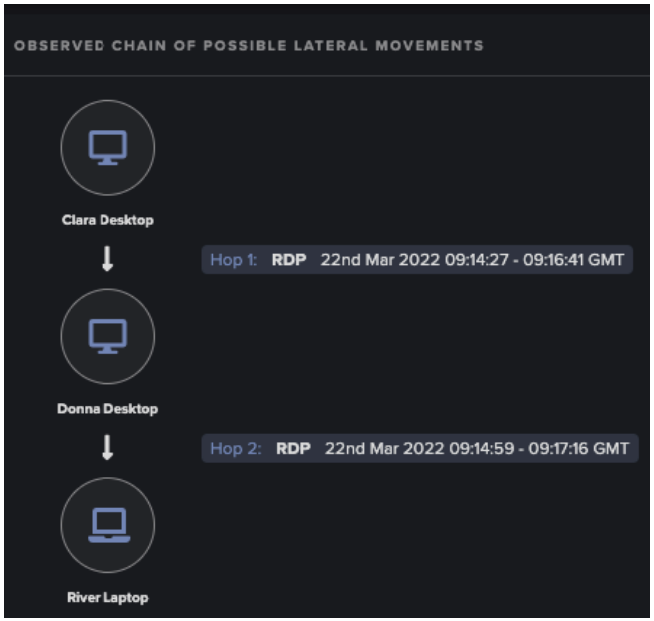
Top Tip:

Using the workflow as outlined so far, each individual AI Analyst incident event can be reviewed and acknowledged ongoing. The next steps can be used to look at and review the incident as a whole.

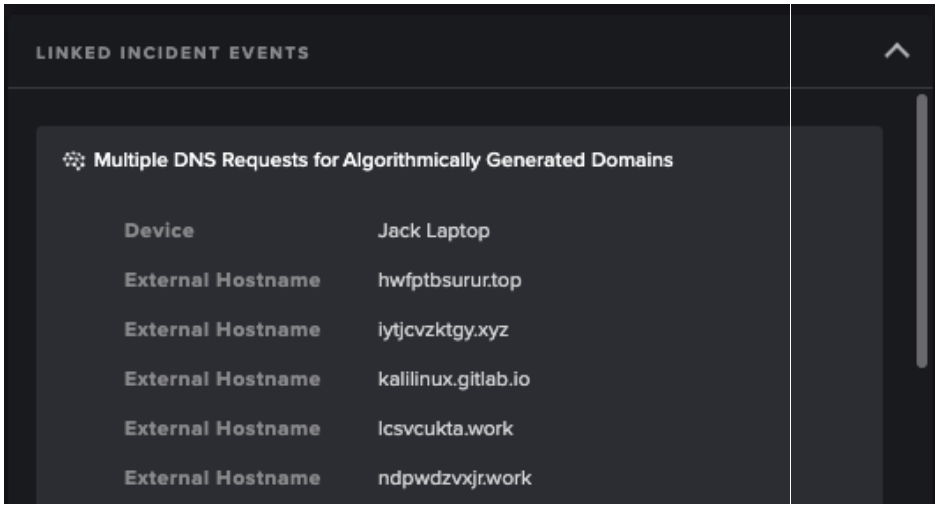
Cyber AI Analyst Additional Information

Sometimes, Cyber AI Analyst may present more information, which can vary from incident to incident.

For example, in cases where a graphical representation can be created, such as lateral movement, the chain of events may be depicted.

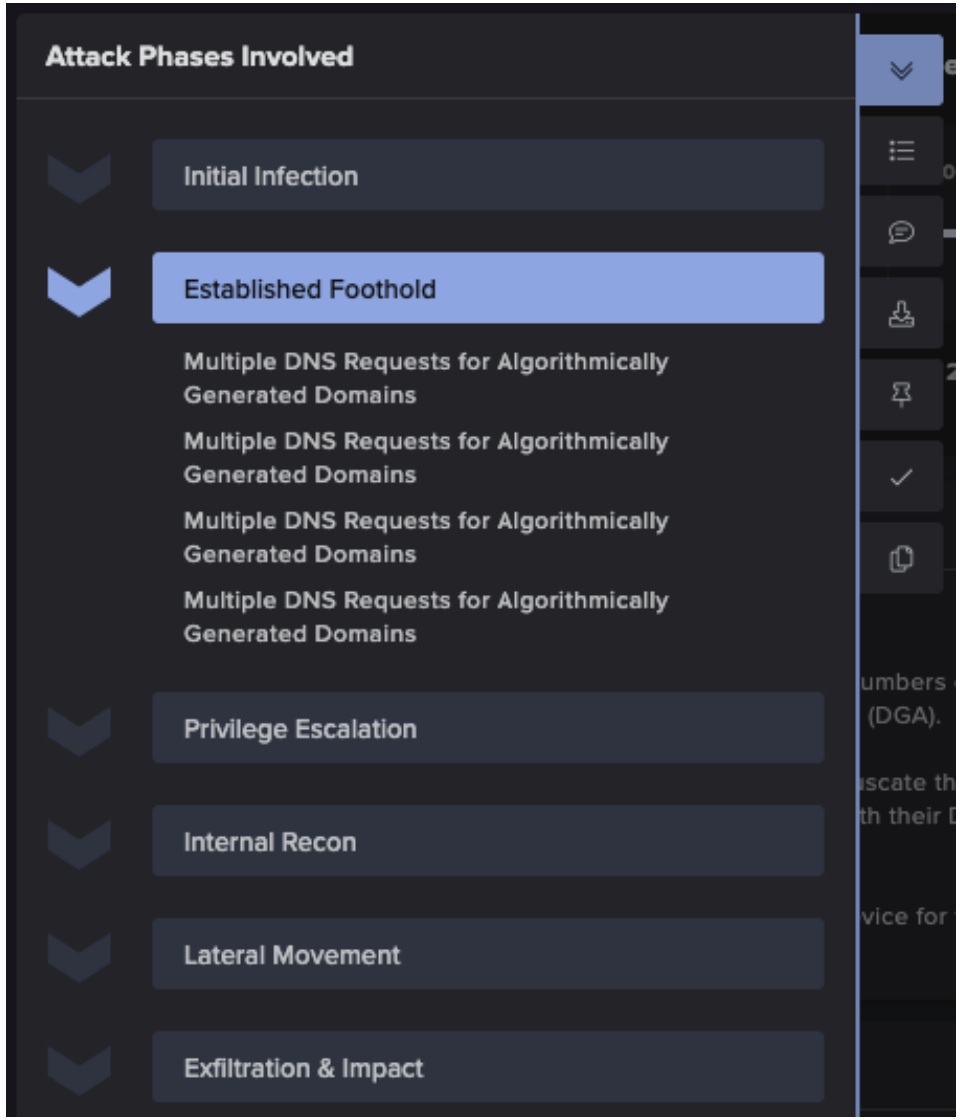


Furthermore, if there are any linked incident events, these may be listed and can provide pivot points to other areas of an incident.

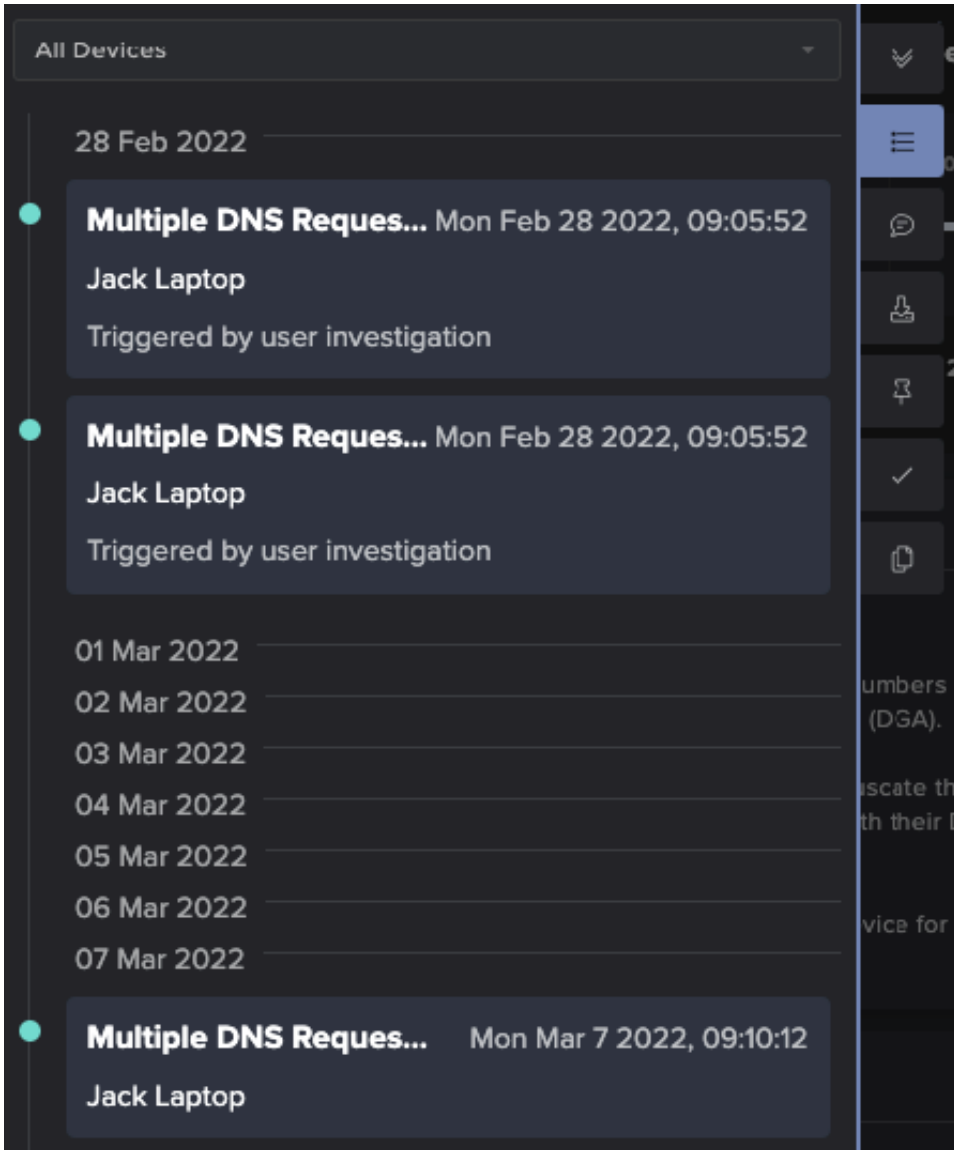


6. Moving onto a wider view of the entire AI Analyst incident, notice the icons down the left-hand side of the incident window.

First, click the **View Incident attack phases** button depicted by the downwards arrows to open a new display. This will highlight which possible attack phases and related activity has been detected during this incident.

