DARKTRACE ACADEMY

THREAT VISUALIZER PART 2 - INVESTIGATION

Training Manual

Threat Visualizer Part 2 - Investigation

Training Manual
v3.4.1
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, Threat Visualizer Part 2 - Investigation, builds on the foundational elements of the Threat Visualizer, allowing you to dive deeper into Model Breaches. It is designed for a range of Cyber Security professionals including IT Security Managers, Architects and Analysts. The following document serves as an educational guide for the key investigative elements of the 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, 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:

- **Use the Threat Visualizer to follow an Analyst workflow**
- **Review individual Model Breaches**
- **Perform basic queries in Advanced Search**
- **Create packet captures and perform packet inspection**

2. Analyst Workflow

The Threat Visualizer comes with a large selection of pre-built models to automatically search, detect, and alert you to anomalous behavior in the network. Any change to a network, such as a new device being located, or a device connecting to an external host at an unusual time of day, could be viewed with suspicion. The Threat Visualizer will identify and classify these potential events to prioritize and facilitate quick analysis. In this chapter, let's explore the ways in which you can select and review Model Breaches and use a combination of interfaces to dive deeper into events of interest.

2. Analyst Workflow

The Darktrace interface firstly alerts you to anomalies and then provides you with the means to work out whether these are legitimate behaviors that you find acceptable in your environment, or genuinely malicious activity.

It is important to understand what Darktrace has highlighted. If it's an AI Analyst Incident, it has already pulled together lots of relevant information in an easy-to-read format. However, Model Breaches in the Threat Tray may also be interesting starting points for deep-dive investigations.

Upon reviewing an incident or breach, there are a number of questions you may ask yourself:

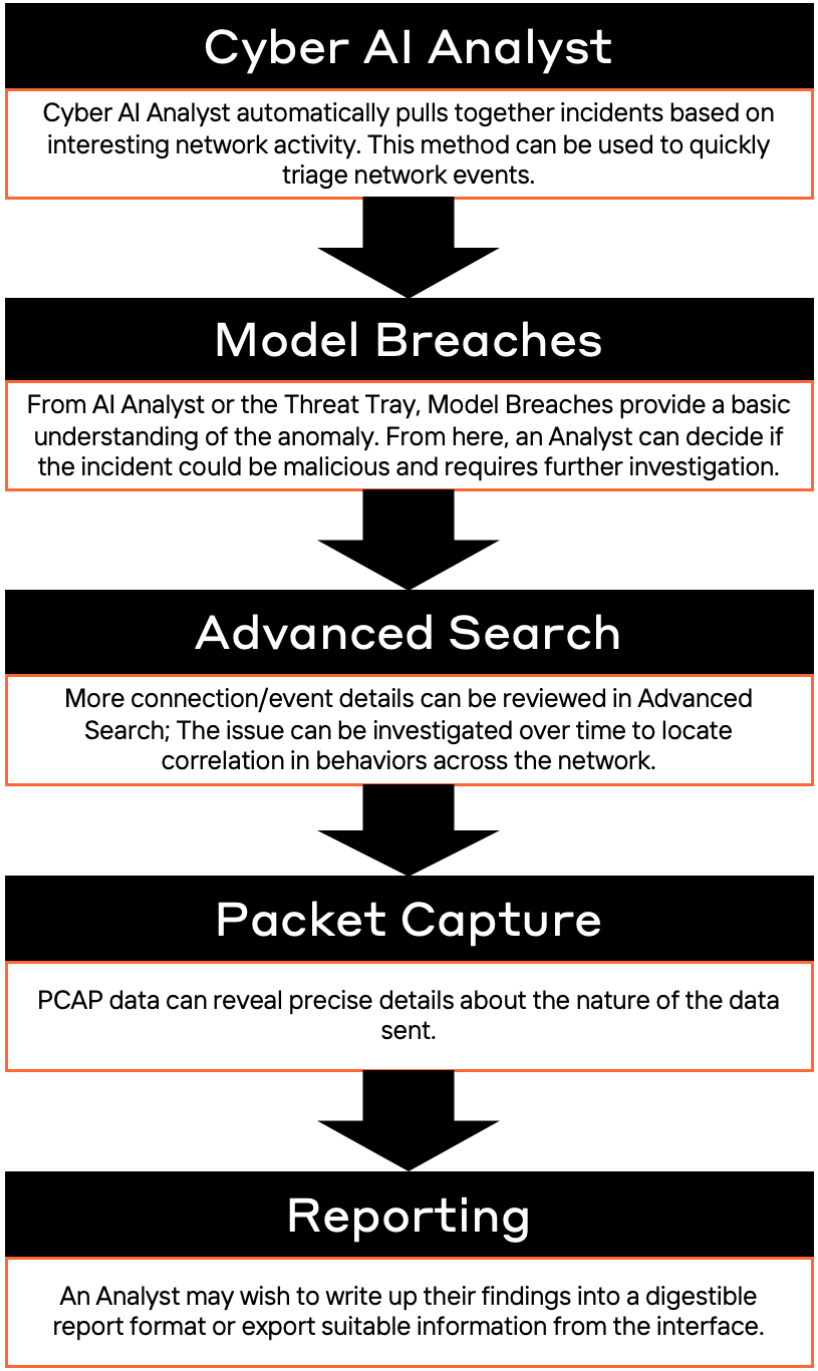
- Why are you being alerted to this activity?
- Is this behavior anomalous?
- Could there be a legitimate reason for this activity?

Darktrace enables you to use the platform in a variety of ways. However, there is no fixed recipe for how to investigate potential threats using the platform. Investigation of different types of model breaches will require different approaches. An example approach can be seen in the diagram to the right. This walks through different interfaces and features that will be covered in this investigation course.

Knowing your environment will assist a great deal in readily recognizing legitimate or expected behavior. Having an understanding of devices and company policies may allow you to quickly eliminate potential risks highlighted by Darktrace. It may also be advisable to note these models to the administrator in your organization for possible tuning.

If legitimacy is not readily apparent through the information presented in the model breach, it may be advisable to contact the end user (or the user associated with the suspect device). If the suspect device is a server, the data or application owner would be the point of contact to verify legitimacy.

While the origins of your investigations are in Darktrace, consultation and collaboration with teammates, colleagues, and end users may be advisable. Additionally, analysis of the data produced by the other tools in your security stack can lead to more complete analysis and provide context to the data being seen in Darktrace.



Example Analyst Workflow

An example of a possible analyst workflow might follow this pattern:

1. In the Threat Tray, increase the **Threat Score Range Slider** to include a manageable number of incidents or model breaches and focus on the most important. The default of 60% is a good starting point.

2. Based on your knowledge of the business and network setup, examine the **most significant breache**s. For example, a 'beaconing' model breach may indicate a malware infection or 'unusual data transfer' could indicate data exfiltration.

3. For each incident or breach, review the offending device(s) in the Threat Visualizer device view and set the correct time of the event. Start with the **Device Summary**, and check if it breached any other Models.

4. Within **Similar Devices** in the Device Summary page, check whether similar devices are behaving in a similar way.

5. Examine the **Model Breach Event Log** and events that contributed to the incident or breach.

6. It can be useful to check the historical activity of the device using any of the aforementioned features or by exploring the device using different visualization methods. Does it have **related anomalies** at the time or in the **last 7 days**?

7. Review what else the device was doing at the time in the **Device Event Log**. In conjunction with the Event Log, open a device's graph and try adding relevant metrics to it to gain a better understanding the device's behavior. Using information obtained from the device, investigate why Darktrace has provided a high score for a threat.

8. Review the event and device within **Advanced Search**. Has any other device contacted a particular domain or IP address that occurs in the breach?

9. Use third party resources for **open-source** context regarding a suspicious domain or file (e.g., WhoIs, Virustotal, Google search or malware research organizations).

10. For more detailed analysis, examine a **raw packet capture file**, for example to investigate content passed over HTTP or to inspect communications involving atypical protocols.

11. Once thoroughly investigated and a decision is made, a **report** can be generated to be shared with the appropriate people.

Common Ports and Protocols

When reviewing AI Analyst incidents, Breach Logs and Event Logs, it may be helpful to refer to the following **key ports**, tabulated to the right.

For researching other ports and their common uses, websites such as **Speed Guide** can be useful.

Input a port number into the following URL structure to search the database:

https://www.speedguide.net/port.php?port={INSERT PORT NUMBER}

PORT	PROTOCOL	ACRONYM	NAME
20/21	TCP	FTP	File Transfer Protocol
22	TCP/UDP	SSH	Secure Shell
23	TCP/UDP	Telnet	Telnet Port
25	TCP/UDP	SMTP	Simple Mail Transfer Protocol for sending outgoing emails
53	TCP/UDP	DNS	DNS Server (DNS lookup uses UDP and Zone transfers use TCP)
67/68	UDP	DHCP	Dynamic Host Configuration Protocol
80	TCP	HTTP	World Wide Web HTTP
110	TCP	POP3	Post Office Protocol (for receiving email)
123	UDP	NTP	Network Time Protocol
137/138/139	UDP/TCP	NetBIOS	NetBIOS
143	TCP/UDP	IMAP4	IMAP4 Protocol (for email service)
161/162	TCP/UDP	SNMP	Simple Network Management Protocol
389	TCP/UDP	LDAP	Lightweight Directory Access Protocol
443	TCP	HTTPS	Secure HTTP over SSL
445	TCP	SMB	Server Message Block Protocol for network file sharing
514	UDP	Syslog	Syslog
993	TCP	IMAP over SSL	Secure IMAP protocol over SSL (for emails)
1433	TCP/UDP	SQL	Microsoft SQL server port
3306	TCP/UDP	MySQL	MySQL/MariaDB Database Server
7680	TCP	WUDO	Windows 10 peer-to-peer update distribution

Workflow Chapter Test

DARKTRACE
Essentials Certification

This page will test your knowledge and check your understanding of the Analyst Workflow 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.*

1. What is the default Threat Score Range Slider starting point?

- [ ] 50%
- [ ] 60%
- [ ] 70%

2. What type of breaches would you start with when reviewing the day?

- [ ] The one with the highest number of breaches
- [ ] The most recent one
- [ ] The most significant one

3. True or False: a report can be exported and shared with anyone.

- [ ] True
- [ ] False

4. How can you review what a device was doing at a specific time?

- [ ] By using third-party resources
- [ ] By checking the Device Event Log
- [ ] By examining the Model Breach Event Log

5. Which protocol uses port 123?

- [ ] File Transfer Protocol
- [ ] Lightweight Directory Access Protocol
- [ ] Network Time Protocol

6. Which port number is the Simple Mail Transfer Protocol using?

- [ ] 22
- [ ] 23
- [ ] 25

Clear All Answers

3. Model Breaches

Model Breaches can form part of an AI Analyst incident, or can be a standalone alert, informing Threat Visualizer users to the anomalous behavior of a device or account. In order to inspect Model Breaches, they must first be selected using an appropriate method. Once selected, a plethora of information can be obtained. In this chapter, we will locate a Model Breach of interest, use its breach log to understand it and also consult external sources before moving onto deep-dive analysis using Advanced Search and Packet Captures.

Selecting a Model Breach

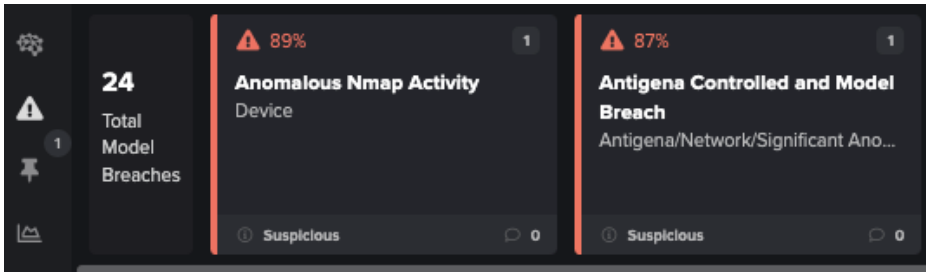
Continue your learning with our dedicated video: 2: Model Breach Filter Options

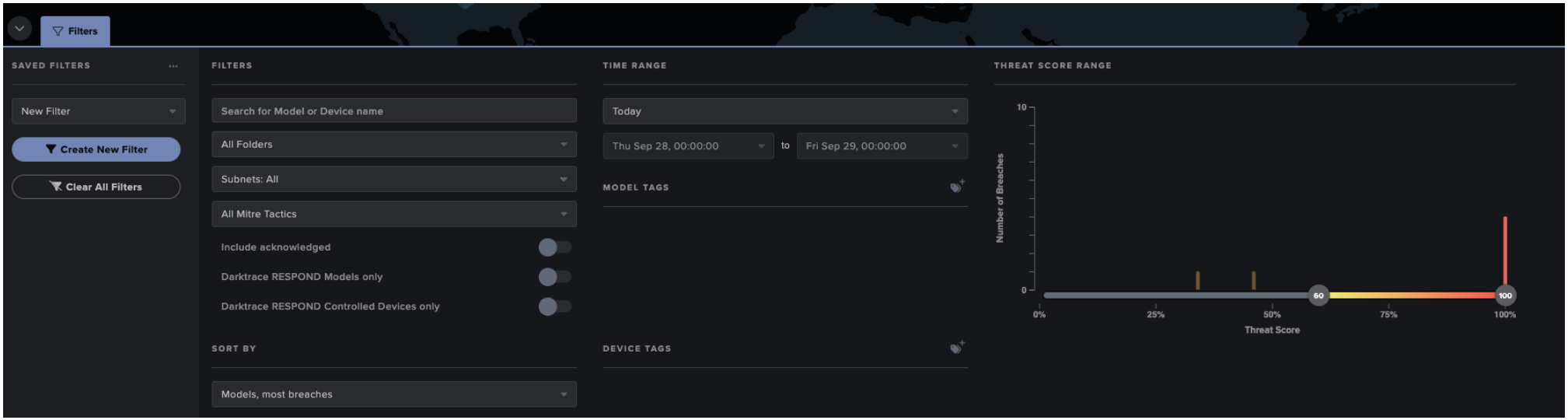
Generally, Model Breaches can be opened from an AI Analyst incident. Here, relevant information about a threat has already been pulled together, meaning individual breaches can be investigated as part of the deep-dive analysis process. However, Model Breaches can also be opened directly from the Threat Tray. The default view is AI Analyst, but by using the icons on the left, this view can be changed to view all Model Breaches.

1. First of all, change the Threat Tray from AI Analyst view (brain icon) to the **Model Breaches (warning triangle)** view.

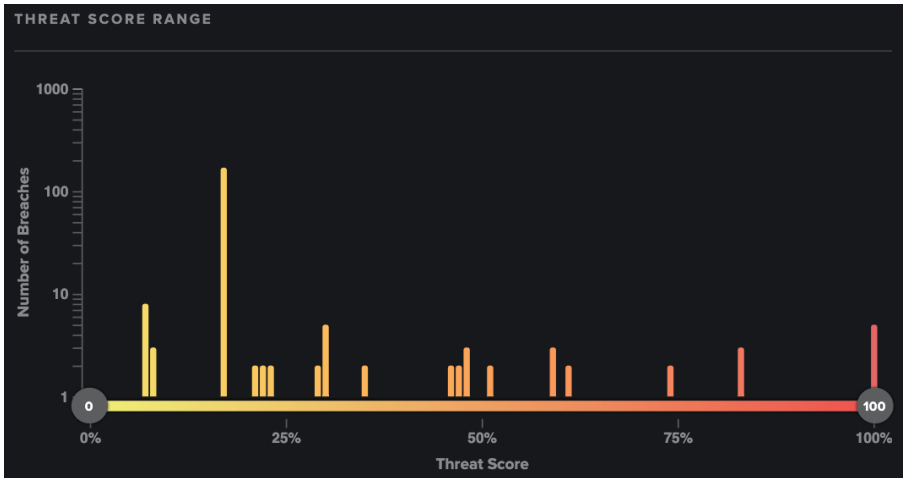
2. Before reviewing the Model Breaches, it can be useful to restrict the results to a manageable number using the **filter** options. As a good starting point, a time range of the **Last 7 days** and the default Threat Score range between **60%-100%** will reveal high scoring breaches over a weekly time frame.

   The default Threat Score Range facilitates concentrating on the most relevant breaches. Other threats are still available, just temporarily hidden from view. The right-hand slider represents the maximum threat score. In practice, it can be helpful to prioritize and focus of the most severe threats.





a. Increasing the **Threat Score** range to include lower scoring alerts can display more breaches in the right portion of the Threat Tray.

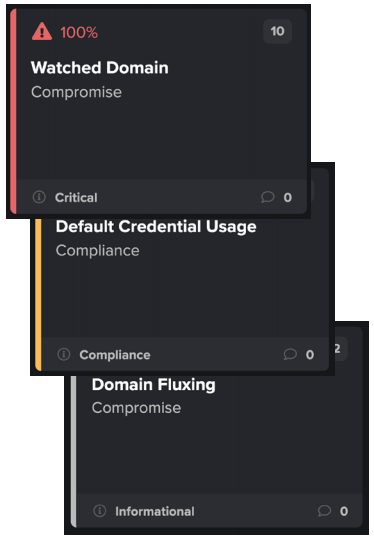


While the Threat Visualizer analyses the network, it employs machine learning to automatically understand and score a breach out of 100%. The higher the score, the greater the risk a potential threat can be thought of posing. The color range (score) in the slider correlates to the color of the entries in the Threat Tray:

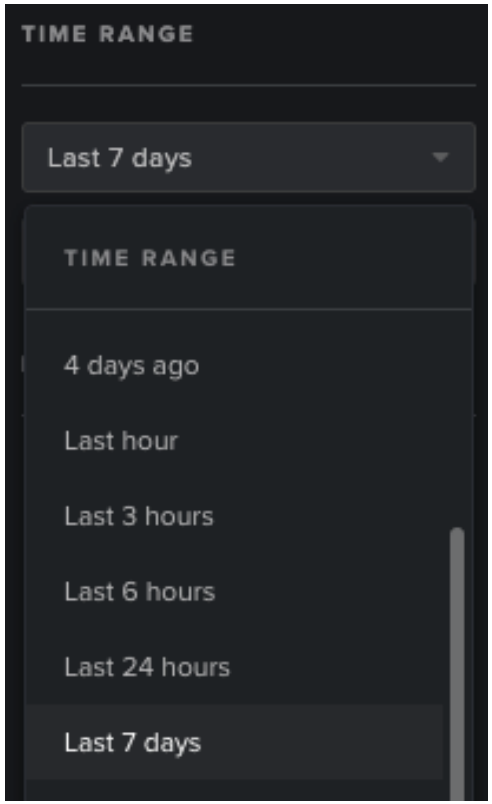
i. A **red** entry indicates a high priority threat which may be critical and require attention.

ii. An **orange** color means medium priority and **yellow** indicates a lower priority. These can warn the user of particular behavior but may not require urgent action.

iii. A gray color indicates a model has been deleted or updated and has yet to trigger a new alert since that update.



b. Depending on the size of the network, different **Time Ranges** may be suitable.

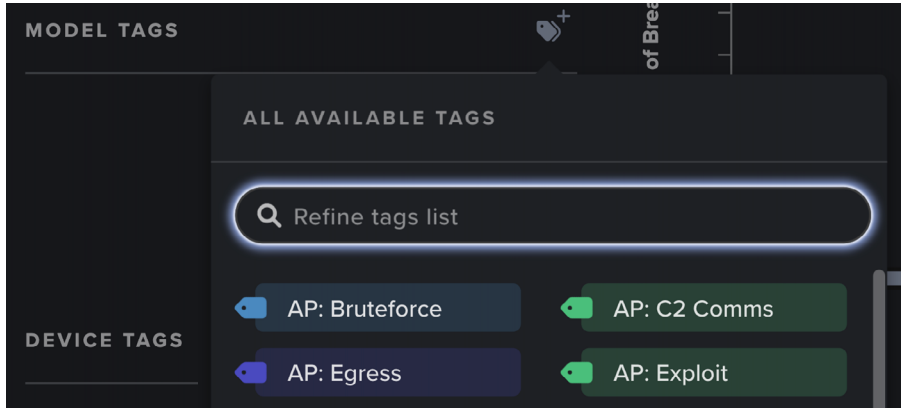


Top Tip

Differing time frames may be better suited to different contexts. For example, smaller networks may suit a weekly overview.

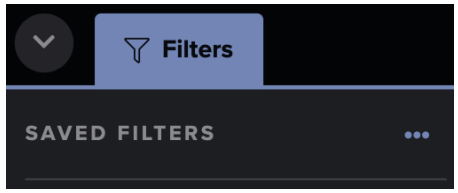
However, a large network may have equally large numbers of model breaches, so if an analyst checks the interface daily, the last 24 hours may provide a more manageable number.

c. Under the Time Selector, users have the options to add **Model Tags** as well as **Device Tags** to restrict the entries in the Threat Tray.

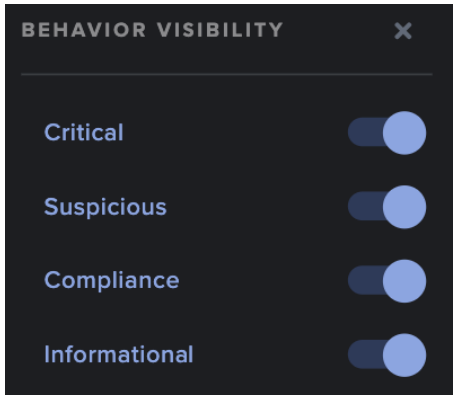


Rather than filtering the logs by Model folders, the tags provide an alternative approach. They can be added in combination with each other to locate breaches with multiple attack phases or categories.

d. To the left of the Threat Tray, notice the three dots on the **Saved Filters** tab.

