DARKTRACE ACADEMY

DARKTRACE RESPOND/ NETWORK

Training Manual

Darktrace RESPOND/Network

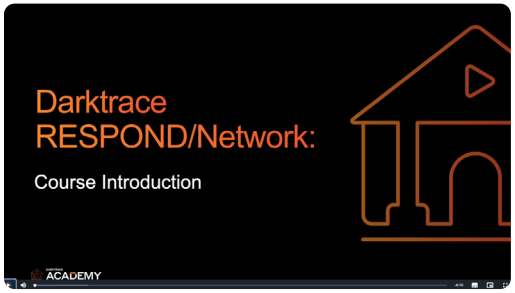
Training Manual
v1.4.3
Darktrace 6.1

Table of Contents

Table of Contents

1. Learning Objectives

Course Agenda



Start your learning with our dedicated video
1. Course Introduction

This course provides a comprehensive understanding of Darktrace's autonomous response capability. It is designed primarily for IT Administrators, who will oversee Darktrace RESPOND/Network. The following document serves as an educational guide for the key elements of Darktrace RESPOND/Network and Darktrace RESPOND/Endpoint.

PDF Navigation

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

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

To access related videos from the Customer Portal, click on the Play button.

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

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

- **Understand the Darktrace RESPOND basic concepts**
- **Configure Darktrace RESPOND options**
- **Handle actions raised by Darktrace**
- **Understand Darktrace RESPOND/Network Models**
- **Tag devices for monitoring**
- **Implement recommended RESPOND set-up options**

2. Prerequisites

Before embarking on the Darktrace RESPOND/Network course, it is imperative that you have completed the appropriate prerequisites beforehand. A basic knowledge of the Threat Visualizer interface is necessary for understanding Darktrace RESPOND/Network.

You should have already attended both Threat Visualizer Courses and therefore be familiar with the following topics:

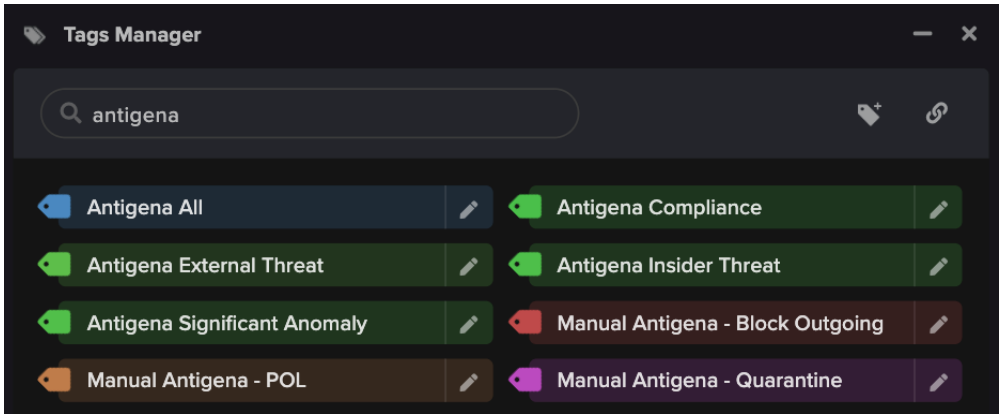
Threat Visualizer Part 1 - Familiarization

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

Threat Visualizer Part 2 - Investigation

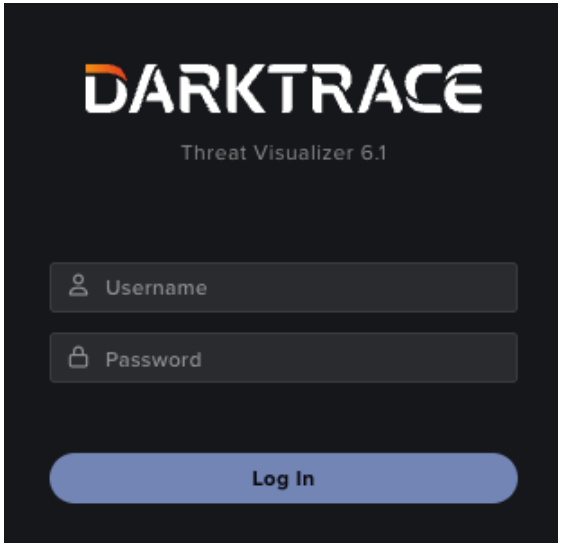
- General analytical workflows
- AI Analyst
- Advanced Search fundamentals
- Creating Packet Captures
- Triaging alerts and assist with Security Operations

It is also advisable that you are familiar with Tags and the Tags Manager as well as the Model Editor and how Models are structured.



This material is covered in the **Cyber Analyst Part 2 - Model Optimization** class, but eLearning concerning the Model Editor can be found on the Customer Portal.

Furthermore, to carry out the workflows outlined in this training manual, it is recommended that you use the "**admin**" user account to access the Threat Visualizer and Console. Otherwise, you may not be able to access all the features and configuration options to enable and use Darktrace RESPOND/Network.



3. Basic Concepts

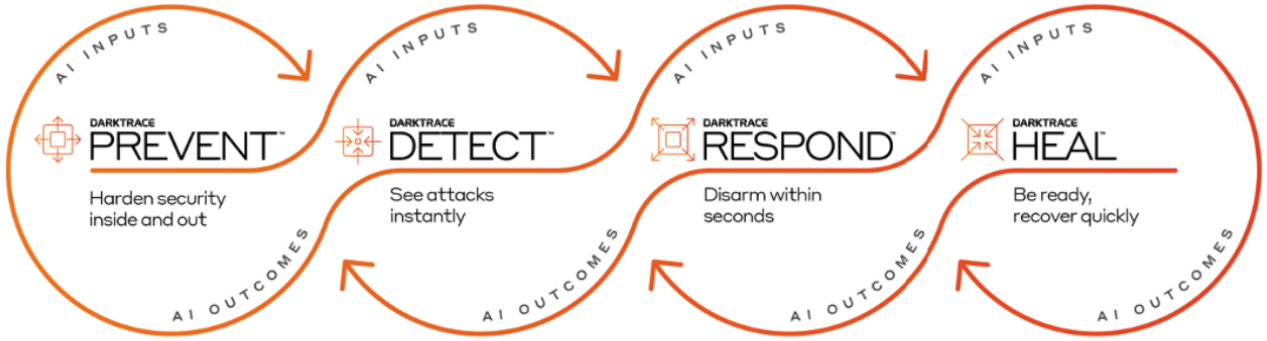
Darktrace RESPOND/Network is an autonomous response technology that can interact with physical, cloud, and apps network traffic and corporate mailflow. In this chapter, let's look at Darktrace's Darktrace RESPOND/Network technology before drilling into Darktrace RESPOND/Network and Endpoint, as well as the actions that can be taken.

3. Basic Concepts

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

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

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



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

Comprehensive Protection Wherever You Need It

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

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

DARKTRACE RESPOND

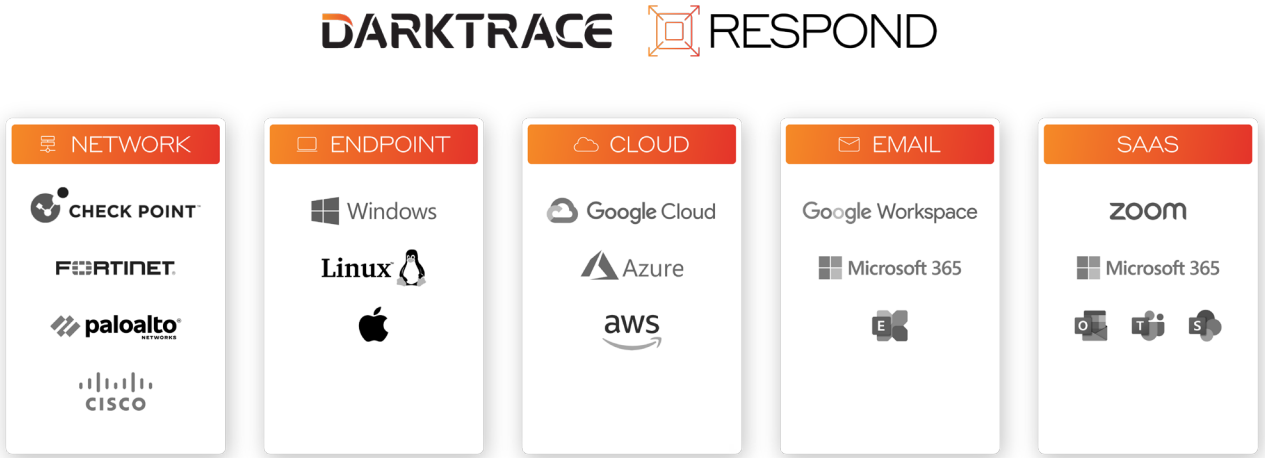
Autonomous Response: Disarm Attacks in Seconds

The first autonomous response solution proven to work in the enterprise. Working with Darktrace DETECT, Darktrace RESPOND autonomously contains and disarms threats, all supported by micro-decision making driven by AI. Darktrace RESPOND uses its understanding of your bespoke organization to take precise and targeted action, interrupting cyber-attacks, without disrupting regular business operations. Darktrace RESPOND has a range of actions it can take to cut attacks short. And crucially, it knows which to take, and where to take them.

DARKTRACE RESPOND/Network

Darktrace RESPOND is available across multiple coverage areas including Network, Email, Endpoint, Zero Trust and Apps, extending autonomous response across the enterprise. Where Darktrace DETECT provides the 'pattern of life' to intelligently identify threats, the Darktrace RESPOND framework places the tools in your hands to action and remediate those threats - autonomously, or with human oversight.

Importantly, it does not rely on predefined signatures or prior knowledge. It takes targeted, surgical action to contain in-progress threats, neutralizing attacks in seconds without disrupting business processes, thereby buying human teams time to catch up. It achieves this by understanding the "patterns of life", so that Darktrace RESPOND/Network can take action in a highly targeted manner, mitigating threats while avoiding over-reactions.



Interrupts Attacks

Understands the business and enforces 'normal'

Unmatched Speed

Responds to machine-speed attacks in 10 seconds

Targeted and Proportionate

Contains the threat without disrupting the business

Rather than generating broad quarantine measures, Darktrace RESPOND can surgically enforce the normal "pattern of life" of an infected device or user, neutralizing the threat within seconds while sustaining routine operations. The Darktrace RESPOND actions are not only granular, but can also dynamically adapt to the severity of a threat as it unfolds. The Darktrace RESPOND/Network module is customizable so can also be scheduled so it only runs on out of office hours such as at the weekend, preventing malicious activity and enabling teams to investigate the incidents in work time.

Furthermore, this technology can seamlessly integrate with your existing ecosystem, informing firewalls and network devices about attacks that have gotten through. Darktrace RESPOND can act as the Cyber "AI brain" of the entire security stack, giving control back to the defenders and transforming the most complex and vulnerable organizations into resilient, self-defending businesses.

Coverage Areas

Network and Endpoint

Traditional defenses fail to detect novel attacks that blend into the noise of the network and sweep through complex infrastructures in seconds. The shift to remote and hybrid working has also taken employees out of firewalled offices, opening their endpoint devices up to new risks.

Informed by an evolving understanding of your business, Darktrace's knowledge of 'self' enforces normal behavior, neutralizing the full range of threats inside your network and stopping emerging attacks on endpoints at the source.

- **Machine-speed ransomware:** Early signs of ransomware trigger an immediate response, enforcing the 'pattern of life' on the device in question and stopping command and control or lateral movement.
- **Unknown unknowns:** By detecting anomalous behavior indicative of signatureless and never-before-seen cyber-attacks, unusual connectivity can be halted.
- **Insider threat:** Malicious insider activity including lateral movement and unusual data uploads can be blocked.
- **Data loss:** Anomalous data transfers indicative of a data exfiltration attempt can be prevented.

Cloud and Apps

As organizations embrace multi-cloud platforms, remote locations, and online collaboration tools, the way we protect the digital enterprise must evolve too.

From providers like Google Cloud, Microsoft Azure and AWS to cloud app platforms such as Teams and SharePoint, Darktrace connects actions in different parts of the digital enterprise and Darktrace responds with surgical precision when cloud accounts are being used carelessly or for malicious purposes.

- **Crypto-mining, API vulnerabilities and data exfiltration:** Upon detecting malicious crypto-mining, unsecured APIs or suspicious file transfers, Darktrace responds to curb the activity by cutting malicious connections.
- **Account takeover or malicious insiders:** Darktrace RESPOND understands the complex human behind the account, identifying abnormal logins and actions, and disabling or logging out users.
- **Multi-faceted attacks:** Attacks leveraging different parts of the network – including cloud and IoT – are neutralized instantly. If unusual account activity is originating from an IP or range, account access from these locations can be prevented.

Email

94% of cyber-attacks begin in the inbox. Darktrace RESPOND takes autonomous, targeted action to neutralize advanced email attacks, intervening to protect employees from spear phishing and other threats.

- **Advanced spear phishing and domain spoofing:** Darktrace/Email recognizes visually similar domains, solicitation attempts and protects the workforce from email impersonation attacks, however convincing.
- **Compromised accounts and out of character senders:** A dynamic understanding of every user identifies and stops account takeover and can prevent emails from being delivered.
- **Payload delivery:** Whether it be attachments or links, Darktrace/Email can take relevant actions to neutralize potential payloads.

Key Darktrace/RESPOND facts:

- Surgical, proportionate, and relevant actions
- Operates across the entire business
- Adapts to persistent, evolving threats
- 24/7 autonomous protection

Flow Structure

Darktrace RESPOND/Network responds to 'high-confidence threats' that strongly point to malicious activity, such as machine speed attacks or ransomware. It can interrupt connections in multiple ways; OS filtering (Darktrace RESPOND/Endpoint only), TCP Resets, or by integrating with your existing infrastructure and messaging directly to a firewall.

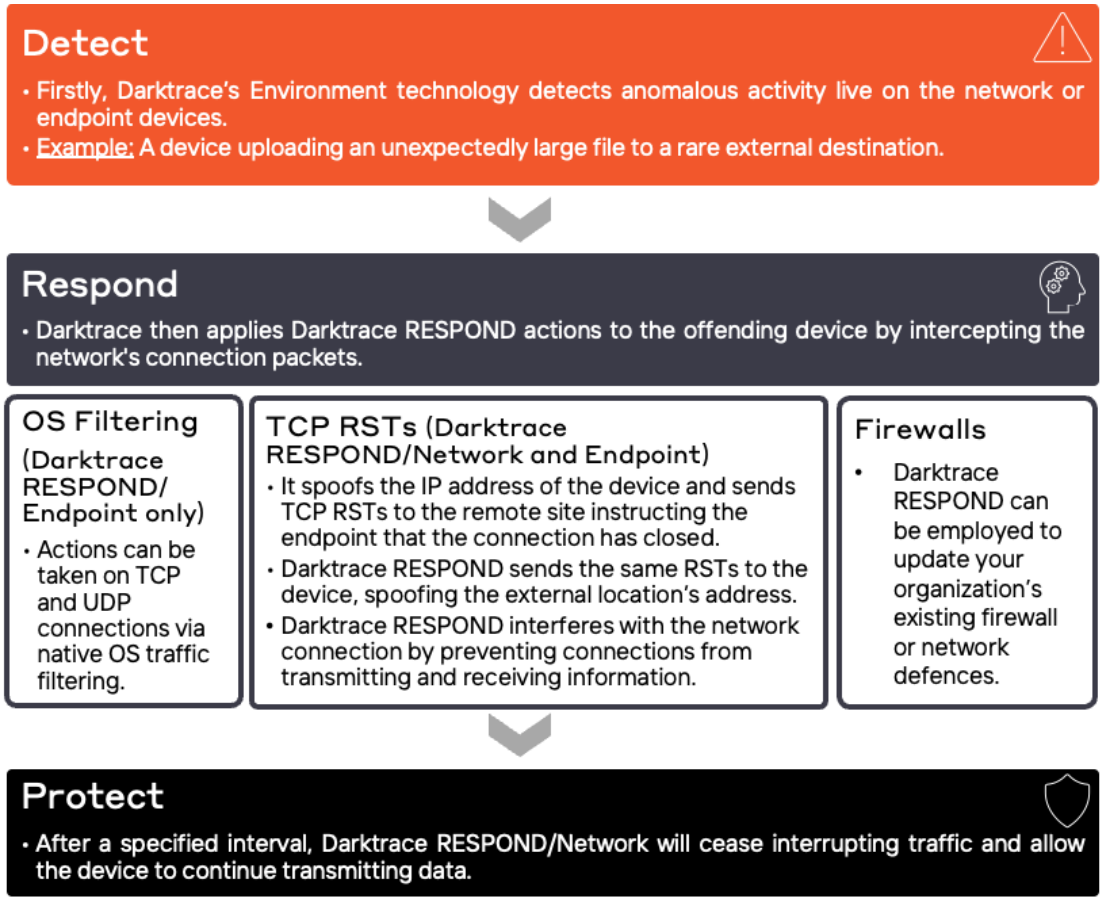
Appropriate actions are defined in the Darktrace Model Deck, hosted on a Darktrace Master appliance. Depending where a device is located dictates how the action is communicated and taken.

When the Darktrace Appliance triggers an Darktrace RESPOND/Network action, it informs all probes, including sensors, to block the identified connections and ports. When they identify traffic to take action on, only the Darktrace appliance or probe that observed the packets of the connection will send the instruction to interrupt network activity.

Actions taken on remote endpoint devices are communicated via cloud infrastructure. The Master Appliance communicates with the cSensor installed on the endpoint and instructs an action to be taken. After the action has been received by the endpoint, it is then managed locally on the device by the installed agent.

For Darktrace RESPOND/Endpoint, Darktrace RESPOND actions can be taken via native OS traffic filtering, meaning both TCP and UDP connections can be blocked. If this mechanism cannot be used, the endpoint action will default to the secondary method - TCP Resets, the method used for Darktrace RESPOND/Network actioning.

TCP Resets are part of normal communications between two devices. When a device receives a reset packet, it will close the TCP connection, be it an internal device or an external service such as a website. When Darktrace identifies suspicious activity, it will attempt to send Resets to both participating devices, the source and destination, both internally and externally. The Reset packet IP addresses are spoofed so that the devices believe the packets are not coming from Darktrace, but from each other.



By default, TCP resets are sent by the Administrative interface of Darktrace appliances. Additional interfaces can be set, however. For more information, review the Dedicated Firing Interfaces article in the Darktrace RESPOND/Network Configuration Guide on our Customer Portal.

RESPOND Actions

Continue your learning with our dedicated video 2. RESPOND Concepts

Darktrace RESPOND automatically acts within seconds to restrain or contain threats, allowing humans the time to catch up. It could only take 20 minutes for a major threat, such as a ransomware attack, to evolve into a crisis.

Therefore, Darktrace RESPOND's automated actions can slow, or stop threats in a targeted fashion, to provide security teams with a vital time window in which to take mitigating action. This technology proactively allows networks to self-defend against specific threats, without disrupting your organization.

Once Darktrace has identified a potential threat, Darktrace RESPOND/Network has the ability to take a variety of actions, depending on the severity of the anomalous activity. When Darktrace detects threats on a network, Darktrace RESPOND is programmed to proactively block threats.

Action Examples

- Darktrace RESPOND can enforce the group's patterns of life of a device, allowing it to make any connections and data transfers that it or any of its peer group typically makes. Therefore, it can stop devices sending an unusually large volume of data to external devices which they do not normally communicate with.

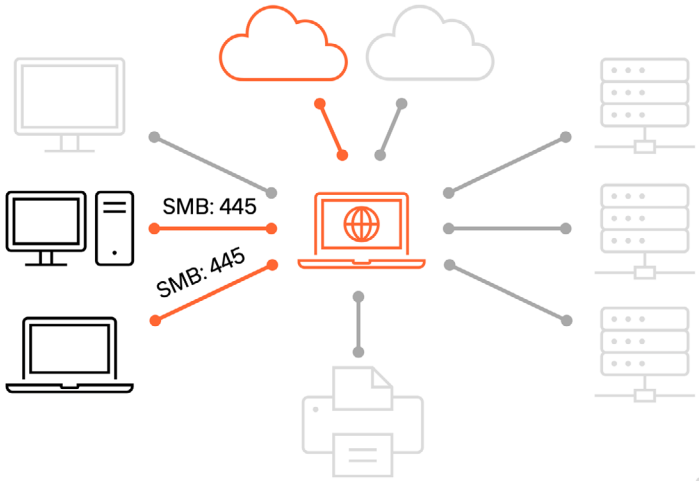
- Darktrace RESPOND may enforce the pattern of life of a specific device, only allowing connections and data transfers which Darktrace considers normal for that device, such as quarantining devices using administrative credentials for the first time.

- Darktrace RESPOND can block specific offending connections. In other words, it can block all connections on a specific port or inhibit connections to a specific device. For example, it might do this to interrupt the download of malicious files from rare external sources.

- Darktrace RESPOND can quarantine a device so that all incoming and outgoing traffic to or from a device is blocked. This is useful to block ransomware encrypting internal network shares.

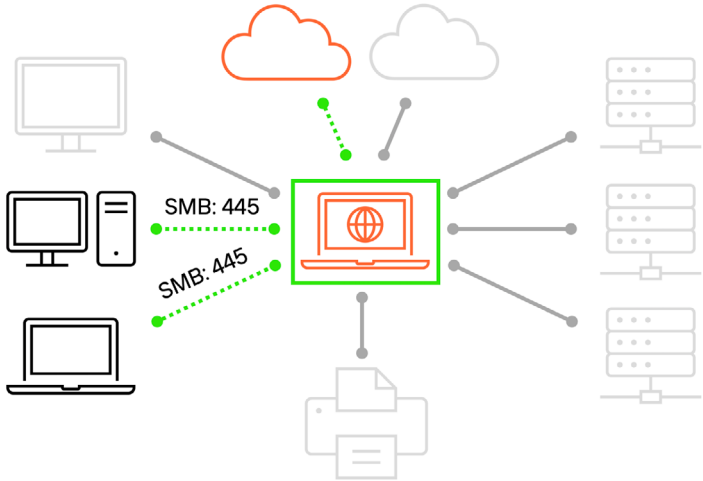
DETECT

A laptop device connects to a rare domain, where a download of an executable is observed. Following this activity, the device begins making anomalous connections to other internal connections. These connections take place over SMB port, 445, and are indicative of high confidence ransomware.



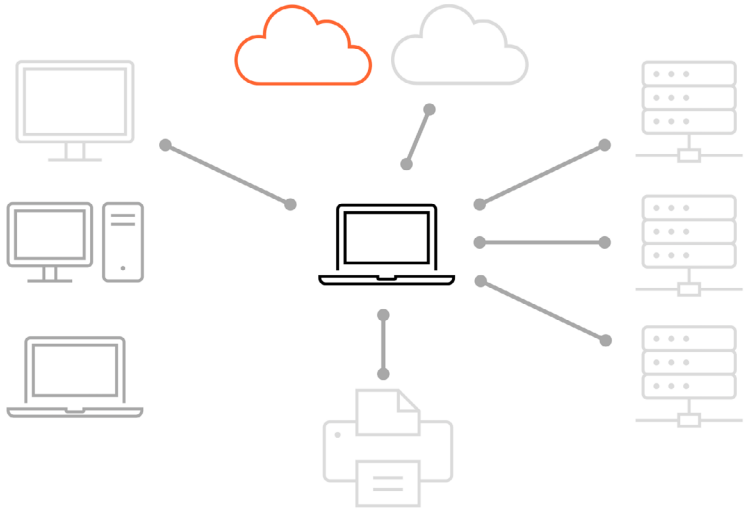
RESPOND

Darktrace RESPOND actions the offending device by intercepting the network's connection packets. It spoofs the IP address of the laptop and sends TCP Resets to the malicious site instructing the endpoint that the connection has closed. Darktrace RESPOND sends the same Resets to the device, spoofing the external location's address. Darktrace RESPOND interferes with the network connection by preventing connections from transmitting and receiving information.



PROTECT

Connections to the external destination and internal vulnerable machines are blocked for a specified interval, averting the immediate threat. The security team is alerted to the incident. After the action time has elapsed, Darktrace RESPOND will cease closing packets and allow the device to resume transmitting data.



RESPOND Modes

Darktrace RESPOND can take a range of proactive, measured, automated actions in the face of confirmed cyber-threats detected in real time. Darktrace understands the 'pattern of life' of users, devices, and networks and so Darktrace RESPOND can take action in a highly targeted manner, mitigating threats while avoiding over-reactions.

Darktrace RESPOND components can be deployed in two distinct ways:

Human Confirmation Mode: Darktrace RESPOND Actions will require human confirmation.
Autonomous Mode: Darktrace RESPOND actions will use model settings.

1. In **Human Confirmation Mode**, Darktrace RESPOND will request approval from a human operator before taking any action.

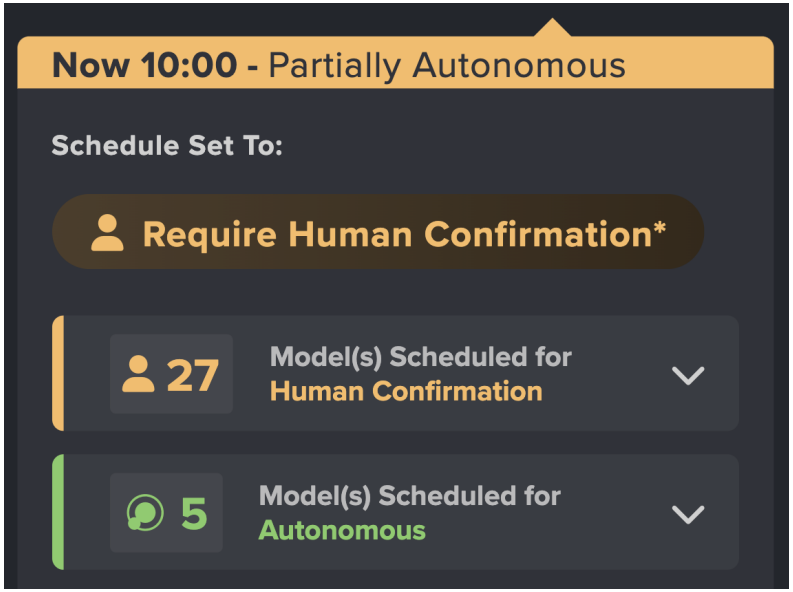
2. In **Autonomous Mode**, autonomous actions are taken without human intervention.

For many organizations, the end goal of a Darktrace RESPOND deployment is some level of **Autonomous Mode** (referred to as "**Partially Autonomous**"), whether applied to select models, select times of the day, or across all devices and use cases.

The Darktrace RESPOND schedule allows you to control when the system will request human confirmation for actions and when it will take them autonomously. The schedule works in 1 hour blocks over a 7 day period and can be localized to the timezone where your subnets are located. The simplest way to control Darktrace RESPOND is to utilize this schedule.

For deployments which have never used Darktrace RESPOND before, for example, setting the schedule entirely to "Require Human Confirmation" can be a quick away to allow Darktrace RESPOND to demonstrate the actions it would take. Actions created during a block of "Require Human Confirmation" will be left "pending" unless a human chooses to approve the recommendation.

Over time, the schedule can be used to permit blocks of autonomous action ("Use model settings") outside working hours. The final goal is to reach fully autonomous operation.



Basic Concepts Test

DARKTRACE
Cyber Engineer Certification

This page will test your knowledge and understanding of the Basic Concepts section. This is the perfect way to work towards your **Darktrace Cyber Engineer Certification**! *Select an answer by clicking on it. Wrong answers are denoted by a red cross and right answers are denoted by a green tick.*

1. Which Darktrace RESPOND product is NOT covered in this course?

- [ ] Network and Endpoint
- [ ] Cloud & SaaS
- [ ] Email

2. Darktrace RESPOND relies on predefined signatures.

- [ ] True
- [ ] False

3. Which of the following options applies to Darktrace RESPOND/Endpoint only?

- [ ] TCP Reset
- [ ] Firewall updates
- [ ] OS Filtering

4. Which Darktrace RESPOND action might be the most useful to block ransomware?

- [ ] Enforce a device's patterns of life
- [ ] Quarantine
- [ ] Enforce a group's patterns of life

5. How long does the protect phase last?

- [ ] 10 hours
- [ ] A specified interval
- [ ] Indefinitely

6. Darktrace Actions fall under which category?

- [ ] Prevent
- [ ] Detect
- [ ] Respond

Clear All Answers

4. Configuration

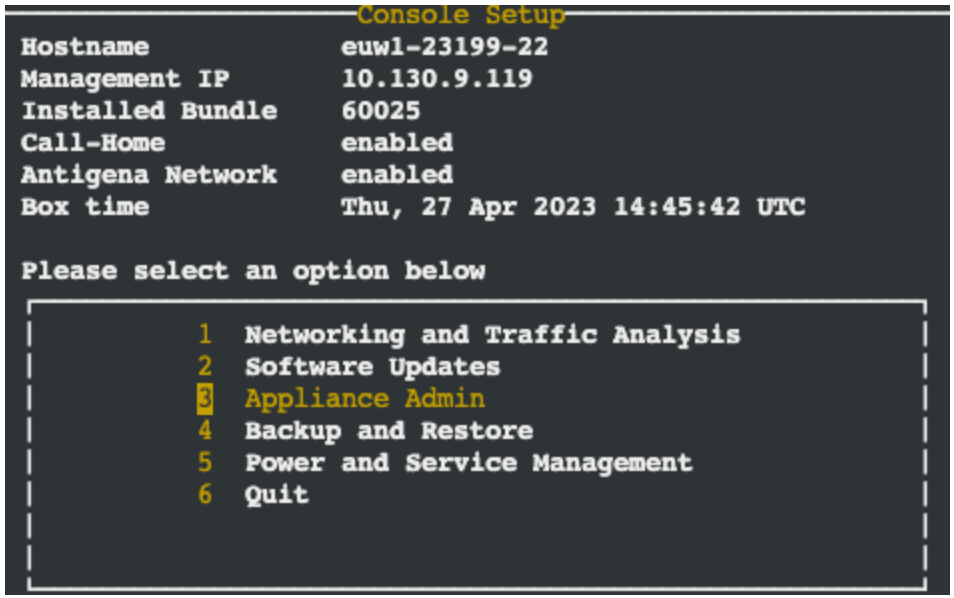
Darktrace RESPOND requires a license and must be enabled in multiple locations: The Darktrace Console and the Threat Visualizer interface. In this chapter, learn how to configure Darktrace RESPOND/Network and Darktrace RESPOND/Endpoint and enable the autonomous technology using different modes.

Console

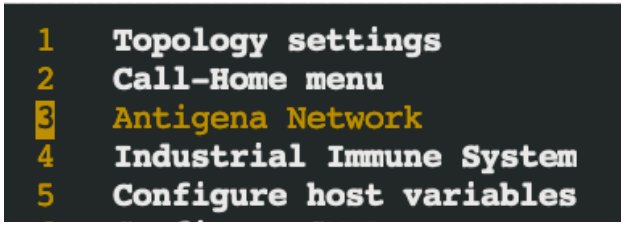
Continue your learning with our dedicated video 3. Console Configuration

Darktrace RESPOND/Network must be enabled both in the console interface and the Threat Visualizer System Config before it can be used. If the following configuration is carried out on a Darktrace Unified View Server, it will propagate down to all connected master appliances.

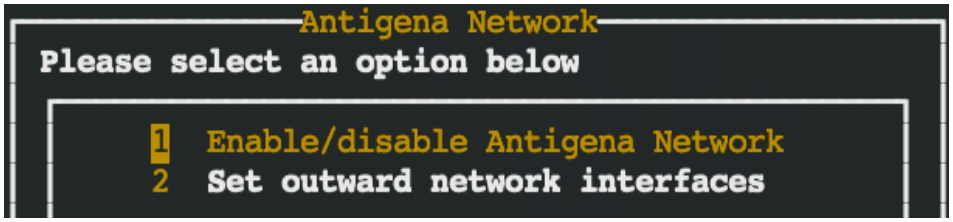
1. Firstly, within the Console, navigate down to option 3, **Appliance Admin**, and select it from the menu. Select **OK** to proceed.



2. From the Appliance Admin page, select the **Antigena Network** option. Select **OK** to continue.

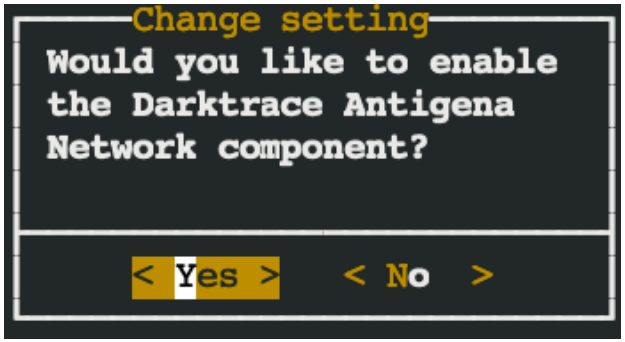


3. From the **Antigena Network** options, select **Enable/disable Antigena Network**. Again, select **OK** to proceed. A prompt may appear describing Darktrace RESPOND/Network. Click **OK** to continue to the next step.



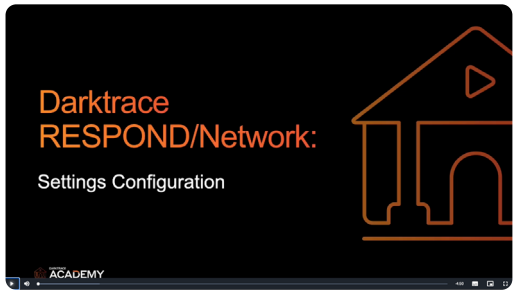
4. When prompted to **enable the Darktrace Antigena Network component**, select **Yes.**

Note: On completion of this step, it is possible the console will log out. Log back in to continue.



5. A window will appear indicating that the console setup process is now complete and this configuration has been **successfully applied**.

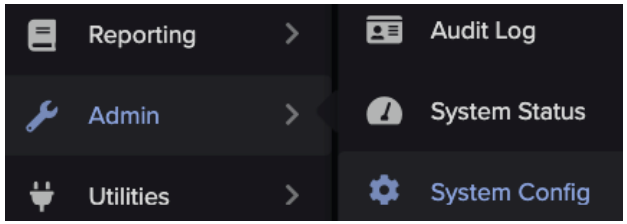
Threat Visualizer System Config



Continue your learning with our dedicated video 4. Settings Configuration

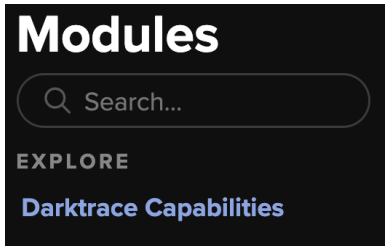
In order to enable Darktrace RESPOND, it is necessary to input the appropriate license keys into the Darktrace System Configuration page.

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



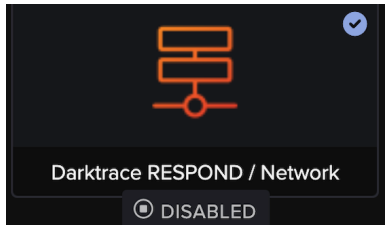
2. Once the System Config page has opened in a new tab, click on the **Modules** menu located on the left-hand side of the screen.

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

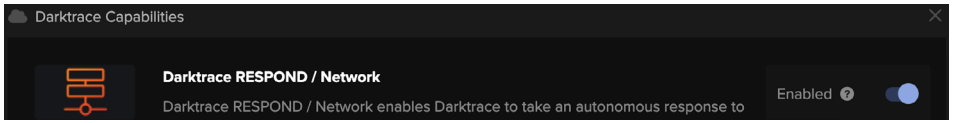


Darktrace RESPOND/Network

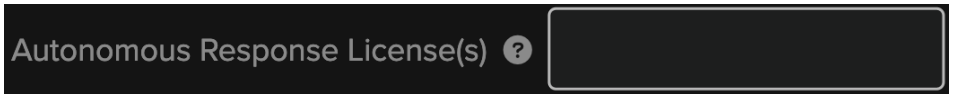
1. From the available applications, choose **Darktrace RESPOND/Network**.



2. A new window will open. Ensure that the Darktrace RESPOND/Network **toggle is enabled**.

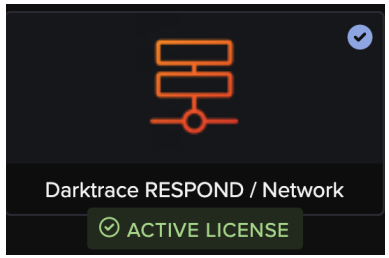


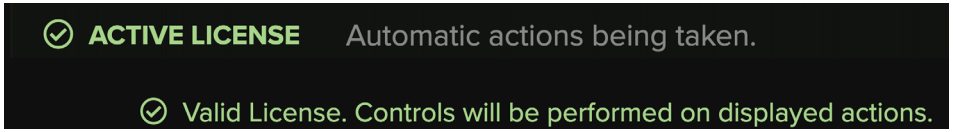
3. Further down this window, paste your **Autonomous License key**, as supplied by Darktrace Support, into the relevant text field.



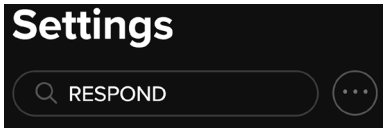
4. At this point, **save** these changes using the button that appears at the top of the window.

5. Refreshing the page, the app should now read **Active License**. Success messages are displayed within the application window and access to Darktrace RESPOND/Network Actions granted in the Threat Visualizer main menu.

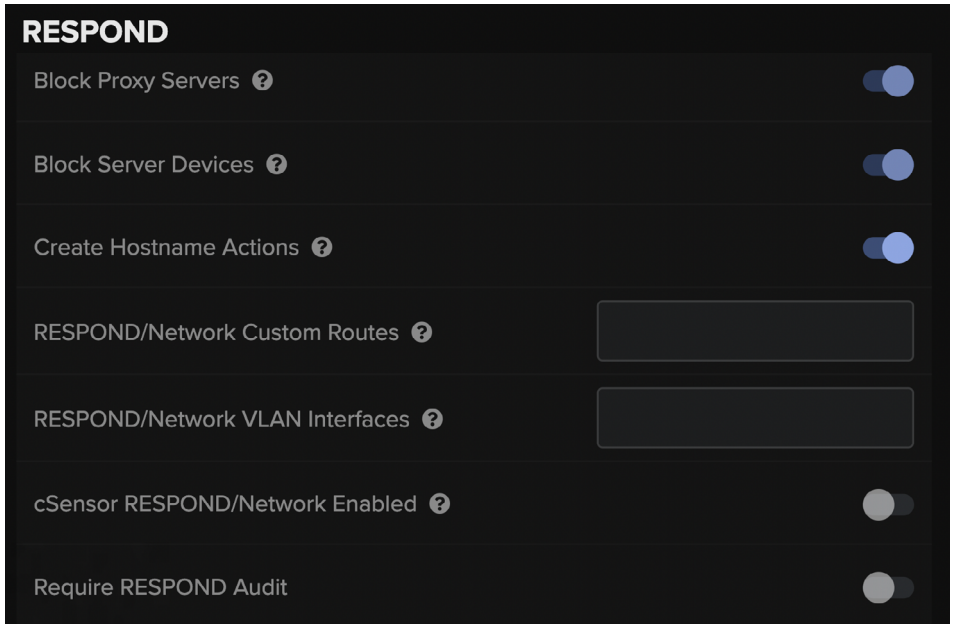




6. Next, navigate to the **Settings** tab on the left-hand side menu. Scroll down to the **RESPOND** section or type **Respond** into the **search bar** and select the **Respond** option to locate the relevant settings.