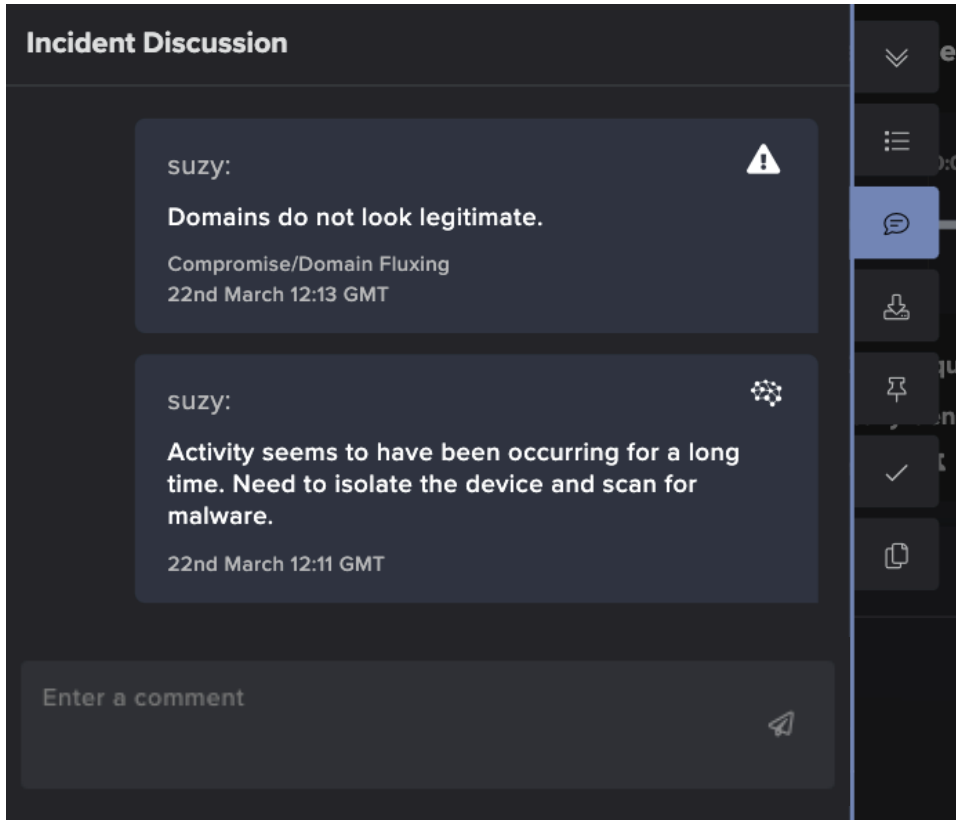


7. Again, to review the incident as a whole, the next icon allows the user to **View the Incident Timeline**.



Note: Some incidents may pull together multiple devices. As such, there is the option to filter this timeline by device using the drop-down at the top.

8. To **comment** on an incident or view any existing incident discussion, click the **speech bubble** icon. Type in the box and click the paper airplane to comment on the incident.

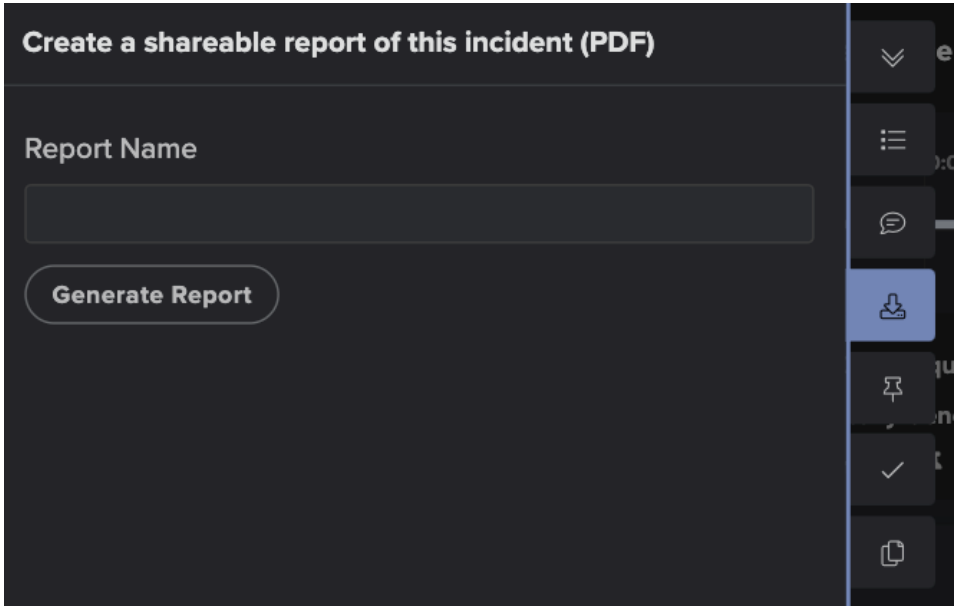


Top Tip:

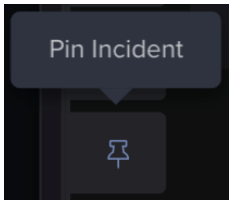
Notice that comments added in different sections of the interface will be distinguished by icons in the top right and may also include information about where this comment was added.

A combination of model breach (warning triangle) and AI Analyst incident (brain symbol) comments can help a team with event tracking and knowledge sharing.

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

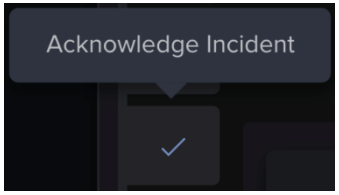


10. To pin the incident and save it for later, click the **Pin Incident** icon. The incident in the Threat Tray will also have a pin icon displayed to demonstrate which AI Analyst incidents have been pinned.

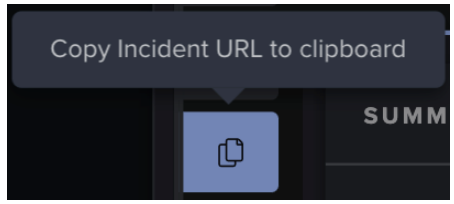


Note: Pinned incidents will remain on the left-hand side of the Incident Tray, regardless of the time frame.

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



12. Finally, notice the **Copy Incident URL to clipboard** icon. This can be clicked to copy the URL of the selected AI Analyst incident to the device clipboard. It can then be easily shared with colleagues or saved locally.

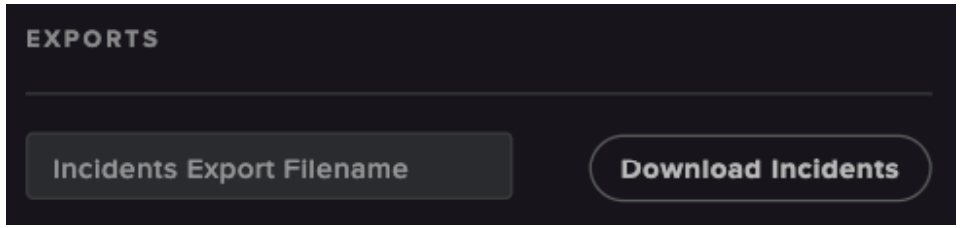


The URL will be of the following format:

https://<servername>/#aiagroup/<unique string>

13. While individual incidents can be downloaded from the Incident Log as previously described, **all the incidents can be downloaded** from the Threat Tray.

With the Threat Tray filters open, notice the **Exports** section. Type in a **filename** and click **Download Incidents** to create a PDF report of all AI Analyst incidents in the Threat Tray.



AI Analyst API

AI Analyst Incidents can also be viewed in a different format via the API.

Such information may be useful for exporting.

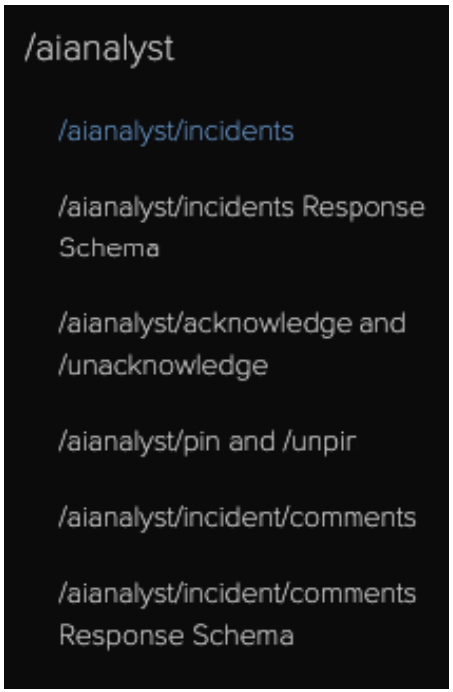
The first endpoint presents all AI Analyst events. To view all events on one page, use a browser to navigate to:

https://<hostname>/aianalyst/incidents

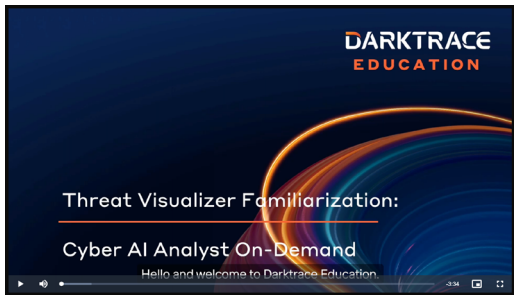
The second endpoint will restrict the results to show a chosen AI Analyst incident, based on its ID, to view any comments. In a browser, the endpoint format will be the following:

https://<hostname>/aianalyst/incident/comments?incident_id=<id-string>

For help with understanding the API schema, refer to the Threat Visualizer API Product Guides on the Customer Portal.

