DARKTRACE

THREAT VISUALIZER PART 1 – FAMILIARIZATION

Threat Visualizer Part 1 – Familiarization
Manual v2.0.0 – Darktrace v5

Table of Contents

1. Learning Objectives

This course provides an introductory familiarization of the Threat Visualizer interface. It is primarily designed for end users of Darktrace, including IT Security Managers, IT Security Architects, and Cyber Security Analysts.

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

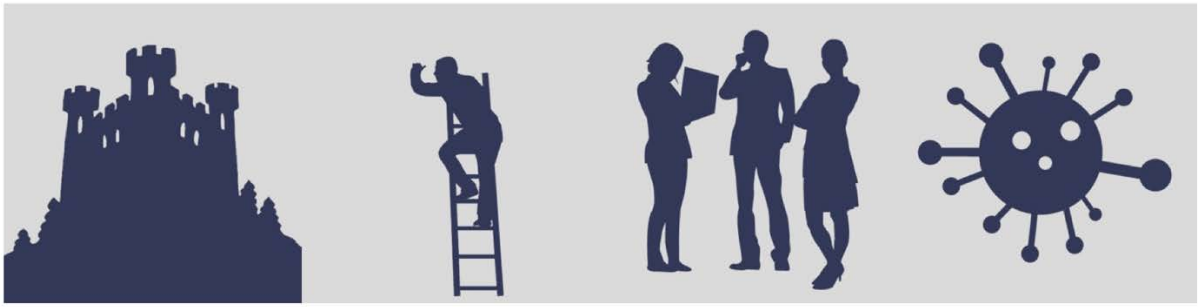
+ Understand Darktrace solutions
+ Navigate the Threat Visualizer Interface
+ Obtain information about network devices
+ Review Model Breaches

On completion of this course, it is advised that you next attend Threat Visualizer Part 2 – Investigation.

2. Introduction to Darktrace

Darktrace was founded in 2013 in Cambridge, UK, by government intelligence experts working with leading mathematicians at Cambridge University. Together, they established the Enterprise Immune System, a technology has continually evolved to form the Cyber AI Platform. Based on important advances in Bayesian probability theory and powered by cutting-edge machine learning, Darktrace ingests communications and creates a unique behavioral understanding of "self" for each operator and device in the organization and, like a biological immune system, it detects threats that cannot be defined in advance by identifying even subtle shifts in expected behavior. The majority of people and devices behave in a unique way, that differs from their peers to varying degrees, but that is significantly more predictable in comparison to their own historical behavior and rates of change.

This technology is ideally suited to detecting malicious communications, even previously unknown threats that are novel or tailored, and regardless of whether they originate in either the IT or operational domains, or traverse between them. By identifying unexpected anomalies in behavior, defenders are able to investigate malware compromises and insider risks as they emerge and throughout stages of the attack lifecycle. Darktrace provides the real-time visibility required to make intelligence-based decisions in live situations, while enabling in-depth investigations into historical activity.



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

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

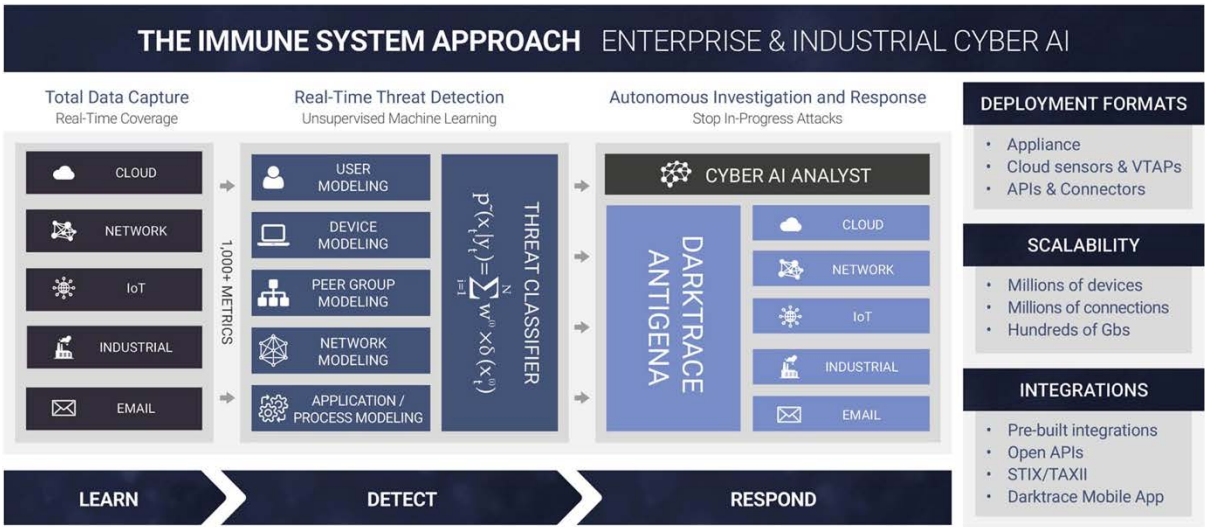
A far more intelligent, automatic and sophisticated technology is required that can detect these subtle changes that can understand the normal pattern of life in a business and what is abnormal and a potential threat.

Darktrace offers a new approach of using mathematics applied to machine learning developed at Cambridge University, which is the foundation of the Enterprise Immune System. It has complete analysis and visibility of 100% of the network traffic. Network traffic is ingested and stored for long periods of time so that it can build correlations and behavioral analysis. By iteratively monitoring network traffic all the time, Darktrace builds up a model of behavioral analysis for users, devices and the network as a whole.

These network interactions can be played back on the network within the Threat Visualizer tool to understand the what factors preceded an event and what the outcomes were.

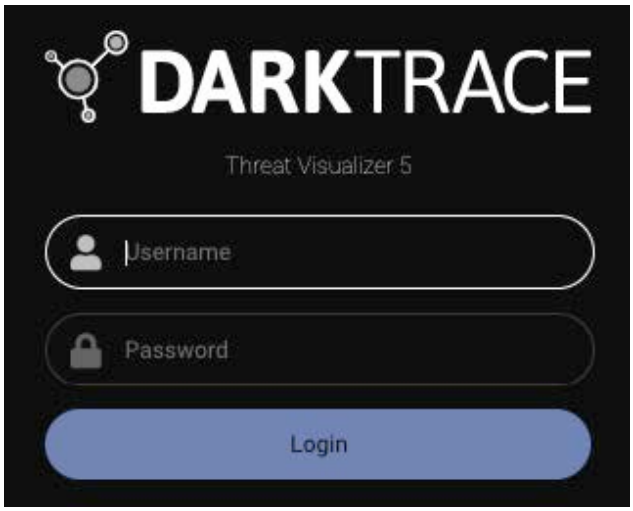
Darktrace's unsupervised machine learning means it literally discovers on its own. It also operates passively, which means it is a technology watching and listening, but not interfering with existing IT network infrastructure.

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



3. Threat Visualizer Navigation

The Threat Visualizer can be broken down into multiple views; global, subnet and device. In order to navigate to any of these views, log into the Threat Visualizer.



1. In a Chrome, Firefox, or Microsoft Edge web browser navigate to the Threat Visualizer at

   https://<servername>

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

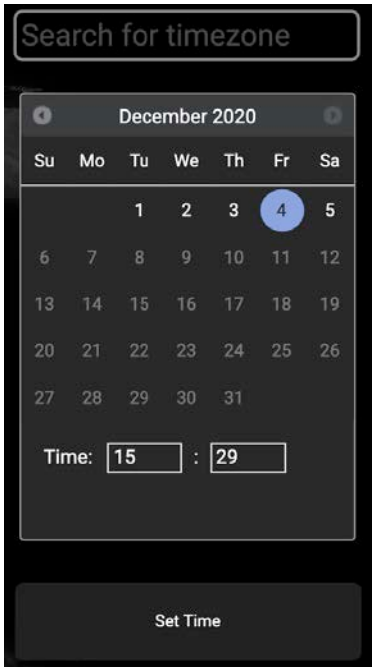
Global View

1. Review the home screen on the **Threat Visualizer**. This provides a global snapshot of the network with shortcut links to key information.

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

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

   Click on the date. Within the **Search for timezone** bar, enter a minimum of three characters of your desired timezone or city, such as GMT or Los Angeles.



   Click the **Set Time** button at the bottom to save your settings.

4. The **Omnisearch** bar can locate all Darktrace objects, such as devices, subnets, models and domains.

5. A **summary of subnets and devices** is a quick way to understand your network and spot any changes.

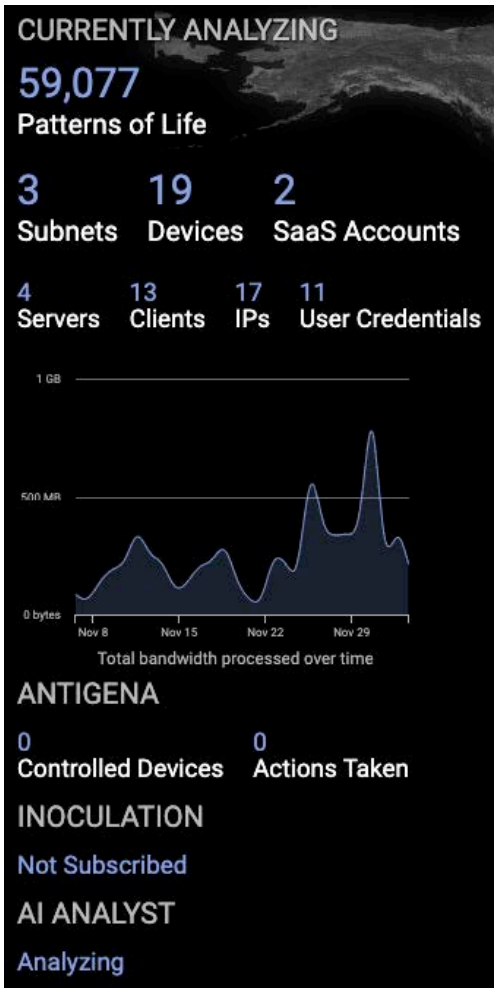
   Note: *If a SaaS connector is enabled, the number of SaaS accounts will also be displayed.*

   Notice the Threat Visualizer automatically tries to detect the type of devices, such as servers and clients as well as the number of IP addresses and user credentials.

   The **Patterns of Life** figure represents the number of unique connections between devices. Connections include every separate pattern interaction with a device such as individual logins and access to network shares of file systems.

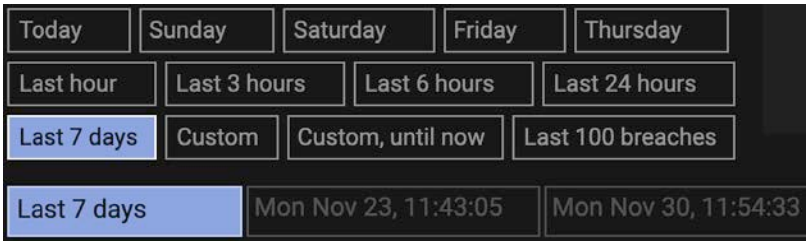
   Typically there are approximately two hundred connections for every device on a network. The graph represents the bytes per day for the entire network being captured by Darktrace.

   Information about other services that may be subscribed to are also presented in this summary.



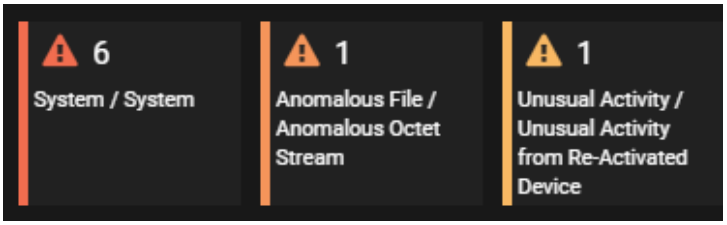
6. On top of the world map, the cubes represent special purpose **network ranges** such as link local, broadcast, multicast and internal traffic.

7. The **Threat Tray** displays all breaches in a set time frame. The Threat Tray has an independent time range distinct from the **Time Selector**.

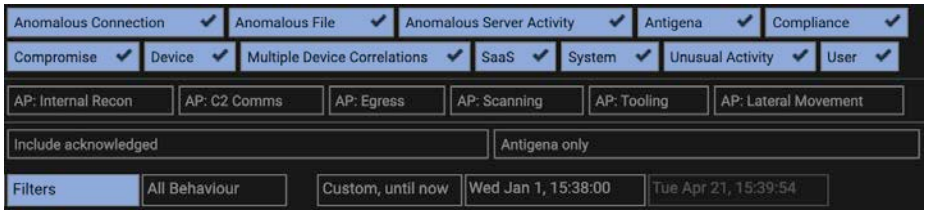


8. The **sensitivity slider** controls the minimum and maximum percentage scores by moving the knobs on the left and right, respectively.

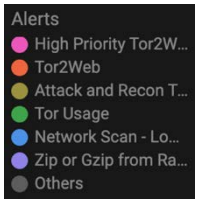
9. Breaches are displayed in real time and **prioritized** based on the selected sorting method. They are colored based on their severity with red and yellow representing high and low scoring breaches respectively.



10. The breaches presented in the Threat Tray can also be **filtered** by Model type or Attack Phase (AP).



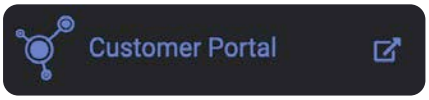
11. Select the **graph icon** from the four icons displayed in the lower left-hand corner of the Threat Tray to present breaches in a graph of time against score. The breaches are colour coded, as seen by the key on the right. Clicking any breach opens the appropriate Breach Log for the device.



12. The **main menu**, found in the top left-hand corner, contains key functions to control the Threat Visualizer including links to the Model Editor and Advanced Search.

