DARKTRACE

THREAT VISUALIZER PART 2 – INVESTIGATION

Threat Visualizer Part 2 – Investigation
Manual v2.0.0 – Darktrace v5

Table of Contents

1. Learning Objectives

This course provides a detailed understanding of the Threat Visualizer interface. It is designed for a wide audience: IT Security Managers, IT Security Architects, and Cyber Security Analysts.

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

+ **Appreciate the benefits of AI Analyst**
+ **Understand the uses for Tags and be able to apply them to Devices**
+ **Perform basic queries in Advanced Search**
+ **Create a packet capture and perform packet inspection**
+ **Generate reports of network activity**
+ **Follow the Analyst Workflow**
+ **Be aware of additional Darktrace offerings**

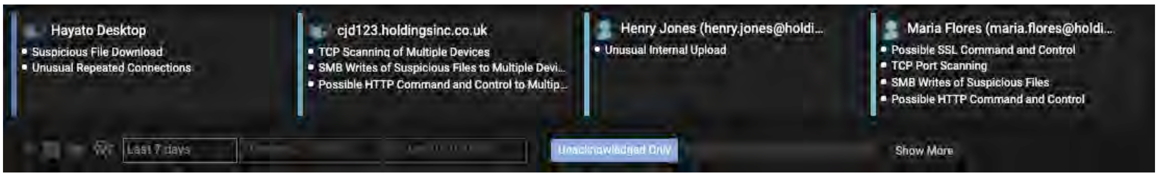
Before embarking on this course, it is imperative that you have attended Threat Visualizer Part 1 – Familiarization.

2. AI Analyst

The Darktrace Cyber AI Analyst (AIA) investigates, analyzes and triages threats seen within your Darktrace environment and forms potentially interesting and unusual incidents centered around a device. Incidents involving multiple devices are classified as 'cross-network' incidents. By learning from the millions of interactions between Darktrace's expert analysts and the Enterprise Immune System, the Cyber AI Analyst combines human expertise with the consistency, speed, and scalability of AI. Not only does AIA perform autonomous, unprompted investigations, it is also available on demand for a selected device.

AI Analyst Incidents

1. The **Cyber AI Analyst Incident Tray** can be found by clicking the **brain icon** in the lower left corner, below the Threat Tray.



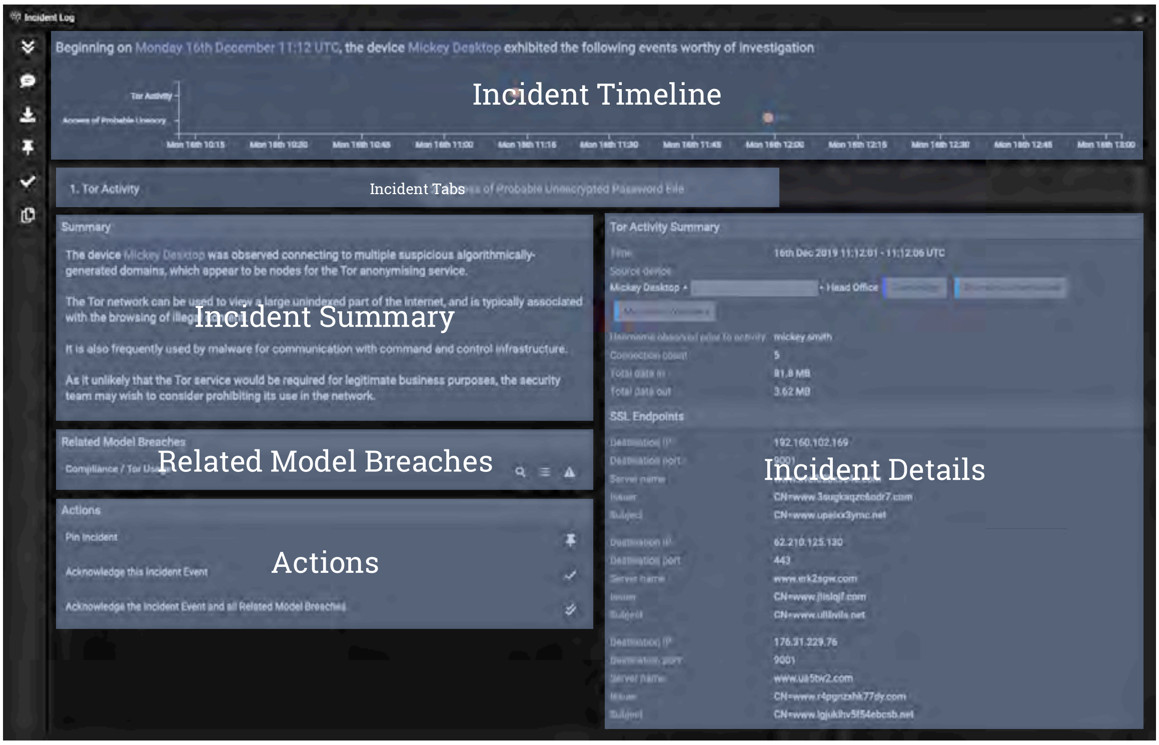
Hayato Desktop
- Suspicious File Download
- Unusual Repeated Connections

cjd123.holdingsinc.co.uk
- TCP Scanning of Multiple Devices
- SMB Writes of Suspicious Files to Multiple Devi...
- Possible HTTP Command and Control to Multip...

Henry Jones (henry.jones@holdi...
- Unusual Internal Upload

Maria Flores (maria.flores@holdi...
- Possible SSL Command and Control
- TCP Port Scanning
- SMB Writes of Suspicious Files
- Possible HTTP Command and Control

2. Click on any Cyber AI Analyst incident to open the **Incident Log** window.



Beginning on Monday 16th December 11:12 UTC, the device Mickey Desktop exhibited the following events worthy of investigation

1. Tor Activity | ...ss of Probable Unencrypted Password File

Summary

The device Mickey Desktop was observed connecting to multiple suspicious algorithmically-generated domains, which appear to be nodes for the Tor anonymising service.

The Tor network can be used to view a large unindexed part of the internet, and is typically associated with the browsing of illeg...

It is also frequently used by malware for communication with command and control infrastructure.

As it unlikely that the Tor service would be required for legitimate business purposes, the security team may wish to consider prohibiting its use in the network.

Related Model Breaches

Compliance / Tor Us...

Actions

Pin Incident

Acknowledge this Incident Event

Acknowledge the Incident Event and all Related Model Breaches

Tor Activity Summary

Time: 16th Dec 2019 11:12:01 - 11:12:06 UTC

Source device

Mickey Desktop + Head Office

Usernames observed prior to activity: mickey.smith

Connection count: 5

Total data in: 81.8 MB

Total data out: 3.62 MB

SSL Endpoints

Destination IP: 192.160.102.169

Destination port: 9001

Issuer: CN=www.3sugkaqzc6odr7.com

Subject: CN=www.upeixx3ymc.net

Destination IP: 62.210.125.130

Destination port: 443

Server name: www.erk2sgw.com

Issuer: CN=www.jlislqjf.com

Subject: CN=www.ullbvils.net

Destination IP: 176.31.229.76

Destination port: 9001

Server name: www.ua5tw2.com

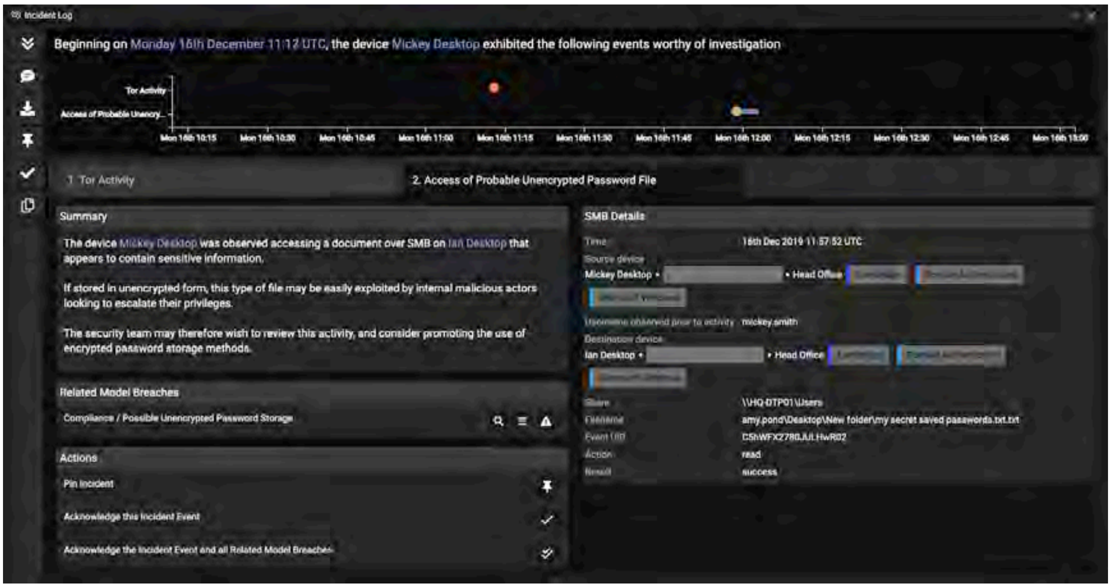
Issuer: CN=www.r4pgnzxhk77dy.com

Subject: CN=www.lgjukihv5f54ebcsb.net

This window will display:

a. **An Incident Timeline.** Model Breaches relating to the Incident Tabs are displayed as dots, where their color indicates severity. The currently selected event will be highlighted in blue. A bar in the same row as an incident represents associated activity. However, if there is a green bar present on the timeline, this represents Antigena activity.