7. Under the **Respond** heading, there are several settings. The **defaults**, as configured in the image below, are Darktrace's recommendations.



a. The **Block Proxy Servers** setting allows Darktrace RESPOND to block all connections to proxy servers when individual hostnames or IP addresses cannot be blocked. It is recommended that this is set to true to provide an effective response for such situations.

b. The **Block Server Devices** setting allows Darktrace RESPOND to take action against any server device type that has been seen by Darktrace for more than 24 hours. If the toggle is turned off, only client devices and new servers (less than 24 hours old) will be actioned by RESPOND.

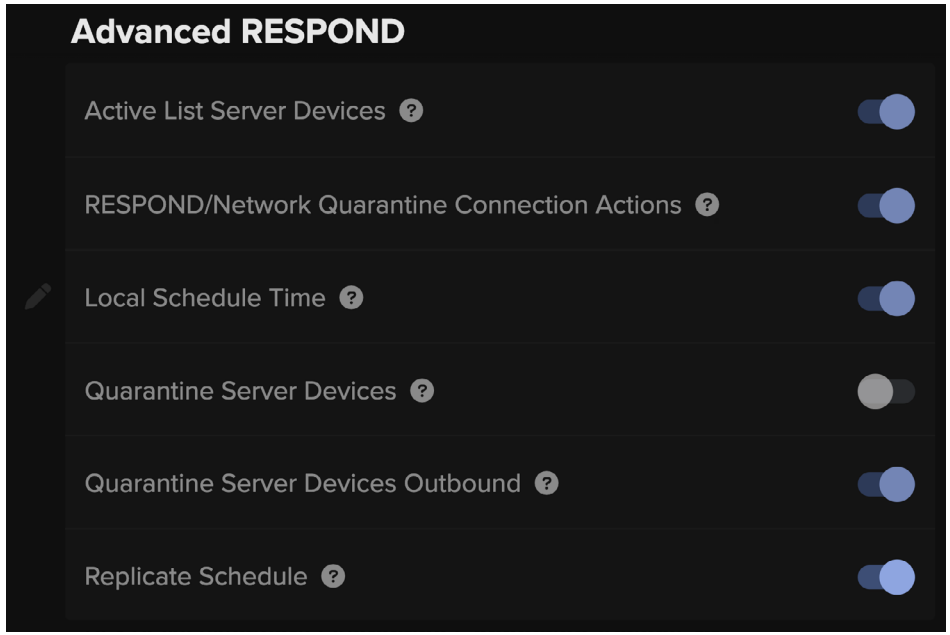
c. The third option, **Create Hostname Actions**, also defaults to true, allowing the creation of actions based on destination hostnames.

d. The **RESPOND/Network Custom Routes** and **RESPOND/Network VLAN Interfaces** fields allow changing the existing interface used by a Master appliance for sending TCP Resets.

e. The **cSensor RESPOND/Network Enabled** setting will forward Darktrace RESPOND/Network actions to be enacted by a cSensor on the target device. It is recommended that this is set to true for Darktrace RESPOND/Network Endpoint users.

f. Finally, the **Require RESPOND Audit** option, if enabled, will require users to add a reasoning behind action changes.

8. **Advanced RESPOND** settings can be found underneath the general RESPOND option.



a. The **Active List Server Devices** setting will use the Darktrace RESPOND/Network Active list for server devices.

b. **RESPOND/Network Quarantine Connection Actions** will enable quarantining action where the connection data cannot be determined.

c. **Local Schedule Time** will use the local time of the subnets based on the Darktrace RESPOND/Network schedule.

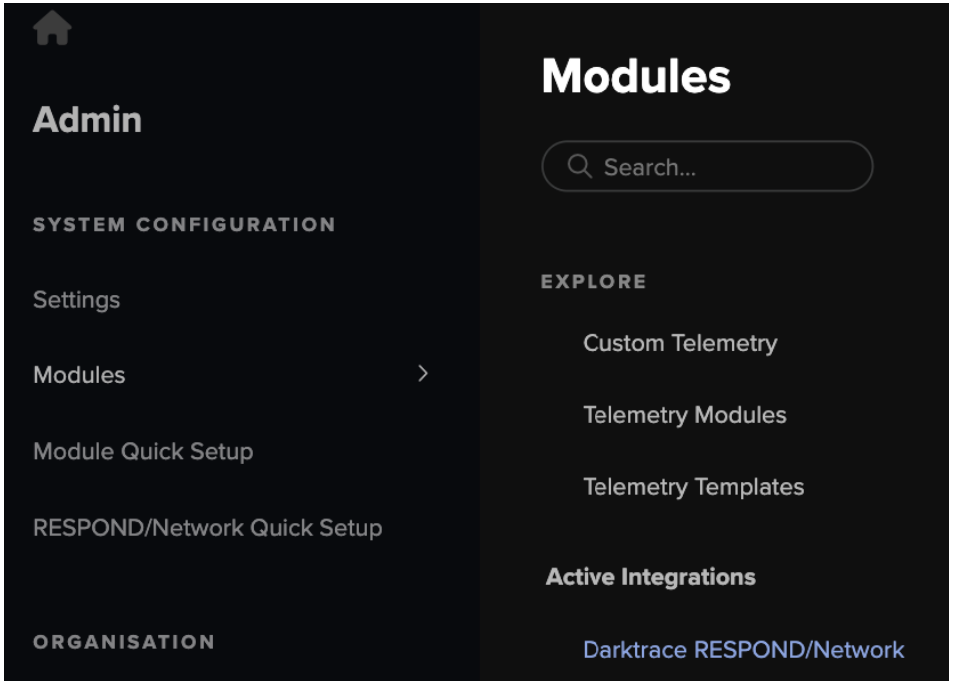
d. The next two settings, **Quarantine Server Devices** and **Quarantine Server Devices Outbound**, allow Darktrace RESPOND/Network to quarantine or block all outgoing connections from server devices respectively.

e. Finally, the **Replicate Schedule** allows for RESPOND schedules to be replicated to every master in the deployment. If this option is disabled, schedules will be configurable on a per-submaster basis.

Configuring Firewalls

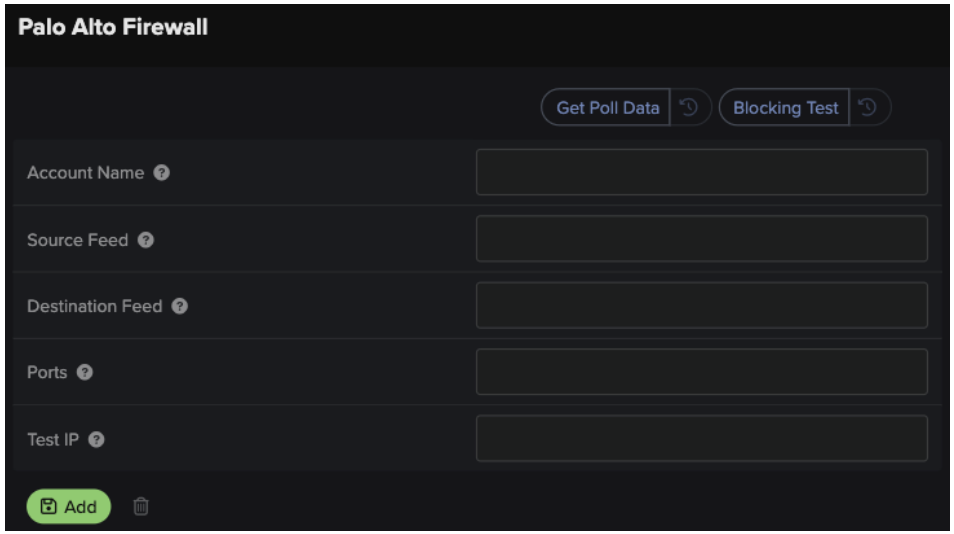
Continue your learning with our dedicated video 5. Firewall Integration

1. **Firewalls** can also be configured to work with Darktrace RESPOND. Navigate to the **Admin System Configuration page** from the main menu in the Threat Visualizer, and locate the **Active Integrations** section from the **Modules**.



2. Choose which **firewall** you want to configure for your network.

3. Follow the instructions and input the appropriate values, as prompted in the new window.

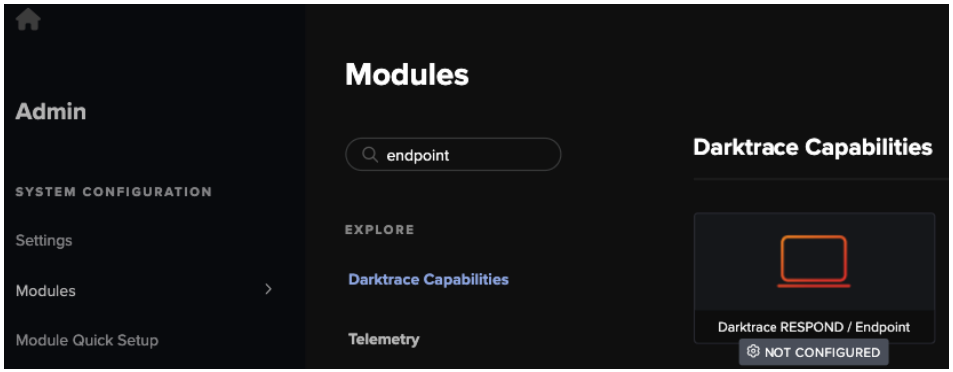


Doing this allows Darktrace to provide an additional layer of protection by instructing your firewall to block IP addresses and ports for defined periods of time.

Darktrace RESPOND/Endpoint

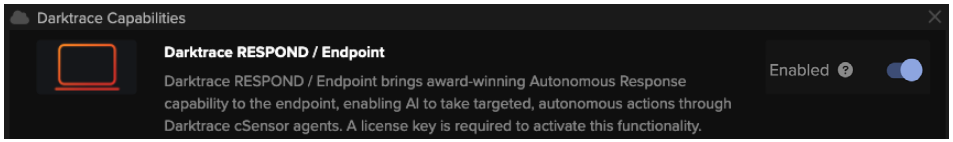
Darktrace RESPOND/Endpoint can be configured in a similar way.

1. From the **System Configuration** page, under **Modules**, locate **Darktrace RESPOND/Endpoint** in the **Darktrace Capabilities** section.

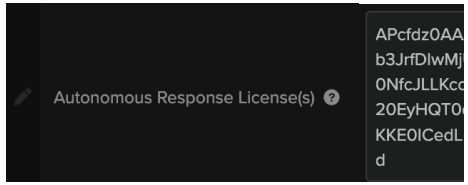


Alternatively, in the Darktrace RESPOND/Network module, choose the **Darktrace RESPOND/Endpoint** module from the available applications.

2. Ensure that the Darktrace RESPOND/Endpoint **toggle is enabled**.

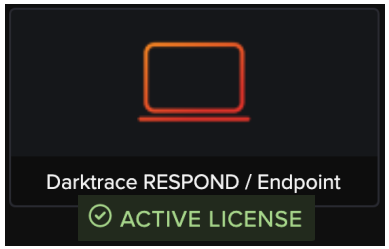


3. Further down this window, paste your **Endpoint License key**, as supplied by Darktrace Support, into the text field.

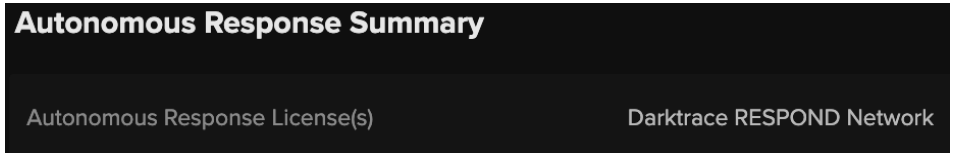


4. A **pencil icon** will appear next to the field, indicating a deviation from the default (empty) value. Save these changes by clicking the **Save** button that will appear at the top.

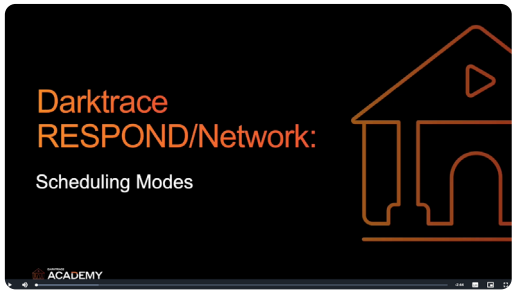
5. Refreshing the page, the Darktrace RESPOND/Endpoint app should now read **Active License**. Success messages are displayed within the application window.



6. Furthermore, any active autonomous response integrations will be listed within the configuration window, with the **licenses** for the deployment.



Enablement Modes



Continue your learning with our dedicated video 6. Scheduling Modes

Darktrace RESPOND can be enabled in two modes: **Human Confirmation Mode** and **Active Mode**.

- In **Human Confirmation Mode** Darktrace RESPOND will alert administrators that it wants to take action, but will **wait for approval** before doing so.
- In **Active Mode** RESPOND will **proactively block threats** for individual models that allow for automatic RESPOND actions, without needing permission from an administrator.

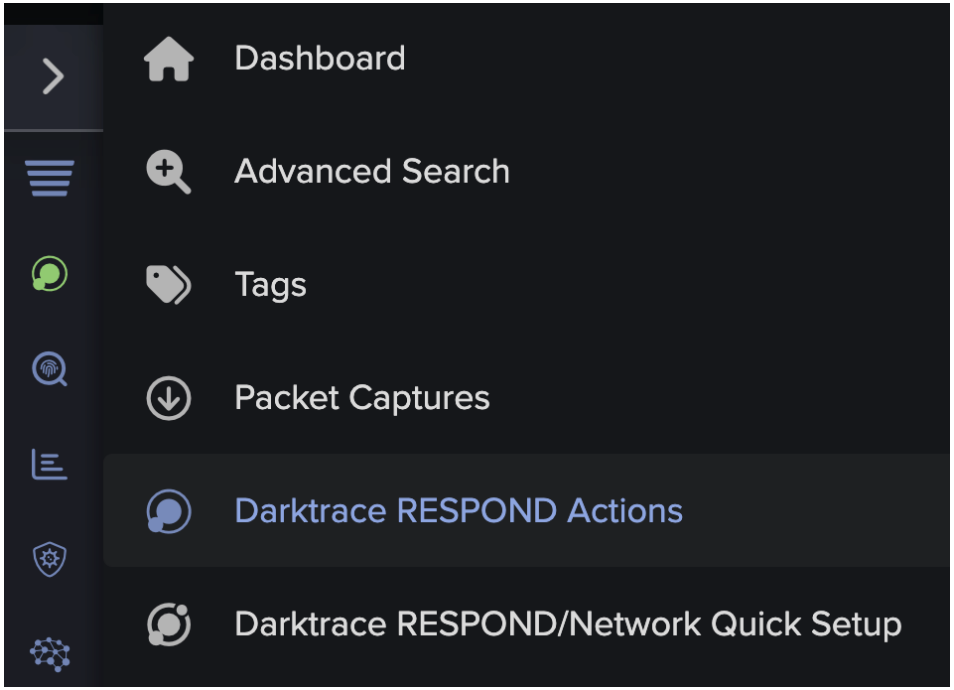
Darktrace Recommends:

Upon deploying Darktrace RESPOND/Network, **Human Confirmation Mode** is recommended in the initial phase. However, once Darktrace RESPOND/Network breaches have been reviewed and optimized, enabling **Active Mode** as soon as possible is recommended, allowing Darktrace to deter threats at all times.

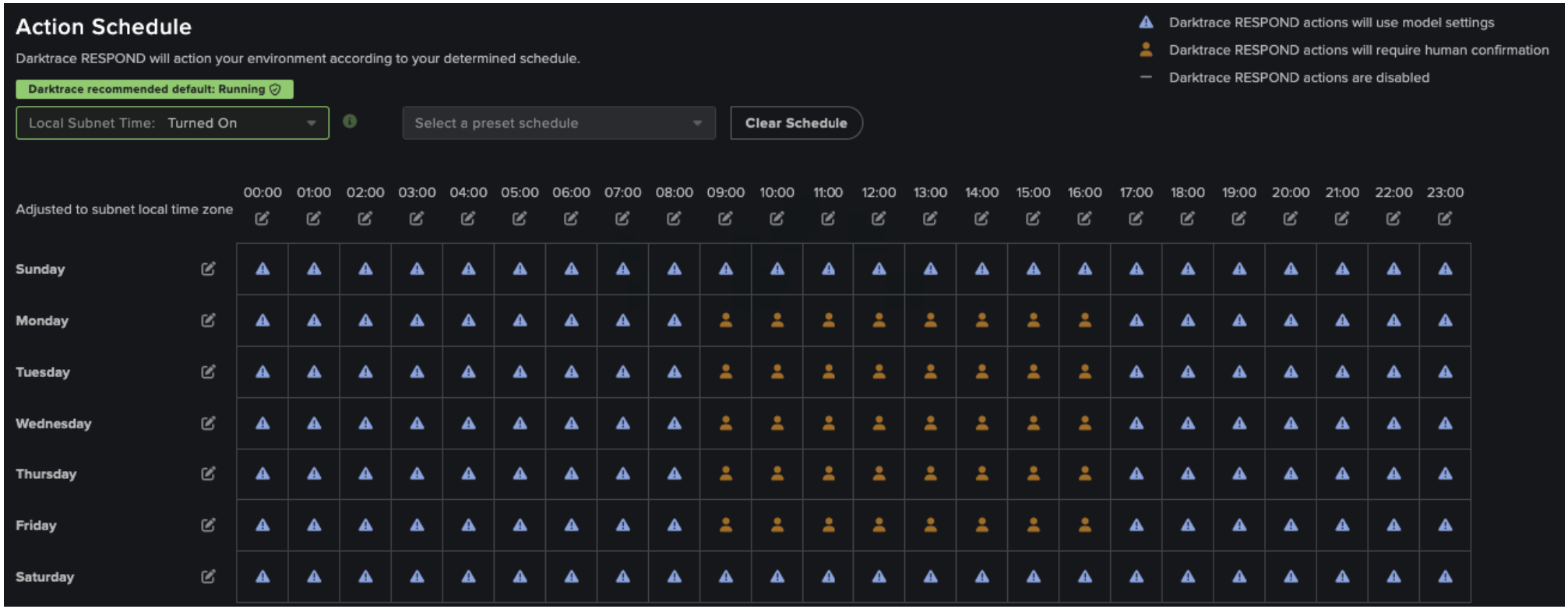
Top Tip:

To enable alerts review and relevant model tuning, the initial deployment will enable Active Mode for out of work hours, for example, during the weekend, evenings and early mornings. This means that if Darktrace RESPOND alerts occur during the day, an administrator can manually decide whether to block connections. However, outside of working hours, they will have the comfort of knowing Darktrace RESPOND will help protect their network and allow them to review incidents on their return.

1. Navigate to the **Darktrace RESPOND Actions** page, which can be found in the main menu.

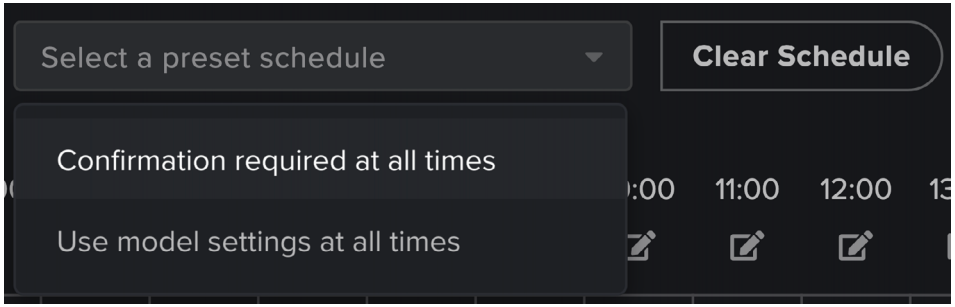


2. Select the **Settings** tab, located along the top of the Darktrace RESPOND Actions window.

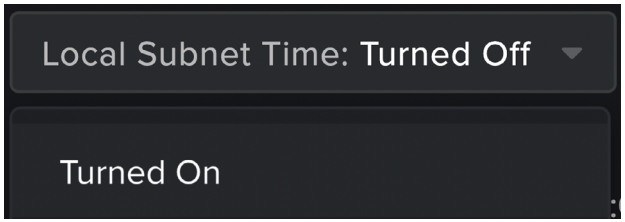


3. We see which mode Darktrace RESPOND is set to for each hour of every day throughout the week.

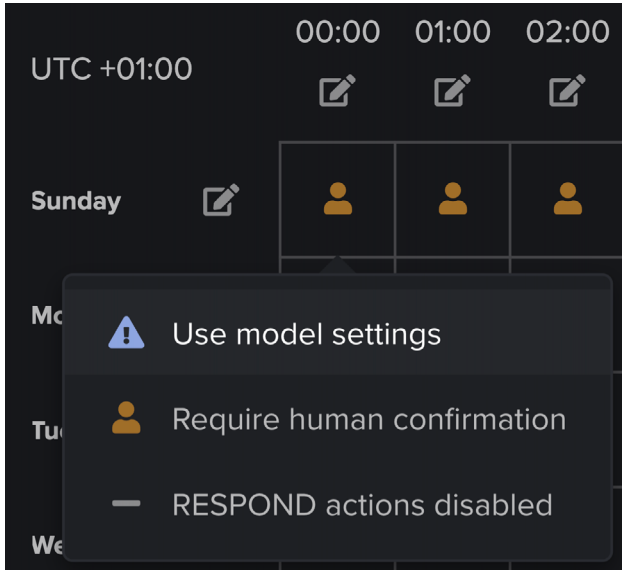
4. Bulk settings can be applied, or cleared, which can provide a useful foundation for a more tailored action schedule. Use the drop-down to select a base schedule (**Confirmation required at all times** or **Use model settings at all times**).



5. You can select the **Local Subnet Time** by turning this setting on.



6. To begin tailoring the settings, click on an **individual square** to select an option from the different icons for a selected hour on a selected day.



7. It is also possible to modify settings for a **full day** or the **same hour every day** by clicking the edit icon next to the relevant day of the week or hour.

Configuration Test

DARKTRACE
Cyber Engineer Certification

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

1. From the console interface, which sequence will enable Darktrace RESPOND/Network?

- [ ] 3-3-1
- [ ] 1-3-3
- [ ] 3-1-3

2. Darktrace RESPOND/Network must be enabled in the console interface only.

- [ ] True
- [ ] False

3. Which of these settings is required to use Darktrace RESPOND/Endpoint?

- [ ] Active List Server Devices
- [ ] cSensor RESPOND/Network Enabled
- [ ] Enable Endpoint License

4. What timeframe does the action schedule cover?

- [ ] A day
- [ ] A week
- [ ] A month

5. Which icon represents the Model Settings mode?



- [ ]
- [ ]
- [ ]

6. In a hybrid scheduled approach, when might you use Model Settings mode?

- [ ] During working hours
- [ ] During the weekend only
- [ ] Outside of working hours

Clear All Answers

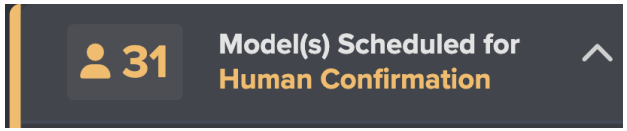
5. RESPOND in Action

There are multiple configurations Darktrace RESPOND can take, which can be deployed separately, or together. In this chapter, learn about Human Confirmation Mode versus Active Mode and see them in action. This can help to determine which configuration Darktrace RESPOND is most suitable for your organization.

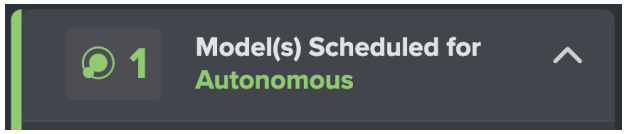
When the criteria for a Darktrace RESPOND action are met, Darktrace RESPOND can either take action autonomously or wait for human approval. These two states are referred to as:

- Human Confirmation Mode
- Autonomous Mode or Active Mode.

In **Human Confirmation Mode**, Darktrace RESPOND will request approval from a human operator before taking any action.

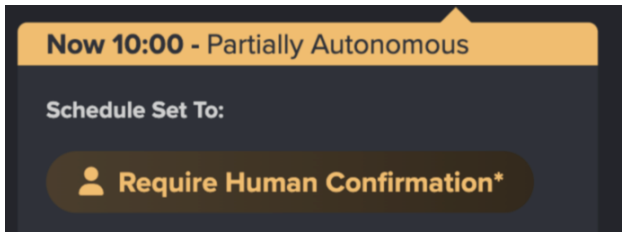


In **Autonomous Mode**, autonomous actions are taken without human intervention.



For many organizations, the end goal of a Darktrace RESPOND deployment is some level of Autonomous Mode, whether applied to select models, select times of the day, or across all devices and use cases.

The majority of Darktrace operators will settle on a **Partially Autonomous** configuration, tailored to their needs.



Human Confirmation Mode

Continue your learning with our dedicated video 7. Human Confirmation Mode

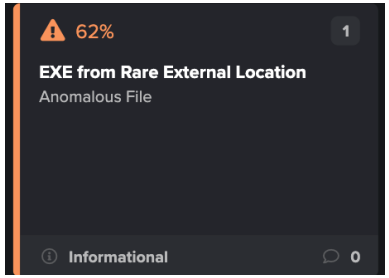
In **Human Confirmation mode** Darktrace RESPOND will create recommended actions but it will not take them unless approved by a user. Actions created but waiting for human confirmation are referred to as "pending" actions, as they are pending human approval.

New deployments of RESPOND/Network are kept in human confirmation mode for a short period to allow Darktrace RESPOND to demonstrate the type of recommended actions it would take across the extended network.

In the following example, the deployment is set to Human Confirmation Mode for all days of the week. As a result, when an Darktrace RESPOND/Network model is breached, no action taken until it has been approved.

1. This example shows the effects of **downloading a Windows executable file** from an external source, not normally visited by the network.

2. Once the executable has downloaded, an **EXE from Rare External Location** Model Breach appears in the Threat Tray.

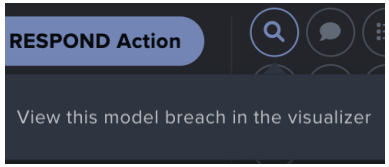


However, there is no accompanying Darktrace RESPOND/Network Model Breach. This is because Darktrace RESPOND/Network needs to be informed of which devices are to be monitored through tagging.

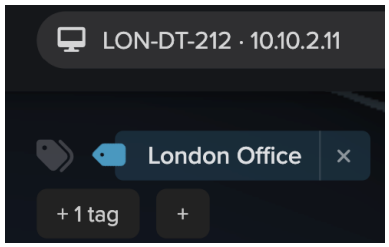
3. To start the tagging process for this device, make sure it is populated in the **Omnisearch bar**.

   a. This can be done by typing **identifiable device information**, such as the device label, user, hostname or IP address, into the Omnisearch bar.

   b. Alternatively, click on the **model breach** in the threat tray to open the Breach Log. Once open, clicking on the **magnifying glass** will display the device in the visualizer.

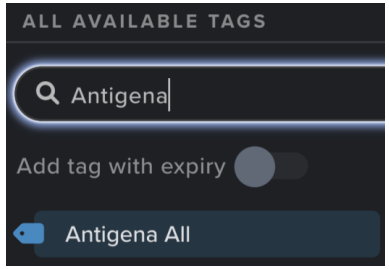


4. Under the Omnisearch bar and the tags, the **+ icon** can be used to add a Darktrace RESPOND/Network tag.

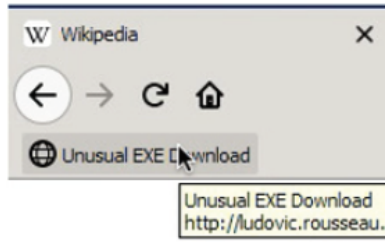


5. In this example, we select the **Antigena All** tag to apply it to the device.

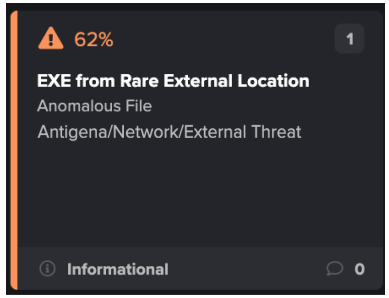
   If required, the tag can be added for a specified period of time by selecting **Add tag with expiry** and selecting the appropriate duration.



6. If we now try to **download a Windows executable** from a rare external site using this device, a model should trigger a series of events.



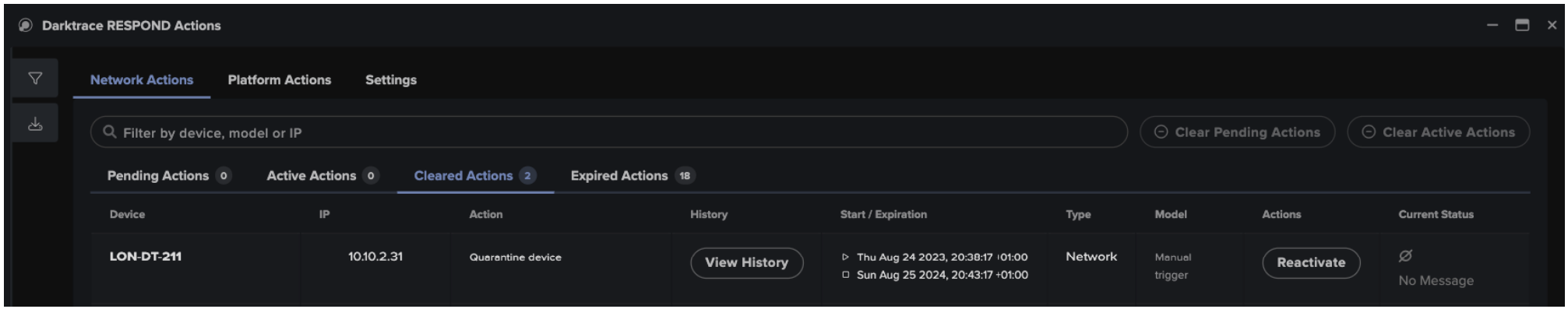
7. Returning to the Threat Visualizer, a new **Darktrace RESPOND/Network Model Breach** should be preset in the Threat Tray. As Human Confirmation Mode is currently configured, the presence of this breach does not indicate traffic has been actioned. Instead, this alert prompts that approval is necessary for action to be taken.



8. To review any actions requiring approval, navigate to the **Darktrace RESPOND Actions** page found in the main menu.

9. Also note that when an Darktrace RESPOND/Network action requires approval, a **pop-up notification** will be visible in the bottom right-hand side of the Threat Visualizer interface.

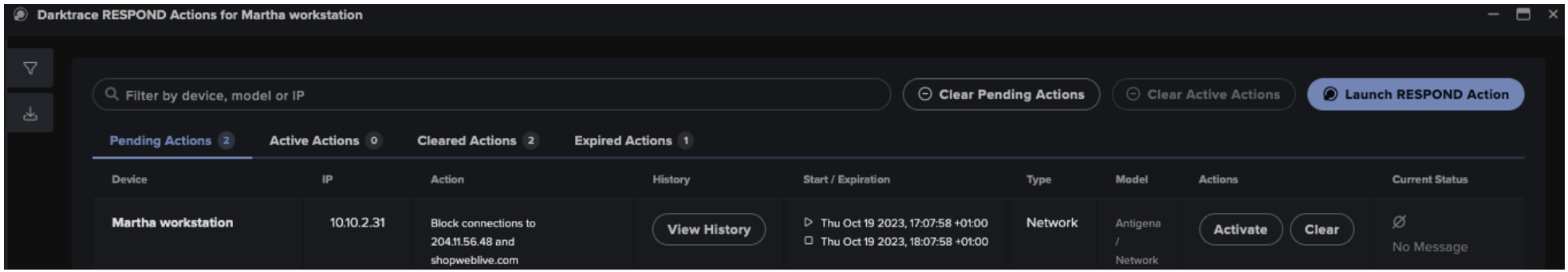
10. The RESPOND Actions page will open with **Pending**, **Active Actions**, **Cleared Actions** and **Expired Actions** tabs.



Within the tab there is information about the device and action, and buttons to select which actions to take. These options will vary slightly depending on whether viewing the Pending Actions, Active Actions, Cleared Actions, or Expired Actions.

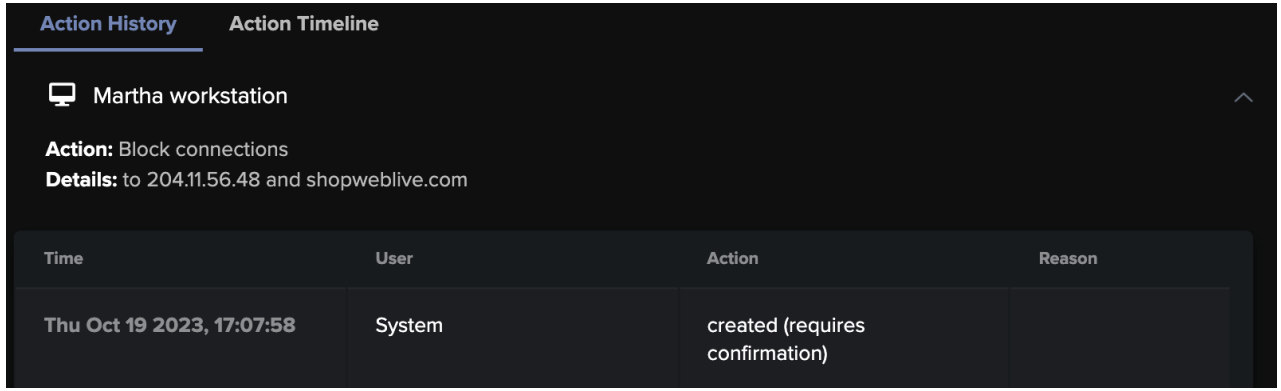
DEVICE	The name that is associated with the device.
IP	The IP address of the device.
ACTION	The suggested action. In this case, to block a connection to a domain on the watched domains list.
HISTORY	Selecting this will show any previous actions that have been taken on the device.
START/EXPIRATION	The date and time period of the action to be taken.
TYPE	This indicates whether it is a network action or an endpoint action.
MODEL	Information about the model that triggered the action.
ACTIONS	Users can activate, reactivate, clear or extend a selected action.
Current Status	The current status of the action.

a. Actions that are awaiting human confirmation will be shown in the **Pending Actions** tab.



In our example we can see the device that has a **pending action**, and the columns with additional information and functions. We can see the name of the domain that is on the Watched Domains list, the action that is suggested to be taken, the related model breach, and an option to View History.

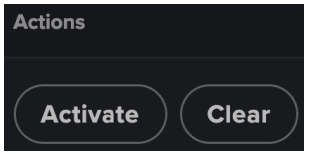
i. Selecting **View History** provides an overview of any RESPOND actions taken on this device.

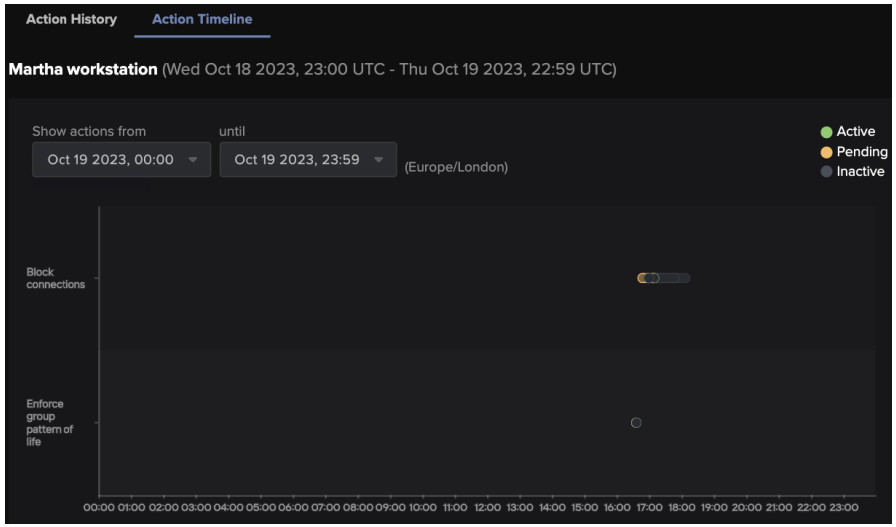


ii. Additionally, the **Action timeline** displays a timeline with RESPOND actions, visually showing the time at which different events occurred.

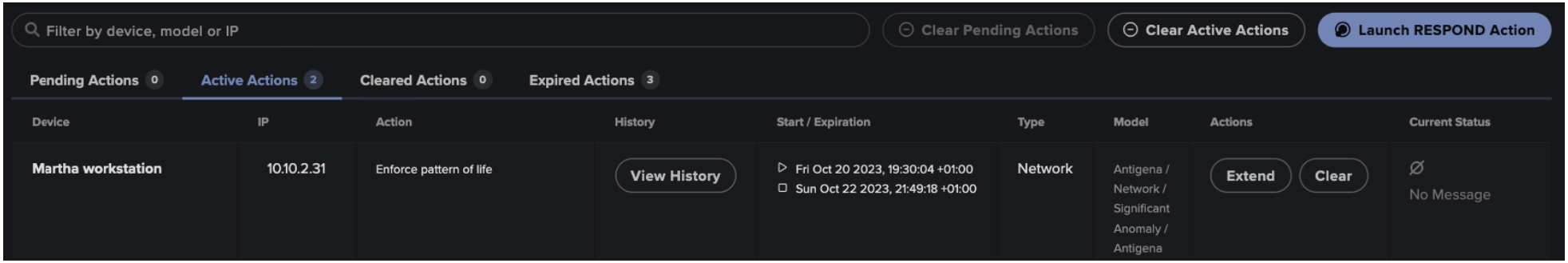
The timeframe can be adjusted using the **Show actions from** and **until** options, while hovering over the RESPOND events, represented by colored circles, will display information about the event.

iii. At the end of the row, notice the **Activate** and **Clear** buttons. Clicking **Activate** will cause Darktrace RESPOND to start taking action on the device while the **Clear** button will not action the device.