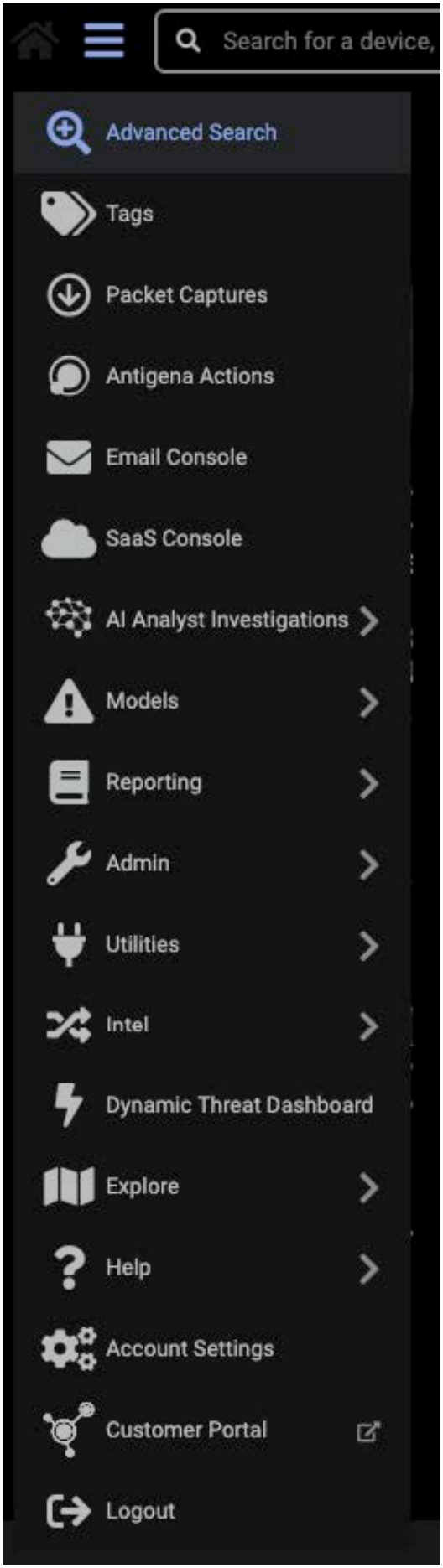
Many of the functionalities displayed in the main menu are permission dependent and can only be access if a user has been granted the appropriate user/group role permissions.

13. From the main menu, it is possible to open a new tab to the **Customer Portal** login page. The Customer Portal is a great resource for creating support tickets, viewing product guides, watching eLearning videos and downloading updates.

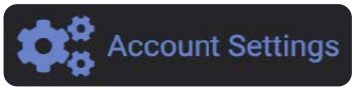


14. There is a **Utilities** submenu which contains the following applications to facilitate investigating breaches:

- PunyCode converter
- Regular expression tester
- Base64 decoder
- JavaScript beautifier
- Epoch converter



15. The Threat Visualizer can be customized for each user. Within the menu options, select **Account Settings**.

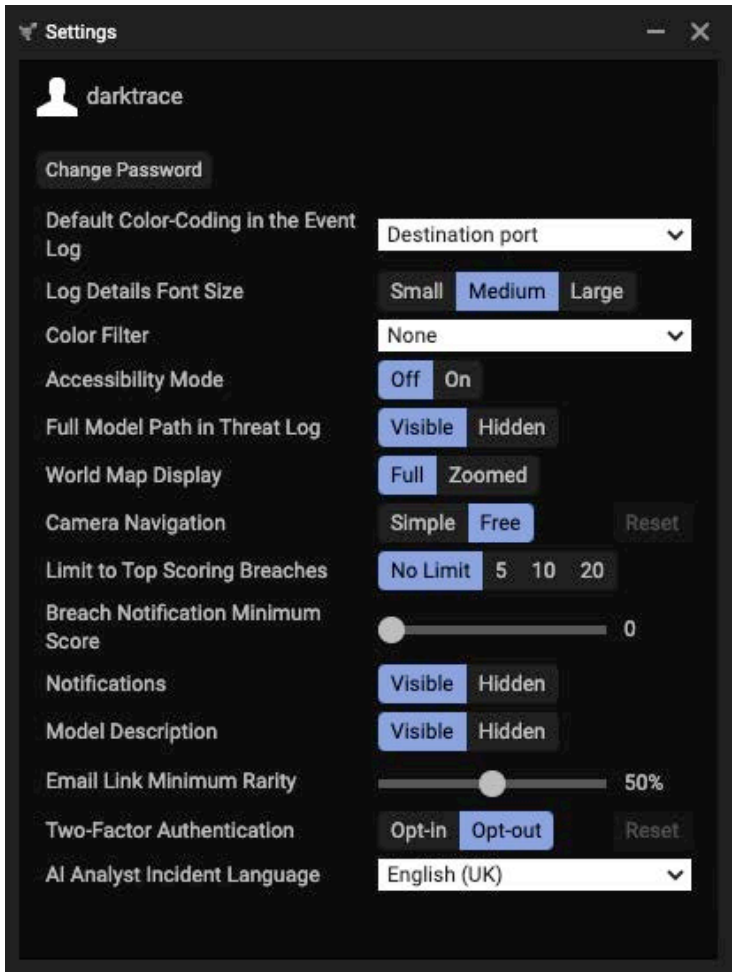


Depending on your screen resolution, you may wish to change the **log details font size**.

For accessibility, there are **color filters** for the three varieties of color blindness as well as an accessibility mode which presents the threat score beside the Model Breaches in the Threat Tray.

It is also a popular choice to set the default color-coding in the Event log to **Destination port**. The **Application protocol** and **External hostname rarity** are also useful considerations.

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



16. If the Global View has been navigated away from within the Threat Visualizer, click the **Home** button in the top right-hand corner to return to the homepage.

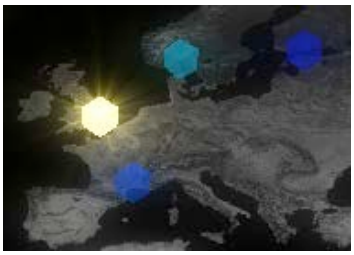
17. Once you have finished using the Threat Visualizer, navigate to the main menu and select the last item, **Logout**, to securely exit the interface.

Subnet View

The Subnet View is a useful way to quickly review subnets and identify their size. It works best for smaller networks.

1. The **global map** displays the location of your networks. Hovering over a group reveals the number of subnets in that location.

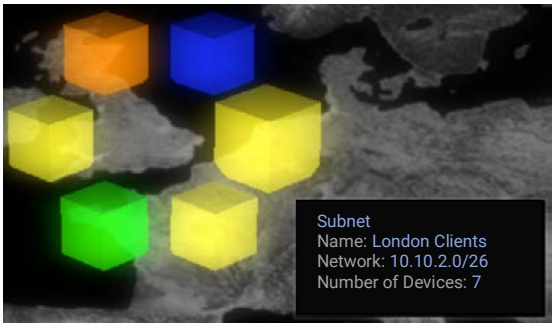
   Click on a cube icon to display subnets for the selected location.



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

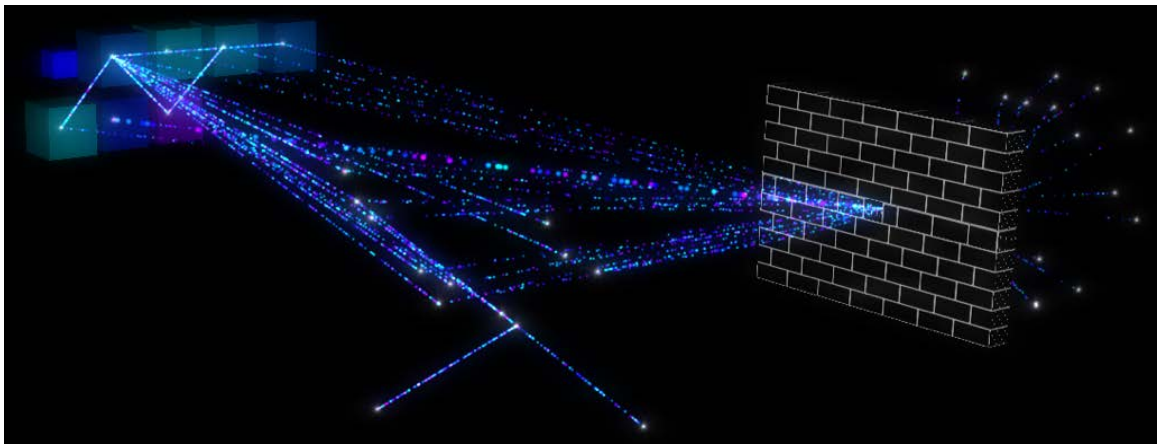
   - **Red**, **orange** and **yellow** cubes indicate a subnet has detected anomalies on the network. The redder the color, the greater the anomalous behavior detected.

   - **Green** is displayed if Antigena is running and monitoring the specified subnet.



   - **Blue** and **purple** colors mean that no anomalies have been detected on the subnet.

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



   The **wall** represents the external perimeter of your network. The data protruding from the subnets or wall represents the network traffic seen in the selected time duration.

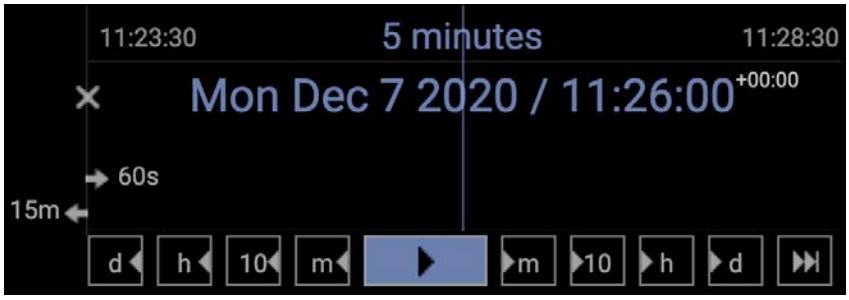
   The thicker the line, the greater the volume of data flow between devices. Yellow lines represent what Darktrace believes to be unusual activity (activity that deviates from a device's normal pattern of life). Each star represents a device.

Tip: *Move the view around to gain a better view of the endpoints. Hold down the left mouse button to freely angle the position of the subnets. Click and hold the right mouse button to drag the view up/down/left/right in more fixed axial movements.*

4. Hover over the stars to view **device details**.

   Clicking a device displays more device information which is covered in the next part of the lesson.

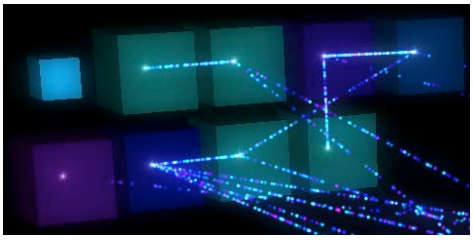
5. Upon opening of the Subnet View, the **Time Selector** in the top-right hand corner will expand to display **5 minutes** of analyzed data by default.



   Use the arrows to change the **duration** to **15 minutes** and watch the data flow increase. (If these buttons are not visible, click the clock symbol to the left of the time selector.)

   Try the shortcut day, hour and minute buttons. The play button allows for a real time view of the data flow on your network. By clicking the double arrows on the far right, you can return to the current time.

6. To select a different subnet, click on the different **subnet blocks**. The network data flow will update.



7. Select the small blue cube labeled **Full Network** to view a global view of subnets.

   This is useful to quickly confirm the largest subnets and which ones are firing the most breaches.

8. Clicking on different subnets will update the **Omnisearch bar** in the top left corner to display the currently selected subnet.

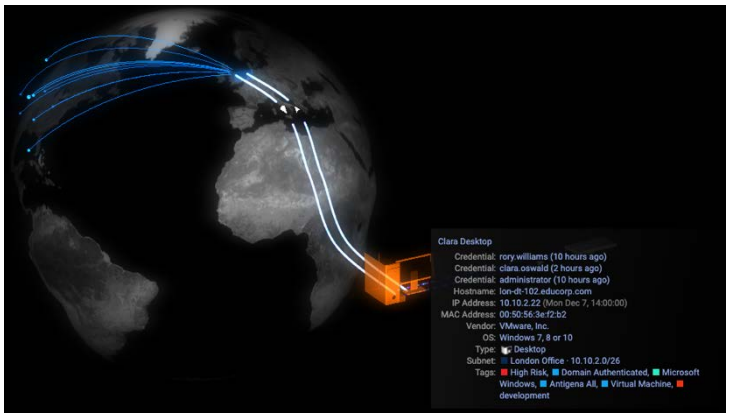
Device View

The Device View focuses on one device and displays all the network communication between it and other devices.

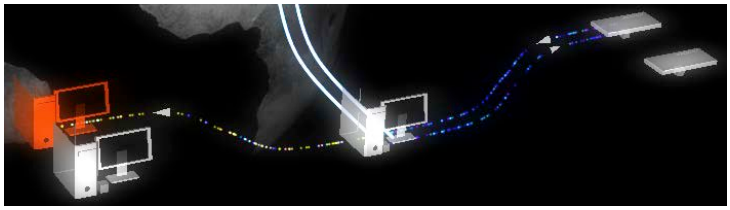
1. Hover over the device to view full details.

   Left click and drag the space around the device to get a better view of its network interactions with other devices.

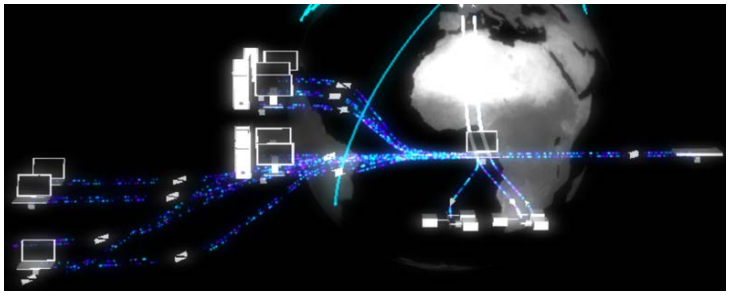
   Hold down the **right mouse button** to move the icons around the screen.