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



Beginning on Monday 16th December 11:12 UTC, the device Mickey Desktop exhibited the following events worthy of investigation

1 Tor Activity

2. Access of Probable Unencrypted Password File

Summary

The device Mickey Desktop was observed accessing a document over SMB on Ian Desktop that appears to contain sensitive information.

If stored in unencrypted form, this type of file may be easily exploited by internal malicious actors looking to escalate their privileges.

The security team may therefore wish to review this activity, and consider promoting the use of encrypted password storage methods.

Related Model Breaches

Compliance / Possible Unencrypted Password Storage

Actions

Pin Incident

Acknowledge this Incident Event

Acknowledge the Incident Event and all Related Model Breaches

SMB Details

Time 16th Dec 2019 11:57:52 UTC

Source device

Mickey Desktop • Head Office

Username observed prior to activity mickey.smith

Destination device

Ian Desktop • Head Office

Share \\HQ-DTP01\Users

Filename amy.pond\Desktop\New folder\my secret saved passwords.txt.txt

Event UID C5hWFX2780JULHwR02

Action read

Result success

c. **The Incident Summary.** A high level event outline is given in the left panel explaining the observed activity, possible implications and a suggested action.

d. **Related Model Breaches.** Any related Model Breaches will be listed here.

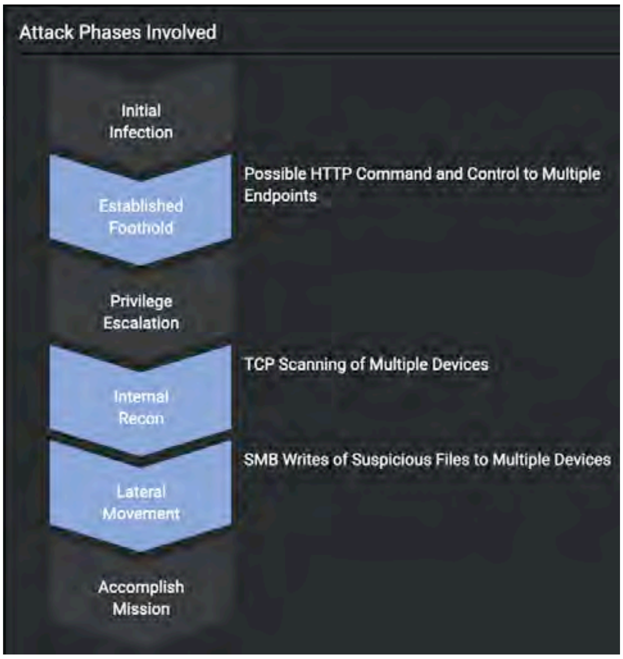
These can be centered on in the Threat Visualizer using the magnifying glass. The associated Model Breach Event Log and Breach Log can be viewed using the other two symbols respectively.

e. **Actions.** AI Analyst incidents can be pinned or acknowledged. All related Model Breaches can also be acknowledged from here.

f. **Incident Details.** The full technical details associated with each event are displayed in the left of the Incident Log.

3. Click the **View Incident attack phases** button depicted by the downwards arrows to open a new display.

   This will highlight which possible attack phases have been detected during this incident.

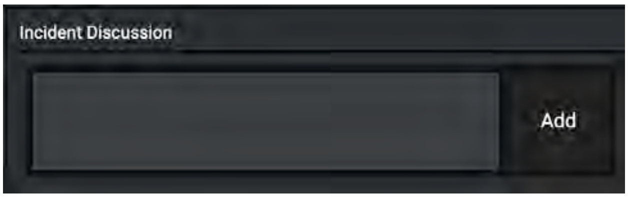


Attack Phases Involved

Initial Infection
Established Foothold
Possible HTTP Command and Control to Multiple Endpoints
Privilege Escalation
Internal Recon
TCP Scanning of Multiple Devices
Lateral Movement
SMB Writes of Suspicious Files to Multiple Devices
Accomplish Mission

4. To comment on an incident or view any existing incident discussion, click the speech bubble icon, **View incident discussion**.

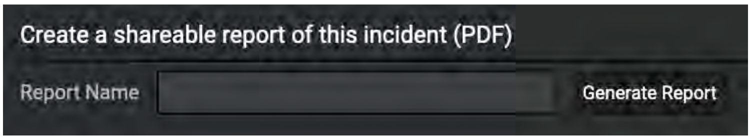
   Type in the box and click Add to comment on the incident.



Incident Discussion

5. To create a report of this particular incident, click the download icon which reads **Download Incident as PDF** when hovering over it.

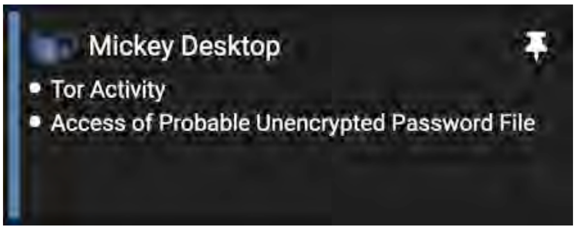
   Give the report a name and click **Generate Report.**



Create a shareable report of this incident (PDF)

6. To pin the incident, click the **Pin Incident** icon.

   The incident in the Incident Tray will also have a pin icon displayed to demonstrate which AIA incidents have been pinned.



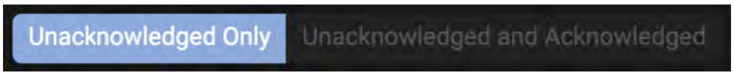
Mickey Desktop

- Tor Activity
- Access of Probable Unencrypted Password File

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

7. Incidents can be acknowledged using **the Acknowledge Incident** tick icon.

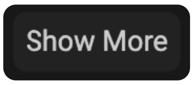
   Incidents can then be filtered in the tray on **Unacknowledged Only** or **Unacknowledged and Acknowledged** incidents.



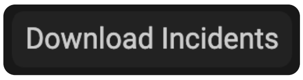
8. Click **Copy Incident URL** to clipboard. The URL will be of the form:

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

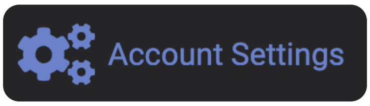
9. Sometimes, AI Analyst will produce a larger number of incidents, but only show a selection of these. Click Show More at the bottom of the tray to **display further incidents** for review.



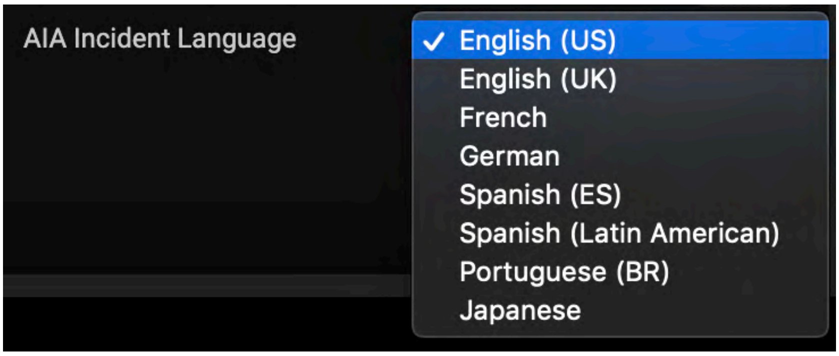
10. While individual incidents can be downloaded from the Incident Log, all the incidents can be downloaded from the Incident Tray by clicking **Download Incidents**.



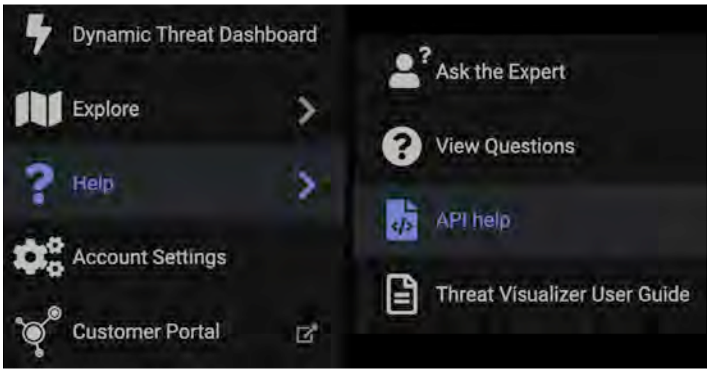
11. To **change the language** of the AIA incidents and reports, go to the main menu and choose Account Settings.