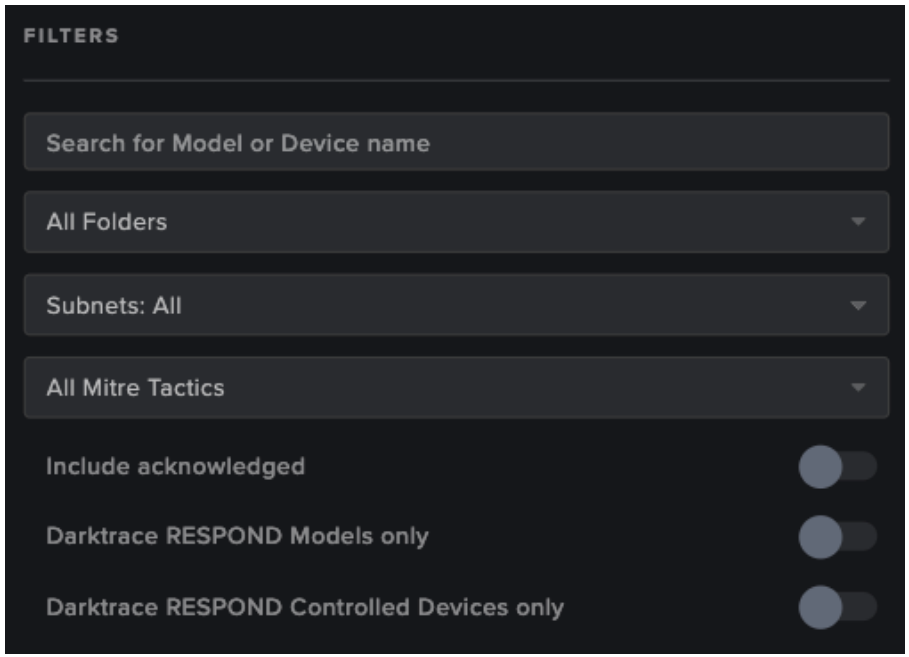


Clicking this opens the **Behavior Visibility** toggles. These can be used to display breaches that match these categories.



Note: The default behavior visibility may be defined by your administrator/account owner when setting up your account's permissions.

e. Depending on a user's role or area of interest, the Threat Tray can be filtered using the range of drop-downs and toggles in the **Filters** section such as:



i. A Search bar allowing you to search for **Model or Device name**

ii. Select specific Model **Folders**

iii. Select specific **Subnets**

iv. Filter by **Mitre Att&ck tactic**

v. A toggle to **Include acknowledged** model breaches

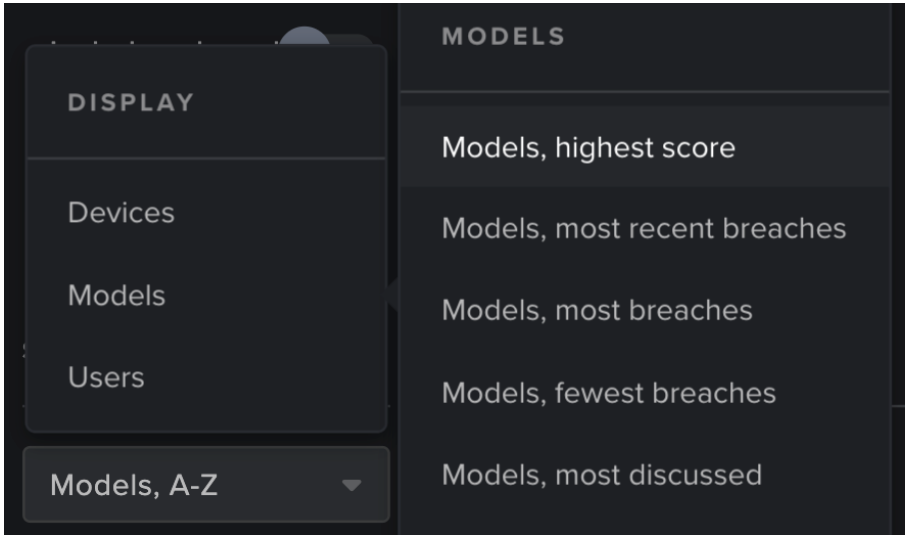
vi. Toggles for **Darktrace RESPOND Models** and **Controlled Devices only** model breaches.

Filtering the Threat Tray

Filter mechanisms may vary from user to user. For example, some users may be responsible for particular devices or subnet ranges, depending on the region they work in. As such, the first search bar allows the Threat Tray to be narrowed down by device, and Subnets can be selected by the Subnet drop-down. Alternatively, it may be possible that the user is interested in threat types and this filtering mechanism can be achieved by using the folders or tags.

There are three toggles: the first will enable filtering acknowledged or unacknowledged breaches; the second enables the filtering of just Darktrace RESPOND models; and the third option will filter Darktrace RESPOND controlled devices.

f. By default, the Threat Tray is sorted by the method used from the last login for the same user. The **sorting methods** are broken down into **Devices**, **Models**, and **Users**.



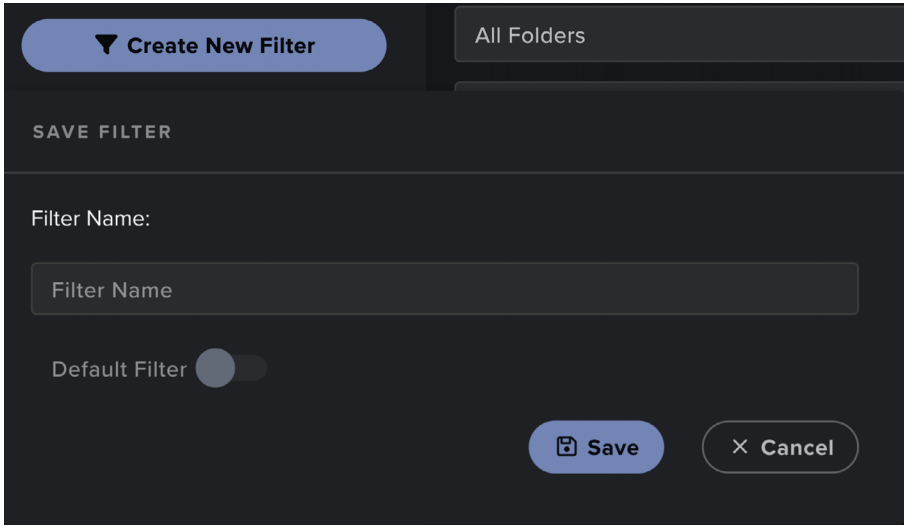
The highest score for a model (**Models, highest score**), can be useful for day-to-day analysis, focusing on breaches which may offer the most significant threat.

In a similar fashion, the Threat Tray can be sorted to highlight the devices or users triggering high scoring breaches (Devices, highest score and Users, highest score) which may offer a short cut to locating anomalous entities on the network.

There are several alternative methods of sorting results, from most recent, the most/fewest breaches, ones which have been commented on, and A to Z.

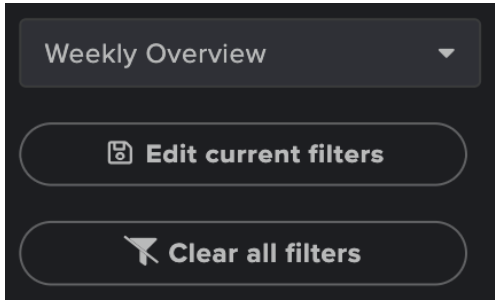
Over time, one of these methods may become a user's favorite, but they all have their merits for different analysis methods.

g. Multiple combinations of these filtering methods can be saved. With the filter pane populated, click **Create New Filter**. This opens a small window which will ask for a **Filter Name**. Input an appropriate title and click **Save**.

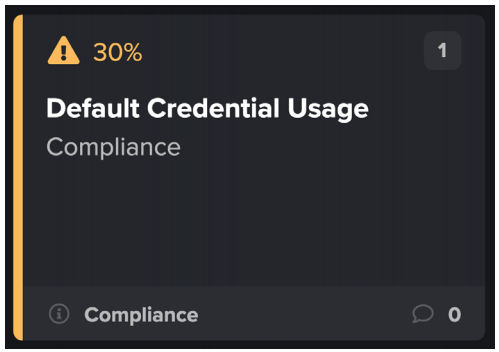


If a particular combination will be in frequent use, it can be set as the default by toggling the **Default Filter on**.

If a saved filter is populated in the filter pane, it can be **edited** or the pane can be **cleared**.

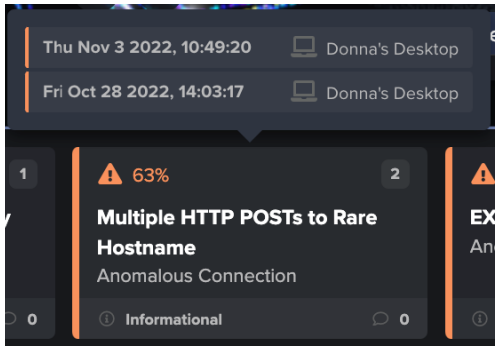


3. With the Threat Tray filtered, relevant breaches discovered by Darktrace will have an entry. These have a **title** indicating the issue discovered, a **number** revealing the sum of breaches found in the selected time range and the **behavior** and the **number of comments**.



4. To view a quick summary of a breach, **hover** over it to **view further details**.

   This summary can indicate the timings of the breaches, which can help when deciding if events may be correlated.



5. Using your knowledge of the network, **select an entry from the Threat Tray** to open the **Breach Log**.

What is a Model?

A Model contains a list of conditions which define an undesirable or notable behavior. Exceeding those conditions will trigger an action such as producing a breach to show which device has misbehaved or initiated a Darktrace RESPOND/Network action.

An alert (Model Breach) cannot be fired without a corresponding Model. The Threat Visualizer comes shipped with a large collection of Models which can be customized for individual subnets and applications. Darktrace constantly invests in developing new Models to understand new threats. It is also possible to create new Custom Models.

Using the Breach Log

Continue your learning with our dedicated video: 3: Investigating Model Breaches

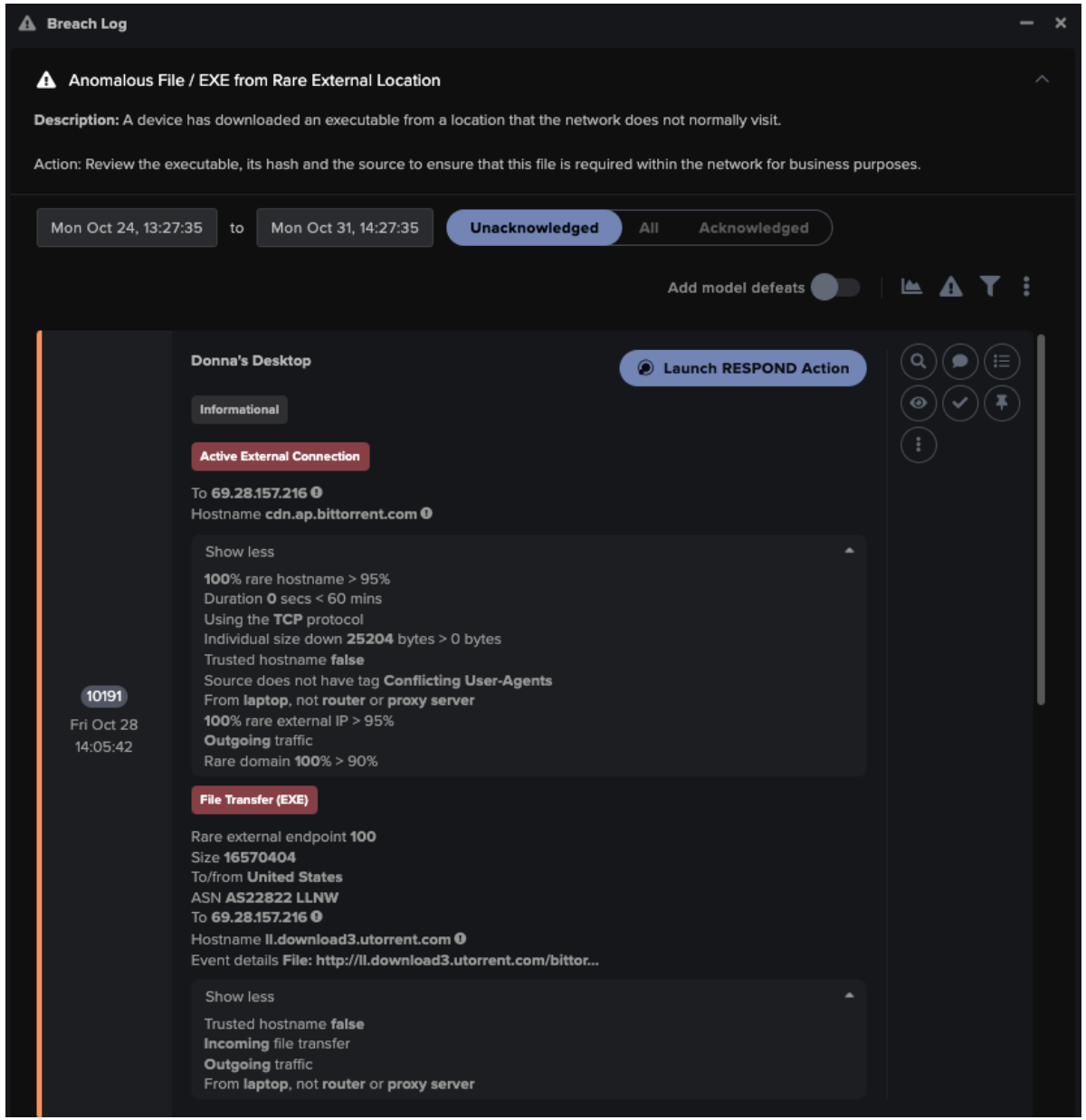
1. Click on a breach to load the **Breach Log**. Each breach reveals the device and date on which the breach was triggered, the Model that was breached and the values that exceeded the Model's filters. Read these details and the description to gain and understanding of the Model Breach.

   In this example, a host downloaded a suspicious executable from a rare external location. The total size of the incoming packet and the file name is confirmed.

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

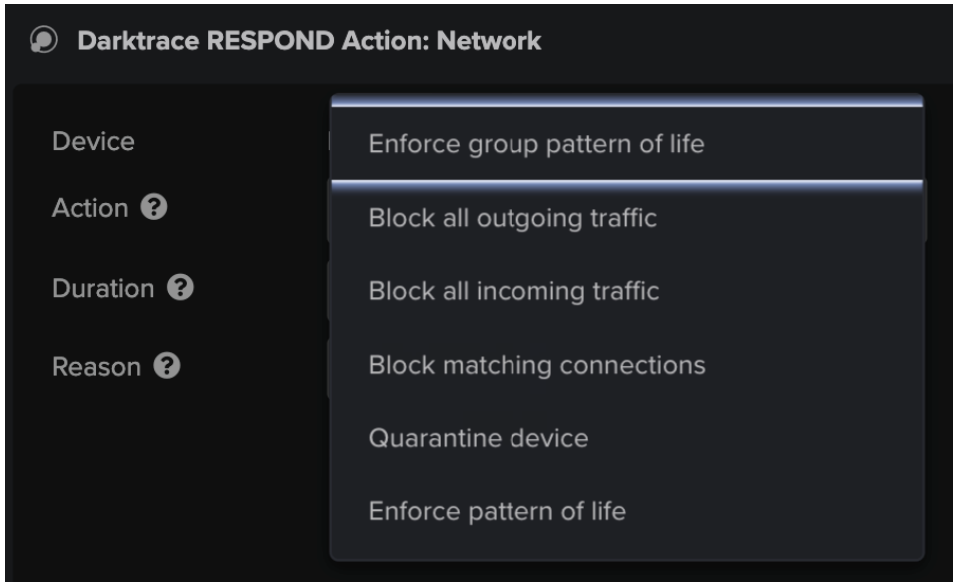
   Notice the rare domain score achieved 100% > 90%. This means it exceeded the Model target of 90% and so triggered the breach.

   Hovering over the vertical colored bar for any breach will reveal the overall Threat score, which in this case was 64%.



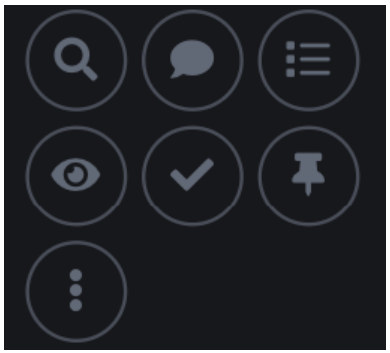
2. The **Launch RESPOND Action** button brings up a new window with options for initiating a Darktrace RESPOND Action, if it is licensed.

From here it is possible to select the specific action that is required.



Note: More information on the Darktrace RESPOND Actions can be found in the Darktrace RESPOND/Network course.

3. Notice a series of **buttons** on the right-hand side of the breach details.



a. The first icon, the **magnifying glass**, will center the Threat Visualizer on the device around the time of the breach.

b. Next is the **Comment** icon, which enables users to make comments about the breach. These are visible to all users.

c. The third icon is the the **Model Breach Event Log**, displaying all connections relevant to the Model Breach.

d. The **eye** icon displays the **One click analysis** which has the log data and a graph with data about to the Model breach.

e. The tick icon is used to **Acknowledge** Model breaches. This hides the breach from the Threat Tray.

f. The pin icon allows users to pin a breach, which keeps the breach displayed in the Threat Tray until unpinned.

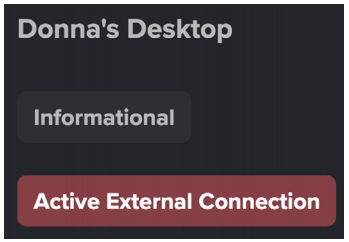
g. The final icon, 3 dots, provides **Additional actions** related to the Model that has been breached.

Note: these options are covered in more detail, in the Further Investigation Techniques chapter.

Top Tip

It is good practice to click on the magnifying glass button before utilizing any of the other features to ensure the visualizer is relevant to the breach being inspected. Remember, the time period can be increased using the Time Selector which may bring up connections between other devices in the Device View or present more information in the summary down the right of the visualizer.

4. Clicking the **metric** displayed in the Breach Log such as "Active External Connection" generates a graph of the metric over time.



Note: Selecting a different metric from the Breach Log will change the subject of the graph.

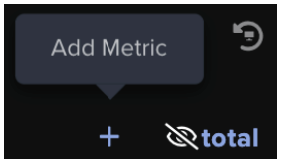
The **dots** represent the breaches and their score. An anomalous spike such as for a file download from a rare domain may indicate suspicious activity.

a. The graph can be **refocused** to other areas of interest. Clicking elsewhere on the graph centers it around the selected time. This can be a useful method to investigate how often breaches in relation to the plotted metric have occurred in the past. (This can be reset at any time by clicking the Breach Log magnifying glass.)

Furthermore, clicking and dragging around a region of the graph will cause it to zoom in, therefore allowing for any activity to be inspected more closely.

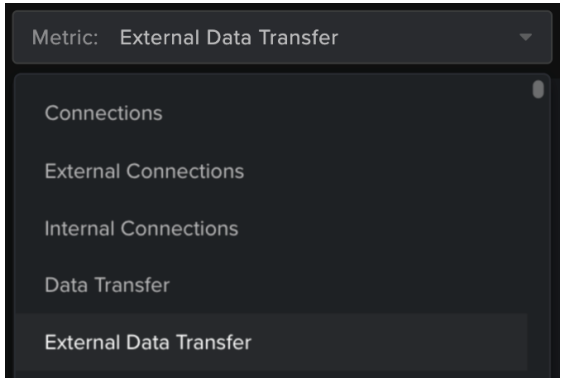
b. Click the **Time range** drop-down under the x-axis to alter the timescale. It can be helpful to set 1 week either side or even 3 weeks before to better understand historical events for a device.

c. Further analysis can be gained by appending additional metrics to the graph. Click the **plus (+) symbol** in the top right and append a new metric to the graph.



d. Append a **corresponding metric** to your graph, for example, External Data Transfer.

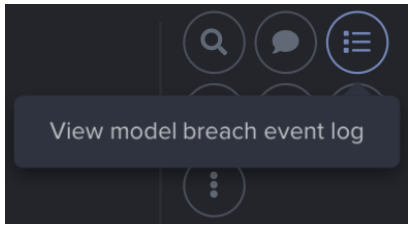
This will show when data was uploaded or downloaded from an external source on your network and can provide an indication about how the device has been used in the timeframe.



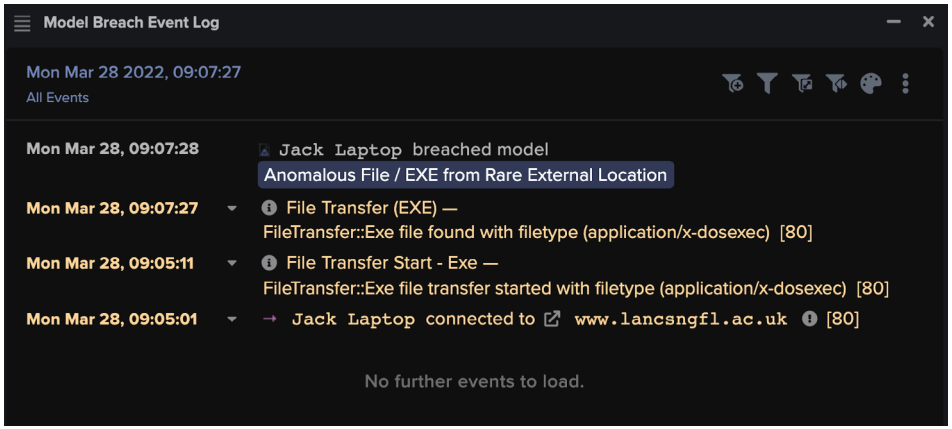
There are many other metrics available. For example, the importance metrics measure how abnormal the behavior is for a device. They are produced by the output of the classifier. It is important to review all this information to determine if the transaction is trustworthy.