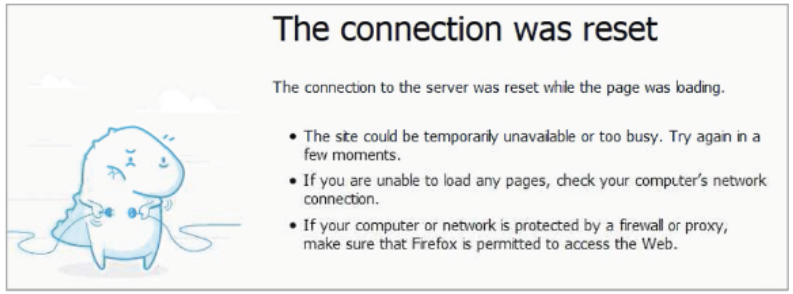




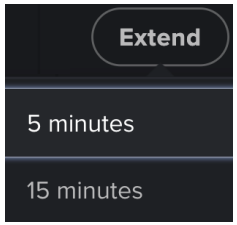
b. The activated action will now move to the **Active Actions** panel. All actions Darktrace RESPOND is currently taking on devices that are still within their expiry periods will appear here.



i. The device that has the active action will be now **blocked** from accessing the endpoint that may have initiated the RESPOND action.



ii. The column headings are the same as we saw in the Pending Actions, however, the Actions column has the option to **Extend**. By selecting this we can extend the duration of the action that is being taken, from **5 minutes** up to **48 hours**.

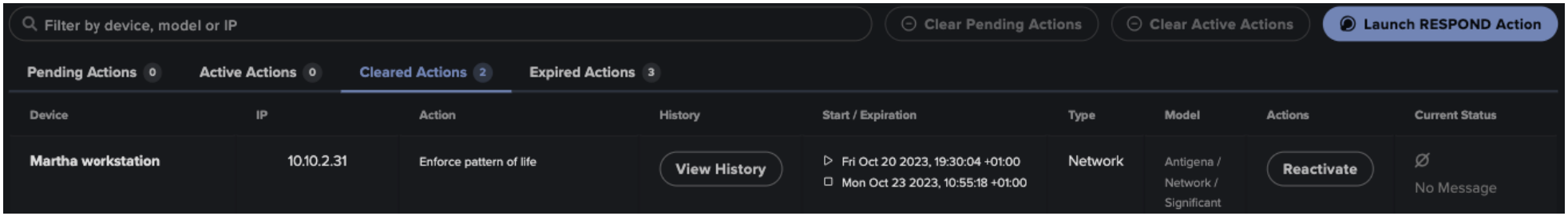


This may be useful if we require further time to investigate the behavior we have seen take place on the device.

iii. The **Clear** button, as in Pending Actions, allows the user to stop Darktrace RESPOND taking an action that is currently active, effectively deactivating it. This will cause the action to be cleared immediately.

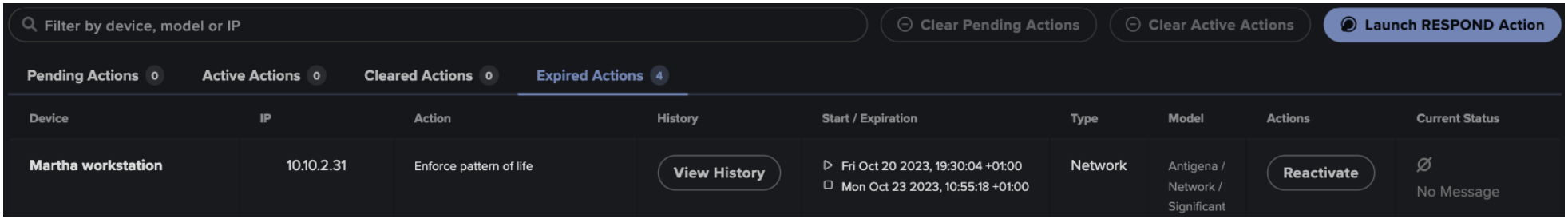
Note: If multiple actions are active, they can be filtered using the search bar at the top, or cleared in bulk using the Clear Active Actions button to the right of it.

c. Any cleared actions that are still within their set time period will appear under **Cleared Actions**. The Cleared Actions tab shares the same format as the previous two, however, there is a **Reactivate** button in the **Actions column**, which enables the action to be immediately reactivated.



Applying this will see the action moved back under the **Active Actions** tab.

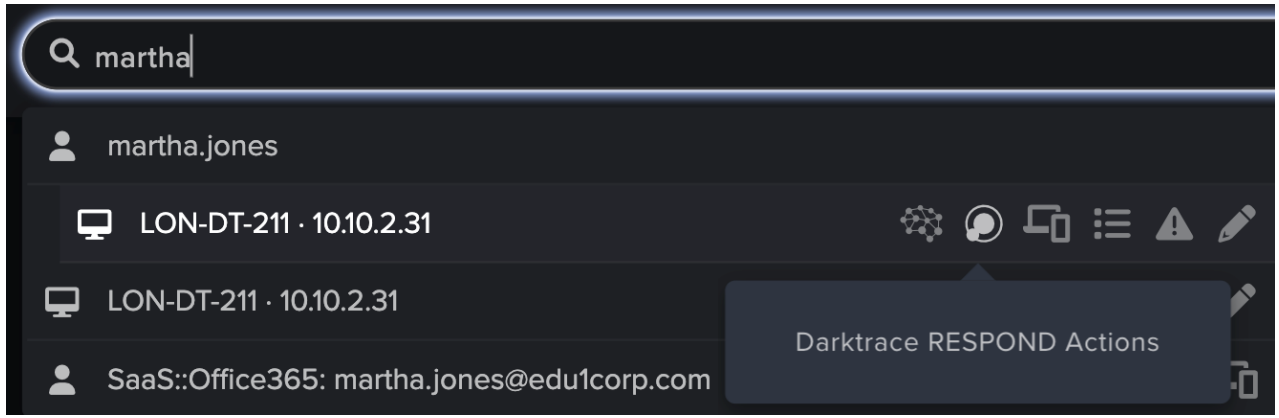
d. The **Expired Actions** panel has the same format as the Cleared Actions panel, with the **Reactivate button** to restart the Darktrace RESPOND action.



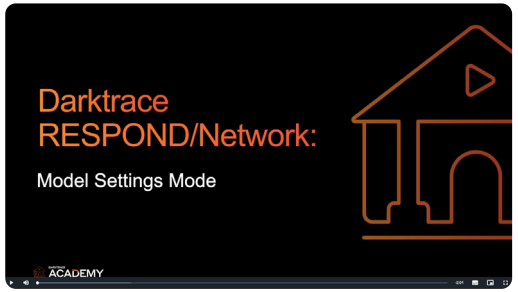
Top Tip:

The RESPOND Actions page for a **device or account** can be accessed by populating the Omnisearch bar and by clicking the circular icon for **Darktrace RESPOND Actions**.

Hovering over a device will also display the option to view RESPOND actions.

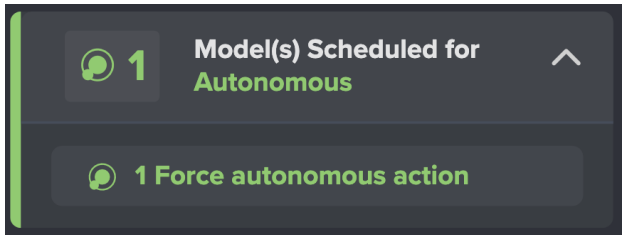


Active Mode

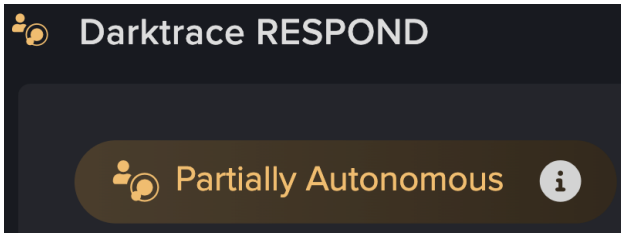


Continue your learning with our dedicated video
8. Model Settings Mode

In **Active / Autonomous mode**, Darktrace RESPOND will create and take actions automatically, without the need for human intervention. These actions can still be cleared or extended at any time by a human operator.



Most operators will settle on a **Partially Autonomous** configuration, tailored to their needs. This combines elements of human confirmation and autonomous activity.

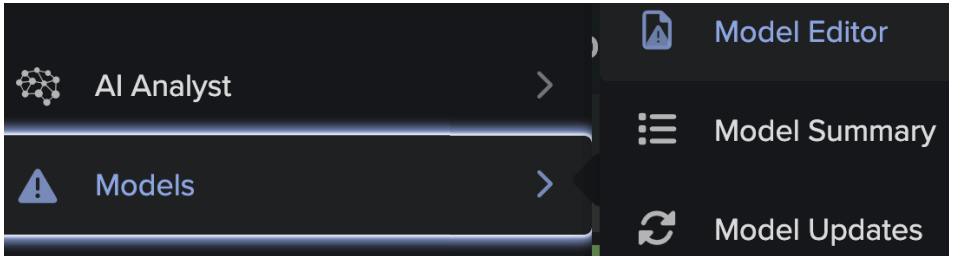


This is the ideal end state for Darktrace RESPOND - actions can be taken at machine speed, without delays waiting for user approval.

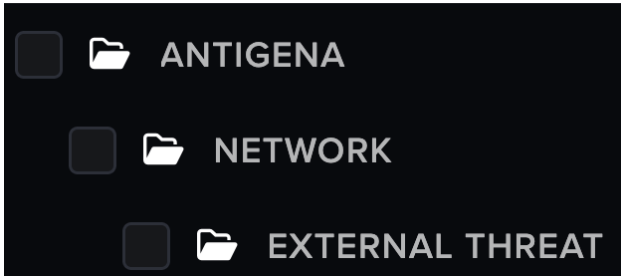
Active Mode In Practice

In this example, we will use **Active Mode** and use the **Antigena Quarantine Example Model** to quickly test that RESPOND is working as expected.

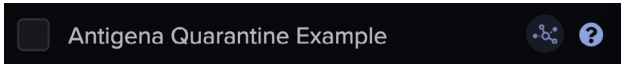
1. Navigate to the **Model Editor** from the Threat Visualizer Main Menu.



2. Navigate through the following folders within the Model Editor: **Antigena > Network > External Threat**.



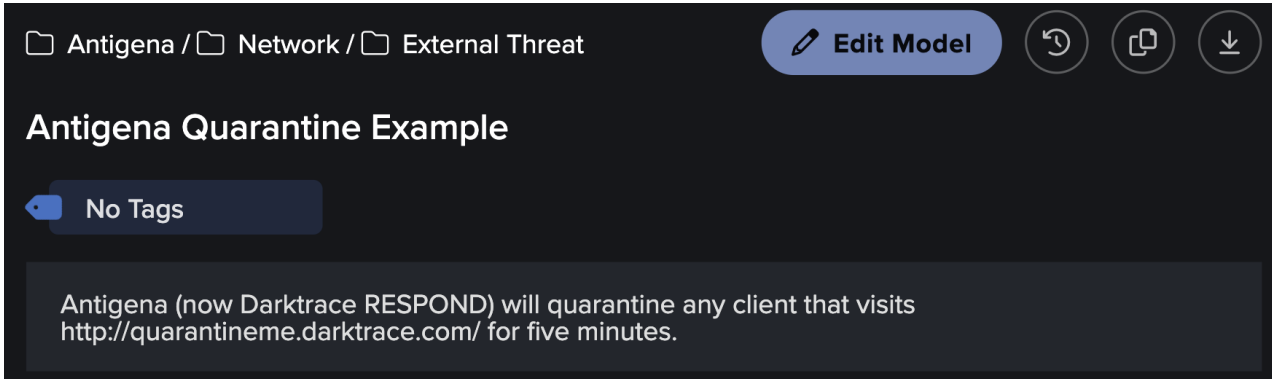
3. Select the **Antigena Quarantine Example** model. It is used for testing Darktrace RESPOND/Network.



   a. The **Antigena icon** indicates models which have RESPOND set to **Take autonomous action**.

   b. The **question mark icon** will display the model's description.

c. In this example the **Antigena Quarantine Example** model will quarantine any device visiting **quarantineme.darktrace.com**, as outlined in the Model preview/description.

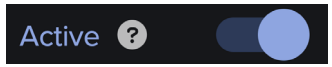


4. Unlike other Darktrace RESPOND/Network Models, this **testing Model** requires no tagging, which can be confirmed by reviewing the model's components.

5. The Model is set to inactive by default:

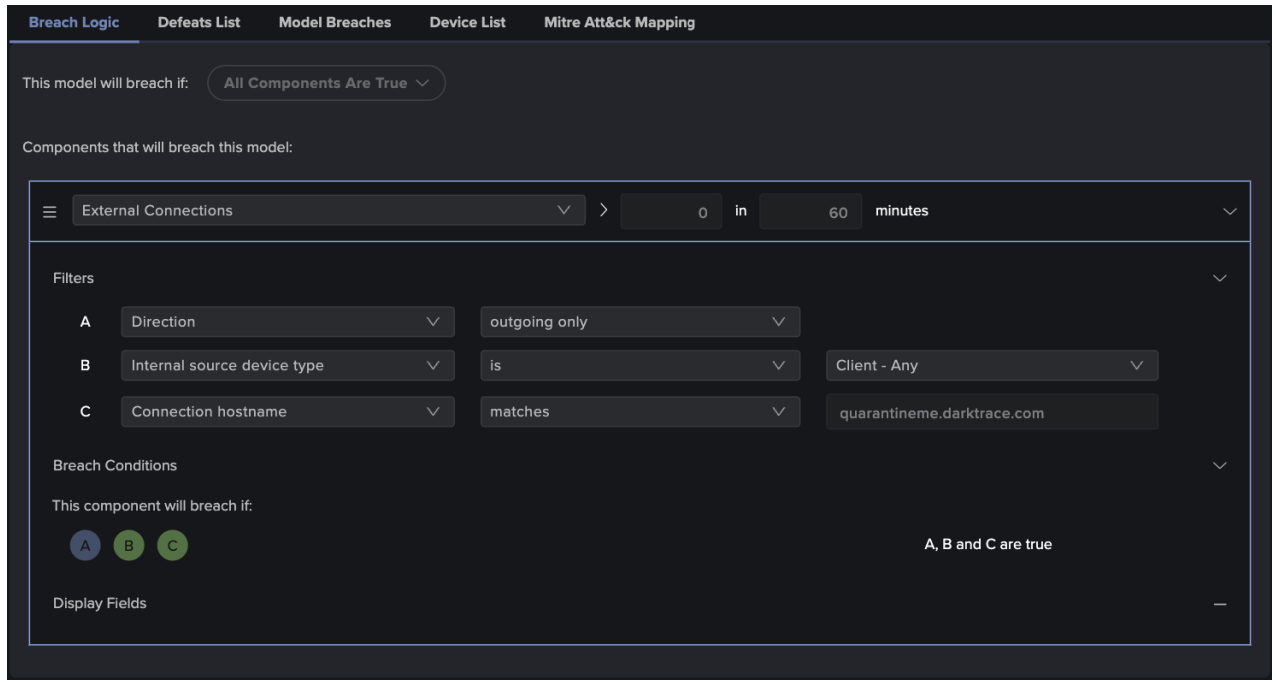
   a. Firstly, click **Edit Model** in the top-right corner of the page.

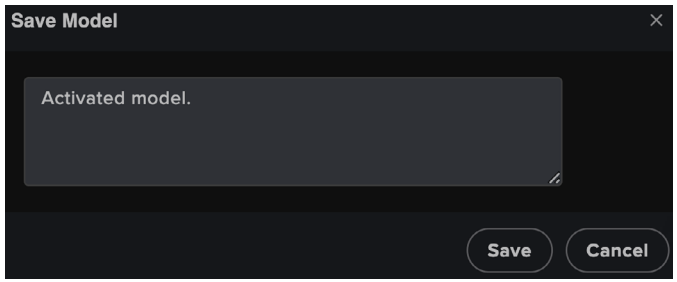
   b. Enable the model by toggling **Active** on.



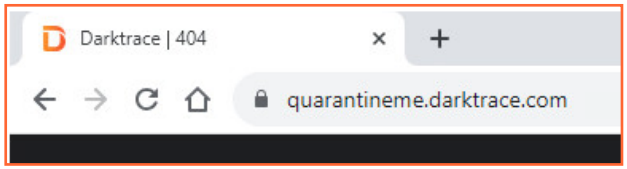
   c. Click the **Save Model** icon in the top-right of the Model Definition.

   d. Write a descriptive **commit message** which will be visible in the Model History.



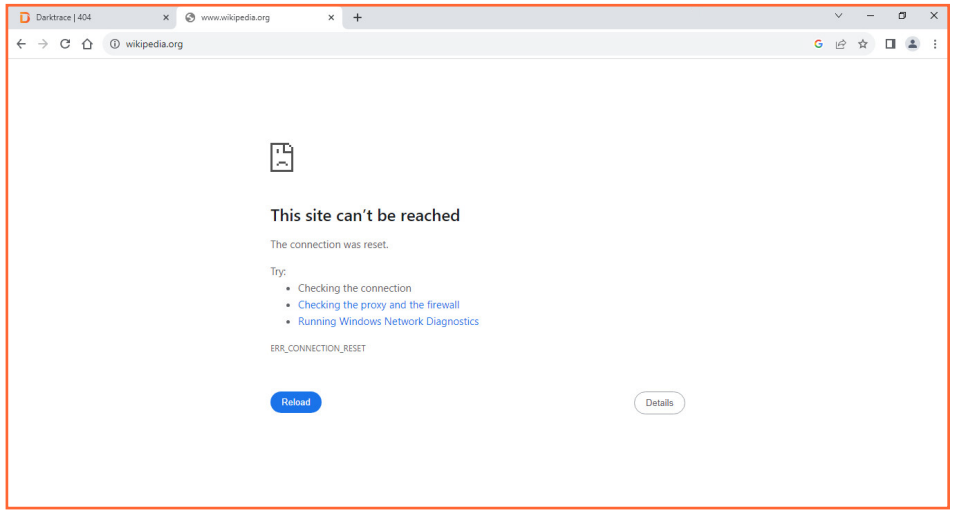


6. Navigating to an appliance being monitored on the network, visit **quarantineme.darktrace.com**.

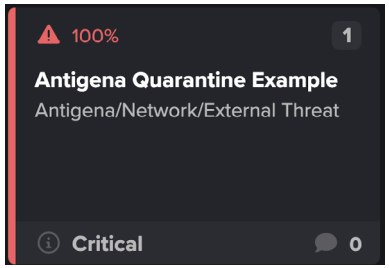


7. In **Active Mode** this should trigger the Darktrace RESPOND response.

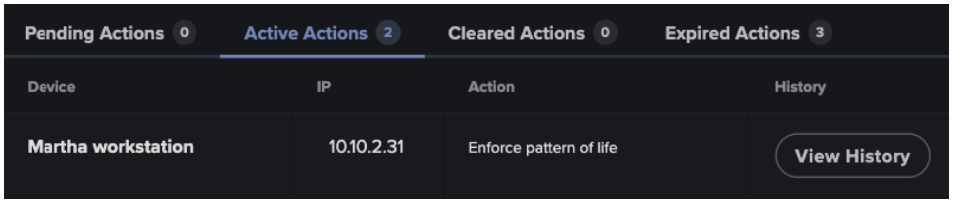
   By navigating to another website, such as Wikipedia, it can be seen that Darktrace RESPOND/Network has already started **blocking the device's network traffic**, meaning that the site cannot be reached.



8. Navigating back to the Darktrace Threat Visualizer interface, the associated **Darktrace RESPOND Model Breach** which has been generated is visible within the Threat Tray.

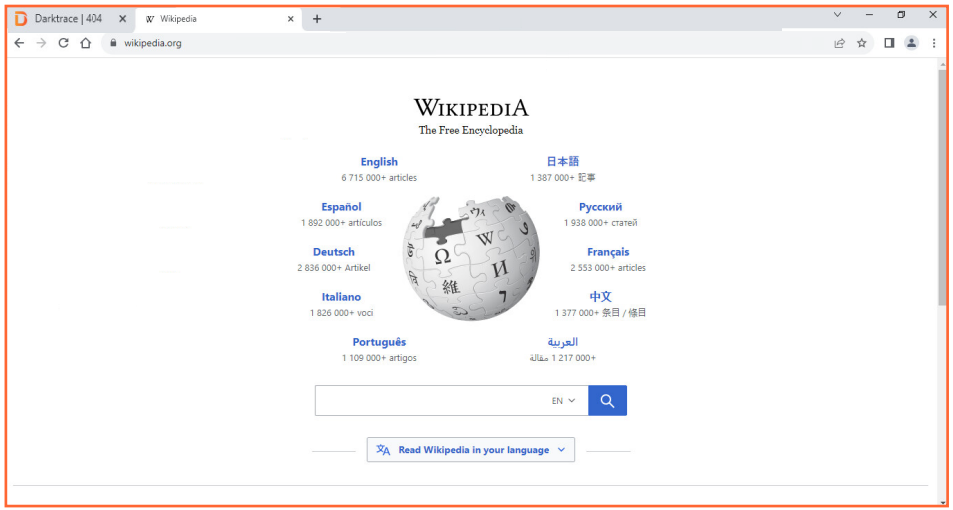


9. Go to the Darktrace RESPOND Actions page. Under the **Active Actions** tab, it is possible to confirm which actions are being taken on the device.



10. Click the **Clear** button to clear the in-progress action.

11. Try to **access Wikipedia again**. The cleared action means that network access has **returned to normal** on the device.



This example demonstrates how Active Mode differs from Human Confirmation Mode, as well as how the Antigena Quarantine Example model can be a convenient way to test whether a deployment is running Darktrace RESPOND as expected.

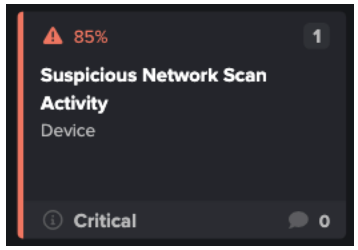
LAUNCH RESPOND ACTIONS

Continue your learning with our dedicated video 9. Manual RESPOND Actions

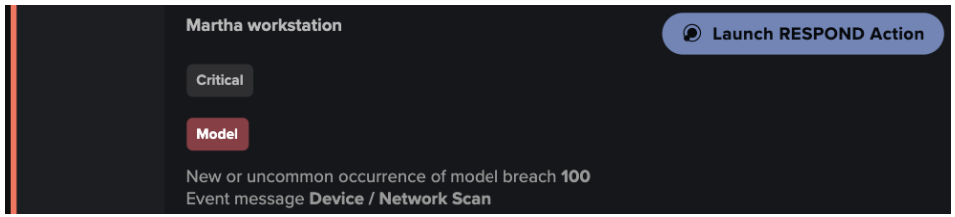
Darktrace RESPOND/Network actions can be launched from the Model Breaches, AI Analyst Incidents and Device Summary. The **Launch RESPOND Action** button allows users to manually trigger a Darktrace RESPOND/Network action, regardless of the modes.

Model Breaches

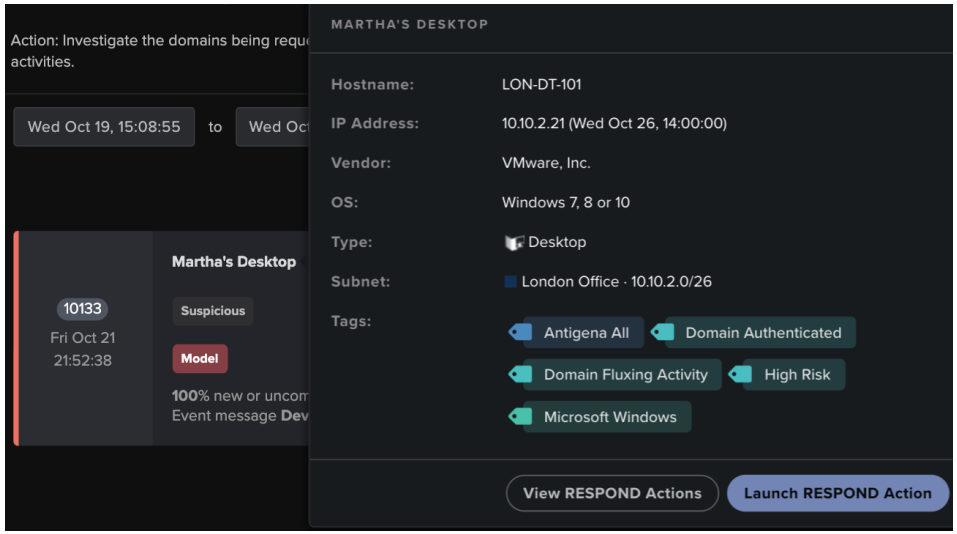
1. From the Model Breaches, select the **Model Breach** in the Threat Tray to open the **Breach Log**.



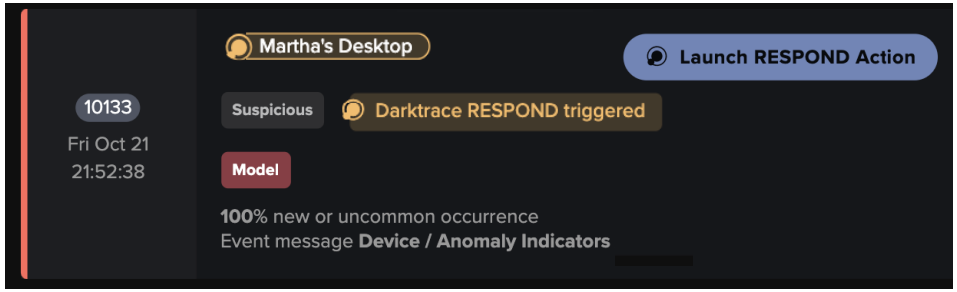
2. On the Breach Log, next to the corresponding breach, notice the **Launch RESPOND Action** button.



3. Hovering over the **Source Device** name will open the device's information, which will also display the Launch RESPOND Action button.

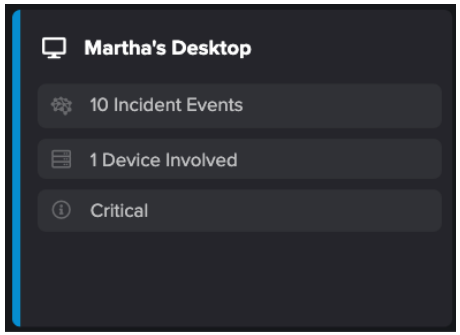


4. An **active** action on a device will be highlighted in **green**, a **pending** action will be highlighted in **yellow** and an **expired** action will be **grey**.

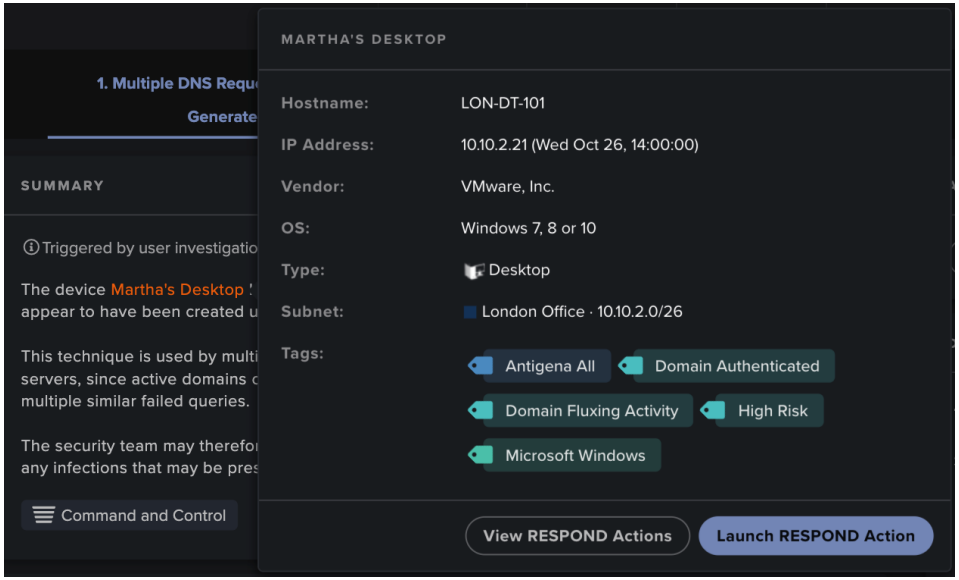


AI Analyst Incidents

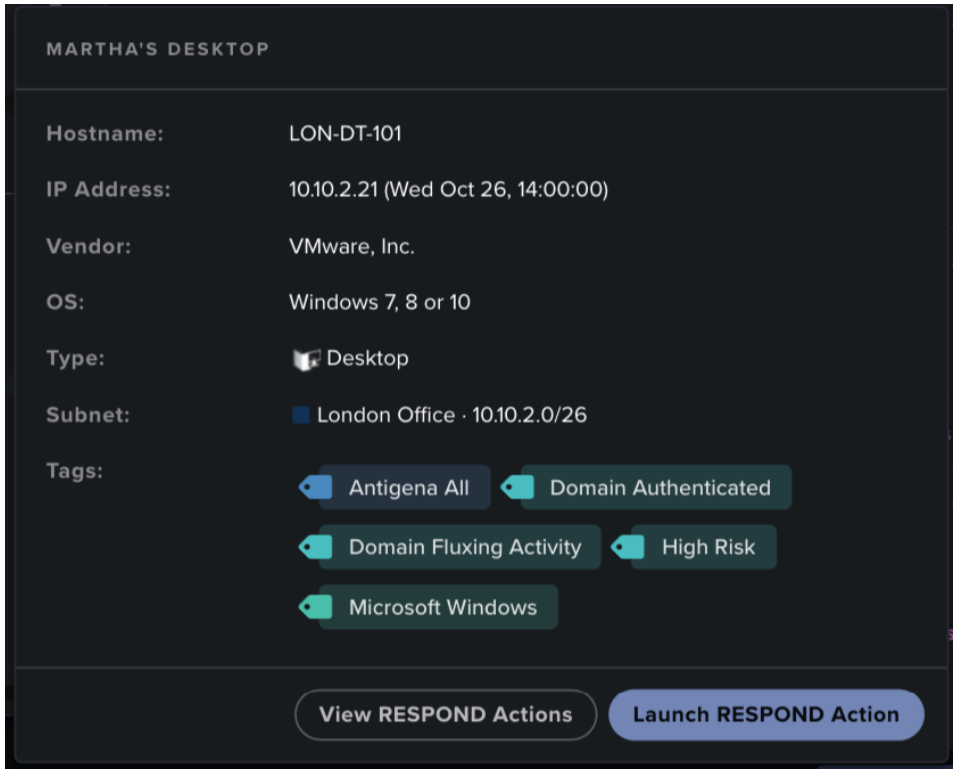
1. From the AI Analyst Incidents, select the desired incident in the Threat Tray and open the **Critical AI Analyst Incident**.



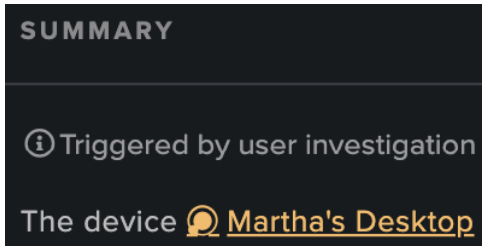
2. On the Critical AI Analyst Incident Summary section, hover over the device's name and notice the **Launch RESPOND Action** button.

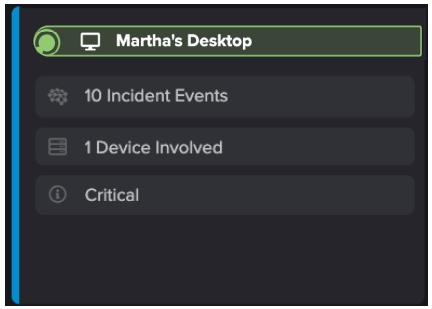


3. Hovering over the **Source Device** name will open the device's information, which will also display the Launch RESPOND Action button.



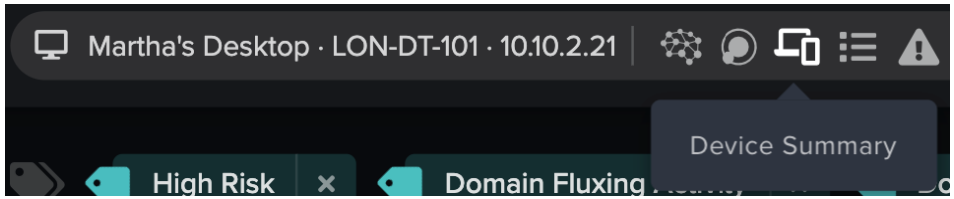
4. An **active** action on a device will be highlighted in **green**, a **pending** action will be highlighted in **yellow** and an **expired** action will be **grey**.



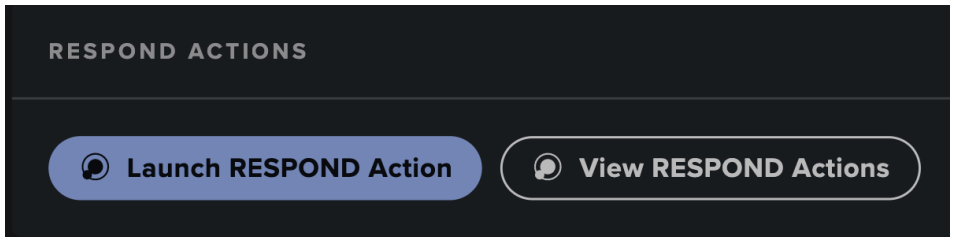


Device Summary

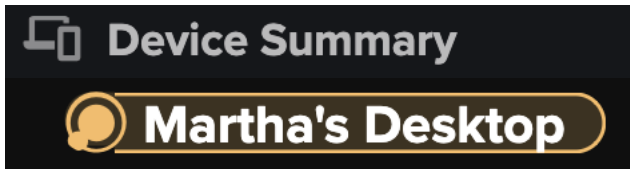
1. From the Omnisearch bar, select the desired device and open the **Device Summary**.

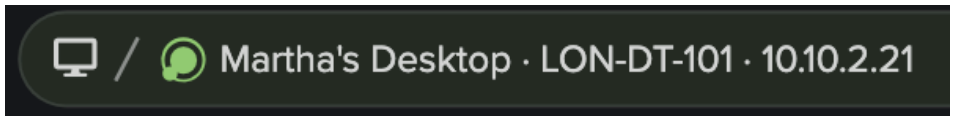


2. On the Device Summary notice the **Launch RESPOND Action** button available from the **Respond Actions** section.



3. An **active** action on a device will be highlighted in **green**, a **pending** action will be highlighted in **yellow** and an **expired** action will be **grey**.

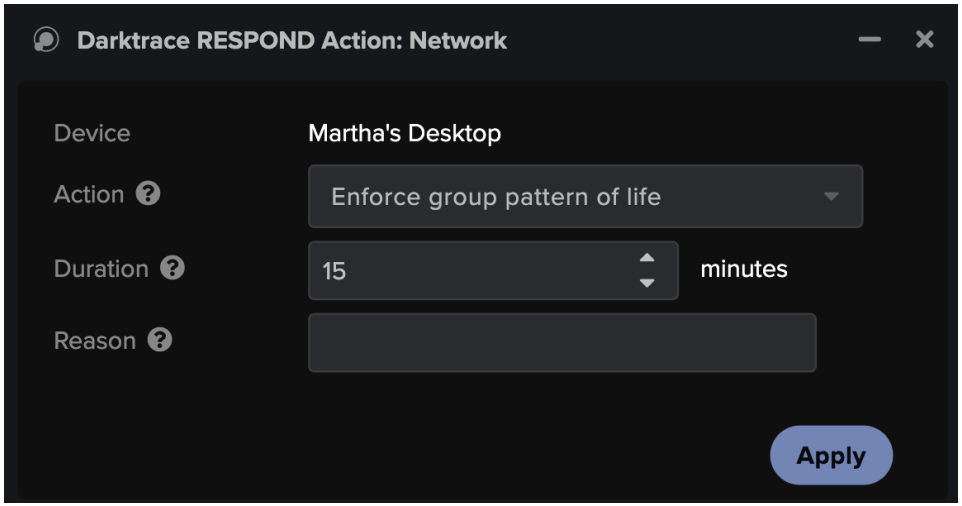




Launch RESPOND Action button

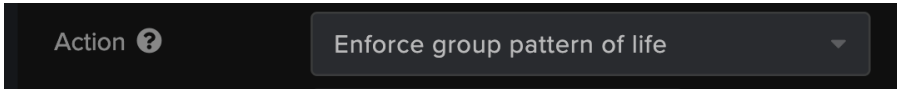
1. The Launch RESPOND Action button allows users to **manually trigger** a Dartkrace RESPOND/Network action.

2. Clicking on this button will open a **Darktrace RESPOND Action: Network** window with several options.



a. The **Device** name will be displayed at the top.

b. The **Action** drop-down menu allows you to select an action for this device.



Available actions are:

i. Enforce Group Pattern of Life

ii. Block all outgoing traffic

iii. Block all incoming traffic

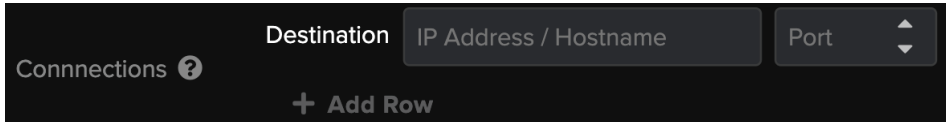
iv. Block all matching connections

v. Quarantine device

vi. Enforce Pattern of Life

vii. Isoloate Machine (Microsoft Defender)

Note: Upon selecting the Block matching connections action, an additional Connections option will appear to enter the specific connections which will be blocked from incoming or outgoing communication with this device.



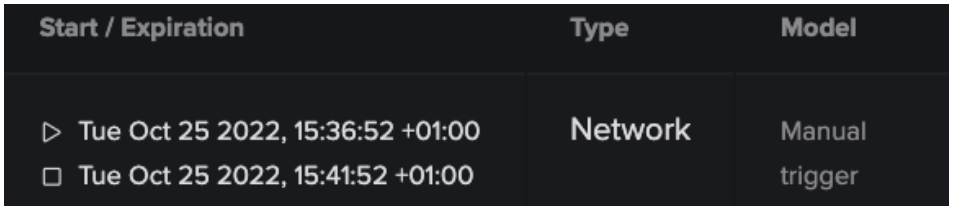
c. The **Duration** allows users to adjust the time during which this action will be valid for, in minutes.

d. Finally, users can enter their reasonning for adding the manual RESPOND action in the **Reason** textbox.