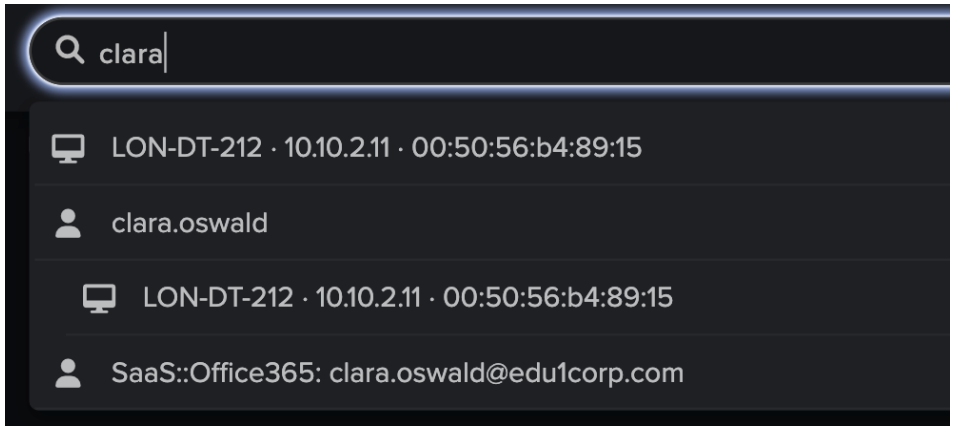


AI Analyst On-Demand

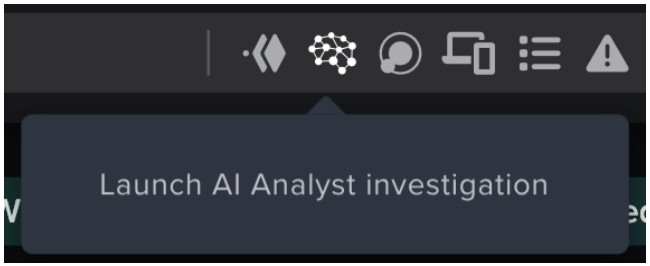


Continue your learning with our dedicated video 9: Cyber AI Analyst - Part 3

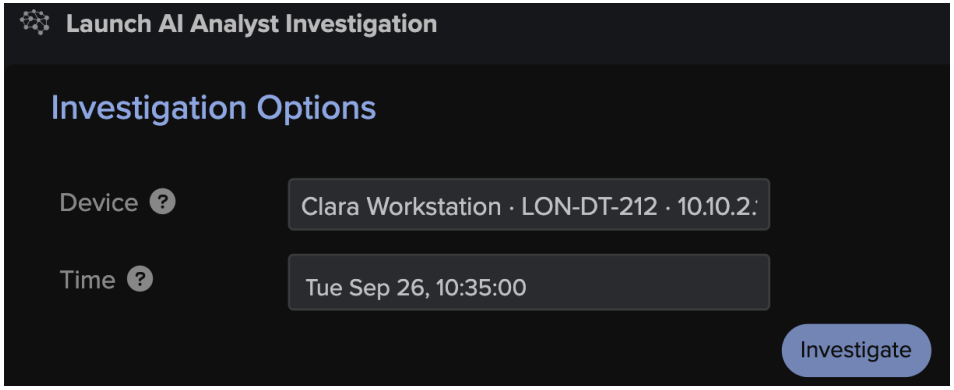
1. A common way of prompting an AI Analyst investigation is to populate a **device or SaaS user** in the **Omnisearch** bar. This can be achieved manually or by using the magnifying glass from an incident/breach log.



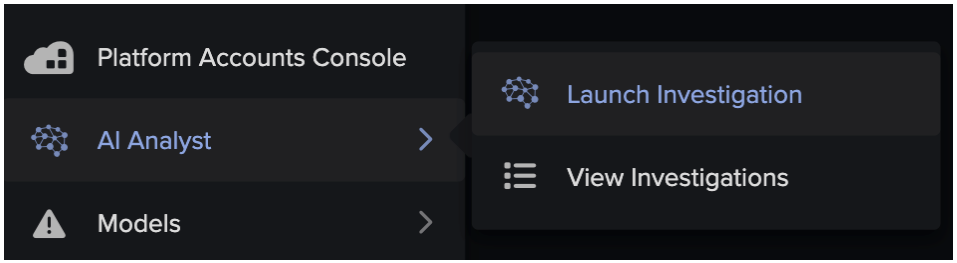
With the device/SaaS account selected, click the **brain** icon.



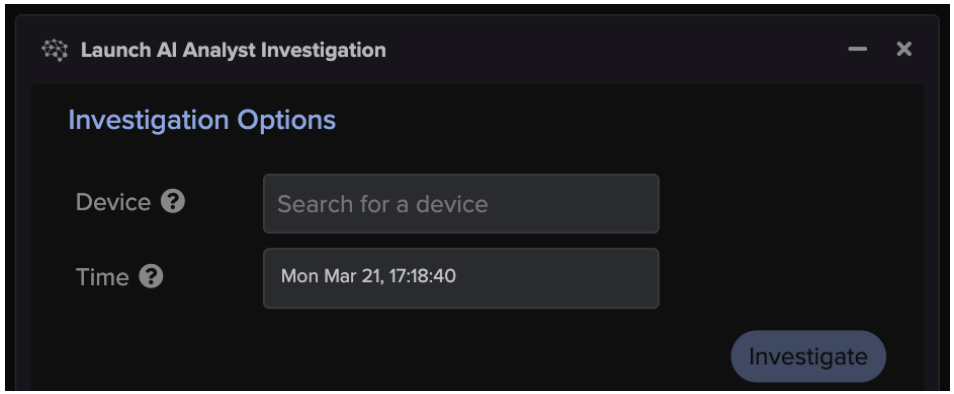
This opens a dialog which prepopulates the **device** name and **time**.



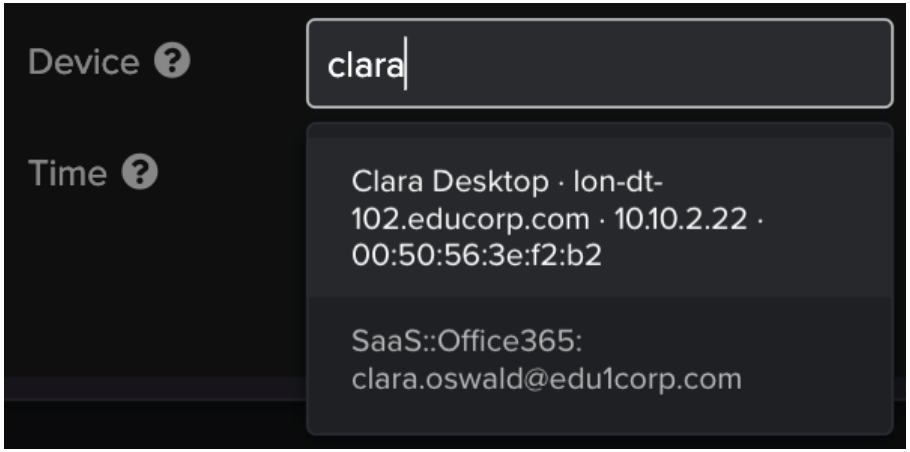
2. Alternatively, open the Threat Visualizer main menu, navigate to the **AI Analyst Investigations** and select **Launch Investigation**.



3. A window will open that allows the user to **input a device/SaaS account** and select a time frame before prompting the investigation.

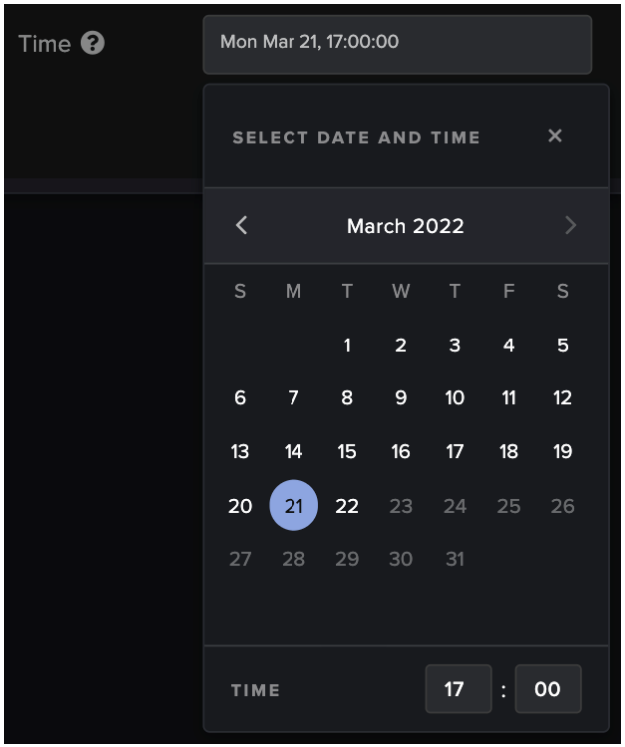


a. First, using a minimum of three characters, start to **input a device/ SaaS user name** into the Search for a device bar to dynamically return results.



b. Next, select a **timeframe** to center the investigation on by clicking on the suggested time.

c. Finally, select **Investigate** to start the analysis.

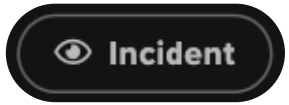


4. The **AI Analyst Investigations** window will automatically open, showing the device, analysis date, user who initiated the analysis and status, as depicted below.

5. AI Analyst will follow a process of Pending, Processing and Finished.

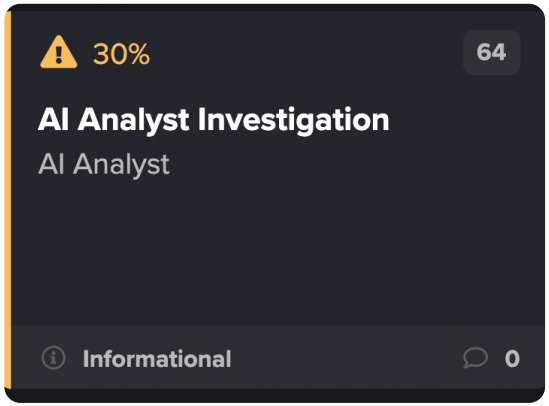
   a. If **no incident is found**, a message will be displayed in the status column.

   b. If an incident is found, a button will appear that allows the user to **open the AI Analyst Incident Log** window.



   The AI Analyst incident can be reviewed as described previously.

   As a result of performing on-demand analysis, a Model Breach will appear in the Threat Tray and the AI Analyst incident.



Top Tip:

The AI Analyst Investigations window can be opened at any time from the main menu → AI Analyst Investigations → View Investigations. This allows existing incidents to be reviewed, and if desired, removed by clicking Delete.

Cyber AI Analyst Chapter Test

This page will test your knowledge and check your understanding of the Cyber AI Analyst section. This is the perfect way to work towards your **Threat Visualizer Essentials Certification**! *Select an answer by clicking on it. Wrong answers are denoted by a red cross and right answers are denoted by a green tick.*

DARKTRACE
Essentials Certification

1. What are the AI Analyst Incident Score Range default slider scores?

- [ ] Between 0% and 100%
- [ ] Between 20% and 100%
- [ ] Between 0% and 80%

2. Which icon will display the AI Analyst Incidents?



3. True or False: the AI Analyst is available in several languages.

- [ ] True
- [ ] False

4. Which action is NOT available from the Incident Log?

- [ ] Acknowledge this Incident
- [ ] Edit the Incident
- [ ] Pin the Incident

5. What does the green color on the Incident Timeline indicate?

- [ ] A critical incident
- [ ] The incident has been cleared
- [ ] A Darktrace RESPOND activity

6. Which icon will open the Attack Phases tab?



Clear All Answers

6. Reporting

Darktrace can provide reports on different aspects of the environment, including Cyber AI Insights and Executive Threat Report. These present insightful professional summaries of the types of incidents and model breaches discovered over a set time period. In this chapter, let's look at the different types of reports and where to download them from once generated.

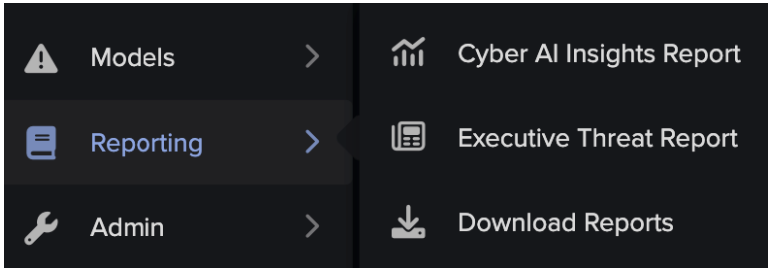
Cyber AI Insights Reports

Cyber AI Insights reports present an overview of coverage, user engagement and value provided by your Darktrace deployment. The report displays currently deployed components, integrations, probes and modules against those generally available.