5. Often it is useful to get more context about an event, such as specific connectivity and port usage.

Using the icons on the right of the Breach Log, select the **list icon** to open the **Model Breach Event Log**.



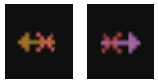
6. Review all the **connection and event information** relevant to a breach. Notice the small arrow by many of the rows which indicate the flow of data.



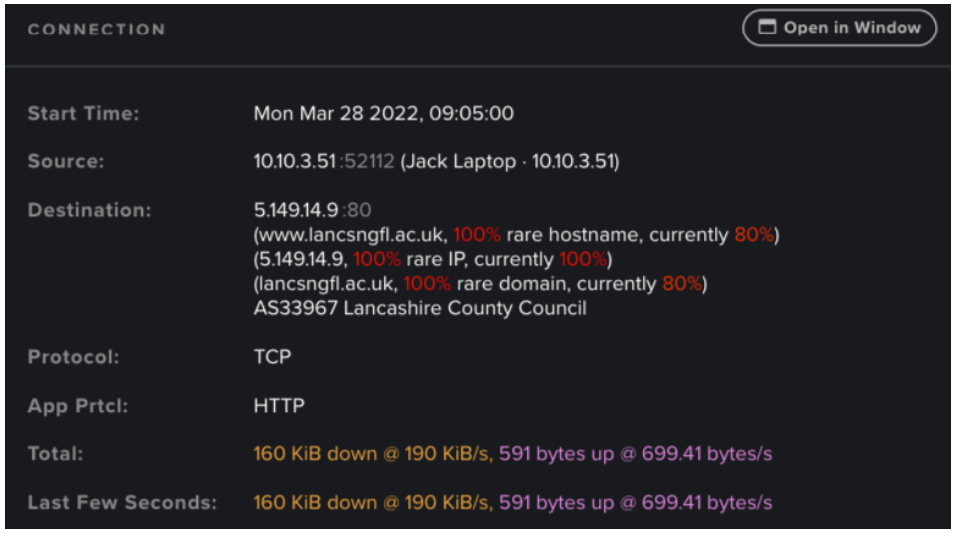
a. A pink/purple **right facing arrow** signifies an outgoing connection. (If it's flashing, it's ongoing.)

b. An orange **left facing arrow** signifies an incoming connection. (If it's flashing, it's ongoing.)

c. A broken **arrow with a cross** through it signifies a failed connection.



7. Click on the **arrows** to reveal full information about the connection. The protocols, amount of data sent, and destination information are included.



Note: Click Open in Window to have the same information presented in a separate window which can be kept open for comparison.

Filtering the Event Logs

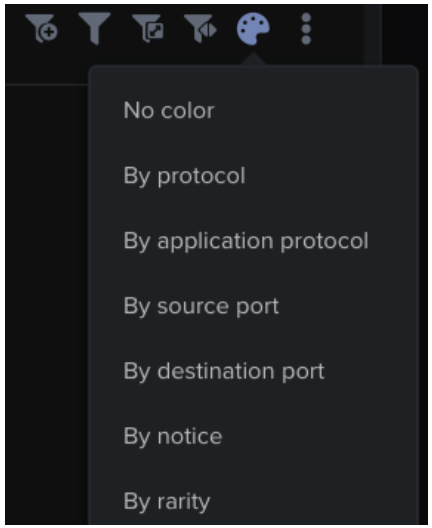
In the Event Logs, a range of filter icons control how and what data is presented.

Review the options to:

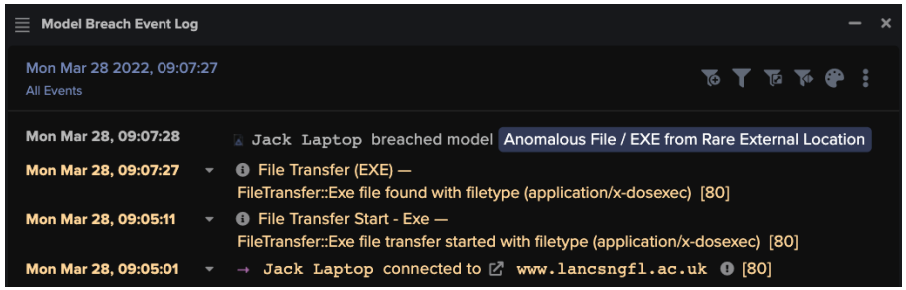
- Add custom filters based on a selected field
- Filter by different event types from a predefined list of types
- Display internal or external events
- Display incoming or outgoing events
- Color code the events based on their properties
- See further advanced options by clicking the three dots.

8. In to the Model Breach Event Log and click the **paint palette** icon to **Color-code** events by their properties.

   Note: The default color coding can be set in the Account Settings. This is outlined in the Threat Visualizer. Part 1 - Familiarization course.



   a. In this case, by default (as dictated by the Account Settings), it is set to **destination port**, which is a good way to quickly recognize and group activity. The destination port can be a good indicator of the protocol.

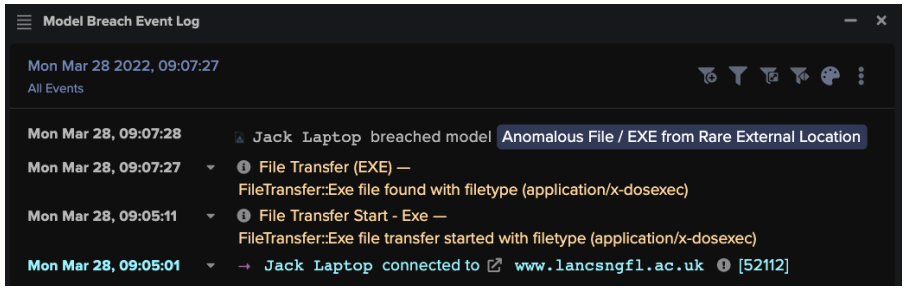


Top Tip

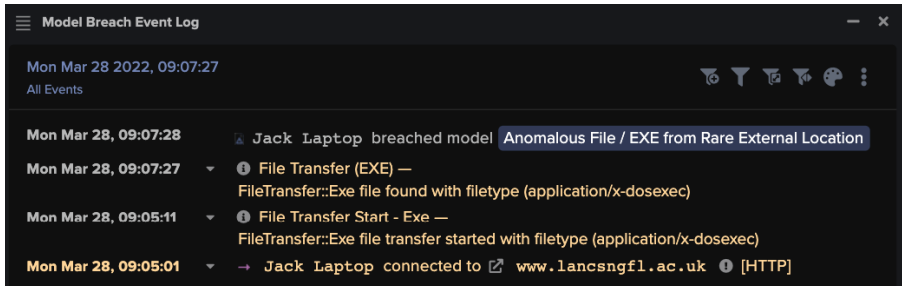
These color coding methods can be coupled with other filter mechanisms to best display events of interest.

For example, combining rarity with external, outgoing events could highlight external risks.

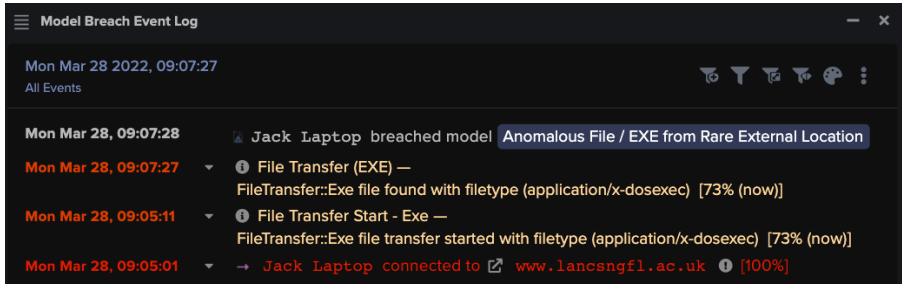
   b. Coloring by **source port** is helpful when reviewing a number of communications to the same destination port but also wish to estimate the number of distinct connections or flows.



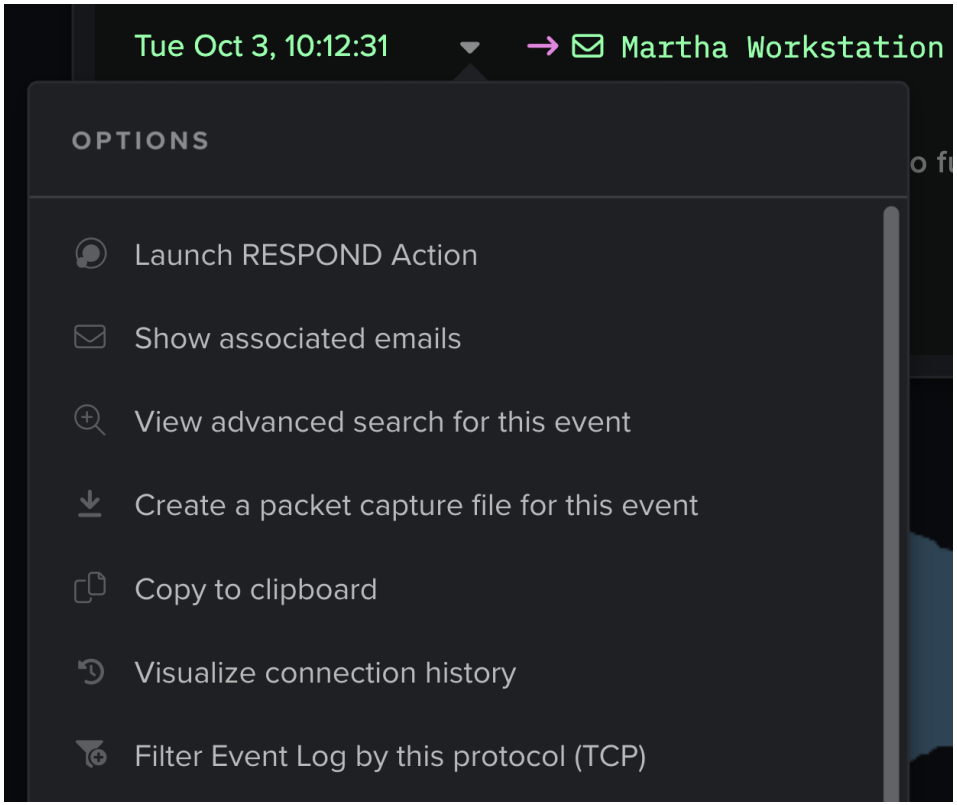
   c. If ports are not easy to distinguish, coloring by **application protocol** may be of assistance.



   d. However, when reviewing several external communications to various destinations, it may be useful to color code by endpoint **rarity**, in order to quickly view this value instead of checking each individually.



9. Click the **downward arrow** to the right of the timestamp in the Model Breach Event Log to open an additional range of options.



Top Tip

For deployments with Darktrace/Email, links accessed from an email can be investigated using the option from the Threat Visualizer.

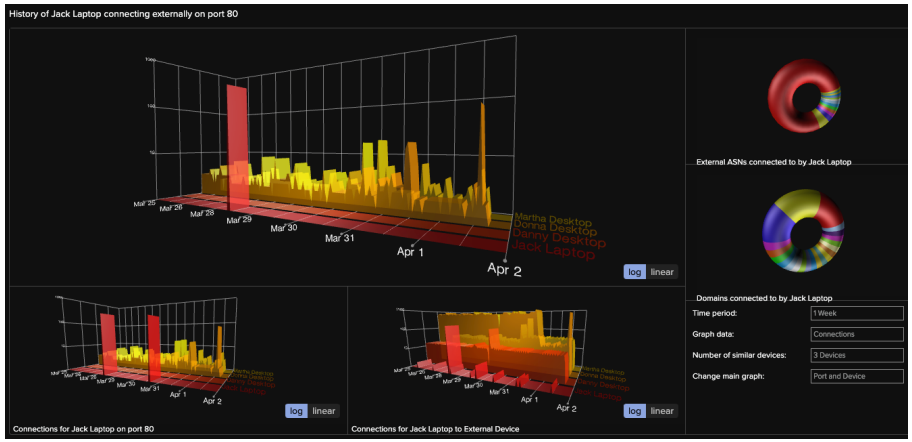
An email icon will appear on the Model Breach Even Log. Click the downward arrow to Show associated emails and start investigating.

a. The **Copy to clipboard** function is a useful way to copy the threat details, such as copying the IP or web address for further investigation.

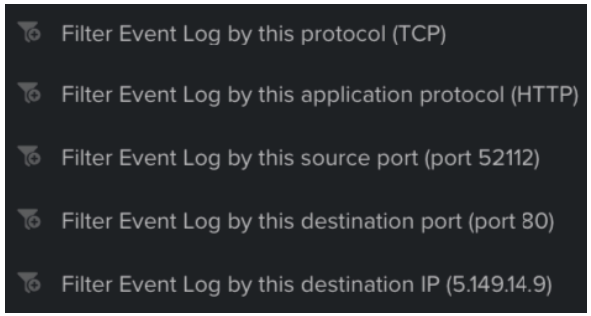
Note: The copied event information may be of a format similar to the following.

2022-03-28 08:05:01 +01:00
**Jack Laptop · 10.10.3.51 ** made a HTTP connection to www.lancsngfl[.]ac.uk on TCP port 80

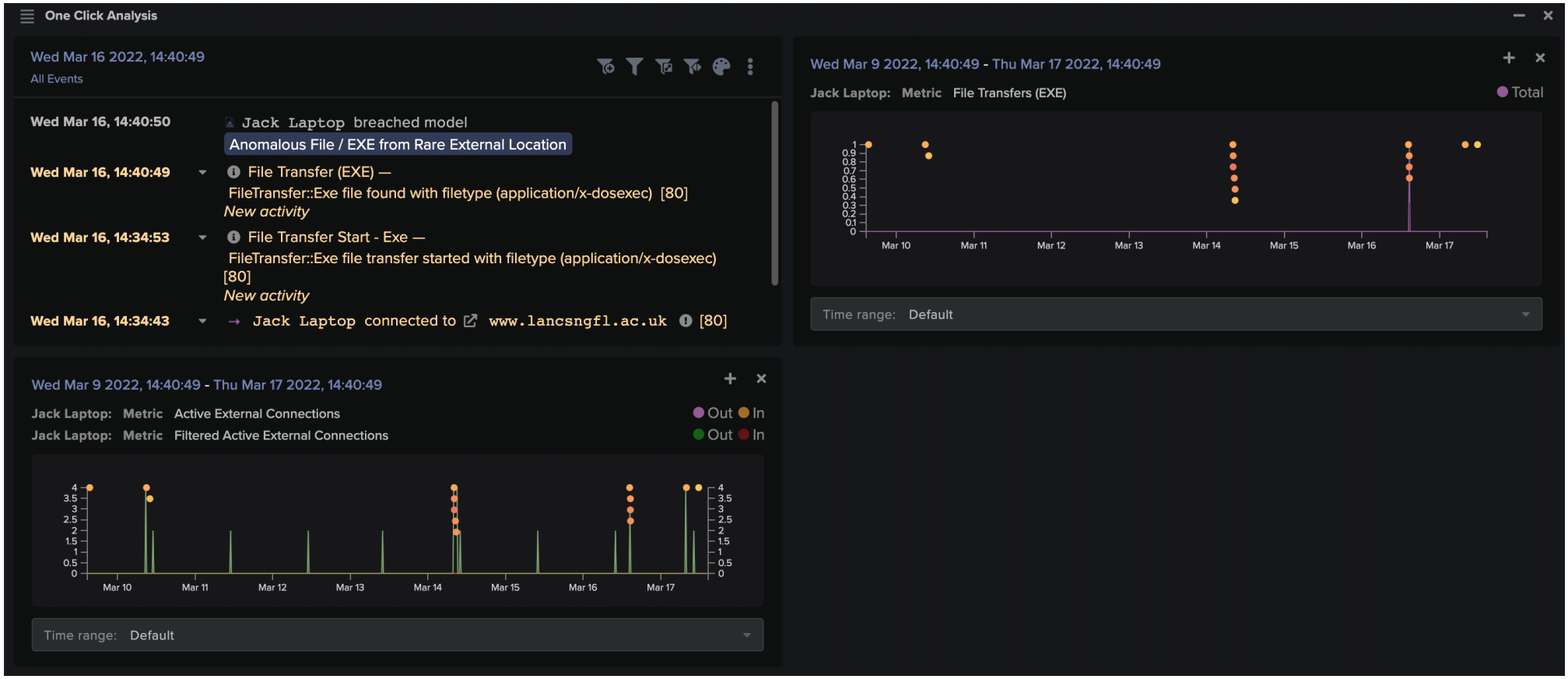
b. Select the **Visualize connection history** option to open a new window displaying a three-dimensional view of a device's history. It includes ports and devices covering a duration of up to 28 days. Try changing the filter options in the bottom right to update the results.



c. Quickly restrict the log to a **specific Protocol, Port, or IP**. The chosen filter will appear at the top left of the Log and can be removed by clicking the cross.



10. Navigate back to the Breach Log window and click the **Analyze this Model Breach** icon. This **one click analysis** window includes an event log alongside graphs for relevant metrics, both of which facilitate detecting similar anomalies.



With the executable download example above, it can assist with answering the following questions:

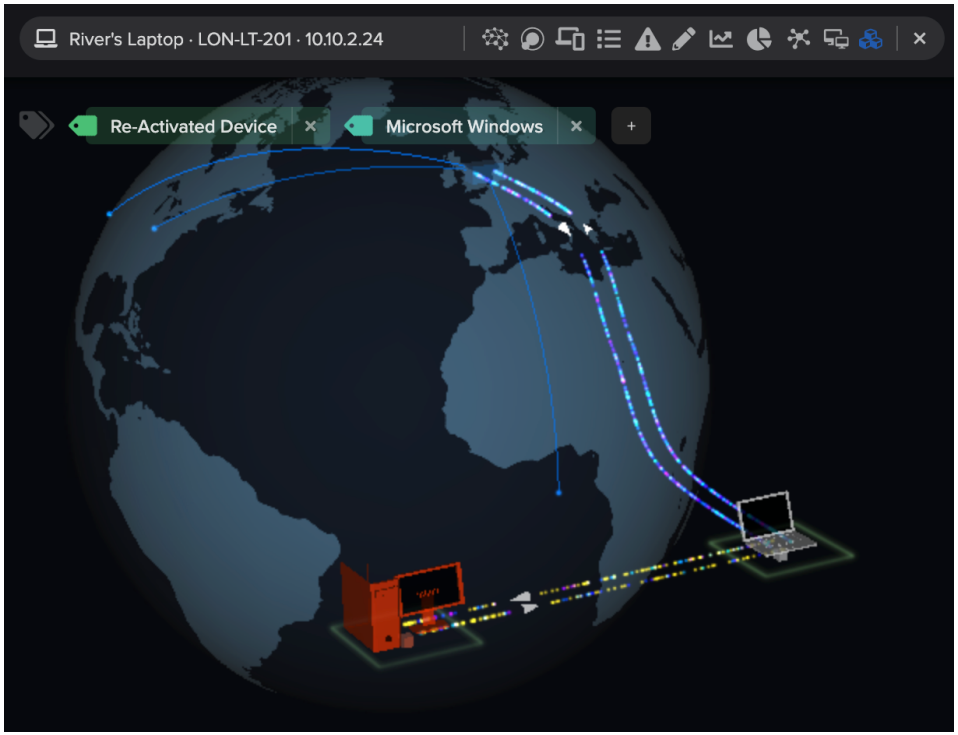
a. Who downloaded executables and from where?

b. Has the same device or user downloaded other EXE files before?

c. Were they downloaded outside of working hours?

d. Is there any suspicious network behavior since the download, such as beaconing to an external destination?

11. When a device under investigation is populated in the Omnisearch bar - using the magnifying glass, or by other means - it will also open the Device view in the background. If centered around the time of a **Model Breach**, the **interactions** taking place at that moment can be **visualized**.



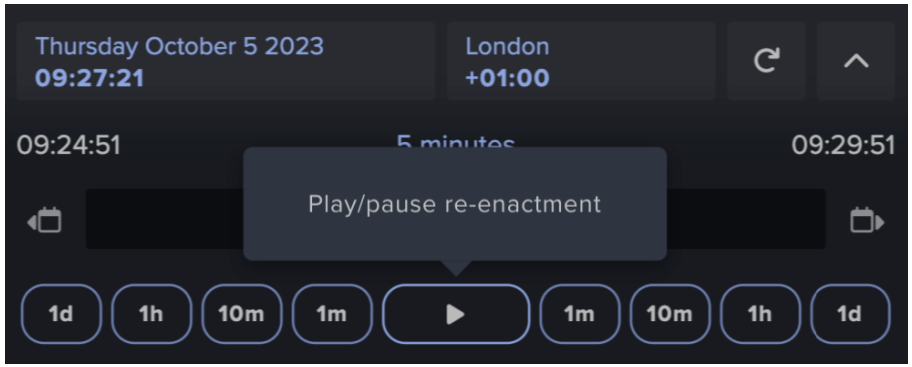
Top Tip

Following the above investigative workflow, it is possible that many windows may be open. While these can be minimized or closed individually, they can also be closed in bulk.