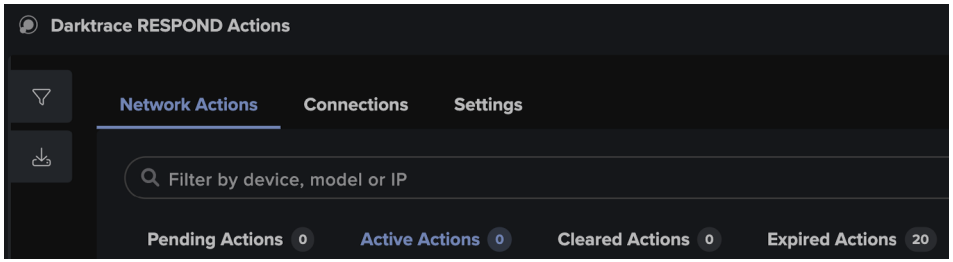
Note: there are two settings that must be set at a minimum - the desired action and the duration for that action.

3. Click on **Apply** to trigger the desired manual action.

4. This action is in the **RESPOND Action** page, as a Manual Trigger, with the Start/Expiration time corresponding to the selected duration.



5. Finally, the **View RESPOND Actions** button, available from the Model Breach, AI Analyst Incident and Device Summary, opens the device's actions with **Pending**, **Active**, **Cleared** and **Expired** actions displayed for this device.



RESPOND in Action Test

DARKTRACE
Cyber Engineer Certification

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

1. Why might there not be an Darktrace RESPOND Model Breach accompanying a breach?

- [ ] The device has not been tagged as Antigena
- [ ] Darktrace RESPOND is in Human confirmation mode
- [ ] Darktrace RESPOND breaches do not appear in the tray

2. Which page will allow you to review any actions requiring approval?

- [ ] System Config
- [ ] Tags
- [ ] Darktrace RESPOND Actions

3. What is the maximum amount of time an action can be extended by?

- [ ] 5 hours
- [ ] 24 hours
- [ ] 48 hours

4. What is the purpose of the Launch RESPOND Action button?

- [ ] To extend an active Darktrace RESPOND action
- [ ] To manually trigger a Darktrace RESPOND action
- [ ] To cancel a triggered Darktrace RESPOND action

5. If an action requires approval, a pop-up notification will appear.

- [ ] True
- [ ] False

6. Which hostname will result in a device being quarantined when visited?

- [ ] quarantineme.darktrace.com
- [ ] darktrace.quarantineme.com
- [ ] quarantineme.darktrace.co.uk

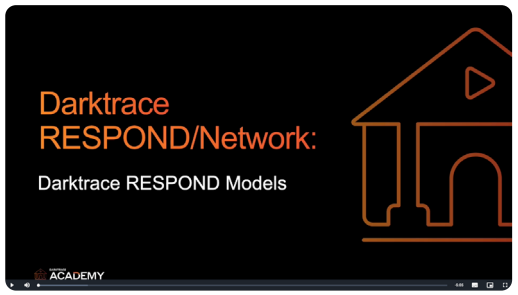
Clear All Answers

6. The Model Editor

In order to detect different threat types, Darktrace has a comprehensive Model deck which can cause Model Breaches to appear in the Threat Visualizer if triggered. Within the Model Editor, there are Darktrace RESPOND specific Models, which not only alert you to unusual activity, but can also apply autonomous actions. This chapter covers the Model Editor in the context of Darktrace RESPOND/Network.

Darktrace RESPOND/Network actions are activated by Model Breaches within the Threat Visualizer. There is a collection of Darktrace RESPOND/Network Models which are set to trigger on specific types of behavior and are designed to perform different actions depending on the incident identified. A large variety of actions are possible. For example, incoming and/or outgoing traffic can be blocked by Darktrace RESPOND/Network or it can block incoming connections from the internet to a server on a specific port.

Model Definition



Continue your learning with our dedicated video 10. RESPOND Models

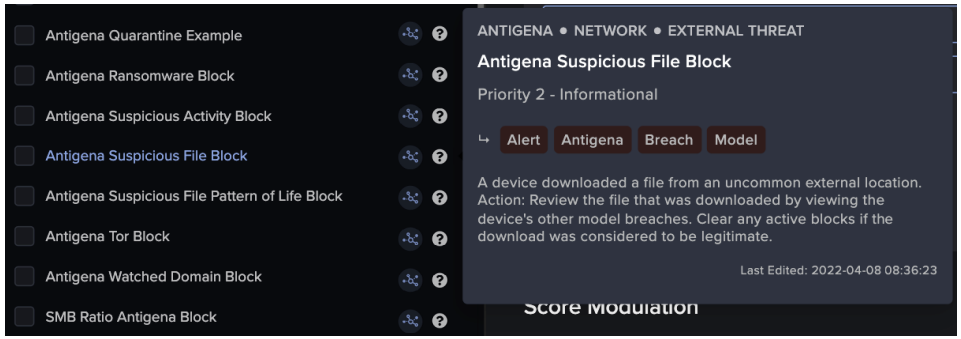
1. Within the **Model Editor**, navigate to **Antigena** folder. Notice there are subfolders for **Network** and **SaaS**.

2. For ease of administration, Darktrace RESPOND/Network Models, in the Antigena > Network folder, are **grouped into different categories**:

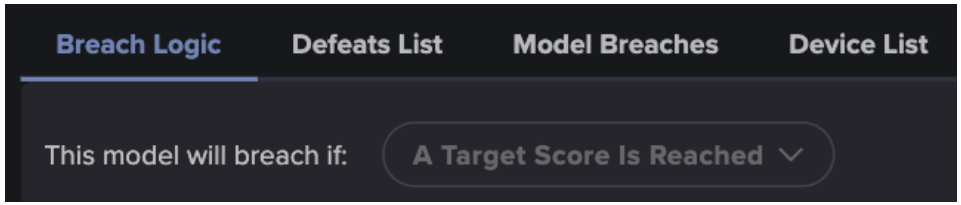
- **Compliance:** These models fire when a device is breaking certain types of common compliance issues, such as the usage of Tor.
- **External Threat:** These fire on external threats such as when ransomware is detected encrypting internal network shares. Darktrace RESPOND identifies such behavior and can quarantine affected devices from the network.
- **Insider Threat:** Insider threats are events within a network such Internal Data Transfer. This can breach, for example, if Darktrace identifies unexpectedly large downloads from internal servers to client devices particularly with devices they do not normally communicate with.
- **Manual:** The models contained within this folder will enforce Darktrace RESPOND/Network actions for any devices manually tagged with a "Manual" Darktrace RESPOND/Network tag.
- **Significant Anomaly:** This can include a large range of activity, usually when there is a large shift in network activity from what Darktrace has established as the norm.

Note: Darktrace RESPOND/Network Models apply to both Darktrace RESPOND/Network and Darktrace RESPOND/Endpoint devices. Darktrace RESPOND/Apps actions act on SaaS accounts so rely on different Models. These are described in the Model Actions section.

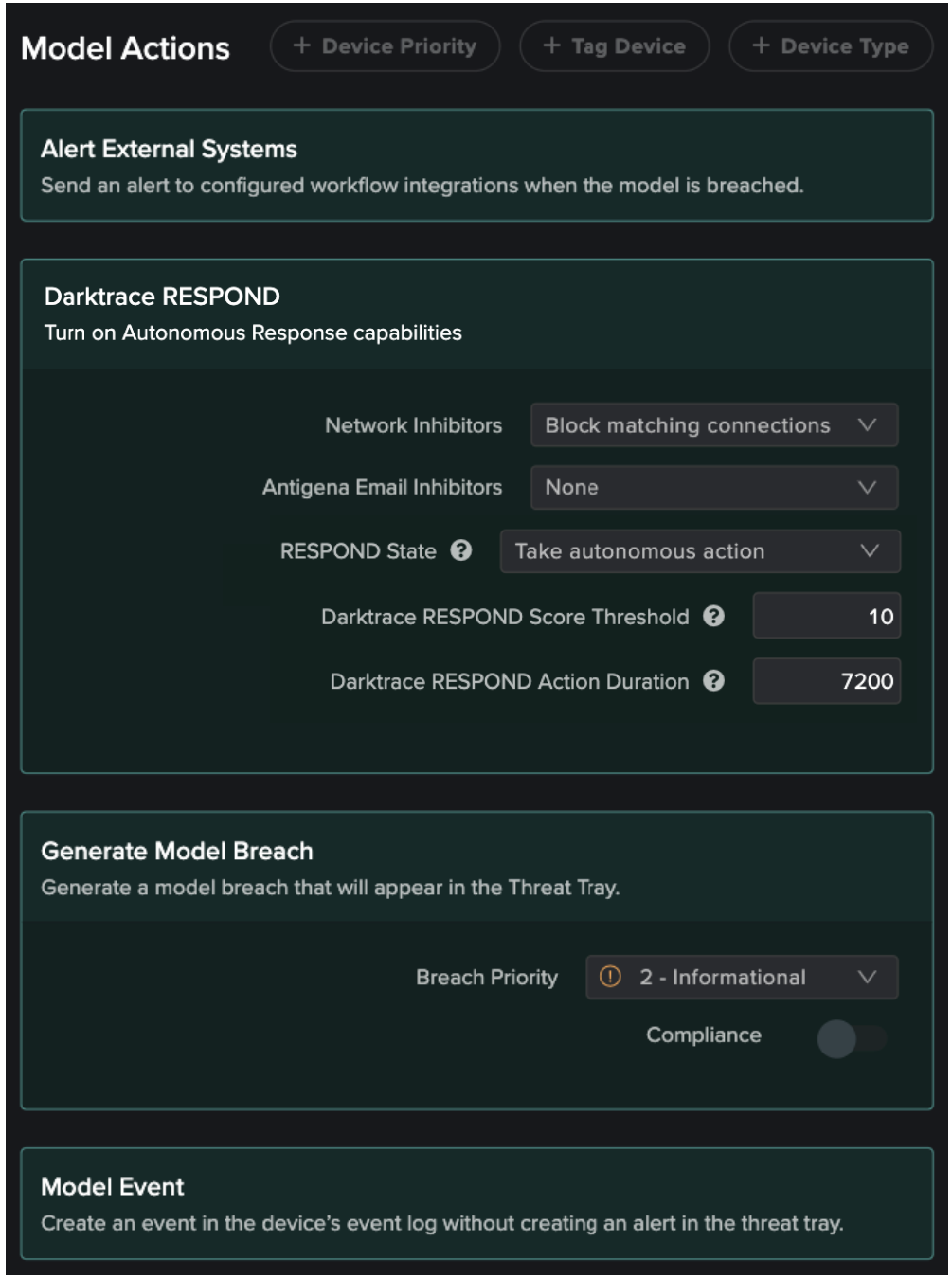
3. Move into the **External Threat** folder and select the **Antigena Suspicious File Block** Model. This is a Model that can react to any device that downloads a file from a rare external location.



4. The Model Definition indicates that this Model will breach if a **target score is reached**.



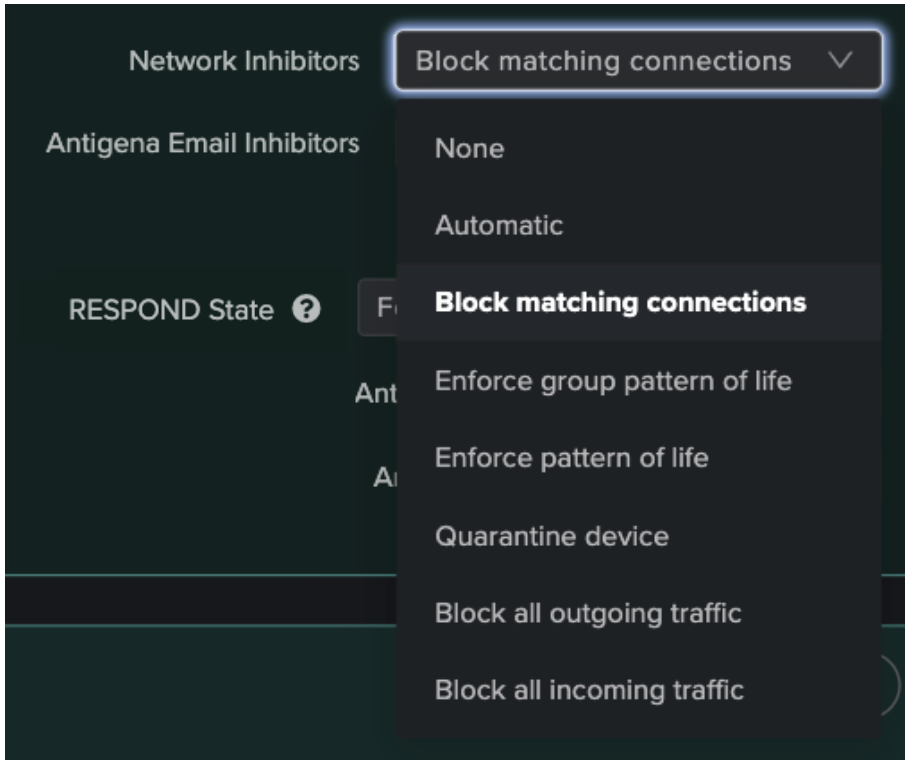
5. Scroll down to the **Model Actions** section of the Model Definition and notice the **Darktrace RESPOND subsection**. This option controls the Darktrace RESPOND functionality of the Model.



Model Actions

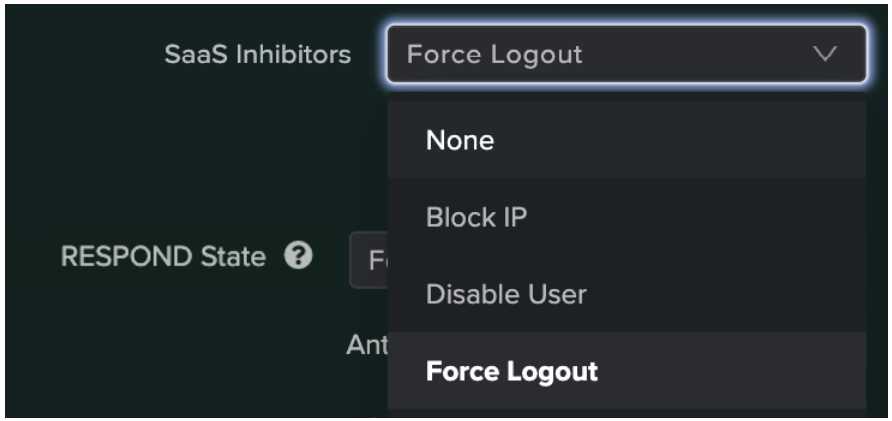
1. The Darktrace RESPOND Autonomous response capabilities is split up into different fields.

   a. First, review the **Network Inhibitors** section. This specifies what kind of action Darktrace RESPOND should take on any offending devices. Notice there may be further inhibitor options, depending on what modules are bundled with your deployment.

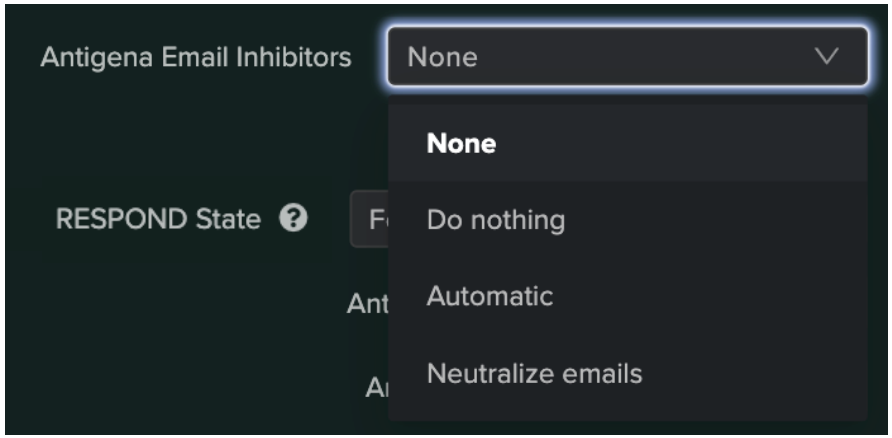


Additional Actions

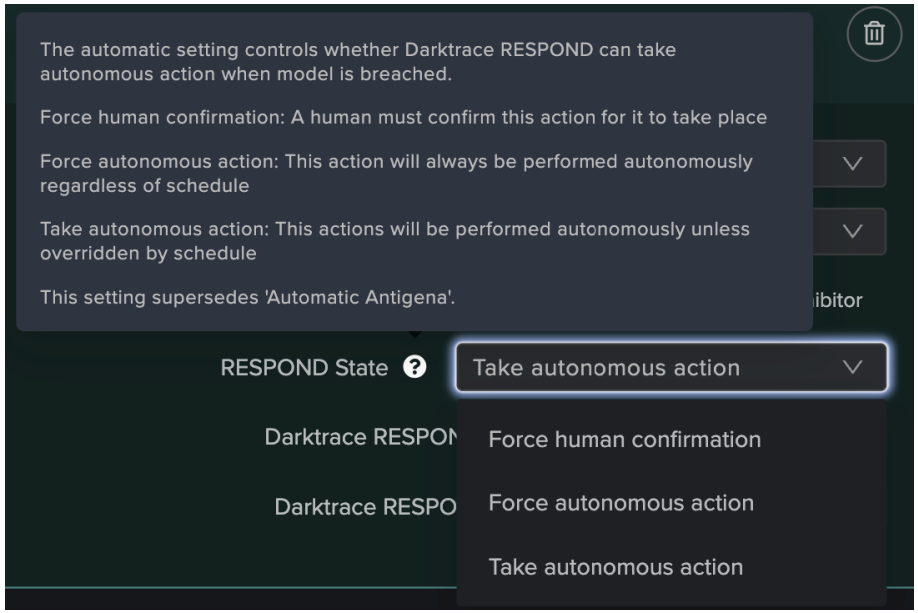
For deployments including **SaaS**, Darktrace RESPOND/Network can take one or more responses as a result of a model. Each SaaS platform is different, and depending on which SaaS platform is installed, the types of responses which can take place may vary.



If you have **Darktrace RESPOND/Email**, there may be additional options to take automatic Darktrace RESPOND/Network actions or neutralize emails.



b. **RESPOND State** is employed when Use Model Settings (Active Mode) is set in the Darktrace RESPOND Actions submenu.



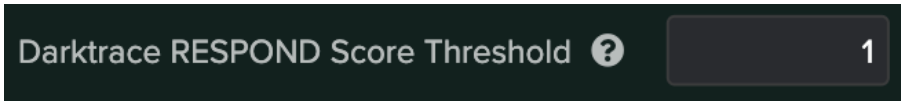
This can provide a more granular approach to Darktrace RESPOND actions on a per-Model basis and can be useful for tuning models to better reflect the needs of the corporate environment.

i. Some Models may be set to **always require confirmation** (force human confirmation) so that human approval is required before Darktrace RESPOND can take action.

ii. The opposite can be true where some Models **never require confirmation** (force autonomous action). Instead, they will always take actions automatically.

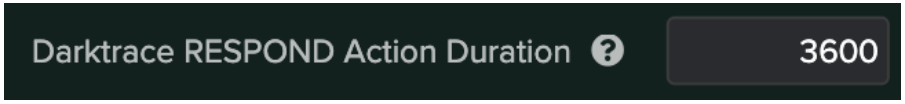
iii. Finally, Models can be set to f**ollow the action schedule** (take autonomous action) as outlined in the Darktrace RESPOND pane. Ultimately, this means Models may be able to take autonomous actions sometimes but require human confirmation at other times.

c. The **Darktrace RESPOND Score Threshold** sets the minimum model breach score that must be achieved in order to trigger the action. This defines how lenient Darktrace RESPOND should be in deciding whether to take action on the offending device.



The lower this is, the more likely Darktrace is to create an action in the Darktrace RESPOND Actions endpoint. This value is part of complex machine-learning based algorithms in the backend that include factors such as the regularity of such behavior for the device.

d. Finally, the **Darktrace RESPOND Action Duration** setting specifies how long in seconds the action should last for. Many Darktrace RESPOND Models will have a default value of 3600 (1 hour).



Darktrace RESPOND/Endpoint Inhibitors

Models can take a series of actions in response to breaching such as triggering an alert, raising the priority of a device or adding a tag. When Darktrace RESPOND is enabled on a deployment, the additional Darktrace RESPOND model action becomes available. When Darktrace RESPOND/Network or Darktrace RESPOND/Endpoint are enabled within your Darktrace environment, category of Darktrace RESPOND (Antigena) models already using the Darktrace RESPOND action are exposed.

This action allows an operator to set an 'inhibitor' - an action to inhibit the behavior that matches the model criteria. Darktrace RESPOND/Network and Darktrace RESPOND/Endpoint share a set of inhibitors that can be selected.

ACTION	DESCRIPTION
Automatic	This option lets Darktrace RESPOND/Network automatically choose the best option using information gathered from the incident. For example, if it sees suspicious behavior to an SMB share on port 445, it would choose to block just that port, but if it saw a range of suspicious connections to various places on the internet it would choose to block external connections instead.
Block Matching Connections	This option will block connections from the device to the destination endpoint seen in the incident on the destination port that was observed. This can be useful when taking highly focused action that minimizes the impact on regular network behaviour.
Enforce Pattern of Life	Allows a device to make the connections that it usually makes based on Darktrace's established patterns of life for the device. It only allows connections and data transfers which Darktrace considers normal for that device. Anything else is blocked.
Enforce Group Pattern of Life	This option is more permissive than enforce pattern of life. It allows a device to make any connections and data transfers that it or any of its peer group typically make. This refers to the device's list of most similar devices. Therefore, if the offending device does not normally access a particular SMB share, but some devices in its peer group do, it will be allowed to access that share.
Quarantine Device	All network traffic coming into the device or originating from the device is blocked. This effectively completely shuts off the device from the rest of the network.
Block All Outgoing Traffic	Any network traffic originating from the offending device will be blocked.
Block All Incoming Traffic	Any network traffic coming into the offending device will be blocked.

Darktrace RESPOND/Apps Inhibitors

Darktrace RESPOND can take a range of proactive, measured, automated actions in the face of confirmed cyber-threats detected in real time. Where anomalous behavior in a third-party SaaS platform begins to escalate, Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules can step in and utilize access policies and administrative tools to control the account and sever the malicious actor's access.

Models can take a series of actions in response to breaching such as triggering an alert, raising the priority of a device or adding a tag. When Darktrace RESPOND is enabled on a deployment, the additional Antigena (Darktrace RESPOND) model action becomes available.

If a Darktrace/Apps, Darktrace/Zero Trust or Darktrace/Cloud module with RESPOND capabilities is enabled within your Darktrace environment, it comes with a category of Darktrace RESPOND models already using the Darktrace RESPOND action to perform responses.

This action allows an operator to set one or more 'inhibitors' - actions to inhibit the behavior that matches the model criteria. Darktrace RESPOND SaaS actions are those taken in third-party environments, primarily against user accounts. The suite of actions differs between each SaaS, Zero Trust and Cloud platform - models can therefore have multiple inhibitors set to ensure they can take an action in every possible environment.

Users and IP addresses can be made 'immune' from specific inhibitors or from all inhibitors on a per-module basis. By default, all users known to a module licensed for Darktrace RESPOND are eligible for actions. Immunity from actions is controlled on the System Config page.

ACTION	APPLICABLE MODULES	DESCRIPTION
Block IPs	**Microsoft 365**	Prevents access to the account from an IP or IP range for the duration set.
Disable User	**Microsoft 365, Zoom, Okta, Duo, Google Workspace, JumpCloud, Salesforce**	Disables a user account for the duration set.
Freeze User	**Salesforce**	Freezes a user account for the duration set.
Force Logout	**Microsoft 365, Zoom, Google Workspace**	Forces the user to log out from the platform. This action is a one-off action, so will be repeated at the configured interval for the duration set. The default interval is 15 seconds and can be altered by a member of Darktrace support if required.
Disable Inbox Rule	**Microsoft 365**	Disables an inbox rule in the Microsoft 365 exchange environment.

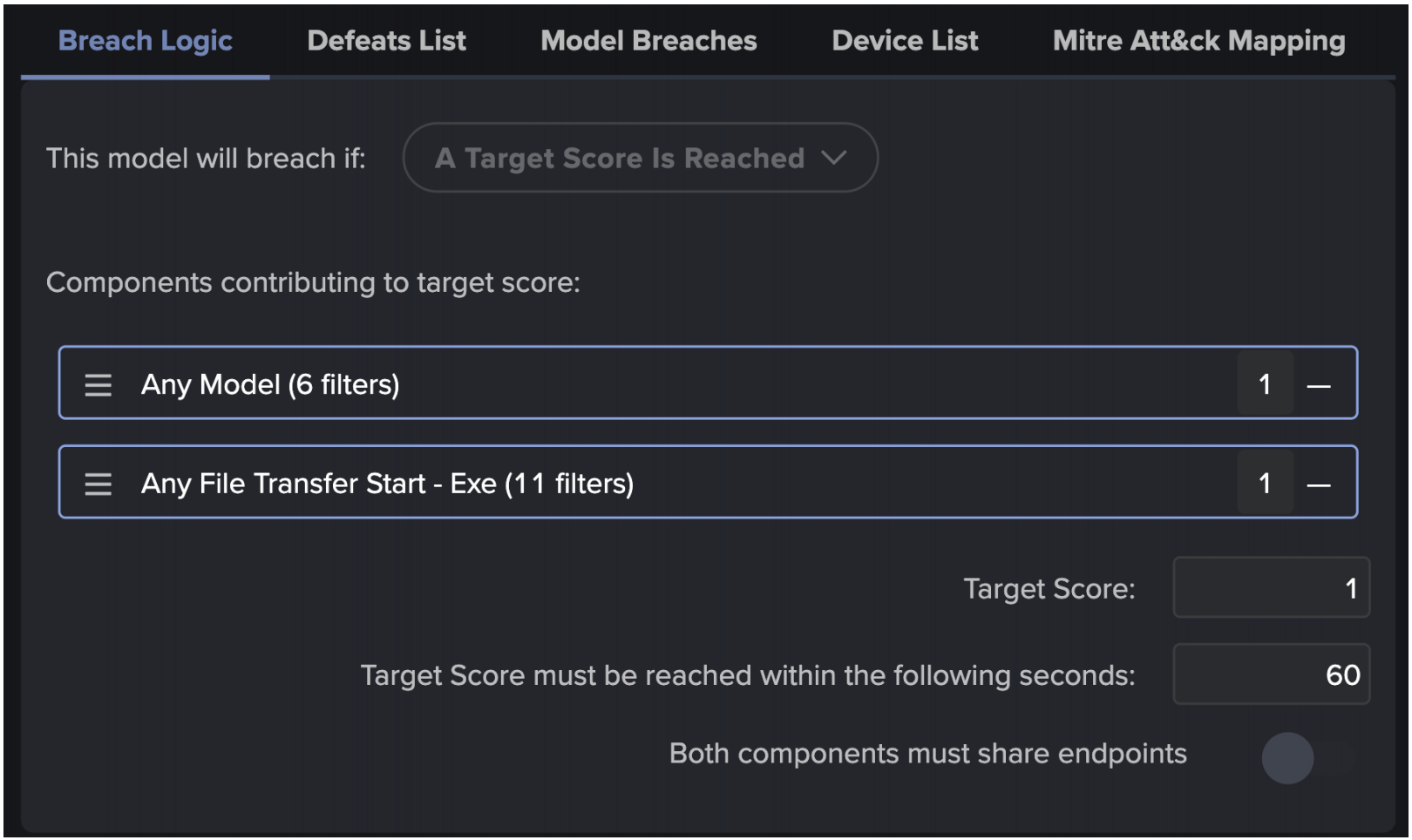
Model Logic

1. Review the **Breach Logic** section for this Model. There are two components, both with a score weighting of 1. So, if either component's prerequisite conditions are met, the Model will fire.

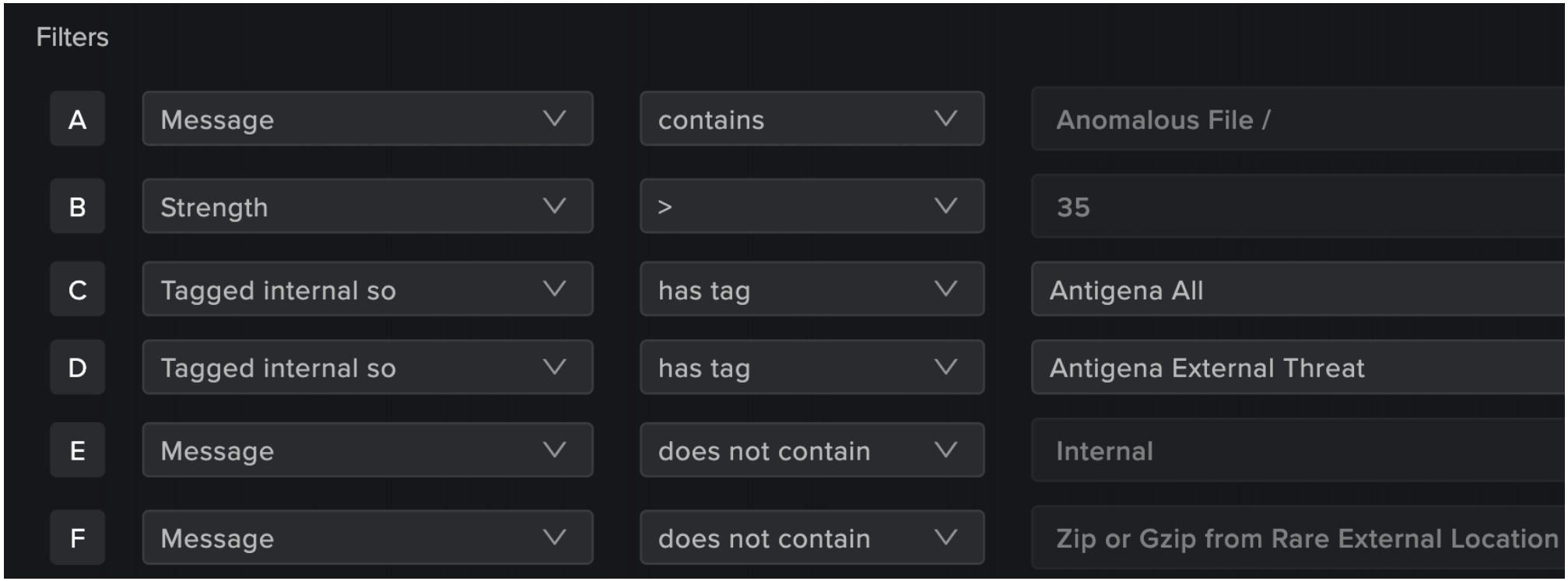
2. Check the **first component**. Many Darktrace RESPOND/Network Models base their detection off of standard Darktrace Model Breaches. This is denoted by the component's logic metric called **Model**. In this example, any Model whose file path contains "Anomalous File" will cause the Model to fire.

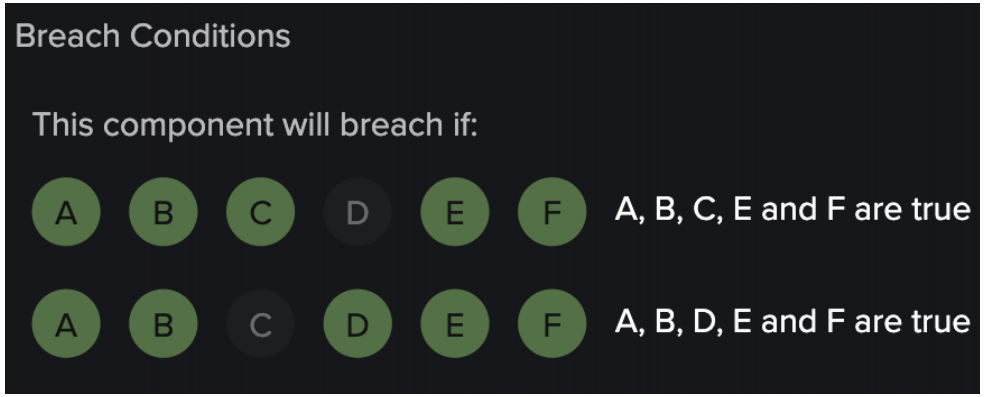
Continue your learning with our dedicated video
11. RESPOND Breach Logic

Example: This Antigena Suspicious File Block example demonstrates how assigning different tags can enable or disable Darktrace RESPOND/Network monitoring for different devices. Often, it is easy to tell which Model relates to which tags based on the subfolder of the Antigena folder they belong to. However, it is useful to check the Model Definition for tag filters, just to be sure, as some Models act on a wider range of tags. This will be discussed more in the next section.



3. Importantly, notice that the Model contains filters checking for two tags: **Antigena All** or **Antigena External Threat**. The "OR" element in this can be confirmed by checking the **Breach Conditions**, located below the components.

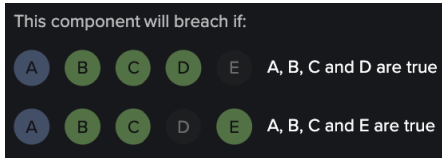




Breach Conditions

Filters on the same row are combined with an AND condition, whereas different rows are joined with an OR condition.

Active and non-active filters are depicted in green and gray respectively. Blue circles indicate the filter is always enabled.



The Model Editor Test

DARKTRACE
Cyber Engineer Certification

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

1. Which of the below is not an Darktrace RESPOND/Network Model category?

- [ ] Data Loss
- [ ] Compliance
- [ ] Manual

2. The Manual category enforces actions for devices tagged as "High Risk".

- [ ] True
- [ ] False

3. Which field is available on all deployments of Darktrace RESPOND/Network?

- [ ] Darktrace/Email Inhibitors
- [ ] SaaS Inhibitors
- [ ] Network Inhibitors

4. Which Automatic Darktrace RESPOND option will NOT force autonomous action?

- [ ] Always require confirmation
- [ ] Never require confirmation
- [ ] Follow action schedule

5. Which action causes minimum impact on regular network behavior?

- [ ] Quarantine device
- [ ] Block all outgoing traffic
- [ ] Block Matching Connections

6.Based on this image, the component will breach if:

- [ ] A, B, C, D, F and G are true
- [ ] A, B, C, D, and F are true
- [ ] A, B, C, D, E and F are true

Clear All Answers

7. Applying Tags

As shown in the previous chapter, Darktrace RESPOND/Network Models require devices to be tagged with Antigena tags in order for them to be included in Darktrace RESPOND's network monitoring. Covered in this section are multiple methods of tagging the devices on the network in order to begin the roll-out of Darktrace RESPOND.

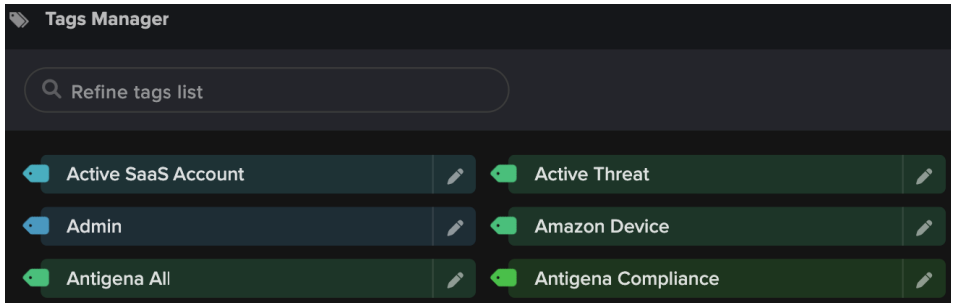
Introduction to Tags

Continue your learning with our dedicated video
12. Tagging

Tags are used to label devices, for rapid navigation and UI context when browsing devices. They can be used for defining "roles" within a network and as filters when creating Models. Models can be configured to only breach if a device has a specific tag, or to exclude devices with a specific tag.

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

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



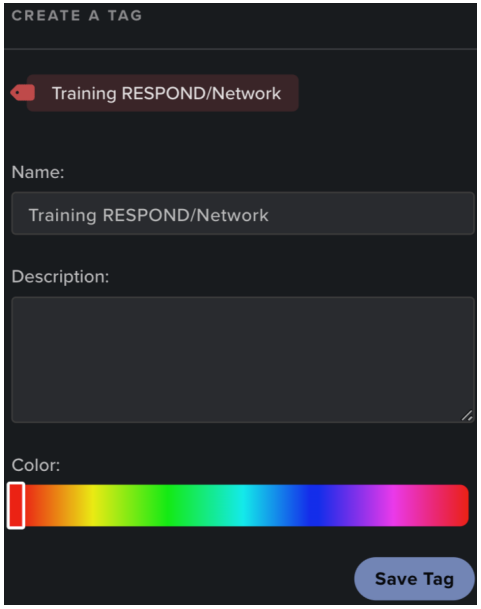
2. From this window, you can create a new tag by clicking on the **Add New Tag** symbol.

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

b. A **description** can also be added to help identify the purpose of the tag.

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

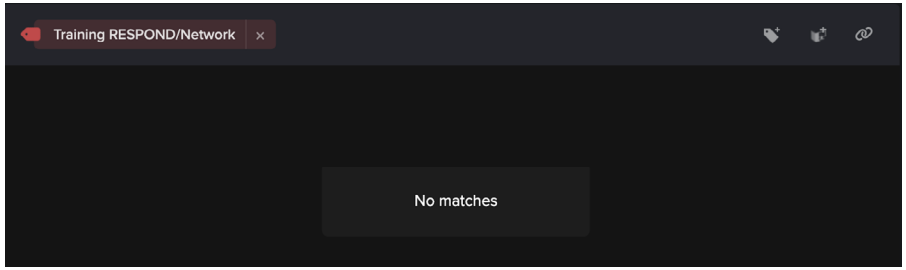
d. When complete, click **Save Tag**.



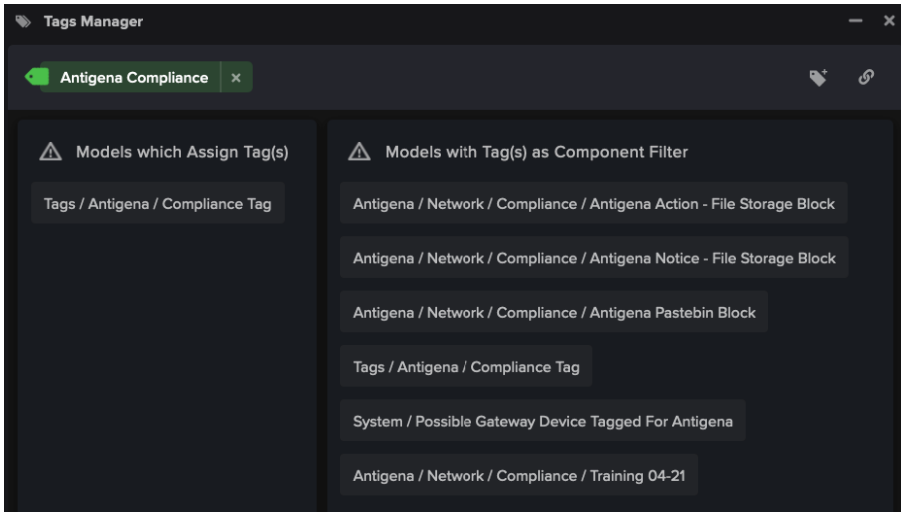
3. The new tag will appear on the **Tags Manager** dialog window.