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

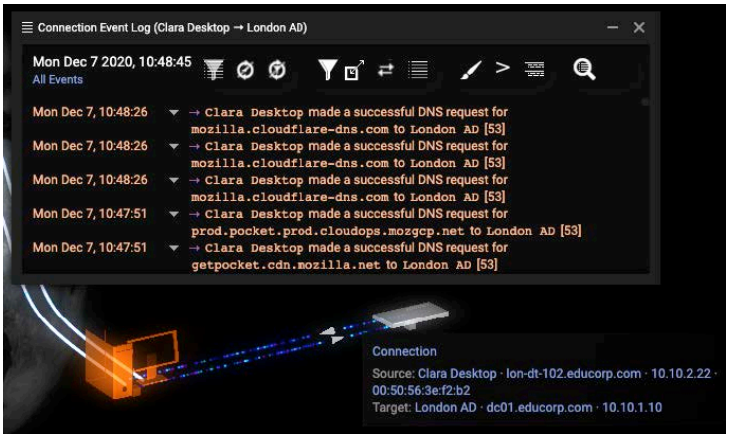


3. Clicking on another device will **refocus** the Threat Visualizer on to it.



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

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



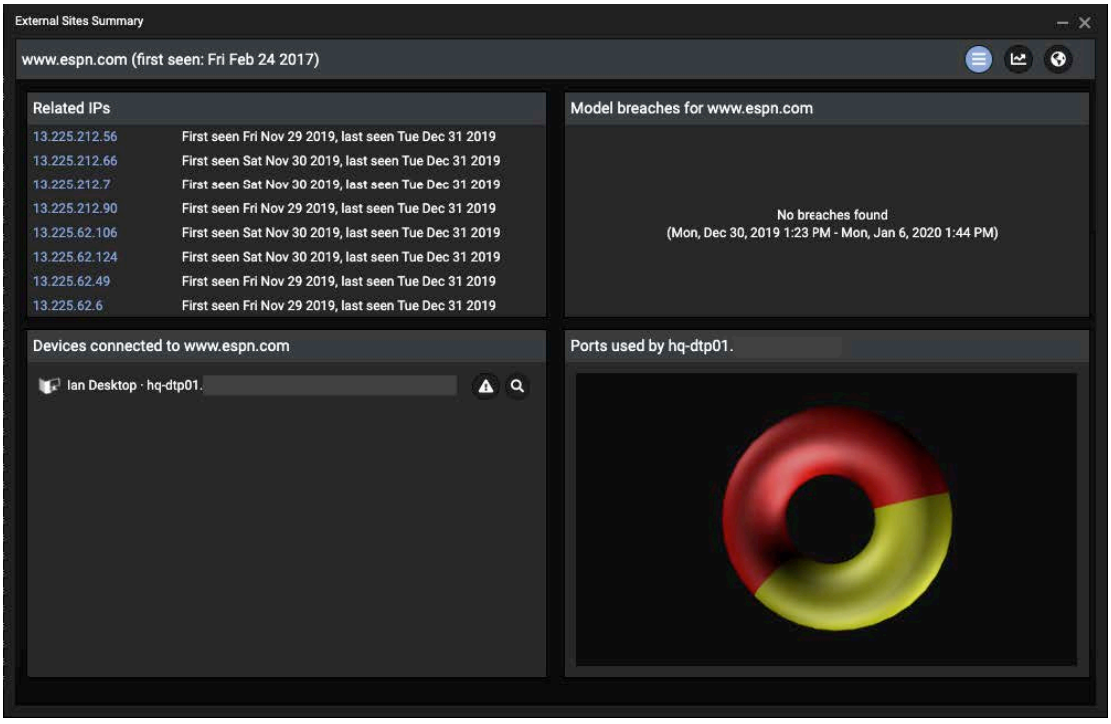
5. If a device has made **external connections**, the locations will appear on the world map.

   Hover over the dots to view domain and country information, as well as the IP address.

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

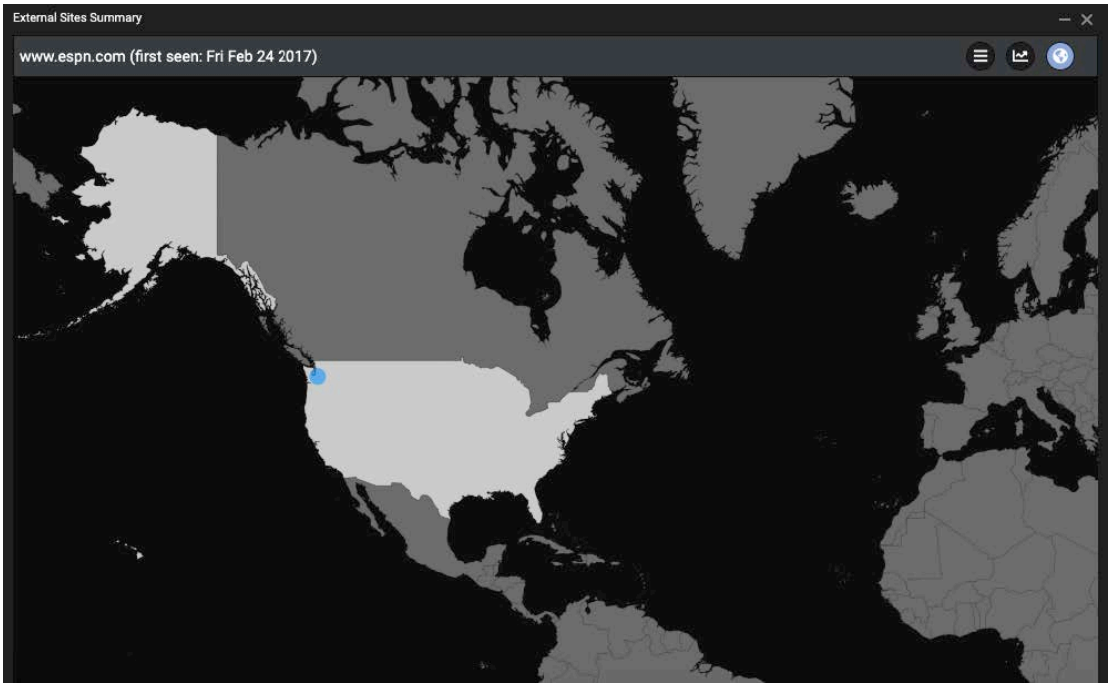
6. Clicking on a dot will open an **External Sites Summary**.

   a. **List icon:** This produces a list of all devices which have attempted to connect to the external domain and its related IP addresses. The Model Breach Event Log for each device can be opened from here to show any breaches from the last seven days. Clicking the magnifying glass next to a device name will change the results presented in the ports used graph, showing which ports have been used by the device to connect to the endpoint. It also shows model breaches related to the external endpoint which is a convenient method for analysts to quickly check which devices have contacted a suspicious domain.

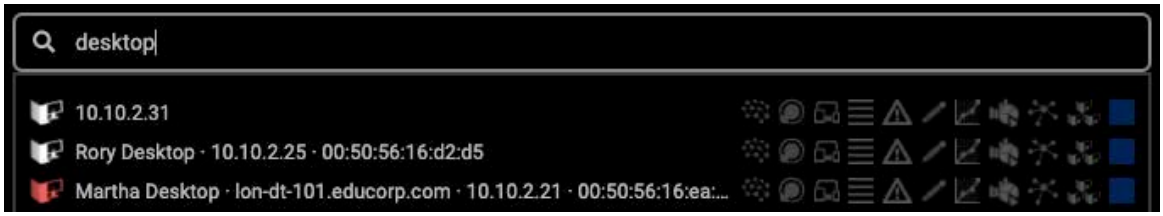


b. **Graph icon:** This changes the view in the External Sites Summary to show the changes in rarity of the endpoint over time.

c. **Globe icon:** The final view in the External Sites summary shows the location of the IP address. It will zoom into the location and be marked by a blue circle.



7. As you select devices, they are set in the **Omnisearch bar**. This Omnisearch bar can display a list of devices, event logs, external sites and models in a drop-down list.



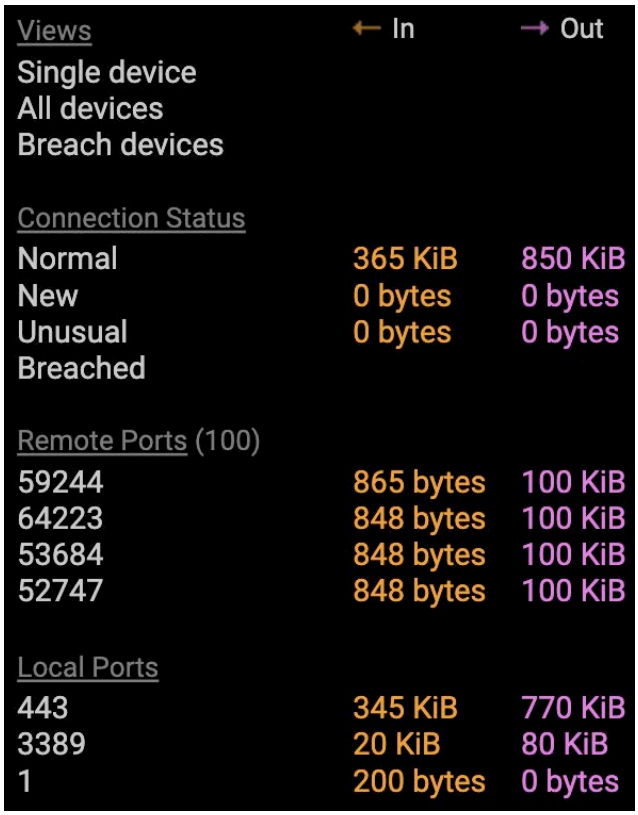
Using a minimum of three characters, you can search for users to view which machines they have logged into, enter a hostname to understand who has visited it, or even search for Models.

8. On the right-hand side, an interactive summary of all communication within the selected time period is displayed.

   The information in **orange** is the received data (In) on the device and the information in **pink** represents the data sent (Out). **Click a port to restrict results.**

   This is a useful way to quickly understand how much data has been sent and which protocols and ports were used. Results can similarly be restricted in other ways by clicking on device or protocol filters for example.

   Look out for unusual data on specific ports. Large volumes may be of particular interest and require further investigation.

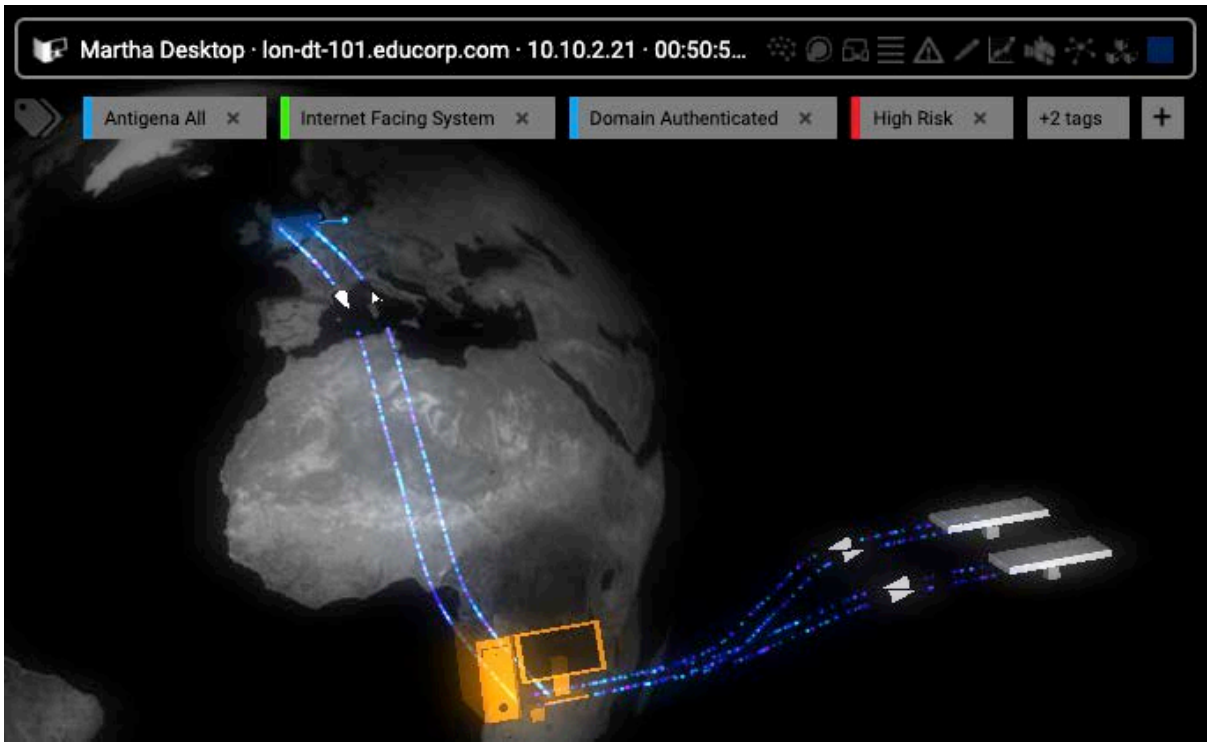


9. Once applied, click the filter to remove and **reset** your selection.

10. Note the same **External Sites Summary** data is also available if you search for an external domain in the Omnisearch bar, a small world icon will be available at the right of the drop-down menu.

Device Details

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



1. Within the Device View, notice a **series of icons** displayed on the right of the Omnisearch bar.

2. The first icon allows the user to instigate an on-demand AI Analyst investigation. 

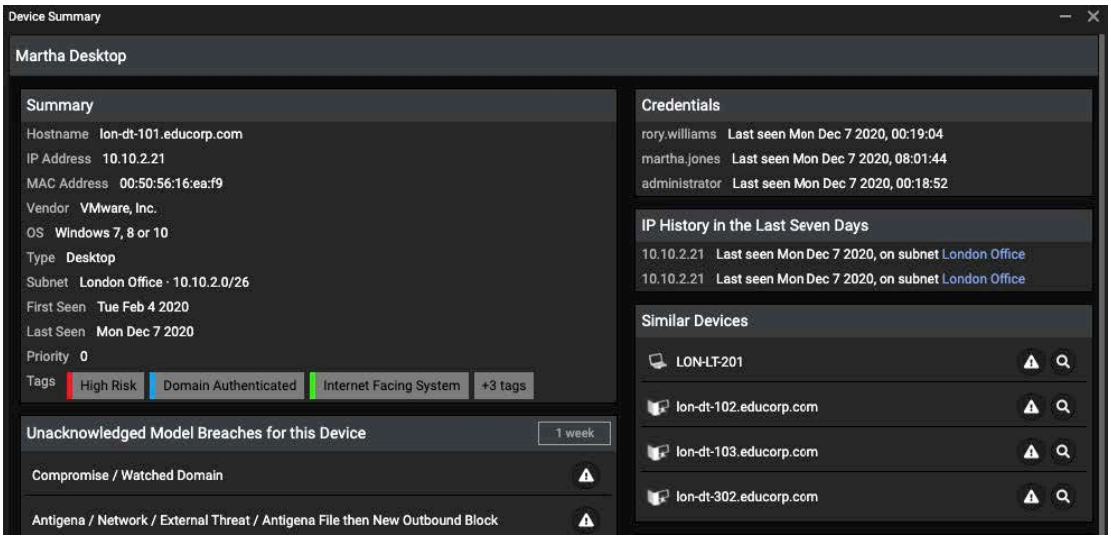
   Note: *This functionality is discussed in more depth in Threat Visualizer Part 2 – Investigation.*

3. The next icon is only visible for deployments with the Antigena Network module. It allows the user to review and confirm actions performed by Antigena Network. 