The last option, AIA Incident Language, has a drop-down menu with multiple options.



12. Finally, AI Analyst Incidents can also be viewed in a different format via the **API**. Such information may be useful for exporting.



a. The first endpoint presents **all AI Analyst events**.

In a browser, navigate to https://<hostname>/aianalyst/incidents to view all events on one page.

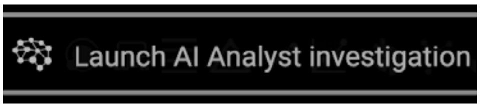
b. The second endpoint will restrict the results to show a chosen AI Analyst incident, based on its ID, to view any **comments**.

In a browser, the endpoint format will be the following:
https://<hostname>/aianalyst/incident/comments?incident_id=<id-string>

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

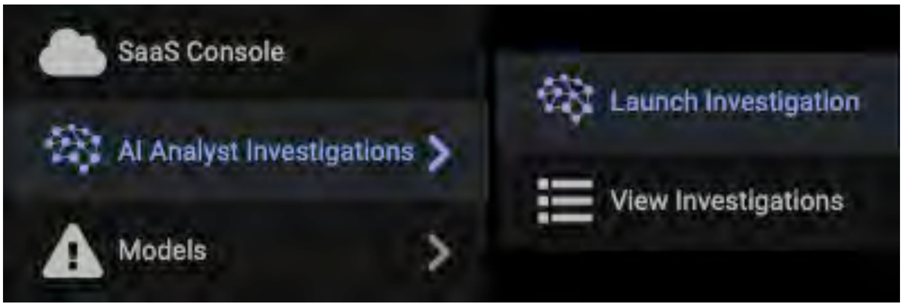
AI Analyst On-Demand

1. The first way of prompting an AIA investigation is to populate a device in the search bar and select the **brain icon**. This opens a dialog which prepopulates the device name and the current time.

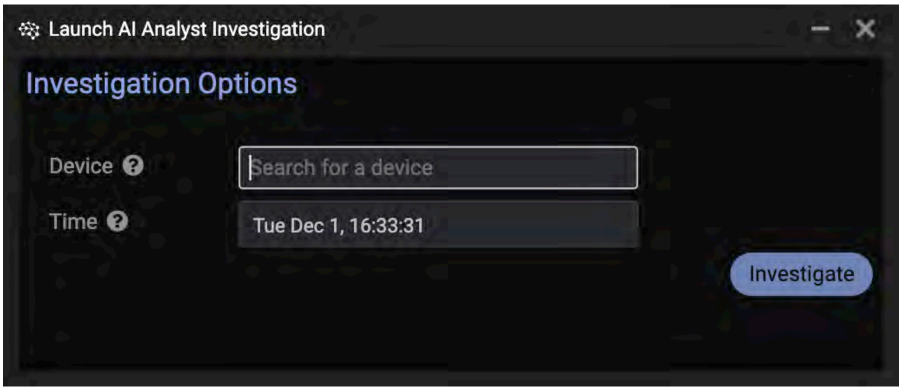


2. Alternatively, open the **main menu** using the icon in the top left of the interface.

3. Navigate to the AI Analyst Investigations and select **Launch Investigation**.



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

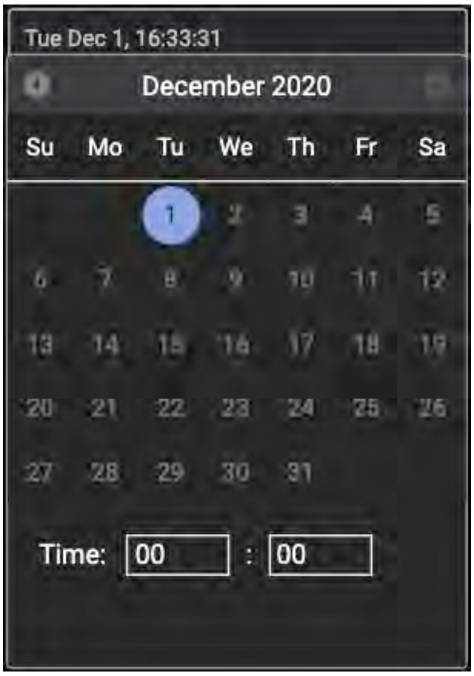


Device: Search for a device

Time: Tue Dec 1, 16:33:31

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

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



Tue Dec 1, 16:33:31

December 2020

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

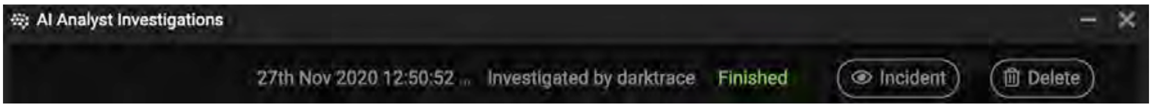
Time: 00 : 00

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

5. Once analysis is complete, return to the main menu, select AI Analyst Investigations and click on **View Investigations**.

   This will open a list of previously performed on-demand AIA investigations to view.

6. The **device name**, **date** of analysis, **who** the device was investigated by and the **status** of the incident can be visible in the window. A successful investigation will show Pending, Processing and the Finished.



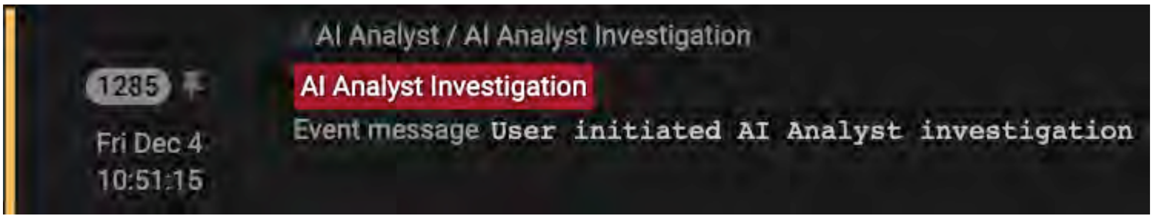
AI Analyst Investigations

27th Nov 2020 12:50:52 ... Investigated by darktrace Finished

7. If AIA does not find anything of interest, it will show a **No incident found** message.

No incident found

8. As a result of performing an on-demand analysis, a **Model Breach** will appear in the device's **Breach Log**.



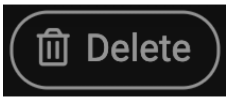
AI Analyst / AI Analyst Investigation

AI Analyst Investigation

Event message `User initiated AI Analyst investigation`

9. However, if on demand analysis finds something interesting, click **Incident** to open up an AIA window including all the same features which can be obtained from the AIA Incident Tray.

10. If the incident is no longer relevant or required, it can be removed from the AI Analyst Investigations list by clicking **Delete**.

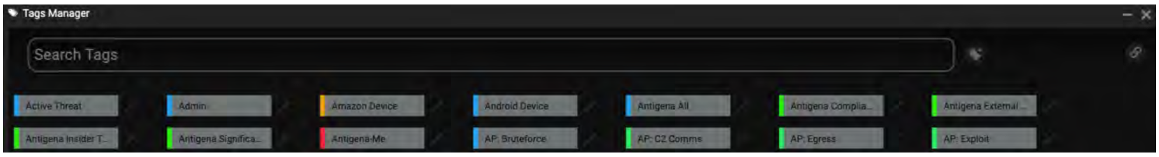


3. Tags

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

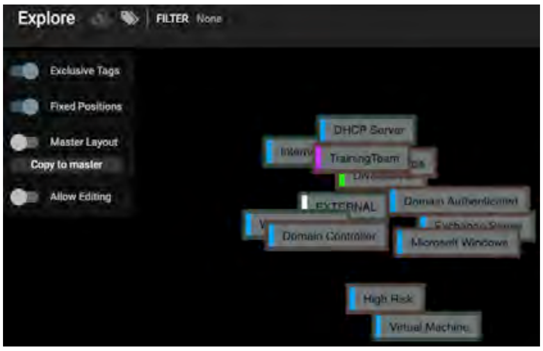
1. On the Threat Visualizer home screen, click **Menu** and select the **Tags** icon.

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



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

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



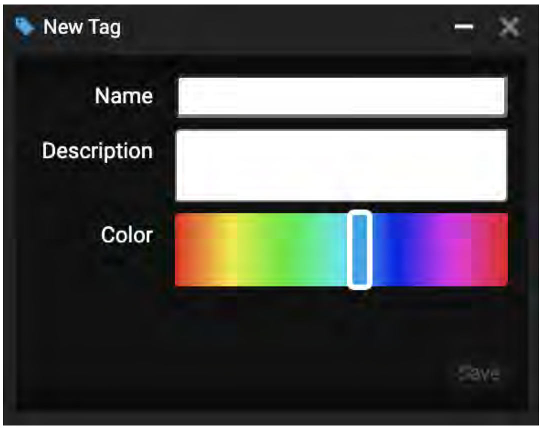
3. Create a new Tag by clicking the **Add New Tag** symbol.