4. Click the **tag** 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.

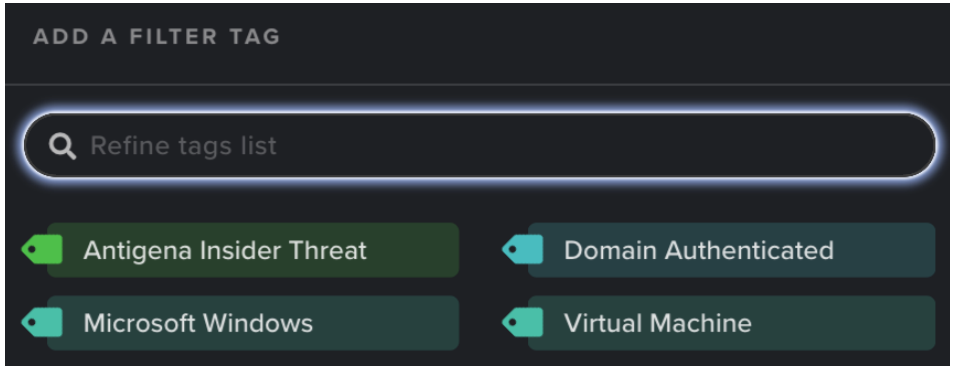


b. By selecting a mature tag, a new view will open in the **Tags Manager window**. It displays the selected tag in the top corner and lists any devices tagged as well as showing if any **models are assigning or using the tag**.



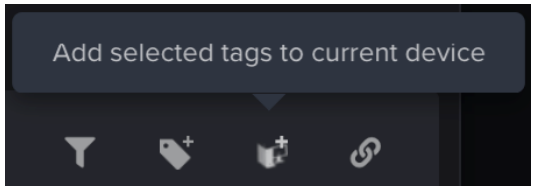
5. Within this Tags Manager view, there may be the option to **add further filters** to narrow down the results displayed.

Here, more Tags can be filtered/applied to the Tags Manager to see which devices are tagged and which models are referred to.

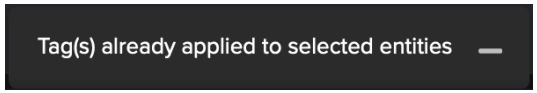


6. When a device view is selected in the Threat Visualizer and is populated in the Omnisearch bar an additional button is displayed in-between the **Add New Tag** and **Explore Tags** icons.

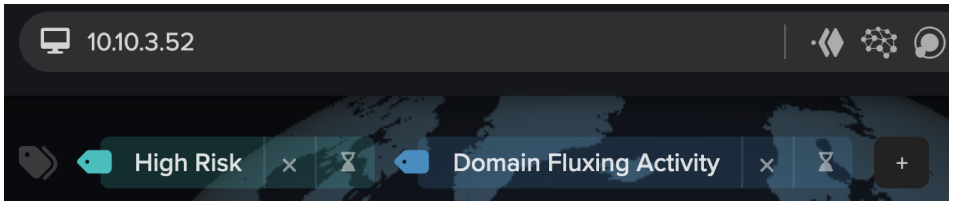
Click the **Add selected tags to current device** button. Refreshing the Tag Manager pane will reveal the device hostname within the **Tagged Objects** pane.



Note: if a device already has the selected Tag and a use attempts to apply the same Tag, a warning message will be displayed.

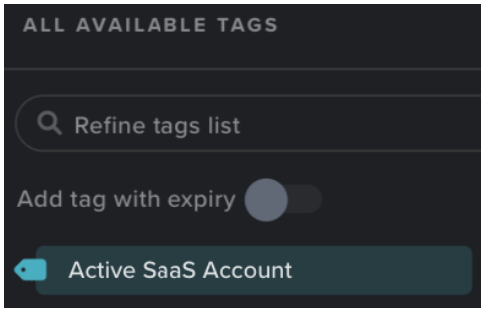


7. When a device is selected, any associated Tags are displayed below the Omnisearch bar.

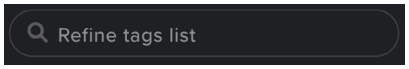


8. Additional tags can be added to the device by selecting the + button next to the existing tags.

a. A **pop-up window** will display all tags that can be added to the device.

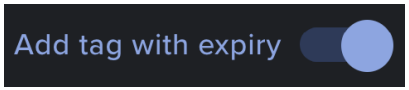


b. **Refine tags list** enables searches to locate the required tag.



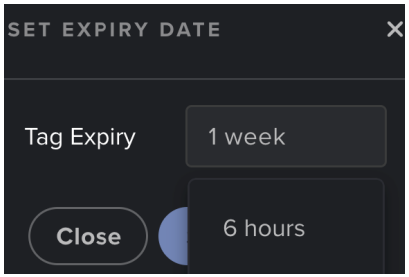
c. Tags can be added with an **expiry time**. This allows for temporary tags to be applied.

i. To add an expiry time with the new tag, toggle the **Add tag with expiry** button on.

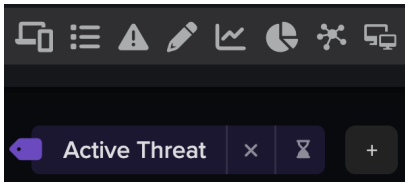


ii. A **timer** will appear next to the name of the tag.

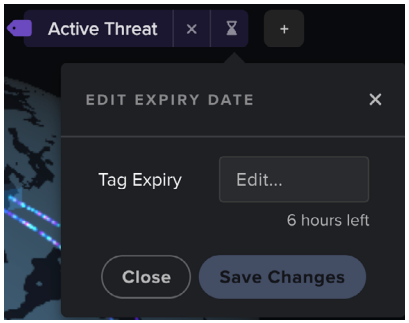
iii. Clicking on the tag will display to **expiry time options**. Simply select the desired expiry time and the tag will be active for that period of time.



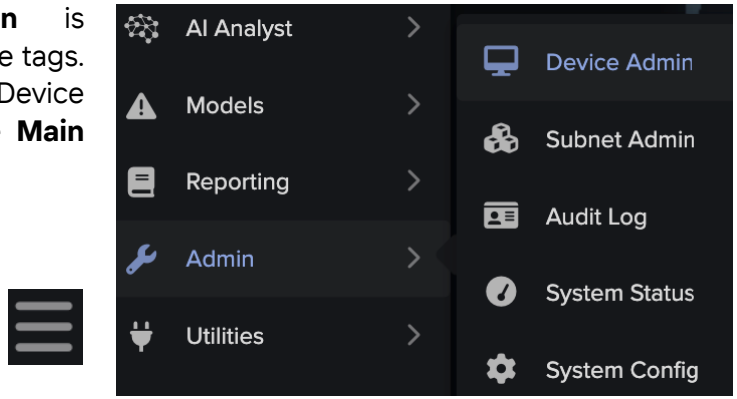
iv. Once the expiry time is set, the tag will be shown below the Omnisearch bar with the **timer icon**.



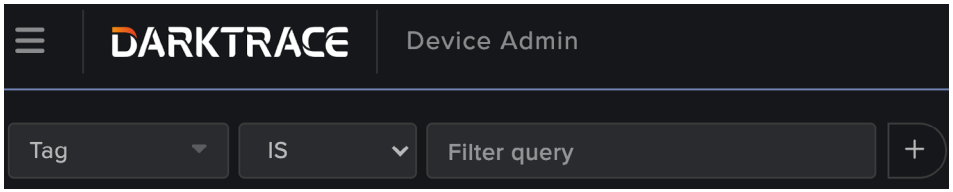
v. The expiry time can be **edited** by selecting the timer icon on the tag



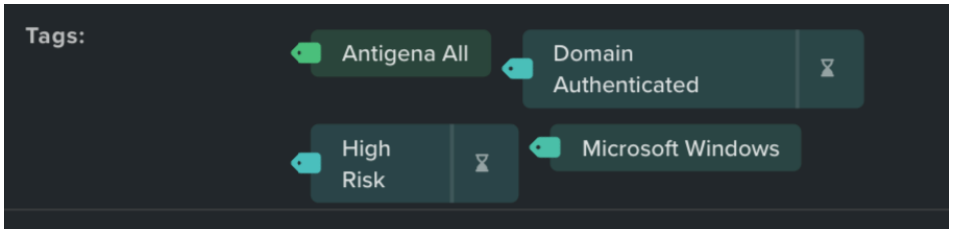
9. **Device Admin** is useful to manage tags. Navigate to the Device Admin from the **Main Menu**.



10. To search for a specific tag select the **Tag search option** and enter the name of the tag. The filter can be adapted using **Boolean operators** if necessary.

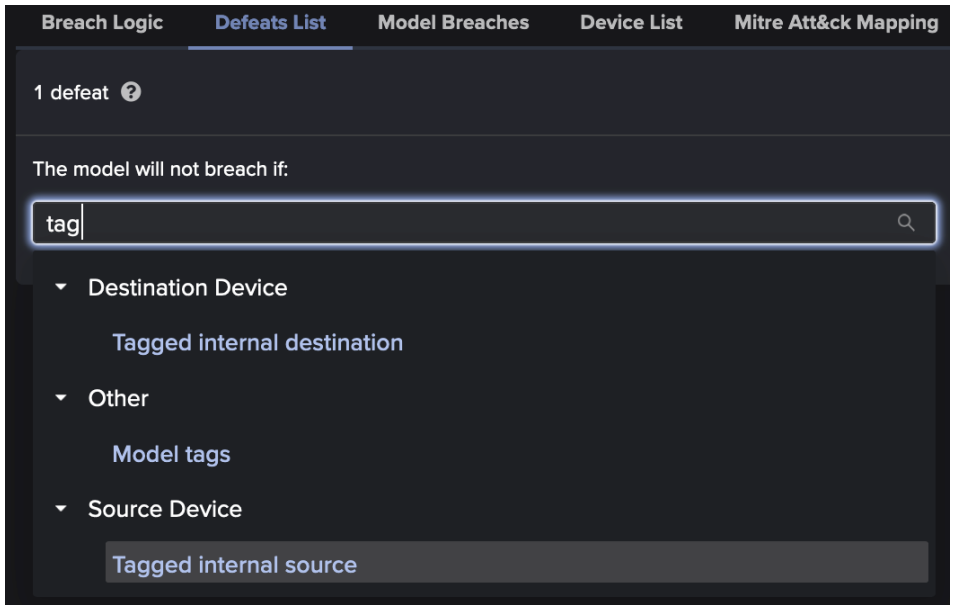


11. Any tags that are applied to devices are displayed when **hovering over a device** in the Subnet and Device view.



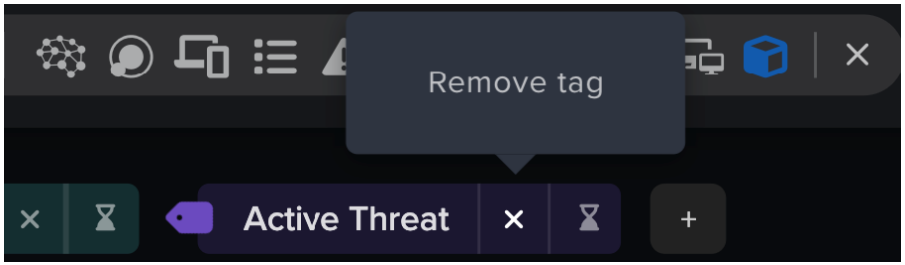
12. Tags can also be employed in the Model Editor as part of the **filter conditions** for a Model in the **Breach Logic** or as a **defeat** in the **Defeat List**.

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

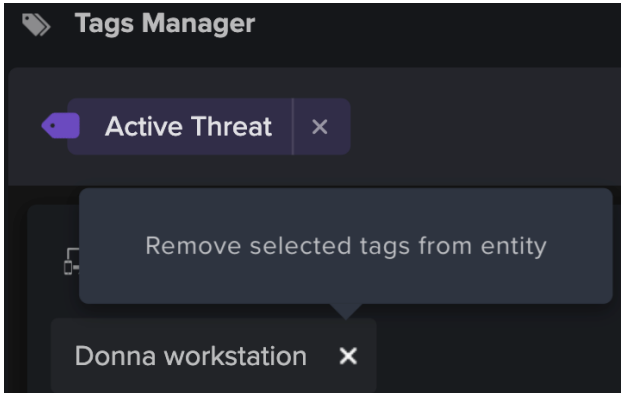


13. Tags can be **removed** using multiple methods.

    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**.

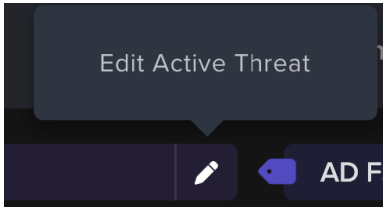


    b. Another method is to click on the tag underneath the Omnisearch bar and then delete the tagged device from the **Tagged Devices** pane.



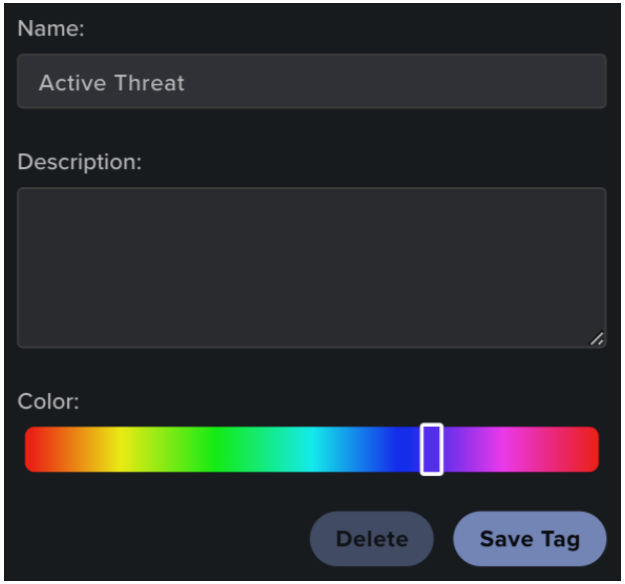
    c. **Deleting** a tag will also automatically untag all devices which share the deleted tag.

        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.

Note: to delete the tag you may require elevated privileges.



Tagging

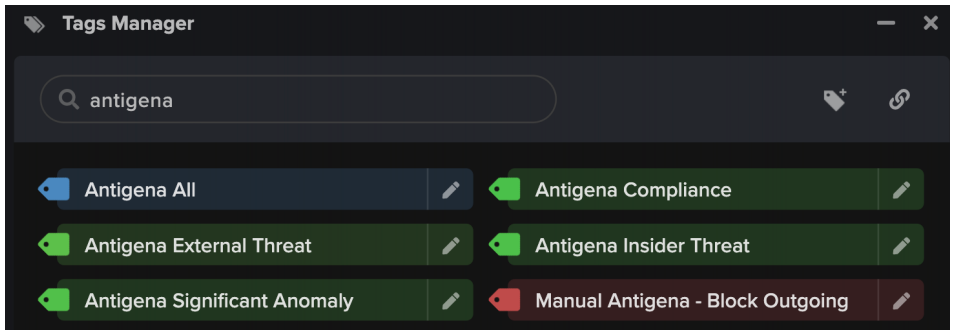
Continue your learning with our dedicated video
13. Tagging Devices

As shown in the previous chapter, Darktrace RESPOND/Network models require devices to be tagged with **Antigena** tags in order for them to be included in Darktrace RESPOND/Network's monitoring.

Covered in this section are multiple methods of tagging the devices on the network in order to begin the roll-out of Darktrace RESPOND/Network.

1. From the **main menu**, select the **Tags** option to open the **Tags Manager**.

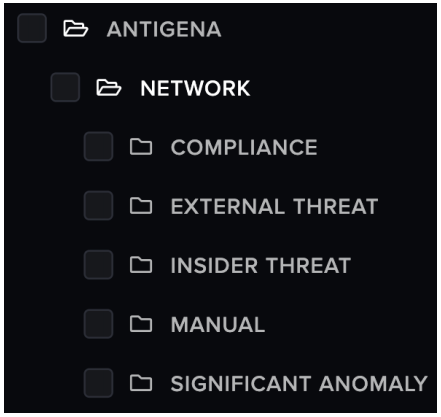
2. Search for **Antigena** to view a range of Antigena Tags that are available.



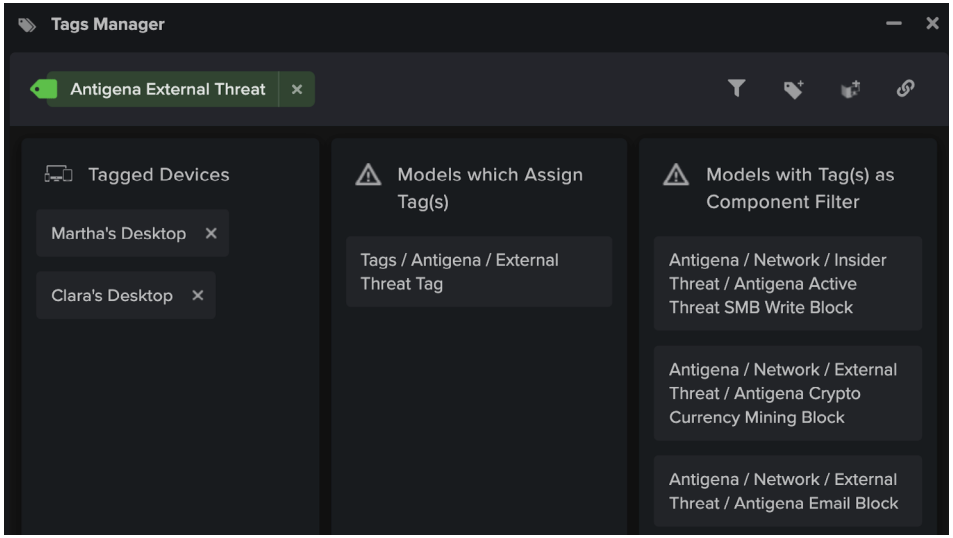
3. The four green tags as pictured above correspond to four of the folders located in the **Antigena > Network folder** in the Model Editor.

Furthermore, the three Manual Antigena tags correspond to models defined in the Manual folder.

Note: Tag colors do not inherit a specific meaning.



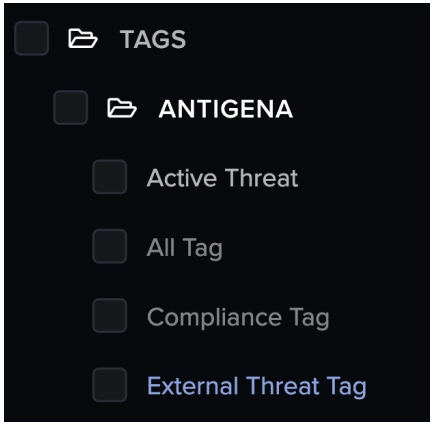
4. While the **Models** in these folders generally look for **tags** that match their folder name, some look for a wider range of tags.



By reviewing the tag in the Tags Manager, it is possible to verify which Models will act on it. For example, click the **Antigena External Threat tag** and we can see that it also allows monitoring by some models in the **Insider Threat folder**.

5. **Automatic tagging** is often the easiest method to implement Darktrace RESPOND/Network.

   Begin by looking at the **Tags > Antigena > External Threat** tagging Model and use it to tag an internal subnets.



Automatic Tagging Recommendations

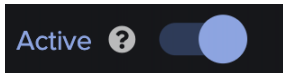
The simplest way to enable Darktrace RESPOND/Network for a small network is to apply the Antigena External Threat tag to every device, which allows devices to breach Darktrace RESPOND/Network Models.

The recommended Darktrace RESPOND/Network setup will vary depending on the deployment; some may initially focus on a specific type of breach and group of devices. This can assist in the process of tuning and removing false positives.

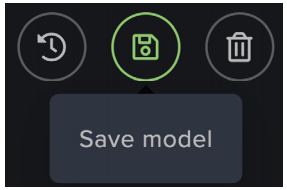
6. The Model is currently **inactive**.

   a. To activate the Model, first click **Edit Model** in the top right.

   b. Switch the **Active toggle to on**.

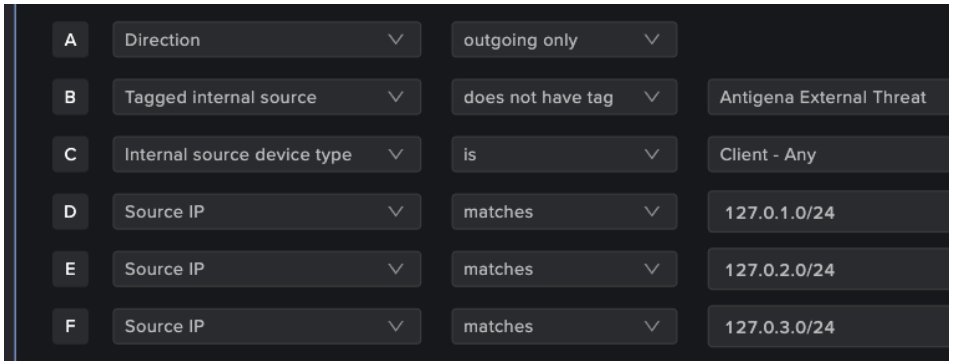


   c. **Saving the changes** will make the Model automatically tag any devices it sees connections from in the IP address ranges specified in its component.

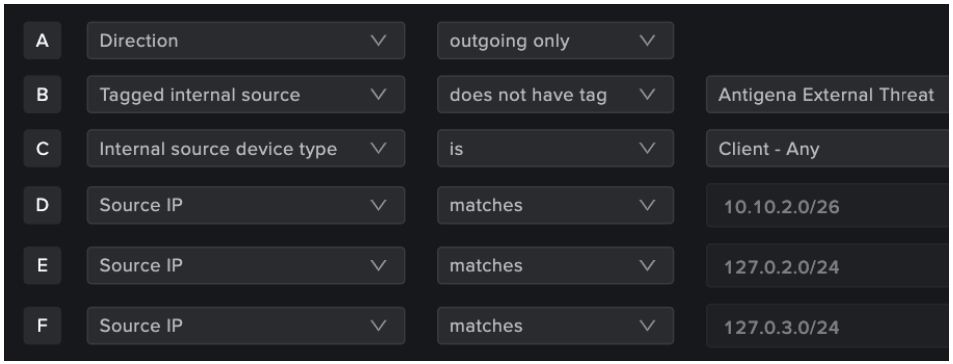


Note: Remember to write a commit message outlining that the Model has been activated.

7. Confirm that the ranges in the **Breach Logic component** are **localhost ranges**. As localhost is reserved for internal loopback, this shouldn't affect tagging on the network until changed.

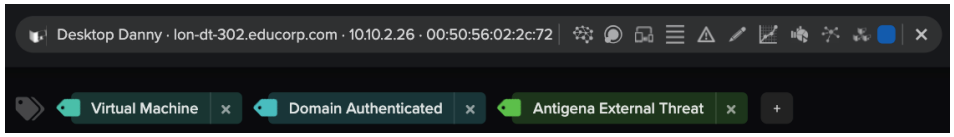


8. By changing one of the ranges in one of the **Source IP** filters to a **subnet on the network** and saving the changes, Darktrace will begin the Antigena External Threat tagging process.



The example above shows that the first localhost range has been modified to the **10.10.2.0/26** range.

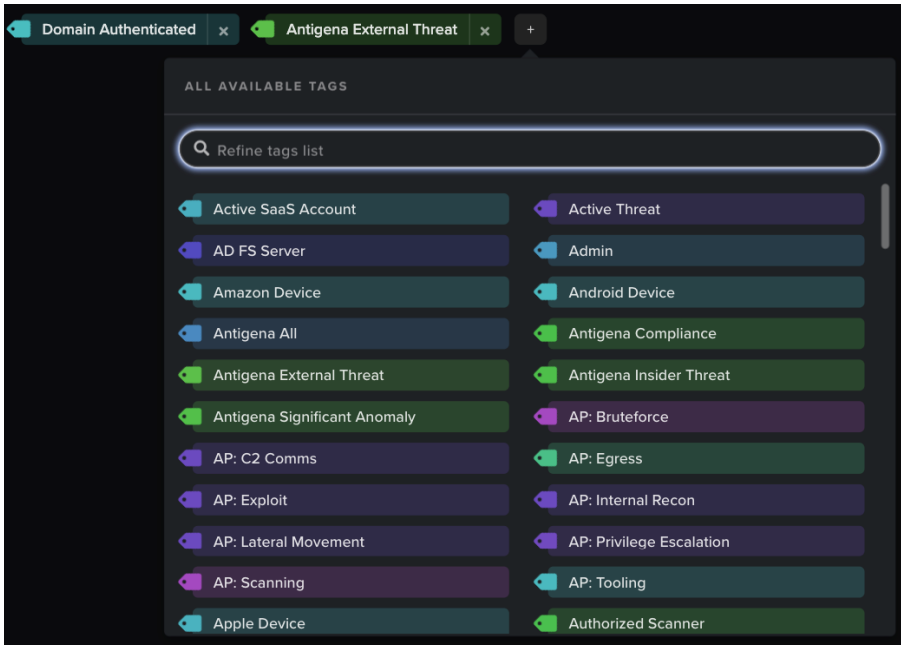
9. After a connection has been observed by a device on the established IP address range, the **Antigena External Threat tag** will be attached to that device.



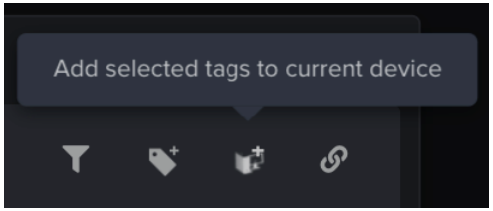
This device will now be monitored and potentially acted on by Darktrace RESPOND/Network Models looking for the Antigena External Threat tag, such as the ones in the External Threat folder.

10. **Specific devices** outside of these subnet ranges can also be monitored **individually**.

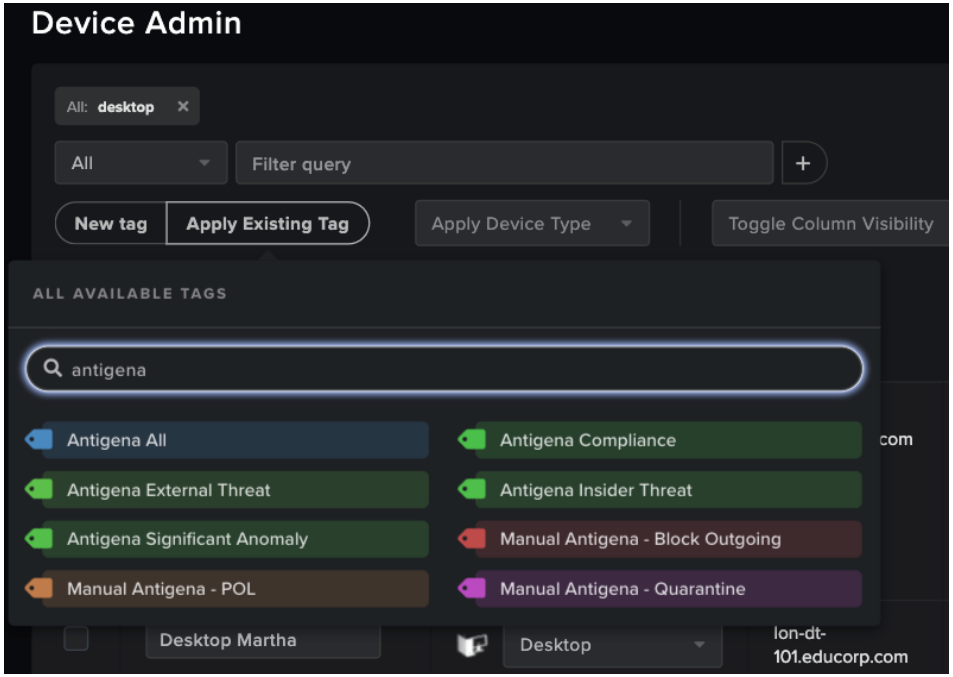
    a. With a device populated within the Omnisearch bar, click the **plus (+) button** to apply a tag from a **drop-down menu** of all available tags.



    b. Again, with the Omnisearch bar populated with a specified device, open the **Tags Manager**. From here, **select a tag** and then click the **Add selected tags to current device** button.



11. It is also possible to attach tags individually or in bulk using the **Device Admin** page. Use the **search bar** to filter the devices displayed in the table, select the **Apply Existing Tag** button and then **choose the tag** to be affixed to the devices.

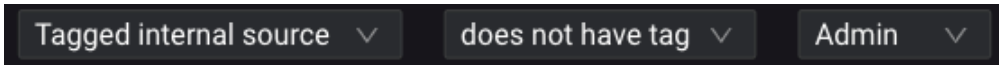


It is possible to select **individual devices** by clicking the **tick boxes** in the appropriate row, or apply a tag in bulk to **all devices** displayed on the page by clicking the tick box **at the top of the tick box column**. The rows of devices which are tagged in this way temporarily inherit the color of the tag.

Exempting Devices

Continue your learning with our dedicated video 14. Excluding Devices

When initially configuring Darktrace RESPOND, or after reviewing the resulting breaches and actions, you may wish to remove key devices from Darktrace RESPOND/Network monitoring.



A common example is that members of the IT Security team often perform different sets of activity from regular network users and are therefore more likely breach Darktrace models. For instance, they could carry out port scans as part of network health and compliance checking. Exempting their devices can have a significant impact on reducing model breaches and actions.

Here are some ways you can accomplish this:

- By making sure the devices do not have any Antigena tags on them. You may have to edit the automatic tagging Models to exempt devices with the **Admin tag** on them by applying an additional filter in the Breach Logic Components.
- Making sure such administrator devices are tagged with the correct Threat Visualizer tags can help in the first place, since this will exempt them from more standard Darktrace Environment Model Breaches which make up the basis for detection in many Darktrace RESPOND/Network Models.
- Furthering on from the second point, tuning and optimizing the Darktrace Environment in general, especially for IT team devices, will have a positive knock on effect on the accuracy of your Darktrace RESPOND enabled deployment.

Applying Tags Test

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

DARKTRACE
Cyber Engineer Certification

1. What is the purpose of tagging for Darktrace RESPOND?

- [ ] To define Darktrace RESPOND's monitoring scope
- [ ] To define the device's alert level
- [ ] To define what time actions are taken

2. What is NOT a benefit of Automatic Tagging?

- [ ] Learning exceptions are automatically added
- [ ] New devices are automatically tagged
- [ ] It is more efficient than manual tagging

3. What effect does the color of a tag have?

- [ ] Bright colors represent compliance tags
- [ ] Dark colors represent more critical tags
- [ ] The color has no specific meaning

4. Deleting a tag will also automatically untag all devices sharing the tag.

- [ ] True
- [ ] False

5. Which icon allows you to add selected tags to current device?



- [ ]
- [ ]
- [ ]

6. Which option CANNOT be used to tag devices?

- [ ] Darktrace RESPOND Actions
- [ ] Tags Manager
- [ ] Device Admin

Clear All Answers

8. RESPOND/Network Quick Set-up

The process to select which devices are eligible, define any activity-based overrides, and to set the timed schedule, make up the main stages of the Darktrace RESPOND/Network Quick Setup Process. This chapter focuses on the various options available through Darktrace RESPOND/Network Quick Setup, including the manual, autonomous, and partially autonomous set-ups; scheduling; and running tests.

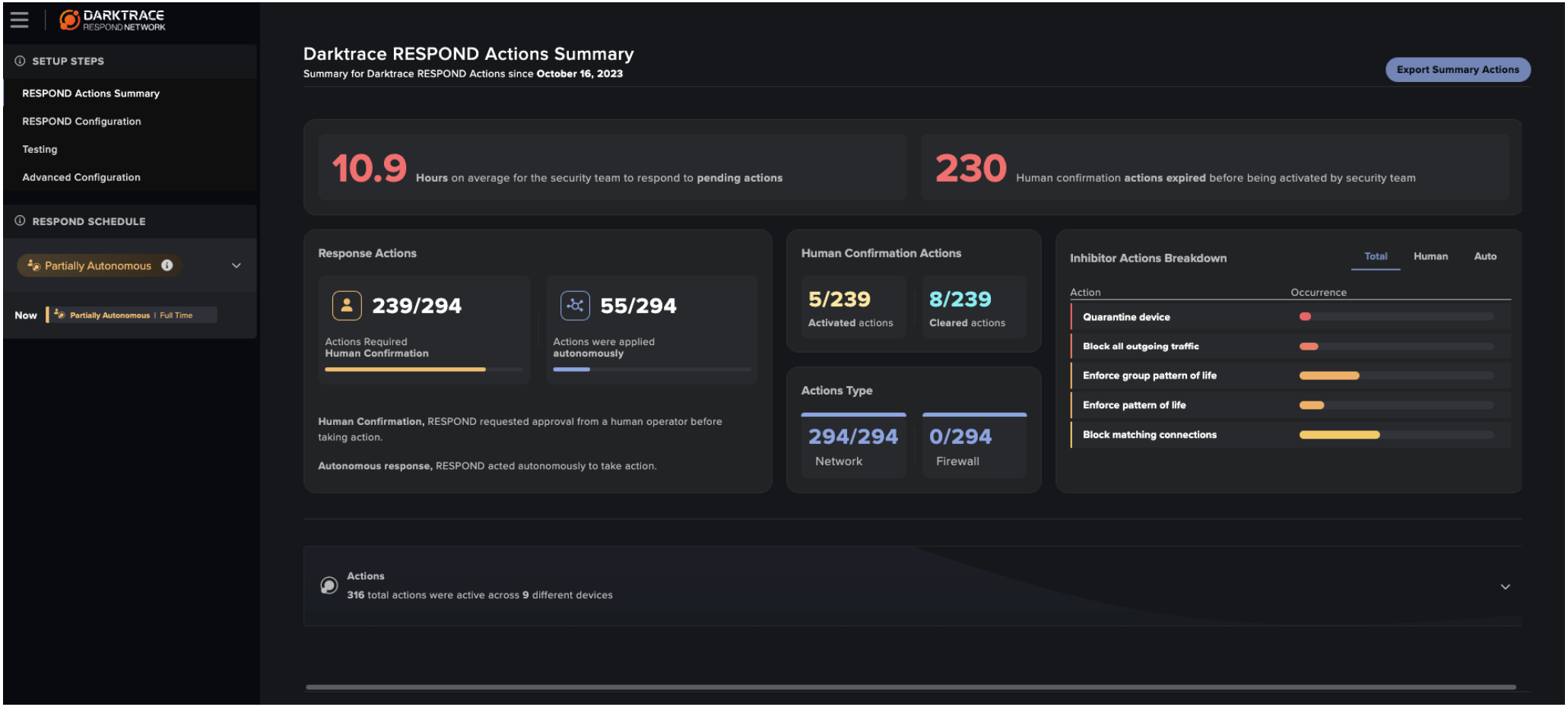
RESPOND Setup

Darktrace RESPOND/Network has a **Quick Setup page** that offers one-click setup, advanced configuration, and testing. The process to select which devices are eligible, define any activity-based overrides, and to set the timed schedule, make up the main stages of the Darktrace RESPOND/Network Quick Setup Process.

1. To access these options to configure RESPOND, navigate to the Main Menu in the Threat Visualizer interface.

2. Clicking on **Darktrace RESPOND/Network Quick Setup** will open a new browser window with the full setup options.

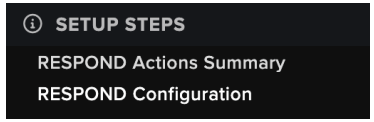
3. The new browser window will display the **Darktrace RESPOND Actions Summary**.

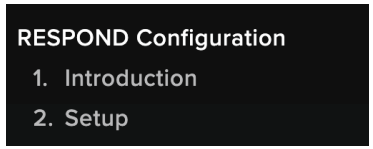


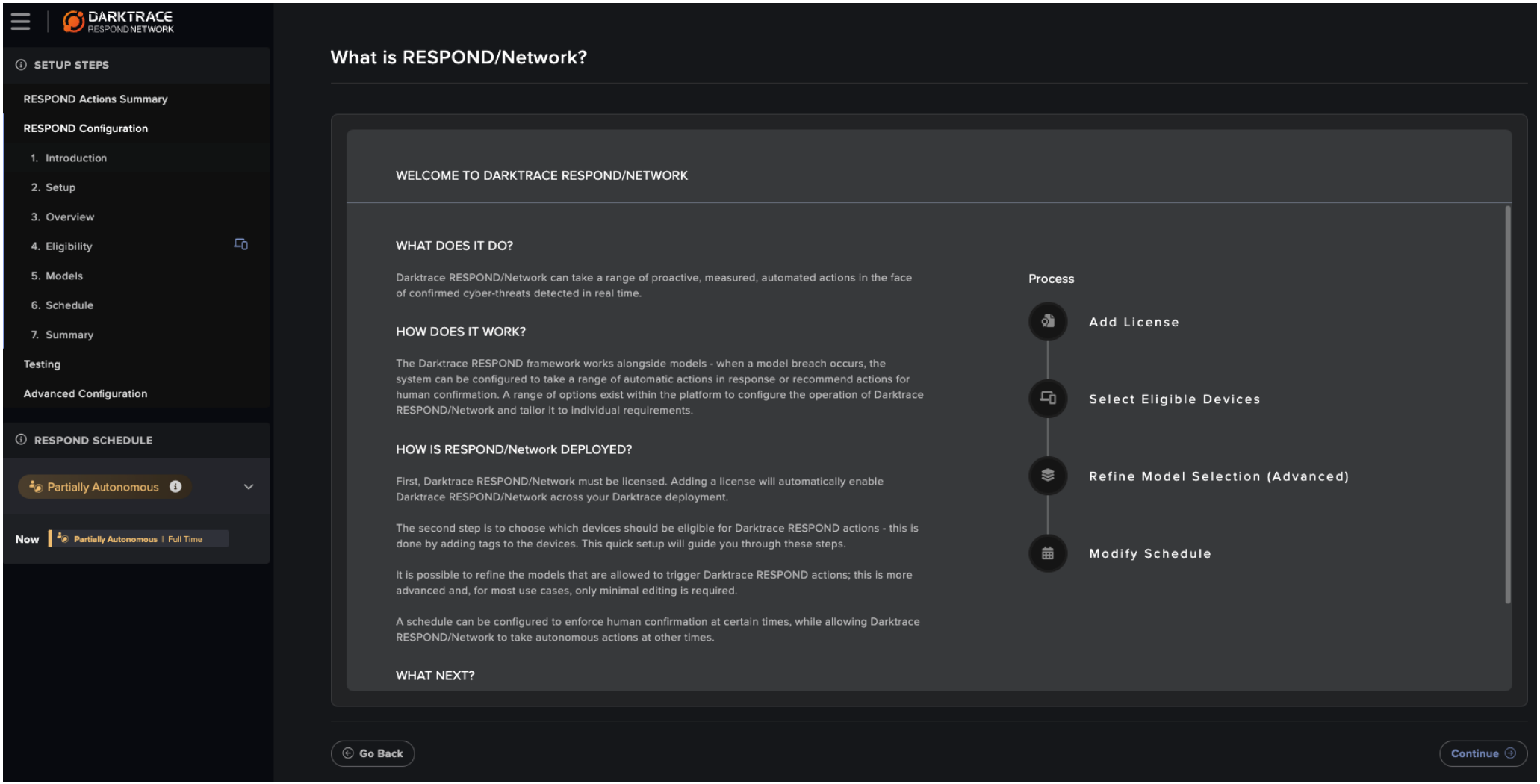
4. To setup RESPOND/Network select **RESPOND Configuration** from the options on the left panel.