If there are multiple windows open, hold the shift key on your keyboard and click the cross in the top-right of the dialog to close all windows simultaneously.

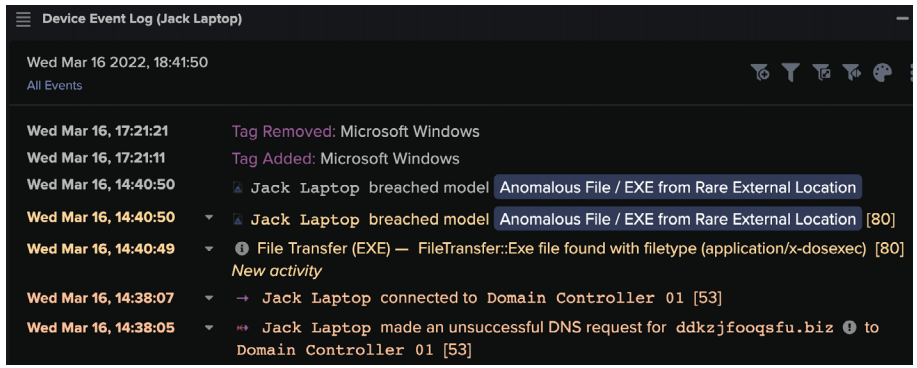
12. The Threat Visualizer has the capability to view the stream of data coming from the network appliances in **real time**. This can be used not only to understand what data is currently being sent, but also to go back in time and replay a sequence of events.

    a. Within the **Time Selector** on the Home page, click the play button.



    b. Moving through time using the **backwards** and **forwards arrows** can help build a picture of other events occurring around the same time.

    c. Notice how live data is automatically streamed in the Device View and **Device Event Log**.

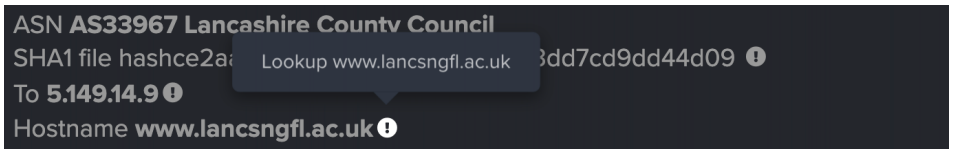


Consulting External Sources

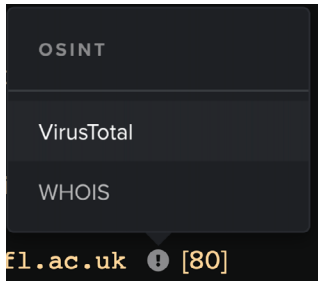
Continue your learning with our dedicated video: 4: Additional Breach Log Filters

Many tools can be used to conduct Open-Source Intelligence gathering on endpoints and files. Having multiple tools in an analytical toolbox can assist with conducting more thorough and nuanced investigations. There are many resources available, the following of which are a handful of examples.

1. If enabled, Darktrace is able to **integrate with open source intelligence** (OSINT), providing a shortcut from the Breach and Event Logs to online databases.



With this feature active, a clickable **exclamation mark** will be presented to the right of relevant details, such as domains or file hashes. When opened, it will give the option insert the information into a VirusTotal or WHOIS search.



Note: To see how to enable this feature, please refer to the OSINT Integration section.

2. If the aforementioned feature is not enabled, these databases can be used independently.

   a. **VirusTotal**, https://www.virustotal.com, can analyze files, URLs, and IP addresses to check for known malware. It is also possible to search for a cryptographic hash (MD5, SHA1, etc.) to identify a file. This hash can be located in the Threat Visualizer's Advanced Search.

   b. When investigating external IP addresses or domains, a **Whois** service can provide owner details of a server. This can help determine if an address is a legitimate trustworthy host. Navigate to https://who.is/ and enter an IP address or domain name to gain more information.

3. **Domaintools**, https://whois.domaintools.com, is also a popular tool to investigate domain information.

   Note: The date of registration can be a subtle, yet important indicator or potentially nefarious activity. Anything less than a few months old may be untrustworthy.

4. **URL scan**, https://urlscan.io/, provides a screenshot of the website from, a URL or IP address. It also gives further information such as if it is on Googles Safe Browsing list, when it has been scanned, how many times it has been scanned, and if scanned images are present for the past scans you are able to view those as well.

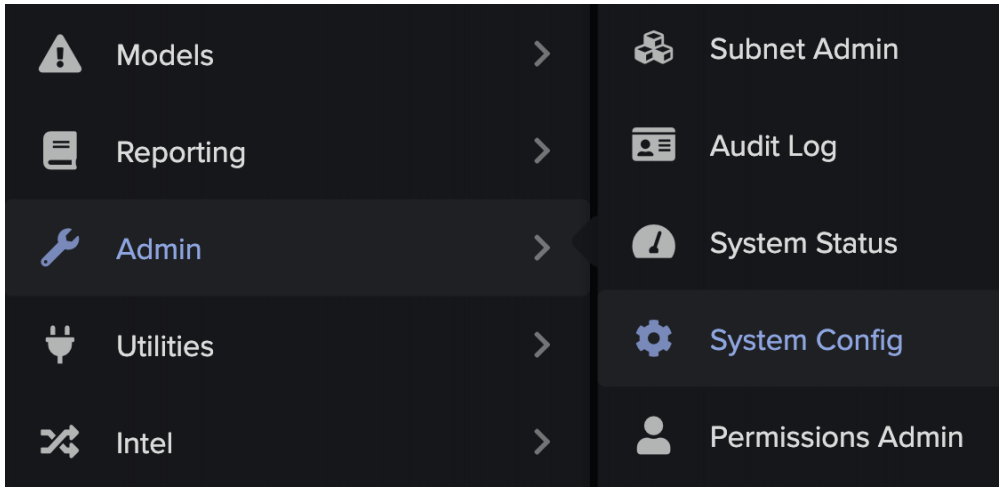
5. Finally, **Shodan**, https://www.shodan.io, is a search engine for Internet-connected devices

OSINT Integration

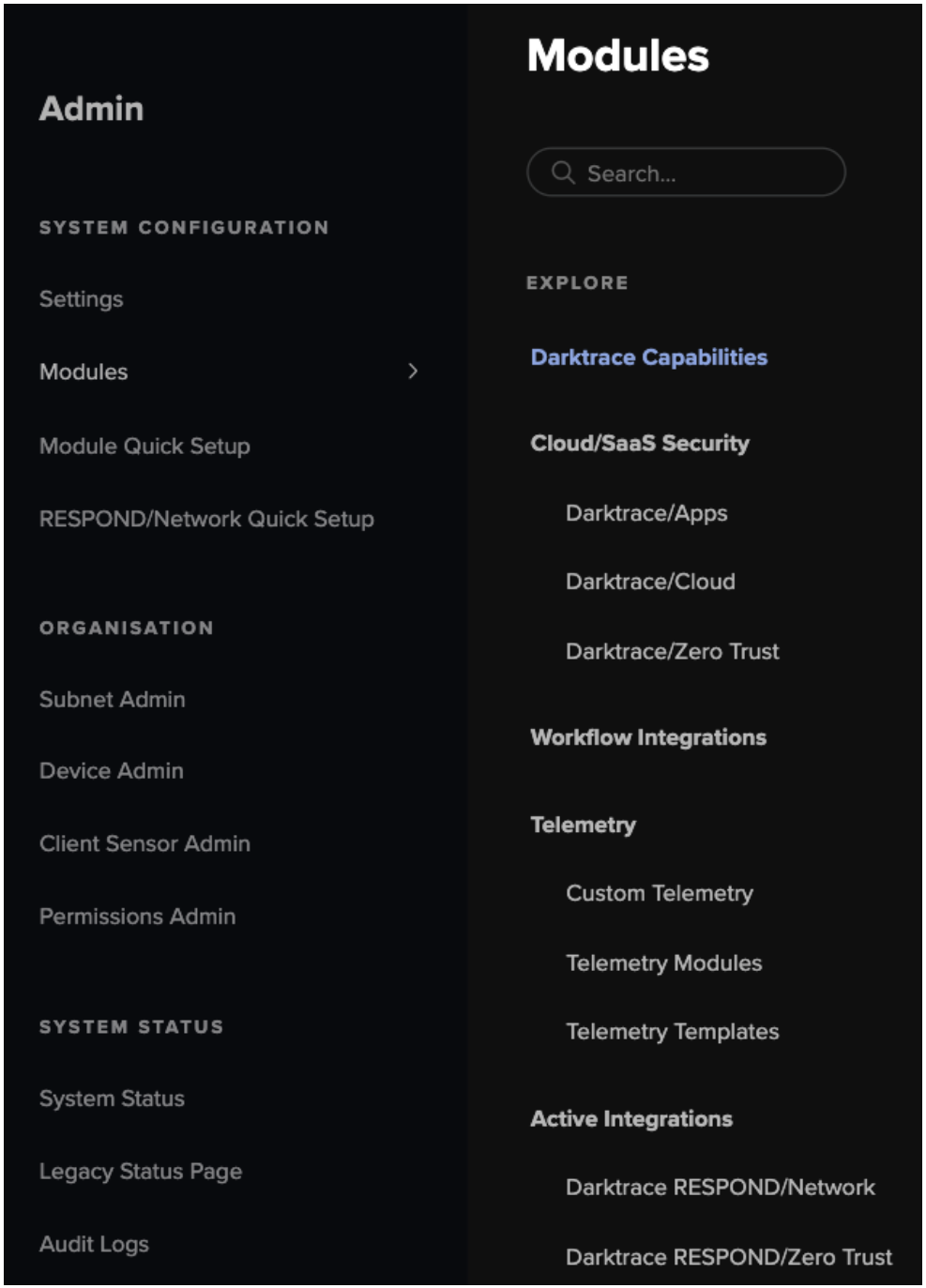
The Darktrace OSINT integrations provide a simple, convenient addition to the cyber analyst workflow. Once Darktrace has identified unusual device activity or connectivity to rare endpoints through 'pattern of life' analysis, many security teams integrate the use of threat intelligence tools in their investigation and response process.

In Event Logs and Breach Logs, the option to look up external IPs, domains, and file hashes directly through online databases is made available. The integration offers an easy way to check relevant data through the incorporation of a user-friendly OSINT button within the log line.

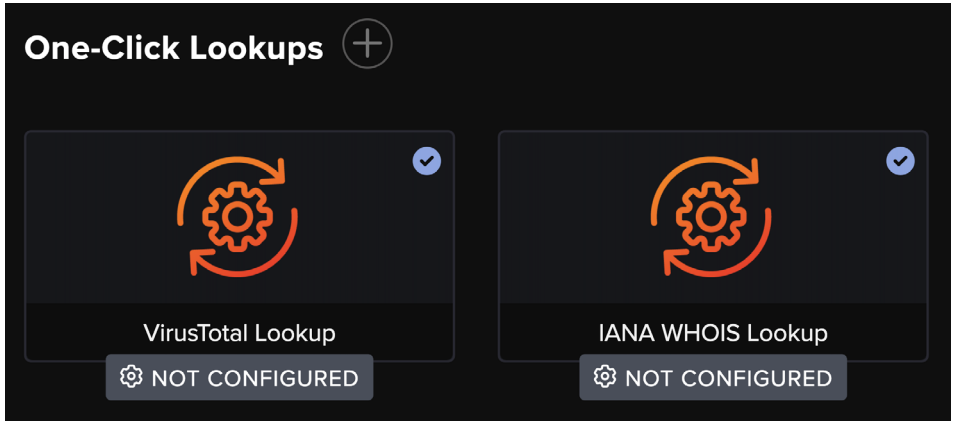
1. Within the Threat Visualizer **main menu**, navigate to the **Admin** option and select **System Config**.



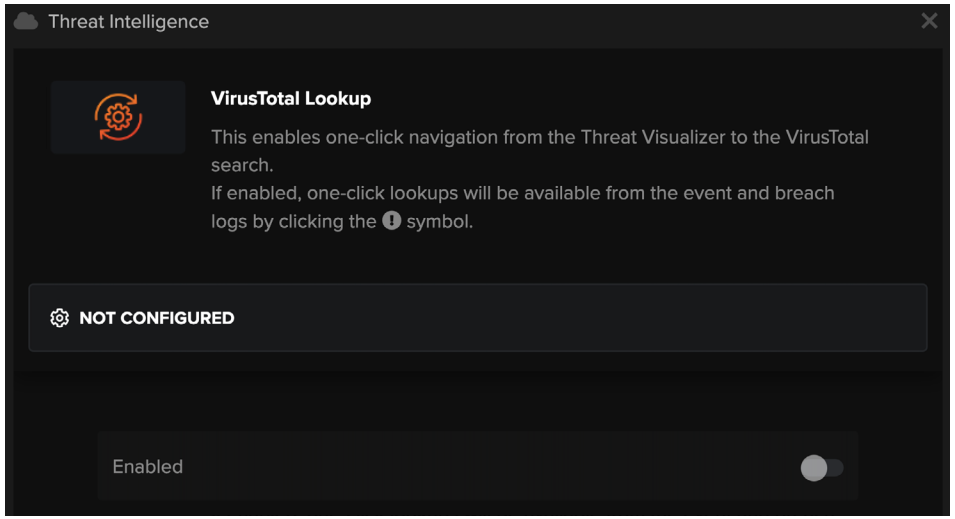
2. From the System Configuration menu, select **Modules** on the left-hand side and choose **One-Click Lookups** from the **Threat Intelligence** section on the right. Alternatively, use the **search** bar to locate the desired module.



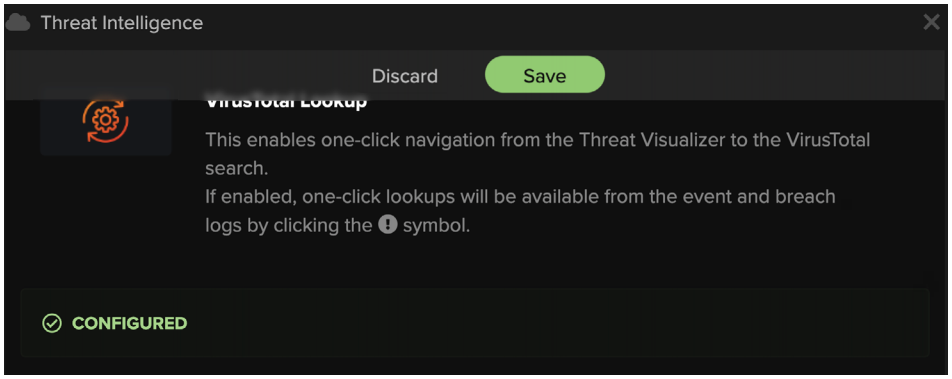
3. Under the One-Click Lookups heading, select either the **VirusTotal or IANA WHOIS Lookup**.



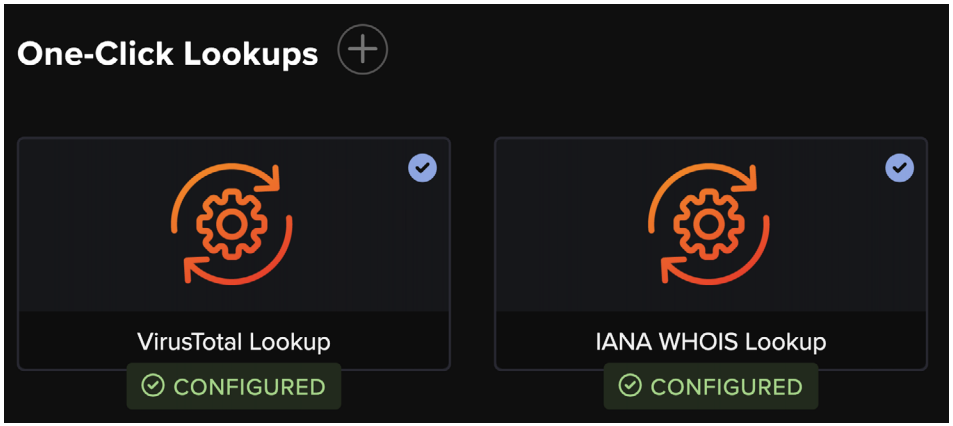
4. If this module is unconfigured, the Enabled toggle will be off. Slide this **Enabled toggle to on**.



5. The module will update to configured. Click the green **Save** button at the top of the window to apply this setting.



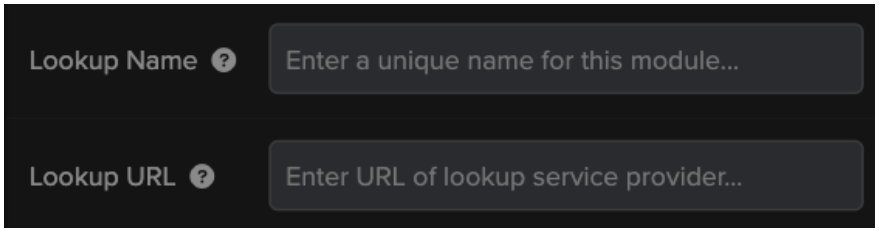
6. Closing the newly configured integration and returning to the Config page will display the configuration status. If successful, this should be green and read "**CONFIGURED**".



7. With these settings saved and the modules enabled, the clickable **exclamation mark icon** will appear next to searchable fields in the interface.

8. Clicking on the **plus icon** next to the heading will allow users to add other OSINT of their choosing.

   a. Start by inputting the new module **Lookup Name** and **Lookup URL**.



   b. Several **Supported Object Types** can be added in the next section:

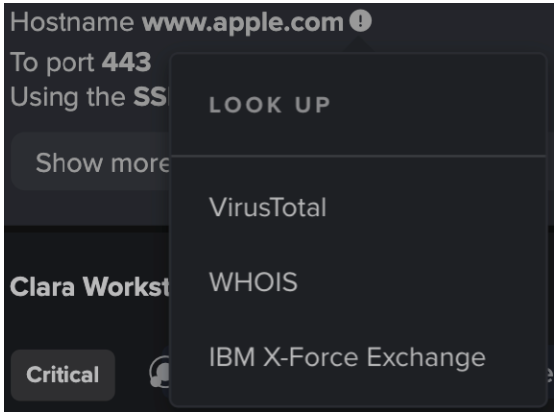
      i. **Domain** which can be enabled with an optional Domain URL Extension;

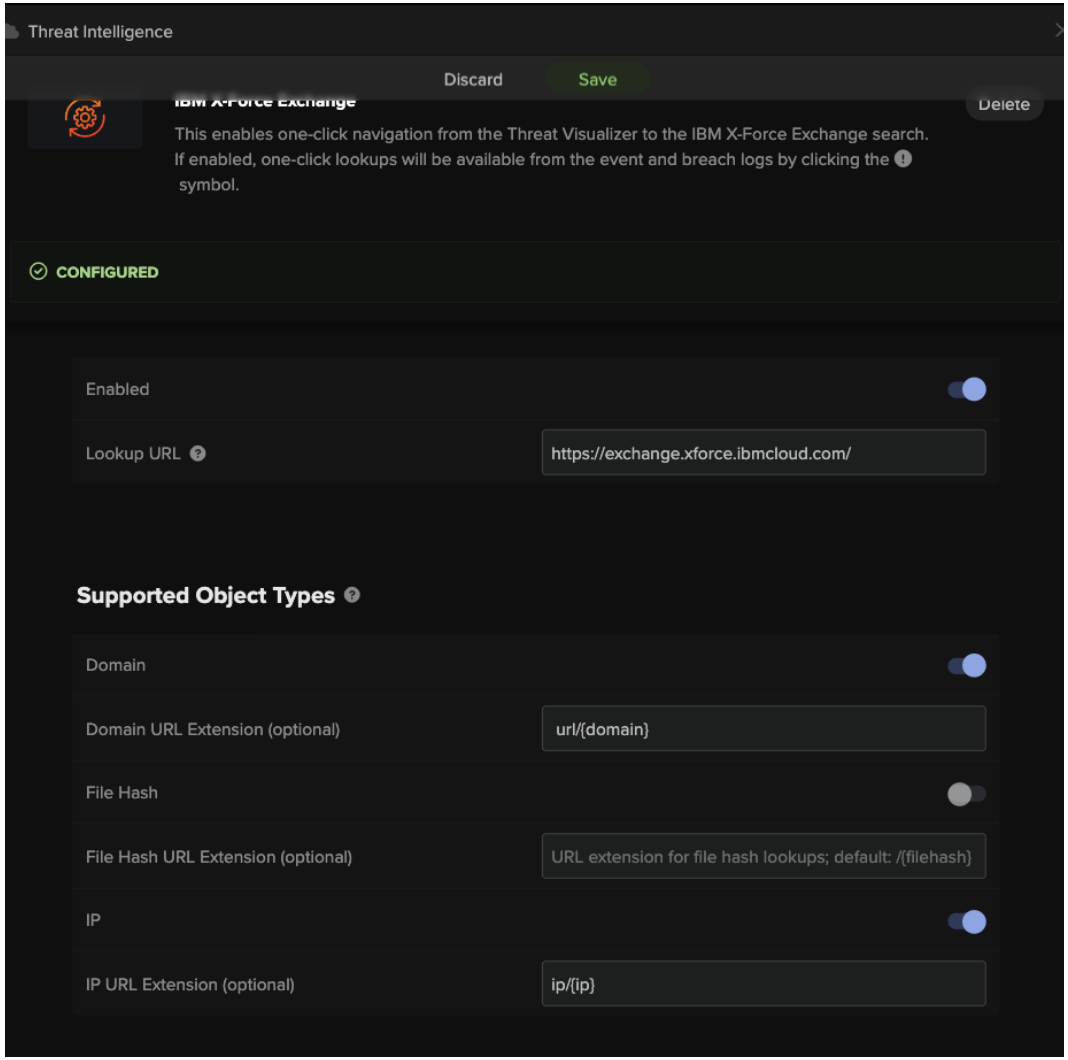
      ii. **File Hash** which can be enabled with an optional File Hash URL Extension;

      iii. **IP** which can be enabled with an optional IP URL Extension.

   c. Finally, click on **Save** to finish the configuration of the module.

   d. The option to lookup Domains, File Hashes or IP addresses via this new module will appear on the Threat Visualizer with an **exclamation mark icon.**



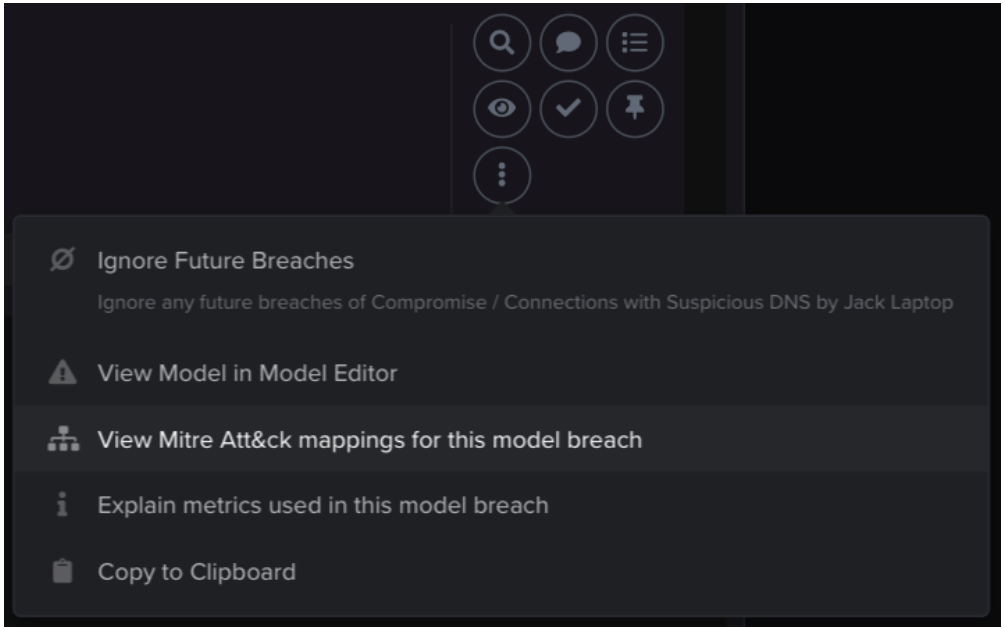


   e. An **External Link Warning** will appear before being able to continue to the new OSINT website.