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

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

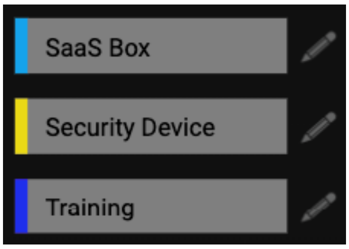
   c. Selecting a **color** assists in identifying the tag when assigned to a device.

   d. Click **Save**.

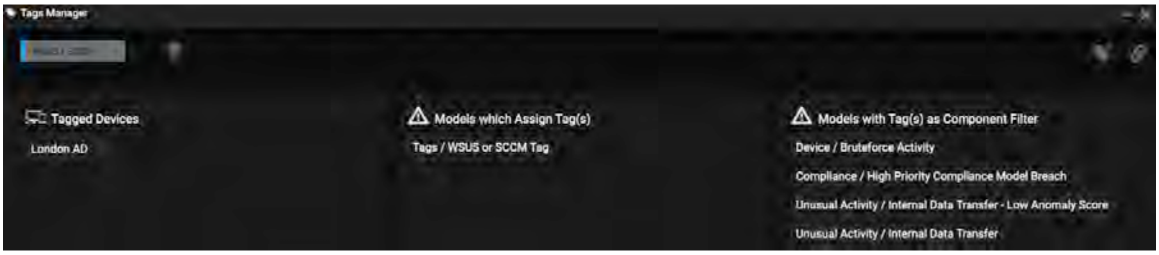


4. The new Tag will appear on the **Tags Manager** dialog window.

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



5. 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**.



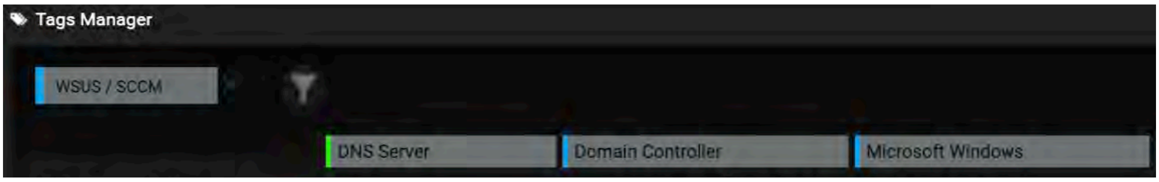
Tags Manager

Tagged Devices
London AD

Models which Assign Tag(s)
Tags / WSUS or SCCM Tag

Models with Tag(s) as Component Filter
Device / Bruteforce Activity
Compliance / High Priority Compliance Model Breach
Unusual Activity / Internal Data Transfer - Low Anomaly Score
Unusual Activity / Internal Data Transfer

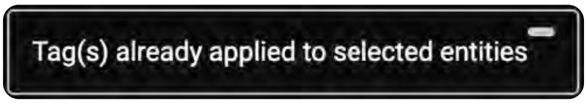
6. Within this Tags Manager view, there may be the option to **add further filters** to narrow down the results displayed. Here, more Tags can be filtered/applied to the Tags Manager to see which devices are tagged and which Models are referred to.



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

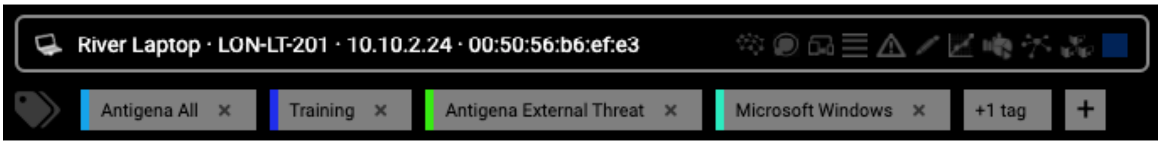
Click the **Add selected tags to current device** button. Refreshing the Tag Manager pane will reveal the device hostname within the **Tagged Objects** pane.

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



Tag(s) already applied to selected entities

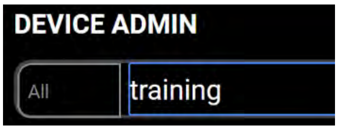
8. When a device is selected, the **Tags are displayed below the Omnisearch bar**.



River Laptop · LON-LT-201 · 10.10.2.24 · 00:50:56:b6:ef:e3

Note: *The plus button is another method to quickly append new tags to a device.*

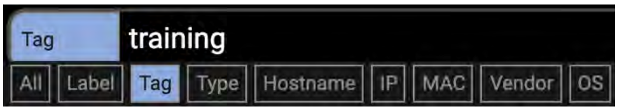
9. Entering a Tag in the search bar of **Device Admin** will list all devices associated with the Tag. This can be a quick way to locate devices on the network.



DEVICE ADMIN

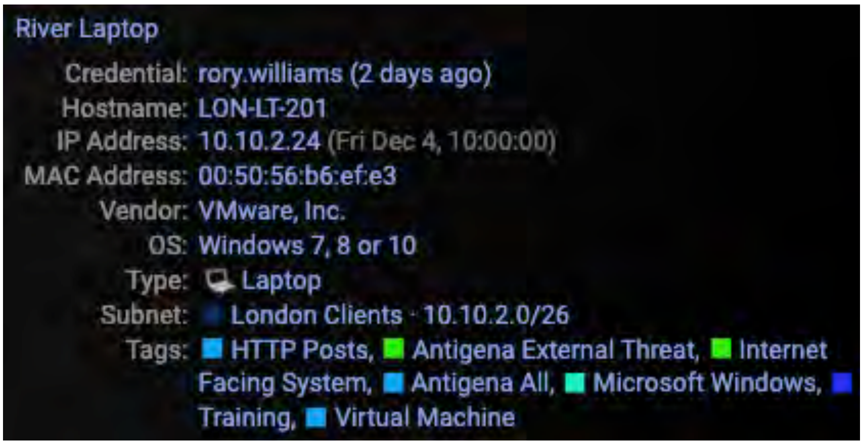
All | training

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



Tag | training

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

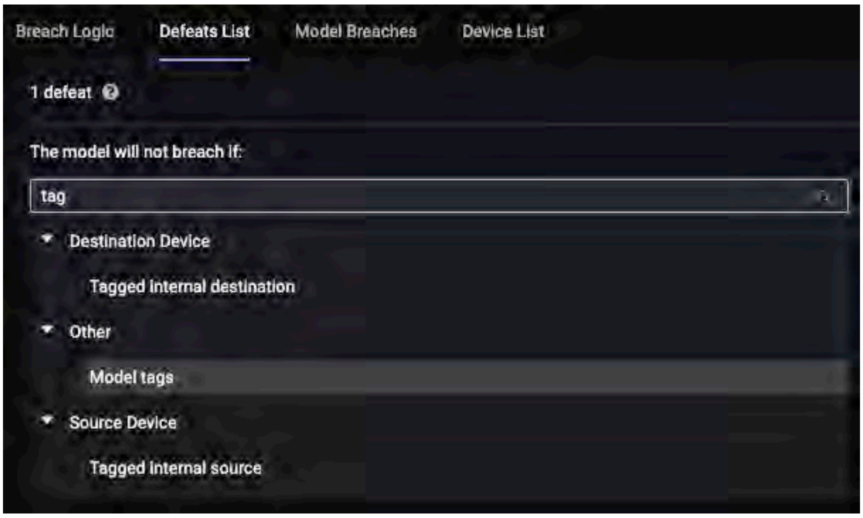


River Laptop

Credential: rory.williams (2 days ago)
Hostname: LON-LT-201
IP Address: 10.10.2.24 (Fri Dec 4, 10:00:00)
MAC Address: 00:50:56:b6:ef:e3
Vendor: VMware, Inc.
OS: Windows 7, 8 or 10
Type: Laptop
Subnet: London Clients · 10.10.2.0/26
Tags: 🟦 HTTP Posts, 🟩 Antigena External Threat, 🟩 Internet Facing System, 🟦 Antigena All, 🟩 Microsoft Windows, 🟦 Training, 🟦 Virtual Machine

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

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



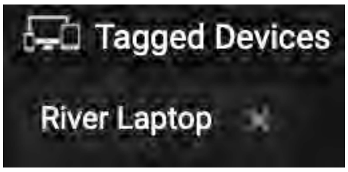
1 defeat

The model will not breach if:

tag

Destination Device
Tagged internal destination
Other
Model tags
Source Device
Tagged internal source

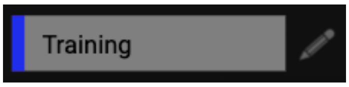
12. One method of removing a tag from a device is to click the **X** in the **Tagged Devices** pane for a selected tag.