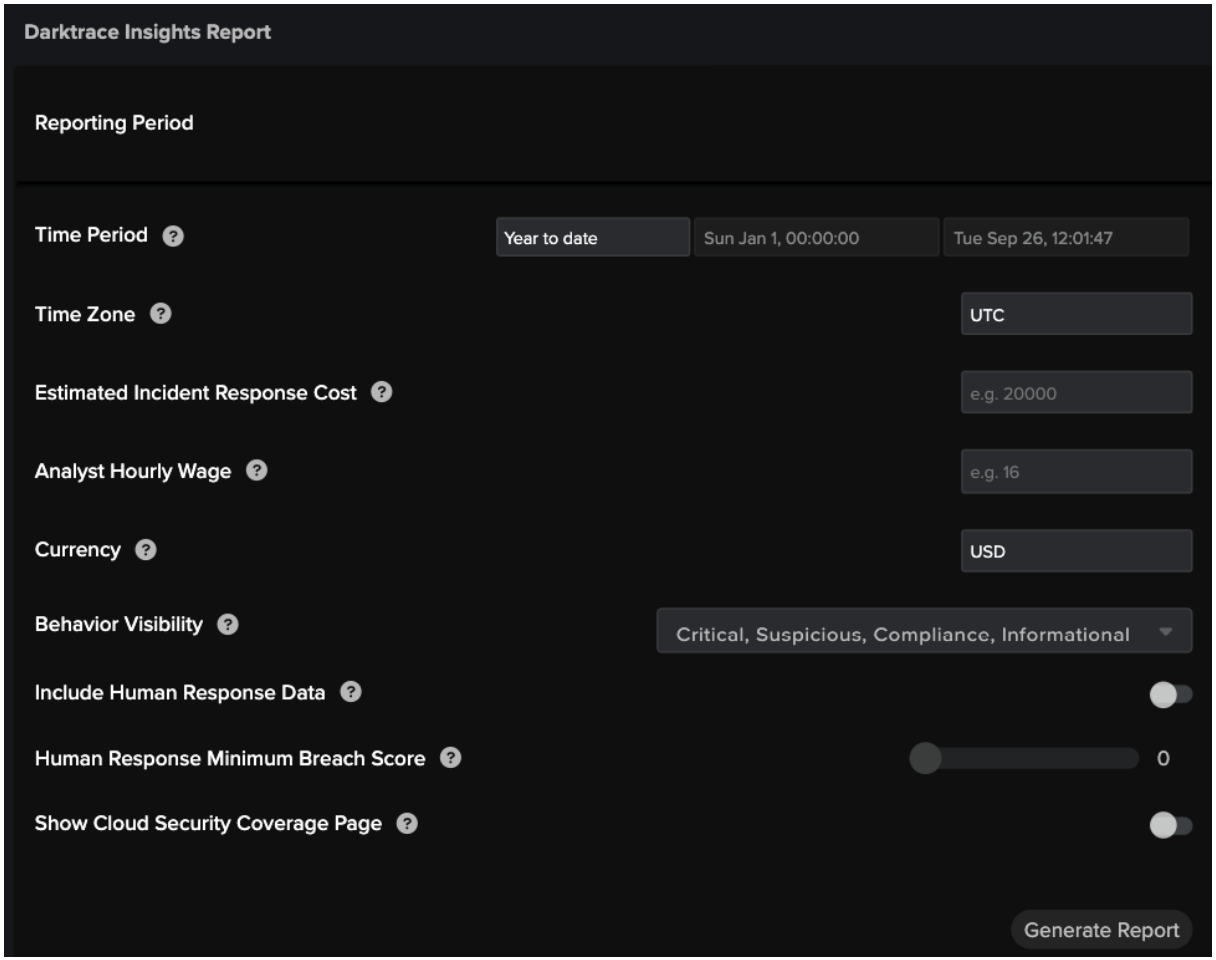
The data contained in each report is specific to your organization and includes trends in processed network traffic, the categories of threat that triggered a Darktrace RESPOND response and a breakdown of events detected by AI Analyst by threat stage. To measure user engagement, the average time-to-acknowledge for human operators is calculated across the timeframe.

Continue your learning with our dedicated video 10: Cyber AI Insights Reports

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



2. This opens the **Darktrace Insights Report** window, as seen on the right, allowing for the generation of a Cyber AI Insights Report.

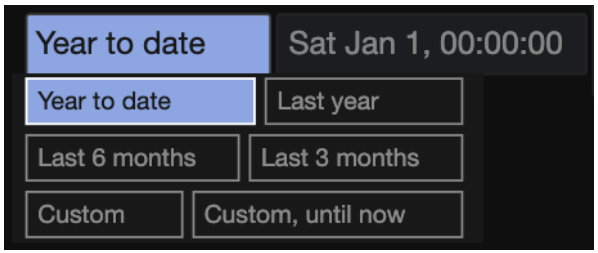


Top Tip:

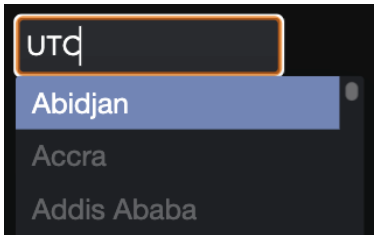
Hover over the tooltip icons beside each field for a short description and any recommendations about whether they should be included in the report.

3. To begin, select the relevant **time frame** for the report.

   a. The **Time Period** can be selected from a pre-set range of dates or can be customized.

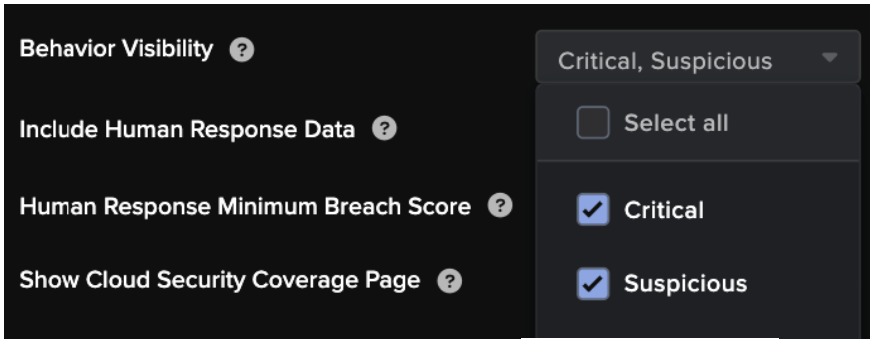


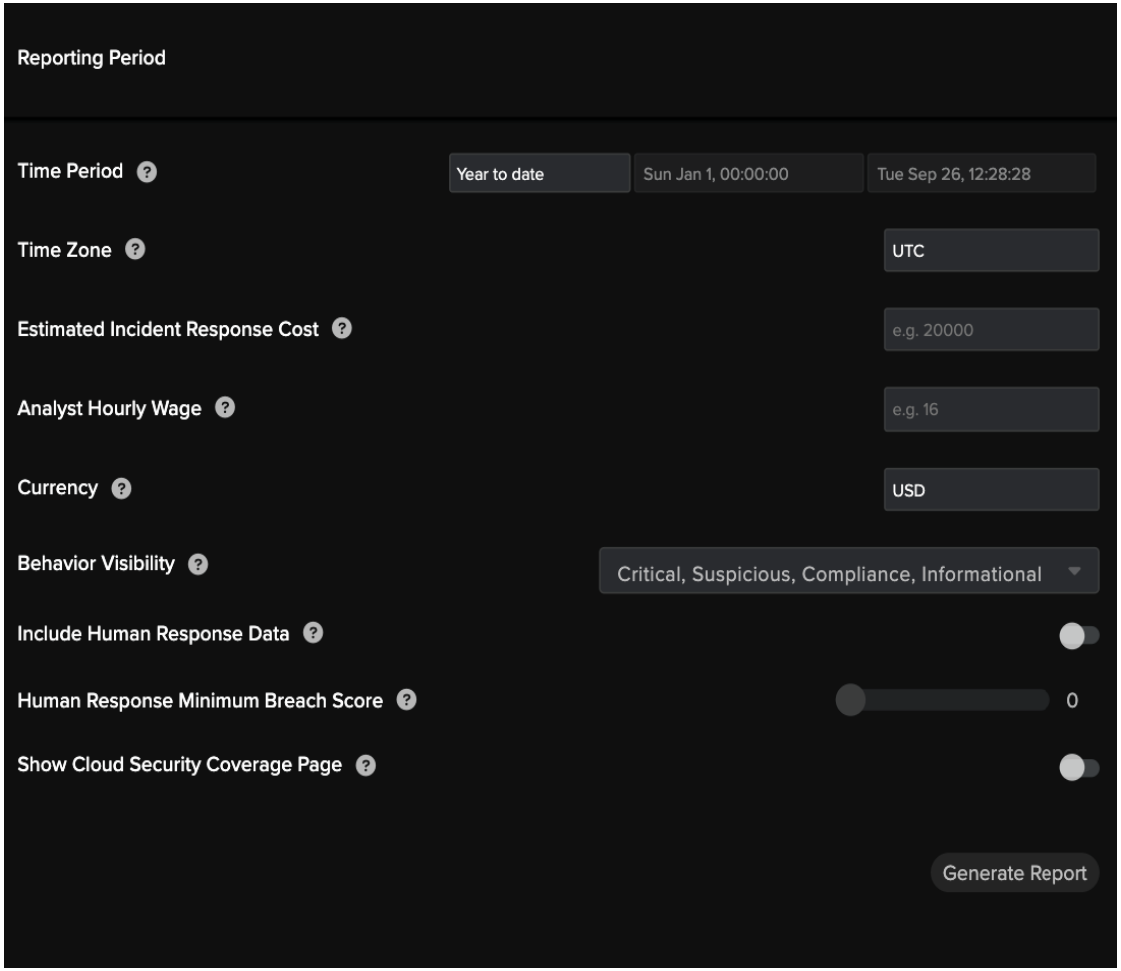
   b. The **Time Zone** will automatically reflect the time zone set by the operator in the top right-hand corner of the interface. This value can be modified by searching the alphabetical list presented when clicking this field.



4. Notice a handful of optional fields: **Estimated Incident Response Cost**, **Analyst Hourly Wage**, **Currency**, **Include Human Response Data** and **Human Response Minimum Breach Score**. Inputting these values will calculate the estimated savings that the AI Analyst has had for the organization over the reporting period.

5. The scope of the report can be modified using the **Behavior Visibility** option. This allows the report to include model breaches from selected behaviors.