> This lookup has been configured by a member of your team via the System Config page. This link is not associated with Darktrace and will open in a separate tab.

MITRE Mappings

For every Model Breach, Darktrace provides the option to view the Mitre Att&ck mappings. This option can be located under the **Additional Options** from a Breach Log.

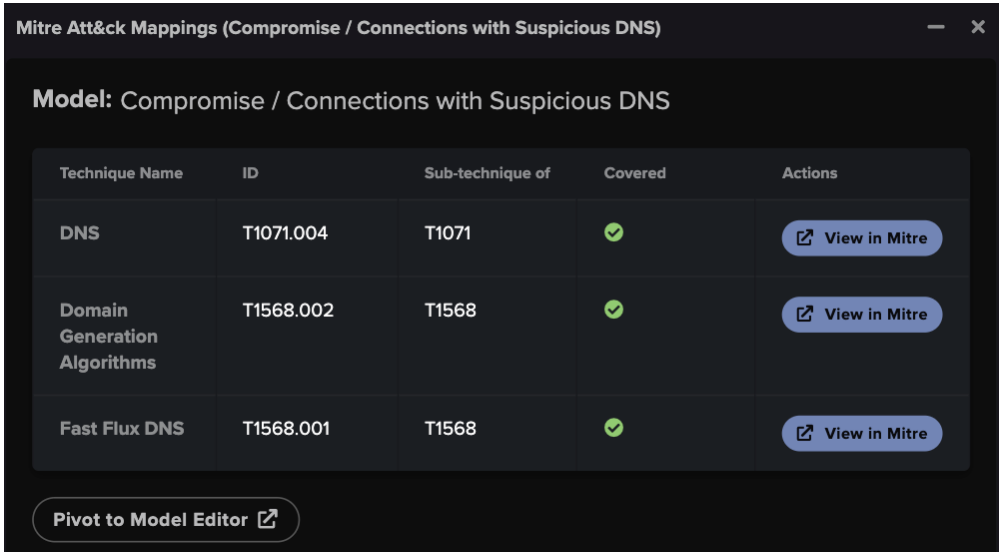


Having Model Breaches mapped to the MITRE Att&ck framework allows users to integrate Darktrace investigations with their existing threat investigation playbooks.

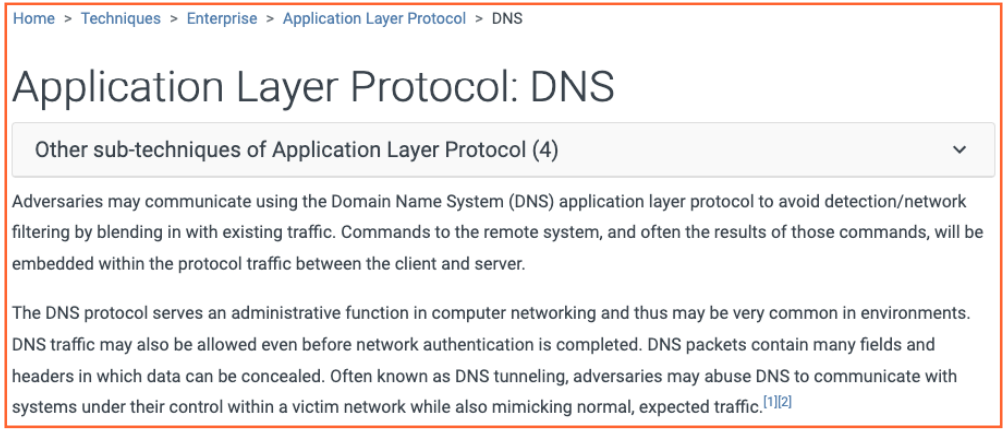
Mappings

Darktrace's EIS mappings can be downloaded in JSON format from the Model Editor and viewed in Mitre's Attack Navigator.

Some Model Breaches may have multiple mappings. For example, by navigating from a **Compromise / Connections with Suspicious DNS** Model Breach, there are three mapped techniques, as highlighted below.



Each technique has an ID, a sub-technique and an indication if the technique is covered by Darktrace detection. Any technique can be **viewed in Mitre** for more information - this might give more context and understanding surrounding an incident.



Navigation Exercise

If you already have access to the Threat Visualizer, carry out the following steps from your own interface in order to test your knowledge on how to navigate the Threat Visualizer. You can keep a record of your attempts by filling in the text boxes and saving the manual. *If you need help or if you want to check your method, click on the tooltip icon to reveal where you can find this information. Click on an answer to hide it or use Show All / Hide All.*

1. Identify your own device on the network.

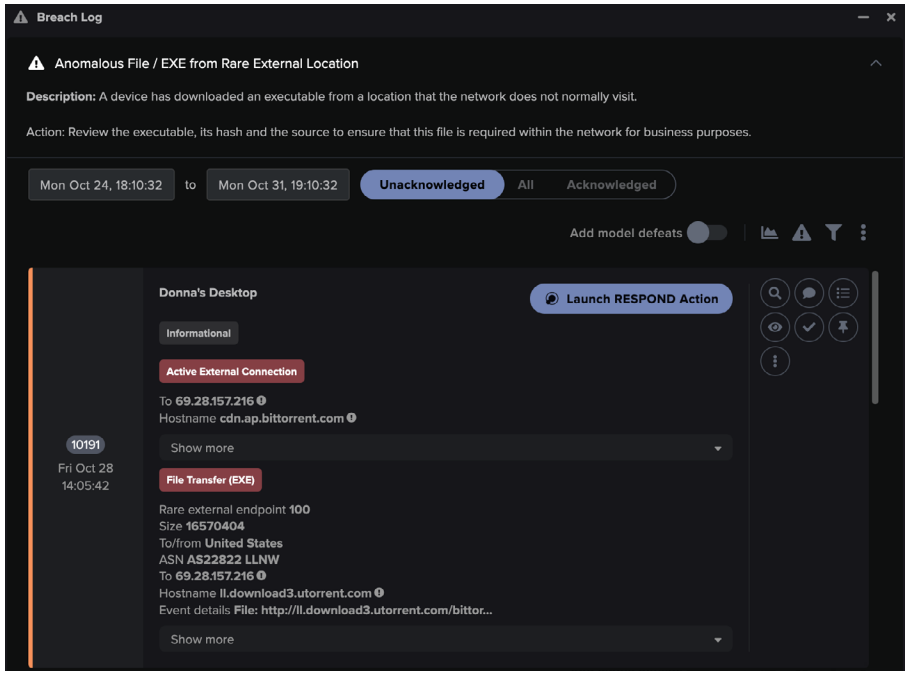
2. How can you identify all mobile devices?

3. Describe how to view all Model Breaches with a threat score of at least 50%.

4. Which device has triggered the most alerts in the last 7 days?

5. Which User has the most model breaches?

6. What steps would you take to investigate this anomaly further?



Model Summary Test

This page will test your knowledge and check your understanding of the Model Breaches 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 a Model?

- [ ] A list of behaviours the deployment should follow
- [ ] A list of conditions defining an undesirable behaviour
- [ ] A set of rules and signatures

2. Which icon represents the Model Breaches view?



3. From the Breach Log , which icon allows you to analyse a model breach?



4. In the Model Breach Log, how can you open a 3D view of a device's history?

- [ ] By selecting View advanced search for this event
- [ ] By selecting Visualise connection history
- [ ] There is no 3D view available

5. True or False: The colours in the Model Breach Event Log have NO meaning.

- [ ] True
- [ ] False

6. Model breaches are linked to which external website that provides 'mappings'?

- [ ] Mitre Att&ck
- [ ] VirusTotal
- [ ] Whois

Clear All Answers

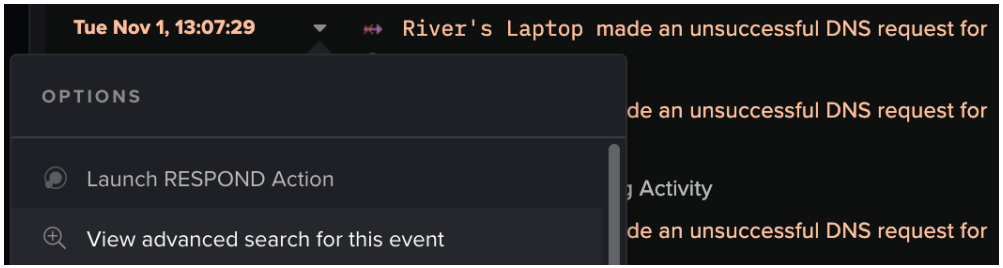
4. Advanced Search

Darktrace captures logs for all network traffic. Each IP connection generates a "conn event" and each "conn event" has a corresponding unique identifier (UID). This identifier is also present in any further events generated in the process of deep packet inspection. The Advanced Search component contains different functionalities and data in addition to the Threat Visualizer's Breach Event Log. In this chapter, let's familiarize ourselves with the Advanced Search interface and discover some useful tools for investigation.

Advanced Search Navigation

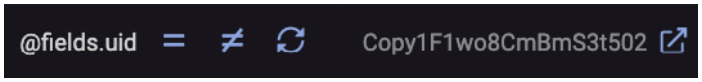
Continue your learning with our dedicated video: 5: Advanced Search - Navigation

There are multiple ways to navigate to Advanced Search. Using the analytical workflow, it is most common to navigate to Advanced Search via an Event Log. Simply use the drop-down arrow beside an event and select **View advanced search for this event**.



By doing so, Advanced Search will automatically populate the search bar with the connection UIDs and choose a relevant time frame to inspect the event. This may display additional details about a connection, but could also be used as a starting point for a broader query of network traffic.

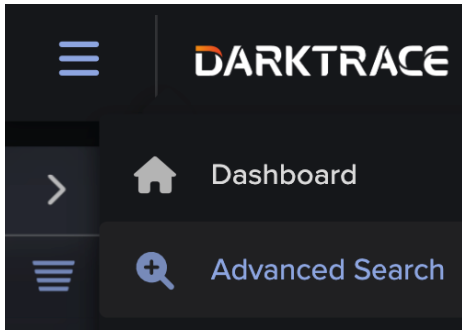
The connection UID can also be used to pivot from Advanced Search to the Threat Visualizer.



By copy/pasting the UID or by clicking the icon to the right of it, the connection can be located using the Omnisearch bar.

Let's now explore Advanced Search without using an Event Log as a starting point.

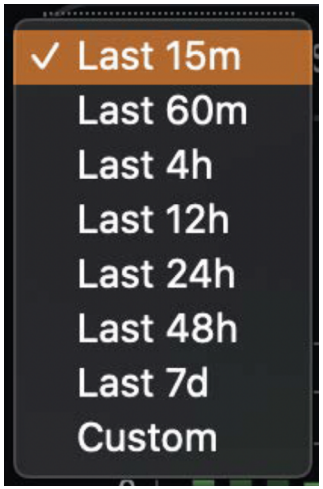
1. The Advanced Search module can be launched by selecting the **Advanced Search** icon under the **Menu** button on the home page.



Alternatively, use a browser window tonavigateto https://<servername>/advancedsearch

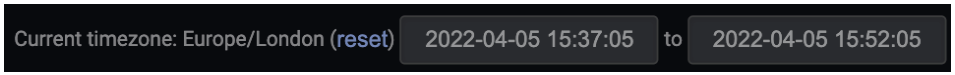
2. By default, Advanced Search displays the last **15 minutes** of captured network activity.

Click **Last 15m** to the left of the search bar to open a drop-down menu. Select a timeframe and click Search to change the time window presented in the Advanced Search graph.



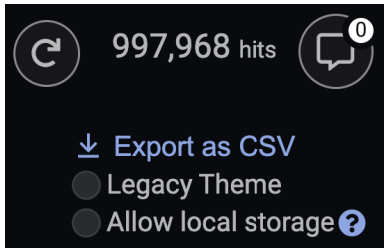
The last 7 days (**Last 7d**) can be a valuable option for smaller networks to gain a visual understanding of the normal flow of traffic over a week.

3. The **current timezone** displayed at the top of the Advanced Search page correlates to the timezone set in the Threat Visualizer. The restriction of date and time values make it easy to search within a specified date range.



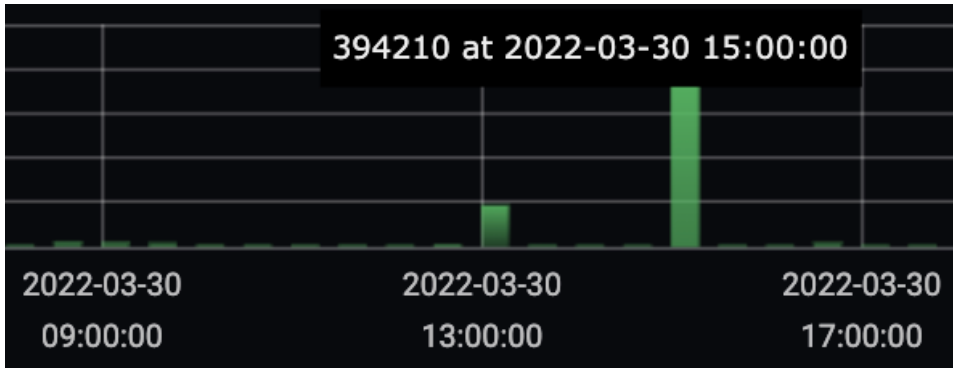
Note: The grouped by auto drop-down menu to the right of the timezone can be used to group the bars by seconds, minutes, hours or days.

4. The total **number of results (hits)** for the chosen timeframe is presented in the top right-hand corner of the interface.



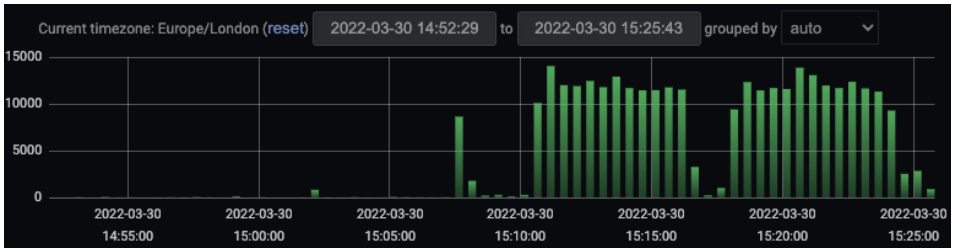
Note: As network data is constantly being recorded, the total number may slightly change for every search or reset.

5. The **graph** located underneath the search bar indicates the **number of matching events** over certain periods. Hovering over the green bars reveals how much data is available in that timeframe.



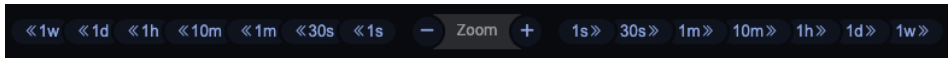
6. **Click and drag** over the green bars to **zoom into** the graph and **adjust the timeframe**. Repeat this as many times as necessary to hone in on spikes in activity.

This can look at data over a number of seconds rather than minutes/hours/days. The events in the Advanced Search logs automatically update to reflect the graph.



Note: The graph can be made taller by dragging it down from underneath the x-axis.

7. Additional **navigation** buttons are included to facilitate navigating the display in time steps of a second up to a week.

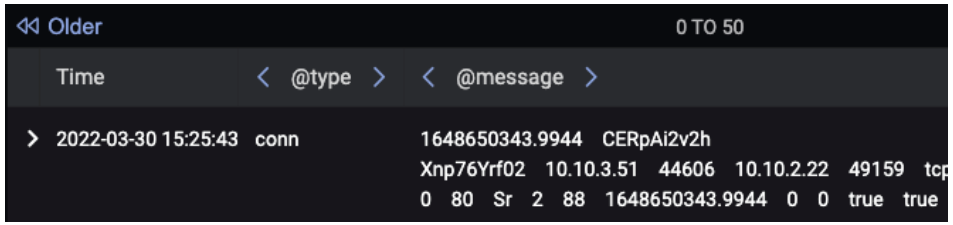


8. The results displayed in Advanced Search can be **reset to display the default view** of the last 15 minutes in one of two ways:

   a. First, notice the **rotating arrow** to the right of the search bar. Click this to **reset** the search results on the page.

   b. Alternatively, click the **Darktrace logo** in the top left-hand corner. This will reset results and is equivalent to the home page of the Advanced Search interface.

9. Underneath the graph, the **most recent 50 events** are displayed in the table. Click the **Older** at the top or bottom of the page to review more results.



10. The main results are broken up into three columns: **Time**, **Type**, and **Message**.

    a. Note the **timestamps** on events are the **start time** of connections. However, events are not generated until the connection has finished.

    b. The **type** represents the **event type** for the message. This includes conn, http, ssl and dns.

    c. The **message** field contains **all content** which is broken down into unique fields which can be searched in the search bar.

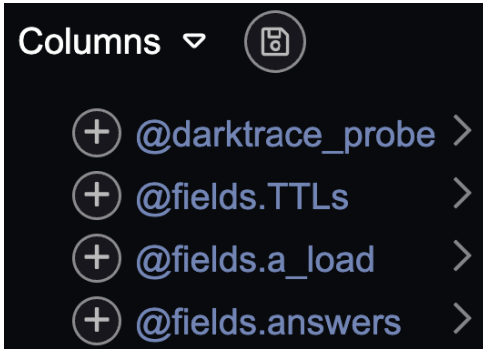
11. The results on the page can be filtered by inputting a query into the search bar and applying it. Click the **Search** button to view the results.

12. Clicking on a row will expand the details for each record, split into three columns: **Field**, **Action** and **Value**. Review the different fields available.

Note: Hovering over any entry in the Field column reveals extra information about the meaning or function of the entry.

Top Tip

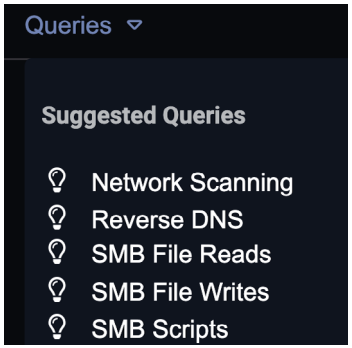
The headings at the top of the table can be customized based on the fields presented in the **Columns** list, on the left of the interface. Clicking the plus symbol will add the field as a column. While the @type and @ message columns will be replaced by selected fields, the Time column will always remain.



Selecting one of the **Queries** at the top will automatically populate the search bar based on the subject of the query. This can greatly facilitate the use of Advanced Search.

The Columns list can be hidden by clicking the **left facing arrow** located under the search bar.

Save you selection as a template by clicking the **save button**. This will use local storage.



13. Notice the three icons beside every field. Choose an event to carry out the following:

a. Click the **equals** symbol for @fields.source_ip.

@fields.source_ip:"10.1.1.10"

The field and corresponding value are automatically appended to the search bar. If an existing query is already populated in the search bar, this will apply the AND operator before the selected field. The results are restricted to only display events from the selected source, which is a useful way to quickly filter results.

b. Reset the search and click the **not equals** symbol beside @fields.dest_port.