Tagged Devices

River Laptop ✕

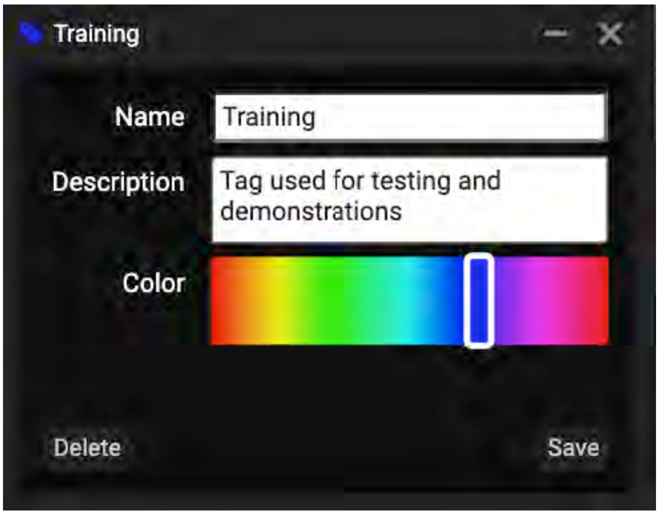
13. Deleting a tag will automatically untag all the devices which share the deleted tag. In the **Tags Manager** dialog window, click the **pencil symbol** by your training tag.



Training

14. Click the **Delete** button in the bottom left corner of the Tag window to permanently remove the tag.

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



Training

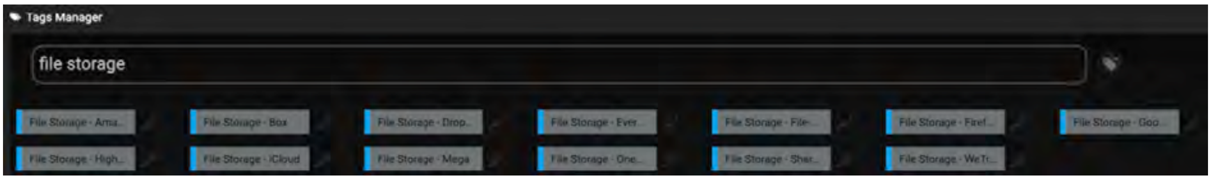
Name: Training
Description: Tag used for testing and demonstrations
Color

Tags Use Case

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

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

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



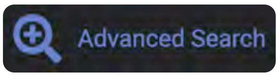
These Tags are also a great way of being able to filter the Device Admin page, allowing you to review the use of these services for compliance without being alerted.

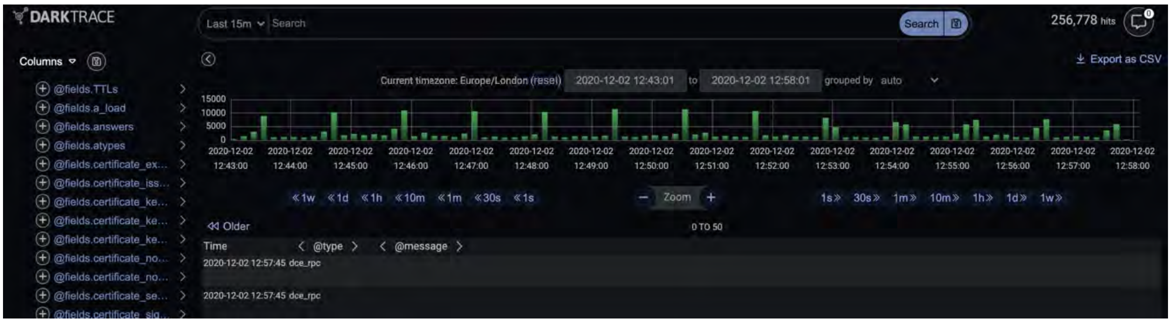
This range of Tags are applied by File Storage Models but, as Models are entirely customizable, the Models can be edited to monitor different solutions using various methods. This could include rolling Models back to previous versions or turning off auto updates for particular services.

4. Advanced Search Fundamentals

Darktrace captures logs for all network traffic. Each IP connection generates a "conn event". Each "conn event" has a corresponding unique identifier (UID). This identifier is also present in any further events generated in the process of deep packet inspection. The Advanced Search component contains different functionalities and data in addition to the Threat Visualizers Breach Event Log.

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



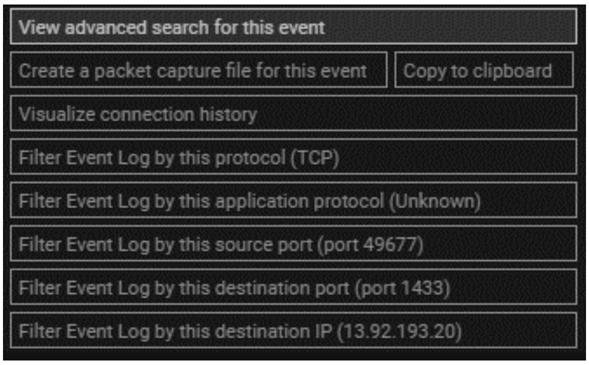

DARKTRACE
Last 15m
Search
Search
256,778 hits
Columns
Export as CSV
@fields.TTLs
@fields.a_load
@fields.answers
@fields.atypes
@fields.certificate_ex...
@fields.certificate_iss...
@fields.certificate_ke...
@fields.certificate_ke...
@fields.certificate_ke...
@fields.certificate_no...
@fields.certificate_no...
@fields.certificate_se...
@fields.certificate_sig...
Current timezone: Europe/London (reset)
2020-12-02 12:43:01
to
2020-12-02 12:58:01
grouped by
auto
15000
10000
5000
0
«1w «1d «1h «10m «1m «30s «1s
Zoom
1s» 30s» 1m» 10m» 1h» 1d» 1w»
Older
0 TO 50
Time
@type
@message

2020-12-02 12:57:45 dce_rpc

2020-12-02 12:57:45 dce_rpc

Alternatively, navigate to https://<servername>/**advancedsearch** in your browser window.

2. Note, Advanced Search can also be located by clicking the downwards pointing arrow in the Model Breach Event Log.



View advanced search for this event

Create a packet capture file for this event | Copy to clipboard

Visualize connection history

Filter Event Log by this protocol (TCP)

Filter Event Log by this application protocol (Unknown)

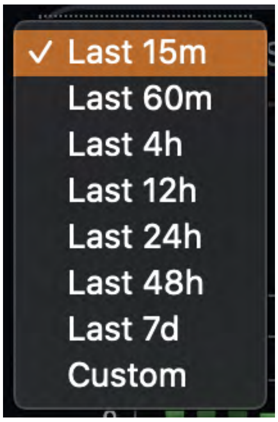
Filter Event Log by this source port (port 49677)

Filter Event Log by this destination port (port 1433)

Filter Event Log by this destination IP (13.92.193.20)

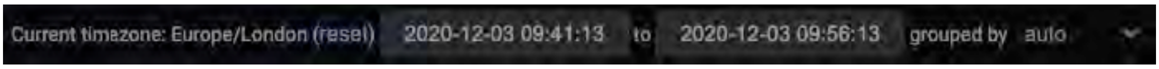
Selecting the **View advanced search for this event**, automatically displays the selected connection in Advanced Search.

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



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

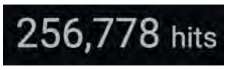
4. The current **timezone** displayed at the top of the Advanced Search page correlates to the timezone set in the Threat Visualizer. The restriction of date and time values make it easy to search within a specified date range.



Current timezone: Europe/London (reset) 2020-12-03 09:41:13 to 2020-12-03 09:56:13 grouped by auto

__Note:__ The auto drop-down menu can be used to group the bars by seconds, minutes, hours or days.

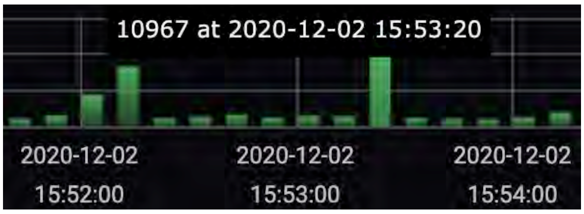
5. The total **number of results** for the chosen timeframe is presented in the top right-hand corner of the interface.



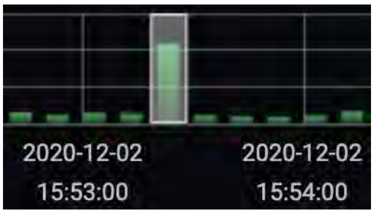
__Note:__ As network data is constantly being recorded, the total number may slightly change for every search or reset.