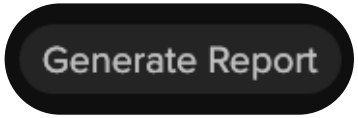




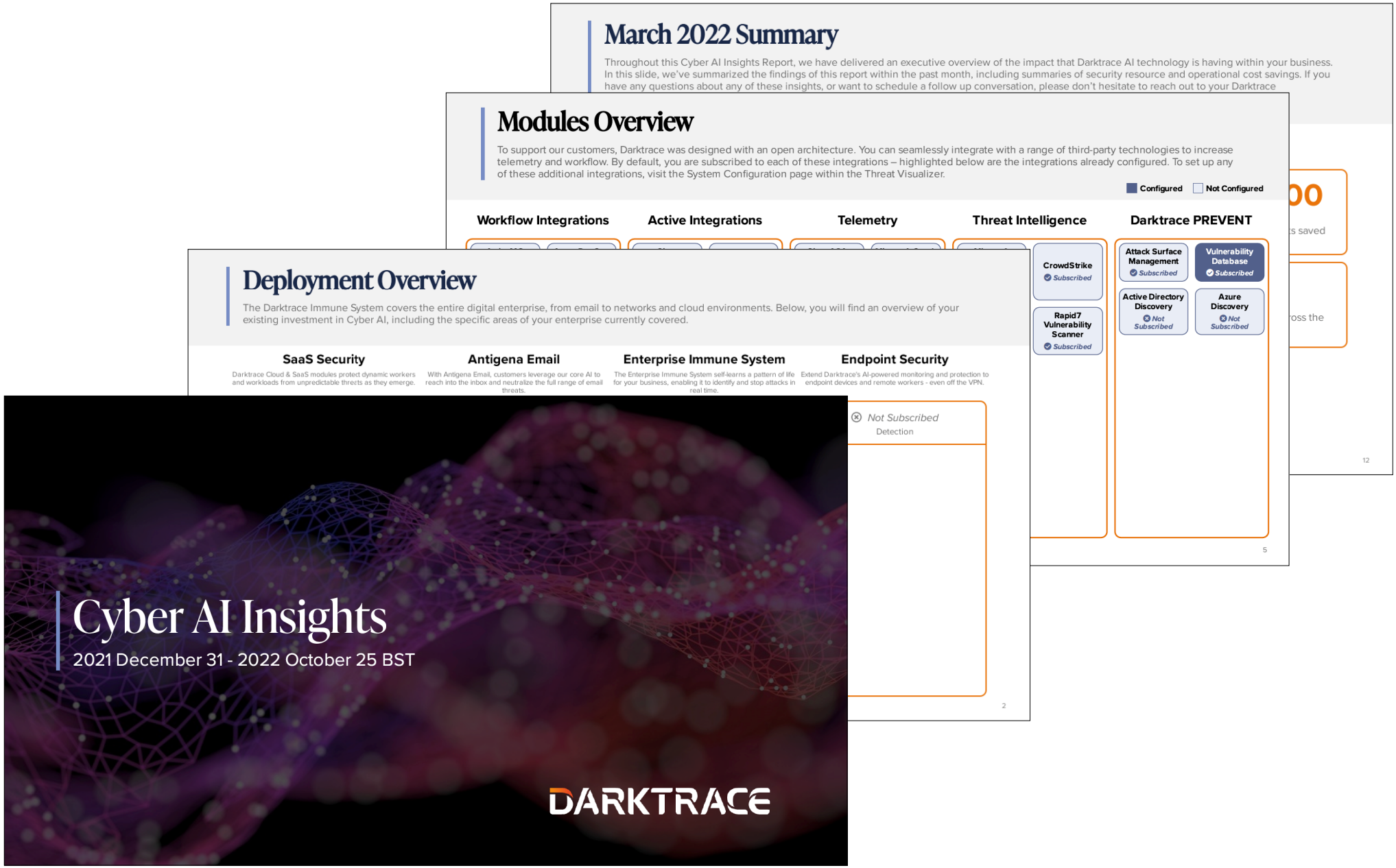
Note: To limit the report to highly anomalous activity, the Critical and Suspicious behaviors are recommended.

6. Finally, select whether or not you wish to enable the option to **Show Cloud Security Coverage Page**.

7. With the fields filled out, click the **Generate Report** button at the bottom of the window.



8. The report can be **previewed** in and **downloaded** from the generation window. It will provide a deployment overview, including cloud security coverage and modules as well as insights into analyst hours saved and Darktrace RESPOND actions taken, if applicable.

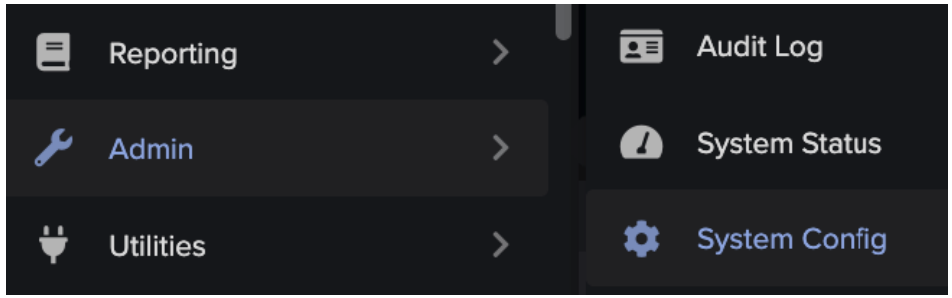


Scheduling Insights Reports

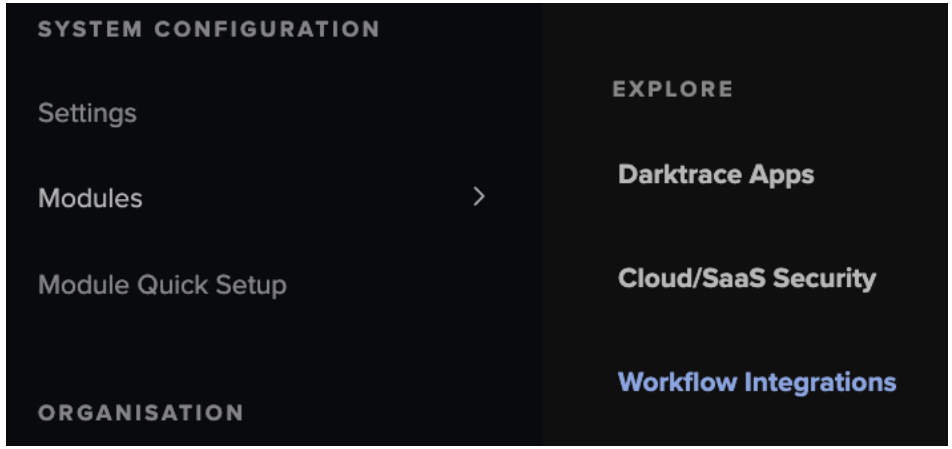
The Cyber AI Insights Report can be scheduled in the System Config page using the Report Scheduler module.

The Report Scheduler Workflow Integration allows Darktrace Cyber AI Insights Reports to be generated automatically and optionally sent to recipients via email.

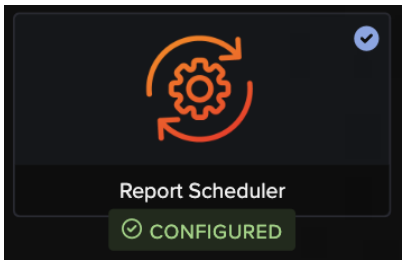
1. Open the Threat Visualizer and navigate to the **System Config** page, under the Admin section of the Main menu.



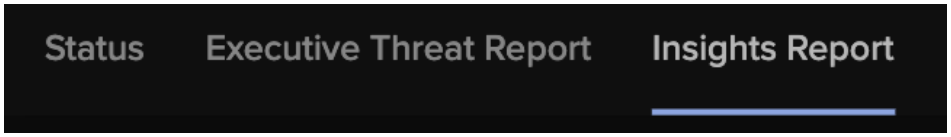
2. From the left-side menu, select **Modules**. Navigate to the **Workflow Integrations** section.



3. From the Workflow Integrations section, choose **Report Scheduler**.



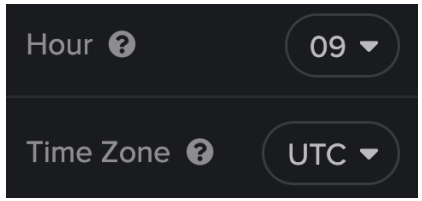
4. Select the **Insights Report** tab.



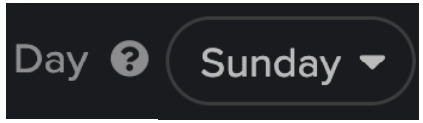
5. Under Configuration for Scheduled Insights Reports, click **New** to define a new recipient config. A new section will appear.

6. From the **Reporting Period** option, choose an interval at which the report should be generated.

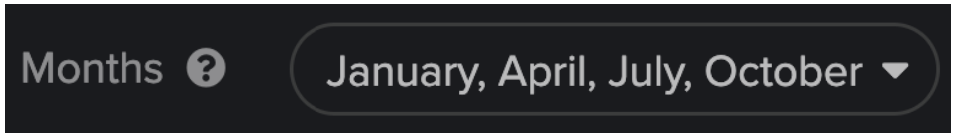
7. Select the **hour of the day** at which the report should be generated, along with the **timezone**.



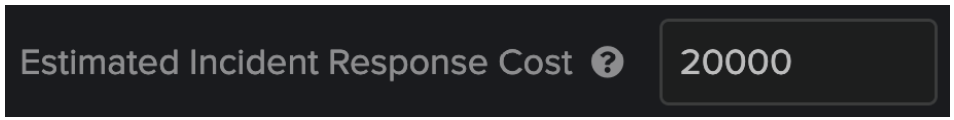
8. For weekly, quarterly and yearly reports, select the **day** on which the report should be generated.



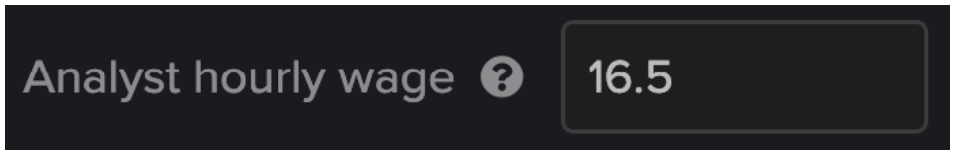
9. For quarterly and yearly reports, select the **month or months** during which the report should be generated.



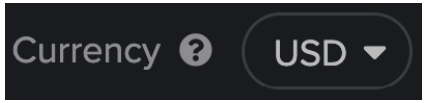
10. To produce an estimate of the savings generated by Darktrace RESPOND, provide the **Estimated Incident Response Cost** in the chosen currency (default USD) of a successful cyber incident to your organization.