5. The first page has a **description of RESPOND/Network** and an introduction to deploying RESPOND. It is advisable to read this to become familiar with RESPOND/Network, how it is deployed, and its capabilities.

6. To continue to the setup click on **2. Setup** in the left panel or on the **Continue** button at the bottom right of the main window.



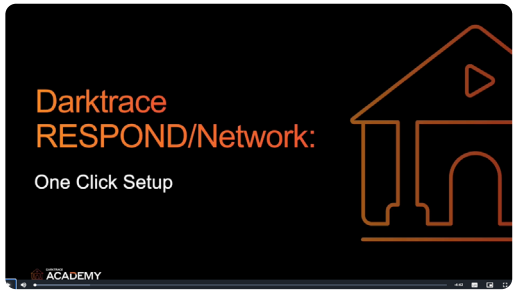




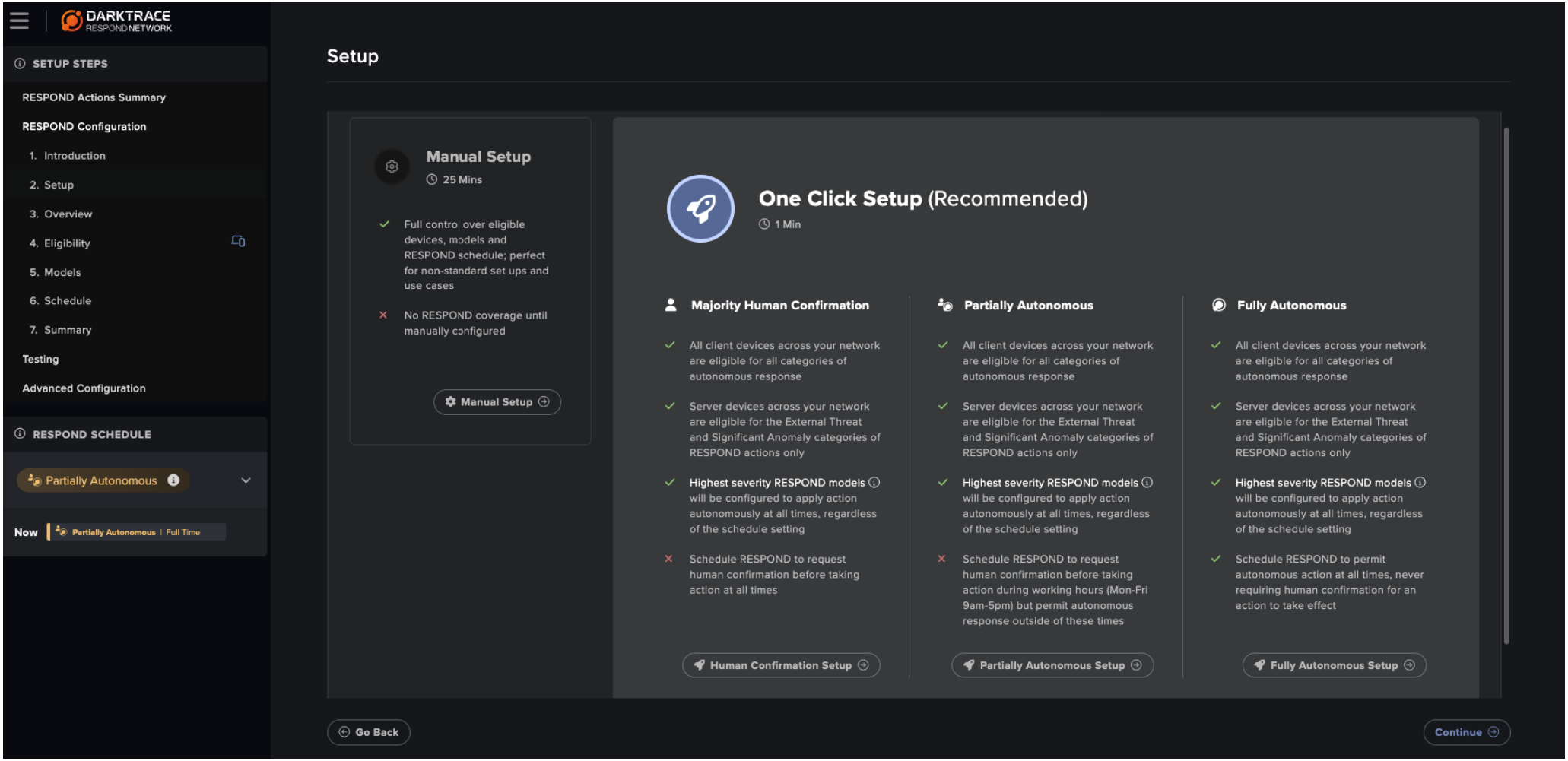
One Click Setup

One Click Setup options provide the option to quickly and easily apply Darktrace-recommended defaults to your Darktrace RESPOND/Network environment. This is the recommended setup, although there is a manual setup option available too, that will be covered later in this chapter.

One Click Setup options are graded from least to most autonomous.



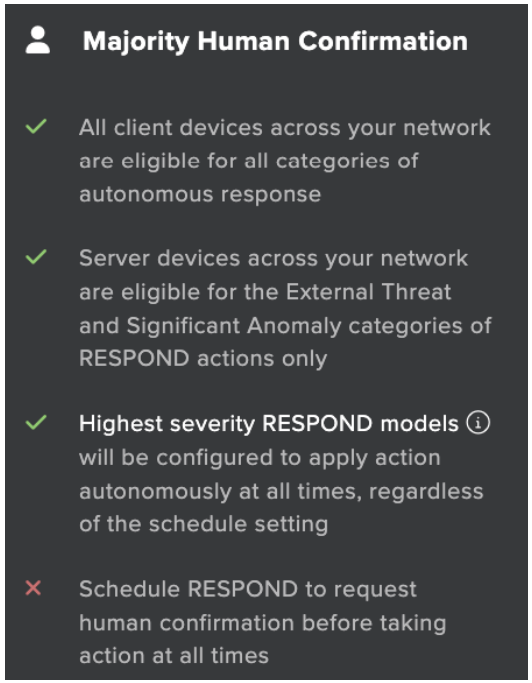
Continue your learning with our dedicated video
15. One Click Setup



Human Confirmation Setup

Human Confirmation is the **most passive One Click Setup option** - in this mode, Darktrace RESPOND/Network will request human confirmation before acting in all but the most severe detections.

Note: As this mode is scheduled around business operating hours, international organizations may wish to localize autonomous actions to outside the business hours of each location.



1. For **Human Confirmation Setup** simply click on the button at the bottom of the first panel.

2. You will see information about the Human Confirmation Setup settings. It is advisable to **carefully review** this and ensure this is the appropriate setup you require.

3. To put this into action, simply press **Apply**. Once done, you will see a summary of the settings.

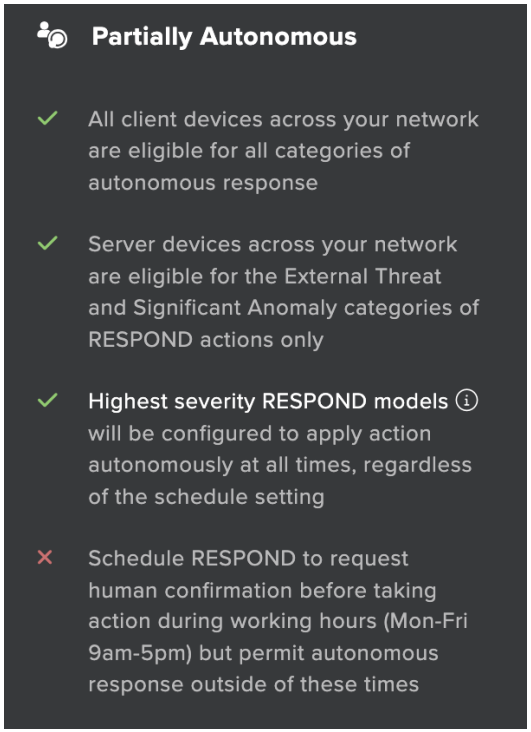
Partially Autonomous Setup

In **Partially Autonomous** operating mode, Darktrace RESPOND/Network will take action autonomously only outside of business hours, when there may be no one to approve pending actions.

The Partially Autonomous option offers a **middle ground between passive and autonomous deployment**.

In this case, Darktrace RESPOND/Network is only permitted to act autonomously outside business hours.

Within business hours, Darktrace RESPOND must request human confirmation for all but the most severe activity.



1. For **Partially Autonomous Setup** select the button at the bottom of the middle pane.

2. As with Human Confirmation Setup you will see information about the settings. You can **review** these to ensure they are appropriate for your needs.

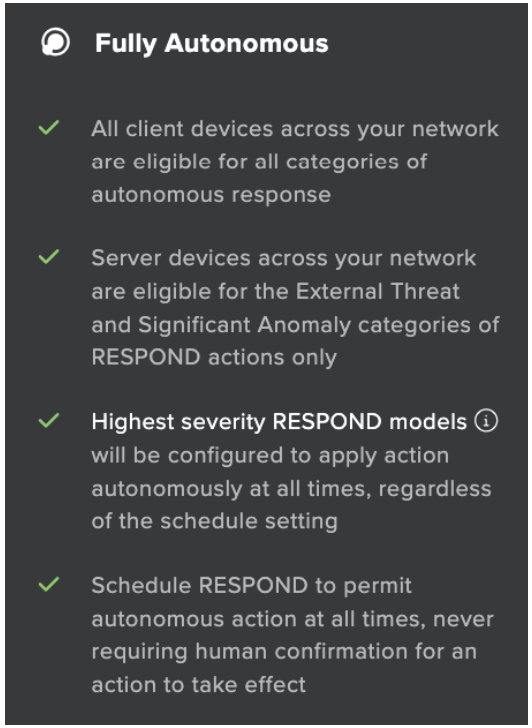
3. To put this into action, simply press **Apply**. Once done, you will see a summary of the settings.

Fully Autonomous Setup

In **Fully Autonomous** mode, Darktrace RESPOND/Network will take action autonomously in all cases, requiring no human oversight.

Fully autonomous mode is the end goal of Darktrace RESPOND deployments; reaching a fully autonomous state where it can take action whenever unusual or concerning behavior is detected, without the need for human oversight.

This mode lends itself to a **minimal-interaction workflow**, however, users may infrequently modify actions through the Darktrace Threat Visualizer interface, API, or Darktrace Mobile App.

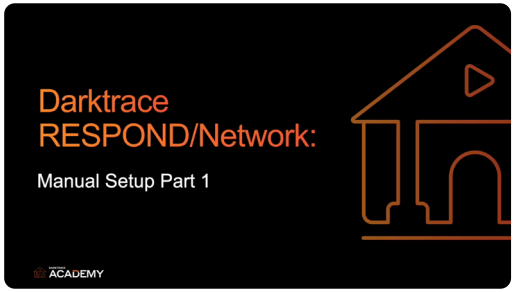


1. For **Fully Autonomous Setup** select this option, on the right panel.

2. Information specific to the setting will be displayed, which should be **reviewed** before continuing.

3. To put this into action, simply press **Apply**. Once done, you will see a summary of the settings.

Manual Setup

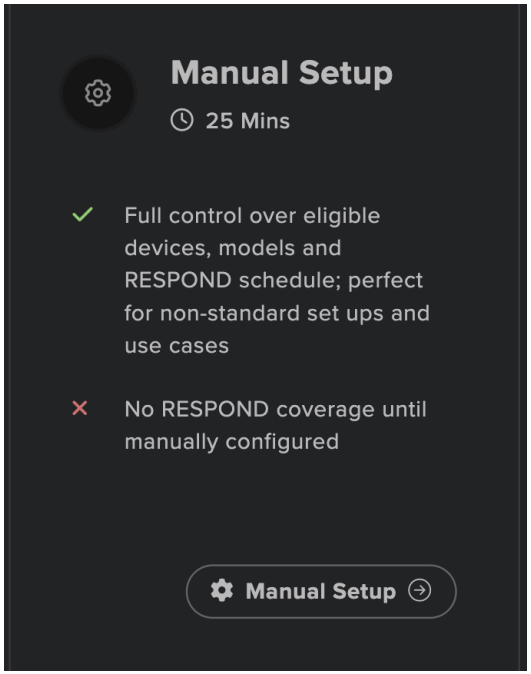


Continue your learning with our dedicated video 16. Manual Setup - Part 1

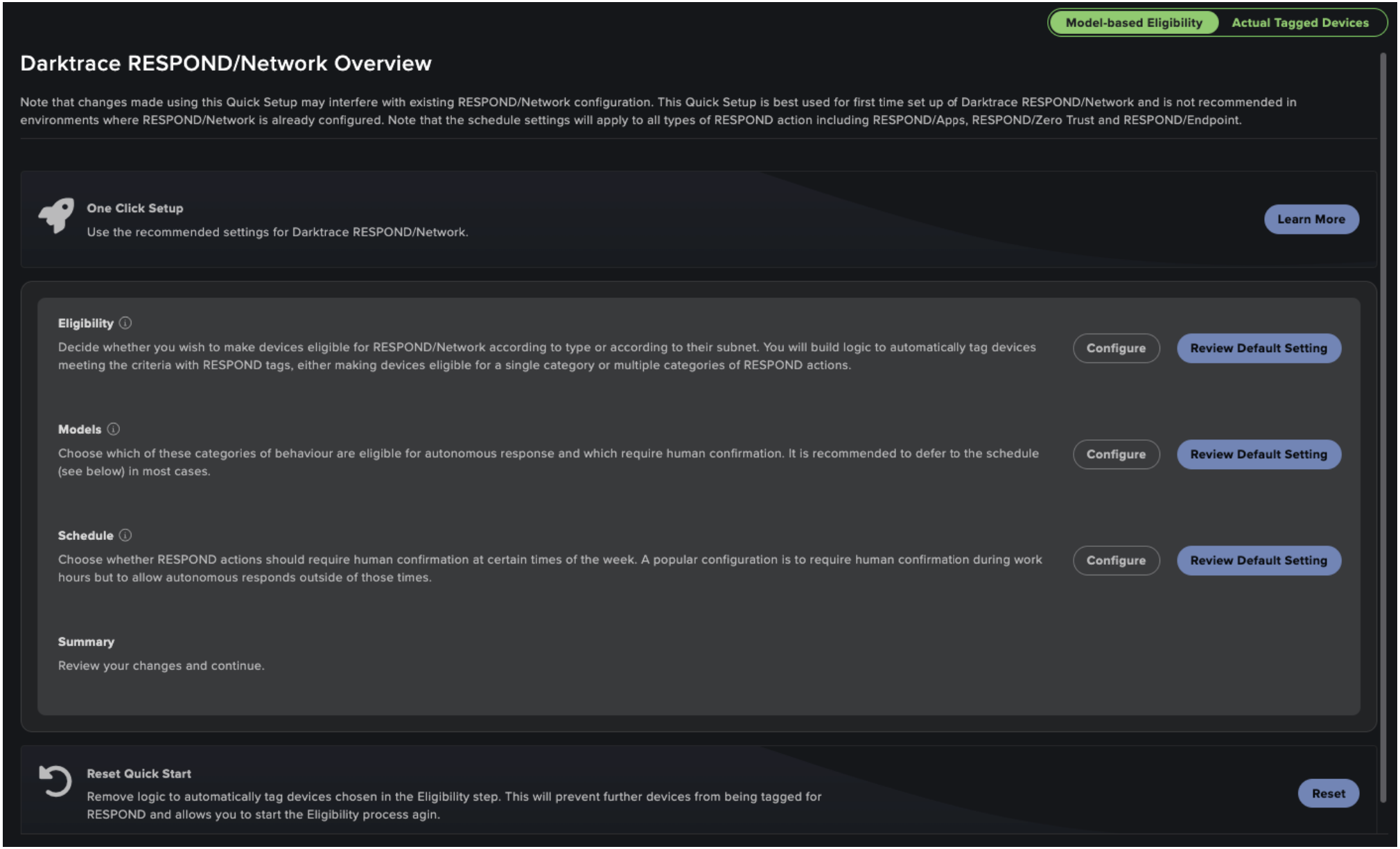
Manual Configuration offers a step-by-step process to define device eligibility, model state, and a weekly schedule for Darktrace RESPOND/Network.

This option is advanced and is suitable for experienced operators who want more granular configuration options.

To setup manually, select the **Manual Setup** option on the Setup page.
You will then be taken through the steps to configure Darktrace RESPOND/Network manually.



After selecting Manual Configuration setup, you will see the three stages of configuration: **Elibility**, **Models**, and **Schedule**.



8. RESPOND/Network Quick Setup Configurations

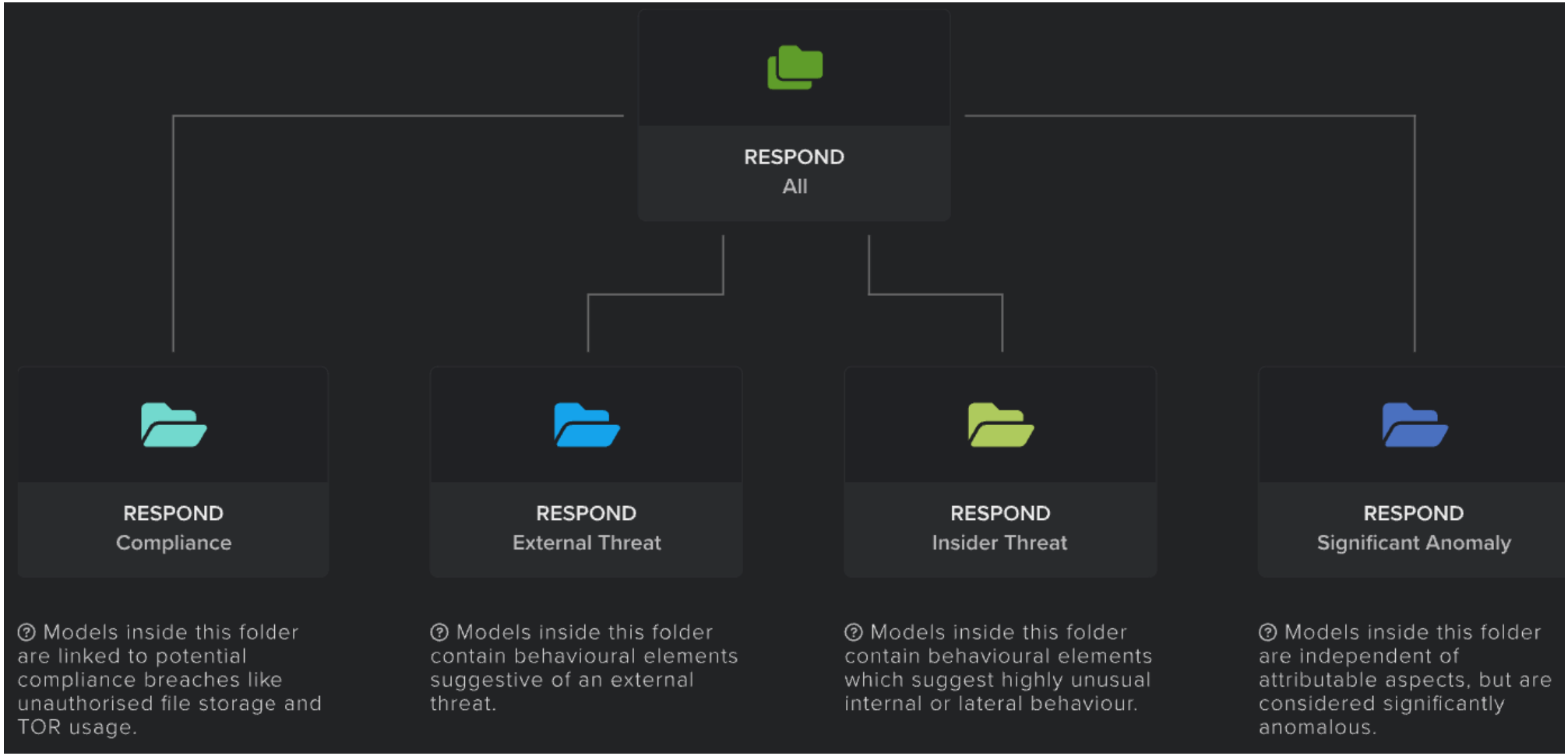
On this page you can review the deafult settings and can start to **configure** each of these options independently, but it is recommended to follow the setup process steps linearly.

Configure

Clicking on **Review Default Setting** displays a pop-up with information about the impact of the default settings for that option, which can be then applied. Selecting the **Configure** option will start the configuration process for the selected option. The configuration options are quite different depending on whether **Eligibility**, **Models**, or **Schedule** is selected.

Review Default Setting

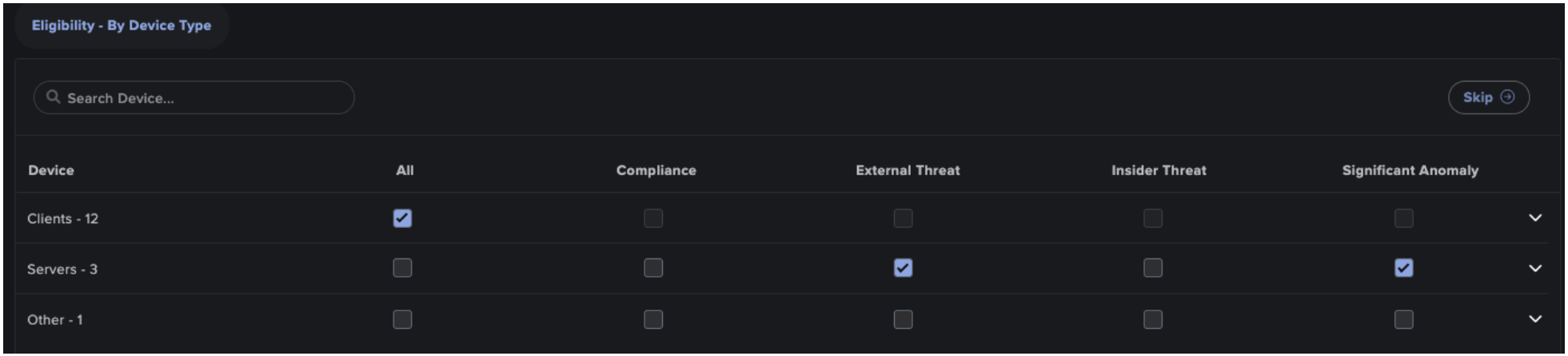
1. **Eligibility** will show the **five RESPOND categories** that models can be part of. When a device performs activity which meets the criteria of a model in one of these categories, Darktrace RESPOND will check if it has a tag which corresponds to the activity category before proceeding to take an action. This is tag-based eligibility.



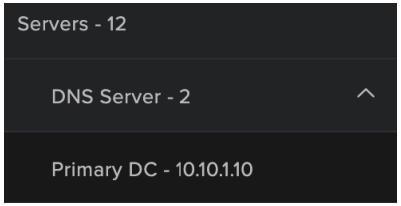
Devices can be eligible for **any combination of categories**. If they are eligible for all categories, they will be placed in Antigena All / RESPOND All.

a. A device can be **opted in** by receiving a category specific tag, such as **Antigena External Threat**, or the general **Antigena All tag** which counts for all categories.

b. Selecting **Continue** takes you to the next stage without changing the default settings. A **table** is then displayed.



c. The first column contains **all network devices**, grouped into **subnet** or **type**. Clicking on the devices or subnets will expand to show associated sevices or subnets.



d. The other five columns represt the **tag options** that can be selected. Click the empty square to opt a row into the specific tag. If the **All** tag is selected, it is not necessary to select individual activity types.

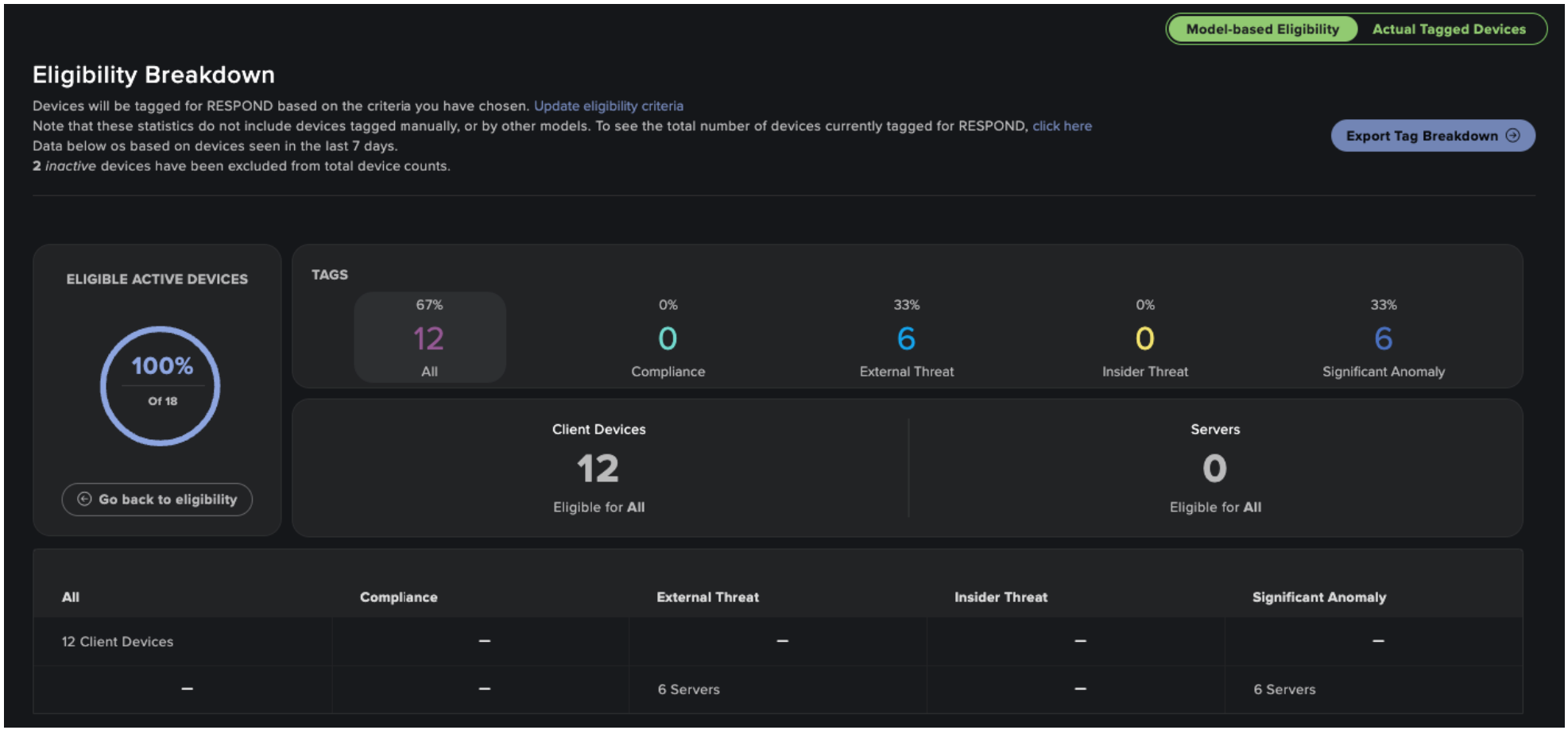
An **empty box** in the column of a tag indicates that no devices within the group are eligible for the given tag.

A **checkmark** in the column of a tag indicates that the whole row is now eligible for that category of Darktrace RESPOND/Network response.

A **box with a line** in the column of a tag indicates that some of the models contained within the folder are eligible, but not all. In this case, click to expand and see the subset that are operating in the given mode.

Tag eligibility can be applied at any level, although it is strongly recommended that tags are applied to **first** or **second-level categories** i.e. the subnets rather than specific devices.

e. After saving the configation eligibility, the **Eligibility Summary** is shown. The summary visualizes how devices across the network are eligible for categories of Darktrace RESPOND/Network response, including the **overall proportion** and the **client/server proportion**, based solely upon the criteria chosen in the previous step.



Note: the Eligibility Summary is the anticipated result of the criteria chosen. For devices to be tagged, Darktrace must see an outgoing or incoming connection for the device after configuration is complete. Any devices which are not observed as active will not be tagged, even if eligible for the criteria.

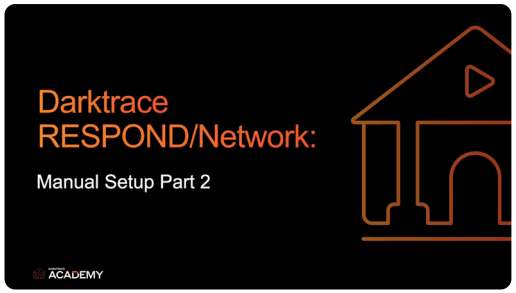
f. To view the **current state** of device eligibility, use the toggle to select **Actual Tagged Devices**.

g. A **summary** of the eligibility for all valid devices can be exported in **.csv** format.

Now devices have been made eligible for one or more high level categories of Darktrace RESPOND/Network response, the next step is to look at the **individual models within those categories** and decide when they should be able to trigger autonomous Darktrace RESPOND actions on the eligible devices.

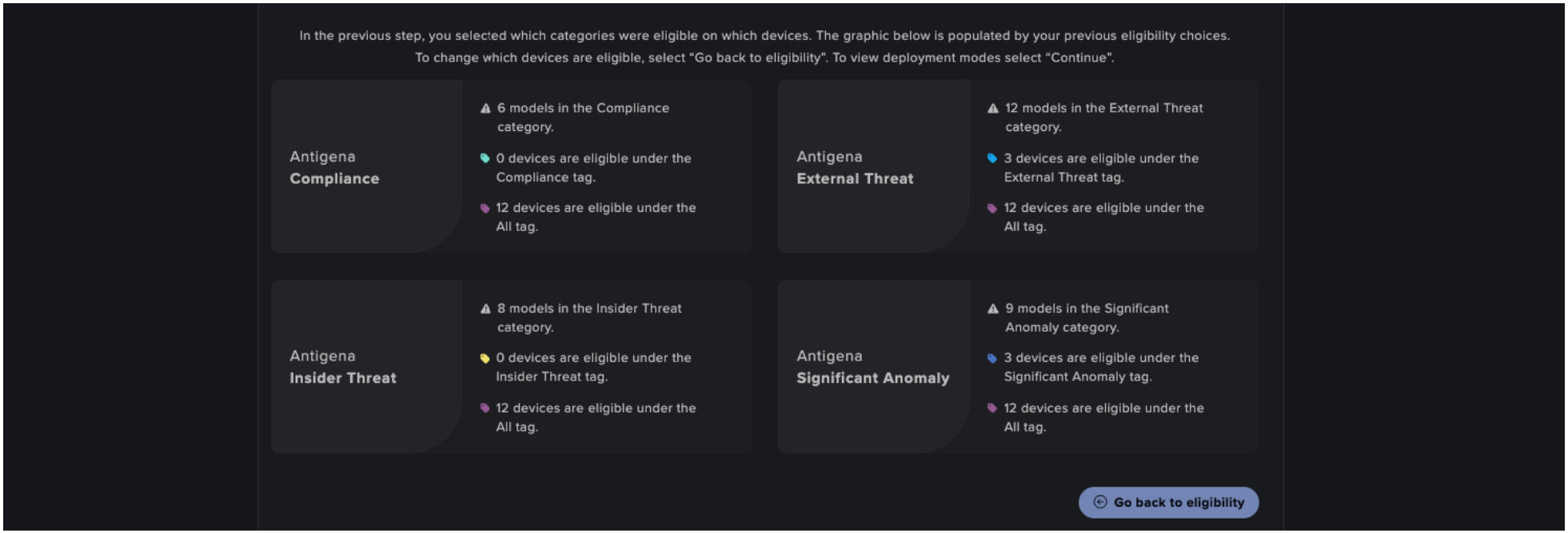
Darktrace RESPOND **models** look for specific behavior or for indicators triggered by other model breaches; the four categories are groupings of these models which describe the kind of activity they target at a high level.

RESPOND Models are split into categories that reflect the threats they target. Devices can be eligible for any category, combination of categories, or for all categories: **Antigena All**.



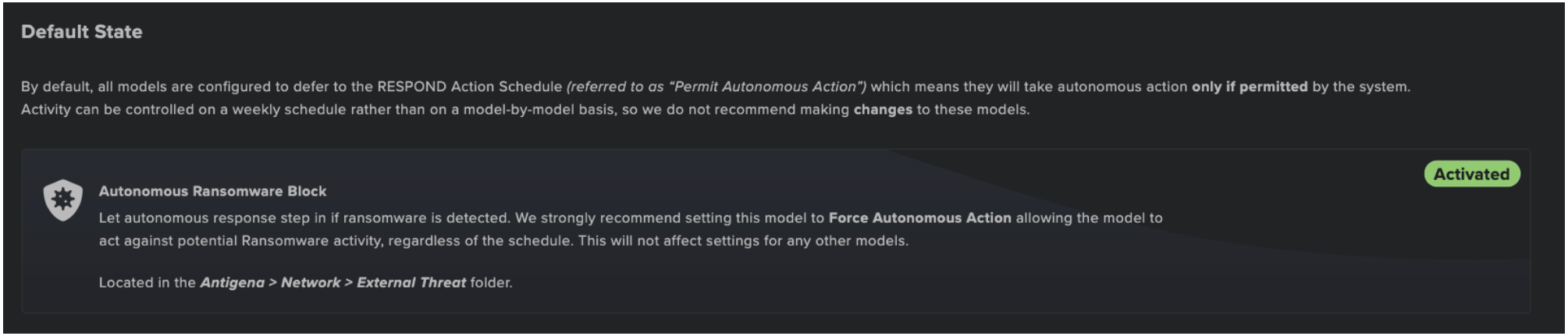
Continue your learning with our dedicated video
17. Manual Setup - Part 2

a. The first page of the models section is a **visualization** of the devices that will be affected when changes are made to models in certain categories, based upon the eligibility set in the previous stage.



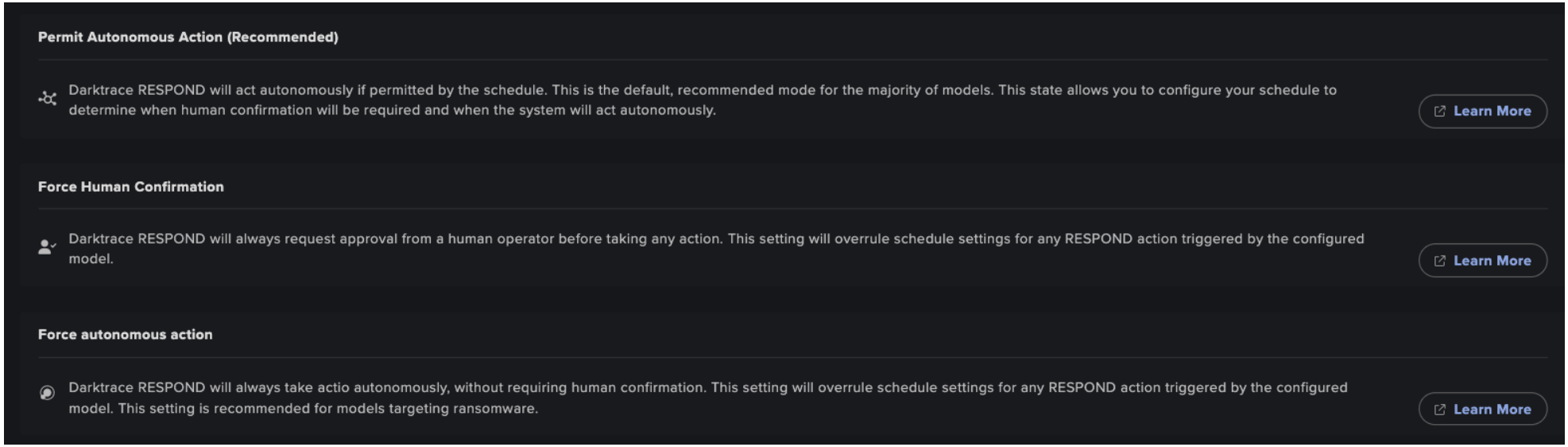
If none or too many devices are opted into a category, you can return to the previous stage by selecting **Go Back**.

2. After selecting **Continue**, the **RESPOND Model Settings** page is displayed. This offers the option to apply the Darktrace-recommended default setting, if not already applied. The deafult sets a subset of the highest severity models into a mode where they do not require human approval to take action.



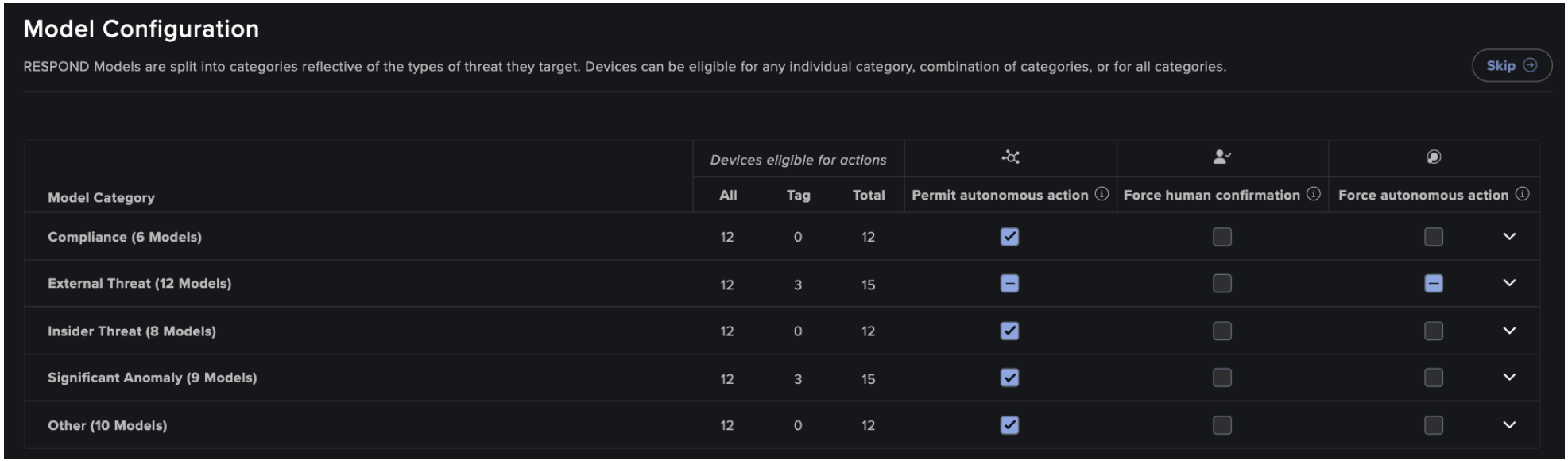
Generally, there is limited need to modify the Darktrace RESPOND/Network models beyond applying this recommendation. The remaining models can be left in their default state and instead controlled from the global, time-based schedule.

a. However, if you do wish to **set individual models** to a state where they can ignore the schedule - whether to always ask for human confirmation, or to never require it - select **Edit Models** at the bottom of the page. Selecting this, the user will be taken to a different page, which shows the **three Darktrace RESPOND model states**.