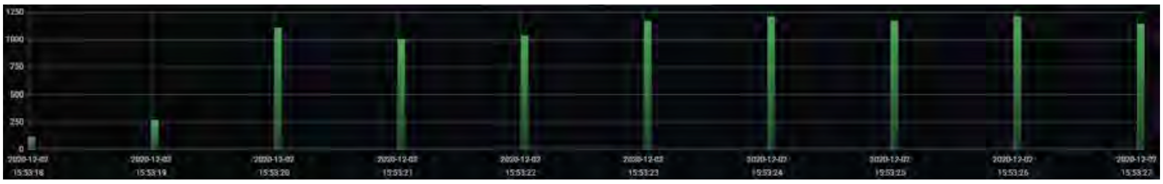
6. The **graph** located underneath the search bar indicates the number of **matching events** over certain periods.

   Hovering over the green bars reveals how much data is available in that timeframe.



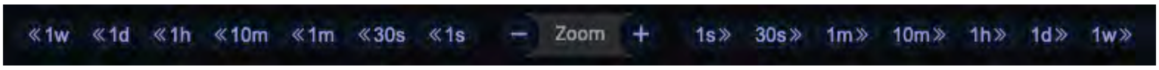
7. **Click and drag** over the green bars to zoom into the graph and adjust the timeframe. This can look at data over a number of seconds rather than minutes/hours/days. The events in the Advanced Search logs automatically update to reflect the graph.



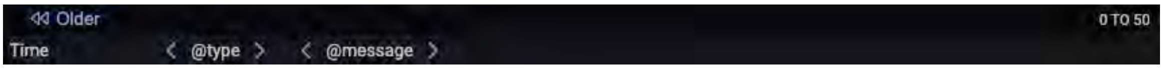


Note: The graph can be made taller by dragging it down from underneath the x-axis.

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


«1w «1d «1h «10m «1m «30s «1s − Zoom + 1s» 30s» 1m» 10m» 1h» 1d» 1w»

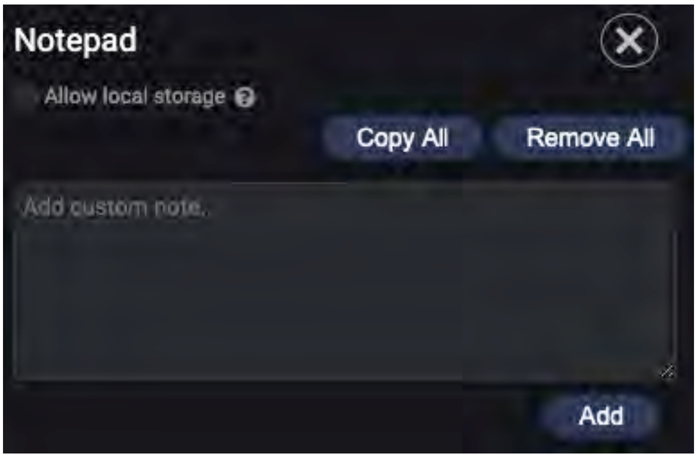
9. Underneath the graph, the most recent **50 events** are displayed in the table. Click the **Older** link at the top or bottom of the page to review more results.



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

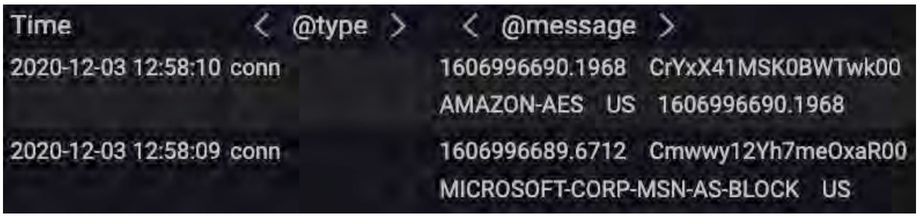
   Notice the **Save** button to the right of the Search button. With a query populated in the search bar, click the save icon to locally save an Advanced Search query.

11. Sometimes, it may be desirable to **make notes** about what has been observed in Advanced Search and also save this locally (not recommended for shared workstations).



To use the **notepad** function, click the **speech bubble** icon in the top right-hand corner of the interface.

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



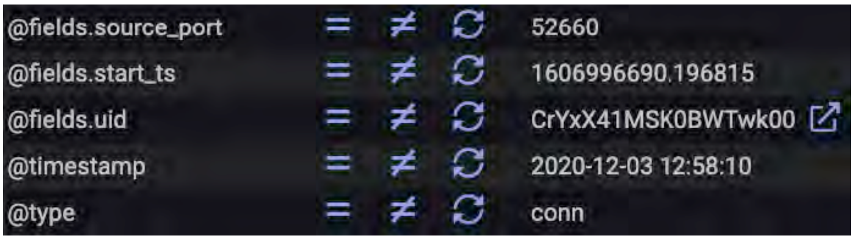
```
Time                  < @type >    < @message >
2020-12-03 12:58:10  conn          1606996690.1968   CrYxX41MSK0BWTwk00
                                   AMAZON-AES   US   1606996690.1968
2020-12-03 12:58:09  conn          1606996689.6712   Cmwwy12Yh7meOxaR00
                                   MICROSOFT-CORP-MSN-AS-BLOCK   US
```

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

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

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

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



@fields.source_port	=	≠	↻	52660
@fields.start_ts	=	≠	↻	1606996690.196815
@fields.uid	=	≠	↻	CrYxX41MSK0BWTwk00
@timestamp	=	≠	↻	2020-12-03 12:58:10
@type	=	≠	↻	conn

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

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

    @fields.source_ip:"10.1.1.10"

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

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

    NOT @fields.dest_port:"80"

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

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

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

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

15. To **reset** the results presented within Advanced Search and return to the default view of the last 15 minutes, click the Darktrace logo in the top left-hand corner of the interface.

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

Operator	Description	Example
AND	Search for multiple terms	@type:"http" AND Mozilla
OR	Find one term or another	@type:"http" OR @type:"ssl"
NOT	Exclude results with this term	@type:"http" AND NOT @fields.dest_port:"80"
" "	Exact Word Search	"Darktrace"
?	Single character wildcard	tlsv1?
*****	Wildcard search	10.100.15.*

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

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

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

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

```
@type:”CONN”
```

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

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

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

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

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

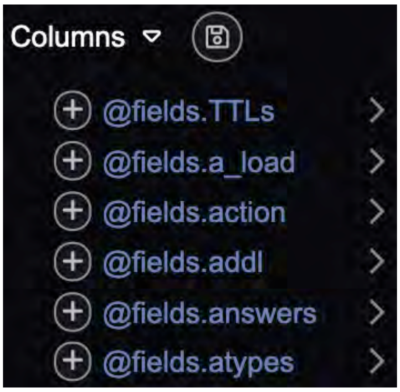
```
@fields.host:/w{3}.darktrace.co.+/
```

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

    Searches over a long period will take longer to complete. Searches that take too long will be aborted to prevent a negative impact on the performance of other parts of the system. Restricting the scope of the search by time or field will help the search return results more quickly.

23. On the left of the Advanced Search interface there is a Columns list. This displays all the fields that are present in the current page of the 50 events. Therefore, more options may be displayed as you search for particular events and content.

    Clicking on the **+** on the left of each field in the Columns list will change the headings in the table of events to include only time and the ‘selected’ field(s).



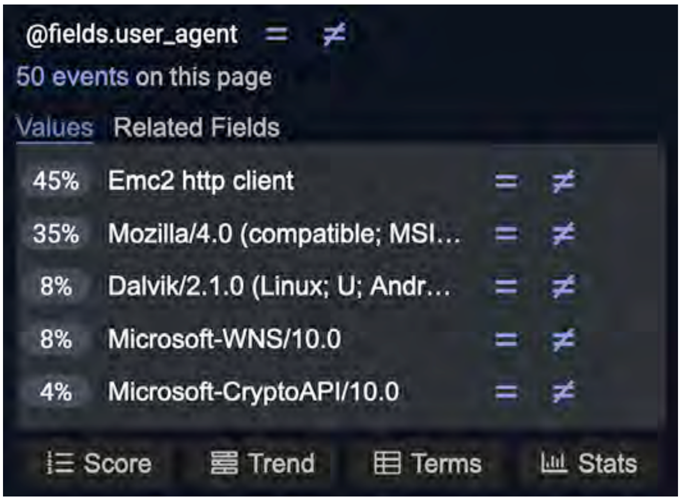
For example, clicking on **@fields.cipher** will restrict results to the different ciphers used in SSL connections. Multiple filters may be selected in this way.

Note: *This Columns list can be hidden, thereby expanding the right portion of the Advanced Search interface, by clicking the left facing arrow above the graph.*

24. If the selected fields are a useful combination, it is possible to **save** them locally by clicking the Save icon to the right of the Columns heading.

25. Clicking the **field itself** on the Columns list displays additional options.

    A useful dialog box reveals up to **5 of the most frequently found results** for a field value in the **50 listed results** currently displayed on the page.