NOT @fields.dest_port:"80"

Now, a NOT Boolean operator has been applied with this field in the search bar. If the search bar is not empty, the stop symbol will apply an AND NOT instead. This example will display all results where the destination port is not 80.

c. Click the **pivoting arrows** icon for the @type field.

@fields.source_ip:"10.1.1.10" AND @fields.dest_ip:"10.2.1.10" AND @type:"dns"

This removes any existing queries from the search bar and automatically populates the search bar with the source and destination IP and type for the selected record.

14. Long queries can easily be built in the search bar by combining AND, OR and NOT **Boolean operators**. Parentheses can group query strings to control Boolean logic and make queries easier to read.

OPERATOR	DESCRIPTION	EXAMPLE
AND	Search for multiple conditions.	@type:http AND @fields.dest_port:80
NOT	Exclude results with this condition.	@type:http AND NOT @fields.dest_port:80
OR	Search for one condition or the other.	@type:http OR @type:ssl
*****	Match any number of characters.	@fields.server:*.darktrace.com
?	Match a single instance of any character.	@fields.version:TLS1.?
" "	Exact string search. Useful when you want to use a wildcard as a normal character.	@fields.uri:"/status?hostname=example.com"

15. For example, **long queries** can easily be built using these Booleans:

@type:"http" AND (@fields.method:"GET" OR @fields.method:"POST") AND @fields.referrer:*download*

Note: All Boolean operators must be written in uppercase. Otherwise, they will be treated as a search term in the message field.

16. Searching on field values is **case sensitive**, so the case must match the value in the returned field. The following search returns no results because 'CONN' is uppercase:

@type:"CONN"

Advanced Search Navigation

17. If **no operator** is applied to the query, a Boolean **AND is automatically inserted** between the fields:

    @type:"http" @fields.method:"GET"

18. The **period (full-stop)** character is not considered the end of the word or sentence. This means that full domains can be searched for using the period as a character.

19. Searching for **"darktrace"** will not find results for www.darktrace[.]com, as this performs an exact search. Typing in **darktrace** without quotation marks will return results for domains and subdomains but may also return any other field that contains that term.

20. Advanced Search also supports **Regular Expressions** so the following will find HTTP results for www.darktrace[.]com:

    @fields.host:/w{3}\.darktrace\.co.+/

    Note: Notice that in the example Darktrace website has been defanged, i.e. rendered ineffectual so it cannot be accessed by clicking on it. As defanged URLs will not work in an Advanced Search query, make sure to remove the brackets.

21. Advanced Search supports a powerful query syntax which builds on the open-source **Apache Lucene 4** Query syntax.

    Searches over a **long period** will take longer to complete. Searches that take too long will be **aborted** to prevent a negative impact on the performance of other parts of the system.

    Restricting the scope of the search by time or field will help the search return results more quickly.

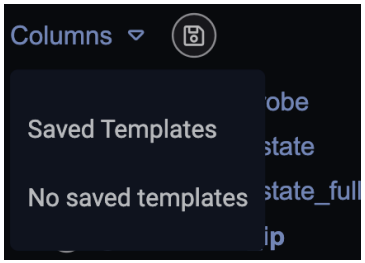
22. Advanced Search data is stored in a '**rolling buffe**r' that typically retains ~30 days worth of data. This can vary greatly depending on the environment.

Continue your learning with our dedicated video:
6: Advanced Search - Basic Searching

Saving Queries and Advanced Search Configurations

There are multiple options within Advanced Search which allow the user the option to save queries, fields and take notes. All of these options require local storage, so this is not recommended for shared workstations.

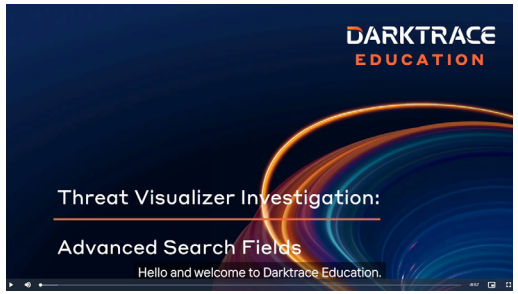
Saving queries can allow for easy access to commonly used searches. This can be achieved by populating the search bar and clicking the save icon to the right of it.



Configurations of the Columns list can be saved so as to display columns of useful information in the Advanced Search table. Simply add the relevant fields and assign a template name to quickly reapply this to the results table in future.

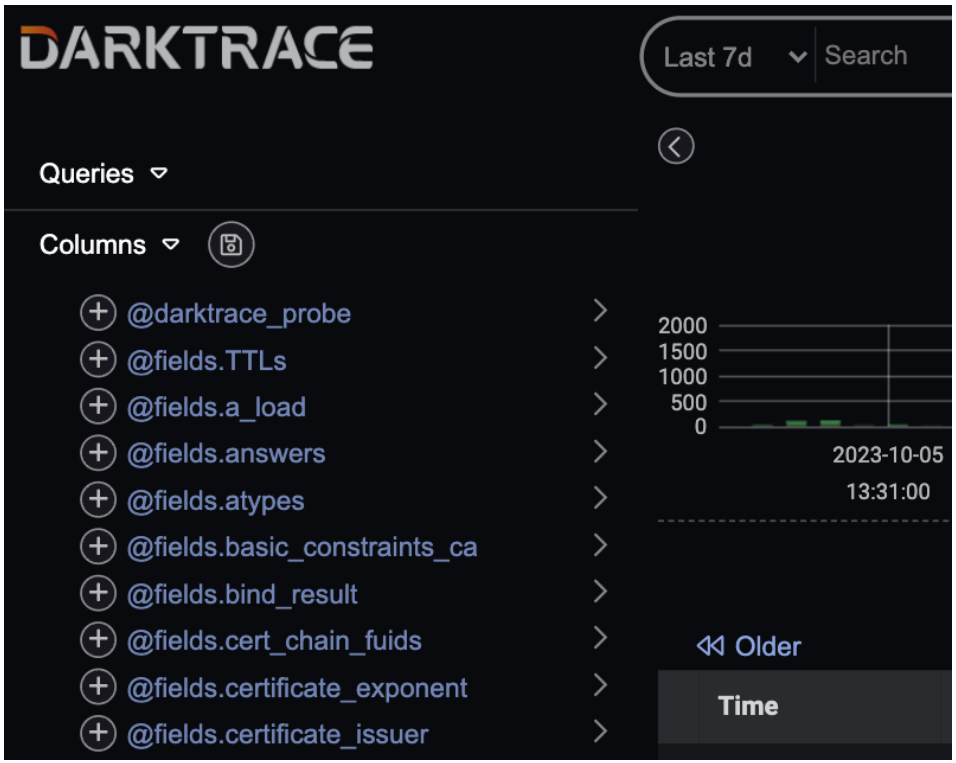
Notepad is a useful feature that is not limited by queries or column arrangements and can be utilized by clicking the speech bubble in the top right of the interface.

Advanced Search Fields

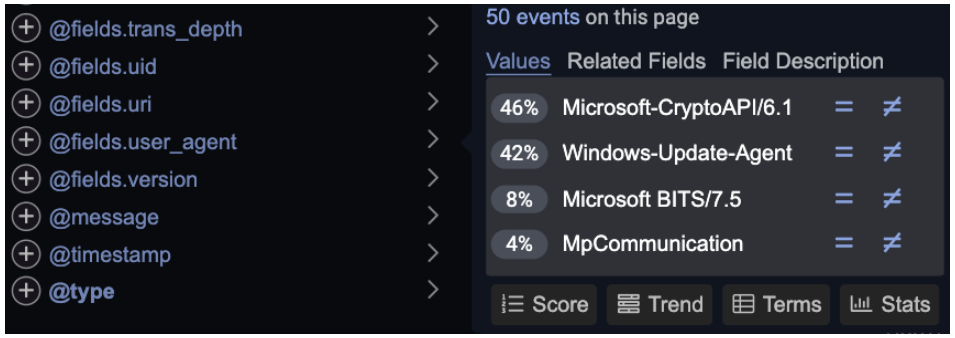


Continue your learning with our dedicated video: 7: Advanced Search - Fields

1. The **Columns list** on the left of the Advanced Search interface displays all the **fields** that are present in the **current page of the 50 events**.



The fields may dynamically change by looking at older events and different options may be displayed as particular events and content are searched.



Clicking the **field itself on the Columns list** displays additional options. A useful dialog box reveals up to 5 of the most frequently found results for a field value in the 50 listed results currently displayed on the page with a percentage breakdown for each.

a. Using the **equals/not equals** icons next to the selected field at the top of the window will filter Advanced Search based on whether the field exists or does not exist.

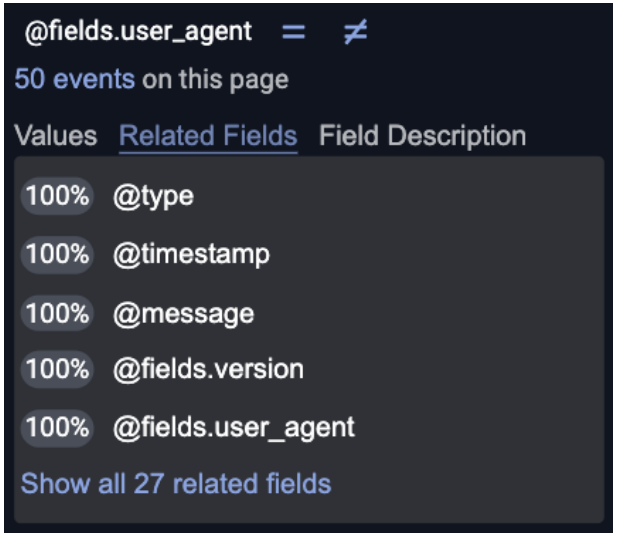
Note: Some of the values may read "blank". This value implies that, on the current page, there are a percentage of entries which do not contain the selected field. By selecting the "blank" value, the field will be prepended with NOT_exists_ in the search bar.

b. The **individual values** can be appended to (**AND**) or excluded from (**NOT**) queries in the search bar by using the **equals** and **not equals** icons respectively.

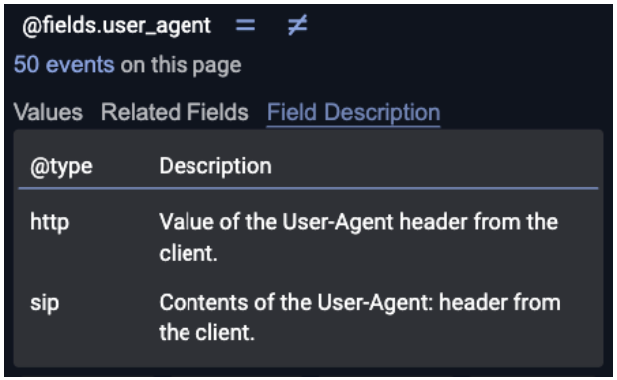
c. Clicking on a **value** within the pop-up window will highlight any events on the page in green where that field value exists. This can help identify events without the need to filter out other surrounding events.

Note: This process needs to be repeated per page.

2. Notice the **Related Fields** tab. Click on this to display similar fields to the selected field. Click **Show all** to view any other related fields. Clicking any of these has the same effect as clicking the + icon to the left of the listed fields – it will apply them as headings to the table of events, thereby only displaying the selected information.



3. A short description of the field can also be read by clicking on the **Field Description** tab.



4. Selecting the **Score**, **Trend**, **Terms** and **Stats** provides further analysis.

   a. Clicking **Score** for a chosen field will rank all results in descending order based on their count/percentage over the selected time frame.

      The limitation of this is it will only score the 10,000 most recent results and will only present the top 100 results. For example, the score produced from @fields.version reveals the different TLS versions observed on the network.

   b. Clicking **Trend** will perform analysis on the chosen field which shows the count, percentage and trend.

      This trend is a rate of change for each individual value, i.e., if the value is more or less popular in the selected time frame, denoted in red and green for decreases and increases in popularity respectively.

   c. Selecting **Terms** will aggregate the results for a chosen field and visually represent them using a pie chart. Similar to the Score function, it also gives the count and percentage for each result.

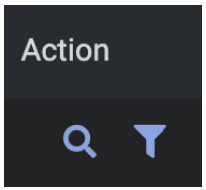
      Empty values are also displayed in the breakdown. However, while Terms can analyze more than 10,000 results, they are limited by the time frame of 48 hours.

   d. Finally, clicking on the **Stats** button will give a statistical breakdown of numeric fields only. Included in this breakdown are the count, minimum, maximum, average and sum.

5. If there are **more than 10,000** results for a statistical analysis, click **Analyse 100k** results to return a more accurate result set for the selected time period.

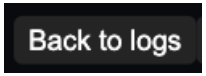
   Note: For small appliances, the Analyze 100k results option will not be available.

6. At the end of every row of one of the statistical analysis methods, there are two **actions** available, denoted by the magnifying glass and filter icons.



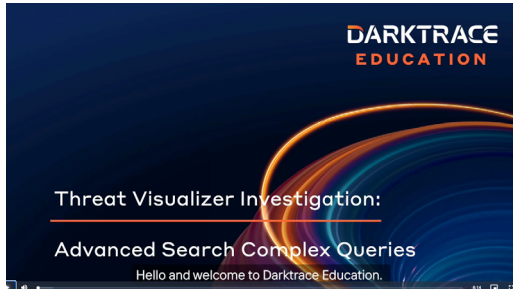
   Both buttons will append the value to the search bar. However, the **magnifying glass** will perform a search and present the logs, while the **filter** will keep the statistical analysis page open.

7. To return to the Advanced Search logs and view rows of events, click the **Back to Logs** button.



8. It is possible to **copy a field UID value** and paste it into the Threat Visualizer. Alternatively, expand the entry, navigate to @fields.uid and click the link icon to the right of the UID to open a new Threat Visualizer tab showing the connection. Both options populate the Omnisearch bar and can provide additional graphics about the events.

TCP Connection States in Advanced Search



Continue your learning with our dedicated video:
8: Advanced Search - Complex Queries

1. Within Advanced Search, perform a search for **@type:"conn"**.

2. Open the Score dialog window for the **@fields.conn_state** field to review TCP Connection states.

   The conn_state reveals the results of the connections. This is a good way to find out more about a connection when investigating network anomalies.

3. **Compare your results** to the table on the right. The **connection state** is expected to be **SF**. Differing connection states should be the subject of review.

4. Review the connection history using the **@fields.history** filter. Once again, a normal termination of **ShADdAFaf** is expected.

   Otherwise, the returned state could provide useful information. For example, a connection state of SO or a history of SR could represent a port scan on your network.

STATE	MEANING	EXPECTED HISTORY
SO	Connection attempt (SYN) only – no response	S
S1	Established	ShA
SF	Normal termination	ShADdAFaf
REJ	Rejected	Sr
S2	Established and originator sent FIN, no FIN|ACK from Responder	ShADdF
S3	Established and responder sent FIN, no FIN|ACK from Originator	ShADdf
RSTO	Established, Originator sent an RST	ShADdR
RSTR	Established, Responder sent an RST	ShADdr
RSTOS0	Originator sent SYN followed by RST with no SYN|ACK from Responder	SR
RSTRH	Responder sent SYN|ACK followed by RST with no SYN from (supposed) Originator	hr
SH	Originator sent SYN followed by FIN with no SYN|ACK from responder (half open)	SF
SHR	Responder sent SYN|ACK followed by FIN with no SYN from Originator	hf
OTH	No SYN seen, just midstream traffic that was not closed later	Dd

Advanced Search Exercises

If you already have access to the Threat Visualizer, carry out the following steps from your own interface in order to test your knowledge on how to use the Advanced Search page. You can keep a record of your attempts by filling in the text boxes and saving the manual. *If you need help or if you want to check your method, click on the tooltip icon to reveal where you can find this information. Click on an answer to hide it or use Show All / Hide All.*

1. What query might find any SSL queries to eBay in the last 60 minutes?

2. What query would you use to find all SSH and RDP connectivity originating from your IP address in the last 7 days? *If your machine is not on the network, select a different host.*

3. What query can return the failed Kerberos Type events over the last 7 days?

4. How might you find the SHA1 hashes of all the EXE files in the last 48hrs? *Remember the fields down the left of the interface will change depending on what you search for.*

Show All Answers Hide All Answers

5. How can you find all events for a connection? Is there a shortcut?

6. What query would you use to find the user agent and the method of the last HTTP request sent by your machine? *If your machine is not on the network, select a different host.*

7. What query locates connections to external IP addresses which use the FTP protocol?

8. Describe how you might locate all internal DNS servers.

Advanced Search Summary Test

DARKTRACE
Essentials Certification

This page will test your knowledge and check your understanding of the Advanced Search 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.*

1. From the main menu, what is the default time period in Advanced Search?

- [ ] The last 15 minutes
- [ ] The last 30 minutes
- [ ] The last 60 minutes

2. Which symbol will replace any existing query rather than append one?



3. True or False: It is possible to save search queries.

- [ ] True
- [ ] False

4. Which operator will you use to look for an exact word?

- [ ] ?
- [ ] " "
- [ ] *

5. Which option will NOT display information about more than 50 results?

- [ ] By exporting the results as a CSV file
- [ ] By using filters
- [ ] By using either Score, Trend, Terms or Stats

6. Which of these TCP connection states is for a failed connection?

- [ ] SF - Normal Termination
- [ ] REJ - Rejected
- [ ] S1 - Established

Clear All Answers

5. Further Investigation Techniques

Following the investigation of a Model Breach in the Threat Visualizer and Advanced Search there are a few additional features that may be useful for sharing information with colleagues and taking remediation steps. In this chapter, let's explore creating a packet capture, commenting, acknowledging and sharing information.

Creating a Packet Capture

Continue your learning with our dedicated video: 9: Packet Capture

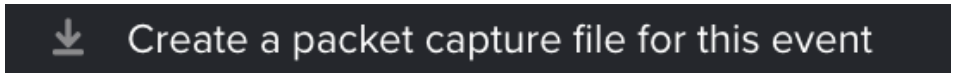
Through the Threat Visualizer interface, packet capture files can be downloaded and examined in more detail. The amount of PCAP data stored significantly depends on the type of network traffic monitored, but typically ranges from three to seven days. PCAPs are created on a per user basis, so are not visible for other users of the system unless shared in other ways.

What is a Packet Capture?

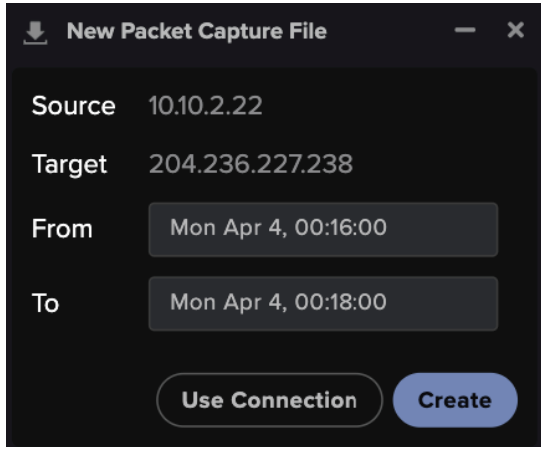
Taking Packet Captures refers to the action of capturing Internet Protocol (IP) packets for analysis by creating copies from a given point in the network. These Packet Capture files are often saved in .pcap format and can be viewed in a variety of applications.

Reviewing PCAPs allows users to examine network traffic which can be useful for network administrators but can also be abused by threat actors attempting to steal sensitive data. To analyze packets, basic network knowledge is required; the files consist of a payload (data transferred) and headers containing information such as source/destination.

1. Select an alert and view its Breach Log. Click the downwards arrow located on the left of a connection. Select the **Create a packet capture file for this event** option.



2. A **New Packet Capture File** dialog box opens.

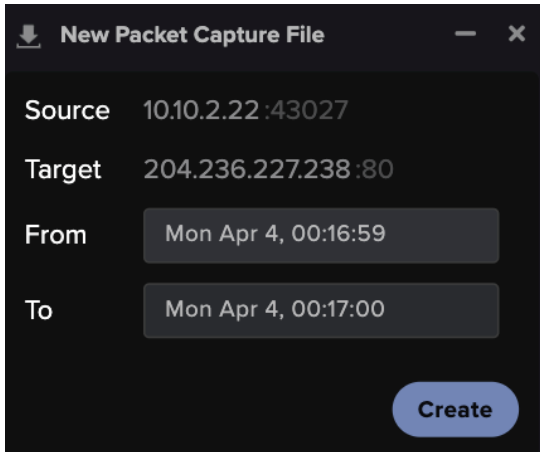


   a. Click **Create** to create a default time period packet capture or change the From and To times.

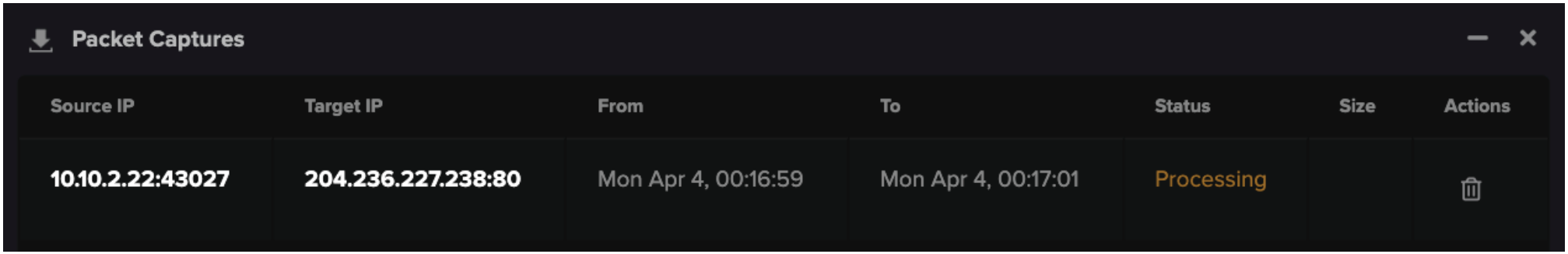
Note: For testing, keep the duration as 2 minutes or less, as creating the packet capture can be a resource intensive exercise.

   b. Alternatively, when creating a packet capture for an event, notice the **Use Connection** button.

