DARKTRACE

CYBER ANALYST PART 2 – MODEL OPTIMIZATION

Cyber Analyst Part 2 – Model Optimization
Manual v2.2.0 – Darktrace v5

Table of Contents

1. Learning Objectives

This course provides further learning on how to investigate and tune Models, as well as being more efficient in the use of the Darktrace Threat Visualizer. It is designed specifically for Cyber Security Analysts, Threat Researchers and Advanced SOC team members needing to expand their abilities in using the Darktrace tools.

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

+ Understand how Components, Metrics, Filters and Models function
+ Create new Models within the Model Editor
+ Understand the uses for Tags and be able to apply them to Devices
+ Edit Models to tune down Model Breaches and inhibit overfiring
+ Utilize Trusted Domain and Model Device Lists to triage the Threat Tray

For this course, a basic knowledge of the Threat Visualizer is assumed. This material is covered in Threat Visualizer Part 1 – Familiarization and Threat Visualizer Part 2 – Investigation. Before embarking on this part of the Cyber Analyst course, it is recommended that you have first attended Cyber Analyst Part 1 – Advanced Analysis.

2. Creating and Editing Models

A Model is used to define a set of conditions which can alert the system to the occurrence of a particular event. Models are made up of one or more components. Each Component can contain one or more Filters. Filters change according to the metric and so not every filter is available for every metric.

The Model Editor

All breaches in the Threat Visualizer will have a corresponding Model. Each breach can raise an alert in a number of ways.

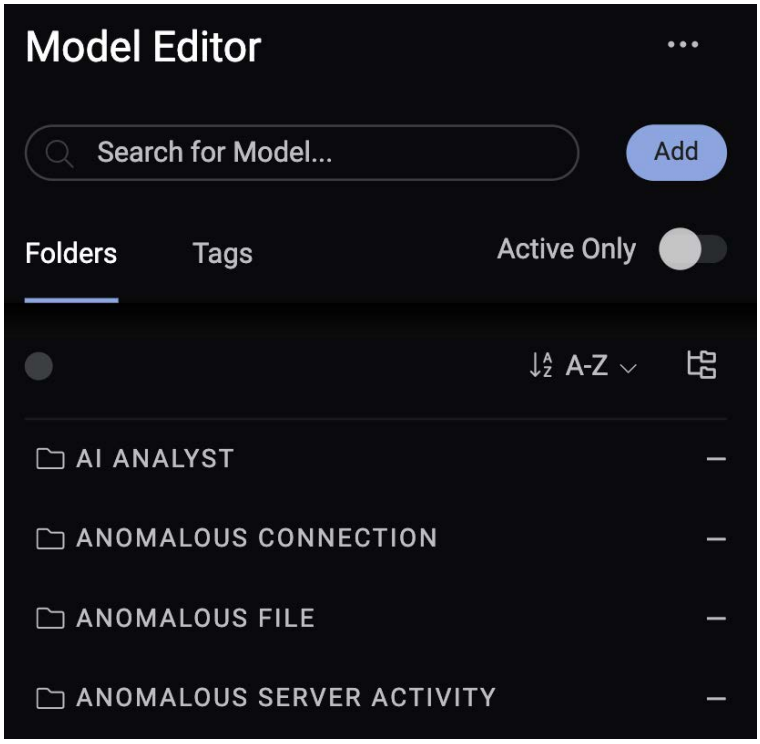
1. Navigate to the **Model Editor**:

   https://<servername>/model-editor

   Each Model is represented as a file and they are grouped into a series of folders.

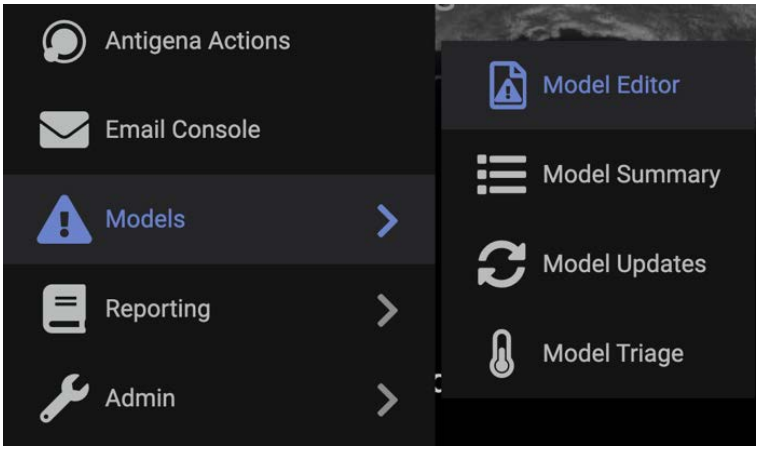
   By default, the Model Editor will display **Select a Model from the list** on the right of the screen until a Model has been opened.

   Note: *Empty folders are automatically removed.*

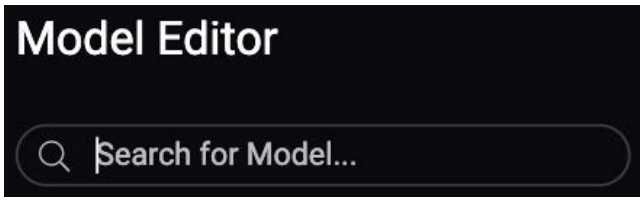


2. The **Model Editor** can also be accessed on the home page, by selecting the option under the menu.

   Furthermore, the **Breach Log** also contains a handy link to edit the Model which caused the breach:

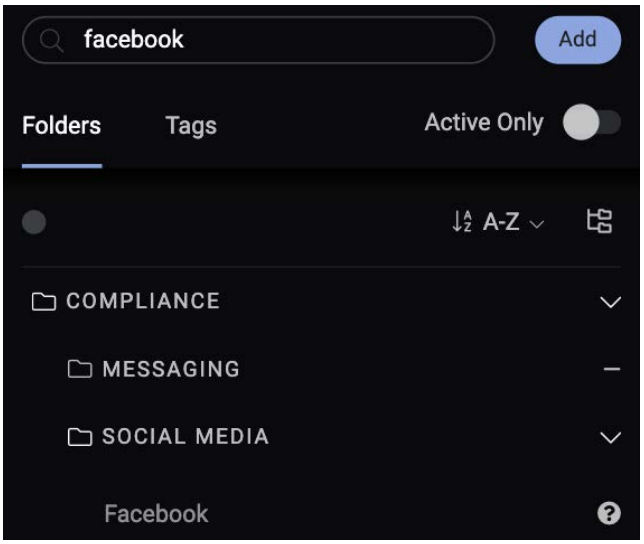


3. Upon entering the Model Editor, notice the **Search bar** at the top. Models can be looked up by typing a minimum of three characters which will dynamically filter the results displayed.



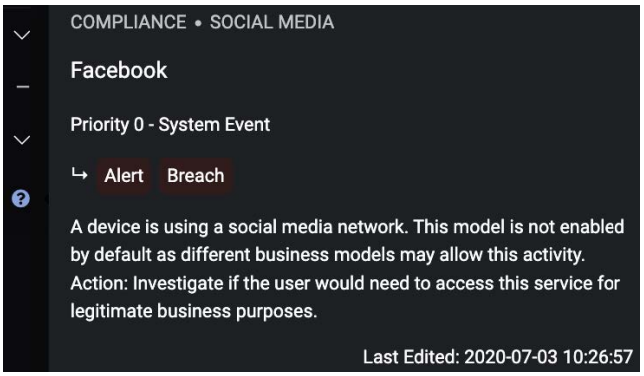
   a. Perform a **search** for Model name such as **Facebook**.

   While in **Folder View**, any folders containing the search term in their Model name are returned. Drill down through folders and subfolders to find the appropriate Models.



   b. When searching within a directory, only Models which match the **search criteria** are displayed.

   c. Click the **tooltip** icon to the right of the Model name to open a summary of the Model without needing to click on and open the Model Definition itself.

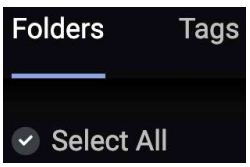


4. Models can also be located in the Threat Visualizer. Search for a Model name in the **Omnisearch** bar and click the Model Editor icon on the right to jump directly to it.

   Remember that the Breach Log also has the same shortcut icon to jump straight to that Model in the Model Editor.

5. When in the Model Editor, it is possible to filter the Models on **Active Only**. Switch the toggle to display the active Models.

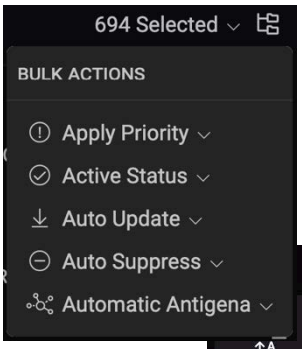
6. Notice **Select All** beneath the Folders tab. Click this to select all Models, or the ones which have been filtered, to gain new options.



7. Once Models have been selected, the **number of selected items** will be presented with a drop-down menu.

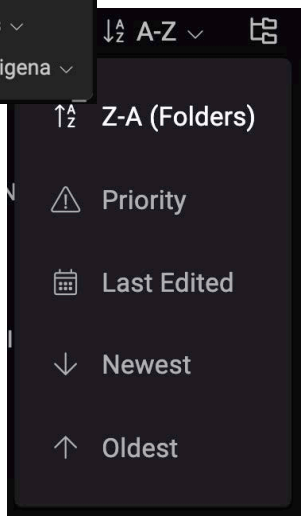
   Click the drop-down menu to view the list of **Bulk Actions** available.

   From this menu, multiple Models can have their **priorities** changed, be **activated**/deactivated, **updated**, **suppressed** or automatic **Antigena actions** applied.



8. The listed Models can also be sorted using a variety of methods.

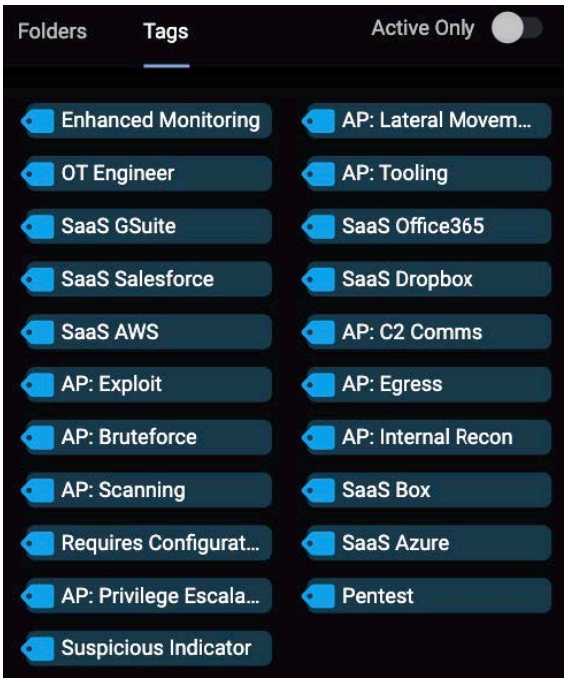
   Click the default **A-Z** icon to open more options and select a **sorting method**.



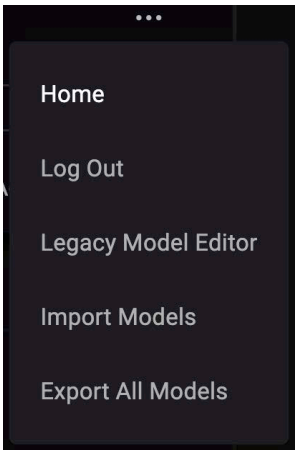
9. If any folders have been opened when navigating through them, click the folder icon to **collapse** them.

10. To change the **Model Editor View** from Folders, select the **Tags** tab.

    Instead of listing Model names, this will display tags which can be clicked on in order to filter Models based on which Tags have been applied to them.



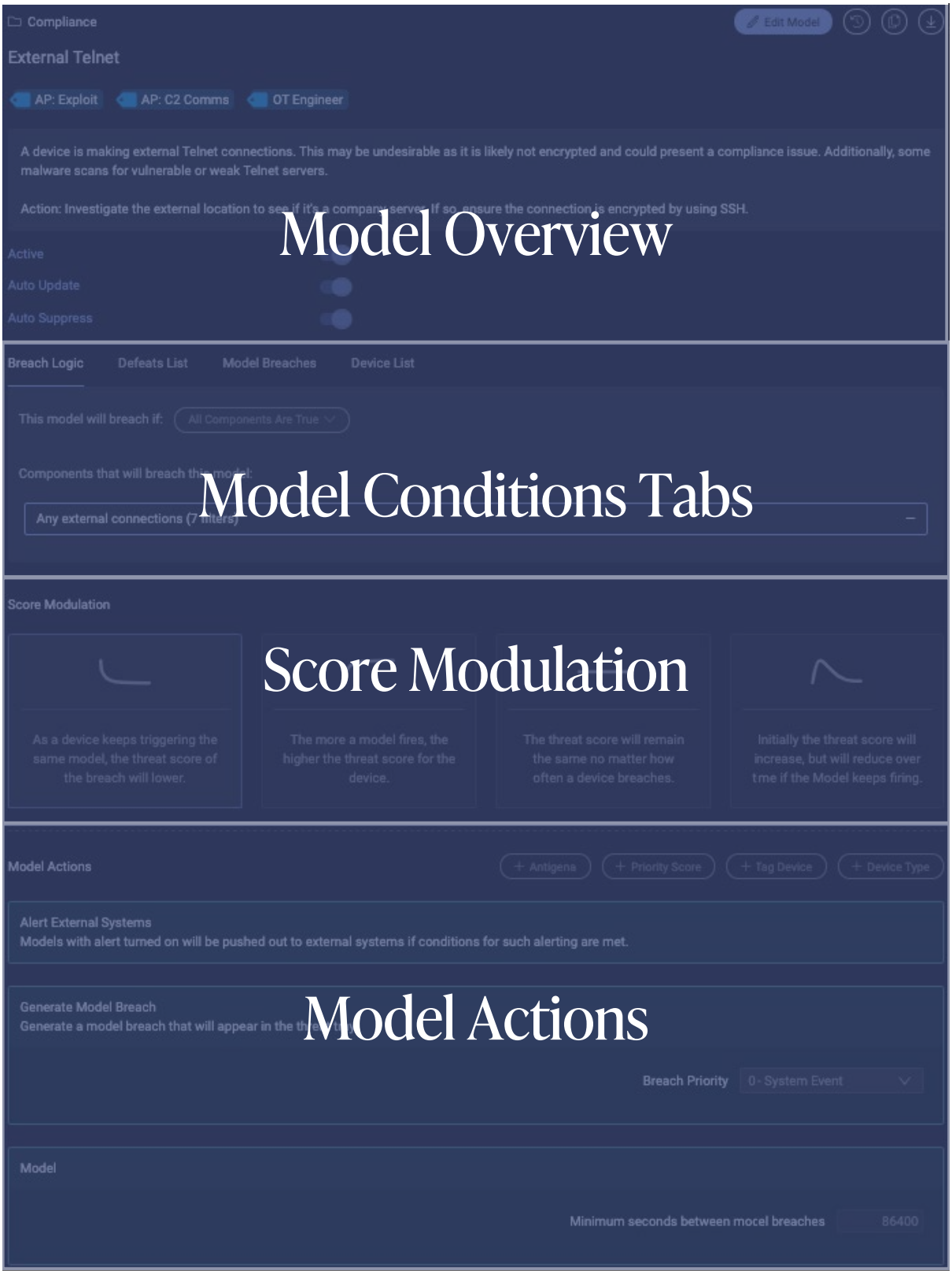
11. By clicking the three dots at the top of the Model Editor, there are further options to **Import** and **Export** (in .xml format) All Models as well as viewing the **Legacy Model Editor**.



Note: *The Legacy Model Editor is also accessible using the following URL: https://<servername>/modeleditor.*

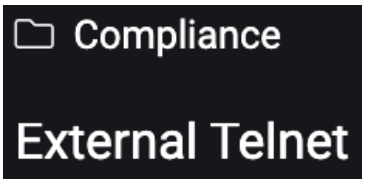
Model Definition

Begin by reviewing a **simple Model**. Navigate to the **Compliance** folder and select the **External Telnet** Model. Notice that the Model Definition can be broken down into basic, model behavior, score and breach logic parameters.



Model Overview

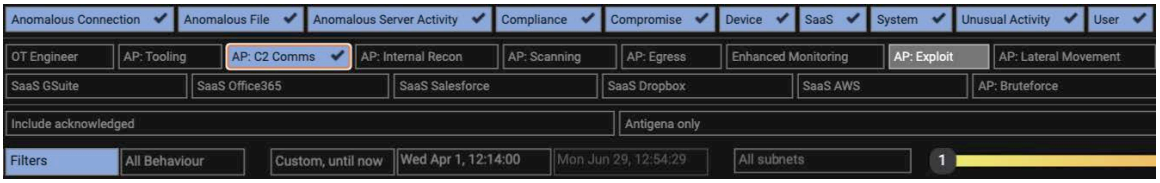
1. Models can be placed in **folders** and sometimes subfolders. The External Telnet Model is located directly in the Compliance folder.



2. Below this, the **Model Name** is displayed.

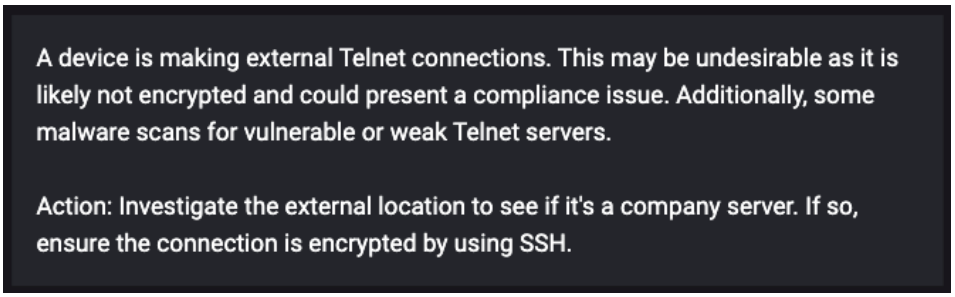
3. If any **Model Tags** have been applied, they will be presented beneath the Model Name.

The External Telnet Model has three tags: **AP: Exploit**, **AP: C2 Comms** and **OT Engineer**. This is because External Telnet could be as a result of an exploit and could be indicative or C2 communication.



Note: *Common Model Tags can be filtered on within the Threat Visualizer by utilizing, for example, the Attack Phase (AP) tags.*

4. Finally, the **Description** is an optional element which can be used to outline the meaning of the Model.



5. With the **Active** toggle switched on, the Model is able to breach.

Setting this to no will not delete the Model, but it will ensure that the Model no longer triggers alerts if the components are breached. Inactive Models appear greyed out in the Model Editor (as depicted on page 6).

6. **Auto Update** has another toggle option. When set to yes, the Model will automatically update when a new version is available from Darktrace.

7. **Auto Suppress** determines whether a Model will be automatically suppressed if it breaches repeatedly in a short period of time.

If a Model breach keeps firing for the same reason, auto suppress will hide the Model Breach, meaning that it will not appear in the Threat Tray. When enabled, one Model breach per week is let through to identify that it is still firing. The auto suppress feature will kick off when the Threat Score begins to decrease.

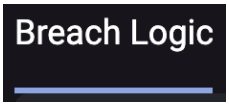
Note: *Auto suppress defaults to No for a certain subset of Models located in the Compliance folder and Yes for all other folders.*

Model Conditions Tabs

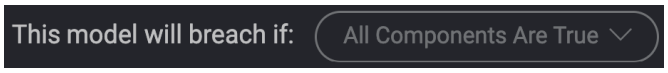
Breach Logic

Models are built up of components, which when met under certain conditions, can cause a Model Breach. These conditions are outlined by components, where every component is made up of a metric which may have its own filter conditions. Together, these elements make up the Model logic.

1. By deafult, the Model Definition will be on the Breach Logic tab. If this page has been navigated away from, click the **Breach Logic** heading.



2. Models can be one of two **types**, as seen in the "This model will breach if:" dropdown:

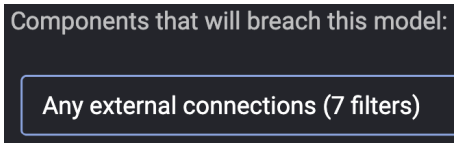


   a. The first, **All Components are True**, is the Model type for the External Telnet example. Every component must breach before Model actions can be triggered.

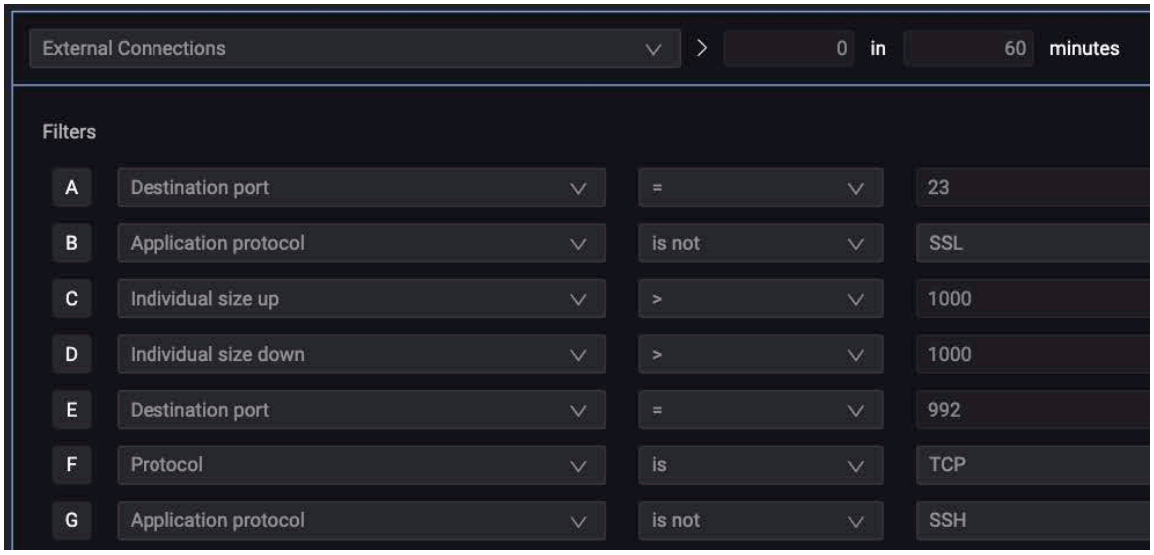
   b. The second, **A Target Score is Reached**, means the each component breach contributes towards a target score before the Model as a whole will breach.

3. For this example, there is only one component which reads **Any external connections (7 filters)**.

   Click the component to view its filters.



4. This Model has a **single component** looking for **any external connection in 1 hour**.



The component is made up of seven filters, each containing a metric which derives from Darkflow. These are features of a device's behavior that are continuously calculated on a scale.

The logic as outlined by the seven filters above is as follows:

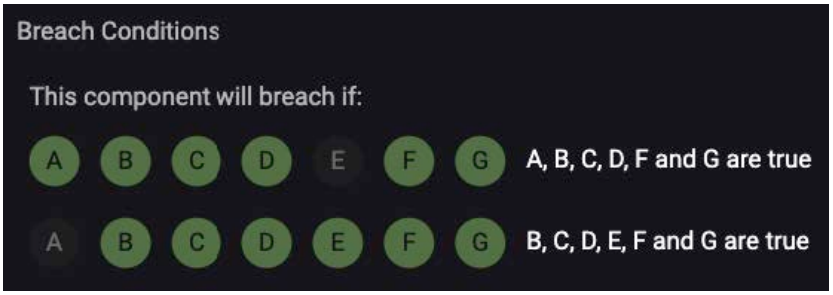
a. It will only alert if the **destination port** is port 23 or port 992.

b. It will only breach if the **protocol** is TCP, but it will not breach if the **application protocol** is either SSL or SSH.

c. For the Model to breach, the **individual size up and down** must be at least 1000 bytes.

5. Scroll down the page to see how each Filter is employed under the **Breach Conditions**.

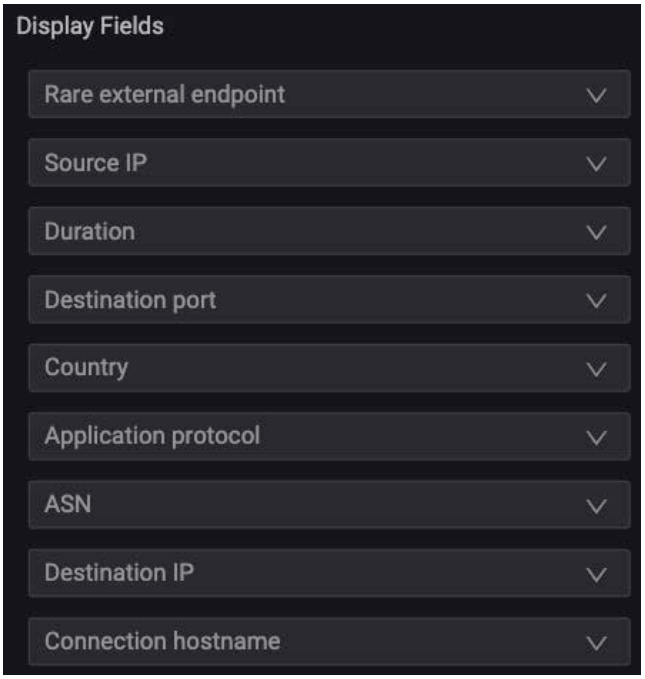
   This example can be breached in two ways – if the destination port is 23 or 992.