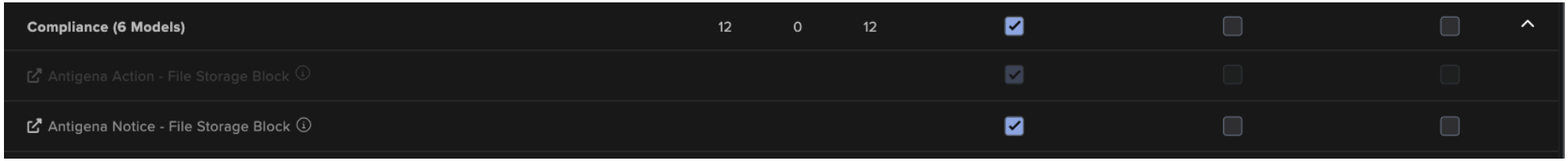


b. A table is shown depicting the **state of Darktrace RESPOND/Network models** and the devices impacted by this state.

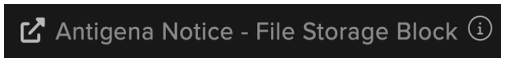
c. The first column contains **all Darktrace RESPOND/Network model**s, grouped into their parent folder. Any custom or non-default model which applies a Darktrace RESPOND action is also shown in the **Other** group for visibility.



d. Click to **expand** and show **individual models** within the folder. Models displayed in dark text are inactive and will not trigger DarktracevRESPOND action.



e. Click the icon beside the model name to **open the model editor** for the model, or hover the **information icon** beside the model name to see the description.

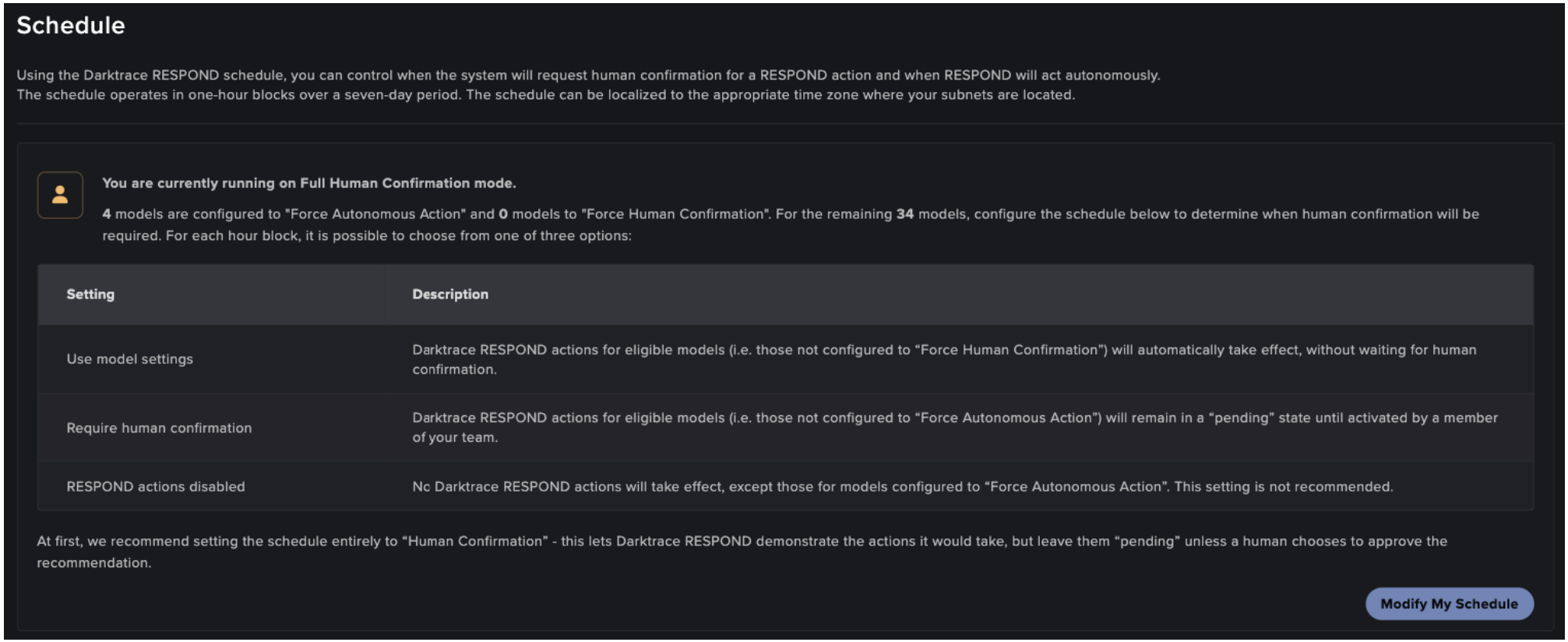


f. The next three columns show the **number of devices opted into actions** from models in that folder, based upon the eligibility criteria previously set.

g. To see the devices currently eligible with actual, applied tags, use the toggle to select **Actual Tagged Devices**.

The Darktrace RESPOND schedule is a **global timetable** which defines how autonomously Darktrace RESPOND can act at any point during the day or week. The grid represents seven days, comprised of 24 hours. Each block defines when Darktrace RESPOND will seek operator approval for actions, when it will take them automatically (unless the individual model indicates otherwise) and when it will take no action at all.

1. Once the eligibility has been set and ay changes made with the models, the next step is to create or modiofy the RESPOND schedule.

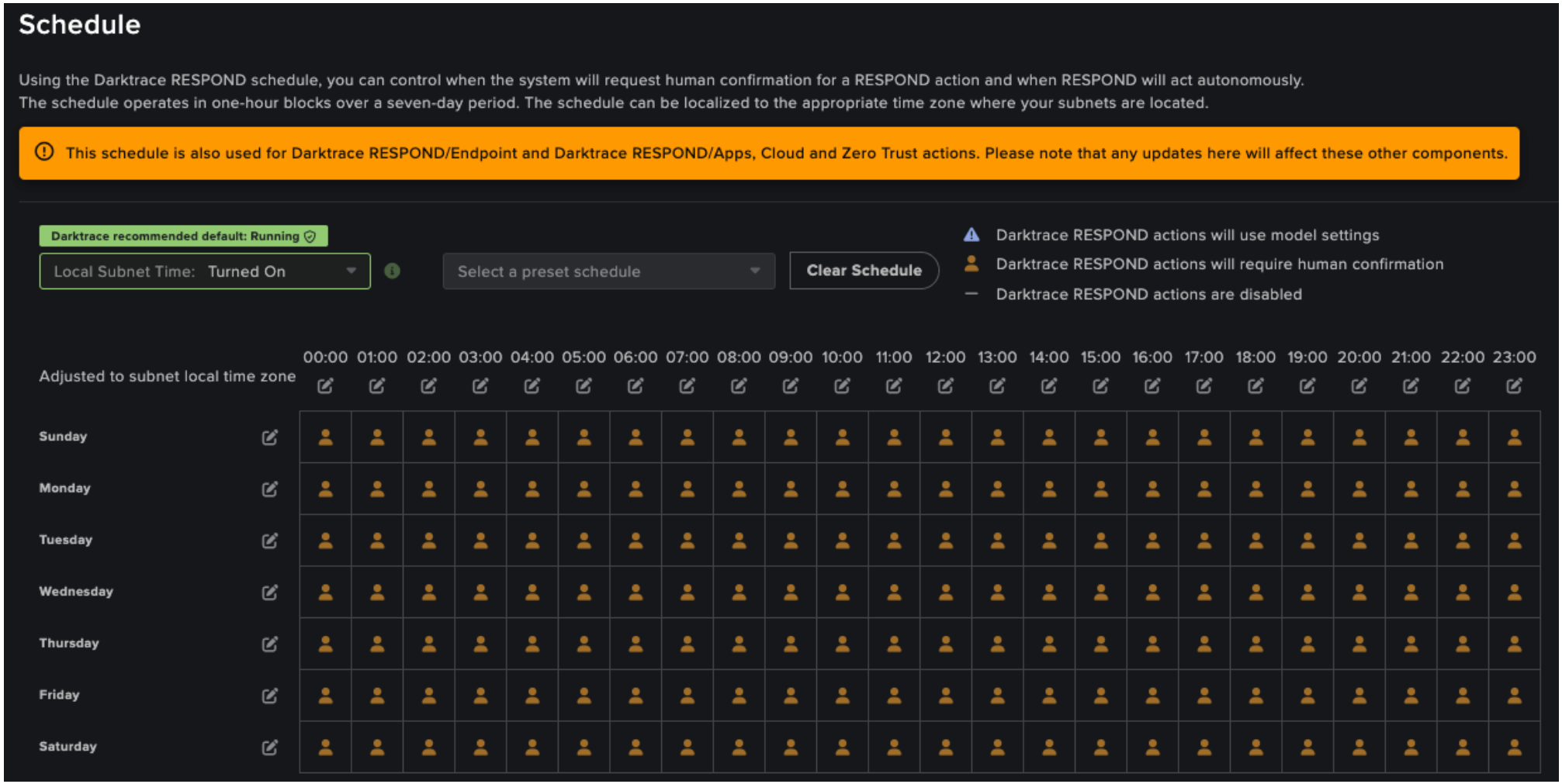


a. The schedule allows periods of time to be **allocated for autonomous actions** and other periods of time **allocated to human confirmation mode**. RESPOND is often configured to be **autonomous** outside working hours, when operators may not be available to approve pending actions.

b. The schedule operates in **one-hour blocks** over a **seven-day period**. The schedule can be **localized** to the time zone where your subnets are located.

c. It is recommended that the schedule is set to **Human Confirmation**, as this shows which actions RESPOND/Network would take. However, to modify the schedule select **Modify My Schedule**.

2. This will display a **summary of the current schedule** configuration, an explanation of these three modes, and the option to alter it if desired. Each hour of the schedule can in be in one of three states:

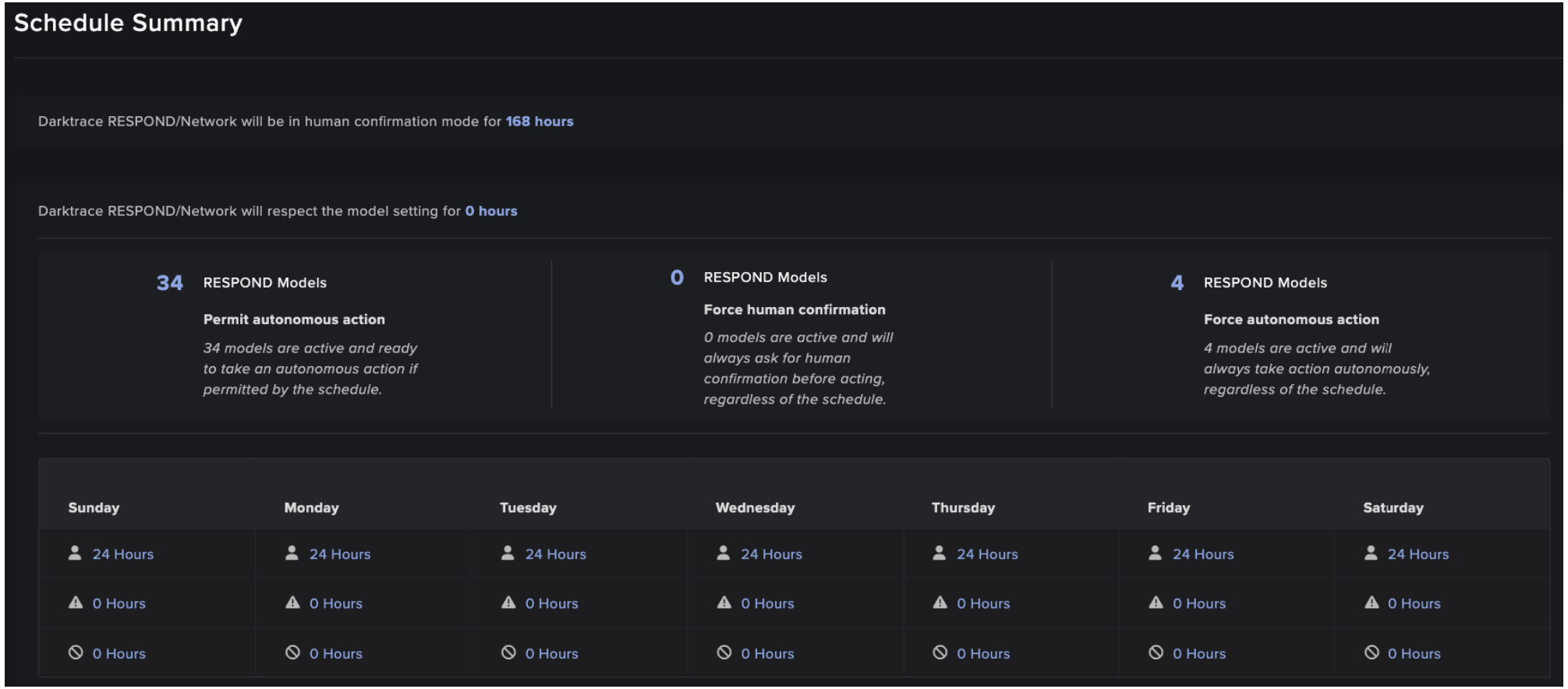


a. In **Model Settings** mode, Darktrace RESPOND will act autonomously unless explicitly forced to request confirmation.

b. In **Always Require Confirmation** mode RESPOND will ask for human approval before taking an autonomous action.

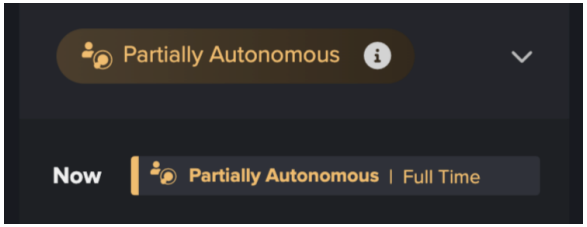
c. In **Disabled** mode, RESPOND is unable to take action except for triggered models which force autonomous actions.

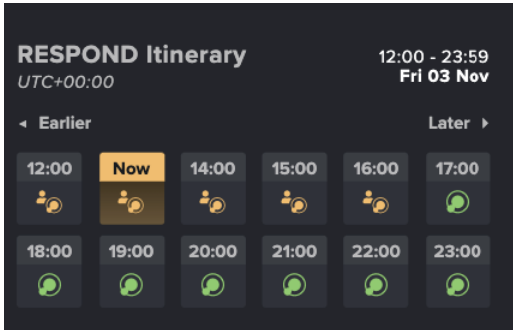
3. This final step displays a **summary of the schedule** behavior on each day of the week. The **count of models** which will obey the schedule and those which will force a specific state of autonomous action are also repeated for reference.



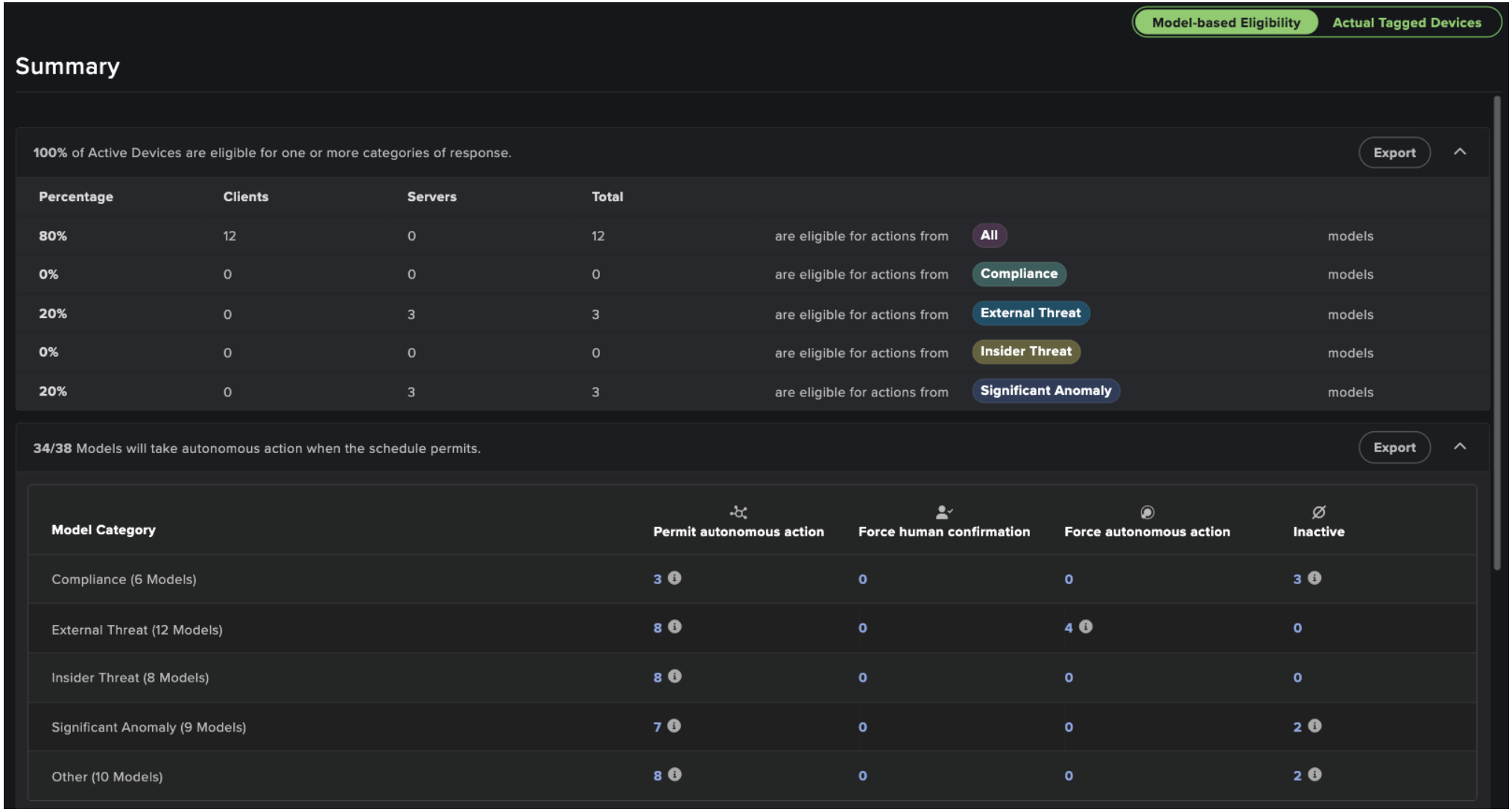
4. The changes that are made in the **RESPOND Schedule section** will be reflected in the RESPOND Schedule panel, which is shown below the **Setup Steps** menu. This shows the

   The **RESPOND Schedule** is also available on the main Threat Visualizer interface, in the **Summary Panel**.





5. Clicking **Continue** when viewing the summary of the schedule will show a summary of all the previously applied changes. If a One Click Setup was chosen, the process will skip all manual steps and navigate immediately to this page.

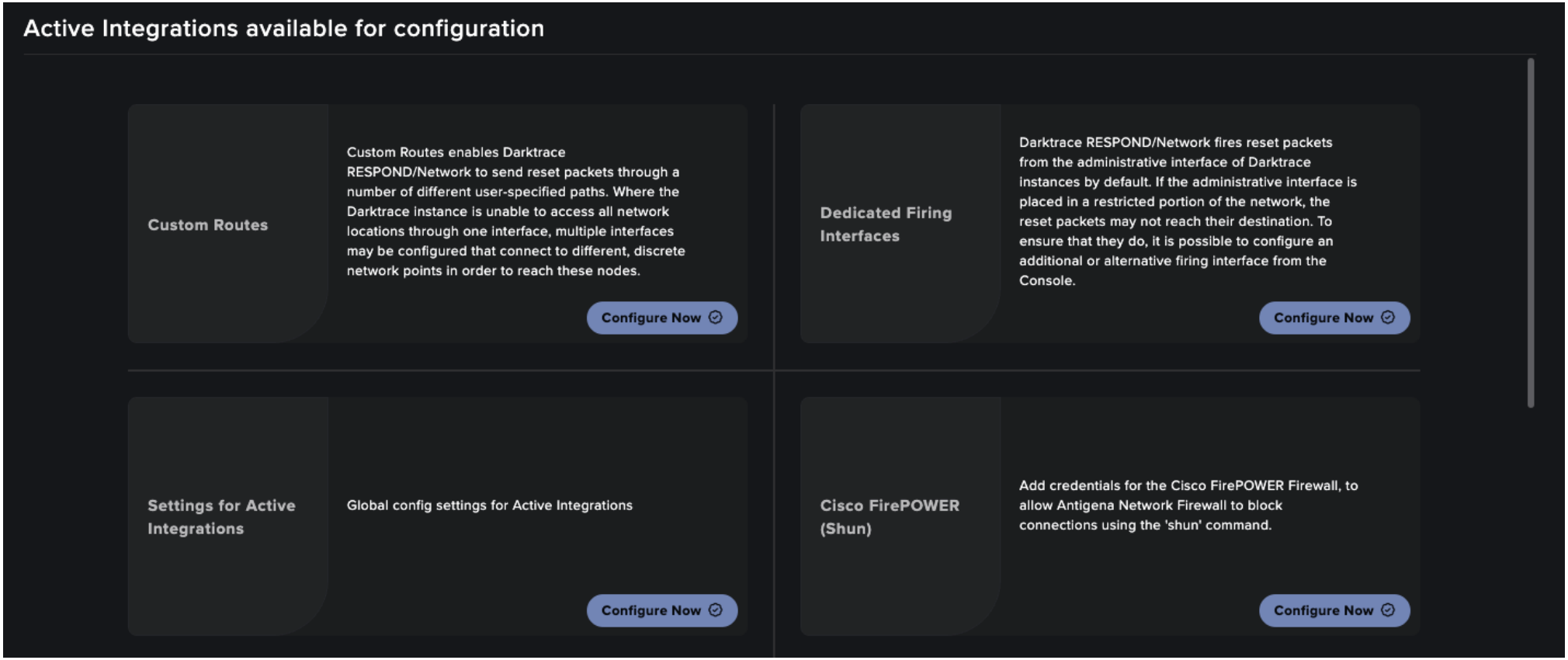


The summary describes the devices **eligible for Darktrace RESPOND/Network actions**, which activities can trigger or force autonomous Darktrace RESPOND/Network actions, and the global schedule which controls whether autonomous Darktrace RESPOND activity is permitted at all. Each section of the summary can be exported in .csv format by selecting **Export**.

Below the initial RESPOND Configuration options and the Testing section is **Advanced Configuration**. This enables the user to select and configure any active integrations. Select **Advanced Configuration** from the menu on the side.

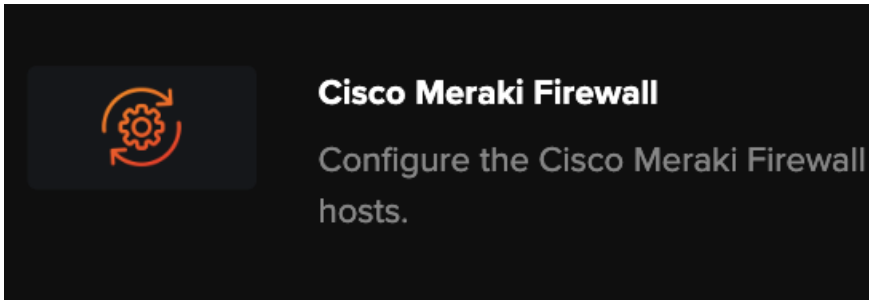
Advanced Configuration

1. Chose the integration from the options in the main panel and select **Configure Now**.



2. This will take you to the **specific integration** on the Configuration page, which was used for the original configuration.

3. **Configure** and **Add** as required.



Testing

The Spot Tester is an automated testing process for RESPOND/Network **reachability**. It works by performing a brief **quarantine action** against a nominated device in each subnet detected by Darktrace. Tests can be scheduled for multiple subnets and for multiple devices; the component will suggest recently active, low priority, client devices (where possible) as recommended targets for testing.

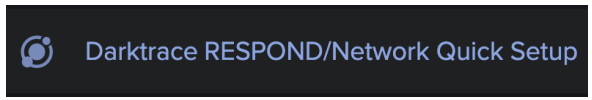
Tests can result in **failure**, **success**, **partial success** or an **inconclusive state**. For failed, inconclusive, and partial success, insights are provided into the potential reason behind the failure to perform actions successfully.

Once the spot tester has concluded, **results** can be viewed in further detail. Actions have a duration of five minutes and are performed sequentially; for longer tests, it may be necessary to schedule the test and return later to confirm the result.

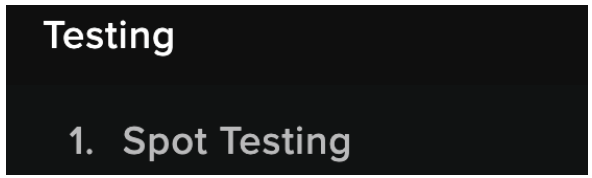
Continue your learning with our dedicated video
18. Spot Tester

Note: Reachability should be tested regularly, particularly after major network changes.

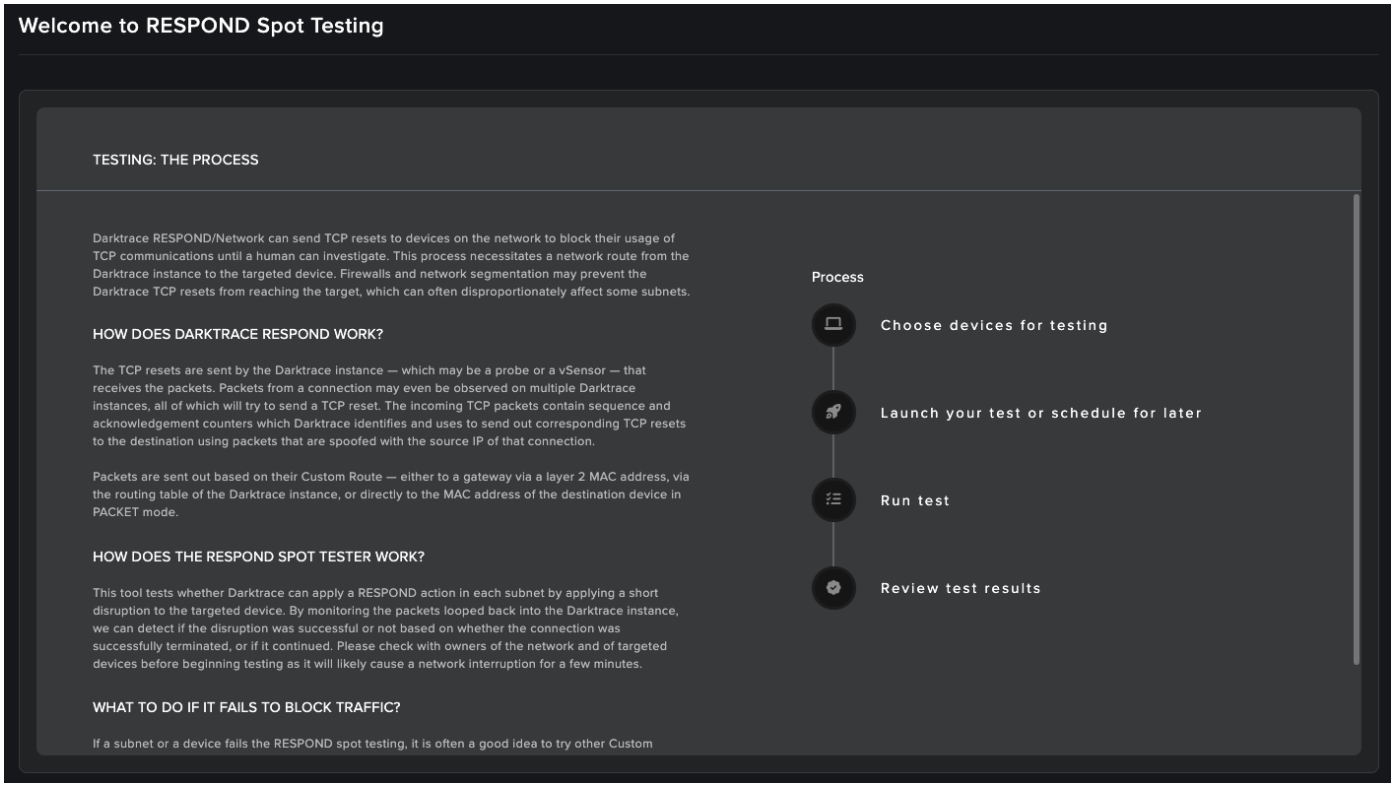
1. To access the Spot test navigate to **Darktrace RESPOND/Network Quick Setup** from the Main Menu of the Threat Visualizer.



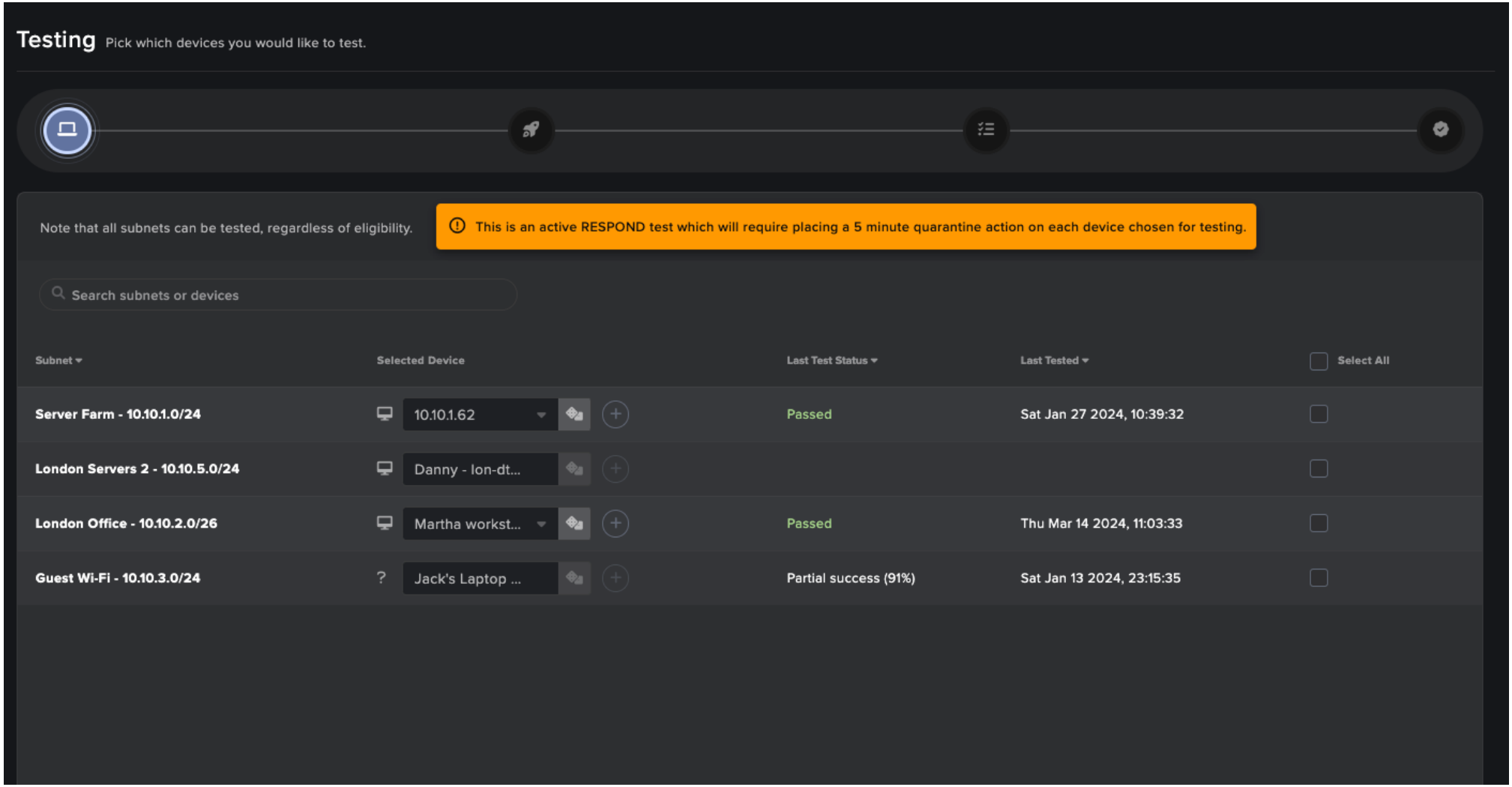
2. Select the **Spot Testing** option from the menu on the left.



3. Click to **continue**.

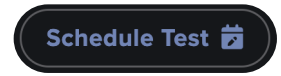


4. Suggested devices are **pre-populated** but can be changed by selecting an alternative from the dropdown, or clicking the dice icon to generate another suggested device.

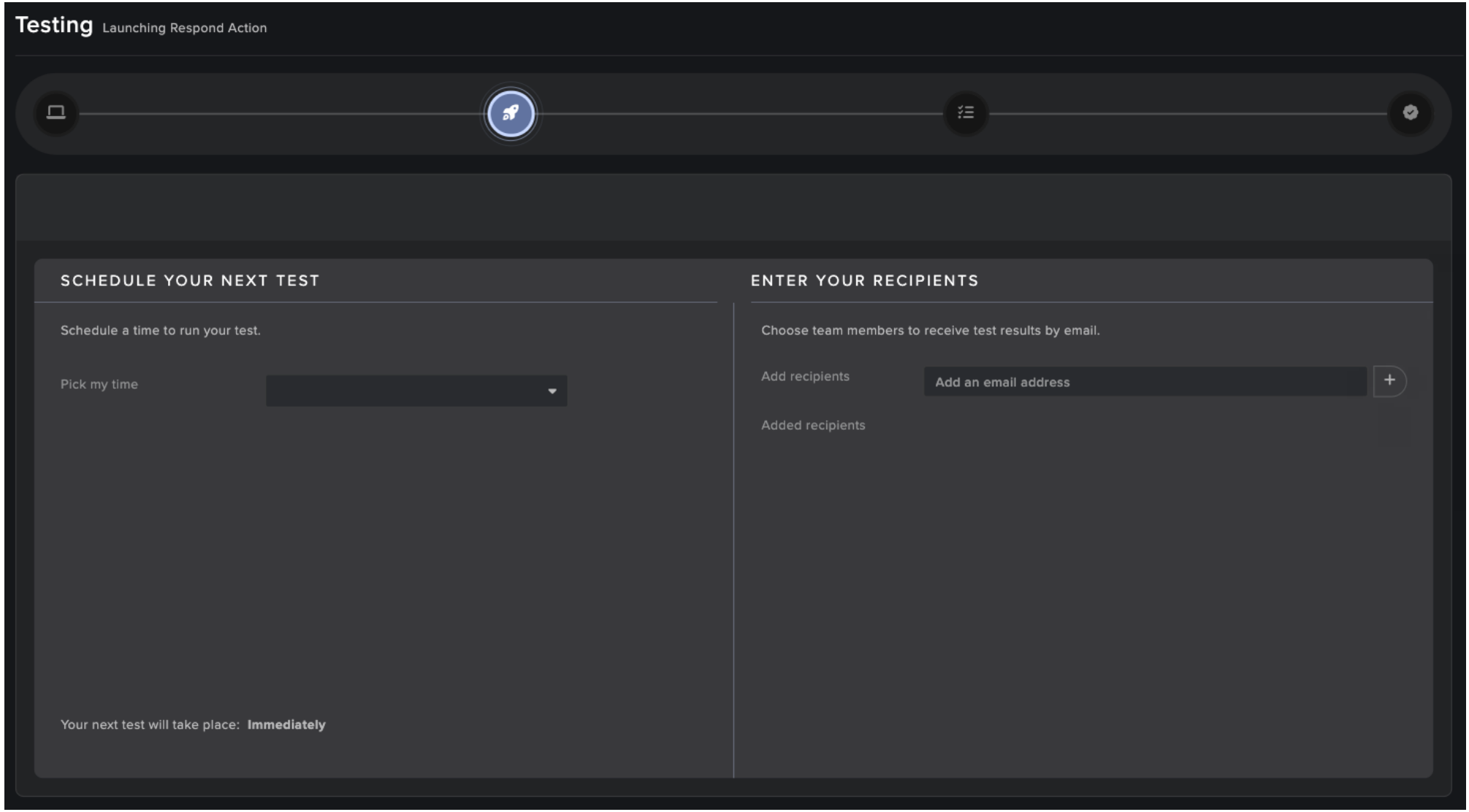


5. To **add an additional device** for testing, click the plus icon. To **remove a device**, click the minus icon.

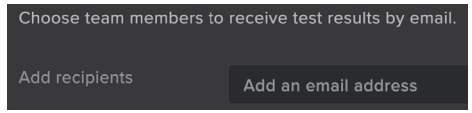
6. Select recently active, low priority, client devices (where possible) as **recommended targets**. Once selected click on Schedule Test.



7. The RESPOND/Network spot test can be optionally **scheduled for a future time**. If left blank, the test will be run immediately. A large delay between choosing devices and the scheduled running of the test is not recommended, as devices active at the time of creation may not be active at the scheduled time.