When clicked, it will specify the source and destination ports and update the From and To date and time stamps to the connection selected. Click **Create**. It may take a few minutes or longer to create the packet capture file, depending on the duration selected.

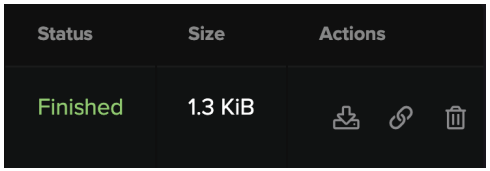


3. The **Packet Captures window** will automatically open and should show the newly created PCAP **Processing**.



Note: This window can also be opened by using the Threat Visualizer main menu and choosing Packet Captures.

4. Confirm the process has **Finished** and notice a range of icons to the right of the packet capture.

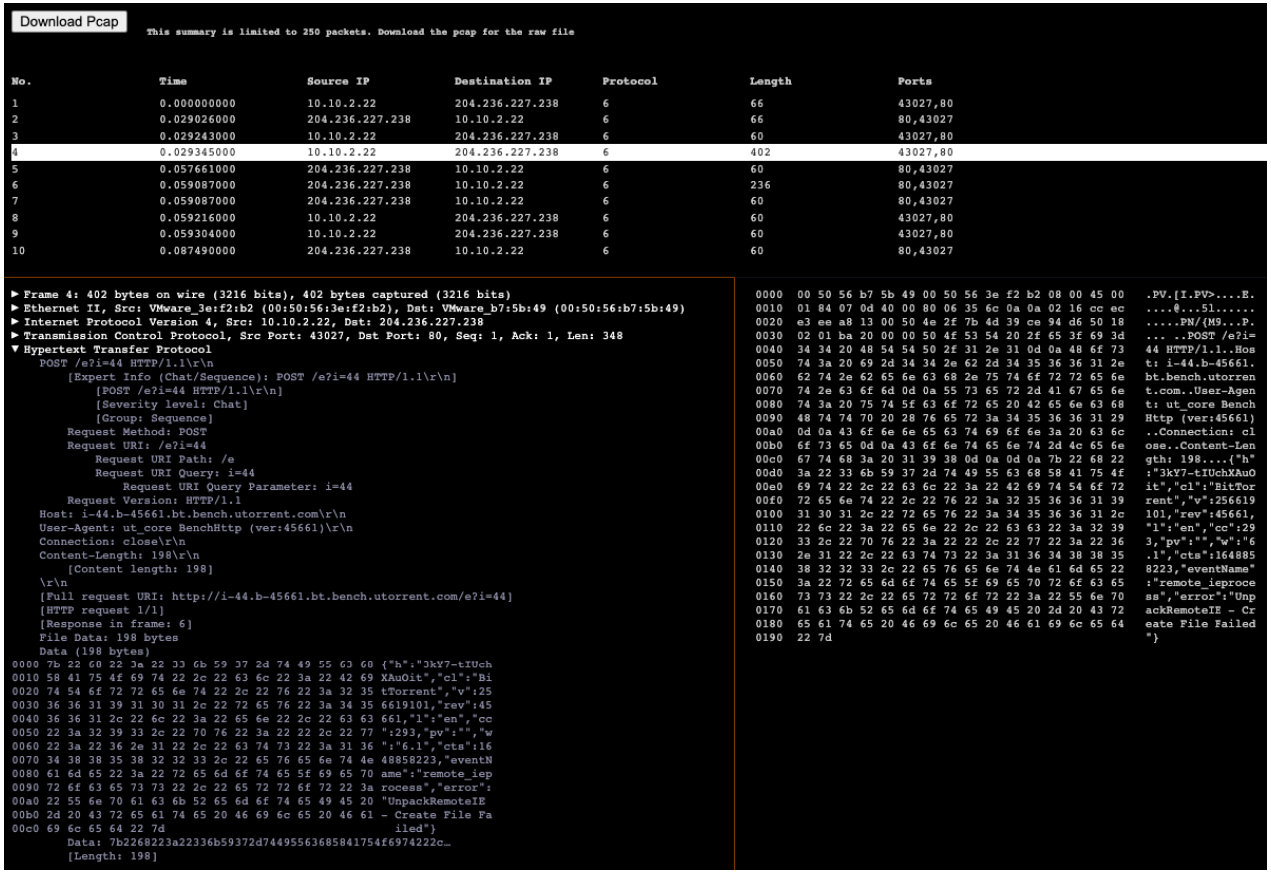


   a. The first icon allows the user to **download** the PCAP file so it can be viewed in another program, such as Wireshark.

   b. The second option, denoted by a **link** icon, will open up click the **View this packet capture file in the browser**.

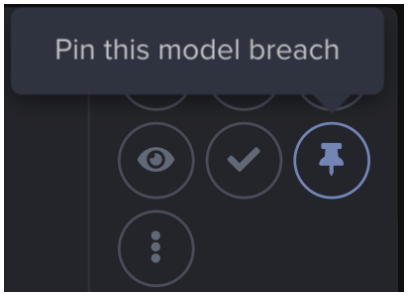
      This will open automatically formatted results in a new tab in an application called Darkshark. Click on the packet frames to view the full details.

   c. Finally, the **trashcan** icon means a packet capture can be **deleted**.

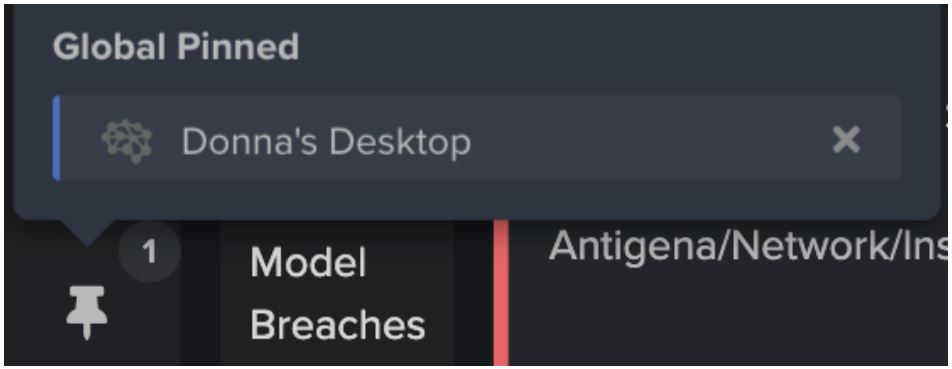


Additional Breach Log Features

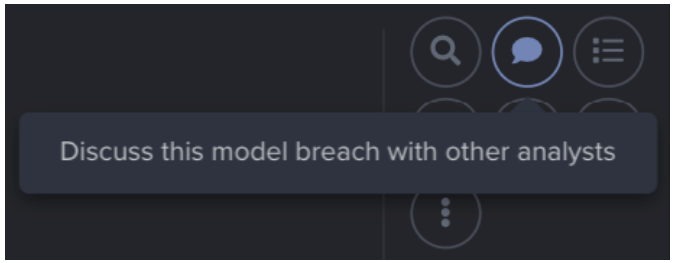
1. Next to the Model Breach ID, notice a **pin icon**. This icon allows Model Breaches to be pinned below the Threat Tray, allowing for further investigation at a later time.



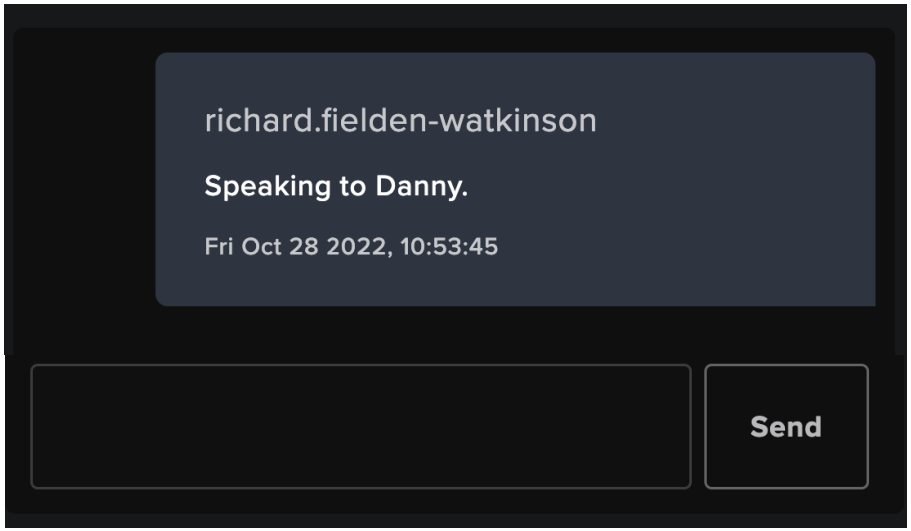
To open a pinned breach, click the pin icon in the lower left of the screen and select the breach.



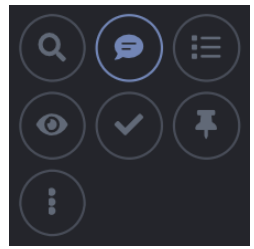
2. Adding **comments** lets analysts check what investigation work has previously occurred on the breach and allows them to communicate with each other.



a. Click the **speech bubble** to open the comment window, type a message and click **Send** to save your changes.



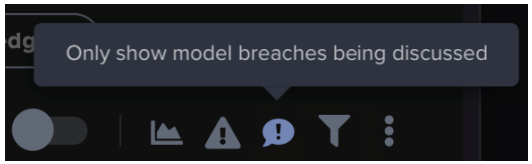
Note: The username of the operator is displayed at the top of the comment so it can easily be tracked by the team.



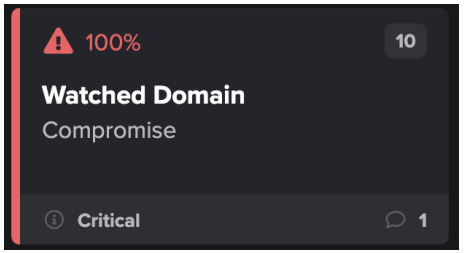
b. The speech bubble in the Breach Log changes and **lines appear** to indicate the presence of a comment for the selected Model Breach.

Top Tip:

Once a breach has a comment, an additional button appears in the Breach Log. This button can be useful to the operator or other users to only view breaches that have comments.



c. Comments are automatically appended to the Alert in the **Threat Tray**. This can be seen by viewing the speech bubble in the bottom right corner of the Threat Tray entry. The number indicates how many comments have been applied.

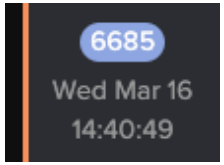


Note: To easily locate breaches with comments, try the "most discussed" filters to sort the Threat Tray.

Sharing Model Breaches

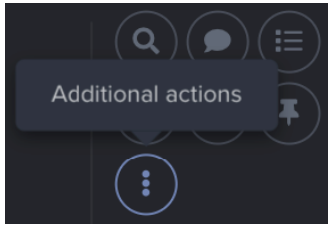
Pinning a Model Breach will only pin the breach for the operator, not their colleagues. In order to share Model Breach information with colleagues, there are a few methods that can be employed. As described above, comments can be utilized because these are visible for all users with access to the interface.

However, if we want to share information via other means, we can copy the details to the clipboard. This can be achieved for a single event, or for an entire Model Breach.



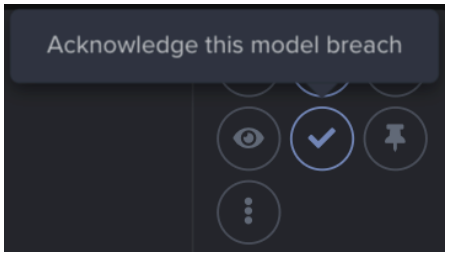
To share the Model Breach URL, click the **Model Breach ID**. This will copy a URL to the clipboard of the following format: <servername>/#modelbreach/<id>

Alternatively, the entire Model Breach details, as seen in the Breach Log, can be copied by utilizing the **Copy to Clipboard** option in the Additional actions.



3. Often, at the end of an investigation it can be useful to let colleagues know what analysis has occurred via the comment function, but also **hide** it from the interface to ensure that the same incident is not analyzed twice. To hide breaches from the list of Model Breaches in the Breach and Threat Tray, they can be **Acknowledged**.

a. The Breach Log window includes the **Acknowledge this model breach** function depicted by the tick. When a breach is acknowledged (hidden), the number of breaches for each alert is automatically reduced by one.



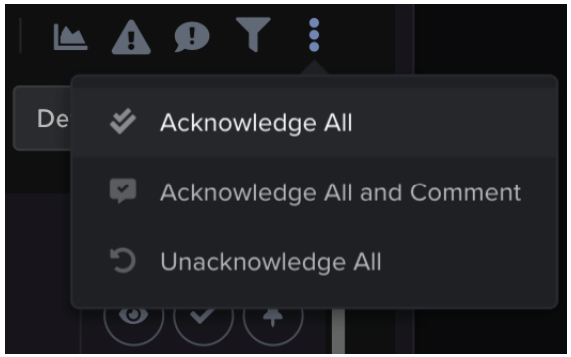
b. An acknowledged breach can be revealed by using the toggle at the top of the Breach Log.

Toggle to **Acknowledged** to show the hidden breach.

c. To show the hidden alert in the Threat Tray, use the Filters menu and turn on the **Include acknowledged** toggle.

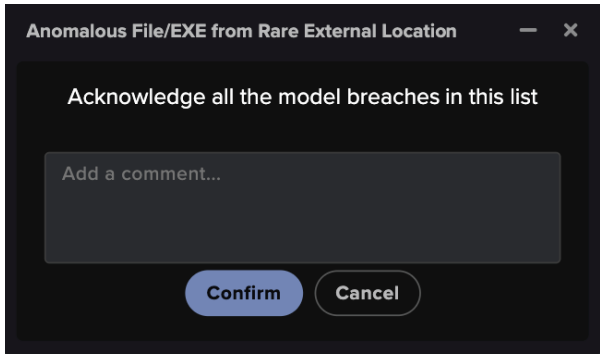
4. It is possible that all alerts of one type can be explained and therefore hidden.

Notice the icons in the top right of a Breach Log. The additional options contains three **acknowledge related options**.

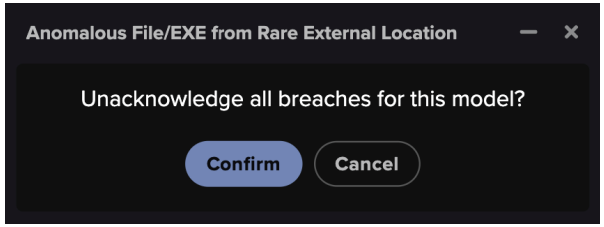


a. **Acknowledge All** will automatically hide all Model Breaches in the Breach Log without impacting on future alerts.

b. However, **Acknowledge All and Comment** combines the two aforementioned features. This feature is useful for marking breaches in bulk as read and providing a reason so that other users can see why they have been acknowledged.

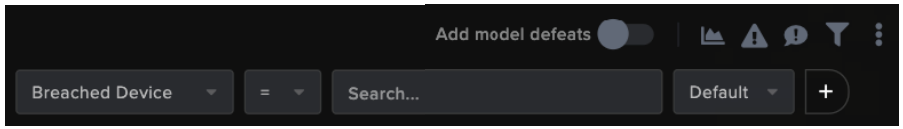


c. Finally, if some/all breaches have been acknowledged, this can be undone by selecting the **Unacknowledge All** button and clicking Confirm in the resulting dialog.

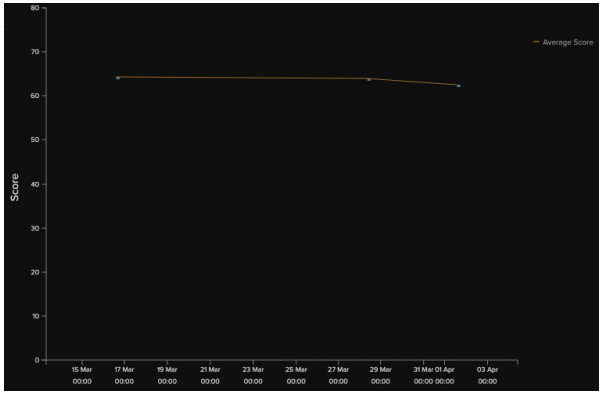


5. After reviewing a single Model Breach, it may be useful to **compare** it to other breaches occurring on the network. Using the Breach Log it is possible to **filter** the results or **expand the scope** of research.

a. In the top right of the Breach Log, the **funnel** icon allows a user to **Add/Remove custom filters**. This will display a new dialogue at the top of the Breach Log which provides a drop-down menu to aid the creation of filters and restrict results



b. To explore the trend of Model Breaches, click the graph icon to **View breaches graphically**. The graph plots relevant breaches over time against the threat score. Device names can be obtained by hovering over each data point.



Note: This is similar to viewing all breaches graphically in the Threat Tray, as depicted below. Simply select the graph icon from the Threat Tray options to open this alternative global view of breaches.

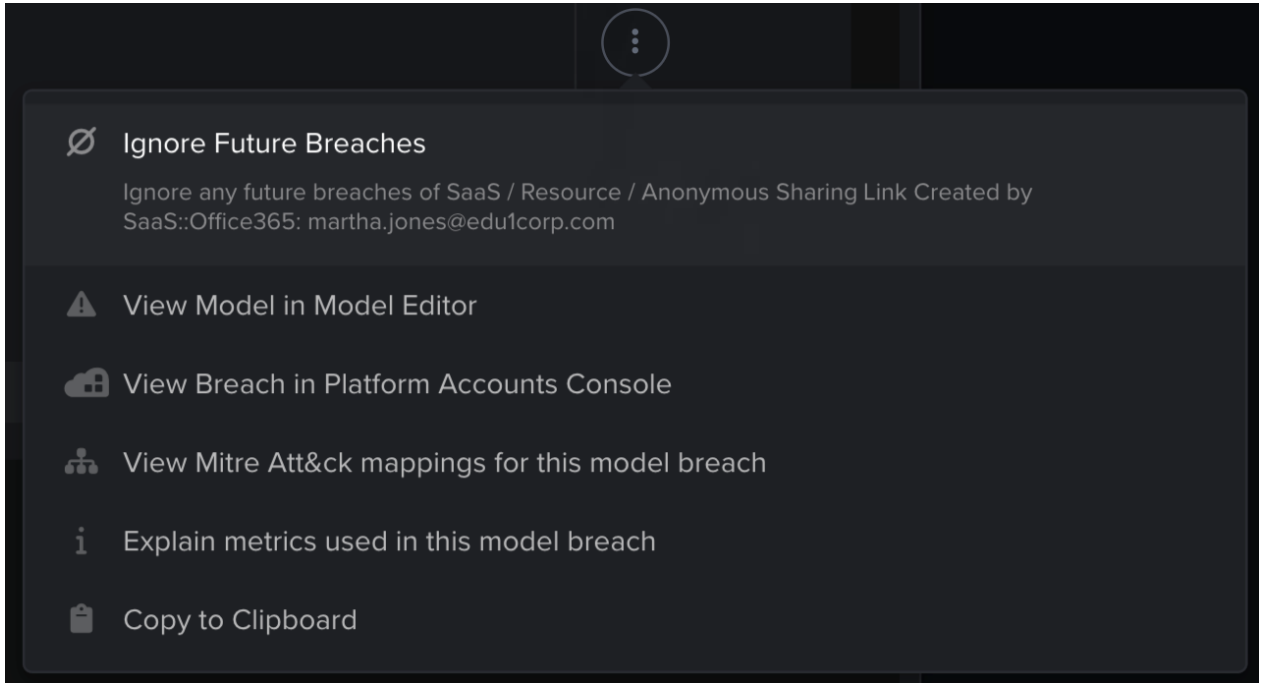
6. Clicking on the last icon with the **three dots** will open more advanced options:

   a. The **Ignore Future Breaches** option adds the device to a list, preventing it from ever triggering another model breach for the model.

   b. The **View Model in Model Editor** icon opens the Model Editor interface focused on the model.

   c. The **View this model breach in the Platform Accounts Console** icon opens the equivalent model breach in the Platform Accounts Console to continue investigation there.

   d. The **View MITRE ATT&CK mappings for this model breach** option opens a window listing the mapped techniques. This mapping is a valuable tool to understand coverage and for teams with internal playbooks for how to address each technique.



   e. To understand what metrics and filters are looking for, click the **Explain metrics used in this model breach** icon to review definitions written by Darktrace analysts for metrics and filters relevant to the model breach.

   f. Finally, the **Copy to Clipboard** option copies the breach details to the clipboard including the device, the model breach display fields and a link to the model breach.

Investigations Summary Test

This page will test your knowledge and check your understanding of the Further Investigation Techniques 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. When creating a Packet Capture, what will the Use Connection option do?