6. If they are met, the filters outlined in the Model Component will be presented in the Model Breach Log.

   However, additional metrics can also be displayed by utilizing the **Display Fields** option below the Breach Conditions. The addition of such information can make it easier to triage breaches from the Threat Tray as it displays interesting features that Darktrace detected as anomalous.

   Note: *Sometimes, if a Model can be breached in multiple ways, the filter which was not met will not be displayed. If it is desirable to display this metric all the time regardless, choose the metric as one of the Display Fields.*



Note About Breach Conditions

When in Edit Model mode, it is possible to enable or disable which filters are required to achieve a breach by clicking them.

Active and non-active filters are depicted in green and gray respectively. The letters encapsulated in the circles correspond to the filter rows outlined in the component. Filters on the same row are combined with an **AND** condition, whereas different rows are joined with an **OR** condition.

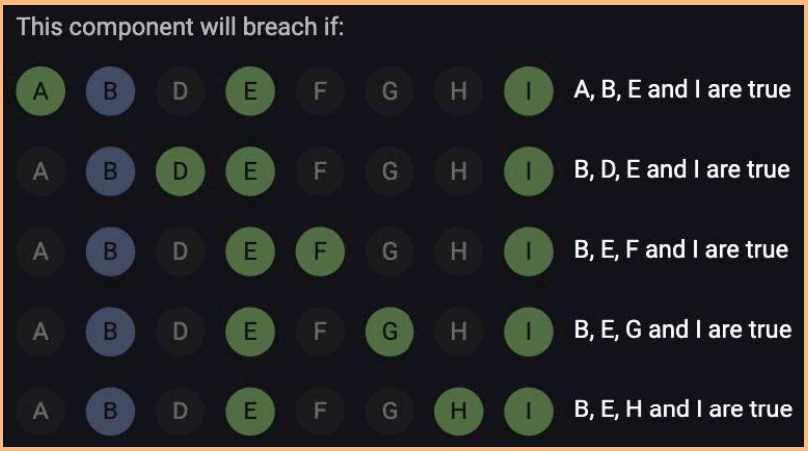
Circles which are automatically colored blue are always enabled, such as direction. This is often because the filter only has one or two options, so must have been selected for a reason. If the filter is not automatically enabled, it is the equivalent of not having this filter present in the component at all.

These filters provide an effective method to combine a wide range of metrics. Also, notice the shortcut buttons, which can automatically select **any** or **all** filters.

As this is a valid preconfigured Model, there is no need to apply or save any changes at this stage.

Note: *In order for some Models to breach), the way in which components are met can be achieved in multiple ways.*

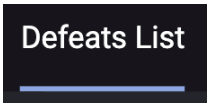
A more complicated diagram is presented to the right obtained from the Active Remote Desktop Tunnel Model. Notice that there are five ways in which the component can breach.



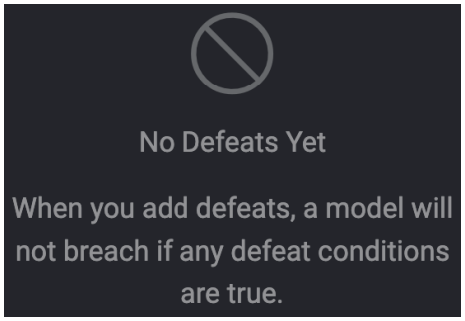
Defeats List

A useful tab for tuning Models is the Defeats List. This allows Darktrace operators to add defeat conditions which will make sure the Model does not fire if one of the outlined conditions is true.

1. Click the **Defeats List** tab to view any existing defeats.



2. By default, the External Telnet Model **does not have any defeats**. For Models where this is the case, a message like the one to the right will be displayed.

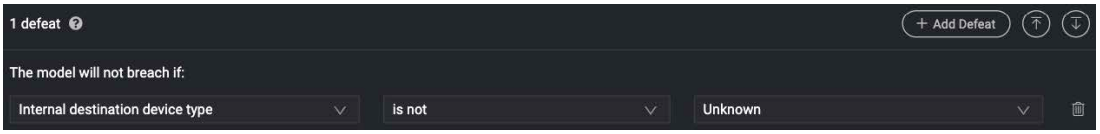


3. In order to add defeats, click **Edit Model** in the top right of the Model Editor.

4. New options will appear where the Defeats List can be populated.

   a. To add individual defeats manually, click Add Defeat.

   b. A new filter will appear where each drop-down menu can be utilized to choose a metric, comparator and value.



   c. These defeat filters can also be deleted by clicking the trash bin icon at the end of the row.

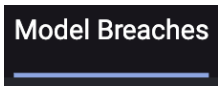
   d. Multiple defeats can be added in one go by utilizing the **Upload defeats list** feature. The file type this accepts is .csv, a template for which can be downloaded from an existing defeats list.

   e. Similarly, a list of existing defeats can be downloaded from the Model Editor by utilizing the **Download defeats list** feature. This will download a .csv file which can be edited and reuploaded or used across other Models.

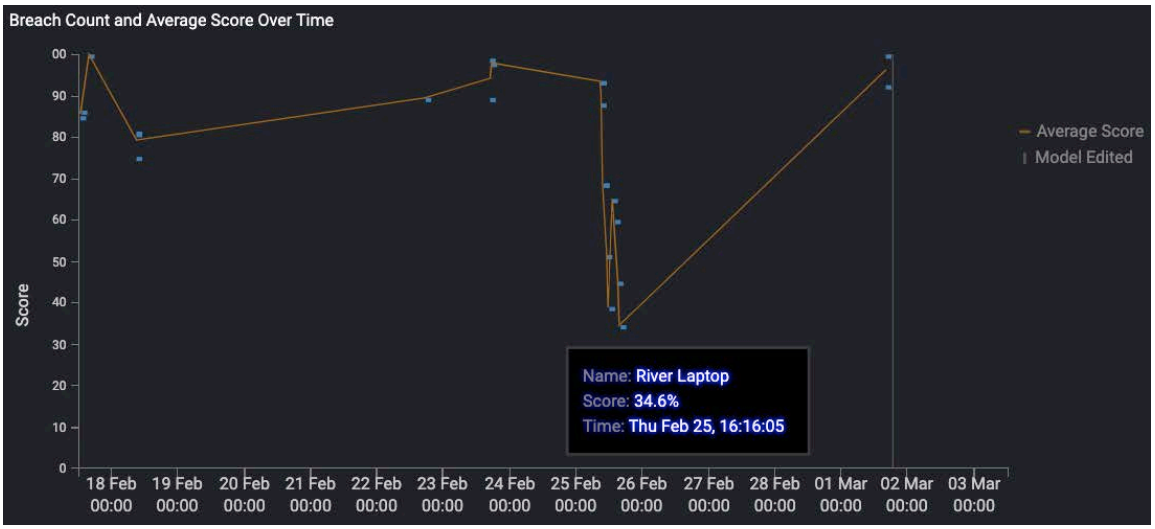
Model Breaches

One of the Model Tabs provides information about historical trends for devices breaching the selected Model. Such information can be useful in order to understand and optimize Models in context of the network.

1. Locate the third tab, **Model Breaches**, and select it.



2. A graph displaying the **Model Breach scores** over the last two weeks is presented. Each data point represents a device breaching the Model. The orange profile depicts the average score of the breaches.

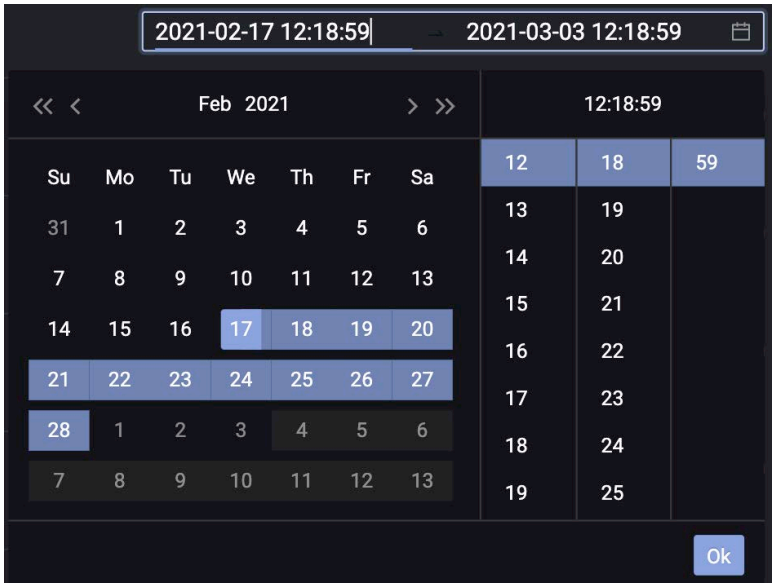


Hover over a data point to read the **device name** (or label), Model Breach **score** and **time** of the Model Breach.

3. The time period of the graph can be modified using the **date range selector** to the bottom right of the graph.

   Click on the a **date** to open the **calendar** and choose a date or modify the time to expand the time period.

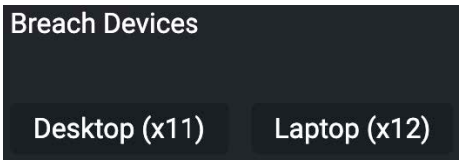
   Once chosen, click **OK** to update the graph to display breaches over the selected time period.



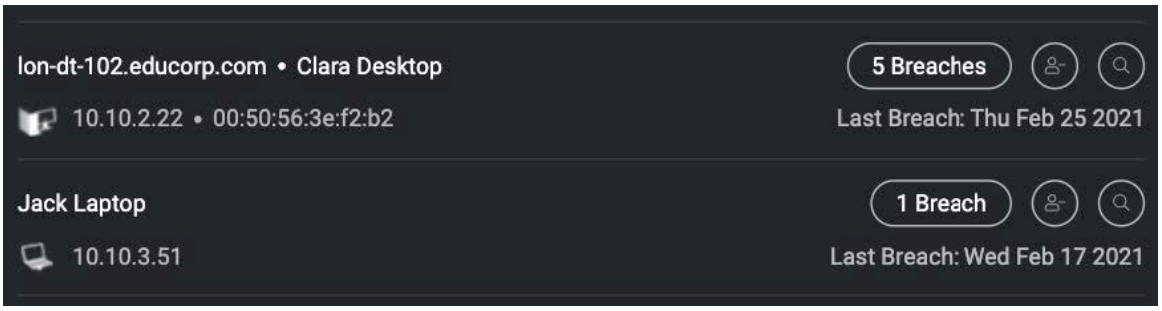
4. Just above the date range selector, notice the **Show Acknowledged Breaches** toggle.

Having the toggle switched to on will display both acknowledged and unacknowledged breaches which provides on overall view of how many times a Model has been triggered on the network.

5. For the selected time frame, a breakdown of **Breach Devices** can be seen to the bottom left of the graph. This categorises devices based on their type and displays how many of each type breached the Model.

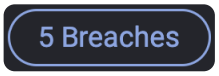


6. Below the graph is a table of device details. Each row represents a device which breached in the selected time frame, including the hostname, IP address, MAC address, if available.



To the right of the device details, the number of times the device breached can be seen, as well as the date of the last breach. With this information, a few buttons can be interacted with.

a. First, click on the **number of breaches**. This will open a Breach Log in the Threat Visualizer which will display all breaches for the time frame selected in the Model Editor.



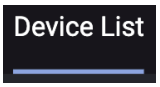
b. The next button allows the user to **ignore any future breaches** of the selected model for the selected device. This will add the device to the Exclude List in the Device List tab.

c. Click the **magnifying glass** to open the most recent breach in the Threat Visualizer interface.

Device List

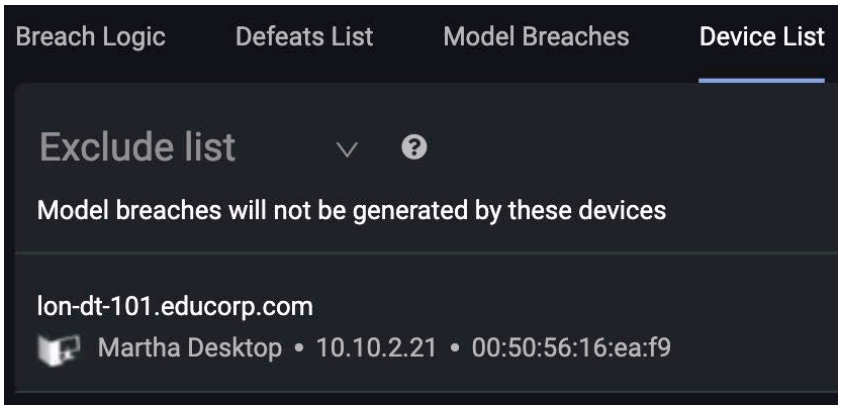
The Device List contains devices which have been excluded from the Model's actions or devices which will generate Model Breaches. These options are mutually exclusive and therefore both lists cannot be utilized at the same time.

1. Click the **Device List** tab to see if any devices are present in the list.

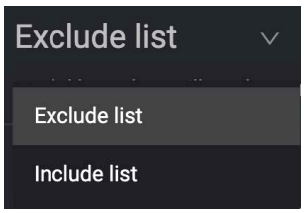


2. The type of device list will be presented in the dropdown; this will either be an **Exclude list** or an **Include list**.

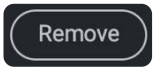
   In this case, a device named Martha Desktop has been excluded, so Model breaches will not be generated for this device.



3. To swap the list type from exclude to include or vice versa, first make sure the Edit Model button has been clicked so the Model details can be modified. Click the list name and choose the appropriate list type from the drop-down. This change will affect all devices currently on the Model Device List.

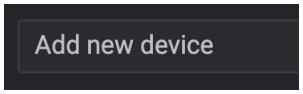


4. From a list in edit mode, devices can be removed. At the end of a device's row, click **Remove** to delete a device from a list.

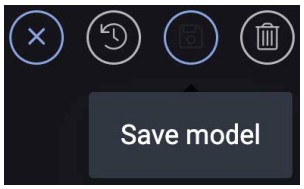


5. While devices can be added to the Model Exclude list from the Threat Visualizer or wherever the user icon as indicated to the right is displayed in the interface, devices can manually be added to the Model Exclude List.

   While in Model Editor mode, notice the **Add new device** bar on the right side of the page. Begin typing in some identifiable device information and select it from the suggestions to add it to the list.



6. If devices have been added to or removed from lists, or if the list type has changed, remember to **save the Model**.



Score Modulation

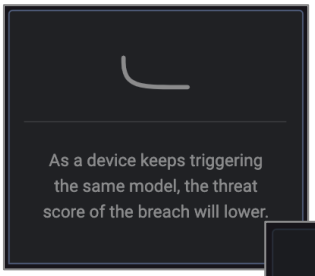
When the same device repeatedly breaches a model, the score of subsequent breaches will be adjusted. For some behavior types, repetition indicates that the activity is likely less worthy of attention from the security team. For other behavior types, repetition makes the activity potentially more serious. Selecting a modulation curve will determine how the scoring of repeated breaches for a given device should be adjusted.

Typically, the more a device breaches a Model, the lower the Threat score. The score is calculated from a combination of parameters:

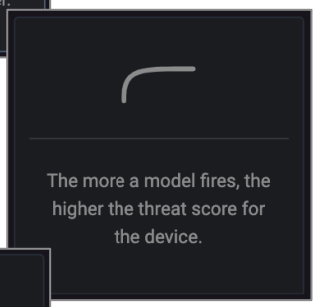
- How often the Model fires. The more it fires the lower it is. This is the most significant factor when calculating the threat score.
- Priority of Model.
- Priority of device.
- Metrics and Filter types in components.
- Actual Score values of Metrics and Filters.
- How much this Model is firing for the device itself.

The **Score Modulation** has four configuration options. The External Telnet example uses the first:

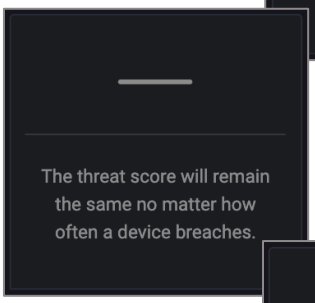
1. As a device keeps triggering the same model, the threat score of the breach will **lower over time**.



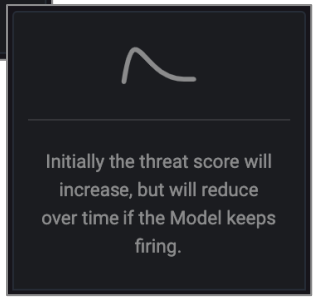
2. The more a model fires, the **higher the threat score** for the device.



3. The threat score will **remain the same** no matter how often a device breaches. For example, every time a device visits “dropbox”, it will keep the same score. This is common for Compliance Models.



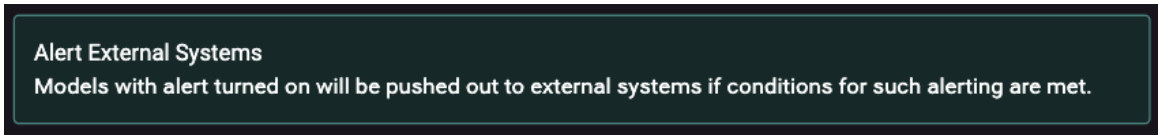
4. Initially the threat score will **increase but will reduce over time** if the Model keeps firing. Sometimes, it is more interesting if a device fires 2-3 times as opposed to only once. For example, if a device downloads multiple EXE files the threat score will eventually tail off.



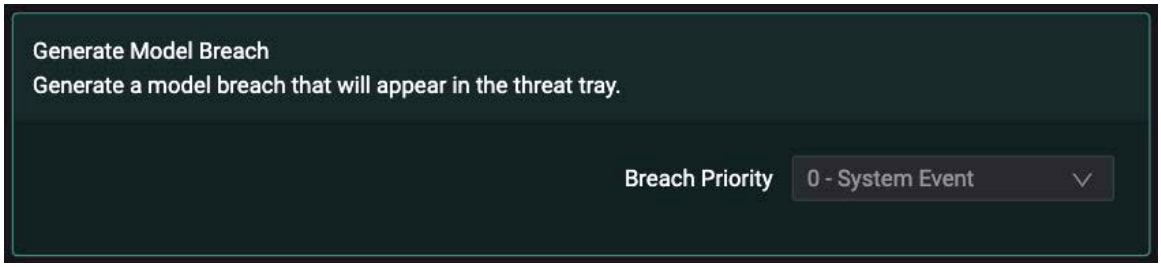
Model Actions

For the External Telnet Model in this example, there are three populated Model Actions. However, Model Actions can be modified if the Model is edited, and other actions can be added if they seem relevant.

1. The first action outlined in this example is the **Alert** setting. This can trigger a range of actions including email, JSON and HTTP alerts which can **Alert External Systems**.

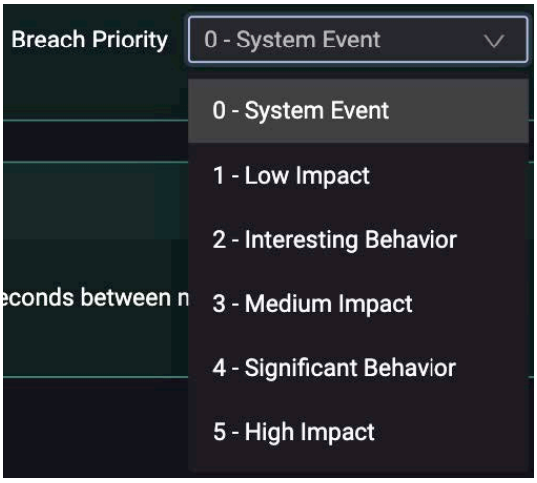


2. The next box indicates this this model **generates a Model Breach** that appears in the Threat Tray.

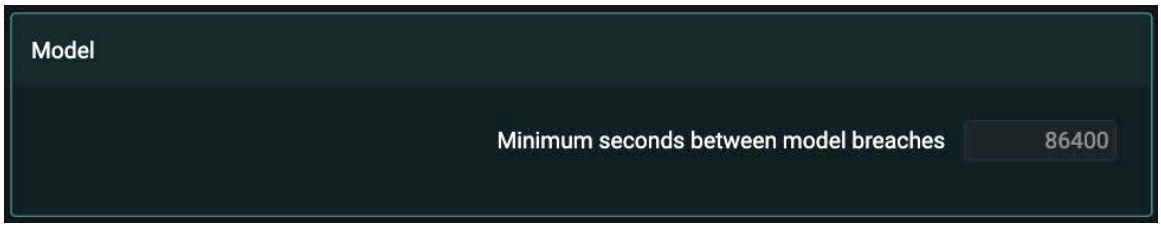


The Model **Priority** affects the strength with which it breaches by assigning the Model a priority score of 0-5. If particular types of behaviors are of greater interest, these behaviors will register as more strongly relevant and will be more obvious in the Threat Tray than if the priority was lower.

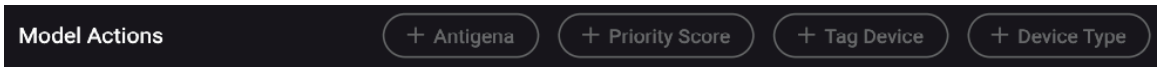
0 – System Event
1 – Low Impact
2 – Interesting Behavior
3 – Medium Impact
4 – Significant Behavior
5 – High Impact



3. The **Model** action at the bottom of the page is applied to all Models by default. The **wait time** defines the cooldown timer for a device once it has generated a breach for this Model. Once a device has caused an alert of this type, this Model will wait 86,400 seconds (one day) until it can fire the same alert again.



4. Notice four more options to the right of the **Model Actions** heading: **Antigena**, **Priority Score**, **Tag Device** and **Device Type**. In terms of the External Telnet Model, these are not relevant Model Actions. Nonetheless, their functions are outlined below...



   a. If licensed and enabled, additional **Antigena** options can be applied as a result of Model Breaches such a inhibitors. By default, these are active for one hour.

      If Antigena is enabled, and if human confirmation is not required, a response will be taken when the Model breaches. Thresholds can also be defined to restrict Antigena responses to breaches that exceed a limit.

   b. A Model is able to **assign a Priority Score** to a device which breaches the Model conditions. Device priority marks device importance – higher priority devices will produce higher scoring Model Breaches.

   c. A model can automatically **tag a device** that meets the outlined conditions. A tag must be selected in this section and can be given an expiring date.

   d. Darktrace assigns device types automatically based on network traffic analysis which can be overwritten in the Device Admin page. However, Models can reassign device types to one of the preset values (e.g. server, IP phone) as a Model action.

Model Editor Buttons

In the top right-hand corner of the Model Editor, a range of buttons are present, some of which enable users with the correct permissions to be able to make modifications to the Model.

1. In the far right of the icon selection, there is an **Export Model** button. Clicking this will export to Model as an .xml file.

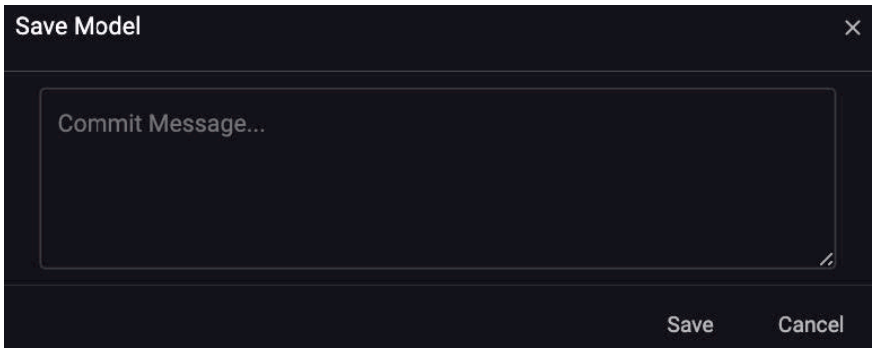
2. Moving to the left, notice the **Duplicate Model** icon. It is sometimes advisable to make a **copy** of a Model rather than making direct edits to the logic outlined by the Darktrace Model Deck.

3. However, for users with the Edit Models permission, click **Edit Model** to display a different set of buttons.

   This option allows the operator to edit the Model Logic, add defeats, modify the device list, change the model actions and much more.

4. If any changes are made to a Model, click the **Save Model** icon.

5. Clicking Save Model will open up a **commit message** dialog. Input some text and click **Save**. Try something memorable which describes the changes made so other users can track modifications.



6. From the Edit Model option, a Model can be **deleted** by clicking the **bin icon**.

   If selected, a dialog opens asking for confirmation. Consequently, the Model will reside in the **Bin** folder for seven days before it is deleted permanently.