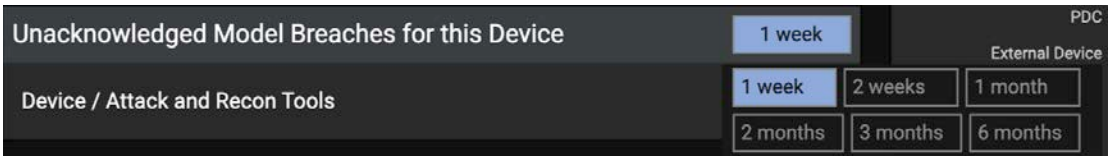
   Note: *This functionality is discussed in the Antigena Network course.*

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

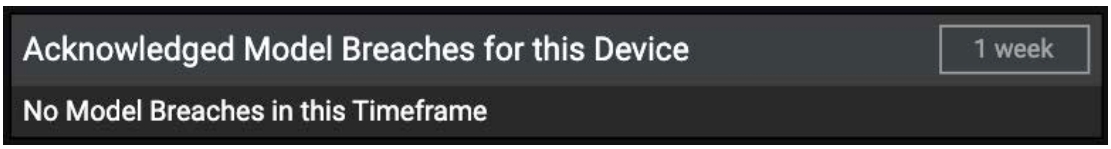
   a. This displays the **key information** captured by the Darktrace appliances, including specific device information, as well as credentials observed on the device, a seven-day IP history and list of similar devices.



   b. There is also a quick and easy way to understand what other **unacknowledged breaches have previously occurred** on this device within the past week up to the past 6 months.

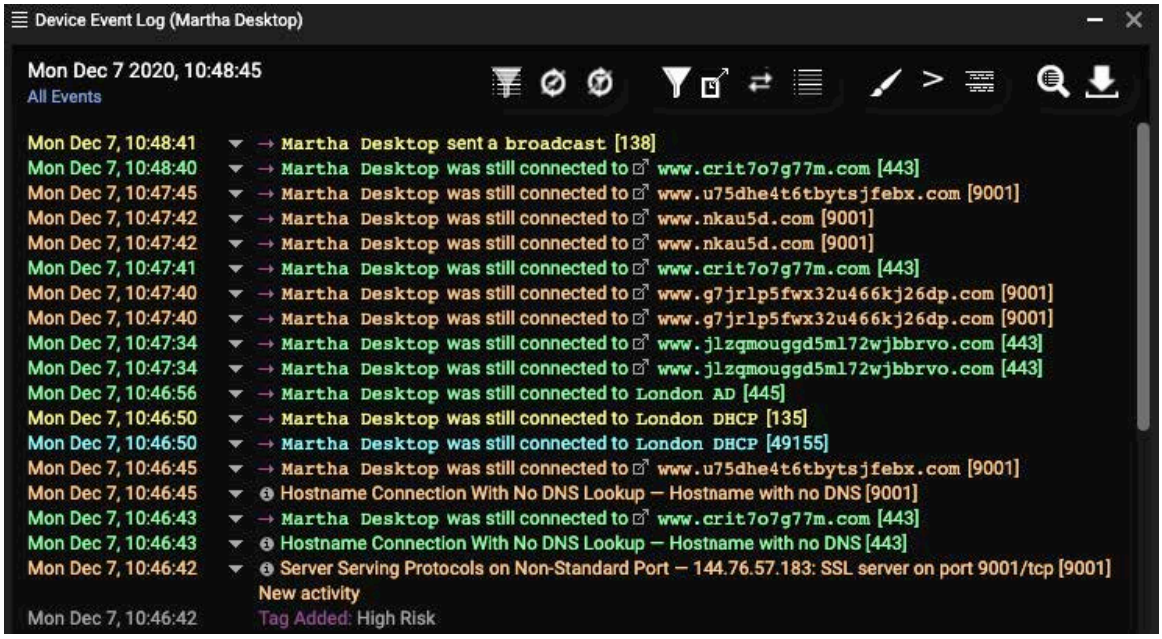


   c. Underneath the Unacknowledged Model Breaches, there is also an **Acknowledged Model Breaches for this Device**. This can be useful to see what activity might be expected from a device by viewing the historical trends over the last week or over the six months, depending on the time frame selected.



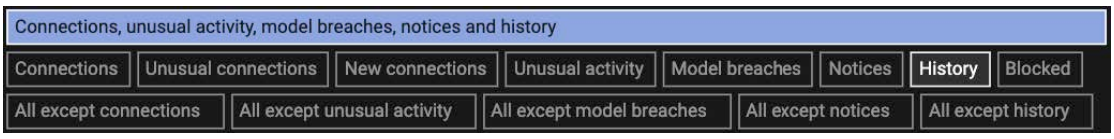
d. **Scroll down the Device Summary** window. This displays the **ports** that are most commonly used and served, as well as the **devices** it most commonly communicates with. This is a handy way to quickly understand what roles the device has on the network.

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



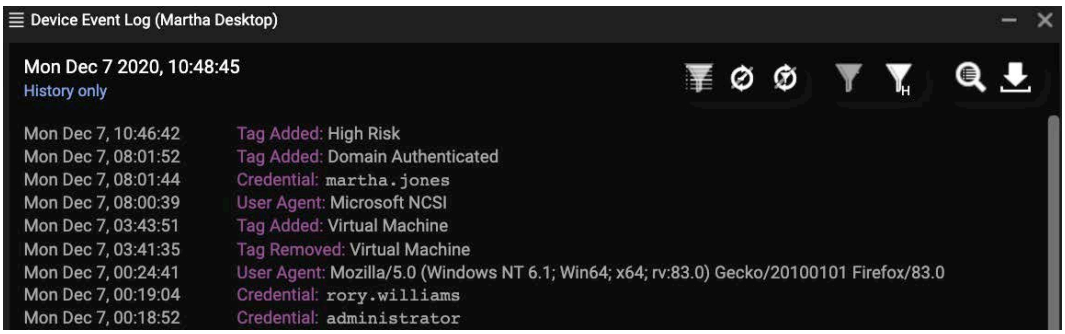
Note: *The Advanced Search and Packet Capture features depicted in the right-hand corner are explained later on.*

a. The history of a device is easy to recall within the **Device Event Log**. Select the **Choose which type of events to show in the log**.



Click the **History** option to reveal a range of key events in the Event Logs, including:

i. Kerberos, RADIUS and POP3 authentications
ii. Changes in IP, MAC, hostname and subnet
iii. Application, removal or expiration of tags
iv. Observed user agents



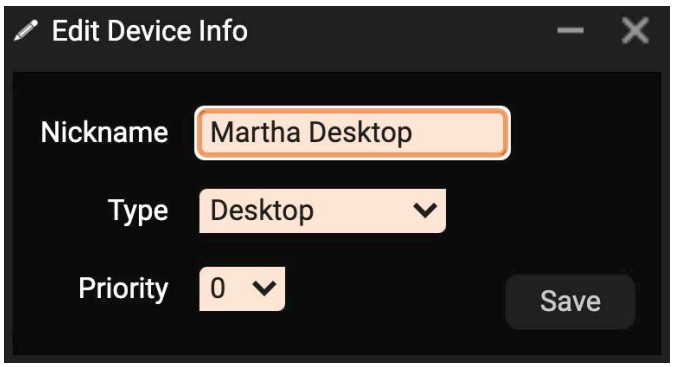
These events can help with understanding how a device is being tracked over time or which user authenticated prior to an event of interest. For example, viewing the credentials can be useful when investigating lateral movement.The entries displayed represent two weeks leading up to the current Threat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

6. The **Device Breach Log** is similar to the Model Breach Log, except it reveals all breaches for the device for the currently selected time frame as specified at the bottom of the UI.

7. The **Edit Device Info** can be used to update the Device label and type.

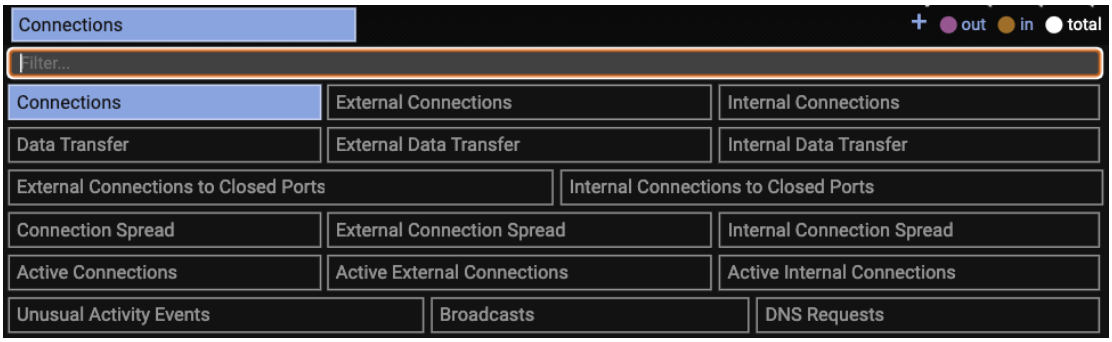
This is information is useful to assist analysts in understanding devices.

Note: *Priority is covered in another class.*



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

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



Note: *View the Darktrace Threat Visualizer User Interface Manual from the Product Guides to obtain a detailed description of each Metric.*

b. Click under the X axis time line to reveal additional **time filters**.

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

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

Through these graphics, it is easy to understand the ports and devices used by each device. It is also possible to click the menu options to filter the data.

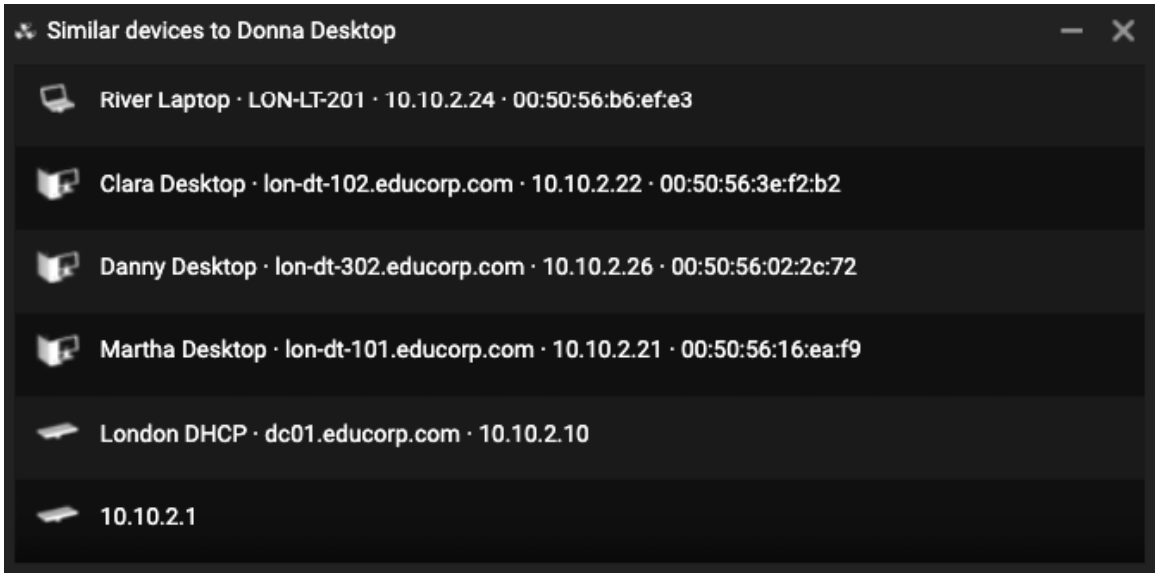
10. The **Similar Device Map** is a three-dimensional view which displays devices grouped together based on their similarity.

This is automatically calculated in real time by Darktrace. It is based on complex mathematics, which at a basic level includes a combination of connecting devices on the network or devices which share the same port usage.

Hover over a device icon to obtain its information.

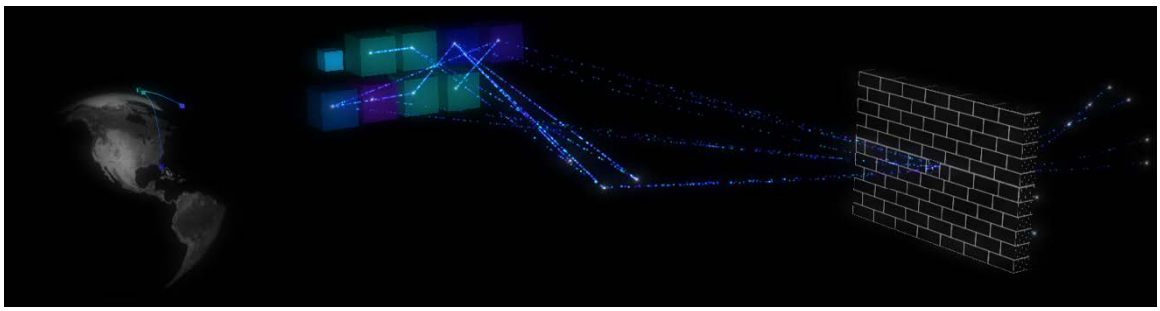
This view automatically rotates. Utilize the pause function in the top right of the window to stop the animation and view any of the devices.

11. The **View Similar Devices** icon provides a list of similar devices which can be easily clicked to explore each device.



Darktrace uses machine learning techniques and mathematical clustering values to calculate how similar one device is to another.

12. The **Go to Device's subnet** button is a handy shortcut to return to the subnet view.



Navigation exercise

Use the Threat Visualizer to carry out the following:

a. Identify your own device on the network.

b. Can you identify all mobile devices?

c. Set the threat score filter to 50%.

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

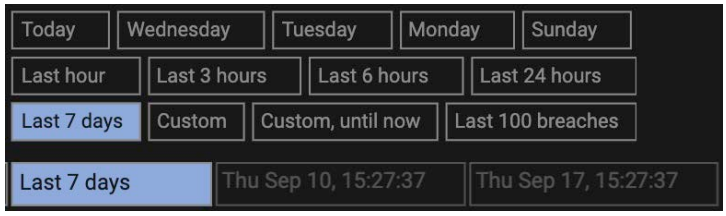
e. What was the last Unusual Activity Model Breach?