@fields.user_agent = ≠

50 events on this page

Values Related Fields

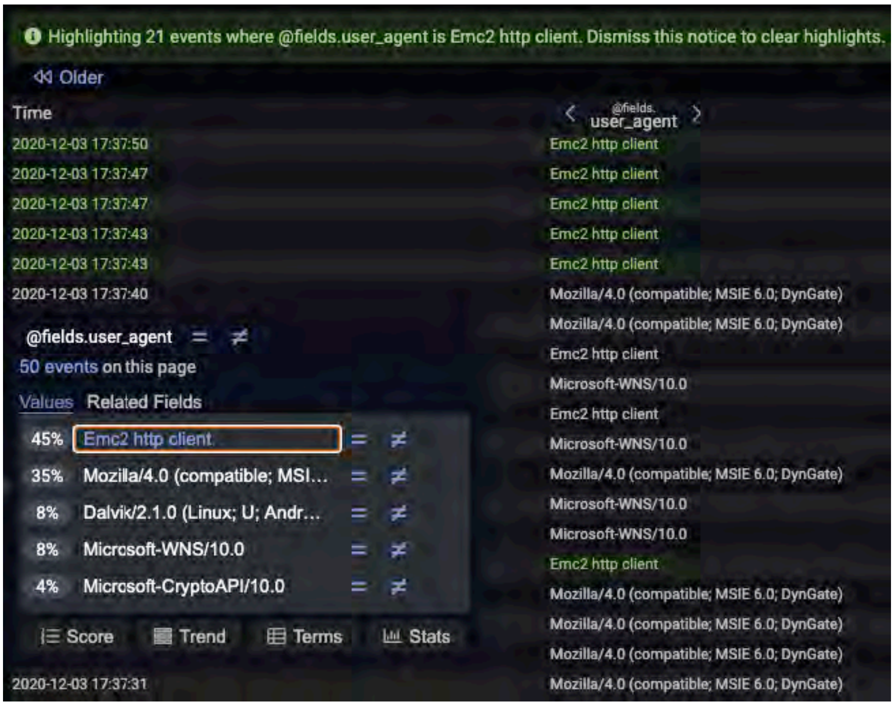
45%	Emc2 http client	=	≠
35%	Mozilla/4.0 (compatible; MSI…	=	≠
8%	Dalvik/2.1.0 (Linux; U; Andr…	=	≠
8%	Microsoft-WNS/10.0	=	≠
4%	Microsoft-CryptoAPI/10.0	=	≠

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

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

   c. Clicking on a value within the pop-up window will highlight any events on the page where that field value exists.

      This can help identify events without the need to filter out other surrounding events.



Highlighting 21 events where @fields.user_agent is Emc2 http client. Dismiss this notice to clear highlights.

```
Time                   @fields.user_agent
2020-12-03 17:37:50    Emc2 http client
2020-12-03 17:37:47    Emc2 http client
2020-12-03 17:37:47    Emc2 http client
2020-12-03 17:37:43    Emc2 http client
2020-12-03 17:37:43    Emc2 http client
2020-12-03 17:37:40    Mozilla/4.0 (compatible; MSIE 6.0; DynGate)
                       Mozilla/4.0 (compatible; MSIE 6.0; DynGate)
                       Emc2 http client
                       Microsoft-WNS/10.0
                       Emc2 http client
                       Microsoft-WNS/10.0
                       Mozilla/4.0 (compatible; MSIE 6.0; DynGate)
                       Microsoft-WNS/10.0
                       Microsoft-WNS/10.0
                       Emc2 http client
                       Mozilla/4.0 (compatible; MSIE 6.0; DynGate)
                       Mozilla/4.0 (compatible; MSIE 6.0; DynGate)
                       Mozilla/4.0 (compatible; MSIE 6.0; DynGate)
2020-12-03 17:37:31    Mozilla/4.0 (compatible; MSIE 6.0; DynGate)
```

@fields.user_agent = ≠

50 events on this page

Values Related Fields

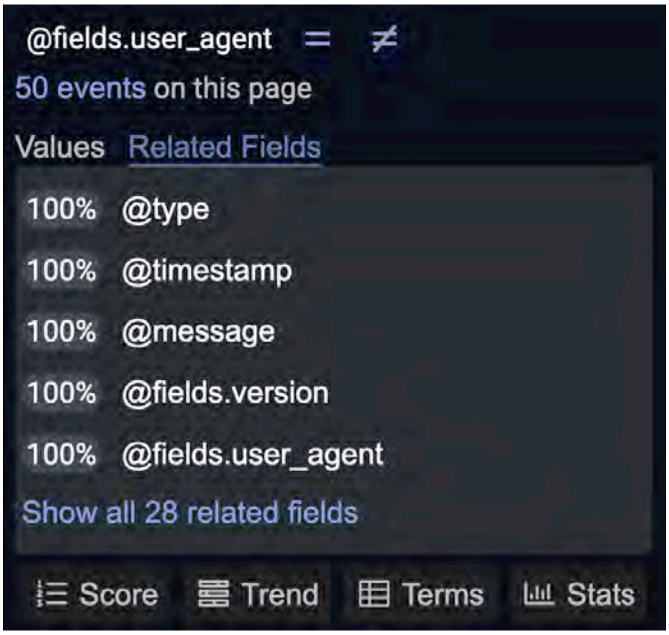
45%	Emc2 http client	=	≠
35%	Mozilla/4.0 (compatible; MSI…	=	≠
8%	Dalvik/2.1.0 (Linux; U; Andr…	=	≠
8%	Microsoft-WNS/10.0	=	≠
4%	Microsoft-CryptoAPI/10.0	=	≠

26. Notice the **Related Fields** tab. Click on this to display similar fields to the selected field.

    Click **Show all** to view any other related fields.

    Clicking any of these has the same effect as clicking the + icon to the left of the listed fields – it will apply them as headings to the table of events, thereby only displaying the selected information.

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



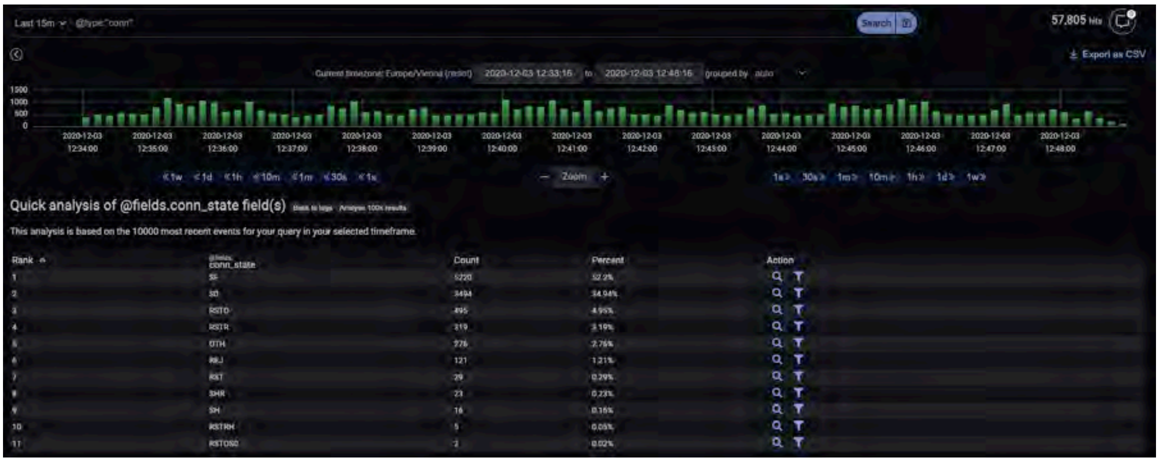
@fields.user_agent = ≠

50 events on this page

Values Related Fields

100%	@type
100%	@timestamp
100%	@message
100%	@fields.version
100%	@fields.user_agent

Show all 28 related fields



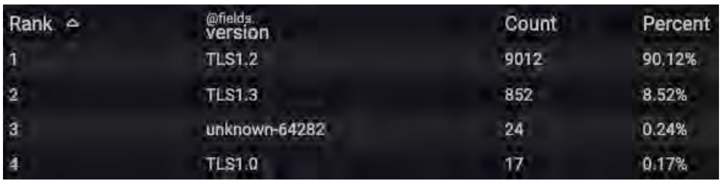
Quick analysis of @fields.conn_state field(s) Back to logs Analyse 100k results

This analysis is based on the 10000 most recent events for your query in your selected timeframe.

Rank	@fields.conn_state	Count	Percent	Action
1	SF	5220	52.2%	
2	S0	3494	34.94%	
3	RSTO	495	4.95%	
4	RSTR	319	3.19%	
5	OTH	276	2.76%	
6	REJ	121	1.21%	
7	RST	29	0.29%	
8	SHR	23	0.23%	
9	SH	16	0.16%	
10	RSTRH	5	0.05%	
11	RSTOS0	2	0.02%	

a. Clicking **Score** for a chosen field will rank all results in descending order based on their count/percentage over the selected time frame. The limitation of this is it will only score the 10,000 most recent results and will only present the top 100 results.