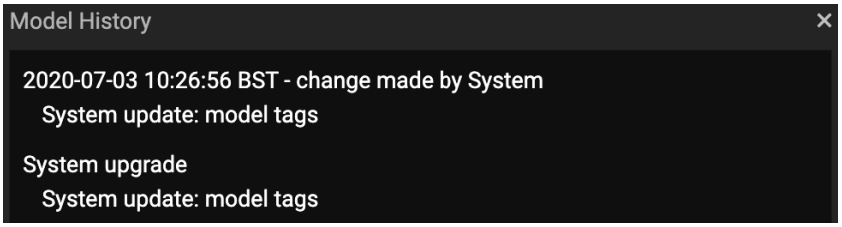
   With the deleted Model still open, click **Restore** if the deletion is no longer required.

7. To discard any changes made in this view, click the **cross** to **cancel**.

8. Visible in both button views is the **View Model History** button, as denoted by the clock icon.

   Clicking this will open a dialog containing the Model History, which can include system changes as well as user defined changes to the Model. The commit messages will be also be displayed here.

   Selecting an entry from this dialog will open a Historical Model dialog, allowing previous versions of Models to be viewed.



Model Type: All Components Are True

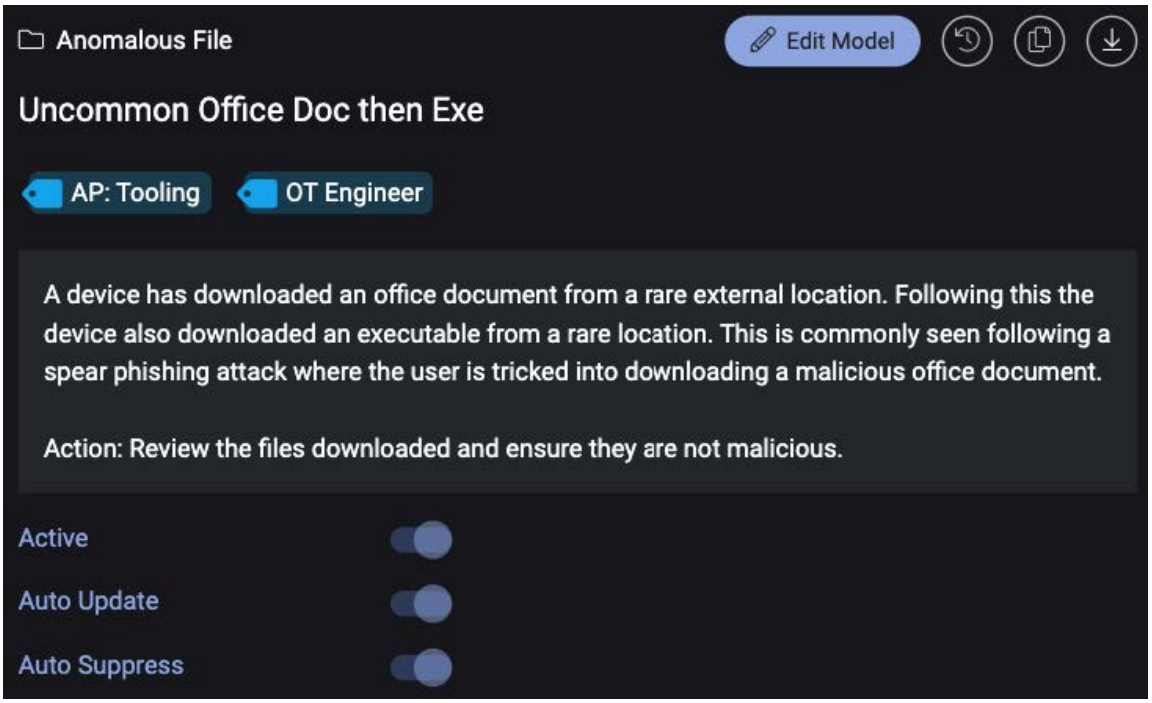
Thus far, the focus of discussion has been the definition of a single component. In practice, Models may include multiple components. Models with multiple components which all must be true can have different conditions:

- **All components must be breached in the above order** (as outlined in the Model Definition) means components must be triggered from top to bottom. Models with this condition can have their components rearranged by clicking and dragging.
- **All components must be breached within a set number of seconds** means there's a time limit in which all components must be triggered.
- **All components must share endpoints** means that all the components must be triggered by the same endpoint.

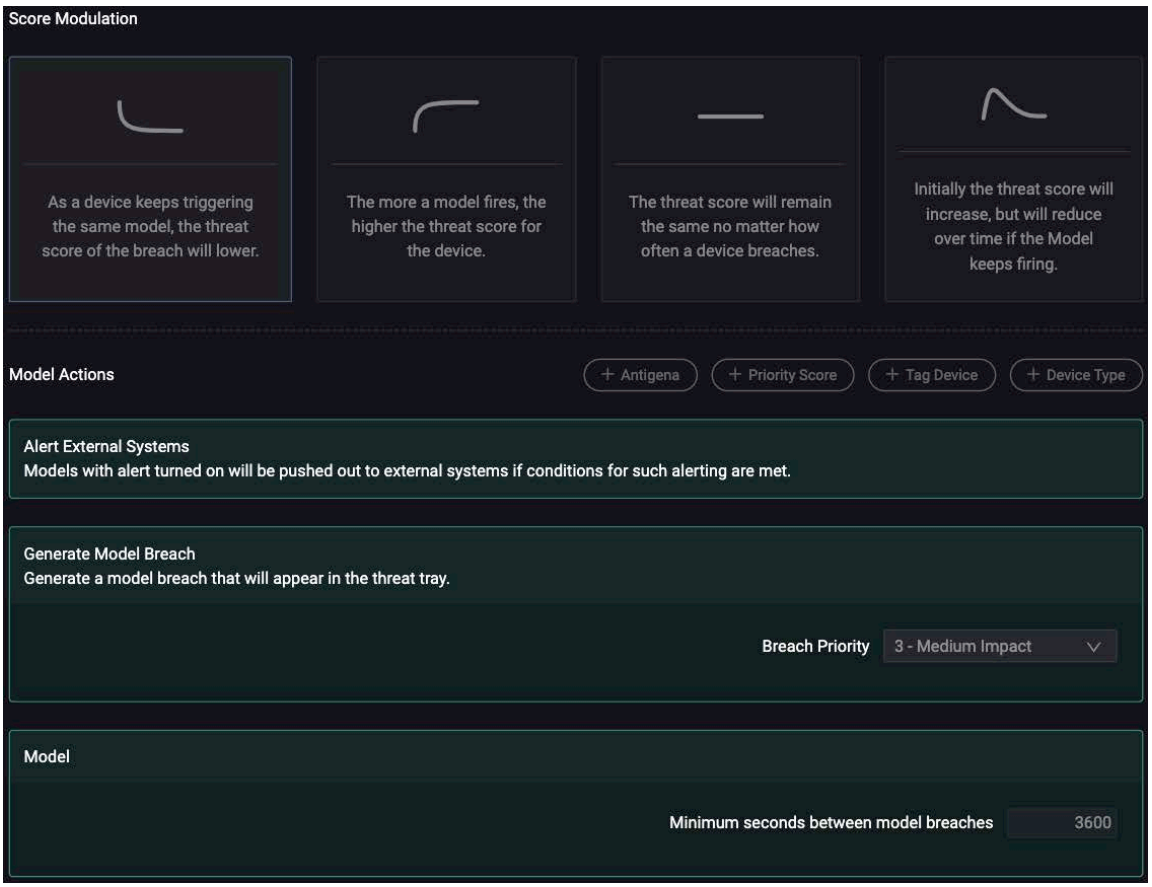
Uncommon Document Followed by Executable Example

This type of behavior can appear during a malware download. Generally, it is rare when an Office document is opened shortly followed by an executable being detected in this order. When this particular Model fires, it does not necessarily mean there is a threat on your network, but it could be indicative of malware being downloaded unbeknownst to the user.

1. Navigate up to the root directory of the Model Editor. Within the **Anomalous File** folder, open the **Uncommon Office Doc then Exe** Model.

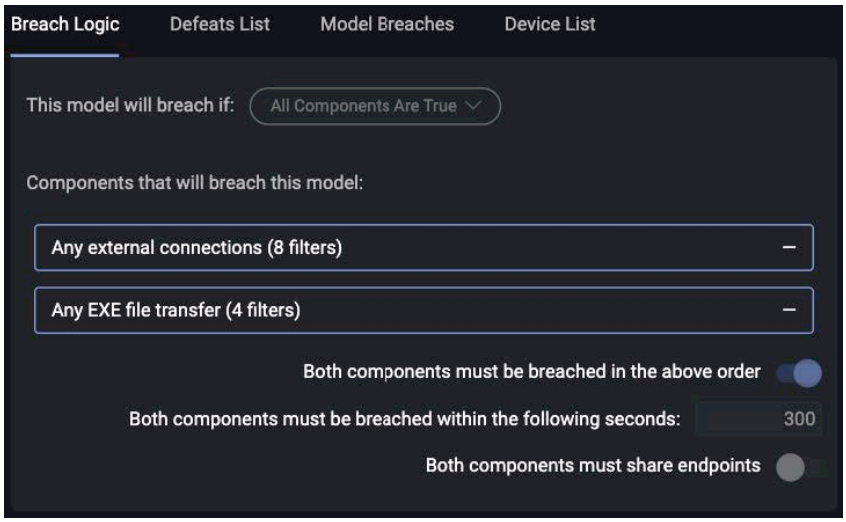


2. Scrolling to the bottom of the Model Definition, it can be seen that this Model has a Breach Priority **Breach Priority** is **3 – Medium Impact**.



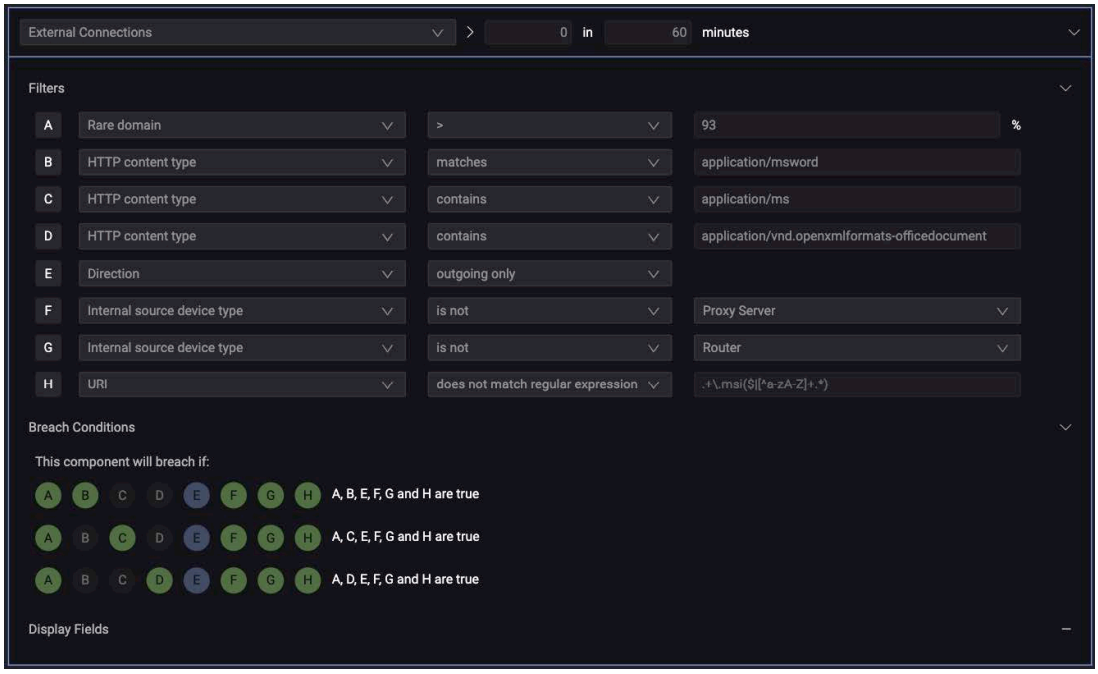
3. Notice there are two components. Underneath these components are a few further conditions.

   When multiple components in this Model type are defined, there is the option to toggle **Both components must be breached in the above order** to on.

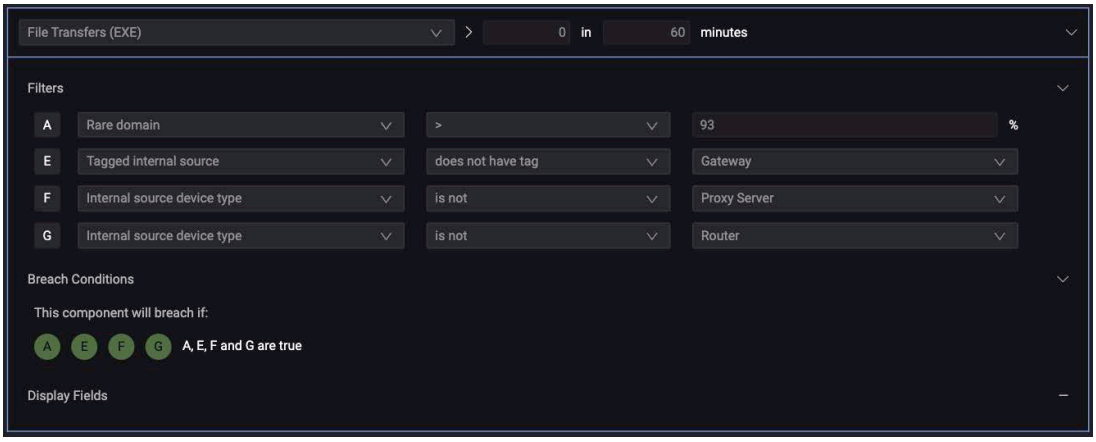


4. For this Model to fire:

   a. First, the breach device must make at least one **outgoing connection** to a domain which is more than **93% rare** with a HTTP content type containing the **word file format**.



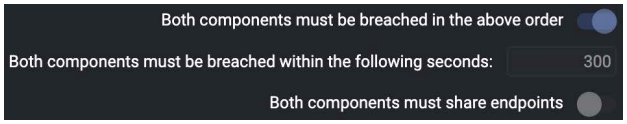
   b. Secondly, an **executable** file must be detected coming from a domain with a **rarity score of more than 93%**.



   Note: *When the Model is in Edit mode, hovering the mouse to the left of an existing component allows the user to click and drag the component. This makes it easy to change the order of the components.*

5. Specify the **time frame** in which the components must be breached within. In this case, the components must breach in the above order in **300 seconds**.

   Shortening the time is useful for events which could occur in quick succession, but longer time frame may be more appropriate for low-and-slow activity.



Model Type: A Target Score is Reached

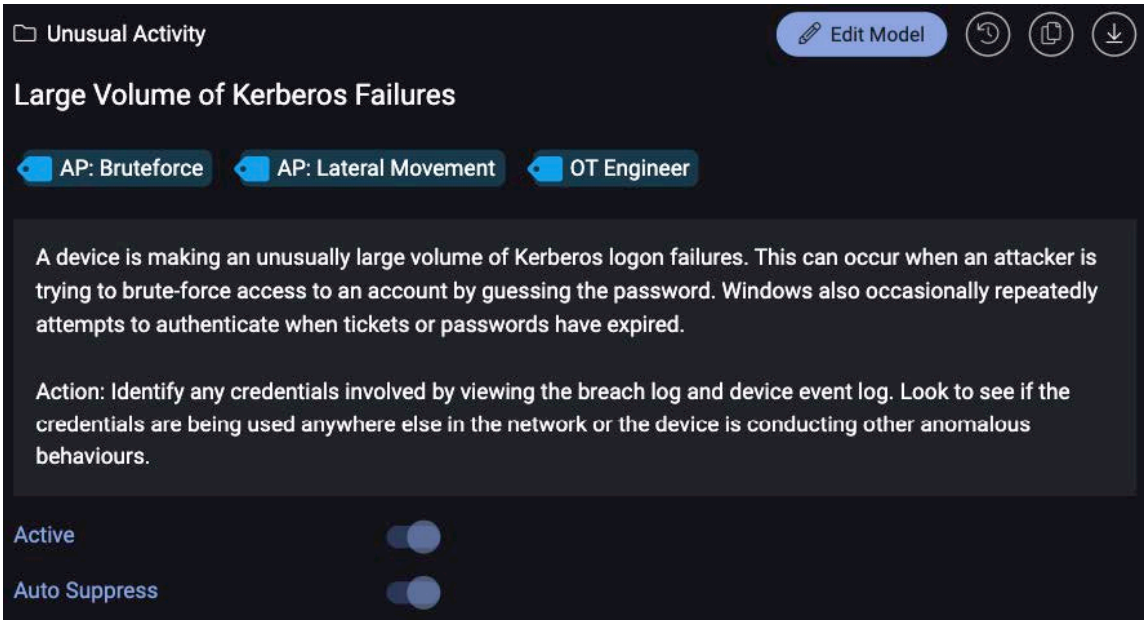
More complicated Models can employ a weighted technique in order to trigger a breach where it may have a mixture of positive and negative components. There are subcategories of this type of model which depend on one at least one of the following Model conditions:

- The **Target Score** of the Model must be reached when components are triggered to create a Model breach.
- The **Target Score must be reached within a set number of seconds** means there is a time limit within which enough components must trigger to breach the overall Model.
- **All components must share endpoints** means that if the Model has multiple components which have to meet a target score, they must be triggered by the same endpoint.

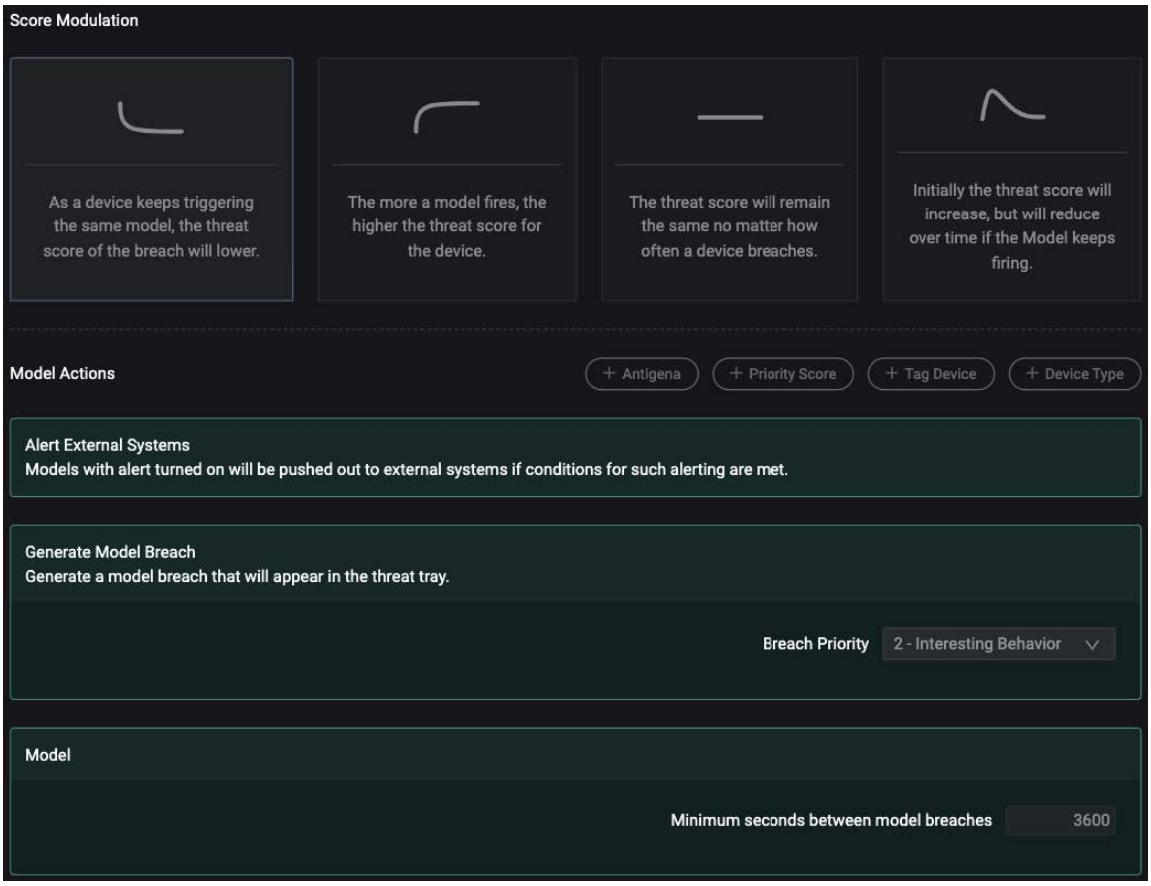
Large Volume of Kerberos Failures Example

This type of behavior can appear when an attacker is trying to bruteforce access to an account. When this particular Model fires, it does not necessarily mean there is a threat to the network, but it can be very interesting to know when these types of actions occur, especially if they represent a misconfiguration that needs resolving.

1. Navigate up to the root directory of the Model Editor. Within the **Unusual Activity** folder, open the **Large Volume of Kerberos Failures** Model.



2. Scrolling to the bottom of the Model Definition, it can be seen that this Model has a **Breach Priority** of **2 – Interesting Behavior**.

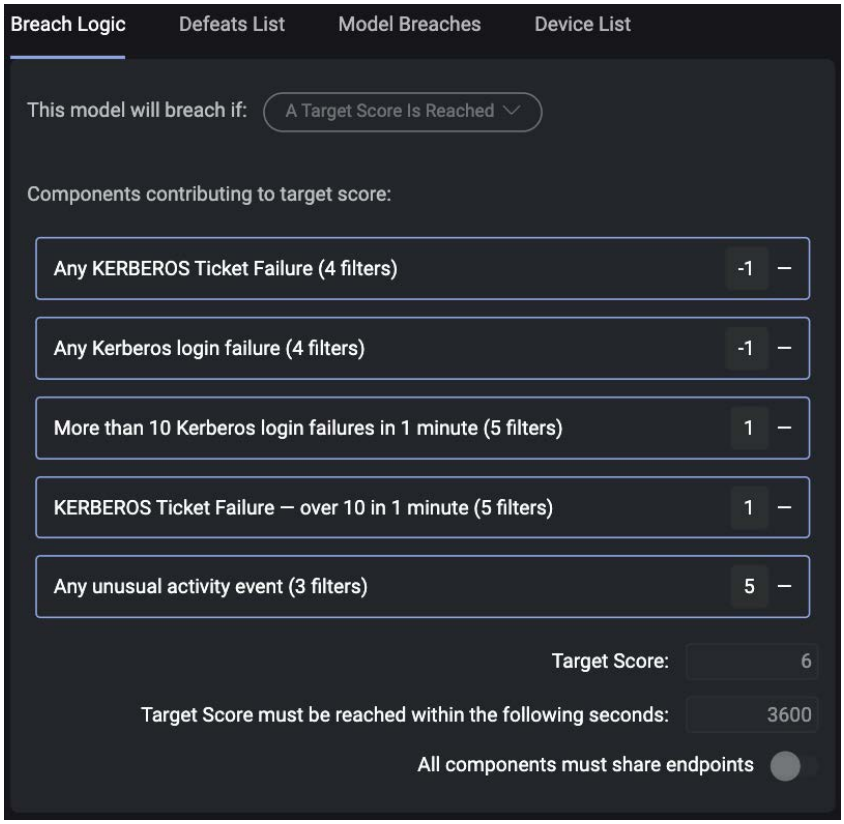


3. Within the **Breach Logic** section, notice that the Model will breach is a **target score is reached**.

   Below this, review the listed **components**.

   Each component has a different number of points which contribute to the target score.

   For the Model to trigger, the points must equal the **Target Score** which is currently set to six.



There are some **rules** to bear in mind:

a. Once a component hit occurs, the **point value** is added to the **running total** and will remain there for the duration of the specified time.

b. The component **cannot contribute** to the running total **multiple times**.

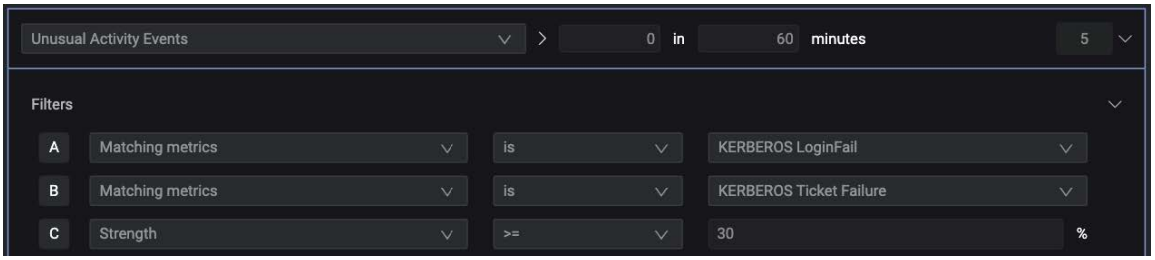
c. If the same component does occur without any other components being hit, the **time period is extended**.

d. As soon as the **target score is reached** or surpassed, the Model is **triggered**.

e. Negative point values can **prevent** others from reaching the target score if they are triggered between them.