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

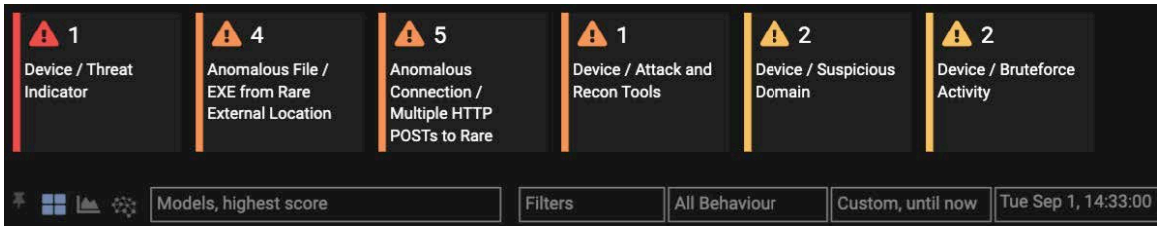
4. Reviewing Model Breaches

The Threat Visualizer comes with a large selection of prebuilt models to automatically search, detect and alert you to anomalous behavior in the network. Any change to a network, such a new device being located, or a device connecting to an external host at an unusual time of day, could be viewed with suspicion. The Threat Visualizer will identify and classify these potential events to prioritize and facilitate quick analysis.

1. Within the Threat Tray, click the **Today** value and set **Last 7 days**. This will reveal anomalies over time. A custom time can be set to investigate a specific date range.



2. An increase in duration will reveal additional alerts, or *breaches* discovered by the Enterprise Immune System. Each *Model* has a title indicating the issue discovered and a number revealing the sum of breaches found in the selected time range. Review the alerts triggered in the **Threat Tray**.

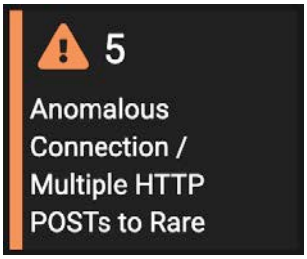


By default, it is sorted by the method used from the last login for the same user. The highest score for a model (**Models, highest score**), can be useful for day to day analysis, focusing on breaches which may offer the most significant threat. However, you can click the breach type to view a number of alternative ways to sort these results. Instead of sorting the model breaches by models, they can be sorted by users or devices.

Notice breaches can be prioritized by a **score**. While the Threat Visualizer analyses the network, it employs machine learning mathematics to automatically understand and score a breach out of 100%. The higher the score, the greater the risk a potential threat can be thought of posing. The score can be represented by a color:

- A **red** breach indicates the threat has a high priority and may be very serious.
- An **orange** color means medium priority and **yellow** indicates a lower priority. These can warn the user of particular behavior but may not require urgent action.
- A **gray** color indicates a model has been updated and has yet to trigger a new alert since that update.
- A **gray** icon with an 'X' indicates the model has been deleted since the alert was generated.

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



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

3. The **Sensitivity Slider** facilitates concentrating on the most relevant breaches.

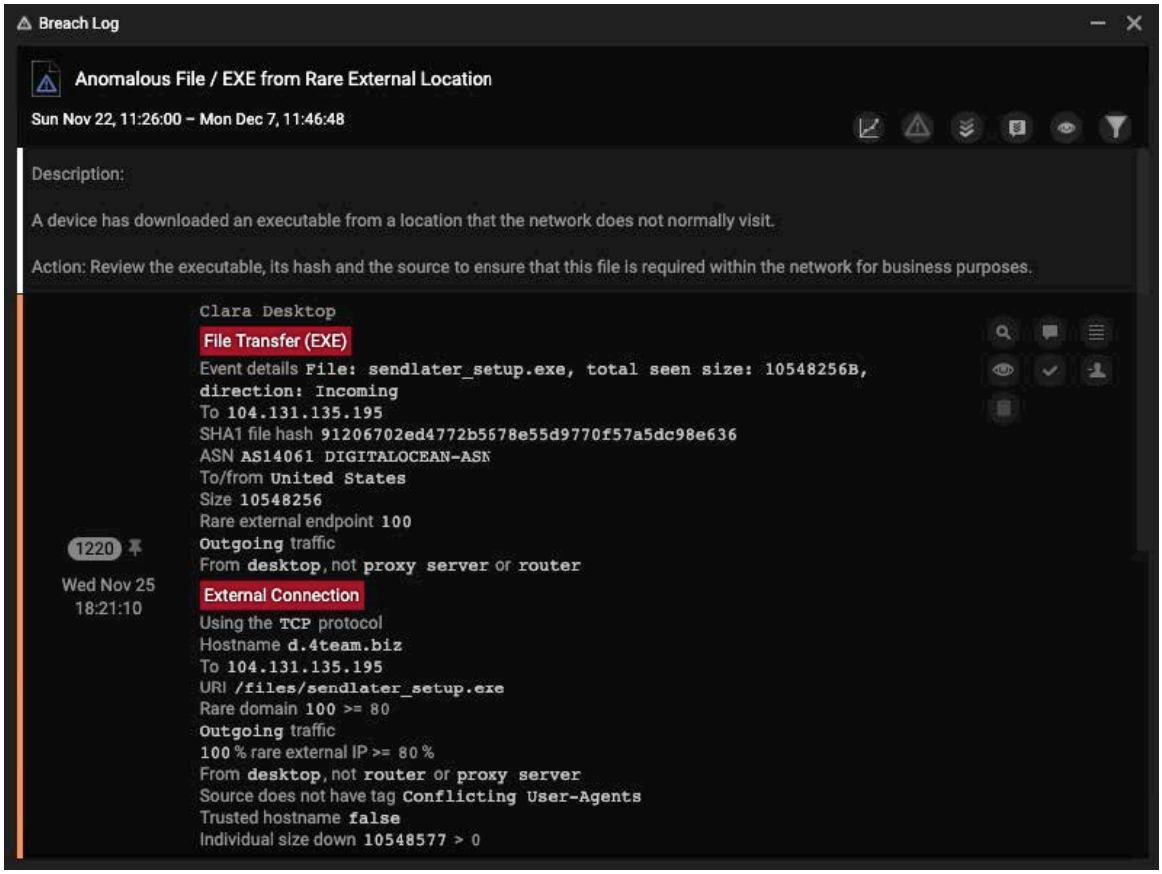
Set the minimum Sensitivity Slider to **60%.** This will only show alerts with score of 60% or more in the Threat Tray. The previous threats are still available, just temporarily hidden from view. The right-hand slider represents the maximum threat score. In practice, it can be helpful to prioritize and focus of the most severe threats.

4. Click on a breach to load the **Breach Log.** Each breach reveals the device and date on which the breach was triggered, the Model that was breached and the values that exceeded the Model's filters.

What is a Model?

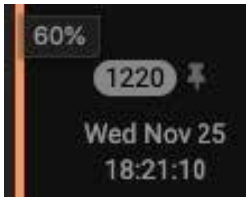
A Model contains a list of conditions which define an undesirable or notable behavior. Exceeding those conditions will trigger an action such as producing a breach to show which device has misbehaved or initiating Antigena network controls.

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



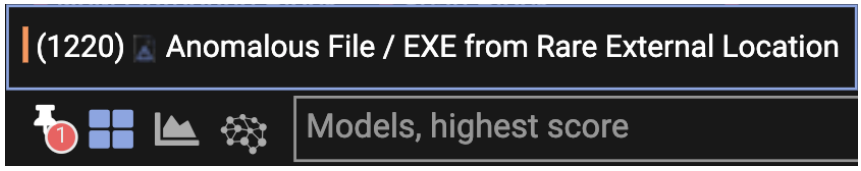
In the example above, a host downloaded a suspicious executable from a rare external location. The total size of the incoming packet and the filename is confirmed.

Notice the rare external domain score achieved 100 > 80. This means it exceeded the Model target of 90 % and so triggered the breach. Hovering over the vertical-colored bar for any breach will reveal the Threat score, which in this case was 61 %.

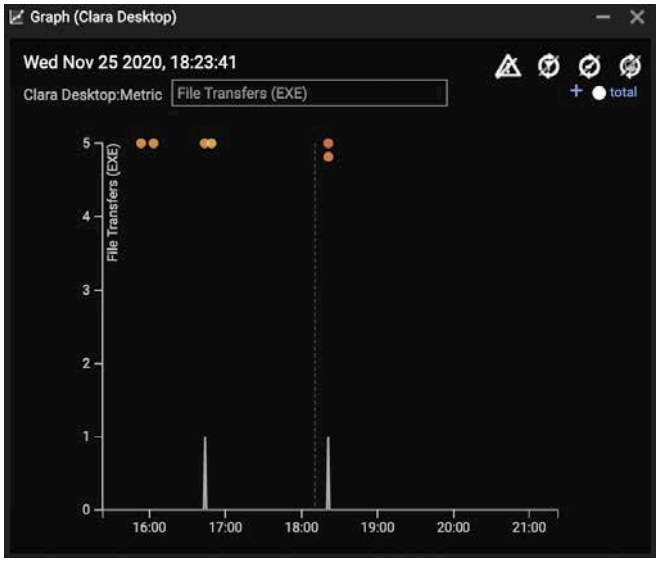


5. Next to the Model Breach ID, notice a pin icon. This icon allows Model Breaches to be pinned below the Threat Tray, allowing for further investigation at a later time.

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



6. Clicking the **red metric** in the Breach Log generates a graph of the metric over time.



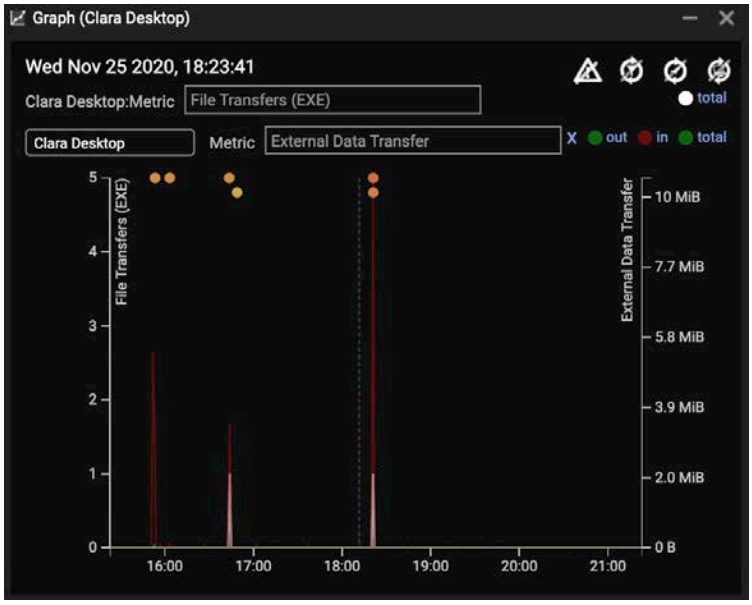
The dots represent the breaches with the color based on their score. Clicking on the graph refocuses the graph to the selected time. This can be a useful method to investigate how often these metric breaches have occurred in the past. An anomalous file or a download from a rare domain, may indicate suspicious activity.

7. Clicking under the x-axis allows you to change the timescale.

It can be helpful to set **1 week before** or **1 week either side** to better understand events for a device.

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

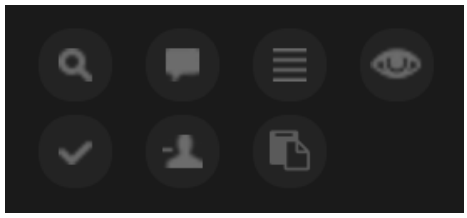
9. Append a corresponding metric to your graph. So, if the first metric is **File Transfers**, select **External Data Transfer**.



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

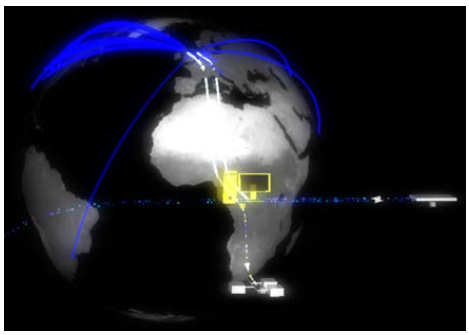
There are many other metrics available. For example, the **importance metrics** measure how abnormal the behavior is for a device. They are produced by the output of the classifier. It is important to review all this information to determine if the transaction is trustworthy.

10. **Review** the **Breach Log** again to view a series of buttons on the right-hand side.



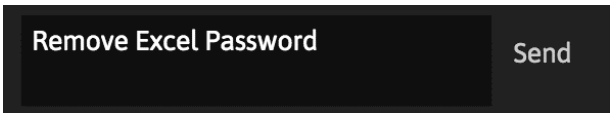
Click the **View this model breach in the visualizer** magnifying glass icon.

11. It is good practice to **increase the time duration** in the top right-hand corner in order to check what other devices the host has been in contact with over time using the Device View.

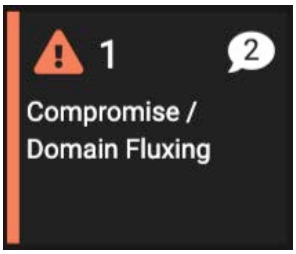


12. Adding comments lets analysts check what investigation work has previously occurred on the breach and allows them to communicate with each other.

Click the comment icon to open the comment window. Click **Send** to save your changes.

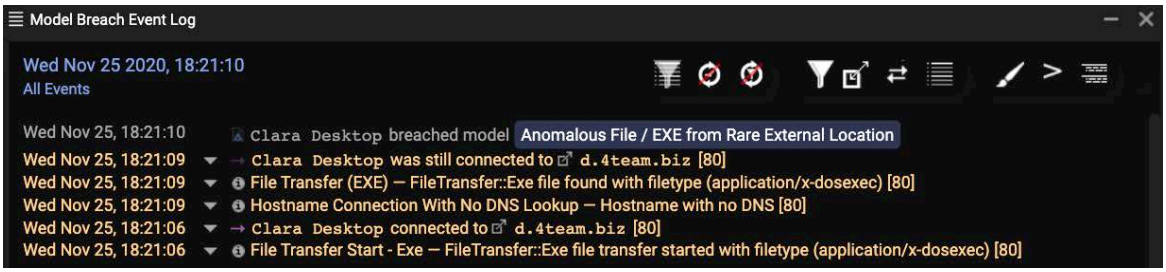


13. Comments are automatically appended to the Alert in the Threat Tray in a speech box.



Also note the comment icon has now changed to indicate the presence of a comment.

14. Click the **Model Breach Event Log** symbol to show all the connection and network event information relevant to a breach.



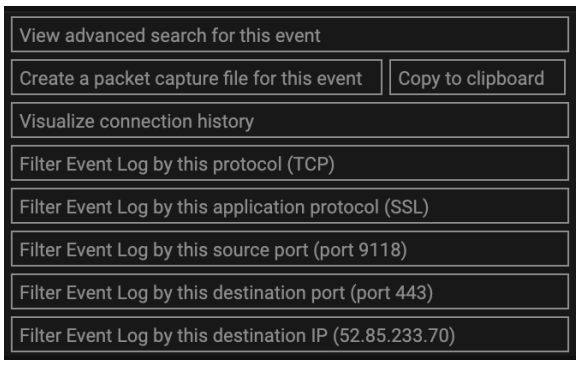
Notice the small arrow by many of the rows which indicate the flow of data.