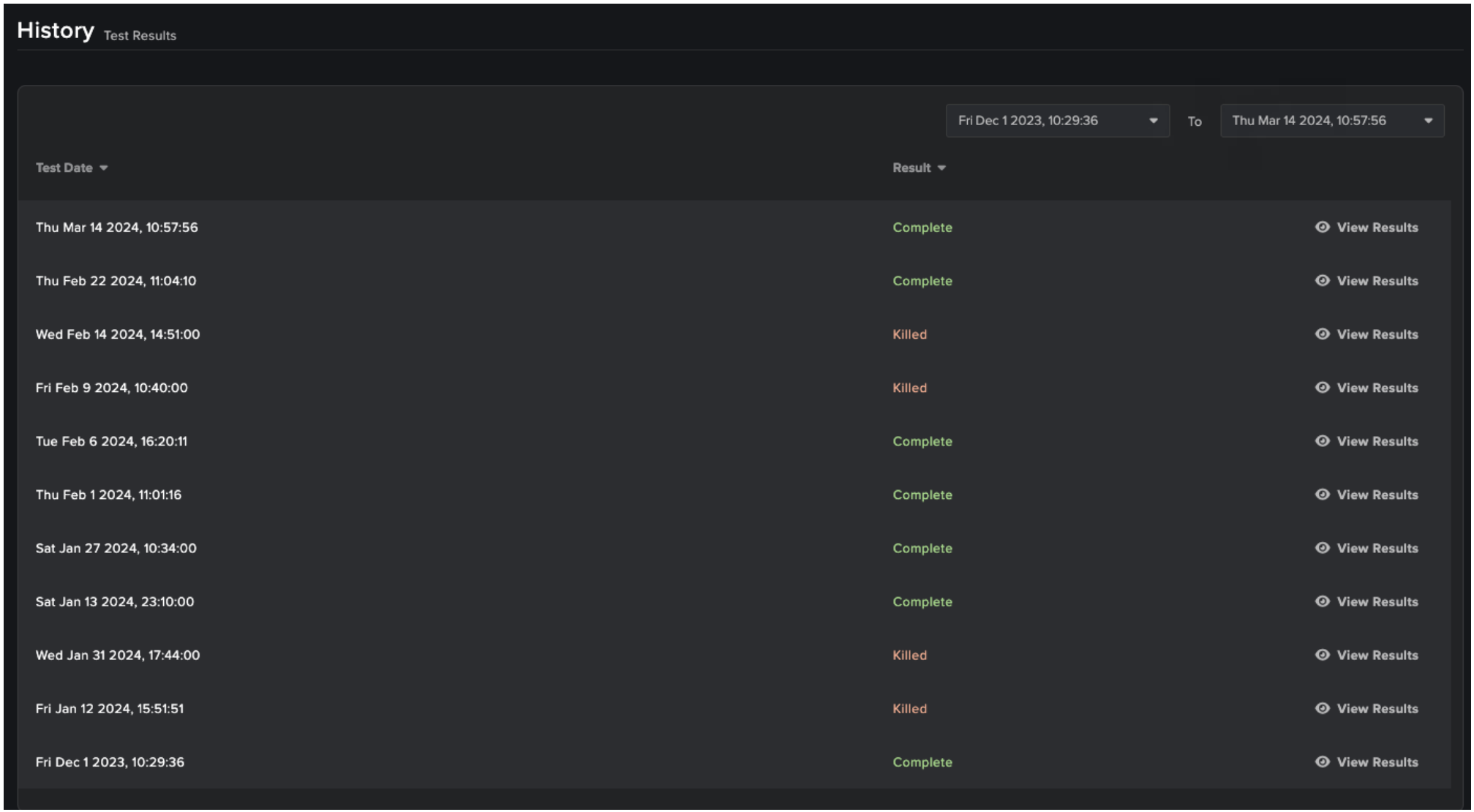
8. An output of the test results can be **emailed** to specified recipients in .csv format on completion (requires "Email" Workflow Integration).



9. Click **Launch Action For All Selected Devices** to proceed. A reminder dialog will appear, confirming you are happy to take action against the nominated devices. Click Yes, Happy to Continue to run the test.

10. On confirmation, Darktrace RESPOND/Network will now proceed to **take quarantine actions** against all nominated devices.

11. On completion, the test will proceed to the **Testing History** page.



RESPOND/Network Summary

This detailed summary dashboard gives you insights into how Darktrace RESPOND is performing in your environment. Users can see key KPIs of how your human security team is making use of Darktrace RESPOND and also a detailed breakdown of what RESPOND actions are taking place in your environment.

It also shows summary data on Darktrace RESPOND eligibility across your devices, showing what type of actions these devices would be eligible for. This all helps give you a really clear understanding of how Darktrace RESPOND is helping you and your security team keep your organization safe.

To access this summary, click on **Darktrace RESPOND/Network Quick Setup** from the main menu on the Threat Visualizer.

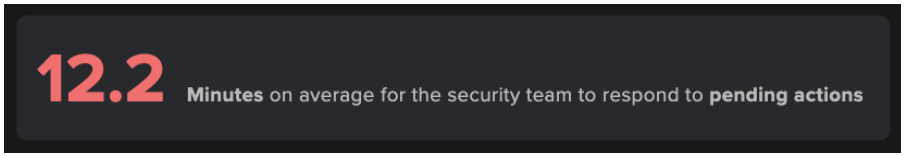
Darktrace RESPOND Actions Summary

1. The first page displayed will show a **Darktrace RESPOND Actions Summary.**

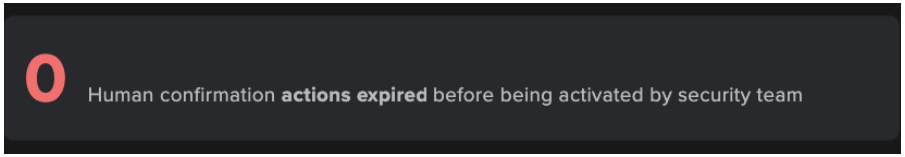
2. This summary page can be exported as a CSV file by using the **Export Summary Actions** button on the top right-hand side of the page.

3. The top row information will provide data on the time your security team takes to respond to Darktrace RESPOND/Network actions.

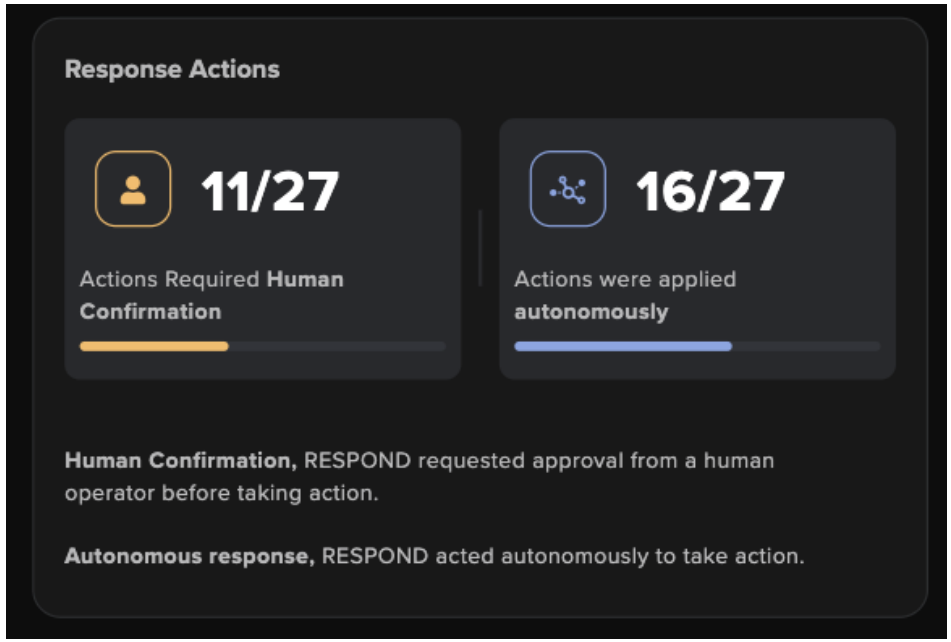
   a. The first information box on the top left-hand side will show the **human response time** to a Darktrace RESPOND/Network pending action.



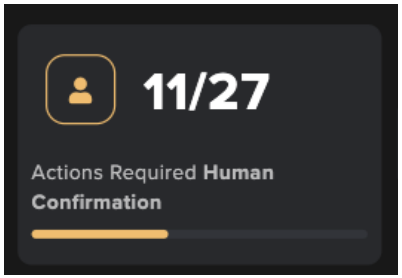
   b. The second information box, on the right-hand side, will show the number of actions **requiring an administrator's permission** which were not activated before their expiry time.



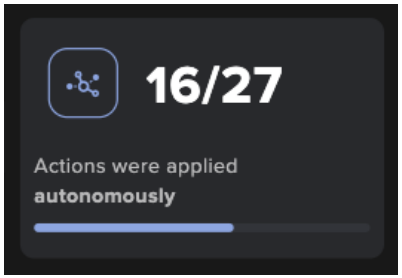
4. The **Response Actions** section will provide information on Human Confirmation and Autonomous Response modes.



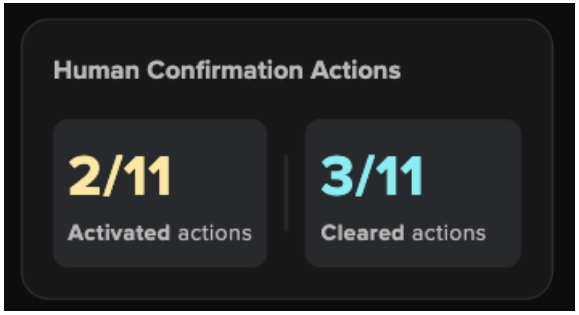
   a. The first number will indicate the number of actions which **required Human Confirmation,** out of the total of Darktrace RESPONSE/Network actions. In Human Confirmation mode, RESPOND actions will request approval from a human operator before taking action.



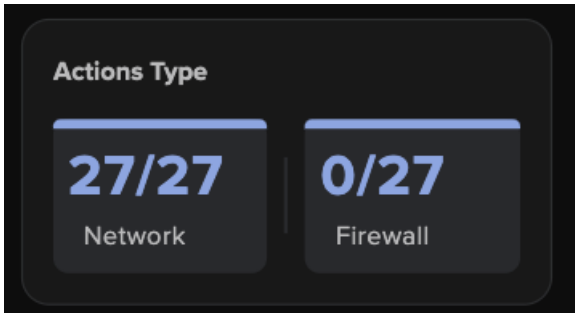
   b. The second number will indicate the number of actions which **were applied autonomously,** out of the total of Darktrace RESPONSE/Network actions. In Autonomous Response mode, RESPOND actions will act autonomously to take action.



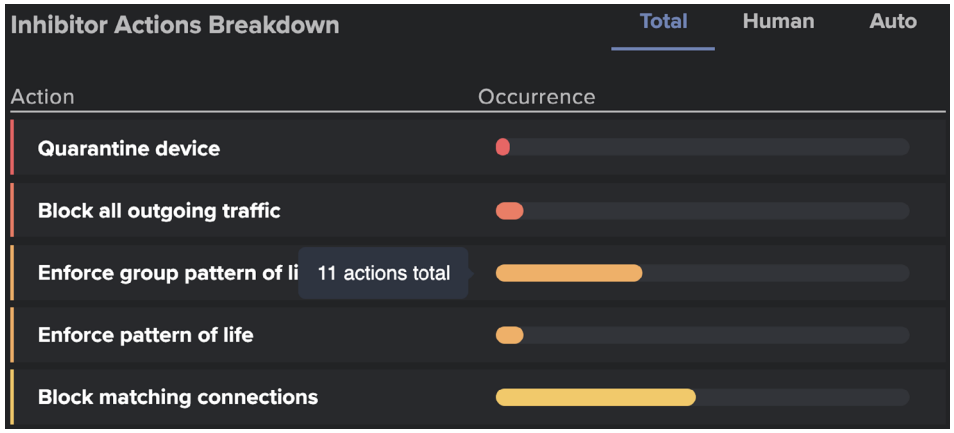
2. The **Human Confirmation Actions** section will show information on the number of manually **Activated actions** and the manually **Cleared actions**.



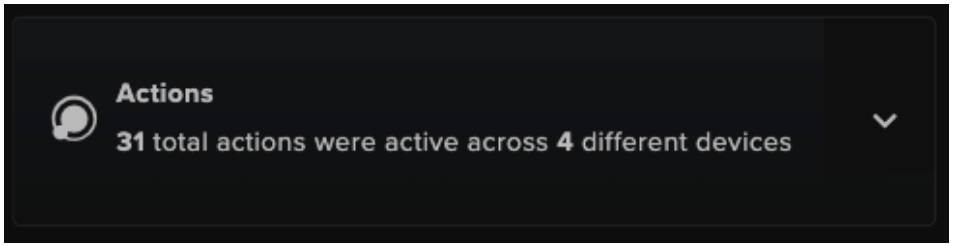
3. The **Actions Type** section will show information on the number of **Network** action and **Firewall** actions.



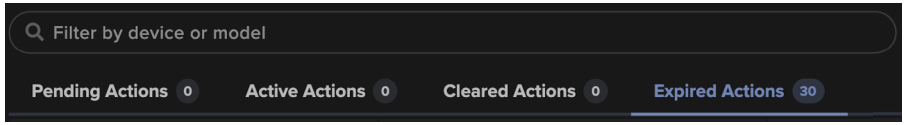
4. The **Inhibitor Actions Breakdown** section provides information on the occurrence of different Darktrace RESPOND/Network actions. **Hovering over** each occurrence bar will show the number of times this particular action has been applied.



5. Finally, the last section available on this page is the **Actions** section. Clicking on the **downward arrow** at the end of the row will open the Actions section and display further information.



a. Similar to the Darktrace RESPOND Network Actions window available from the Threat Visualizer interface, this section will display the **Pending**, **Active**, **Cleared** and **Expired Actions** tabs.



The columns for the **Actions** section are as follows:

DEVICE	This is the device that is to be actioned.
ACTION	This is the action that Darktrace RESPOND would like to take. In this case, it will block the activity that matches the offending connection.
START/ EXPIRATION	This is the time period of the action to be taken.
BLOCKED	This is to indicate if this action has attempted to prevent a connection.
TYPE (NETWORK)	This indicates whether an Darktrace RESPOND action is a network action or an endpoint action.
MODEL	This is the Darktrace RESPOND Model, or user if it's a manual Darktrace RESPOND action, that triggered the action.

b. An action relating to the executable should be awaiting consent under the **Pending Actions** panel.

c. All actions Darktrace RESPOND is currently taking on devices that are still within their expiry periods will appear in the **Active Actions** panel.

d. Any actions that are still within their set time period but have been cleared will appear in the **Cleared Actions** panel, to the right of the Active Actions panel.

e. Any expired actions will move to the **Expired Actions** panel.

2. To access the next page of Darktrace RESPOND/ Network Summary, click on **Continue** at the bottom of the page.

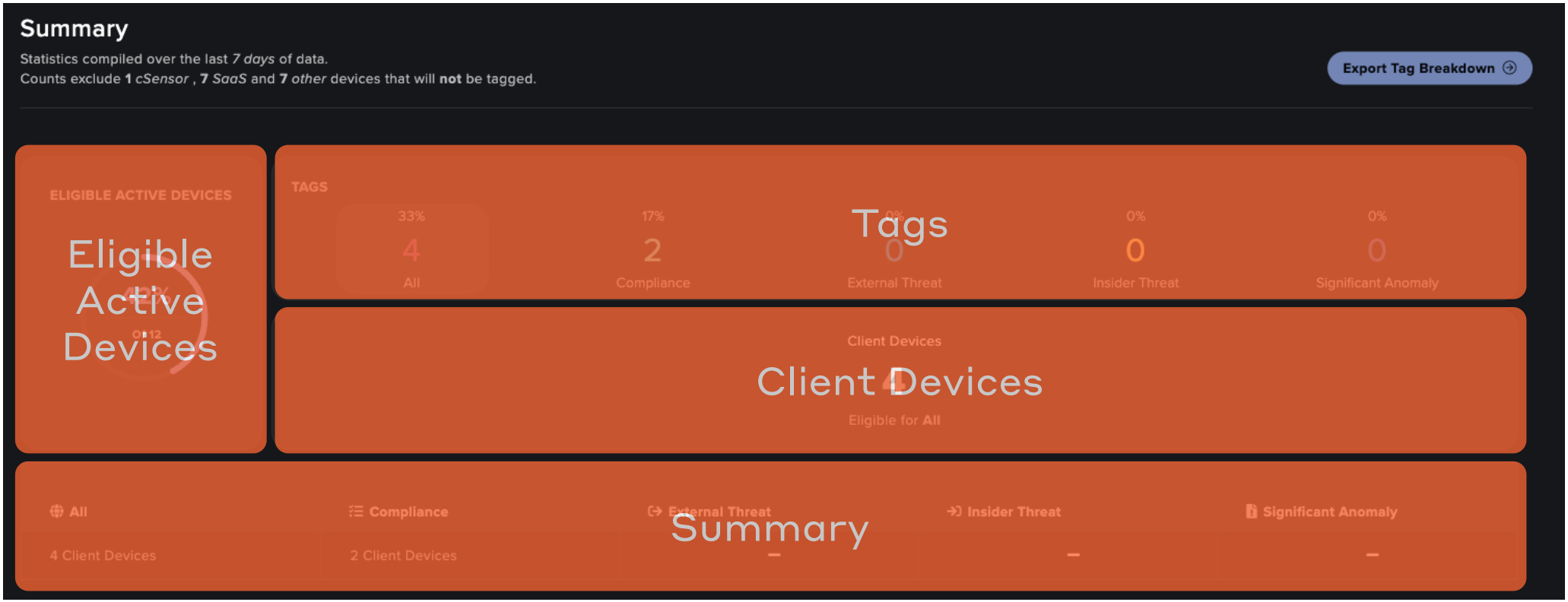
Darktrace RESPOND Tags Summary

The next page of this summary will focus on **Model-based Eligibility** and **Actual Tagged Devices**.

The **Model-based Eligibility** tab will show which devices are eligible for Darktrace RESPOND/Network tags, based on the models that they are triggering. This can be modified by your Darktrace Representative.

The **Actual Tagged Devices** tab will show the devices which have already been tagged with a Darktrace RESPOND/Network tag. W

This page will also contain summary data such as the number of **Eligible Active Devices** and how many have already been tagged, a dedicated section on **Tags** and the number of devices they each tag, the number of **Client Devices** which are eligible for the All tag and a **Summary** panel based on the different tag categories and their devices.



This page can be exported as a CSV document by clicking on the **Export Tag Breakdown** button.

Darktrace RESPOND Models Summary

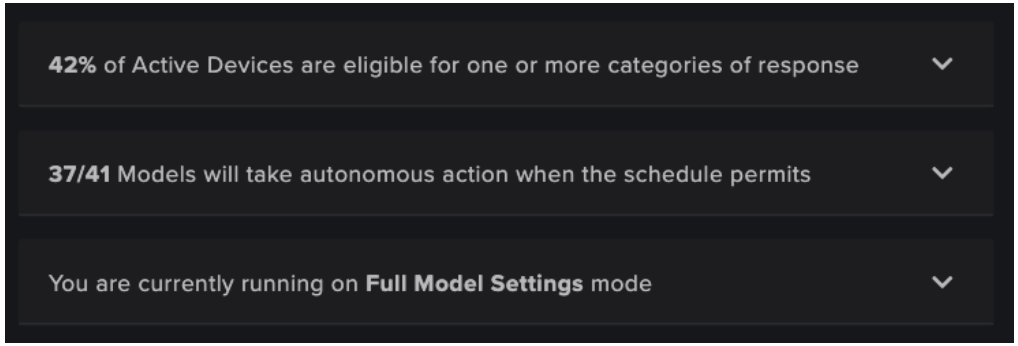
The last page will provide an overall summary of the active devices, models and settings.

The **Model-based Eligibility** tab will provide a summary for devices which are eligible for Darktrace RESPOND/Network tags, based on the models that they are triggering. This can be modified by your Darktrace Representative.

The **Actual Tagged Devices** tab will provide a summary for devices which have already been tagged with a Darktrace RESPOND/Network tag.

This summary is divided into three different tabs: **Active Devices**, **Models** and **Settings mode**.

The information on each of these tabs can be separately exported using the **Export** buttons at the end of each row.



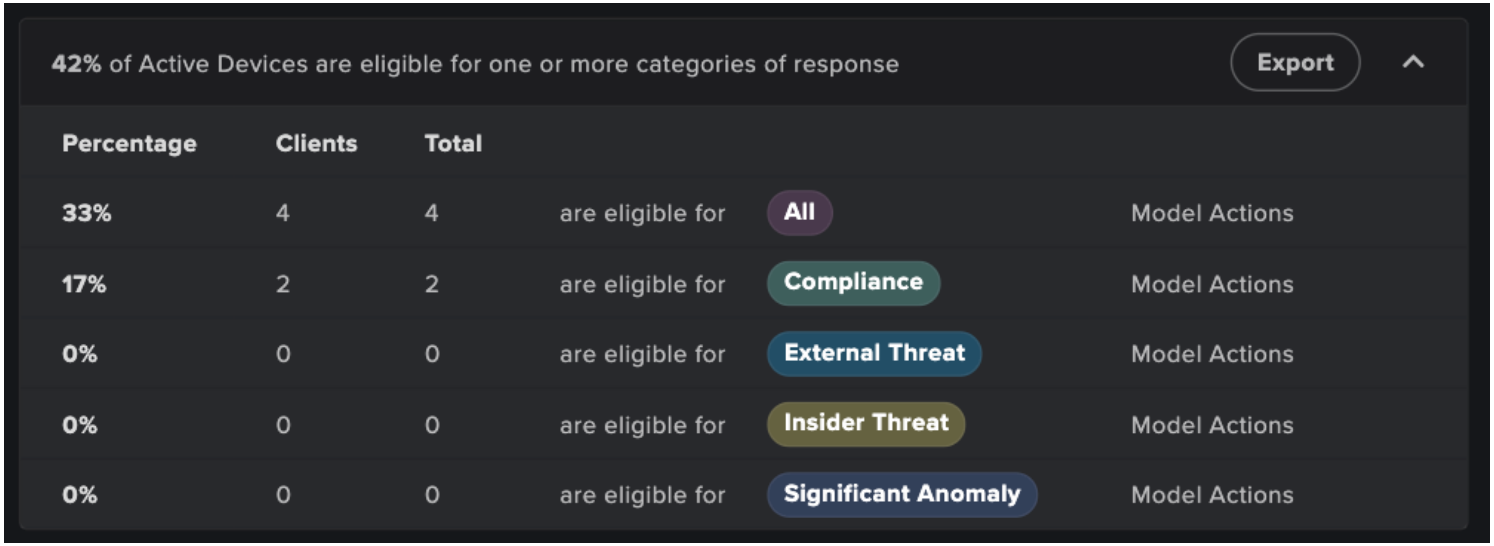
1. The first summary tab available is the percentage of **Active Devices** eligible for one or more categories of response. The table will display the following information:

   a. The **Percentage** of active devices eligible for each tag category

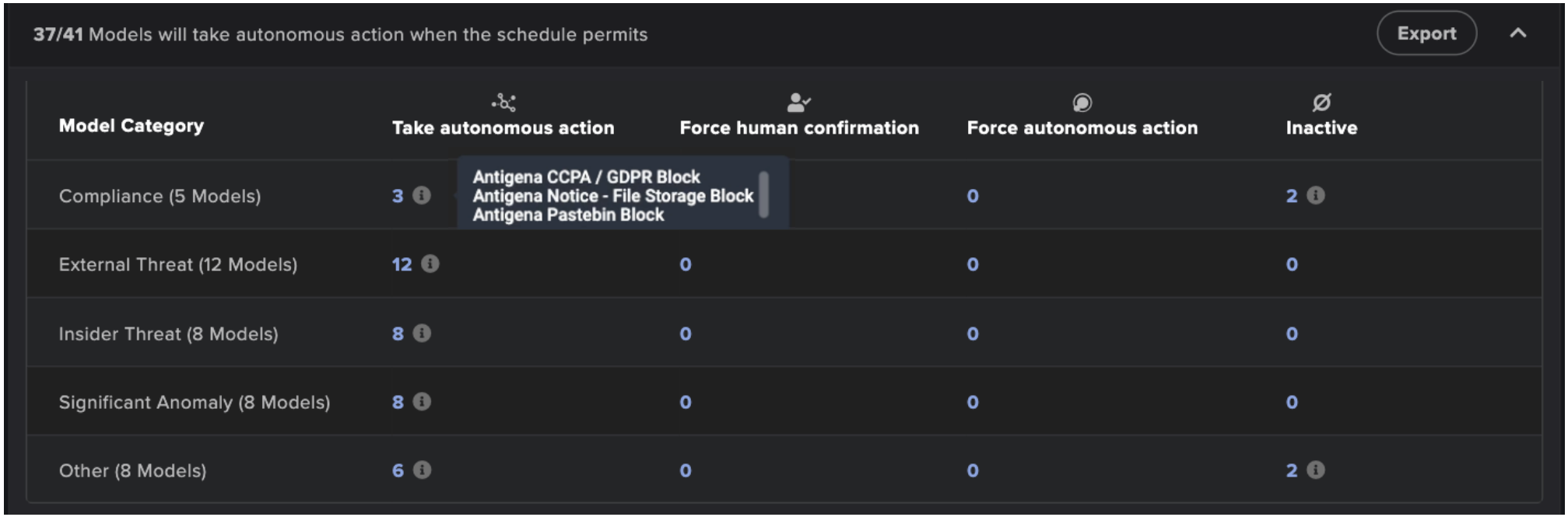
   b. The number of **Clients** devices

   c. The **Total** number of devices eligible

   d. The **Tags** categories



2. The next tab will reference the **Models** which will take autonomous action when the schedule permits it. The table will display the following information:



a. The **Model Category** will be displayed in the first column. There are 4 main Darktrace RESPOND/Network model categories: Compliance, External Threat, Insider Threat and Significant Anomaly.

b. The models settings will be displayed, showing if these are set to:

   i. **Take autonomous action**, meaning models will take an autonomous action if permitted by the system schedule

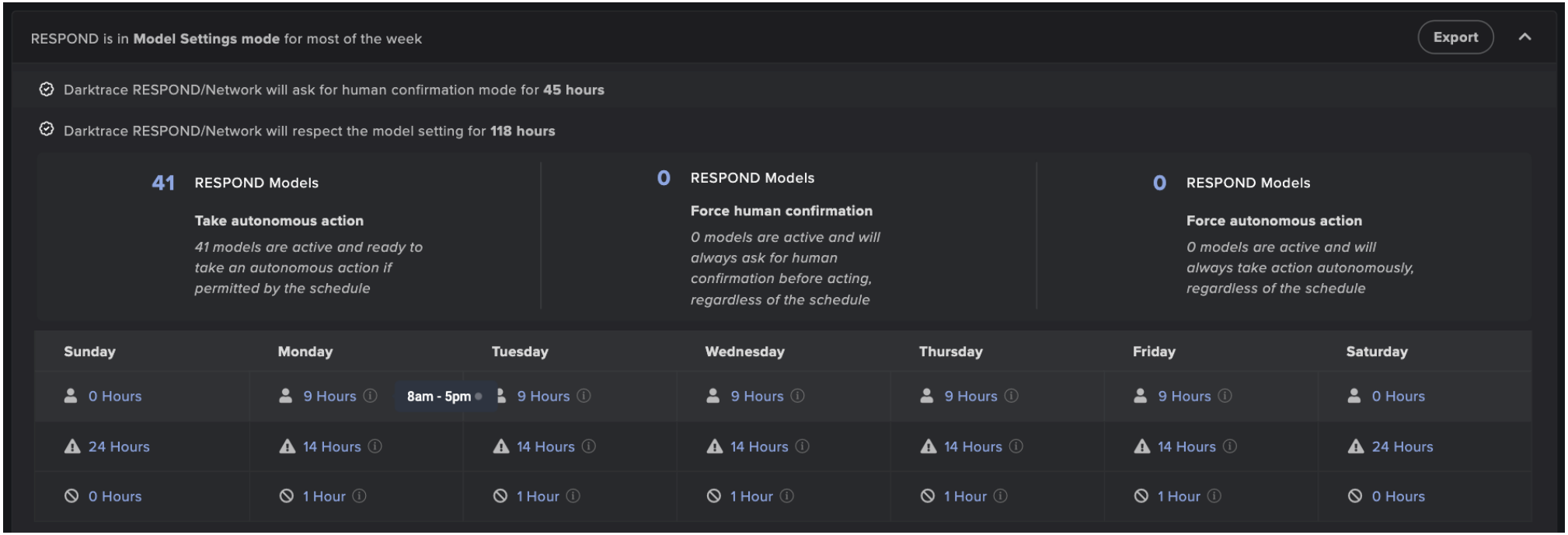
   ii. **Force human confirmation**, meaning models will not take an autonomous action unless approved by a user

   iii. **Force autonomous action**, meaning models will ignore the global schedule and follow their own setting.

Note: Hovering over the tooltip icon next to the displayed number will show the name of the models included in the selected category.

c. The final column will show the number of **Inactive** models

3. The final tab will show which **Setting** the deployment is currently running on, with data based on the week. The table will display the following information:



a. The number of hours Darktrace RESPOND/Network has been set to **human confirmation mode** and **model setting mode**.

b. The number of models which will either **Take autonomous actions**, **Force human confirmation** or **Force autonomous action**.

c. A weekly summary displaying the **number of hours** based on the different available settings:

   i. The first row will represent the number of hours during which Darktrace RESPOND/Network will require **human confirmation**,

   ii. The second row will represent the number of hours during which Darktrace RESPOND/Network will use **model settings**,

   iii. The third row will represent the number of hours during which Darktrace RESPOND/Network will be **disabled**.

Note: Hovering over the tooltip icon next to the displayed number will show the hours of the selected setting.

Quick Setup Test

DARKTRACE
Cyber Engineer Certification

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

1. In which confirmation setup will Darktrace RESPOND/Network require confirmation before taking action?

- [ ] Autonomous
- [ ] Partially Autonomous
- [ ] Human Confirmation

2. RESPOND/Network is often configured to be autonomous outside working hour

- [ ] True
- [ ] False

3. Eligibility for RESPOND actions can be set based on which two aspects?

- [ ] Operating System and software version
- [ ] Device type and subnet
- [ ] Time on network and rarity score

4. Which of the following icons indicates that RESPOND/Network will use model settings?



5. Which of the following is NOT an action state shown in RESPOND/Network?

- [ ] Active
- [ ] Confirmed
- [ ] Expired

6. In model configuration, which icon indicates that no models within the folder are operating in that state?



Clear All Answers

9. RESPOND protection Checklist

RESPOND/Network 4-Point Checklist

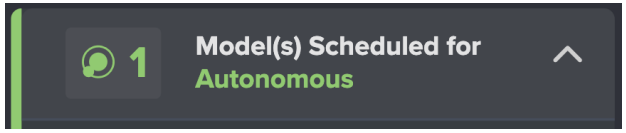
Continue your learning with our dedicated video RESPOND Protection Checklist

Here is a **4-point checklist** to make sure you are getting the maximum protection from Darktrace RESPOND/Network.

Enable Autonomous Mode

Darktrace RESPOND has two modes: **Human Confirmation mode**, in which RESPOND will usually require confirmation from an administrator, and **Autonomous Mode**, in which actions will mostly act autonomously.

Ensure you get familiar with Autonomous Mode and that this becomes the **deafult mode**. This will enable REPOND to work on your behalf.



Tag the Breadth of the Network

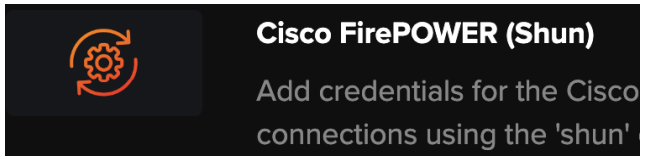
Devies without the **Antigena tag** are not protected by RESPOND. It is imporant, therefore, that tags are used, to ensure RESPOND has the correct reach across your network.

Use the **Quick Set Up** to set up Automous mode, which will also apply the recommended tagging options across your deployment.

Integrate with Firewall

Integrating RESPOND with your **firewall** gives you an additional layer of protection and is especailly good for increasing your protection against UDP based activity.

Use the **Threat Visualizer System Config**, or the **RESPOND Advanced Configuration** options to make sure that your firewall is integrated with RESPOND.



Test Reachability

Once Darktrace RESPOND is configured, the **Spot Tester**, which is to be found in the RESPOND/Network interface, enables you to test its ability to reach devices by performing a brief quarantine action. Scheduling and emailing options are also available.

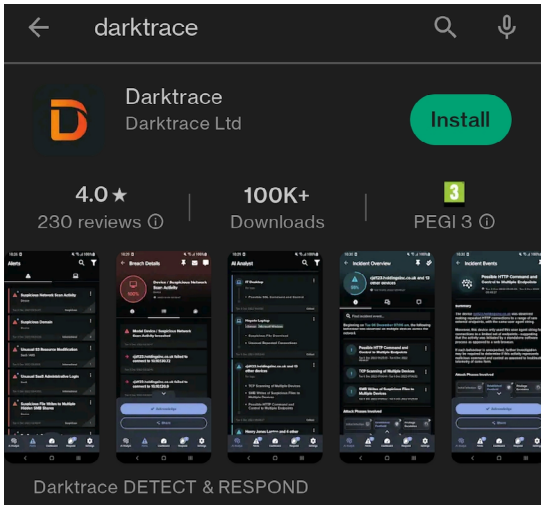
It is important that this is done **regularly**, particularly after major network changes.

9. Mobile App

The Darktrace Mobile App can be used to manage Darktrace RESPOND Actions on the go. Any decisions made in the Mobile App will be mirrored in the Threat Visualizer.

For the purposes of this manual, it is assumed that the Mobile App has already been configured within the System Config page and has been downloaded and registered in the Account Settings.

For more information about setting up this app, refer to the Customer Portal Product Guides.



1. The **Respond** screen of the Mobile App displays recent Darktrace RESPOND actions listed by category available in their relevant tabs: **Pending**, **Active**, **Cleared** and **Expired**.

   Note that **Active** devices are currently being controlled by Darktrace RESPOND whereas **Inactive** devices are not being controlled by Darktrace RESPOND.

2. Tap on an **individual Darktrace RESPOND action** to review details of the device, the Model that prompted the action and the timing of the Darktrace RESPOND action.

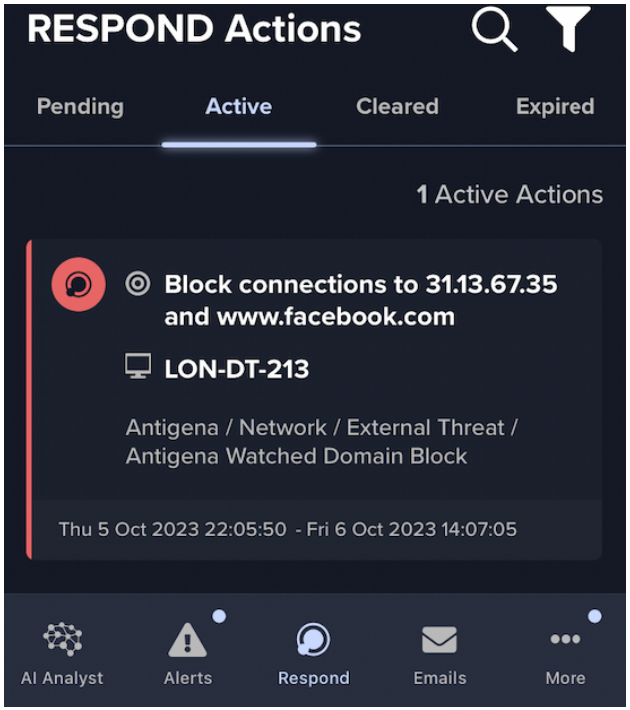
3. **Swipe up** to open up more options, allowing for changes.

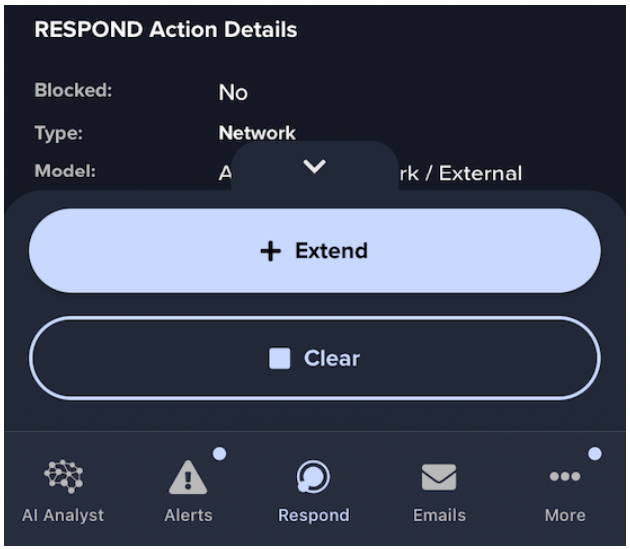
   a. **Extend** will lengthen the Darktrace RESPOND action on the device for the specified time.

   b. **Activate** will inform Darktrace RESPOND to start controlling the device with the specified action. **Reactivated** will be available if the action has been clear or has expired.

   c. **Clear** will inform Darktrace RESPOND to stop controlling the device.

4. Tap the desired action to provide **time options** for how long the action should be Extended, Activated or Cleared for.





10. Learning Outcomes

Course Agenda Checklist

Review this Course with our dedicated video
19. Course Summary

Thank you for completing this course on Darktrace RESPOND/Network.

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

Contact Us

For all further education inquiries, contact:

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

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

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

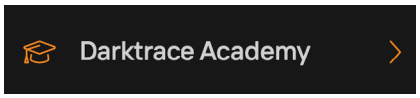
Complete the learning outcomes checklist below:

- [ ] **Understand Darktrace RESPOND basic concepts**
- [ ] **Configure Darktrace RESPOND options**
- [ ] **Handle actions raised by Darktrace**
- [ ] **Understand of Darktrace RESPOND/Network Models**
- [ ] **Tag devices for monitoring**
- [ ] **Implement recommended RESPOND set-up options**

11. Additional Educational Material

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

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



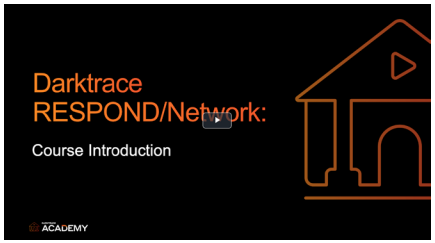
Training Courses

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

COURSE	AUDIENCE
Darktrace PREVENT/ASM	All end users
Darktrace PREVENT/E2E	All end users
Threat Visualizer Part 1 - Familiarization	All end users
Threat Visualizer Part 2 - Investigation	All end users
Darktrace HEAL	All end users
Cyber Analyst Part 1 – Advanced Analysis	Super Users (Tier 2 Analysts)
Cyber Analyst Part 2 – Model Optimization	Super Users (Tier 2 Analysts)
Cyber Engineer	Partners / Installers
Threat Visualizer Administration	Administrators
Darktrace RESPOND/Network	Administrators and Analysts
Darktrace/Email Part 1 - Familiarization	Email Administrators and Analysts
Darktrace/Email Part 2 - Customization	Email Administrators
Darktrace/Apps	All end users

Training Videos

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



Darktrace Certification

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