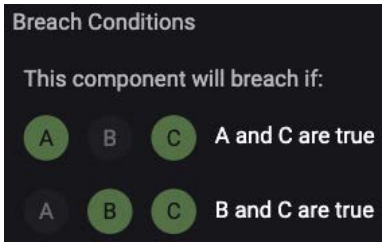
Therefore, in the example above, it is imperative that the "Any unusual activity event" must be met as this component contributes a score of 5. As long as neither of the top two negatively weighted components fire, if the third or fourth component is met within 3600 seconds of the last component, the Model will fire. However, there are various other combinations which might cause the above Model to fire.

4. Select the final component, **Any unusual activity event**, to view its Filters.



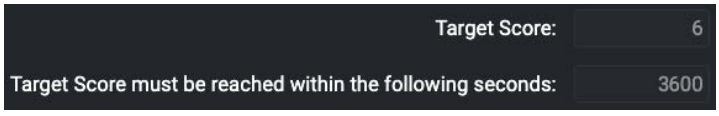
This component looks for any unusual activity event matching the filters within an hour (60 minutes). It contains filters for matching metrics and strength, i.e., a score of how unusual the activity is.

5. Below the filters, it can be seen how each filter is **employed**.

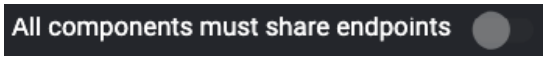


In this case the component can be breached in two ways, where the strength must be 30% or higher and must match either the KERBEROS LoginFail or KERBEROS Ticket Failure metric.

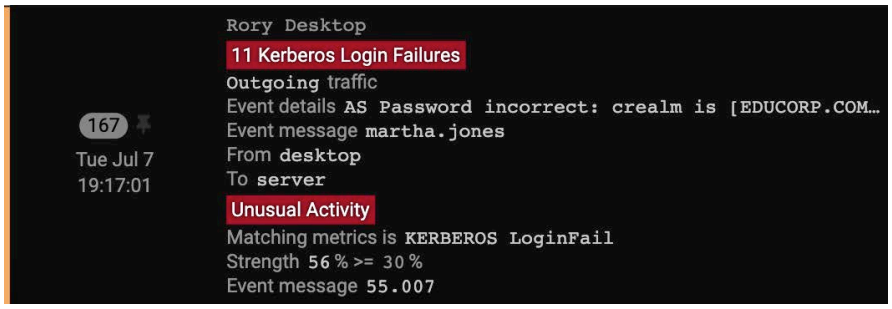
6. The **target score** of 6 must be met within one hour (3600 seconds) and the Model will wait an hour before triggering another breach.



7. The final option controls whether multiple components must **share the same endpoint** device i.e. the other end of the connection must be the same.



8. When the **Component** and **Filter** criteria are met, and the Model is triggered, the outcome of the Model can be seen in the Breach log.



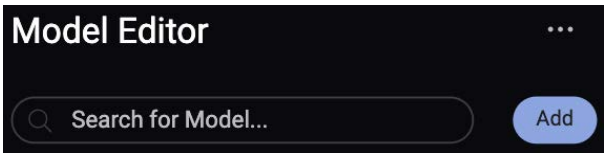
The data depicted is as a result of the **Display Fields** outlined in the Model Definition.

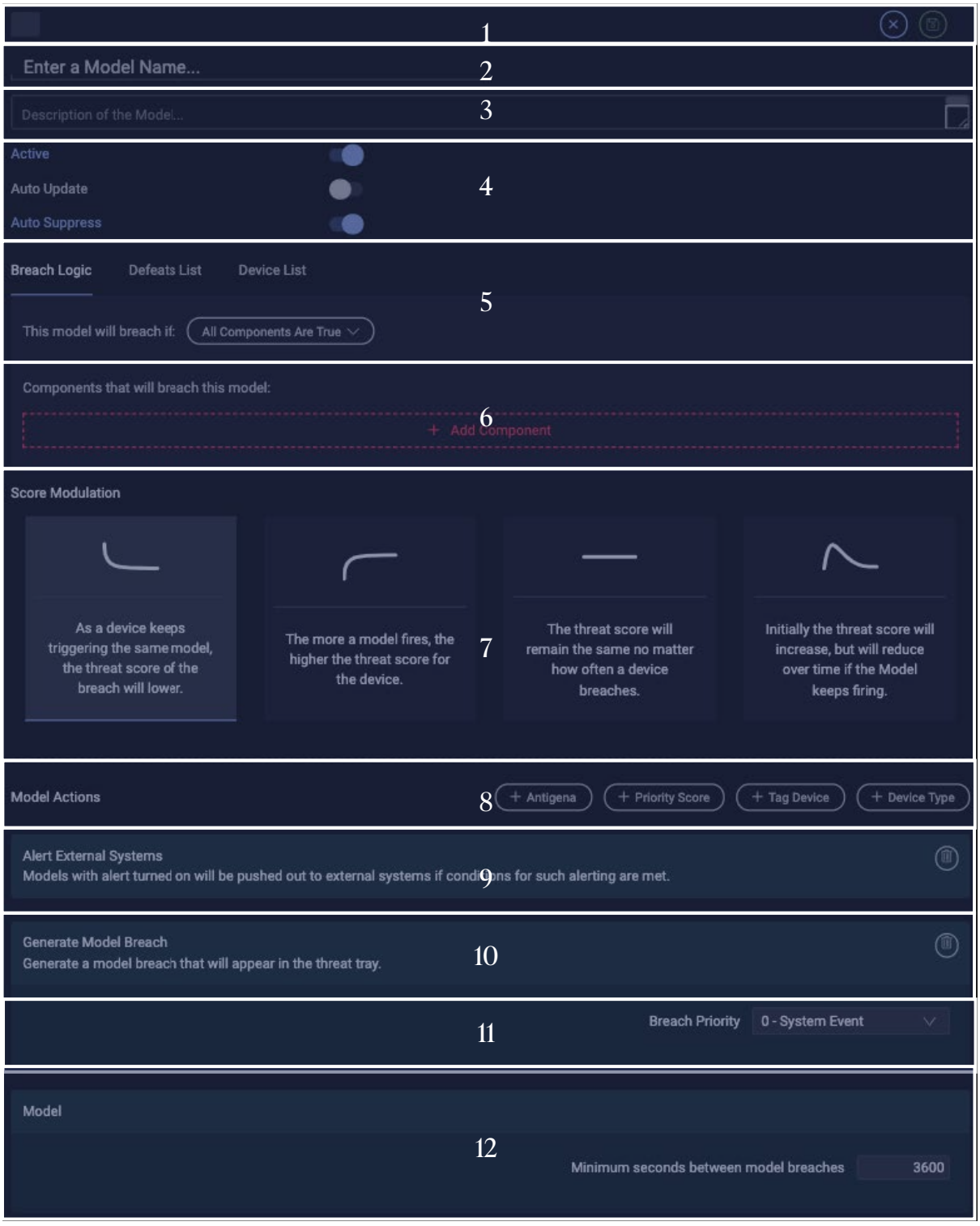
9. Review the other filters for each component set on this Model. The Metric filters can contain a series of **comparators** but not all filters need a comparator.

String	**Matches/Does not match:** This comparator is not case-sensitive. It performs a simple wild card match if the string has an asterisk or a question mark in it. This operation has a lower CPU usage then the regular expression comparator. The asterisk in the expression means that the value at that location can be zero or any number of arbitrary characters. The question mark means that the value can have either nothing or one occurrence of an arbitrary character at that location. *Examples:* **google.co.uk would match mail.google.co.uk and google.co.uk.* *?oogle.co.uk would match google.co.uk and also oogle.co.uk.*			
	Contains/Does not contain: Both comparators are case insensitive. It performs a string match, the same as Match="*<StringToMatch>*".			
	Matches Regex: This comparator is case sensitive. The Matches Regular Expression comparator can be tested with the Regex Tester.			
	Is longer than/Is shorter than: This comparator accepts a number, representing the number of characters.			
List	A predefined list of values which can be picked from the interface.			
Numeric	This comparator allows integer type operations:			
	<	Less than	>	Greater than
	<=	Less than or equal to	>=	Greater than or equal to
	=	Equal to	!=	Not equal to
Boolean Flag	A Boolean Flag is either True or False.			
Percentage	A score created by a mathematical formula.			

How to Create a Model

Models can be created by users of the Threat Visualizer interface. Navigate to the Model Editor and click **Add** beside the search bar to open a blank Model Definition.





1. Leave the box blank to place the Model in the **folder** where the new Model was added or input a value into the box to create a folder.

2. Give the Model an appropriate **name** which means the Model can be intuitively identified when a breach occurs.

3. Write a short **description** to outline what the Model is looking for alongside suggested actions which can be taken as a result of the breach. This can help with handling breaches when they occur.

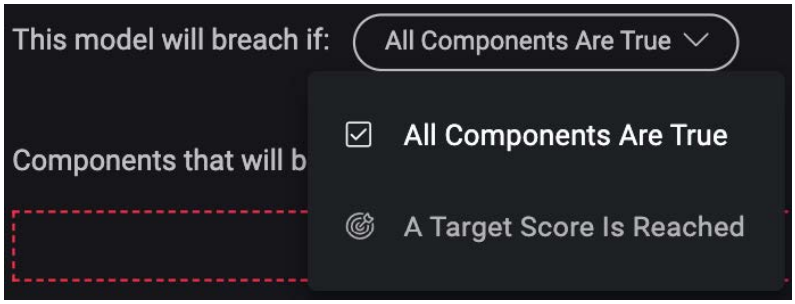
4. Next, there are three toggles set to their default values:

    a. New Models are switched to **Active** so can trigger Model Breaches or other actions after they've been saved.

    b. By default, **Auto Update** is off for custom Models, so will not be overwritten by Darktrace Model Updates.

    c. Finally, **Auto Suppress** is on by default. While it can be useful in early days of Model creation to stop it over firing, turning it off will allow a user to view Model Breaches and tweak ongoing.

5. By default, new Models will be open on the Breach Logic tab. Before creating any Model Logic, first select whether the Model will breach if **All Components Are True** or **A Target Score Is Reached**.



6. Next, notice the **Add Component** button. The core criteria governing when and whether the Model is triggered is embedded within the **component**. A valid Model must include at least one component. Defining the Model Logic will be covered in the next section.

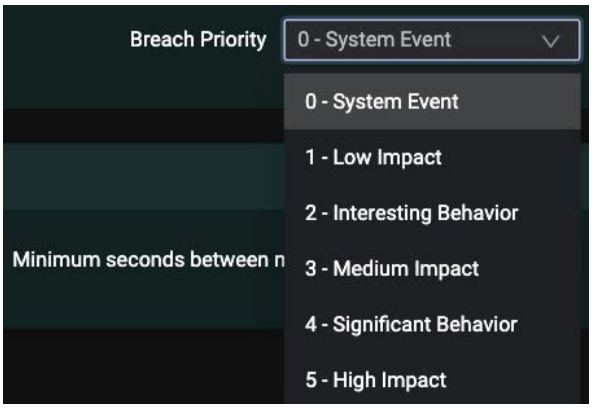
7. Choose a **score modulation curve** to determine the progression over multiple Model Breaches.

8. Review the possible additional Model Actions that may be desirable for the Model being created: **Antigena**, **Priority Score**, **Tag Device** and **Device Type**. Optionally, choose the appropriate actions to be triggered as a result of Model conditions being met. One or more actions can be selected, which represent what occurs as a result when a Model is triggered.

9. Some actions are already available by default. The first is **Alert External Systems**, which can be deleted if the Model is not intended to alert external systems.

10. **Generate Model Breach** is also on by default and will generate a Model Breach in the Threat Tray.

    Select a Breach Priority between 0-5 to influence the scoring of the Model.



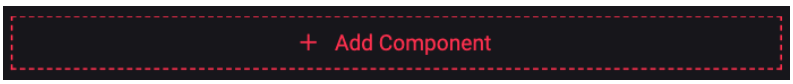
11. The final element of the Model Definition is **Minimum seconds between model breaches** with a default value of 3600 seconds.

    This **Model throttle** value ensures the same device will not trigger the Model again until the specified duration expires.

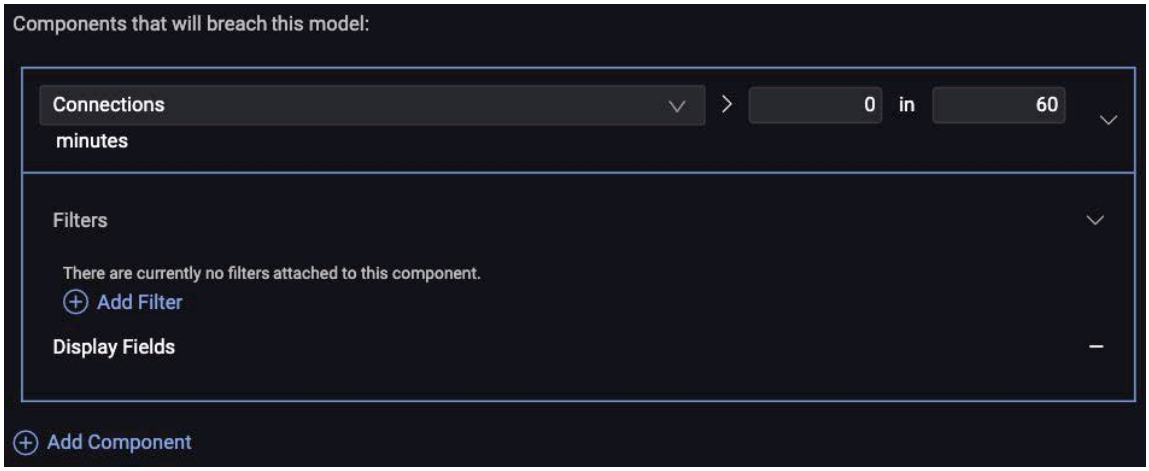
12. Once the Model has been created, click **Save**.

How to Create Components

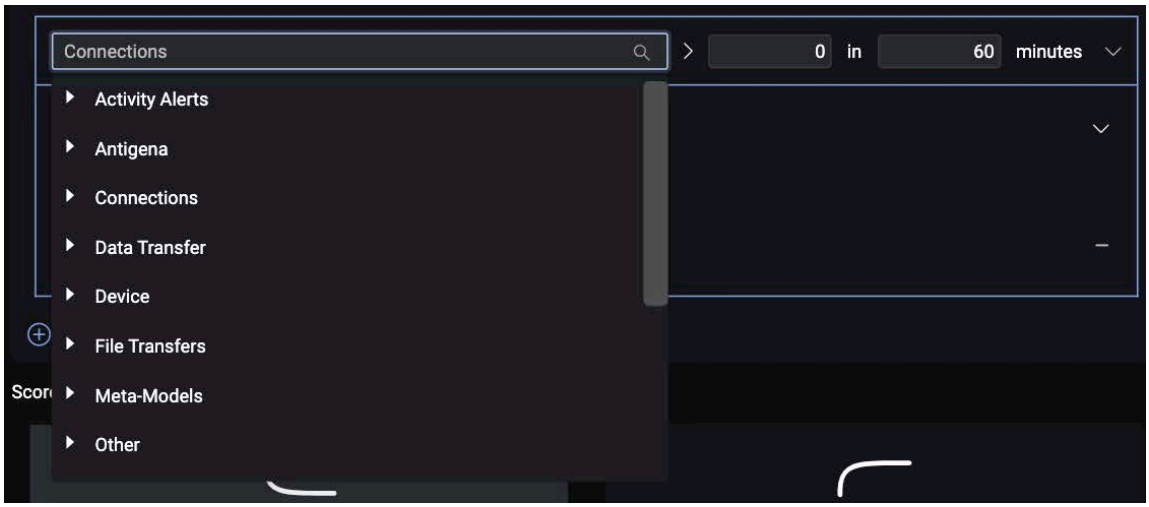
1. To add a new component to a Model, click the **Add component** button.



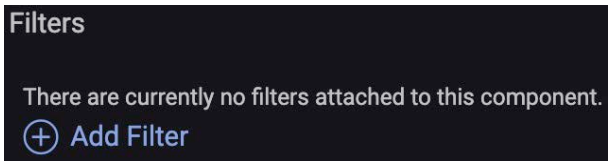
2. A section will expand containing a component that reads more than **0 connections in 60 minutes**.



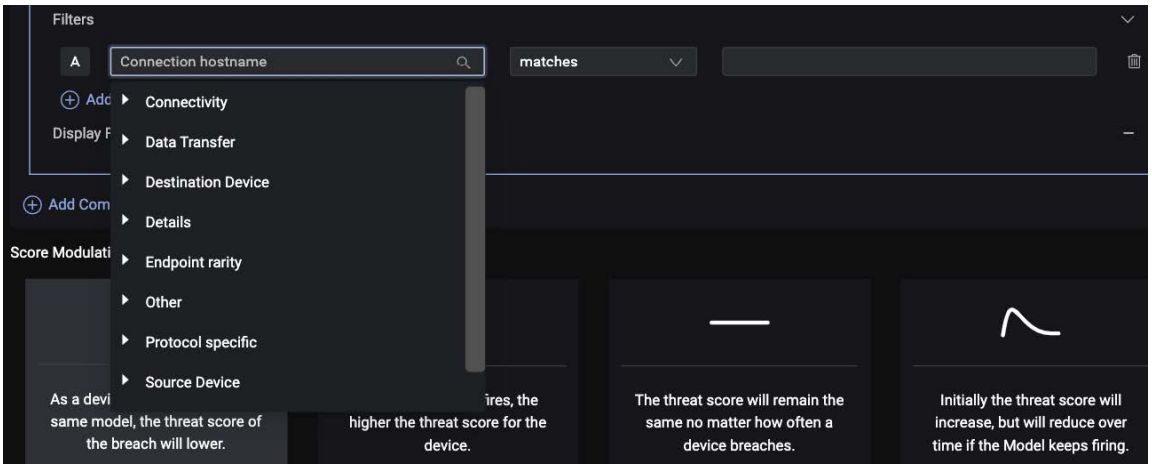
3. Click the **Connections metric** to open a menus/submenus of available component metrics. Depending on the Model type, a variety of metrics may be valid. To find more metrics, they can be dynamically filtered by typing in the **Filter** bar.



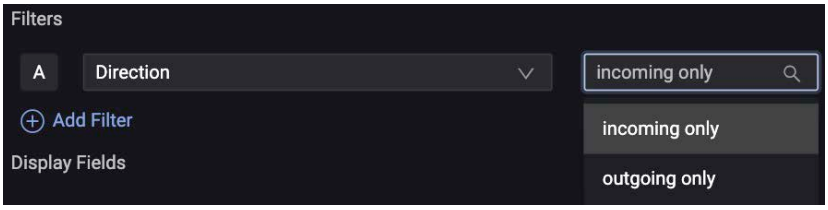
4. The Connections > 0 in 60 minutes component without filters will fire for any external connection. Once a metric has been selected, click **Add Filter**.



5. Filters can be **searched** and **dynamically filtered**. Note that the available filters may vary depending on the selected metric.

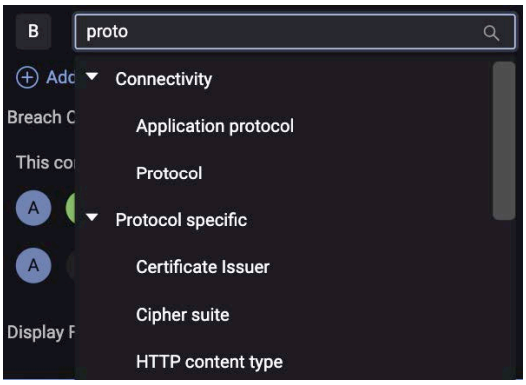


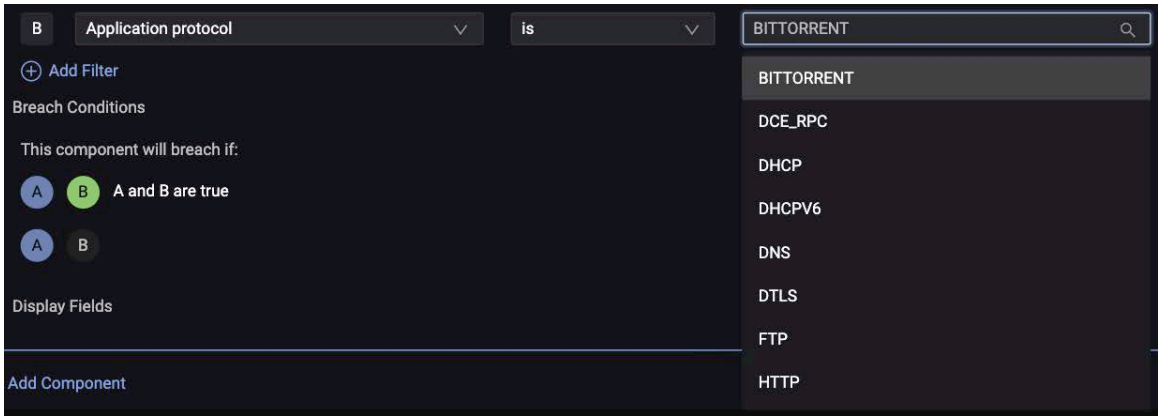
6. Some filters will have pre-populated values. With the **Direction** filter, the component can be restricted to **incoming** or **outgoing** only.



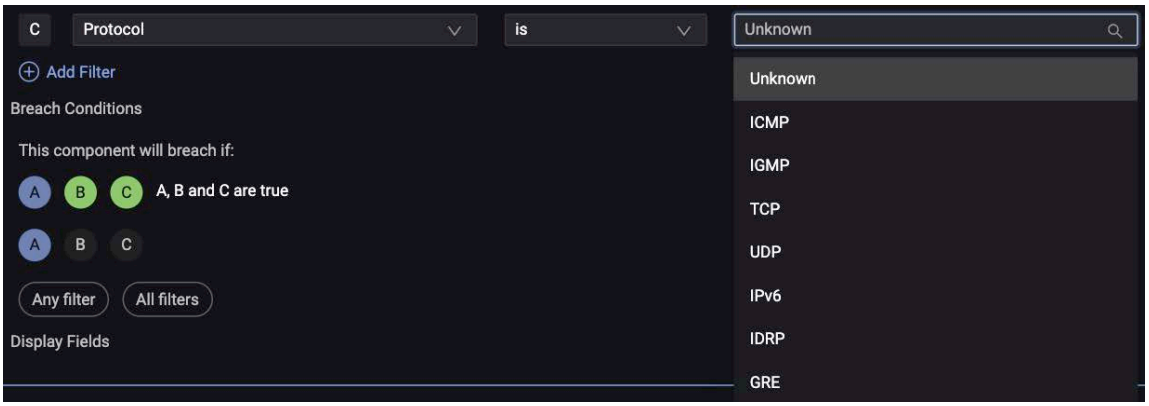
7. Connectivity can also be restricted by protocol. Add a new filter and start typing protocol in order to locate appropriate filters. Select **Application protocol**.

8. With the comparator set to is/is not as appropriate, select an application protocol from the **list of available values**.





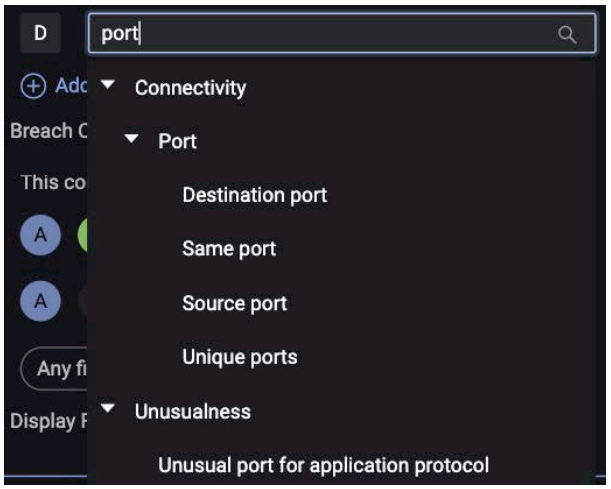
9. Not only can the Application protocol be chosen, but the **Protocol** may be a useful alternative, depending on what the Model is looking to detect.