- A **flashing** arrow signifies an ongoing connection.
- A pink right facing arrow signifies an outgoing connection.
- An orange left facing arrow signifies an incoming connection.
- A broken arrow with a cross through it signifies a failed connection.

15. A range of **filter icons** control how and what data is presented.

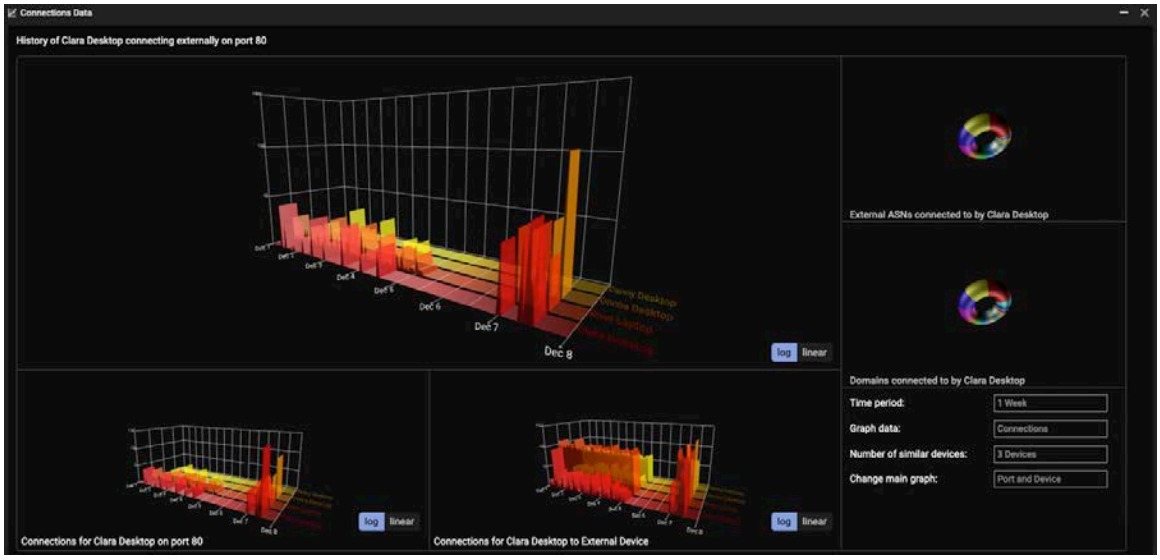
Review the options to restrict the log to internal or external events, hide duplicate connections, or only highlight events over a set size.

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



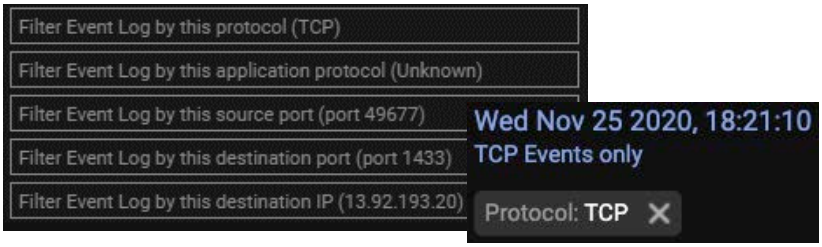
17. The **Copy to Clipboard** function is a useful way to copy the threat details, such as copying the IP or web address for further investigation.

18. Select the **Visualize connection history** option to open a new window displaying a three-dimensional view of a device's history.



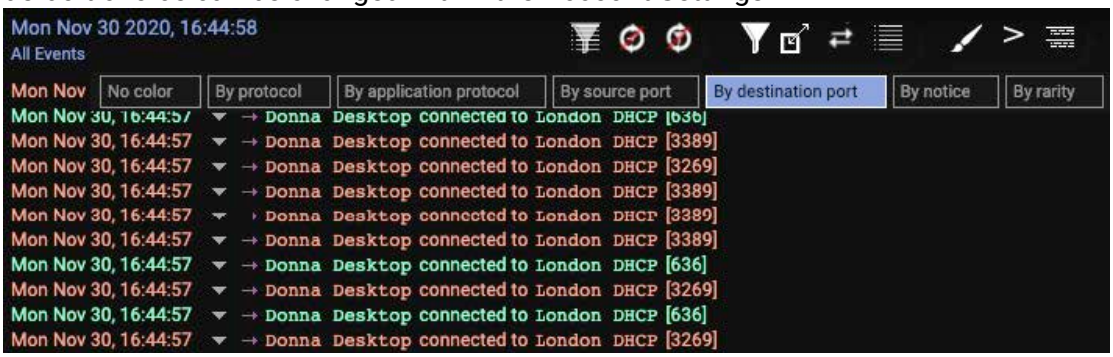
It includes ports and devices covering a duration of up to 4 weeks. Try changing the filter options in the bottom right to update the results.

19. Try the additional event log filters to quickly restrict the log to a specific **Protocol**, **Port** or **IP**.

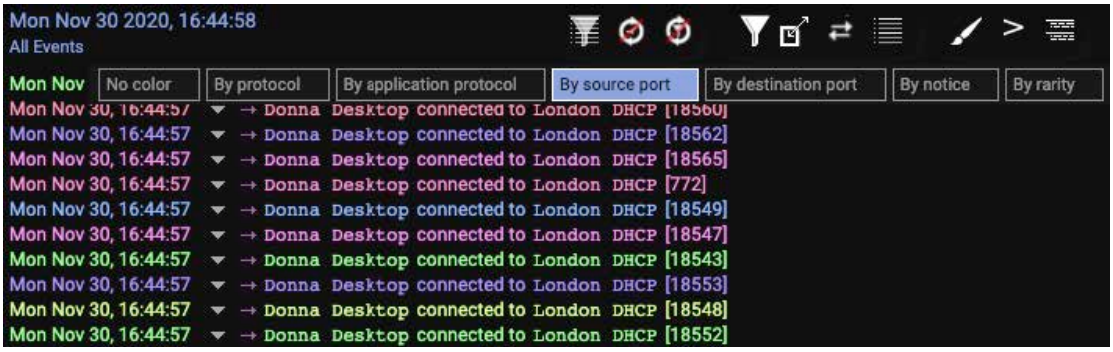


20. Go back to the **Model Breach Event Log** and click the paint brush icon to **Color-code events by their properties**.

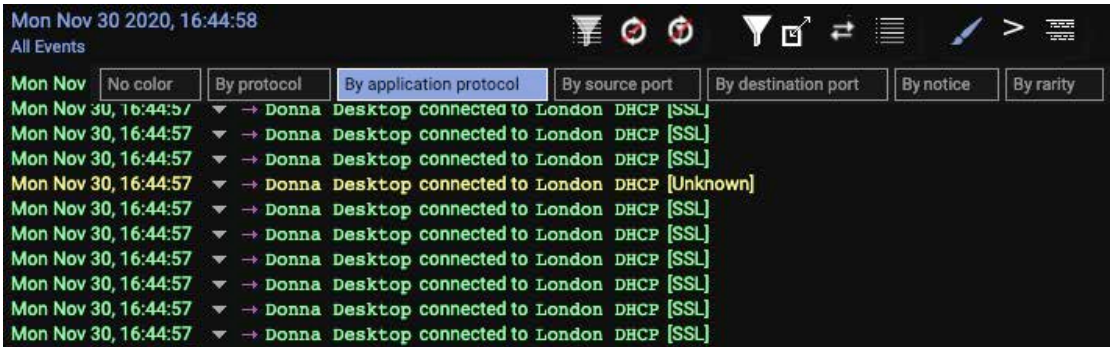
a. By default, it is set to **destination port**, which is a good way to quickly recognize and group activity. The destination port is a good indicator of the protocol, but this default choice can be changed within the Account Settings.



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

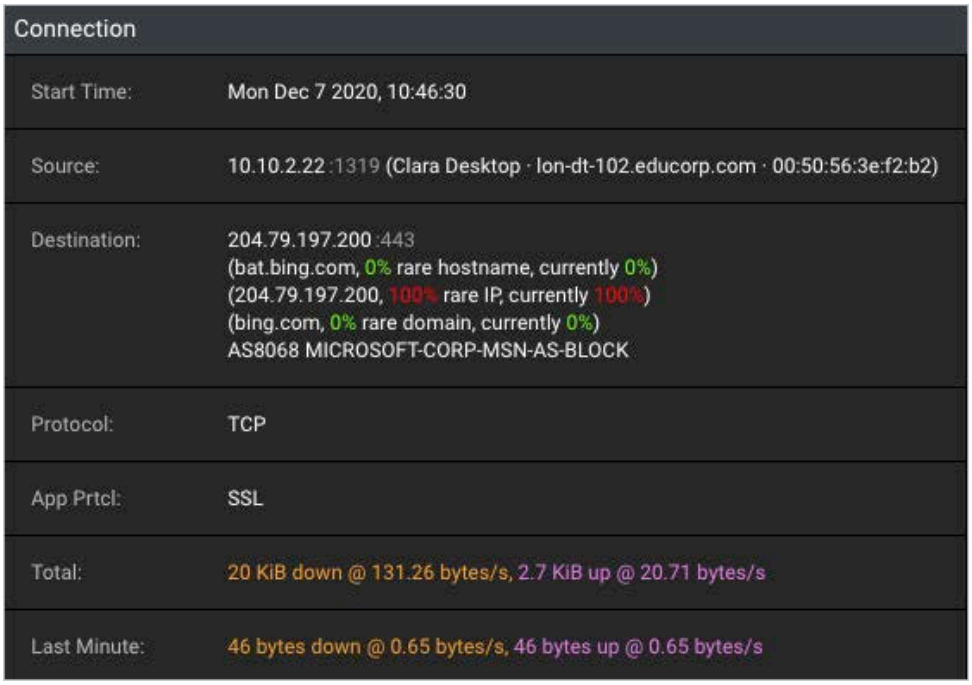


c. If ports are not easy to distinguish, coloring by application protocol may be of assistance.

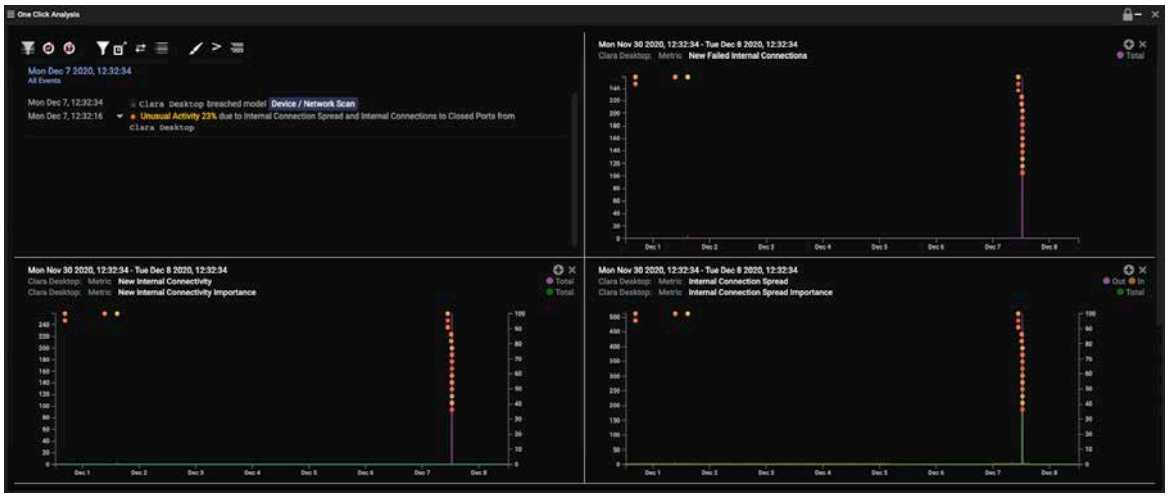


d. However, when reviewing several external communications to various destinations, it may be useful to color code by endpoint **rarity**, in order to quickly view this value instead of checking each individually. Coupling this with **External events only** can enhance this view even further to highlight external risks.

21. Hover over the arrows to reveal full information about the connection. The protocols, amount of data sent, and destination information are included.



22. Navigate back to the **Breach Log** window and click the **Analyze this Model Breach** icon.



This window includes graphs for relevant metrics, which facilitates detecting similar anomalies. With the executable download example above, it can assist answer the following questions:

- Has the same device or user downloaded other EXE files before?
- Who else has downloaded executables?
- Were they downloaded out of working hours?
- Is there any suspicious network behavior since the download, such as beaconing to an external destination?

23. The Threat Visualizer has the capability to view the stream of data coming from the network appliances in real time. This can be used not only to understand what data is *currently* being sent, but also to go back in time and replay a sequence of events. Within the **Time Selector** on the Home page, click the **play** button.

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

Note: *If you have multiple windows open, hold the shift button on your keyboard when closing the dialog window down to close them all down at the same time.*

24. When reviewing the Model Breach Event Log, it may be helpful to refer to the following **key ports**:

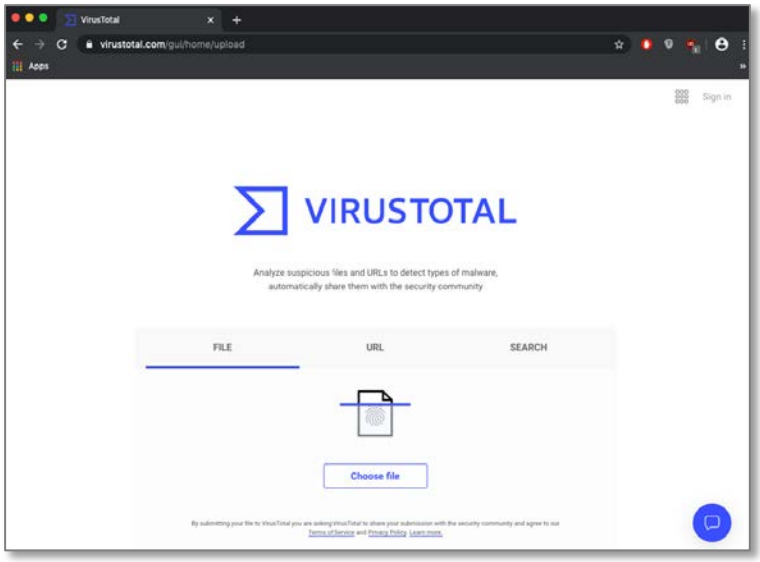
Port	Protocol	Description
20/21	TCP	File Transfer Protocol (FTP)
22	TCP/UDP	Secure Shell (SSH)
23	TCP/UDP	Telnet Port
25	TCP/UDP	Simple Mail Transfer Protocol (SMTP) for sending outgoing emails
53	TCP/UDP	DNS Server (DNS lookup uses UDP and Zone transfers use TCP)
67/68	UDP	Dynamic Host Configuration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

For researching other ports and their common uses, websites such as Speed Guide can be useful. Using the following URL structure, https://www.speedguide.net/port.php?port={INSERT PORT NUMBER}, to input a port number and search the database.