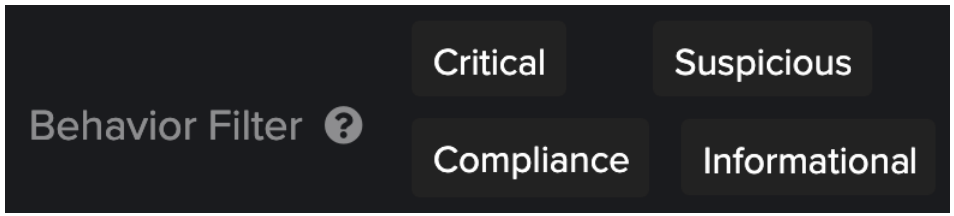
11. To produce an estimate of cost savings created by AI Analyst investigations, provide the expected **Analyst hourly wage** of a cyber analyst in the chosen currency (default USD).



12. Next, select a **currency** for monetary fields.

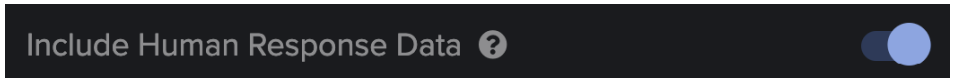


13. **Behavior filter** categories are high level filters that allow an operator to focus in on specific levels of severity or behavior. There are four categories: Critical, Suspicious, Compliance and Informational.



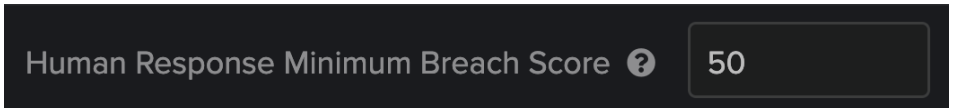
Note: Select the categories to restrict data on the optional "Mean Time to Acknowledgement" page (requires "Include Human Response Data": On).

14. Turn on the **Include Human Response Data** option to include an estimate of how much time it would have taken human analysts to acknowledge a model breach.



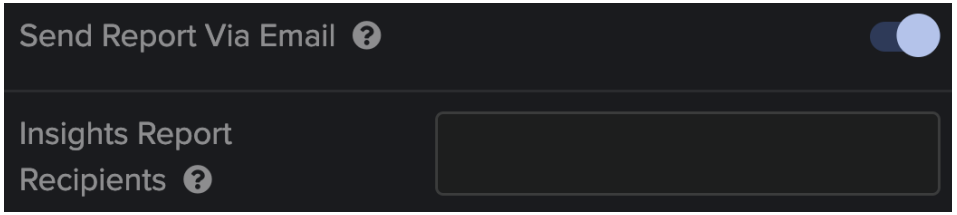
Note: If you do not use breach acknowledgement as part of your workflow, it is advisable not to include this data.

15. For operator acknowledgment statistics on the optional "Mean Time to Acknowledgement" page, set a **Human Response Minimum Breach Score** for response time to be calculated against.



Note: This allows acknowledgement time to be focused on high-level events. Requires "Include Human Response Data": On.

16. If the report should be automatically emailed to recipients, turn **Send Report Via Email** On and specify a minimum of one **Insights Report Recipient**.



Note: A configured email server is required to send reports via email.

17. Finally, review your changes before clicking **Add**, and observe a confirmation message.

Executive Threat Reports

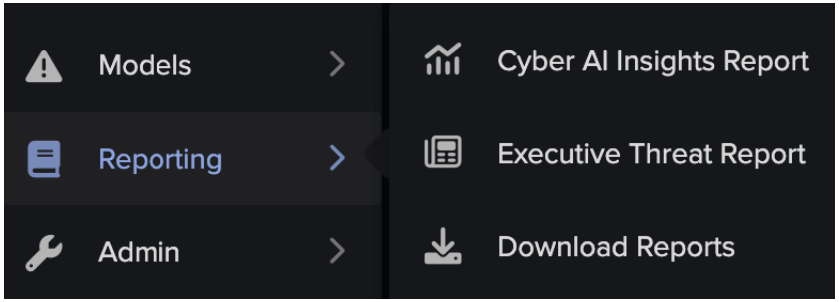
Executive Threat Reports present a simple visual overview of model breaches and activity in the network environment.

The report is separated into a graphical representations of network traffic, model breaches and Darktrace RESPOND response, and an optional detailed breakdown more suitable for advanced audiences.

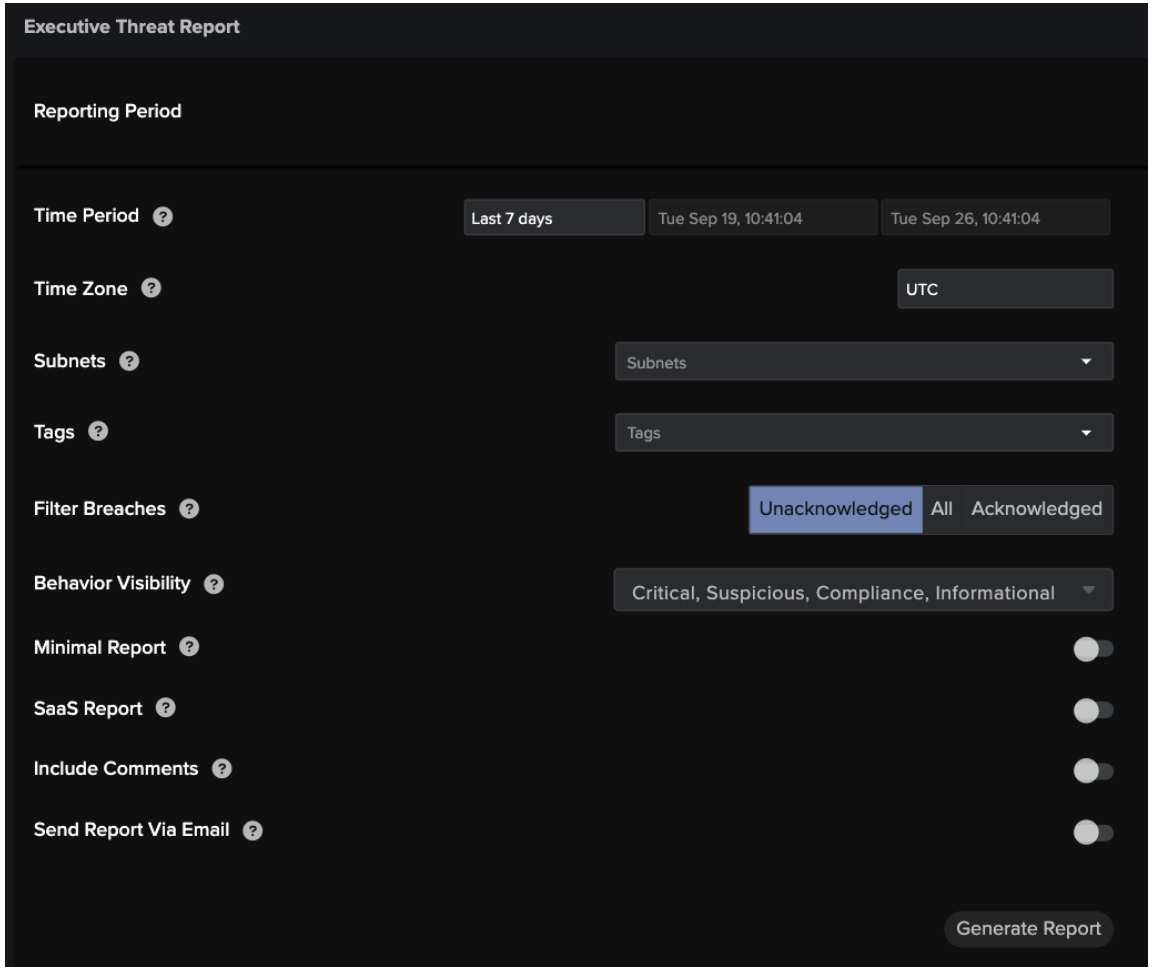
Reports can be customized to include extra details or restricted to high level information.

Continue your learning with our dedicated video 11: Executive Threat Reports

1. From the **Reporting** menu, click **Executive Threat Report**.



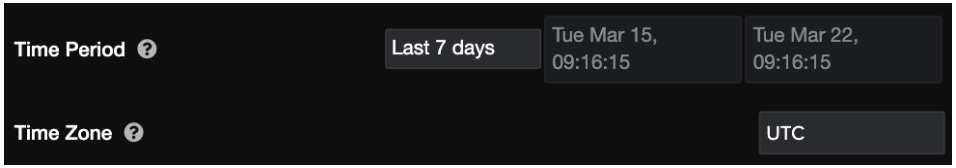
2. This opens a new **Executive Threat Report window,** as seen on the right, where fields can be toggled and reports can be generated.



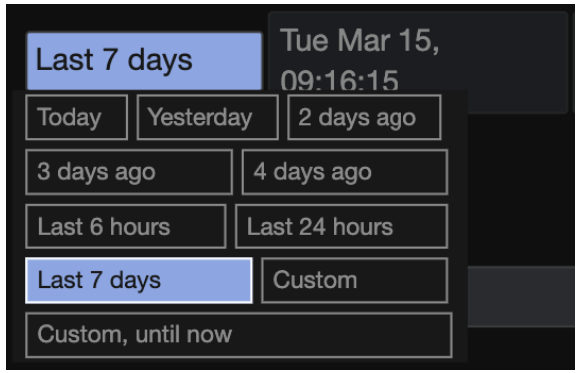
Top Tip:

Hover over the tooltip icons beside each field for a short description and any recommendations about whether they should be included in the report.

3. To begin, select the relevant **time frame** for the report.

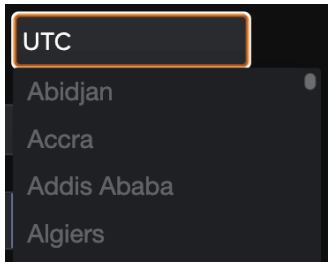


a. The **Time Period** can be selected from a pre-set range of dates or can be tailored using the custom options.

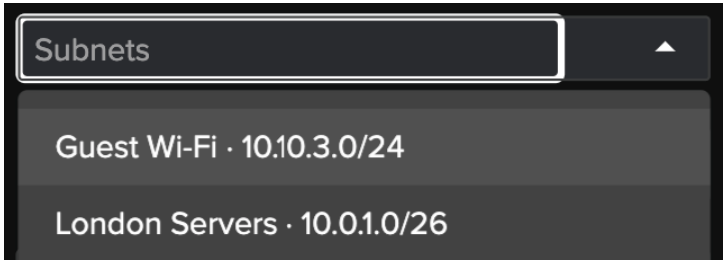


Note: Any custom time period longer than the last 7 days will not allow the Filter Breaches or Include Comments toggles to be changed.

b. As mentioned previously, the **Time Zone** will automatically reflect the time zone set in the time selector. This value can be modified for the report by searching the alphabetical list presented when clicking this field.