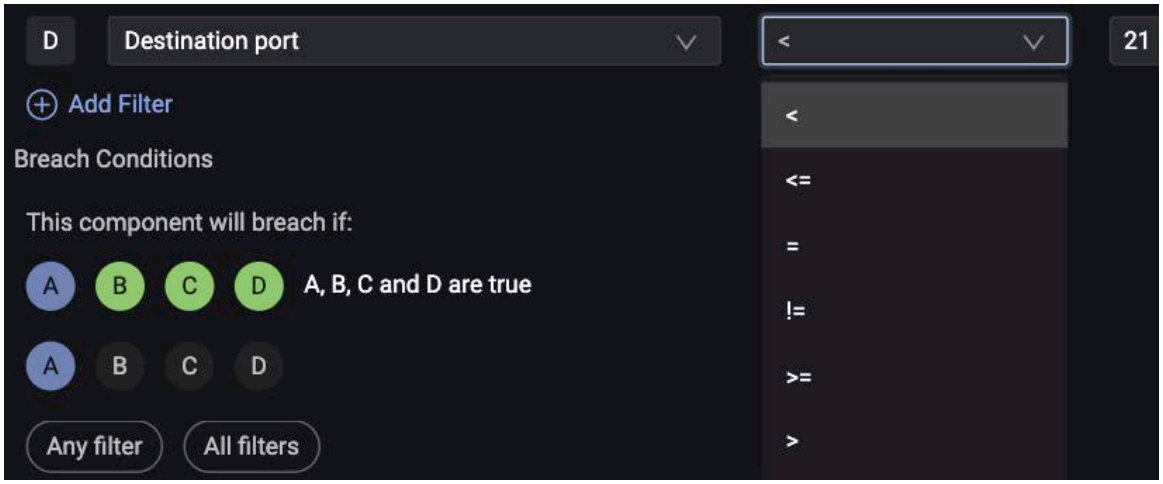


10. It is also possible to restrict connectivity on **port usage**. Again, by typing **port** into the filter bar, a range of options are presented. Select **Destination port**.

11. Due to the numerical nature of the filter, notice the comparators.

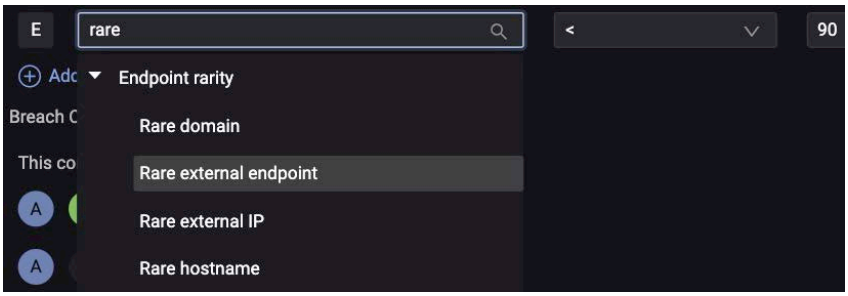
    Select equals and input a **port number**. This can be a useful way of detecting connection attempts on a port for a protocol, whether or not the protocol was initiated, nor the connection established.





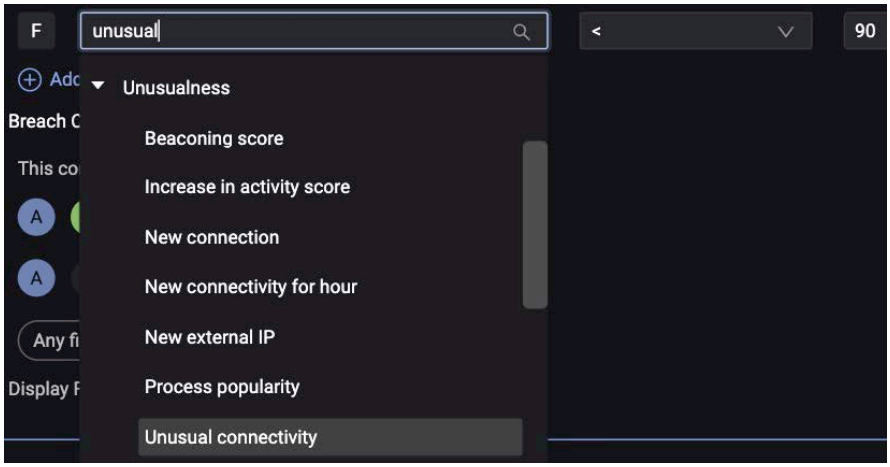
12. The detection can be further restricted by adding a filter to detect cases where the **external endpoint is rare** for the network.

    The rarity of domains, external IP addresses and hostnames are tracked individually but endpoint rarity accounts for all three; corresponding filters can be used to target one of those values.

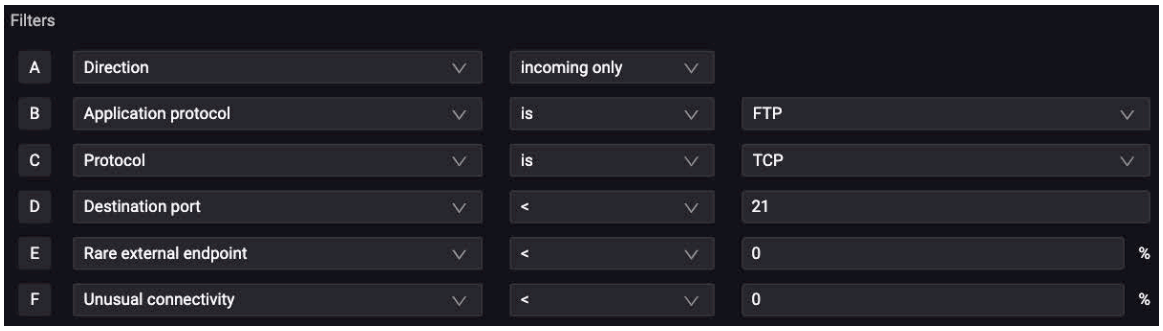


    Choose the **Rare external endpoint** metric and choose a numerical value.

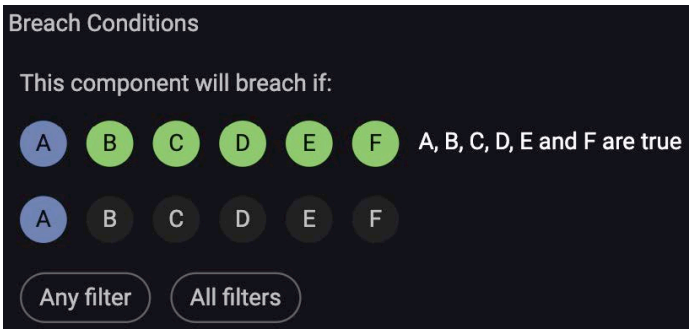
13. Connectivity can also be deemed **unusual**, which is evaluated per device rather than network wide. It may be desirable to avoid repeated detection of connections that are rare for the network but common for a triggering device.



14. It is advisable to set reasonably low minimum values for endpoint rarity and unusual connectivity to ensure a larger pool of example Model Breaches which can be reviewed to determine **thresholds**. Therefore, a component of the following format may be a good starting point:



15. Filters can provide multiple conditions for the component to hit. Scroll down to **Breach Conditions** to review combinations.



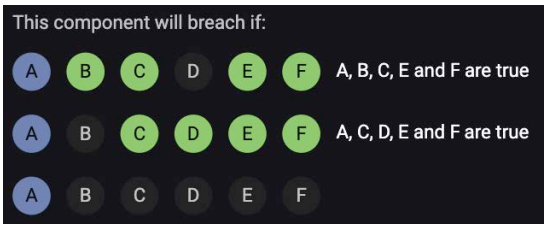
16. Each **green letter corresponds to the filter**. The **default selection** will put all the filters in the same row.

    If all letters, i.e. filters, in the row are satisfied, the component will be true and therefore hit. This follows the **All filters** pattern.

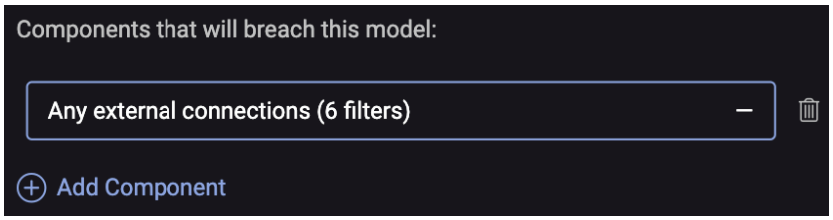
17. Clicking **Any filters** will automatically rearrange the filters which follow an OR pattern. This means each filter will be given a separate row, with the exception of blue filters which have to remain the same.

18. Each additional row indicates an **alternative set of filters**. To add a new row, simply select one or more of the letters within an empty row. Empty rows will automatically be created.

    The example to the right shows that the component will be triggered by the user if the connection uses **either** FTP **or** has a destination port of 21.

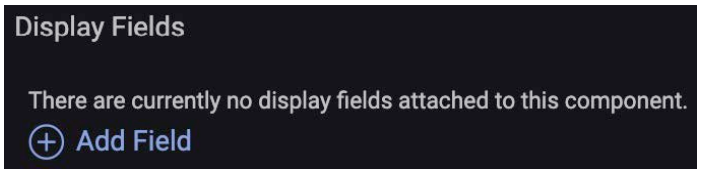


19. Once finished, the component window can be collapsed and the component appears in the **component list**.

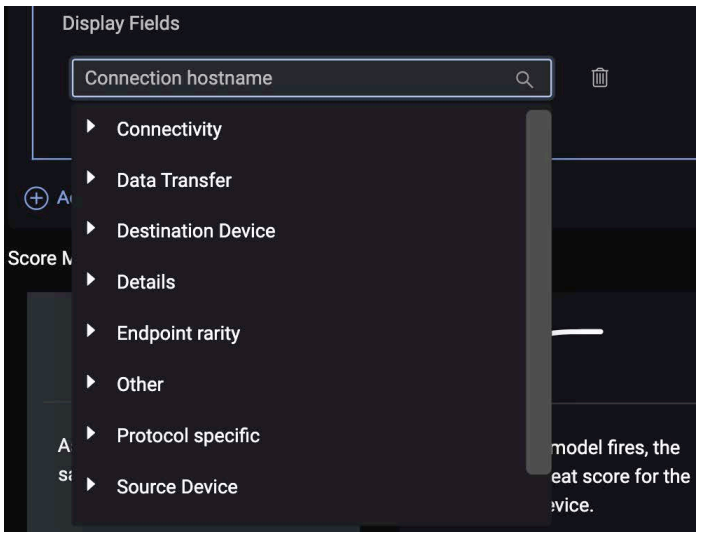


20. For **testing and viewing thresholds**, it may be useful to add display fields. These may also be useful as they can be presented in the Breach Log summary without impacting whether the Model was triggered:

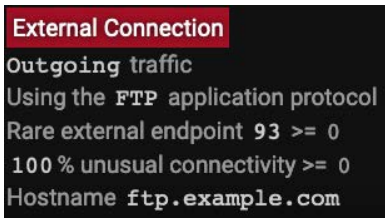
    a. Click **Add Display Fields** to open up a new section in the component.



    b. Choose **appropriate display fields** in the same way as selecting filters from the list.

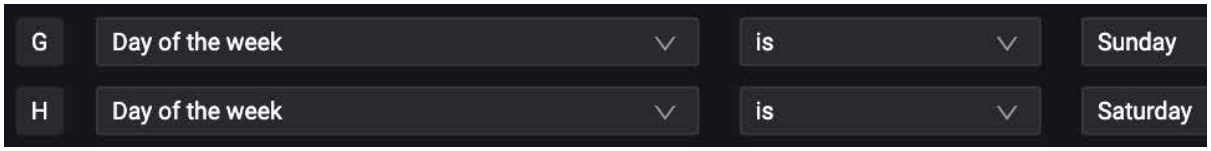


    c. When the component is triggered, elements of the component definition will be recognizable in the resulting **Breach Log** summary

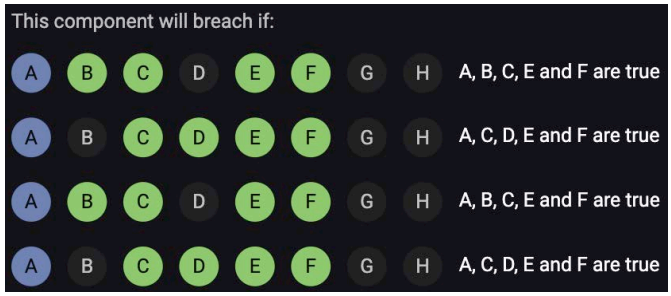


Complex Filter Combination Tip:

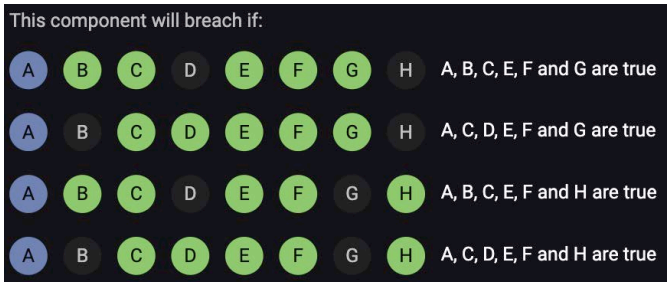
Notice there is no weekend filter. To combat this, create a **pair of filters** by clicking **Add Filter**, searching **week**, selecting **Day of the week** and applying **Saturday and Sunday** values.



Duplicate existing Model Logic.



Add the new filters to both sets of the Model Logic so one set covers filter G and the other set covers filter H.



Exercise: Creating a New Model

a. The use of internal RDP connections pivoting from one device to another is interesting behavior and should be investigated.

Within the Model Editor, create a new Model and save it into a new folder in the root directory called "**Training**". This is achieved by entering the value into the Folder text field:

Set the **Model Name** as your first name.

Configure the Model to the following criteria:

- Ensure the Model will breach if **All Components Are True**.
- Internal connections > 0 in 60 mins
  - A. Application Protocol = RDP
  - B. Destination Port = 3389
  - C. Direction = Outgoing
  - D. Unusual outgoing data volume > 10 %
  - E. Day of the week is Sunday
  - F. Individual size up > 1000
- Set the Model to only breach if all the Filters are true. However, configure it so that it will breach if either the **Application Protocol** or the **Destination Port** filters are true.

View the **cheat sheet** at the end of the manual to check your answers.

b. Create a new Compliance Model to check if a server is accepting significant volumes of incoming SMB connections using the smb1 protocol. The Model requires the definition of two Components:

- Set the **SMB Write** metric:
  - Exclude administrative connections types, such as backups, known scanners or other predictable admin activities that are observed in SMB traffic.
  - Check the direction of the connection.
  - Verify if the device is a Security Device.
  - Is 'smb1' string used anywhere (Use Advanced Search to discover what value this is stored in).

- Set **Internal Data Transfer (Server)** using a data volume you decide:
  - Check it is using the Same IP.
  - Verify which of the two SMB ports are actually used.

Once these components have been created, think about how they should be evaluated. For example, do they need to breach in a specified order? Within what time frame must both components breach? Also, think about how to employ the components in such a way that the Model checks for a minimum volume of data/writes between the client and server rather than general SMBv1 usage on the server.

View the **cheat sheet** at the end of the manual to check your answers.

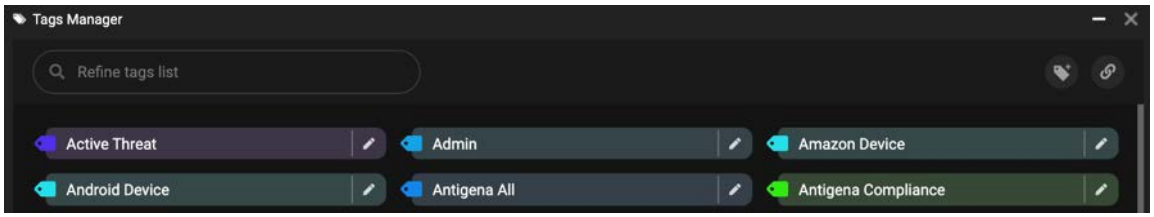
3. Darktrace Optimization

Tags

Tags are used to label devices. They can provide rapid navigation and UI context when browsing devices. Tags are a good way of defining “roles” within a network. They can also be utilized as filters when creating Models. Therefore, Models can be configured to only breach if a device belongs to a specific tag, or to exclude devices with a specific tag.

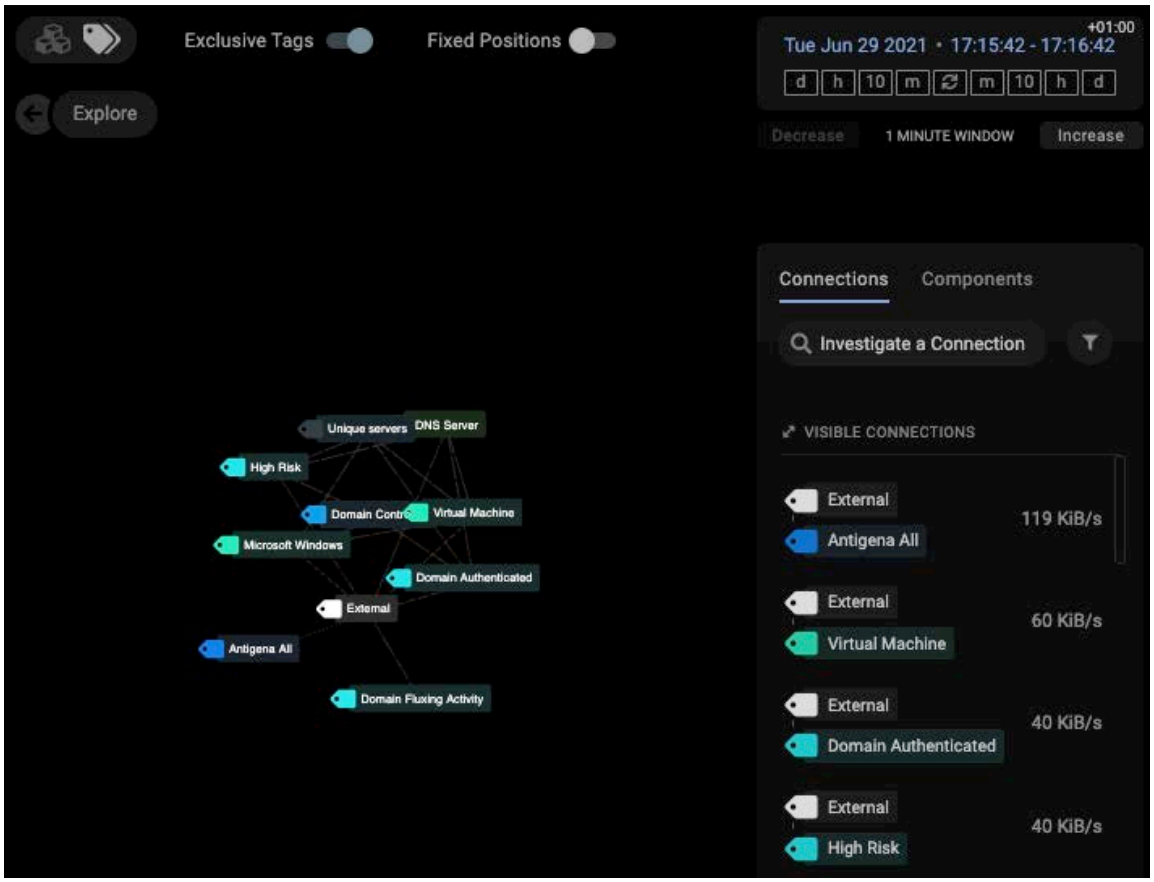
1. On the Threat Visualizer home screen, click **Menu** and select the **Tags** icon.

A **Tags Manager** dialog window will open displaying all current tags for the network.



2. In the top right of the Tags pane, there is a button called **Explore Tags**.

Once clicked, this opens a new tab demonstrating the Explore feature. This allows interactions between different tagged devices to be observed in an alternative visual format.



3. Create a new Tag by clicking the **Add New Tag** symbol.

   a. Enter a tag name, e.g., **Training**, in the Name field.

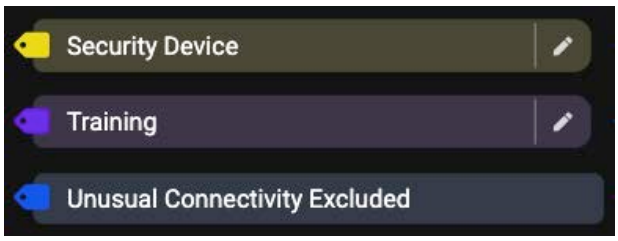
   b. A **description** can also be added to help identify the reason for the tag.

   c. Selecting a **color** assists in identifying the tag when assigned to a device.

   d. Click **Save**.

4. The new Tag will appear on the **Tags Manager** dialog window.

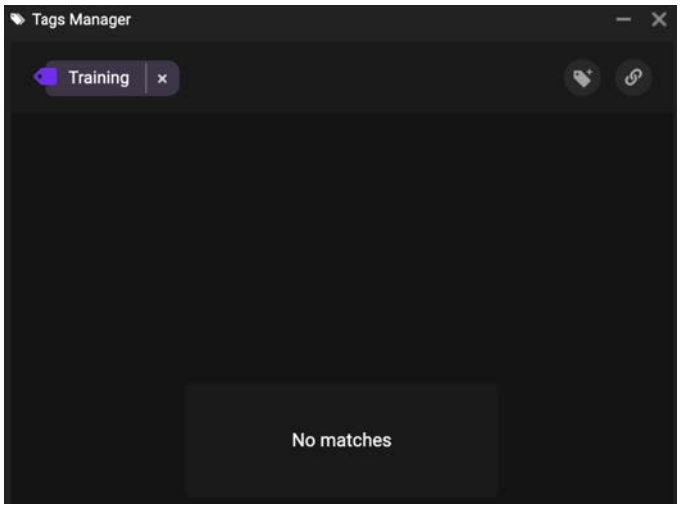
   Note: *As seen with the Unusual Connectivity Excluded tag, some tags may not have a pencil symbol. This means they are protected and cannot be edited or deleted.*

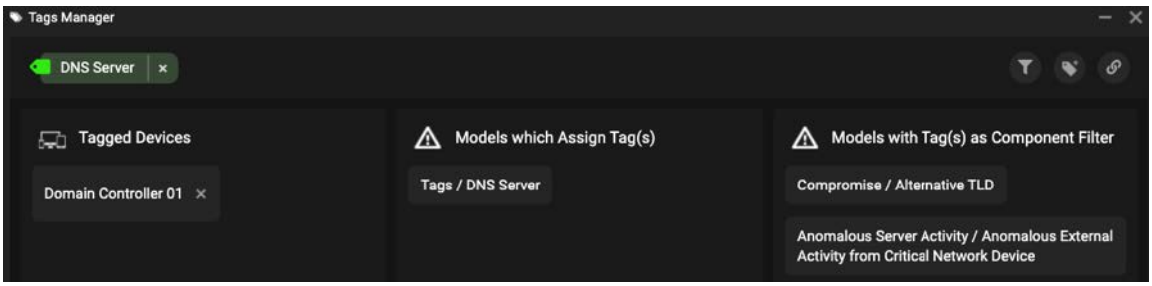


5. **Click the tag** (not the pencil symbol) to reveal new options.

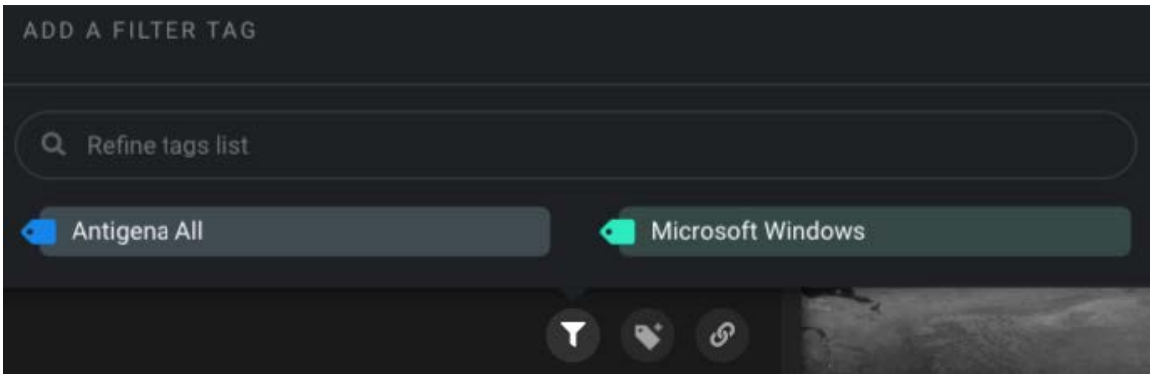
   a. The newly created tag will show No matches, because it has not yet been applied to any devices or Models.

   b. By selecting a mature tag, a new view will open in the **Tags Manager window**. It displays the selected Tag in the top corner and lists any devices tagged as well as showing if any **Models are assigning or using the Tag**.





6. Within this Tags Manager view, there may be the option to **add further filters** to narrow down the results displayed. Here, more Tags can be filtered/applied to the Tags Manager to see which devices are tagged and which Models are referred to.

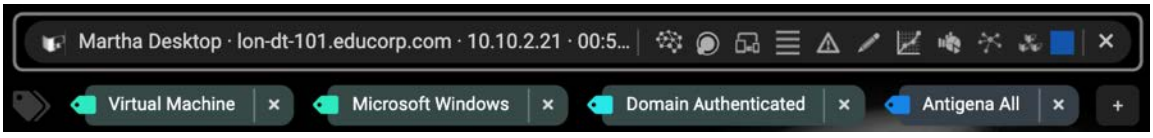


7. When a device view is selected in the Threat Visualizer and is populated in the Omnisearch bar an additional button is displayed in between the Add New Tag and Explore Tags icons.