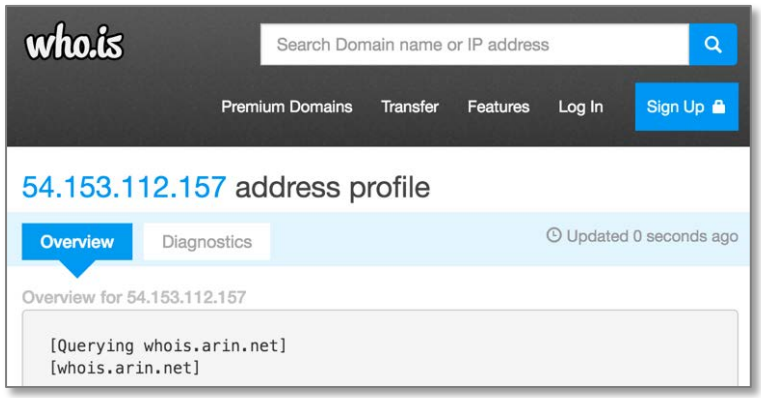
25. It is often useful to check suspicious files, URLs and IP addresses against internet databases. For example, https://www.virustotal.com can analyze files, URLs and IP addresses to check for known malware.

    It is also possible to search for a cryptographic hash (MD5, SHA1, etc.) to identify a file. This hash can be located in the Threat Visualizer's Advanced Search.

    Remember such web tools can be inaccurate and so it should be considered a first step in your analysis rather than a definitive result.

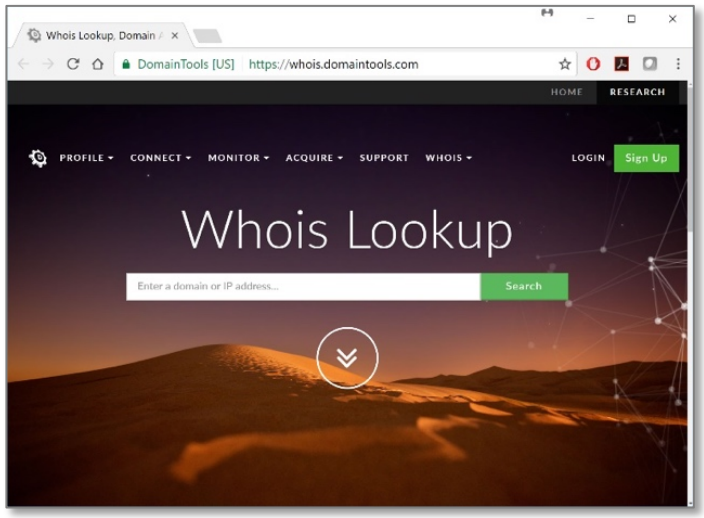


26. When investigating external IP addresses or domains, a **whois** service can provide owner details of a server. This can help determine if an address is a legitimate trustworthy host. Navigate to https://who.is/ and enter an IP address or domain name to gain more information.



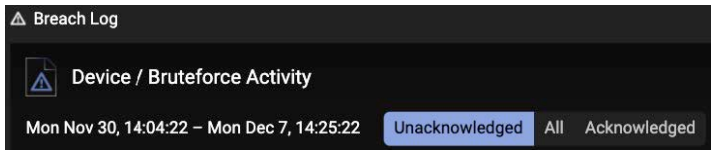
27. Domaintools, https://whois.domaintools.com, is also a popular tool to investigate domain information.

    Note, the date of registration is also important. Anything less than a few months old may be untrustworthy.

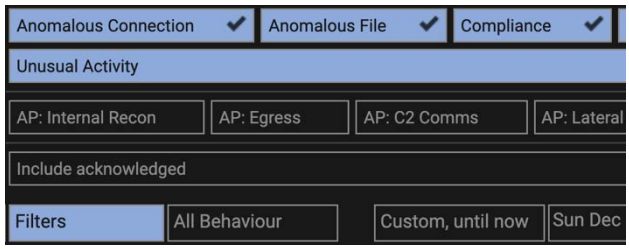


28. The **Breach Log** window includes the **Acknowledge this Model breach** function which will hide alerts from the list of Model breaches. When a breach is acknowledged (hidden), the number of breaches for each alert is automatically reduced by one.

29. Acknowledging a breach reveals additional options to toggle between **unacknowledged**, all and **acknowledged** breaches in the Breach Log.



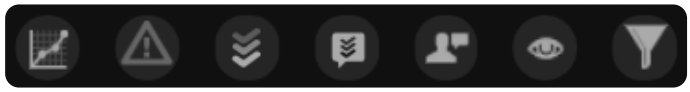
30. To show the alert again, click the Filters menu in the Threat Tray and select **Include acknowledged**. Options displayed in the Filters menu dynamically change based on the Model breaches in the Threat Tray. It is a useful method to quickly find breaches such as ones made by Antigena.



31. The **Ignore any future breaches** for the model on the host can be employed to prevent alerts which are deemed not relevant, such as false positives. This adds the device to the Model Exclude List for the selected Model.

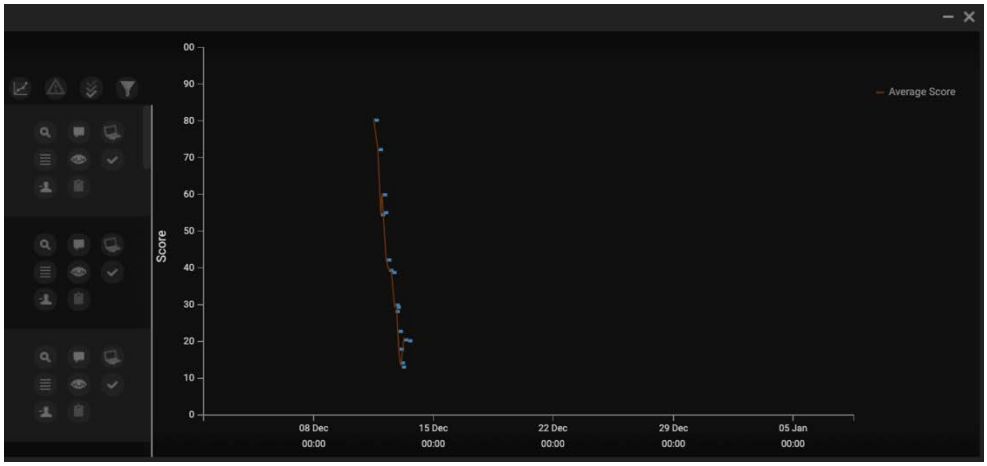
32. The final icon in the series of buttons on the right-hand side of the Breach Log is the **Copy to Clipboard** icon. This copies all the relevant breach information rather than just the connection information.

33. Review the icons located at the top right of the **Breach Log**.



34. Select the **View breaches graphically** icon. The graph plots all breaches over time, including the threat score. These can be obtained by hovering over each datapoint.

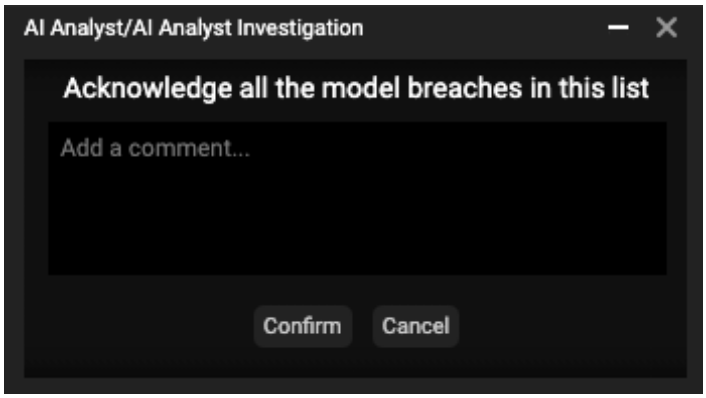
A laptop symbol will appear which reveals how often the selected device caused a breach.



35. **Click to view model** is the second icon. This will open the Model Editor which will be discussed later.

36. As described earlier, breaches can be acknowledged. The **Acknowledge all the model breaches in this list** icon can be used to quickly hide all previous breaches presented in the Breach Log without impacting on future alerts.

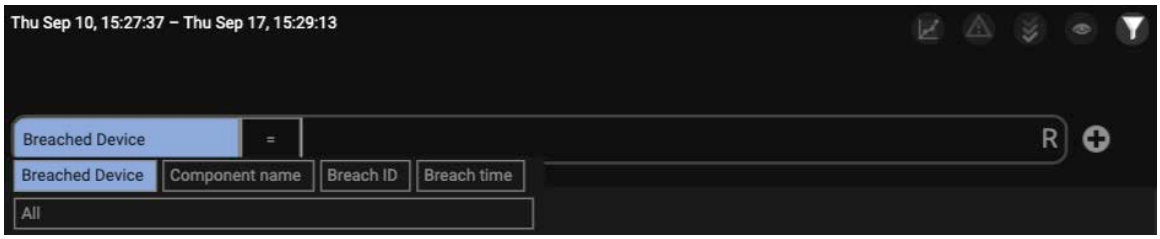
37. Taking this one step further, there is the option to **Acknowledge all the model breaches in this list and leave a comment**.



This feature is useful for marking breaches in bulk as read and providing a reason so that other users can see why they've been acknowledged.

38. Examine the next option, the **Only show model breaches being discussed** icon. This restricts alerts in the Breach Log to only show alerts where a comment has been added.

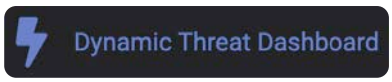
39. The final icon, **Add/ Remove custom filters**, will open a new dialogue at the top of the Breach Log. This will give a drop-down menu to aid the creation of filters.



5. Dynamic Threat Dashboard

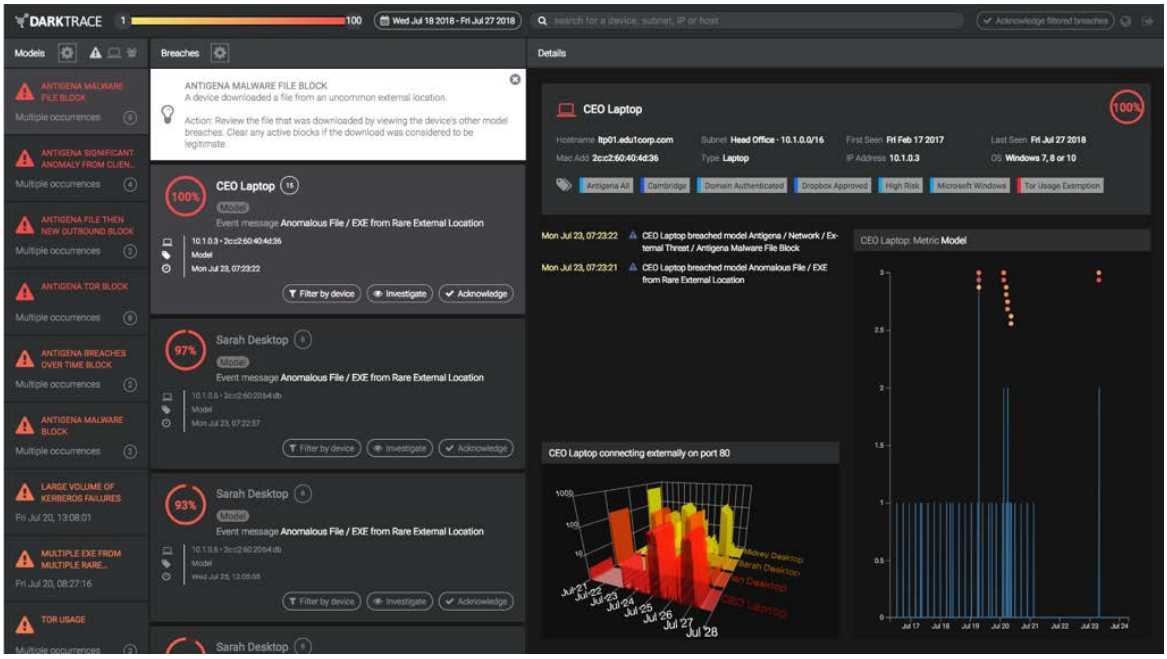
The **Dynamic Threat Dashboard** provides a simplified view of the Threat Visualizer to facilitate investigating breaches and performing actions on the results.

1. Select **Dynamic Threat Dashboard** under the **Menu** on the home page.



   It can also be accessed directly at: [https://<servername>/**threatdash**](https://<servername>/threatdash)

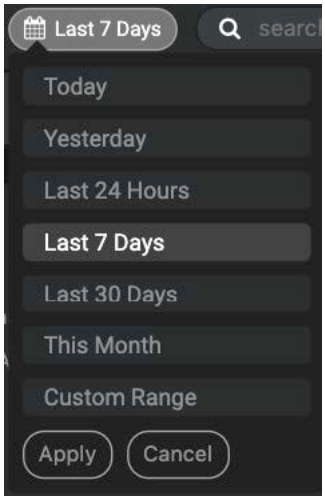
2. A new tab will open displaying a new **dashboard** interface. This is a simplified view of the Threat Visualizer and can make it quick and easy to process model breaches.



3. The breaches displayed in this dashboard can be narrowed down using the **sensitivity slider**.

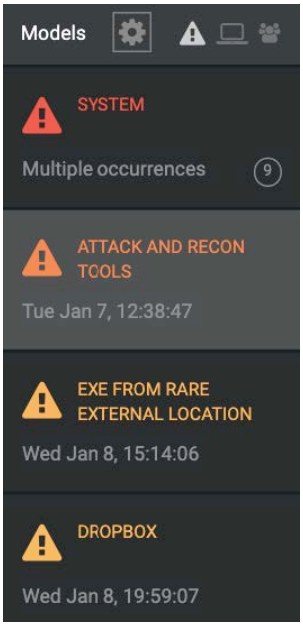
4. Just as with the Threat Visualizer, the alerts in the Dynamic Threat Dashboard can also be displayed for different time periods.