- [ ] You can select specific IPs and Ports
- [ ] It will focus on the source and destinations IPs
- [ ] It will specify the source and destination ports

2. True or False: Packet Captures can be opened via the Darkshark application.

- [ ] True
- [ ] False

3. How do you know if a breach has been commented on?

- [ ] The breach will be brought to the front of the Threat Tray
- [ ] Lines will appear in the speech bubble icon
- [ ] There is no way to know if it has been commented on

4. What does Acknowledge this Model Breach do?

- [ ] It will prevent the Model from being breached in the future
- [ ] It will analyse the selected Model Breach
- [ ] It will hide the selected breach from the Threat Tray

5. Which of the below is NOT a way to share the selected Model Breach?

- [ ] Pinning the Model Breach
- [ ] Clicking Model Breack ID
- [ ] Selecting Copy to Clipboard

6. How can you prevent a Model from breaching?

- [ ] Using the Acknowledge this Model Breach option
- [ ] Using the Add Model Defeats option
- [ ] You cannot prevent a Model from breaching

Clear All Answers

6. Darktrace Services

Darktrace Mobile App offers the possibility to deal with breaches and incidents on the move. Furthermore, Darktrace offers services which can assist in outsourcing some SOC responsibilities to Darktrace Analysts.

6. Darktrace Services

Darktrace has a number of additional services on offer. These include 24/7 Proactive Threat Notifications (PTN) and access to 24/7 Ask the Expert (AtE). In these cases, no additional software or downloads are required as these services can be accessed directly through the main interface.

Proactive Threat Notifications

The Proactive Threat Notifications are part of Darktrace's round-the-clock SOC, which is comprised of expert analysts located around the globe, covering all time zones.

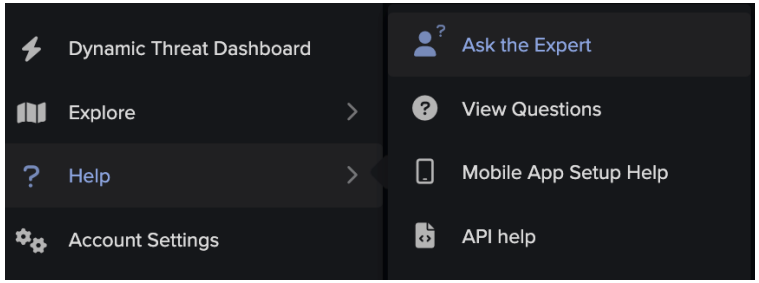
If you have call-home enabled and you are signed up for this service, Darktrace Analysts will review any breaches in your Threat Visualizer that fall under the Enhanced Monitoring category. They will consequently notify you if they find anything significantly suspicious via email, text or a phone call. Darktrace can offer real time advice and assistance to help you tackle live attacks.

These PTNs, provided by one of our analysts, will include a short summary of the threat in question, the breach device and the Model Breach ID, effectively arming you with the appropriate knowledge before investigating the breach in your Threat Visualizer Interface.

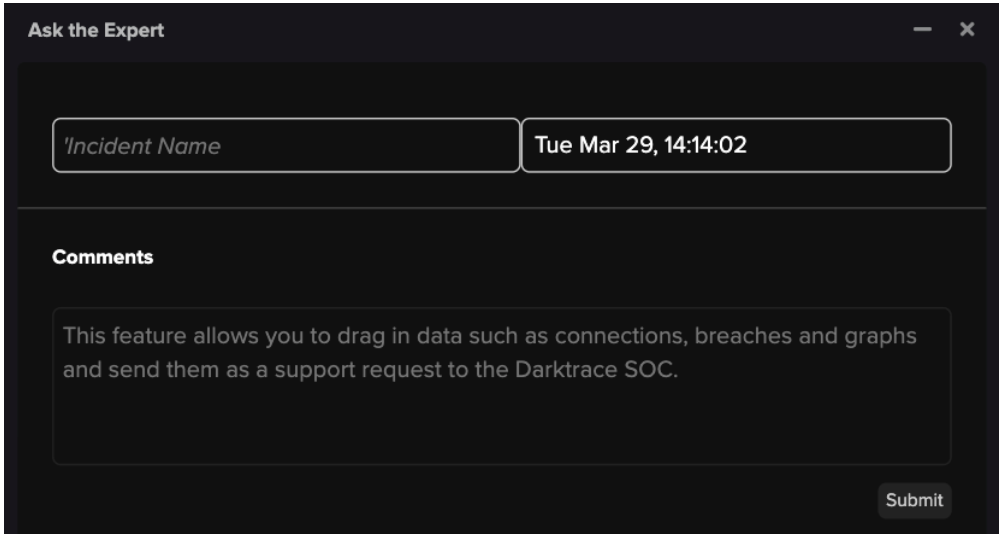
Ask the Expert

This service allows you to contact Darktrace experts about any live threat, investigation or general query. Our teams can show and tell you what to do and signpost you to resources and useful information.

To access this feature, navigate down to Help in the Threat Visualizer main menu and select Ask the Expert from the submenu.



Doing so will open up a window, allowing you to type in information which will be sent to our cyber security experts.

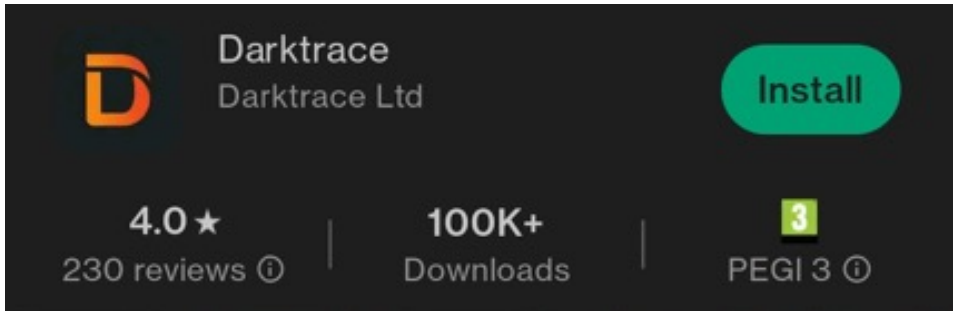


Alternatively, you can create Ask the Expert tickets through the Customer Portal in the same way as Support tickets.

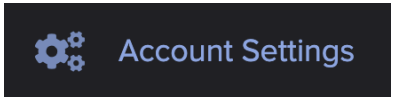
Darktrace Mobile App

The Darktrace Mobile App, available for iOS and Android, allows users to easily access Darktrace Alerts when they are on the move. In order to associate the Darktrace Mobile app with an existing Darktrace deployment, the Threat Visualizer must be authorized to send alerts.

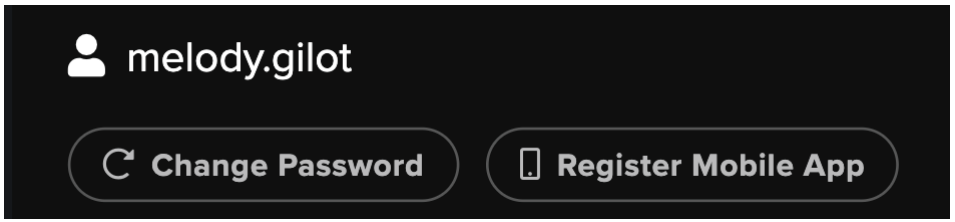
1. On a smartphone, open the app store and search for Darktrace. The Darktrace iOS app is available on the App Store and the Android app is available on Google Play. **Download and open the Darktrace app**.



2. Navigate to **Account Settings** from the main menu.



3. Click **Register Mobile App** at the top of the dialog.

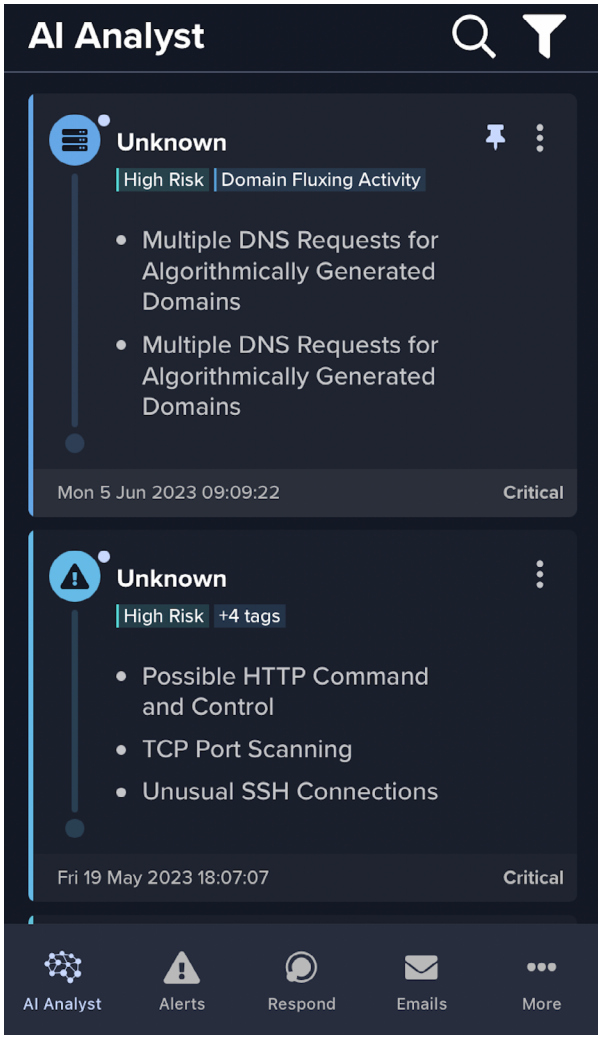


4. A **QR code** will open in a dialog on the Threat Visualizer.

AI Analyst

This screen displays AI Analyst incidents.

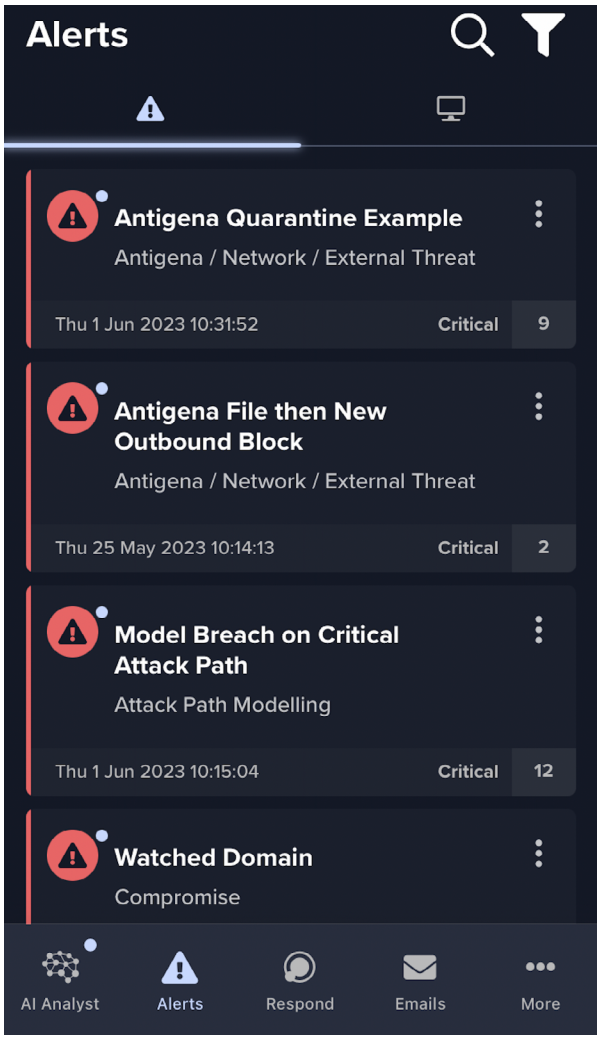
- Tap the icon to pin an incident.
- Swipe left to acknowledge an incident.
- Tap to review Cyber AI Analyst incidents:
  - Open the left tab to view incident events and information.
  - Swipe left on an incident event to acknowledge it.
  - Open the middle tab to view incident devices.
  - Open the right tab to view incident comments.
  - Tap the pin icon to pin or unpin the incident and its events.
  - Tap the tick icon to acknowledge or unacknowledge all events for this incident.
  - Shre a link to the Mobile App incident.
  - Read summary of events. and view attack phases involved.
- Drag down to refresh.



Alerts

This page lists Model Breaches.

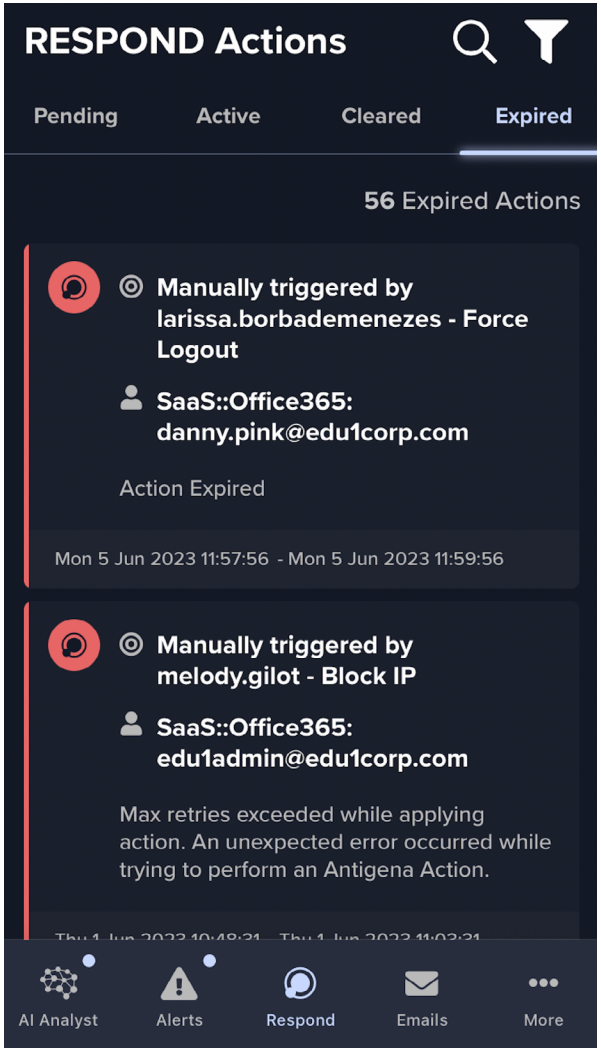
- Tap to modify the alerts page filter settings
- Open the left tab for model breaches by model
- Open the right tab for model breaches by device
- Tap on the more icon to pin or mark read a model or device
- Drag down to refresh and reveal a search bar.
- Review Model and Breach details.
  - Swipe left on a model breach to acknowledge it
  - Swipe left and right to view other model breaches
  - Swipe up from the bottom to view quick actions
  - Open the left tab to view a summary
  - Open the middle tab to view events within the model breach
  - Open the right tab to view related RESPOND actions
  - Tap on an event to view details



RESPOND

The RESPOND Actions screen displays Active, Pending, Cleared and Expired Actions.

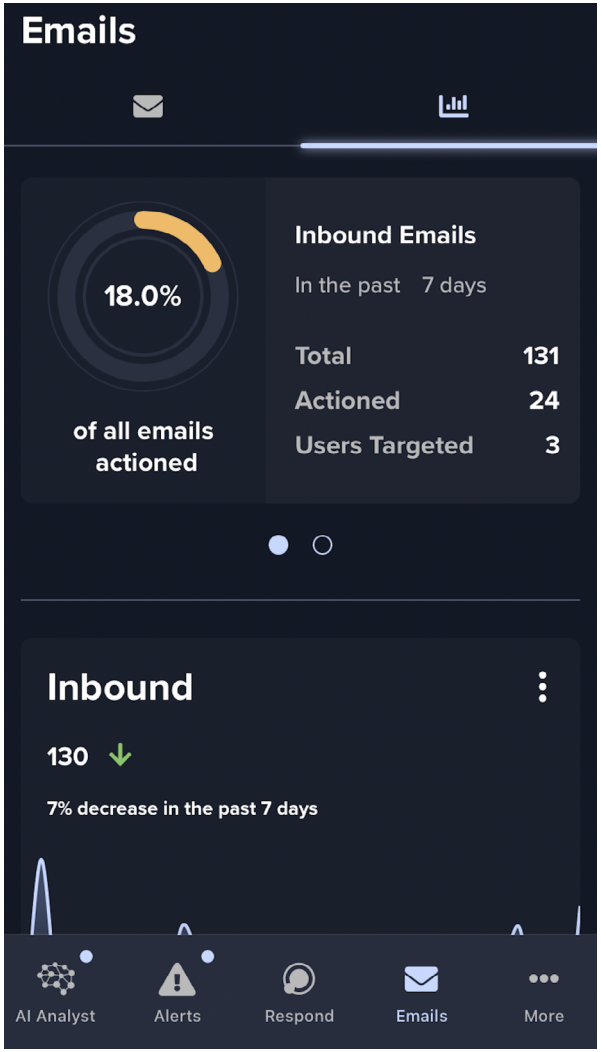
- Use the tabs to filter by action status
- Swipe left on a RESPOND action for actions
- The Pending, Active, Cleared and Expired actions will be shown in different tab
  - Tap an action to review details.
  - Swipe up from the bottom to view quick actions such as Extend, Clear or Activate
  - Open the left tab for information about the action
  - Open the right tab for related model details.



Emails

The Email screen displays ounbound and inbound emails.

- Use the Email tab to filter and find emails
- Use the Graph tab for an overview of emails
- Swipe left on an email to manually hold it
- Swipe right on an email to manually release it
- Click on an email to have access to the Overview and more actions at the bottom
  - Tap Release Email to release it.
  - Once an email has been released, the option to add a Learning Exception will appear.
  - Tap Hold Email to hold it.
- Tap Investigate Campaign to view similar emails from the same sender.



More

Dashboard

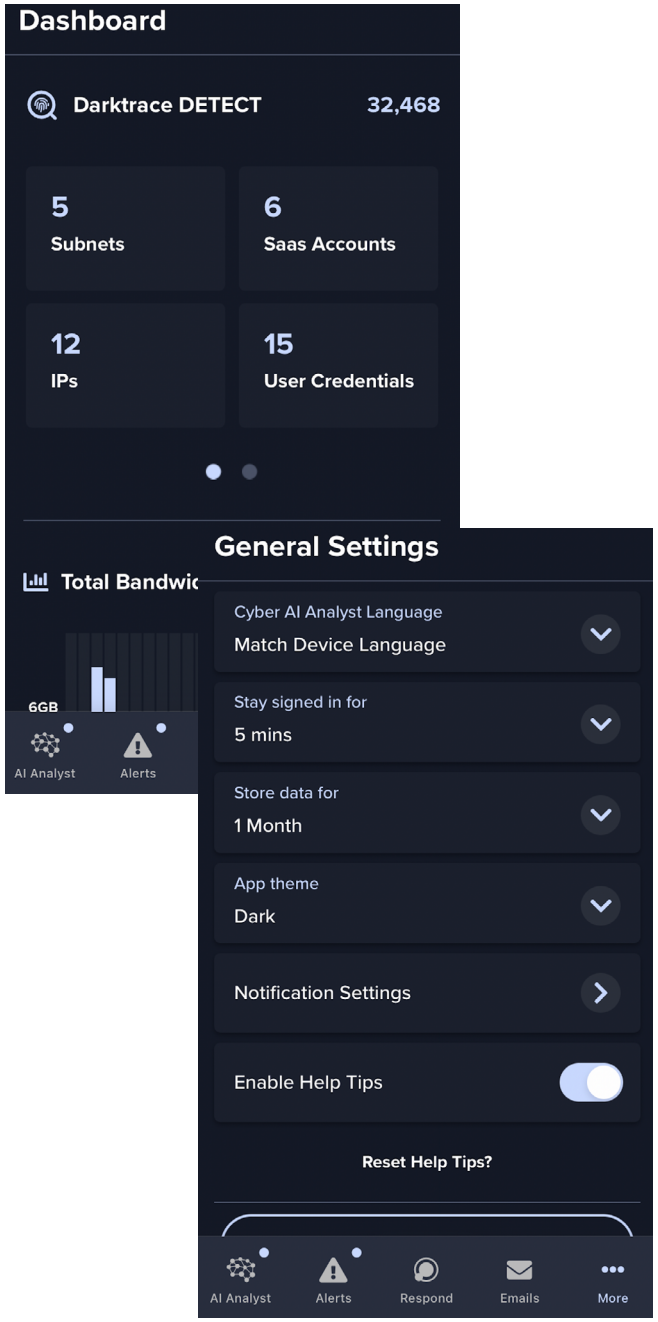
The Dashboard screen mirrors the high-level summary presented on the left of the Threat Visualizer home page.

Settings

Multiple filtering options and customization for how data is displayed in the app are available on this screen, obtained by clicking the cog on the right of the app.

Notifications

Notifications can be seen from this page. The notification types include Model breaches, RESPOND actions, AI Analyst incident events and System alerts.



7. Learning Outcomes

Course Agenda Checklist

Review this course with our dedicated video:
11: Course Summary

Thank you for completing this Threat Visualizer Part 2 - Investigation course.

We hope this have given you the confidence to using the Threat Visualizer and start investigating breaches and incidents.

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.

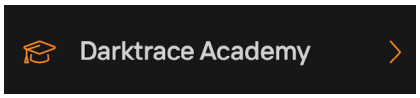
Complete the learning outcomes checklist:

- [ ] **Use the Threat Visualizer to follow an Analyst workflow**
- [ ] **Review individual Model Breaches**
- [ ] **Perform basic queries in Advanced Search**
- [ ] **Create packet captures and perform packet inspection**

8. Additional Educational Material

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

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



Training Courses

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

COURSE	AUDIENCE
Darktrace 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.