Click the **Add selected tags to current device** button. Refreshing the Tag Manager pane will reveal the device hostname within the **Tagged Objects** pane.

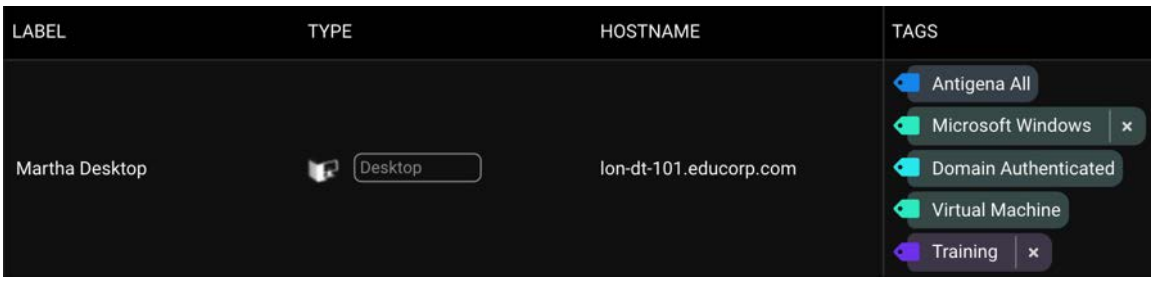
__Note:__ If a device already has the selected Tag and a user attempts to apply the same Tag, a waning message will be displayed.

8. When a device is selected, the **Tags are displayed below the Omnisearch bar**.

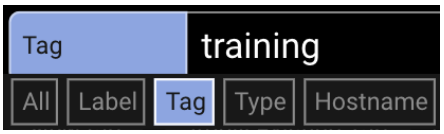


__Note:__ The plus button is another method to quickly append new tags to a device.

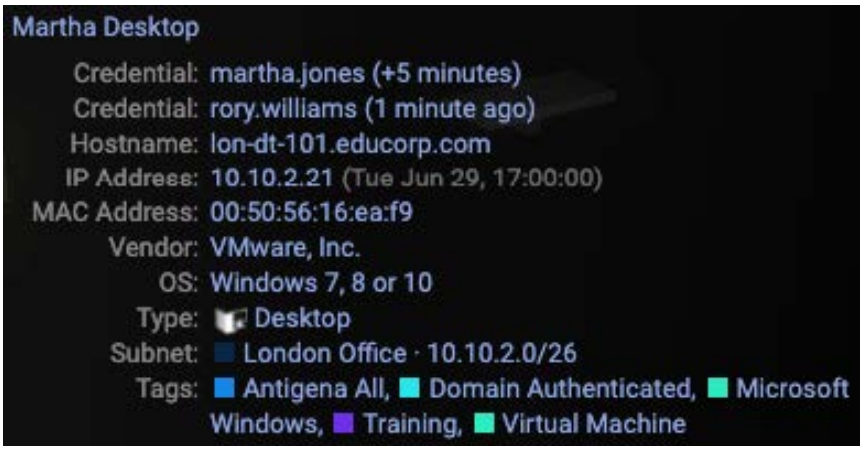
9. Entering a Tag in the search bar of **Device Admin** will list all devices associated with the Tag. This can be a quick way to locate devices on the network.



__Note:__ While searching for a term using All, for more accurate results, change this to the selected search element.

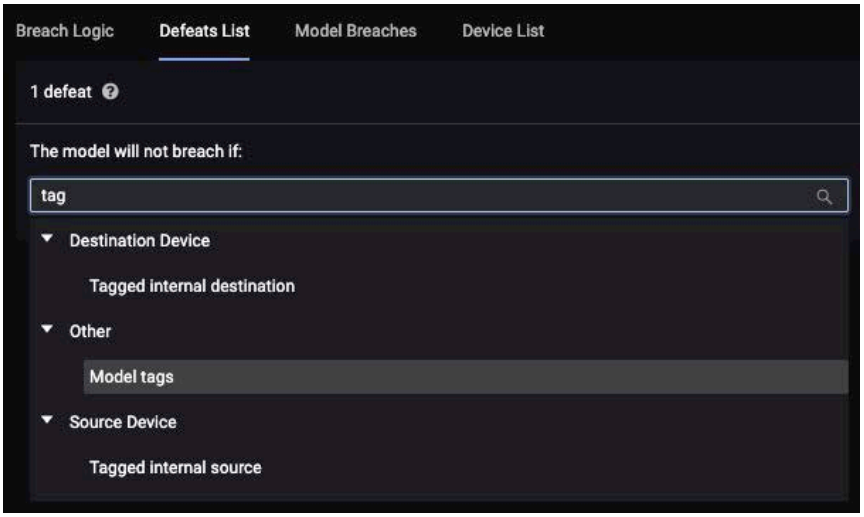


10. Tags are automatically displayed when **hovering over devices** in the Subnet and Device View.



11. Tags can also be employed as part of the **filter conditions for a Model** in the **Breach Logic** or as a **defeat** in the **Defeats List**.

    Select a relevant filter such as **Tagged internal source or destination**. Then set the comparator and value to reflect the desired action.

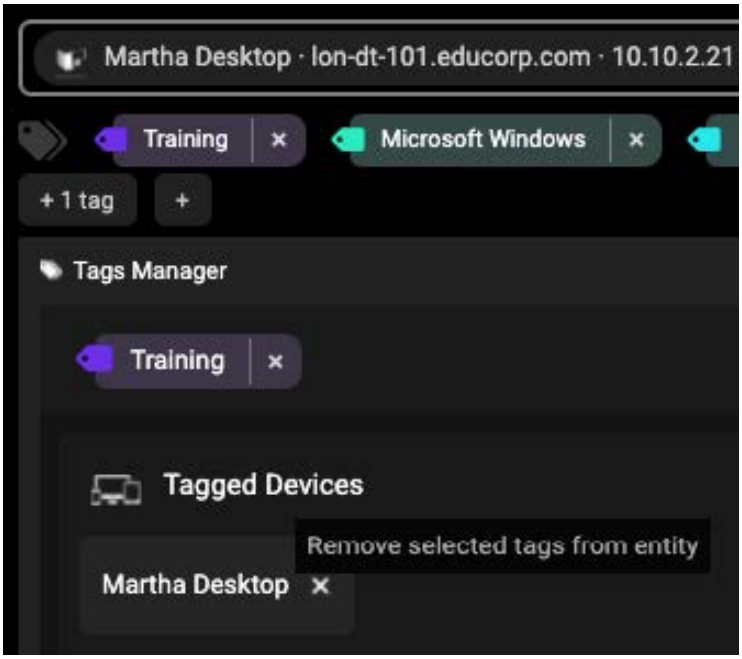


12. Tags can be removed using multiple methods.

    a. A simple way to remove a tag is by clicking the cross beside the tag name when the device is populated in the **Omnisearch bar**.

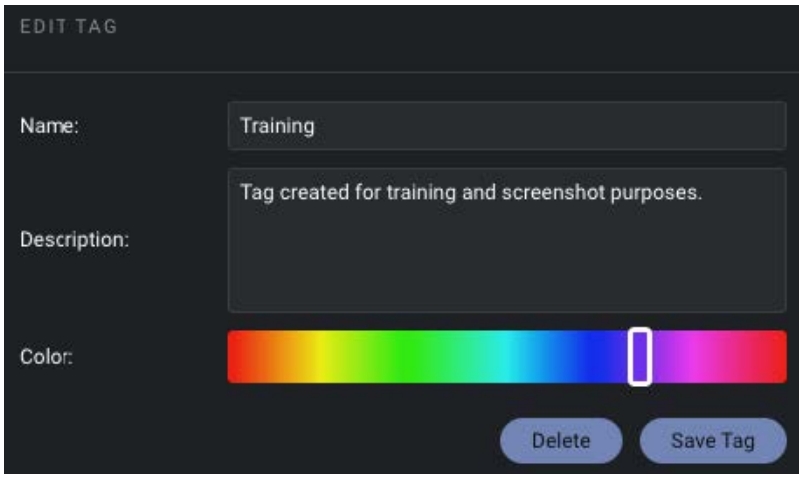
    b. Another method is to click the **X** in the **Tagged Devices** pane for a selected tag.

    c. **Deleting** a tag will also untag all the devices automatically which share the deleted tag.



i. To delete, click the open tag, or locate it in the Tags Manager and click the pencil symbol to **Edit tag**.

ii. Click the **Delete** button to permanently remove the tag.



Tag Tip:

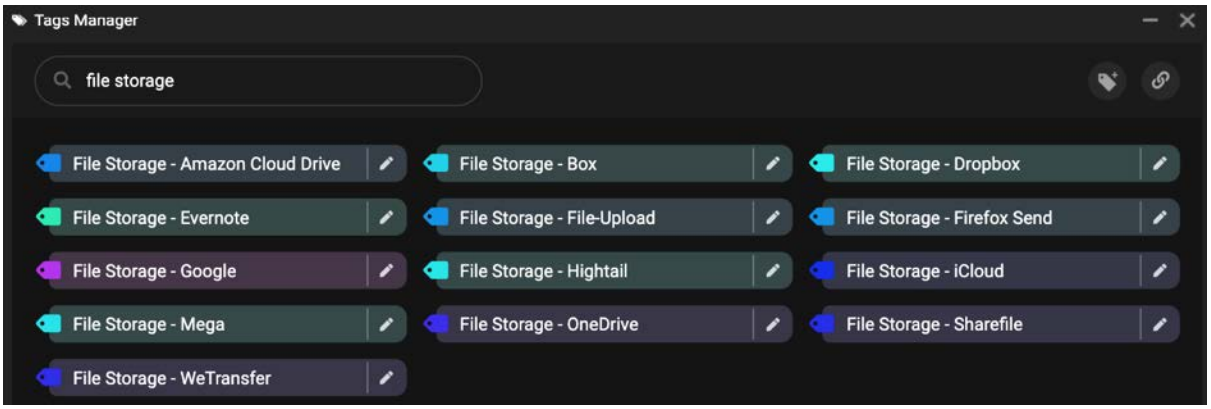
Models can be configured to automatically tag devices when breached. This is achieved by setting the Model action to Tag. It is better not to perform this step on a production system unless you are clear about the impact of such an action.

Tags Use Case

While some Models have been created to alert you to unusual or large data volumes to file storage solutions, it is not necessary to cause a Model Breach for every time a user accesses one of these endpoints.

However, some file storage solutions may not be compliant on your network. Therefore, it may still be important to you to be able to locate devices which have been identified accessing these.

By utilizing the search bar in the Tags Manager, search for “file storage” to see a list of associated Tags. These different Tags can be clicked on to view which devices have been using particular types of file storage solutions.



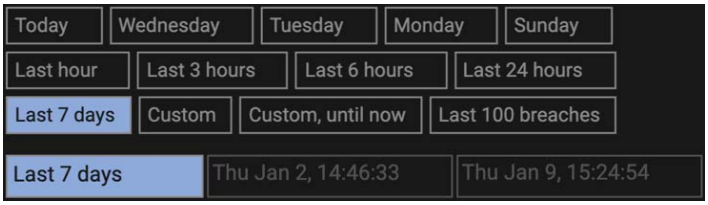
These Tags are also a great way of being able to filter the Device Admin page, allowing you to review the use of these services for compliance without being alerted.

This range of Tags are applied by File Storage Models but, as Models are entirely customizable, the Models can be edited to monitor different solutions using various methods. This could include rolling Models back to previous versions or turning off auto updates for particular services.

Model Tuning

To get the most value out of a Darktrace appliance, it is important to keep it manageable and ensure Models do not breach too frequently. This can be achieved by optimizing and tuning Models to make them more relevant to your particular corporate environment and thus more accurate. This not only lowers the risk of important Model Breaches being missed, but it also lowers overhead for the appliance, thereby improving performance.

1. Firstly, in order to ascertain which Models are breaching more than they should, it can be a good idea to zoom out to a larger time frame to try and get a wider overview. We recommend this be at least the **last 7 days**.



2. Then sort the Threat Tray by **Models, most breaches** in order to gain and understanding of which Models are generating too many breaches.

3. Now presented in the Threat Tray is an **ordered list** of candidate Models. Using this method, it should be easy to make a create a shortlist of Models which should be considered for tuning.

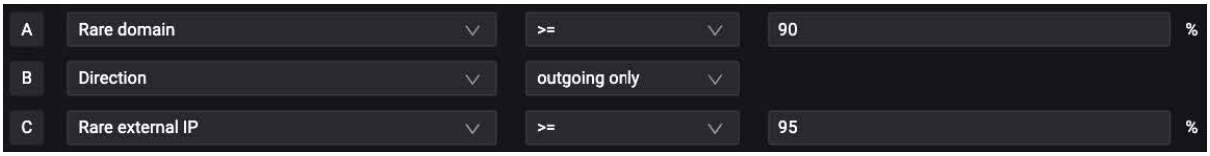
Covered in this Model Tuning section are the following three most important and widely used tuning techniques:

- The whitelisting of external domain names and IP addresses.
- The adding of internal devices to a model's device list.
- The attaching of defeat tags to devices.
- Extra considerations to help decide whether Models need tuning.

Intel: Trusted Domains

While adding devices to a Model's Exclude List is an option, it is also possible to add domains and IP addresses to a Trusted Domains list. Adding an external domain name or IP address to this list will keep the rarity score of those domain names or IP addresses at 0% for as long as they remain in the list. This action will affect Models which include a rarity filter in one of the components.

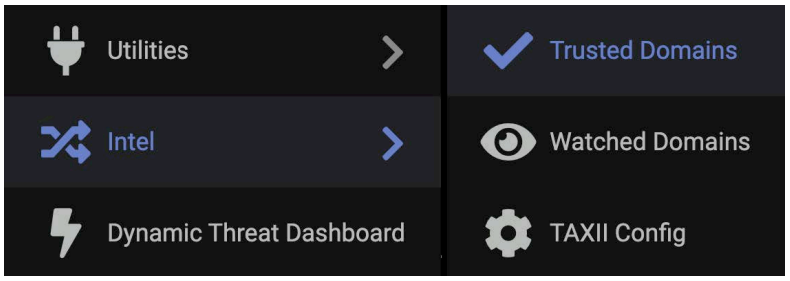
For example, notice the 90% and 95% thresholds in the filters for the **EXE from Rare External Location** Model.



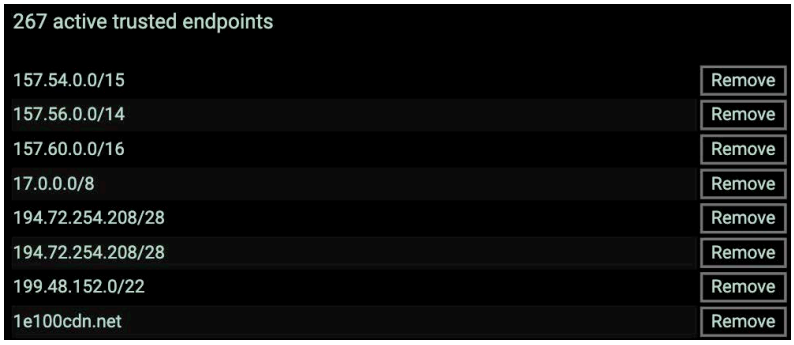
This method of tuning is normally used on larger networks of multiple thousand devices where a select few devices are commonly accessing a legitimate external endpoint and causing model breaches, but the scale of the networking means that the small number of the internal devices using this endpoint is not enough to bring it below the offending models rarity thresholds.

1. On the home page under Menu, select **Intel** > **Trusted Domains**.

   Alternatively, navigate to: https://<servername>/**whitelisteddomains**



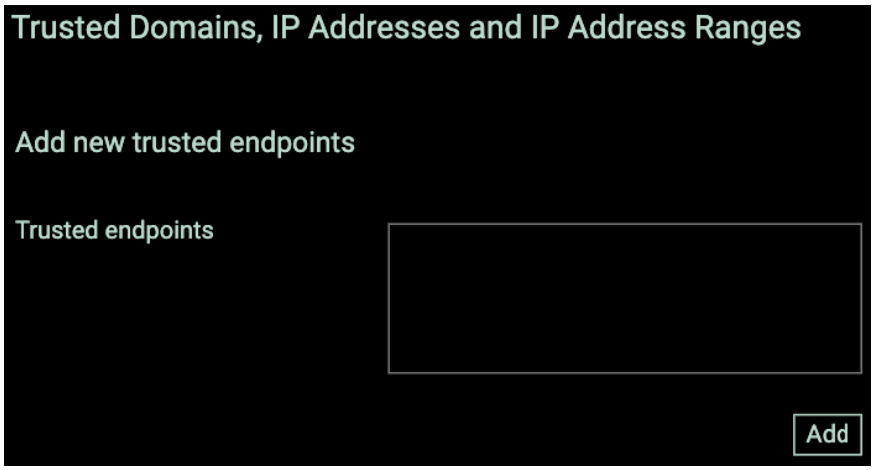
2. In the new browser tab, review any listed domains. By default, when Darktrace is first installed the Trusted Domains list contains **common domains**. Also, the system automatically adds very popular domains and presents a number of active trusted endpoints.



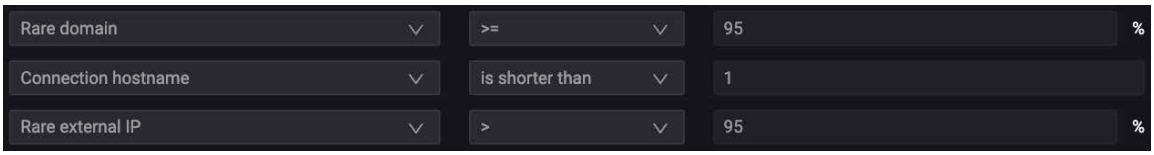
   Note: *IP ranges, such as one of Microsoft's (157.54.0.0/15), can also be included as an entry.*

3. When reviewing list entries, note that they can be removed from the Trusted Domains list by clicking the **Remove** button on the appropriate row.

4. To **include** an endpoint on the trusted endpoints list, input it into the text box at the top of the page. This will stop the endpoint from causing further breaches for models where rarity score is used as a component filter.



5. To understand the impact of adding an endpoint to the Trusted Domains list, review the **HTTP Beaconing to Rare Destination** Model in the **Compromise** folder and view the component.



The **Rare domain** and **Rare external IP** filters are examples which contain a **rarity score**. In this case, the Model will only breach if the domain is at least 95% rare or the external IP address is at least 95% rare. If the endpoint is a domain set on the **Trusted Domains** list, the corresponding **Rare domain** filter is set to 0 and so the filter contributes to preventing a breach.

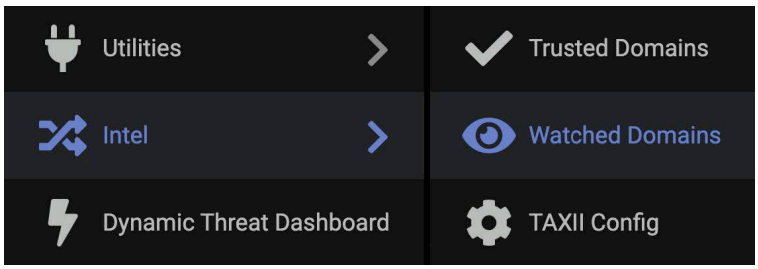
Adding endpoints to the Trusted Domains list is a quick way to reduce false positive breaches on Models which include rarity filters.

Intel: Watched Domains

Under the same Intel menu as the Trusted Domains, there is another option called Watched Domains which contains a list of domains and IP addresses which will cause an alert when a connection to a set domain is observed on the network. While this may not tune Models down, it can be utilized to cause alerts based on certain endpoints. A use case could be that company policy dictates that users should not connect to certain domains, such as dropbox.com.

1. On the home page under Menu, select **Intel** > **Watched Domains**.

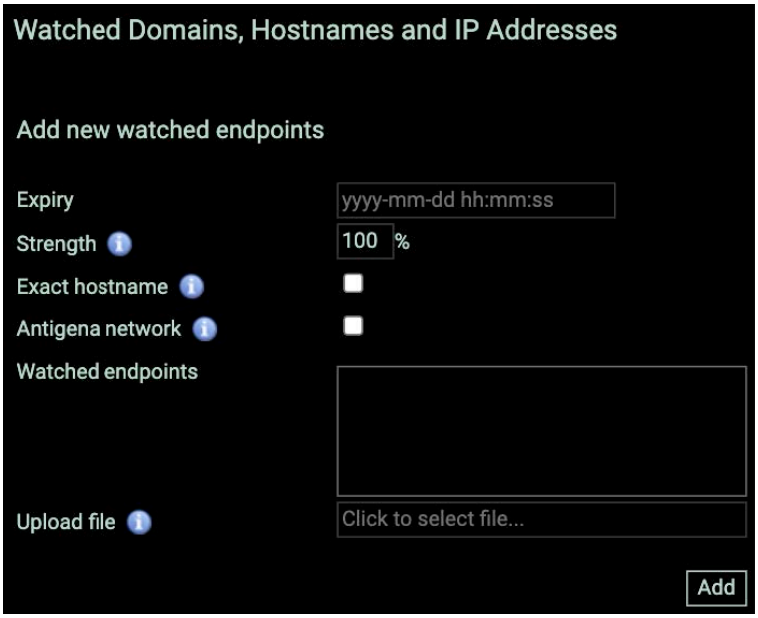
   Alternatively navigate to https://<servername>/**watcheddomains/**



2. Watched Domains can be **manually added** either individually or can be **uploaded** as a list in a text file.

   Entries can be given an expiry time and a strength to be used as a Model filter. Entries will match a domain by default but can be set to match an exact hostname instead.

   Also, if licensed, Watched Domain entries can cause Antigena Network actions to be triggered.



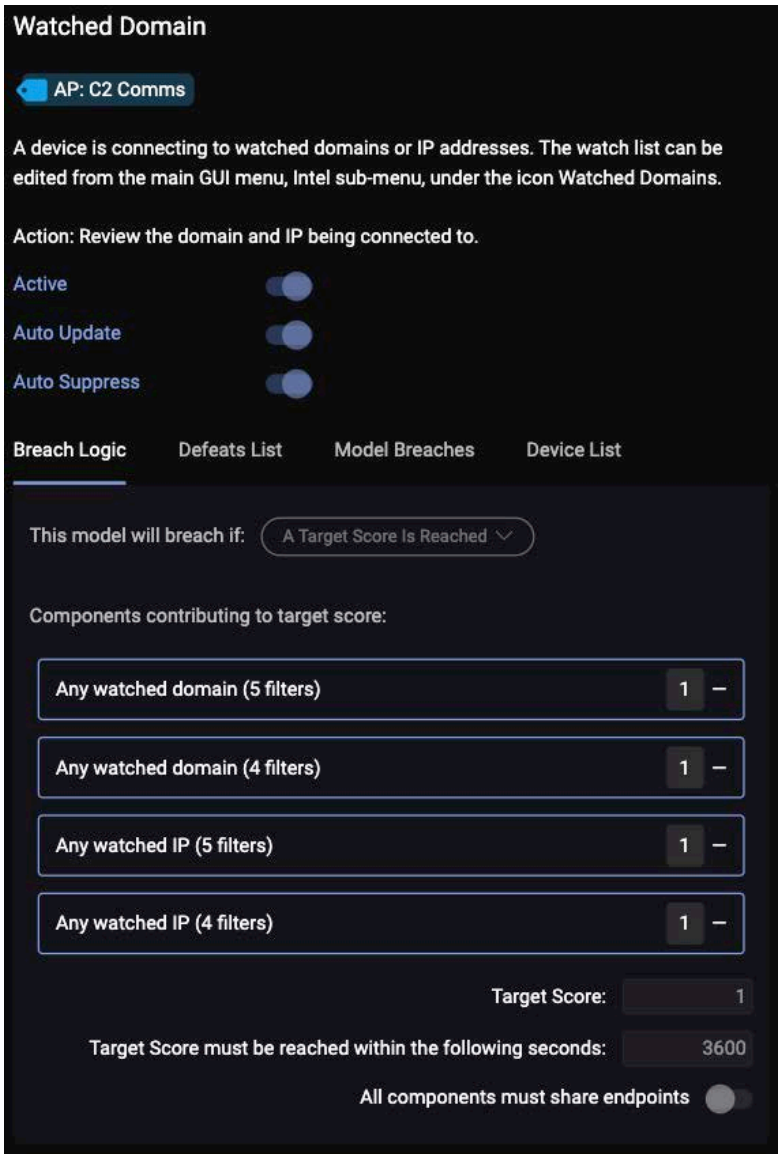
Note: *Watched Domain entries can also be managed through the API using an Intelligence Feed command called /intelfeed.*

3. Review the list of **active watched endpoints** beneath the input section.

4. Watched endpoints can be removed by clicking the **Remove** button at the end of the respective row.

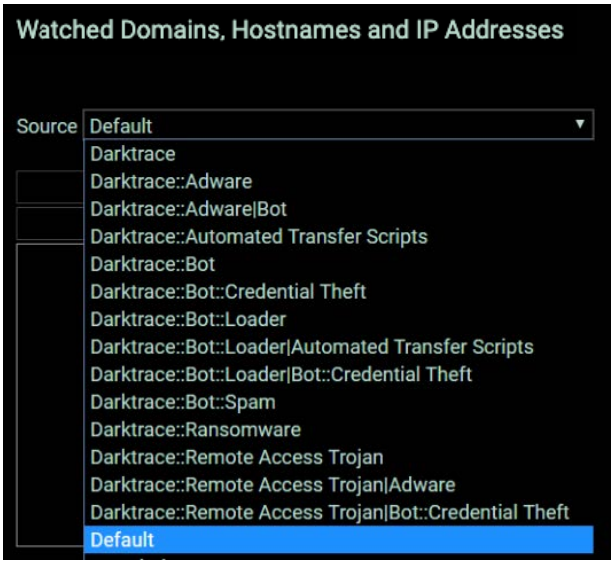
5. Any domain or IP address entered in the watch list will trigger the **Watched Domain** Model breach in the **Compromise** folder whenever a connection on the network is made to that domain, providing immediate alerting to this activity.