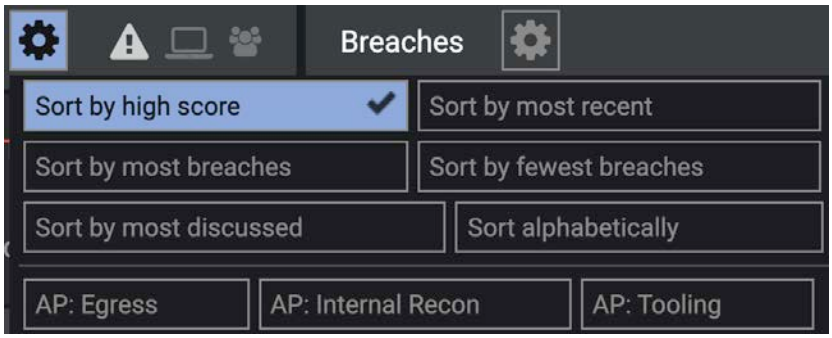
   Click Last 7 Days to **change the time period**.



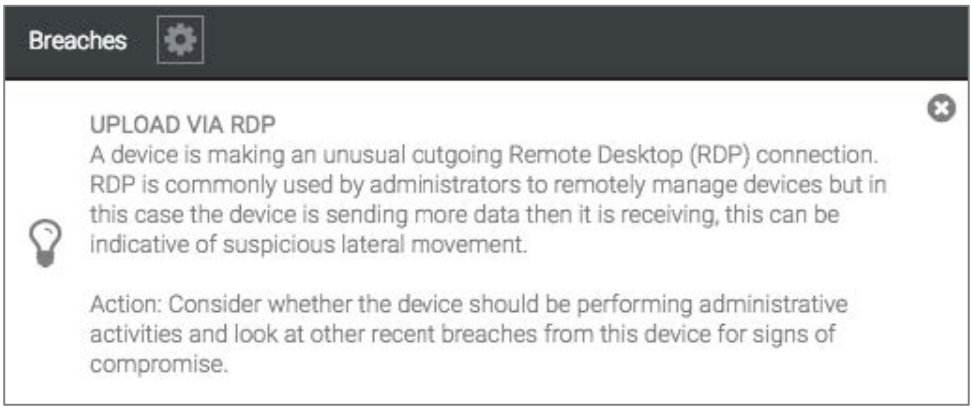
5. The top left of the display is similar to **sorting Model Breaches**.

   It can be sorted using the options presented when clicking the **cog icon**. Alternatively, the alerts be grouped per **Model**, **Device**, or **User**, as indicated by the three icons to the right.

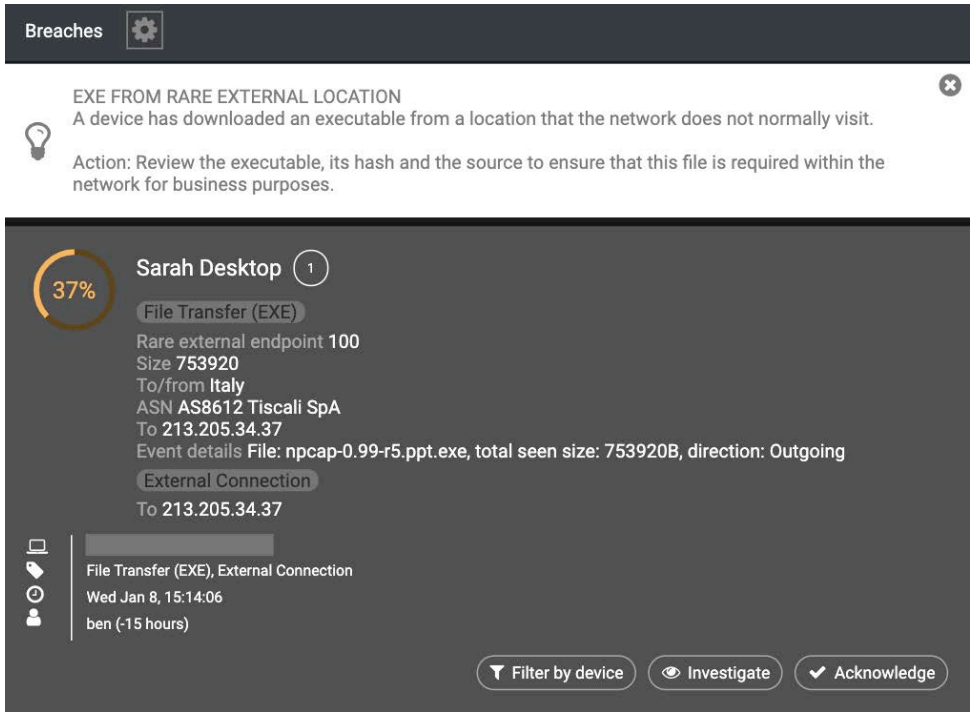




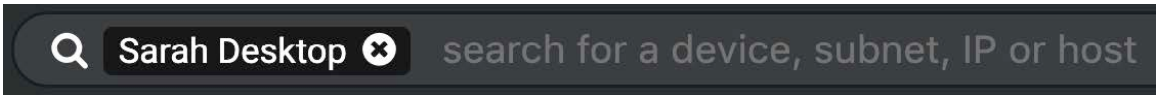
6. As Model breaches are selected, the **Model description** is displayed below the Breaches header.



7. In the example to the right, the EXE from Rare External Location Model has been selected, and only **related breaches** are displayed underneath.



8. Clicking the **Filter by device** button appends the selected device to the search bar. This will restrict all details on the Dynamic Threat Dashboard to that device.

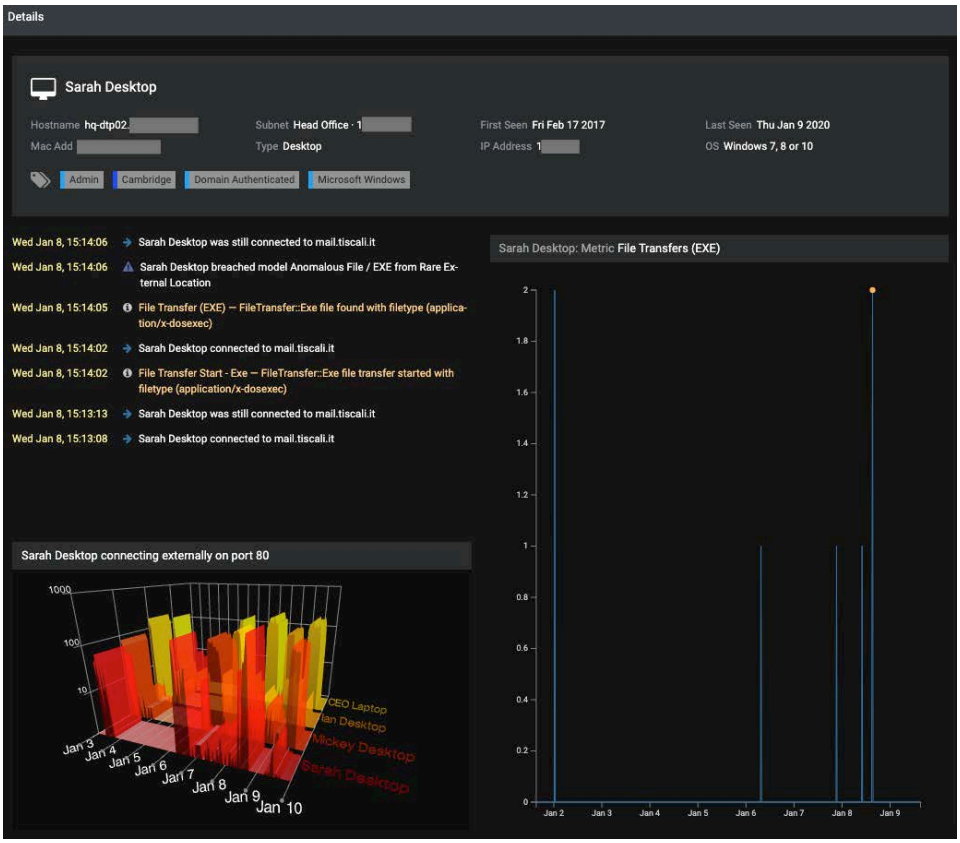


   a. Once items have been added as filters, all filtered beaches can be acknowledged in one go by clicking the Acknowledge filtered breaches in the top right of the screen.

9. In a similar fashion to the Threat Visualizer, breaches can be **acknowledged** directly through this interface.

10. A breach can be investigated further in the regular Threat Visualizer by clicking the **investigate** icon.

11. The **Details** pane will automatically update to display individual device information as you click on breach results. The Breach Log, Connection History, device details, and graph are all displayed together.



12. To return to the **Threat Visualizer** interface directly from the Dashboard, click the globe icon in the top right-hand corner of the screen.

13. Similarly, to **exit the whole interface**, including the Threat Visualizer, click the icon in the very top right-hand corner. This will completely log the user out of Darktrace.

6. Learning Outcomes

Thank you for completing the Part 1 of the Threat Visualizer course. We hope this has familiarized you with a variety of aspects within your deployment.

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

☐	**I understand Darktrace solutions**
☐	**I am able to navigate the Threat Visualizer Interface**
☐	**I know how to obtain information about devices on the network**
☐	**I can successfully review Model Breaches**

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

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

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

7. Cheat Sheet

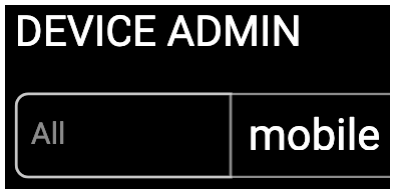
Navigation Exercise

a. Identify your own device on the network.

With a minimum of three characters, begin typing your device hostname, IP address or your user credential into the Omnisearch bar and select your device from the list of suggested results.

b. Can you identify all mobile devices?

Type "mobile" into the Omnisearch bar or Device Admin page.



c. Set the threat score filter to 50%.

Use the sensitivity slider to reflect a minimum Model Breach score of 50%.

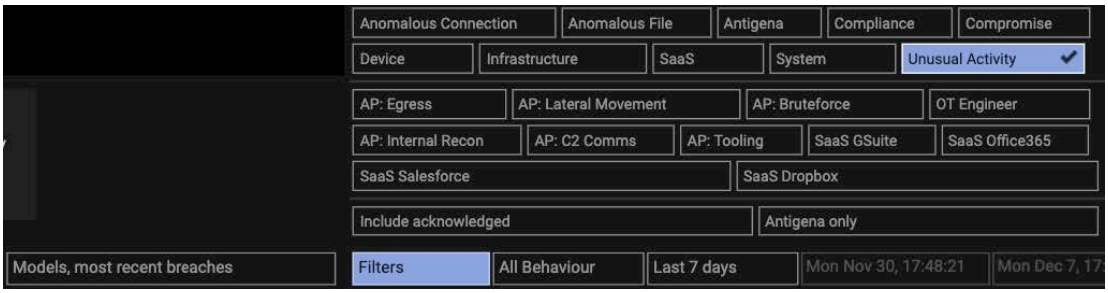
d. Which device has triggered the most alerts in the last 7 days?

Set the time period to the Last 7 days and use the "Devices, most breaches" Threat Tray sorting method.

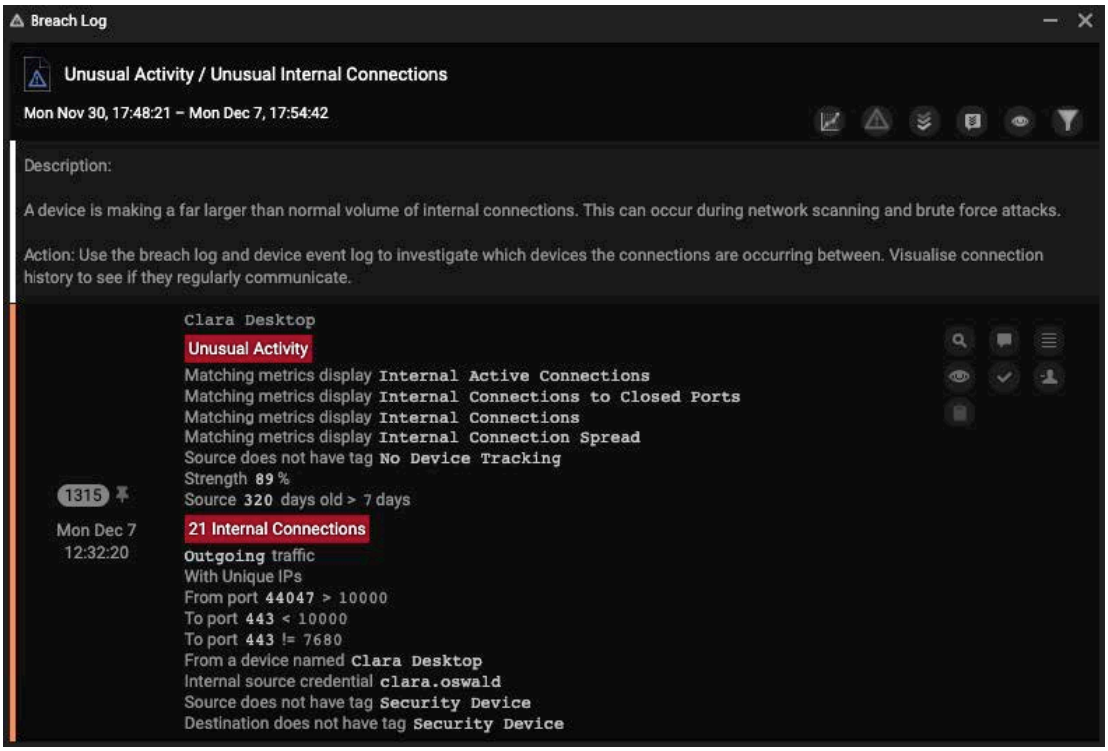
Locate the device presented on the left-hand side of the Threat Tray.

e. What was the last Unusual Activity Model Breach?

Set the Threat Tray to be sorted by Models, most recent breaches. Within the Filters menu, shift and click the Unusual Activity filter to deselect the rest. The breach on the left-hand side of the Threat Tray is the most recent Unusual Activity Model Breach.



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



Any of the following:

- ***Click on the Model Breach in the Threat Tray to review the Breach Log***
- ***Visualize the device in the Device View using the magnifying glass and see what internal and external connections it made during the time frame of the breach***
- ***Look at the Model Breach and Device Event Logs.***
- ***Use One Click Analysis or visualize the Connection History.***