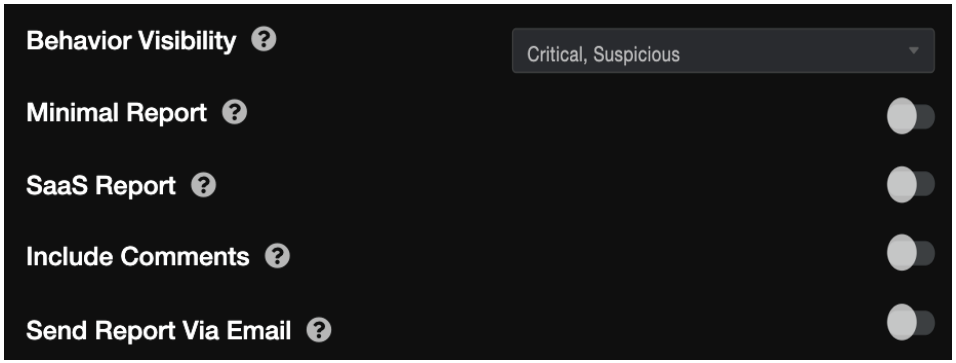


4. Click the **Subnets** drop-down to select an existing subnet range to limit the report's scope.



5. Next, decide what kind of breaches to include using the **Filter Breaches** row.

6. Notice the selection of toggles which can be used to **customize the contents** of the report.



a. The scope of the report can be modified using the **Behavior Visibility** option which allows the report to include Critical, Suspicious, Compliance, Informational, or a combination of these behaviors to be highlighted. Critical and Suspicious are the defaults.

b. It may be helpful to enable **Minimal Report** to remove the connection details and Appendix in order to reduce the size of the report.

c. To include only SaaS device type breaches, enable the toggle for **SaaS Report**.

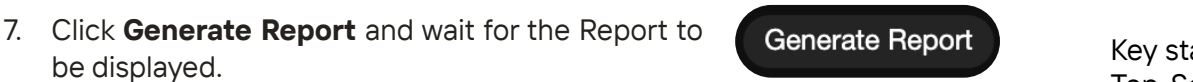
Note: Enabling this toggle will switch off the Subnets drop-down and display all SaaS events.

d. If many breaches have been commented on, discussion can be included by switching the **Include Comments** toggle on.

Note: This toggle can only be used on reports which cover the last 7 days.

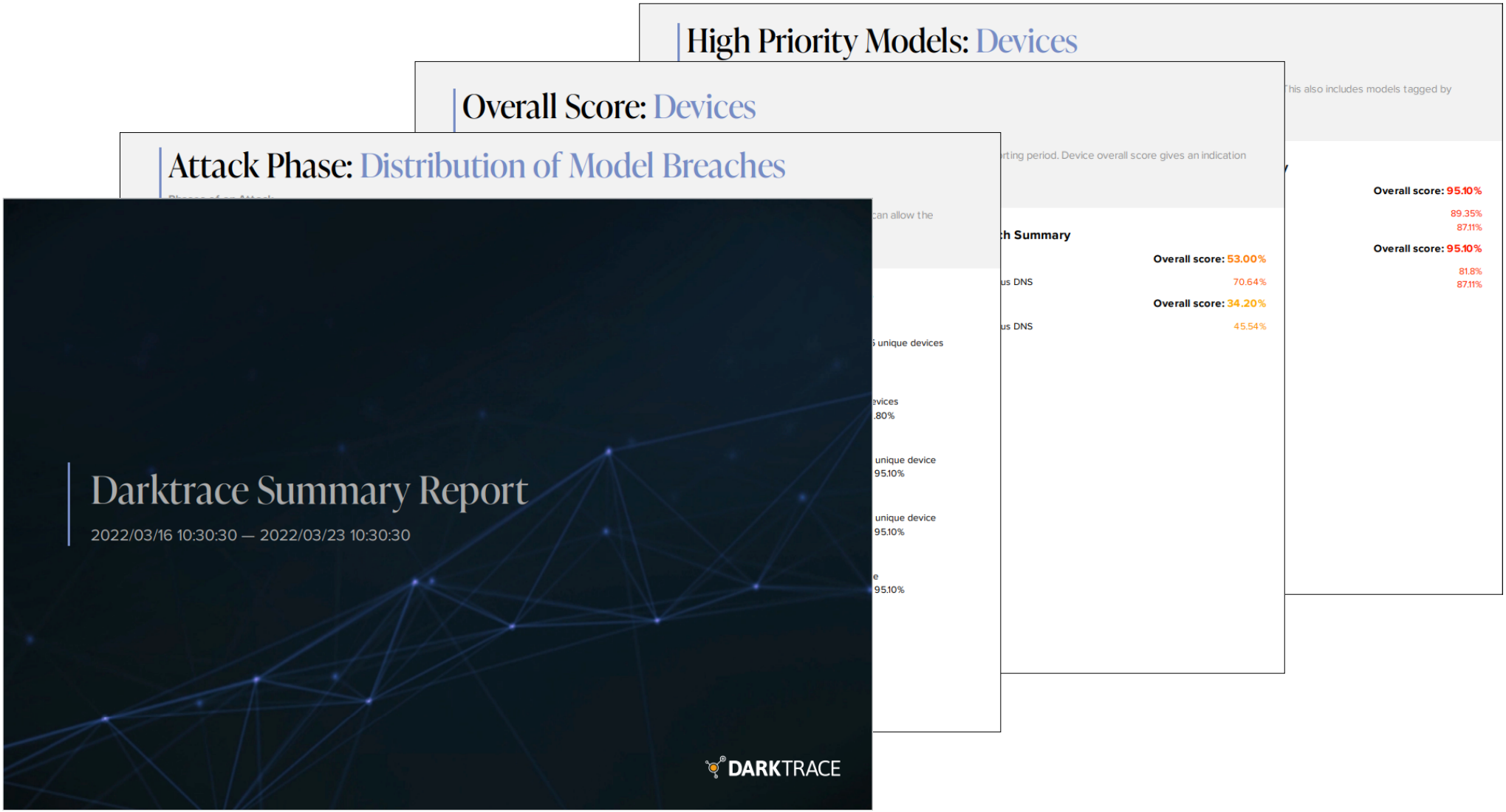
e. If the report is to be emailed to addresses defined in the System Config page, enabling **Send Report Via Email** will do so.

7. Click **Generate Report** and wait for the Report to be displayed.



8. The report will open as a **preview** in the Executive Threat Report window. It can be opened as a pdf in a new browser tab by downloading it. Review the report to understand the full range of statistics covered.

Key statistics across a range of categories are presented: Attack Phases, Top Scoring Devices, High Priority Models and a Distribution of Model Breaches are just some examples of what's contained.

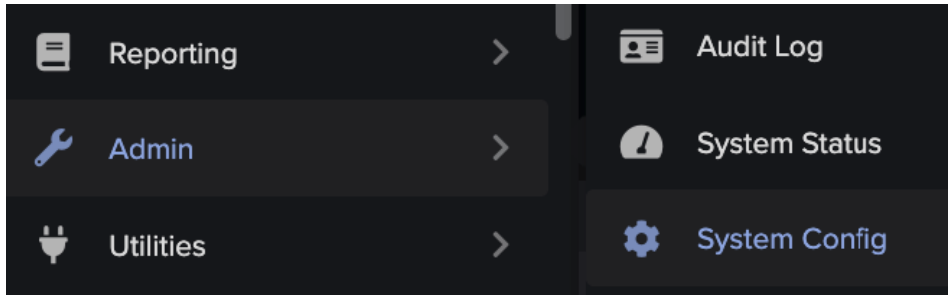


Scheduling Executive Threat Reports

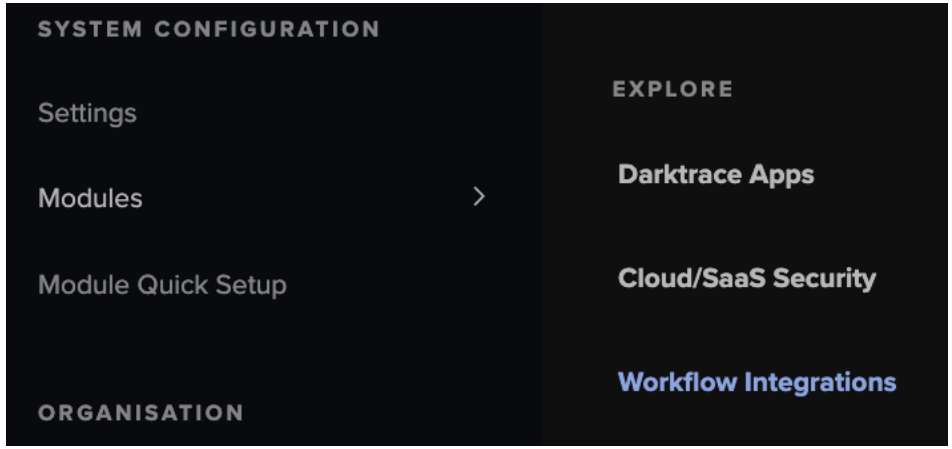
The Executive Threat Report can be scheduled in the System Config page using the Report Scheduler module.

The Report Scheduler Workflow Integration allows Darktrace Executive Threat Reports to be generated automatically and optionally sent to recipients via email.

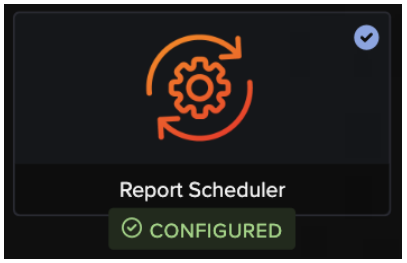
1. Open the Threat Visualizer and navigate to the **System Config** page, under the Admin section of the Main menu.



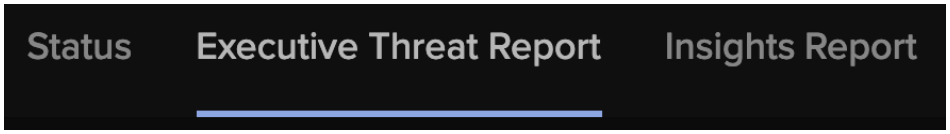
2. From the left-side menu, select **Modules**. Navigate to the **Workflow Integrations** section.



3. From the Workflow Integrations section, choose **Report Scheduler**.



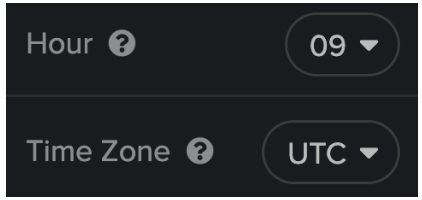
4. Select the **Executive Threat Report** tab.



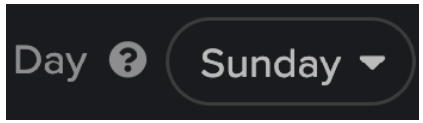
5. Under Configuration for Scheduled Executive Threat Reports, click **New** to define a new recipient config. A new section will appear.