   Note: *Similarly, if Antigena Network is licensed and enabled, an* ***Antigena Watched Domain Block*** *Model will* ***block any connections*** *to entries on the Watched Domain list.*



6. If subscribed to **Darktrace Inoculation**, Darktrace will automatically populate a drop-down menu with a Source of lists.

   These lists are hashed, but they contain anonymous IPs and domains which through the inoculation service have been identified as important and will trigger a model breach.



Adding to a Model Devices List

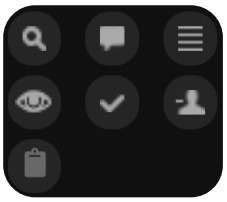
Adding a device to a Model's exclude list allows us to make certain devices exempt from breaching specific Models, effectively telling the Model to **ignore devices on that list**.

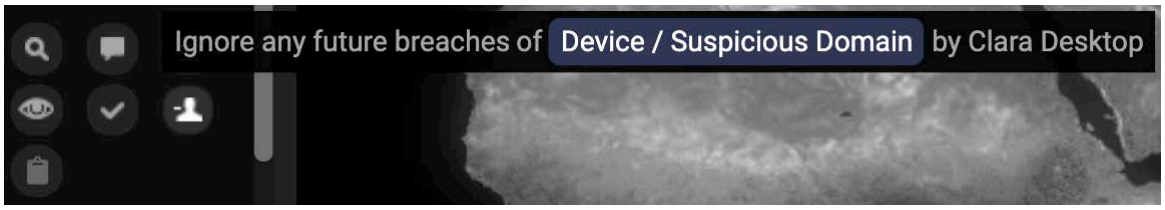
This method is useful in multiple cases, such as:

- Telling Darktrace that a device is allowed to carry out specific activity.
- Tuning Models that deal with external activity, but **do not have a rarity filter**.

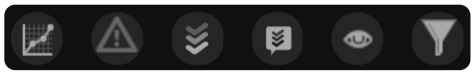
1. The quickest way to perform this tuning is to click the **ignore future breaches** button in the **Breach Log**, as indicated by the person icon in the middle row on the right.

   This will add the device that caused to the Model breach to the current Model Devices list and ignore any future breaches.





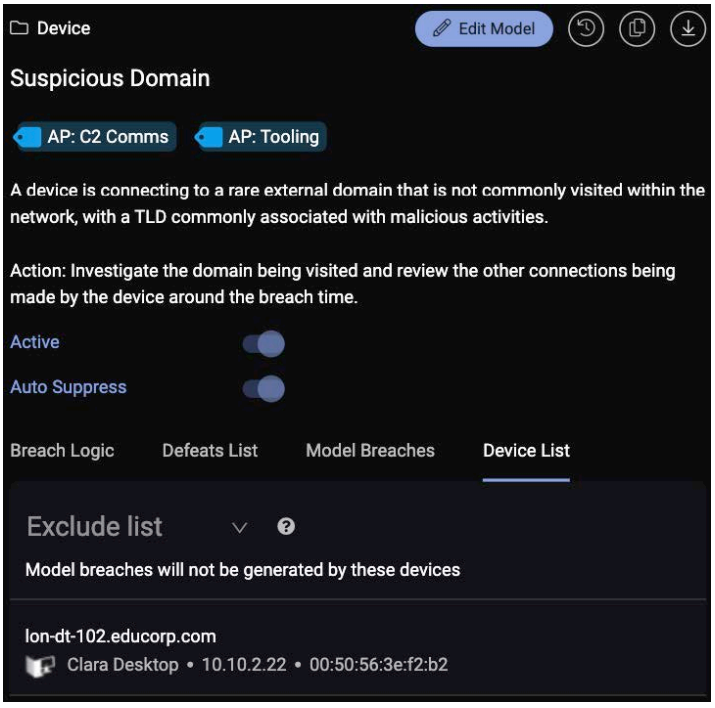
2. To confirm this was successfully carried out, navigate to the **Model Editor** by clicking the **warning triangle** from the selection of icons at the top right of the Breach Log.



3. Within the Model Editor, locate the **Models tabs** underneath the Model description. Select the **Device List** tab.

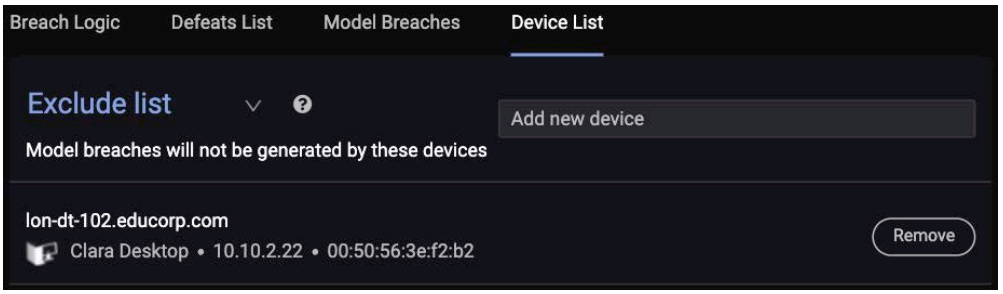
4. Here, it is possible to confirm that the device has been added to the Model's **Exclude list**. This list displays which devices are currently being ignored by the Model.

   Note: *Devices can either be on Exclude list or an Include list. When adding devices to the Exclude list, Model breaches will not be generated by them.*



5. To remove devices from the Exclude list, first click **Edit Model** in the top right-hand corner.

6. Within the **Device List**, notice some subtle changes:



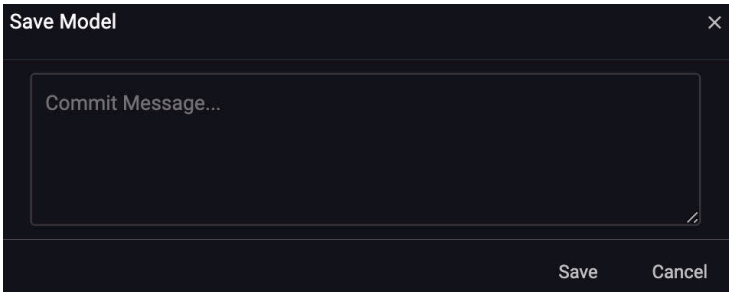
   a. The Exclude list is now blue. By using the drop-down menu, it can be changed to an **Include list** which means the Model will only fire for listed devices.

   b. Also, there is now the option to **Add new device**. This enables the user to search for and append devices to the chosen list type.

   c. Finally, notice that the recently added device now has to option to be removed. Click **Remove** to take this device off the Exclude List.

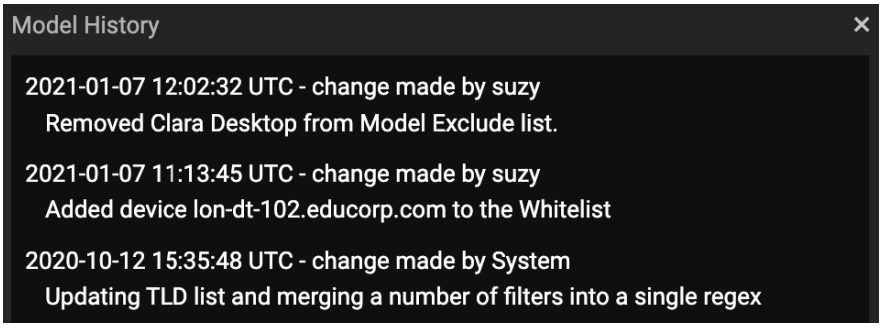
      i. If removing a device, the Model needs to be saved. Click the **Save Model** icon in the top right of the Model Editor.

      ii. A **Commit Message** must be input in order to apply changes. Ensure that a sensible message is entered so anyone reviewing the Model History can understand what changes have been made.



      iii. Changes made to a Model can be viewed by clicking **Model History** in the top right.

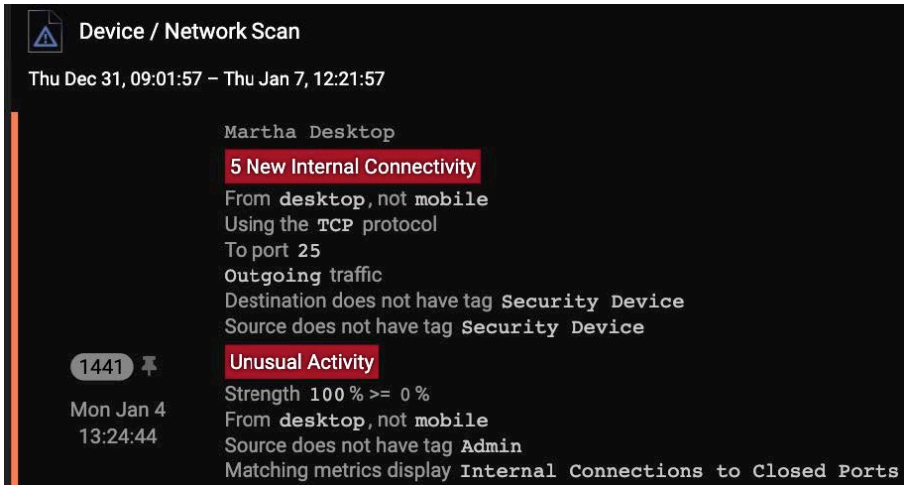
      This opens up a dialog which will list changes, who made them and at what time.



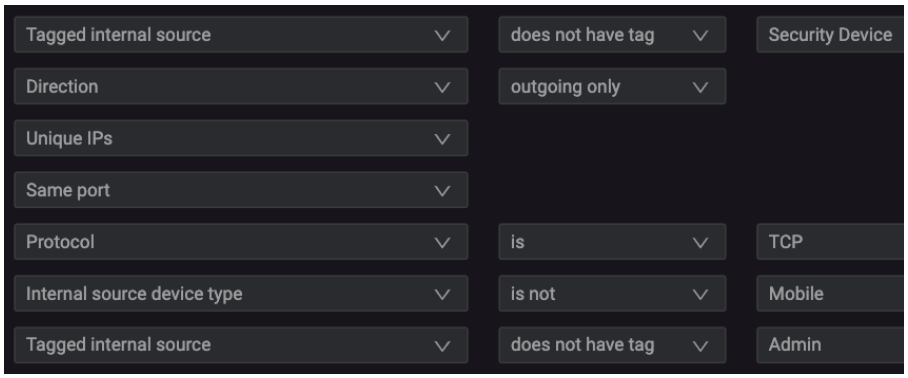
Using Defeat Tags

Tags can be useful for informing Darktrace of the specific roles of a device. This means that devices can be made exempt from breaching on activity expected for such a role. As such, many Darktrace Models have defeat tags listed in their **component filters**. Usually, adding a one of these tags to a device can stop it from breaching a range of Models. These defeat tags can normally be seen in the **display fields** of a Model Breach, as seen in the example below.

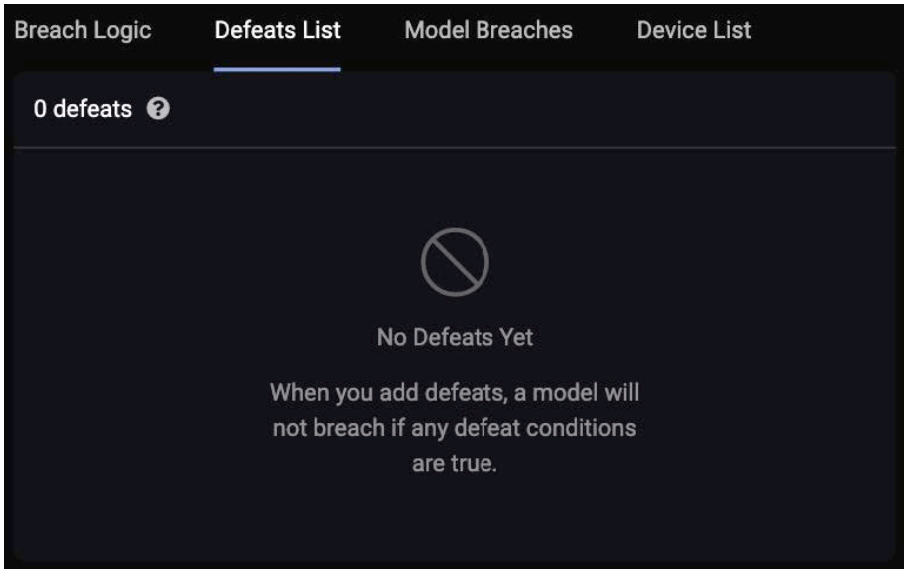
- *Source does not have tag **Admin***
- *Source does not have tag **Security Device***
- *Destination does not have tag **Security Device***



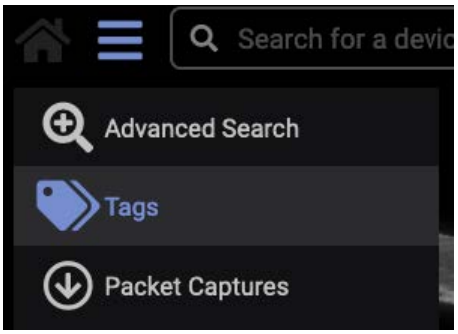
In the **Network Scan** Model, it can be seen that the **Security Device** and **Admin** tags are being used as defeats which, in this case, means any devices with this tag applied are exempt from this Model.



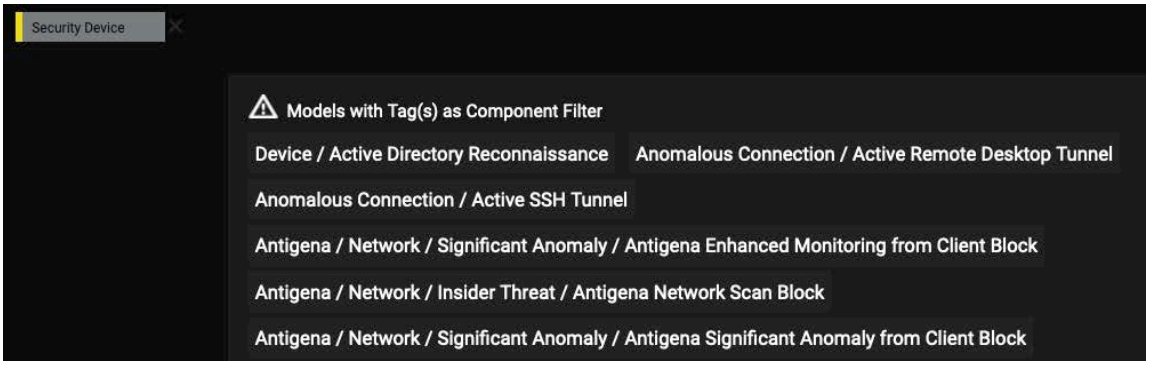
If tags are not already included in the Breach Logic, it is also possible to add Model defeats or tags directly to the **Defeats List**.



1. It is important to be aware of other Models which use the same tags and what effect adding the tag to a device may have. To check this, access the **Tag Manager** by selecting **Tags** from the Threat Visualizer main menu.



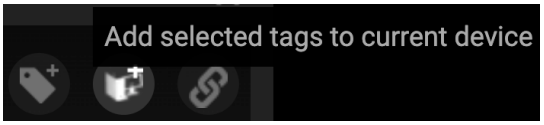
2. Locate the relevant Tag to see a list of all the Models that use the selected Tag as a filter in one or more of their components. Remember that tagging a device with this Tag will affect **all of those Models**.



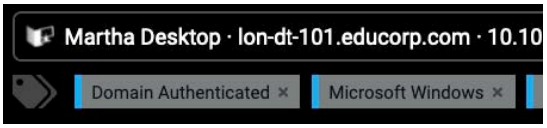
__Note:__ Any of the Models in the Tags Manager can be clicked so they can be reviewed in the Model Editor.

3. There are multiple ways to apply a Tag to a device. The first way could be carried out with the **Tags Manager** still open on the selected Tag. Make sure that the device to be tagged is populated in the Omnisearch bar.

   If this is the case, there is the option to **Add selected tags to current device** in the Tags Manager pane.

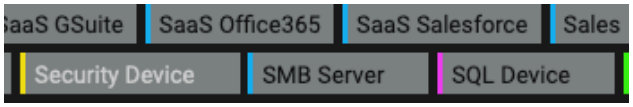


4. Without the Tags Manager open, Tags can instead be applied to a **device directly** from the Threat Visualizer. Navigate to a device in the Omnisearch bar.



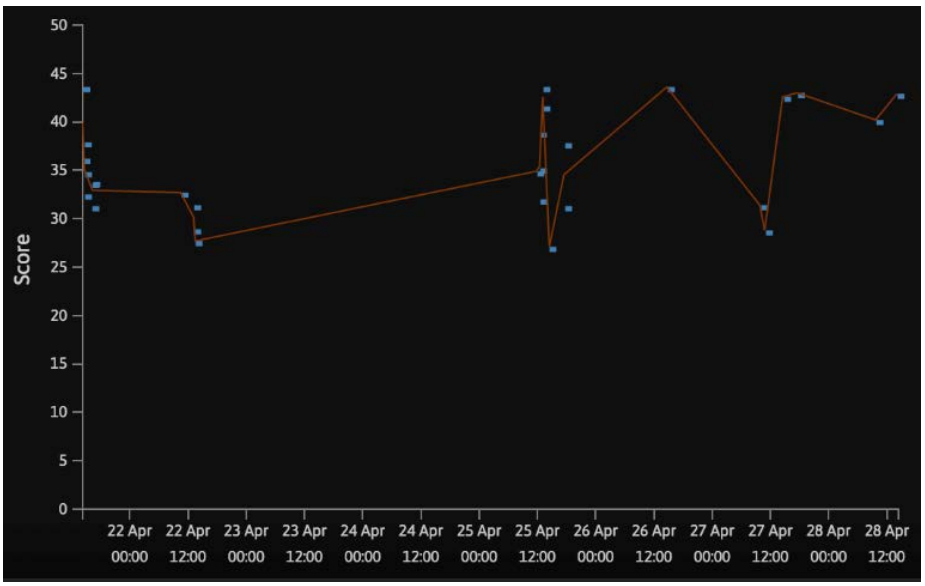
   a. Click the **plus icon** to the right of the exisiting Tags displayed below the device.

   b. From the alphabetical **list of Tags** presented below the plus icon, hover over the desired tag and **click** it to **add it to the current device**.



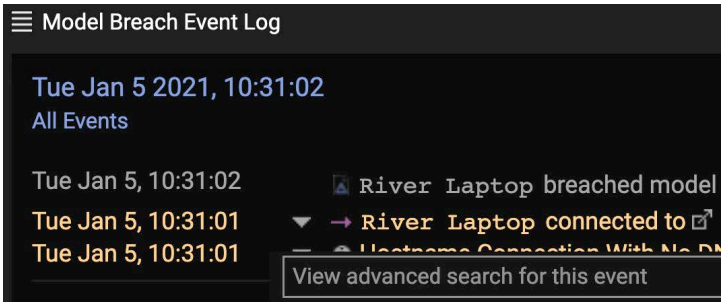
Considerations for Tuning Models

1. With a Breach Log open on a Model selected from the Threat Tray, view the breaches over time by clicking **View Breaches Graphically** from the selection of icons in the top right.



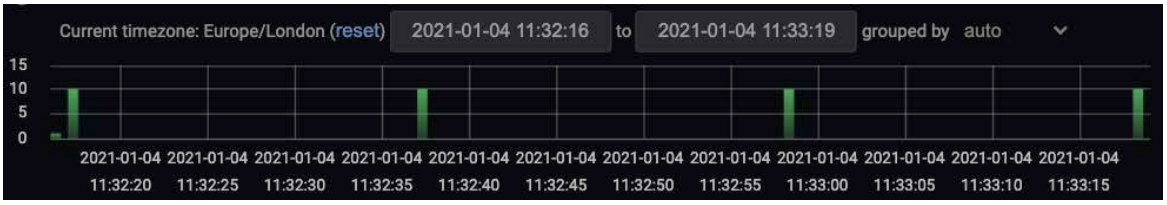
   a. Does the same device breach all the time?
   b. Are breaches of this Model common?
   c. Are these legitimate routine operations?

2. From a breach that may require further investigation, use the drop-down arrow within the Model Breach Event Log.



   Selecting the **View advanced search for this event** link will open the event in Advanced Search.

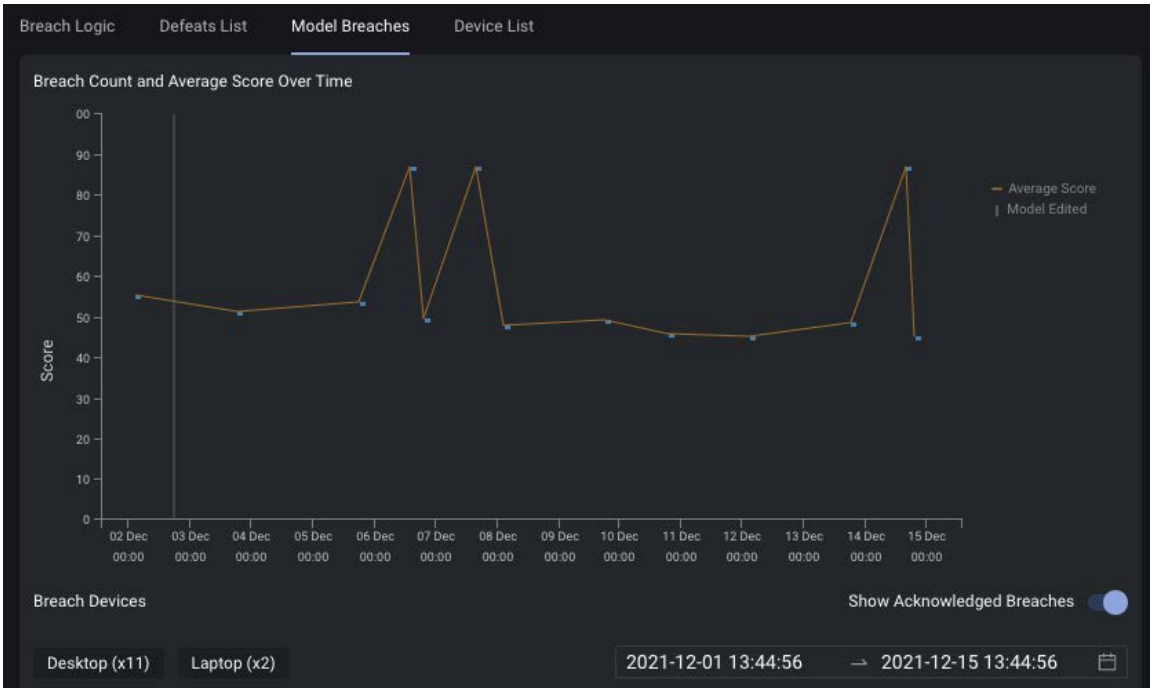
   This will focus on one particular event, so it is important to explore similar connectivity and review the spread of events.



   a. Are the events grouped together or is there a predictable history of activity on the network?
   b. How far does the activity go back?
   c. Are these routine operations that shouldn't be alerted?

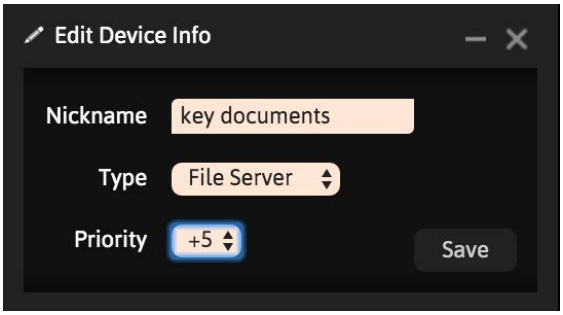
3. Returning to the Threat Visualizer, click the **View Model** icon at the top of the Breach log. This will directly jump to the Model Editor which triggered the breach.

Open the **Model Breaches** tab to see a graph of historical breaches.



a. Are there too many breaches or not enough?
b. Is it always the same device or device type causing breaches?
c. Do the Component and Filter settings need modifying?

4. With a device populated in the Omnisearch bar in the Threat Visualizer, click the **Edit Info** button.



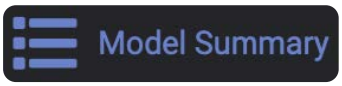
Notice the **priority** score. This will increase or decrease the device's threat score and flag greater interest to analysts about anomalies on the device.

a. Does the device contain sensitive documents?
b. Should the priority be raised to ensure breaches carry greater significance?

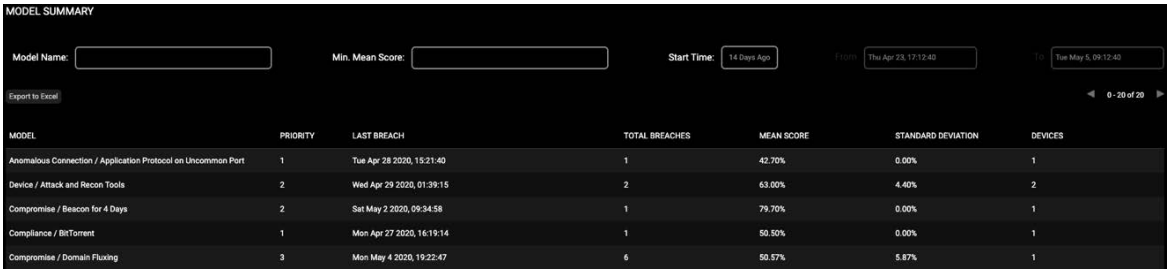
4. Model Menu

Model Summary

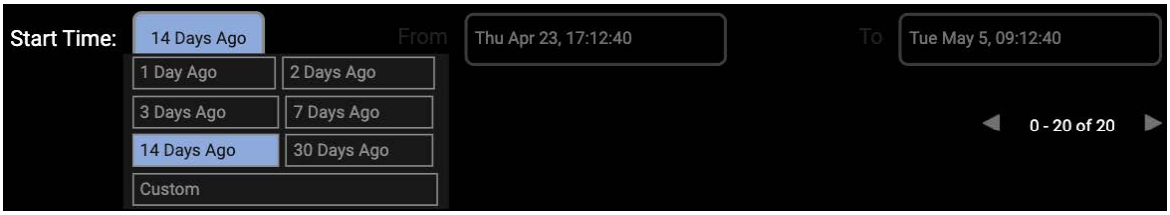
1. From the main menu, navigate to **Models** and select **Model Summary**.



2. The **Model Summary** page opens in a new tab. This page gives a **breakdown** of all the Models that breached on the network within a set period of time.



3. Set the **time period** in the top right of the page to determine how many results are displayed in the table. Clicking the **Start Time** option allows a range of pre-set time periods to be chosen. Selecting Custom allows the dates to be clicked on and changed.



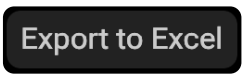
4. Within the **Model Name** box, type in a **search term** and hit enter to apply a filter to the table of Models.

5. Type a number into the **Min. Mean Score** and hit enter to filter the table.

6. Any of the columns can be **ordered** by clicking the headings.

MODEL	PRIORITY	LAST BREACH	TOTAL BREACHES	MEAN SCORE	STANDARD DEVIATION	DEVICES
Anomalous Connection / Application Protocol on Uncommon Port	1	Tue Apr 28 2020, 15:21:40	1	42.70%	0.00%	1
Device / Attack and Recon Tools	2	Wed Apr 29 2020, 01:39:15	2	63.00%	4.40%	2
Compromise / Beacon for 4 Days	2	Sat May 2 2020, 09:34:58	1	79.70%	0.00%	1
Compliance / BitTorrent	1	Mon Apr 27 2020, 16:19:14	1	50.50%	0.00%	1
Compromise / Domain Fluxing	3	Mon May 4 2020, 19:22:47	5	51.22%	6.23%	1

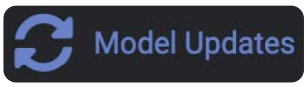
7. Finally, click **Export to Excel** to export the table into a spreadsheet format.

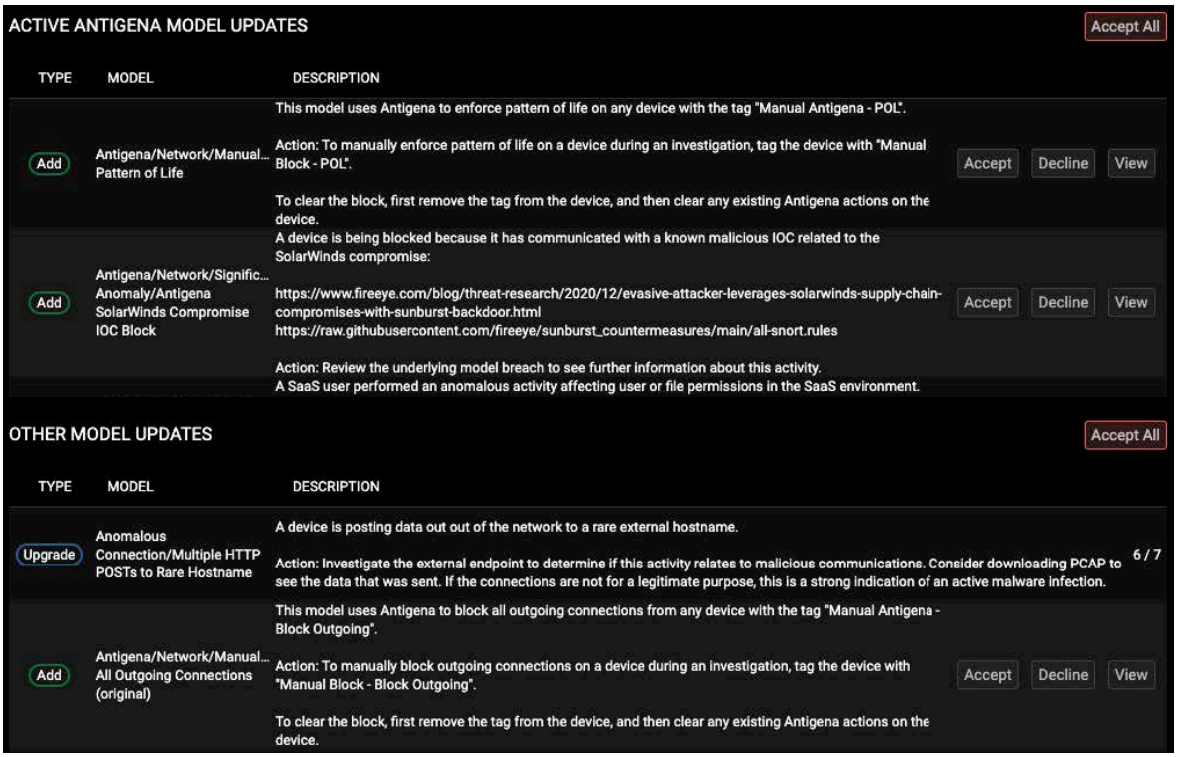


Model Updates

The Darktrace appliance will use the **Call-home** connection to check for new **updates** to Models every evening.

1. To compare user made Model changes with Darktrace updates, the Threat Visualizer menu includes a **Module Updates** function in the Models section. Changes implemented will be highlighted on this page.

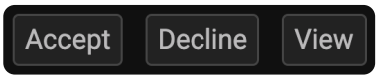


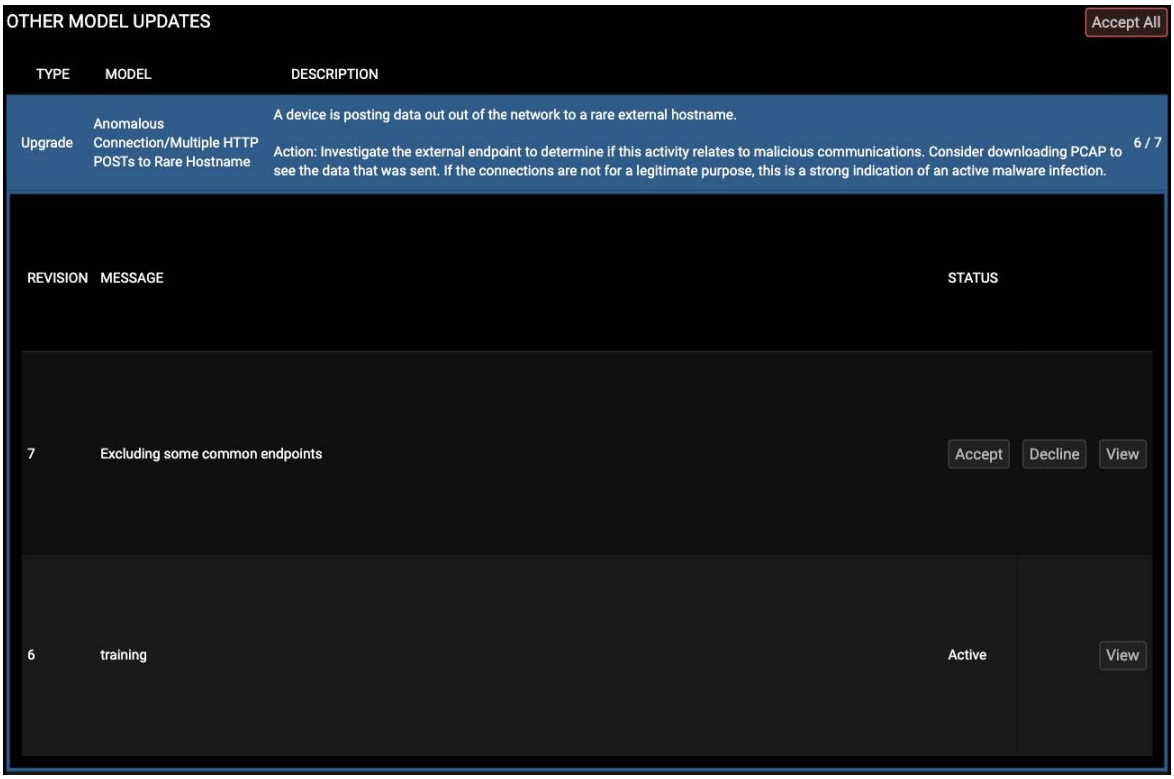


__Note:__ User updates made to a Darktrace Model will not be automatically overwritten. However, if a newer version of a Model that has been edited by a user is released by Darktrace, the Threat Visualizer application will ask if the user would like to proceed with the update. If yes, it will take the most recent version and user made changes will be lost (but they will still be visible in the Model History). Alternatively, it is advisable to duplicate a Model and edit the new one. The original Model can then be disabled so comparisons can be made over time.

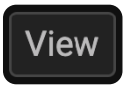
2. When Models are ready for updating, a message is displayed in the bottom-right hand corner of the Threat Visualizer interface. Click the **blue pending updates** button to review the Models.

3. Upon clicking and reviewing a Model, there are options to **Accept**, **Decline** or **View** the Model changes.





4. Click the **View** button for the current Model and suggested Model Upgrade to compare and examine what has changed in detail.



5. Once examined, choose whether to **Ignore** or **Upgrade** the Model.

5. Learning Outcomes

Thank you for completing the Part 2 of the Cyber Analyst course. We hope this has given you the confidence to successfully navigate the Model Editor.

Please complete the learning outcomes checklist below to check your learning.

☐	**I understand how Components, Metrics, Filters and Models function**
☐	**I can successfully create new Models within the Model Editor**
☐	**I understand the uses for Tags and be able to apply them to Devices**
☐	**I am able to edit Models to tune down Model Breaches to inhibit overfiring**
☐	**I can utilize Trusted Domain and Model Device Lists to triage the Threat Tray**

For all further education enquires, contact training@darktrace.com

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

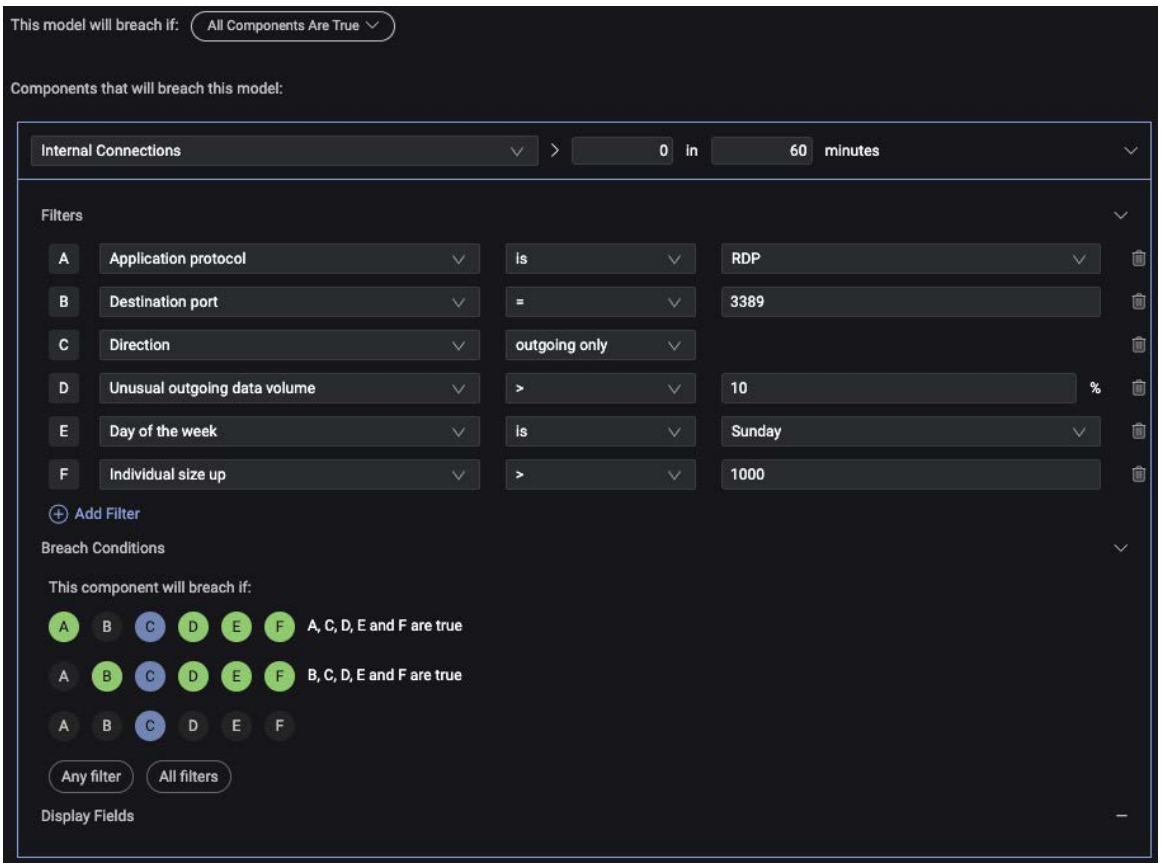
When contacting support, please make sure you provide as much detail as possible.

6. Cheat Sheet

Creating a New Model

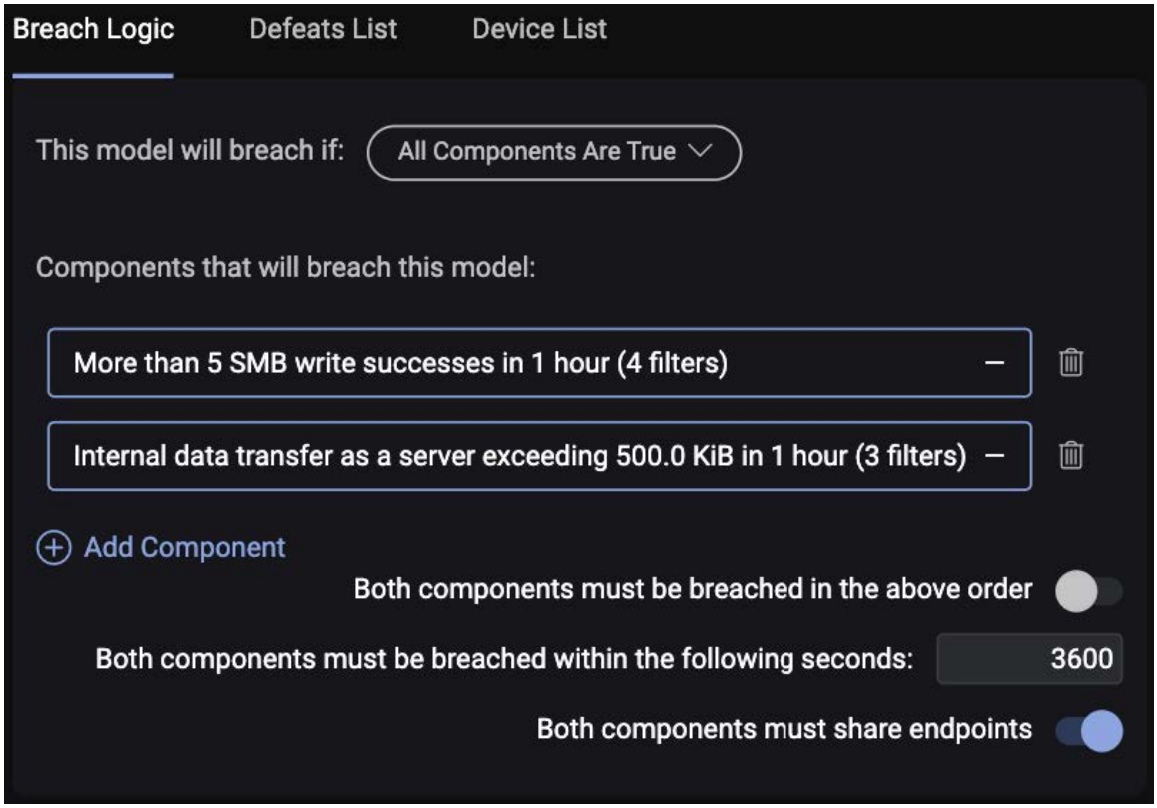
Remember: There is no need to reinvent the wheel! If you are thinking about creating a Model, first look through the Model Editor and see if any similar ones exist.

a. Creating a new Model to breach on a suspicious RDP connection:



Note: To assist in managing folders, Model files can be dragged and dropped into different folders to move them around.

b. Creating a Model to check for any **smb1 shares** still in use:

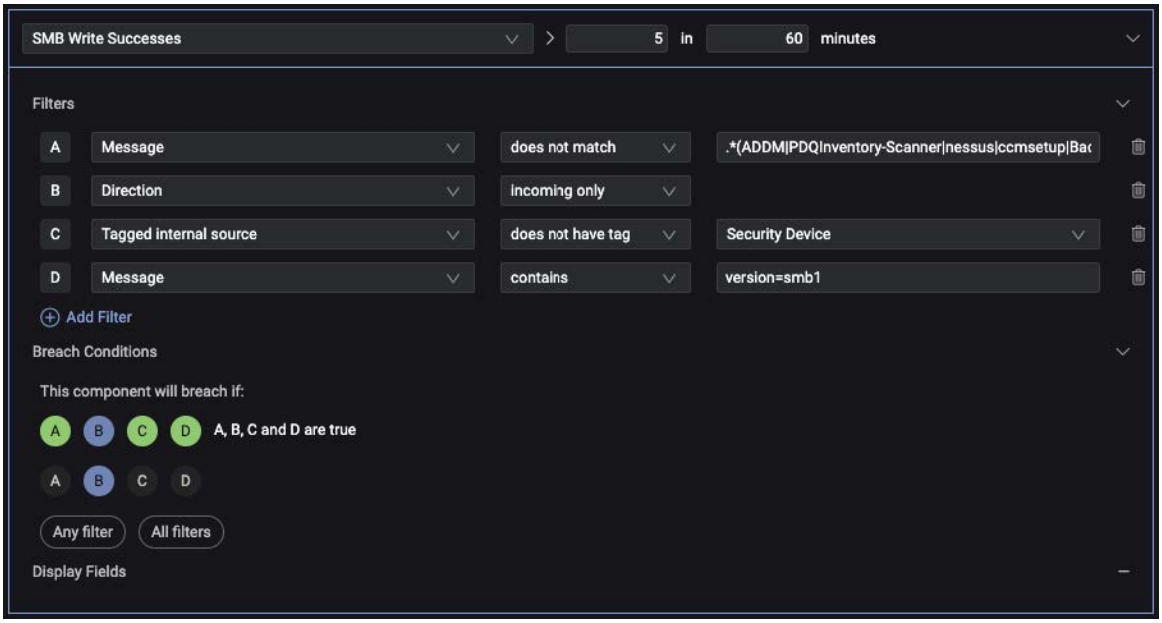


The toggle for **Both components must be breached in the above order** is set to NO so it does not matter which one fires first. However, for the Model to breach/alert, they both must be true in the same hour interval.

The toggle for **Both components must share same endpoints** is set to YES. This ensures that the Model fires specifically for the client performing SMB1 writes in the first component and the server outlined in the second component.

As this is a Compliance Model, it does not need alerting daily. As such, the wait time can be set to 3 days (259200 seconds).

Component 1



Review the Filter options:

- The selected component checks for more than **5 SMB Write Successes** in an hour using filters A, B, C and D.

- Only administrative connection type strings are allowed. This is why we check that the Message Filter obtained from the Connection does not contain any of these strings by using the following RegEx script: **.*(ADDM|PDQInventory-Scanner|nessus|ccmsetup|Backup).***

    - If one of the strings is found, the condition will be false, and therefore, the Model will not fire.

    - Utilize the RegEx tester in the Darktrace Utilities to help test your regular expressions.

- Unless a data transfer metric is selected, the Direction refers to that of the connection from the perspective of the device triggering the Model. Therefore, in this case, if you want to check for traffic to the device, you need an incoming direction.

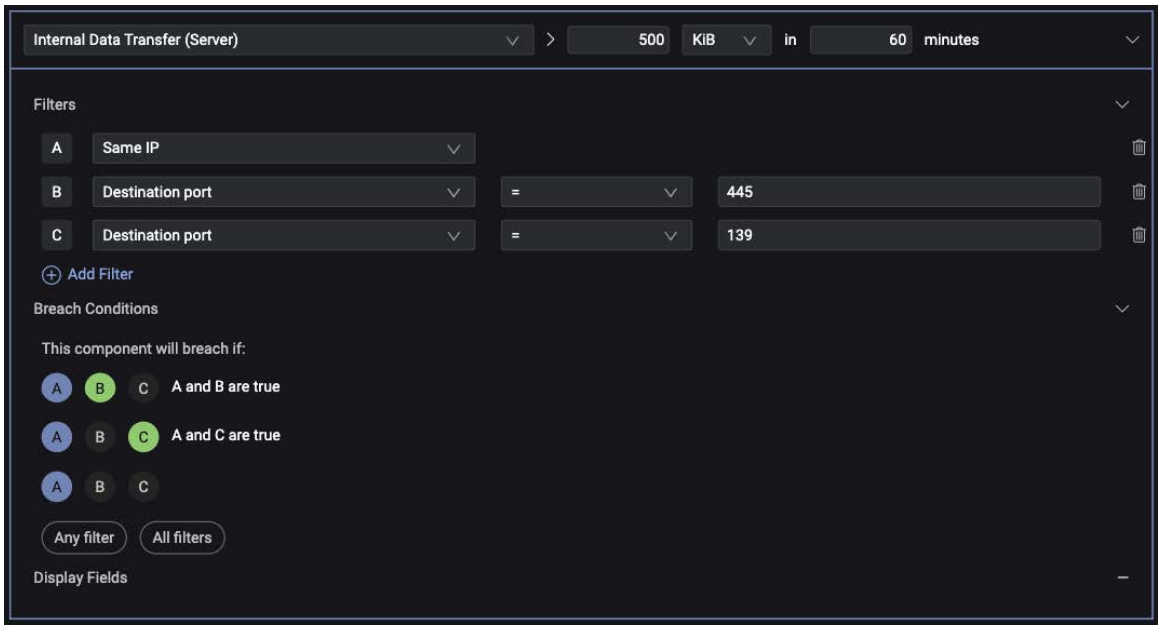
    Note: *When a data transfer metric is used, Direction refers to the transfer direction.*

- If the originator of the connection has been tagged as a 'Security Device', the condition will be false and the Model will not fire.

- If the protocol version is **not smb1**, the condition is false and the Model will not fire.

- All highlighted conditions have to be TRUE for the component to breach.

Component 2



Review the Filter options:

- The value of 500 KiB is used to avoid unnecessary alerts caused by simple handshakes that do not involve a real data transfer.

- For SMB traffic two ports can be used, 445 or 139. The implemented logic therefore tests if port 445 OR port 139 is used.

- All highlighted conditions have to be TRUE in one of the rows in order for the component to breach.

  Note: *An SMB connection starts off using the smb1 version protocol and writes/reads/deletes using the smb2 version protocol.*