6. From the **Reporting Period** option, choose an interval at which the report should be generated.

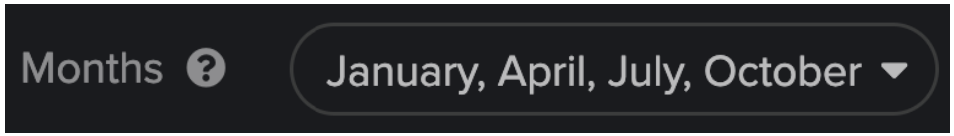
7. Select the **hour of the day** at which the report should be generated, along with the **timezone**.



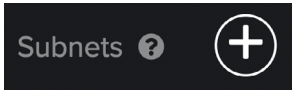
8. For weekly, quarterly and yearly reports, select the **day** on which the report should be generated.



9. For quarterly and yearly reports, select the **month or months** during which the report should be generated.

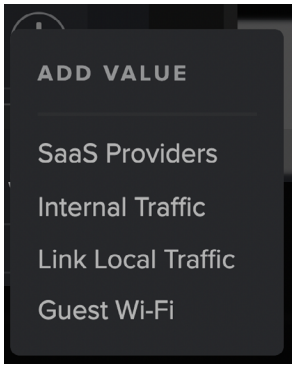


10. Reports can be generated for a single subnet, or for multiple **Subnets**.



Executive Threat Reports generated manually by users respect their data visibility; reports generated automatically are generated with full data visibility.

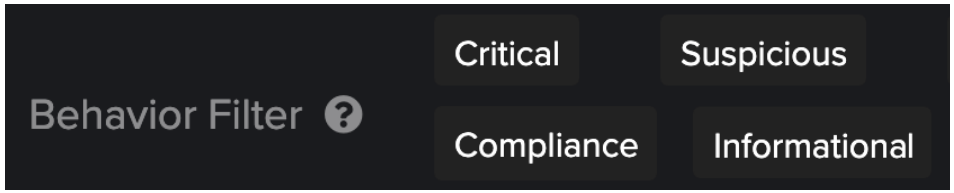
By default, all subnets are included. Multiple entries can be selected from the dropdown menu with the plus icon.



Note: Enabling SaaS Report will clear this field.

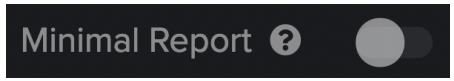
11. The **Filter Breaches** option alters the report to include only unacknowledged model breaches (default), only acknowledged breaches or both acknowledged and unacknowledged.

12. **Behavior filter** categories are high level filters that allow an operator to focus in on specific levels of severity or behavior. There are four categories: Critical, Suspicious, Compliance and Informational.

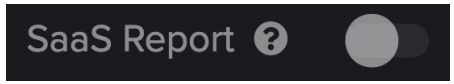


Note: Select the categories to restrict included Model Breaches to only those that match the category filter.

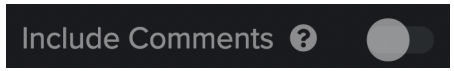
13. If the **Minimal Report** option is On, it will generate only high level summary pages, excluding the detailed appendix.



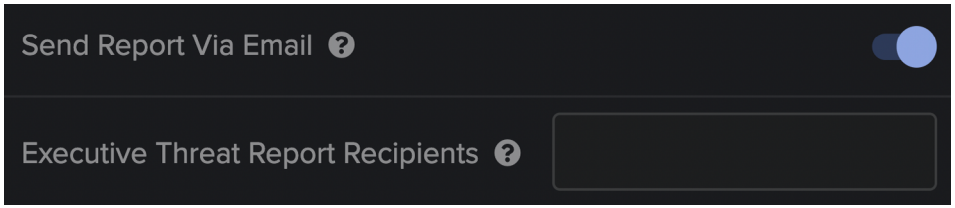
14. Restricts the content of the report to only SaaS user devices and SaaS breaches by toggling the **SaaS Report** option. The Antigena page is also restricted to Antigena SaaS only.



15. The **Include Comments** option will include any comments made by users or analysts in the detailed appendix.



16. If the report should be automatically emailed to recipients, turn **Send Report Via Email** On and specify a minimum of one **Executive Threat Report Recipient**.

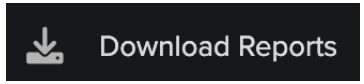


Note: A configured email server is required to send reports via email.

17. Finally, review your changes before clicking **Add**, and observe a confirmation message.

Download Reports

1. Generated reports are automatically saved. In the Threat Visualizer Menu under Reporting, select **Download Reports**.



   a. When in the appropriate tab, reports can be **searched**. This can be particularly useful if trying to locate a report from a date range.

   b. Click the **Download** button to save the file locally.

   c. Reports can be removed from this page by utilizing the **Delete** button.

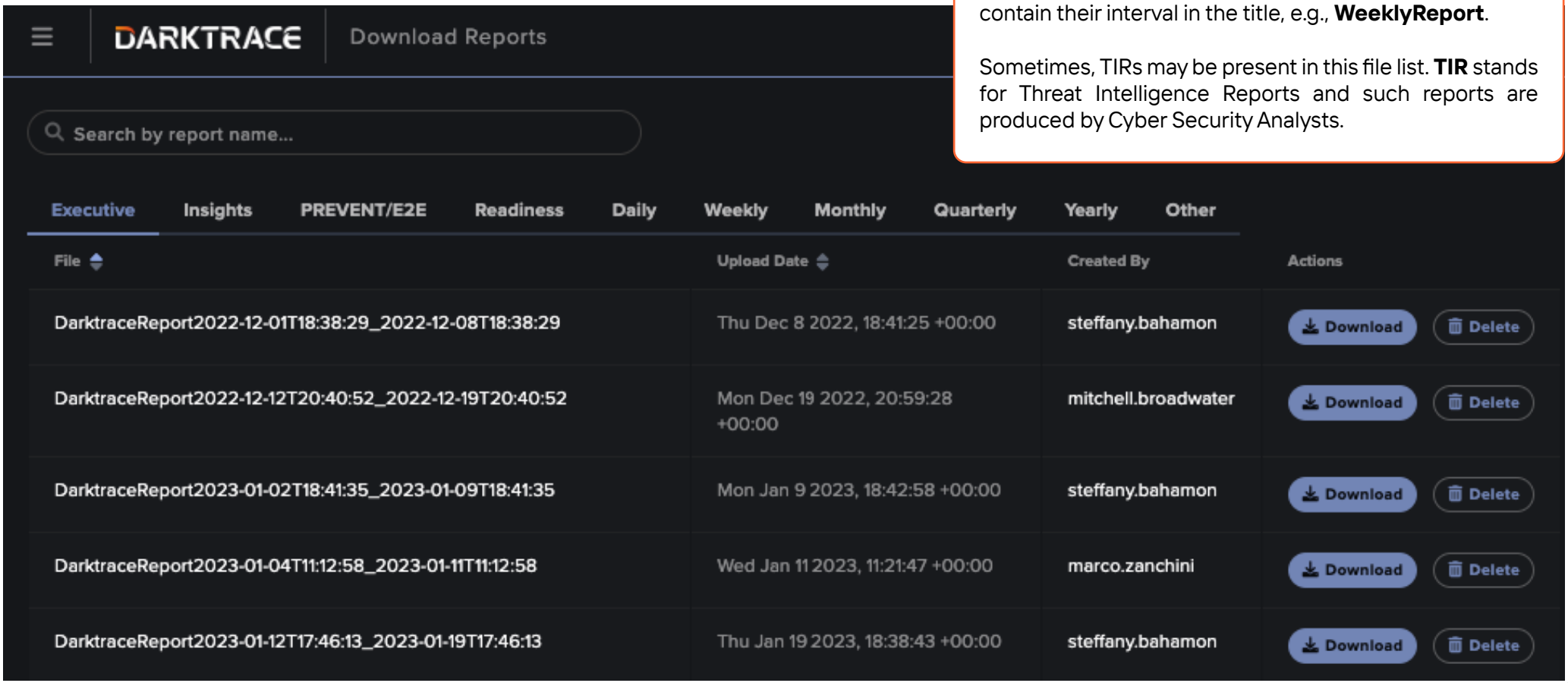
Report Types

The Cyber Analyst Insights Reports are stored under the Insights heading and can be easily distinguished as they contain **DarktraceInsights** in the title.

The Executive Threat Report which have been generated can be found in the Manual list. Such files begin with **DarktraceReport**.

Other reports which are automatically generated using selected time periods are easily recognizable as they contain their interval in the title, e.g., **WeeklyReport**.

Sometimes, TIRs may be present in this file list. **TIR** stands for Threat Intelligence Reports and such reports are produced by Cyber Security Analysts.



Reporting Chapter Test

This page will test your knowledge and check your understanding of the Reporting section. This is the perfect way to work towards your **Threat Visualizer Essentials Certification**! *Select an answer by clicking on it. Wrong answers are denoted by a red cross and right answers are denoted by a green tick.*

DARKTRACE
Essentials Certification

1. Where can Cyber AI Insights Reports be scheduled from?

- [ ] Executive Threat Report page
- [ ] Cyber AI Insights Report page
- [ ] System Config page

2. Which Behaviour Visibility option has the highest severity level?

- [ ] Critical
- [ ] Suspicious
- [ ] Informational

3. True or False: Executive Threat Reports CANNOT be scheduled.

- [ ] True
- [ ] False

4. If enabled, what does the Minimal Report option do?

- [ ] Exclude Comments
- [ ] Exclude Connection Details
- [ ] Exclude SaaS device type breaches

5. In Download, which header corresponds to Cyber Analyst Insights Reports?

- [ ] Cyber
- [ ] Analyst
- [ ] Insights

6. What is a use of Cyber AI Insights Reports?

- [ ] To confirm your configured Modules
- [ ] To check Model Breach Analytics
- [ ] To review an Audit Log

Clear All Answers

7. Learning Outcomes

Course Agenda Checklist

Continue your learning with our dedicated video 12: Course Summary

Thank you for completing this course on Threat Visualizer Part 1 - Familarization. We hope this have given you the confidence to tackle a variety of aspects within your deployment.

To learn about some of the more advanced Threat Visualizer concepts, we recommend the Threat Visualizer Part 2 - Investigation course.

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.

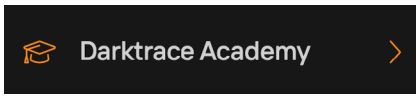
Complete the learning outcomes checklist:

- **Understand Darktrace Solutions** ☐
- **Navigate the Threat Visualizer Interface** ☐
- **Obtain basic information about network devices** ☐
- **Investigate Cyber AI Analyst Incidents** ☐
- **Generate reports of network activity** ☐

8. Additional Educational Materials

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 PREVENT/ASM	All end users
Darktrace PREVENT/E2E	All end users
Threat Visualizer Part 1 - Familiarization	All end users
Threat Visualizer Part 2 - Investigation	All end users
Darktrace HEAL	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 RESPOND/Network	Administrators and Analysts
Darktrace/Email Part 1 - Familiarization	Email Administrators and Analysts
Darktrace/Email Part 2 - Customization	Email Administrators
Darktrace/Apps	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.