   From example, the score produced from **@fields.version** reveals the different TLS versions observed on the network.



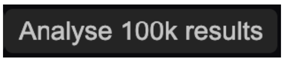
Rank	@fields.version	Count	Percent
1	TLS1.2	9012	90.12%
2	TLS1.3	852	8.52%
3	unknown-64282	24	0.24%
4	TLS1.0	17	0.17%

b. Clicking **Trend** will perform analysis on the chosen field which shows the count, percentage and trend. This trend is a rate of change for each individual value, i.e. if the value is more or less popular in the selected time frame, denoted in **red** and **green** for decreases and increases in popularity respectively.

c. Selecting **Terms** will aggregate the results for a chosen field and visually represent them using a pie chart. Similar to the Score function, it also gives the count and percentage for each result. Empty values are also displayed in the breakdown. However, while Terms can analyze at more than 10,000 results, they are limited by the time frame of 48 hours.

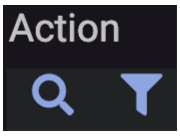
d. Finally, clicking on the **Stats** button will give a statistical breakdown of **numeric fields only**. Included in this breakdown are the count, minimum, maximum, average and sum.

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

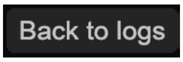


__Note:__ For small appliances, the Analyse 100k results option will not be available.

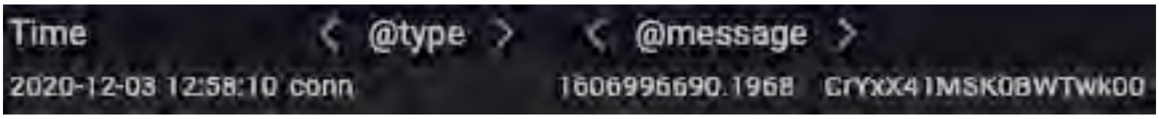
29. At the end of every row of one of the statistical analyses, there are two actions available, denoted by the **magnifying glass** and **filter** icons. Both buttons will append the value to the search bar. However, the magnifying glass will perform a search and present the logs, while the filter will keep the statistical analysis page open.



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

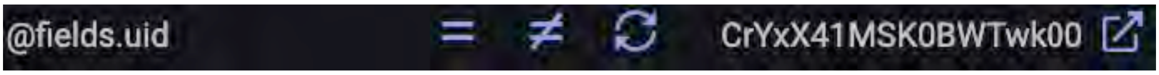


31. When using Advanced Search, it is possible to copy a field **UID value** and paste it into the Threat Visualizer tool.



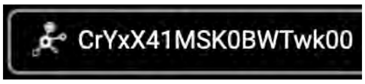
Time @type @message
2020-12-03 12:58:10 conn 1606996690.1968 CrYxX41MSK0BWTwk00

Alternatively, expand the entry, navigate to **@fields.uid** and **click the link icon** to the right of the UID to open a new Threat Visualizer tab showing the connection.



@fields.uid CrYxX41MSK0BWTwk00

Both options populate the **Omnisearch bar** and can provide additional graphics about the events.



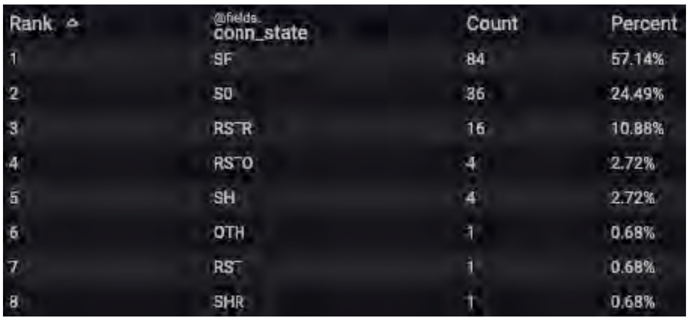
__Note:__ When searching Threat Visualizer, confirm your date range is ahead of the copied event or no results will be found.

Using Advanced Search to Understand TCP Connection States

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

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

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



Rank	@fields. conn_state	Count	Percent
1	SF	84	57.14%
2	S0	36	24.49%
3	RSTR	16	10.88%
4	RSTO	4	2.72%
5	SH	4	2.72%
6	OTH	1	0.68%
7	RST	1	0.68%
8	SHR	1	0.68%

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

State	Meaning	Expected History
S0	Connection attempt (SYN) only – no response	S
S1	Established	ShA
SF	Normal termination	ShADdAFaf
REJ	Rejected	Sr
S2	Established and originator sent FIN, no FIN|ACK from Responder	ShADdF
S3	Established and responder sent FIN, no FIN|ACK from Originator	ShADdf
RSTO	Established, Originator sent an RST	ShADdR
RSTR	Established, Responder sent an RST	ShADdr
RSTOS0	Originator sent SYN followed by RST with no SYN|ACK from Responder	SR
RSTRH	Responder sent SYN|ACK followed by RST with no SYN from (supposed) Originator	hr
SH	Originator sent SYN followed by FIN with no SYN|ACK from responder (half open)	SF
SHR	Responder sent SYN|ACK followed by FIN with no SYN from Originator	hf
OTH	No SYN seen, just midstream traffic that was not closed later	Dd

4. Review the connection history using the **@fields.history** filter. Once again, a normal termination of **ShADdAFaf** is expected. Otherwise, the returned state could provide useful information. For example, a connection state of SO or a history of SR could represent a port scan on your network.

Advanced Search Exercises

Use Advanced Search to find the following:

- **a.** Were there any SSL queries to eBay in the last 60 mins?
- **b.** Find all SSH and RDP connectivity originating from your device in the last 7 days. (If your machine is not on the network, select a different host).
- **c.** Find the SHA1 hashes of all executable files observed over the last 48hrs. Remember the side filters will change depending what you search for.
- **d.** Return the failed Kerberos Type events over the last 7 days.
- **e.** How can you find all events for a connection? Is there a shortcut?
- **f.** Find the user agent and the method of the last HTTP request sent by your machine. (If your machine is not on the network, select a different host).
- **g.** Locate all the internal DNS servers.
- **h.** Find connections to external IP addresses which use the FTP protocol.

View the **Cheat Sheet** to check your answers at the end of this manual.

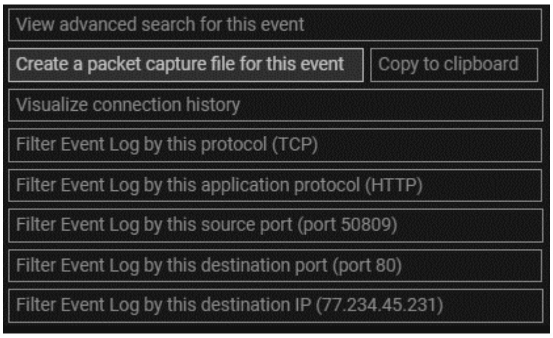
5. Creating a Packet Capture

Advanced users have the capability to access raw packet capture files to investigate device communications. Through the Threat Visualizer interface, packet capture files can be downloaded and examined in more detail. PCAPs are created on a per user basis, so are not visible for other users of the system unless shared in other ways.

1. Select an alert and view its **Breach Log**.

   Click the downwards arrow located on the left of a connection.

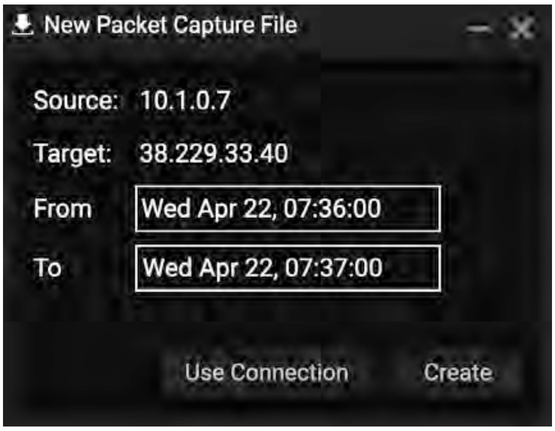
   Select the **Create a packet capture file for this event** option.


View advanced search for this event
Create a packet capture file for this event
Copy to clipboard
Visualize connection history
Filter Event Log by this protocol (TCP)
Filter Event Log by this application protocol (HTTP)
Filter Event Log by this source port (port 50809)
Filter Event Log by this destination port (port 80)
Filter Event Log by this destination IP (77.234.45.231)

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

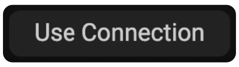
   Click **Create** to create a default time period packet capture or change the **To** and **From** times.

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



Source: 10.1.0.7
Target: 38.229.33.40
From Wed Apr 22, 07:36:00
To Wed Apr 22, 07:37:00

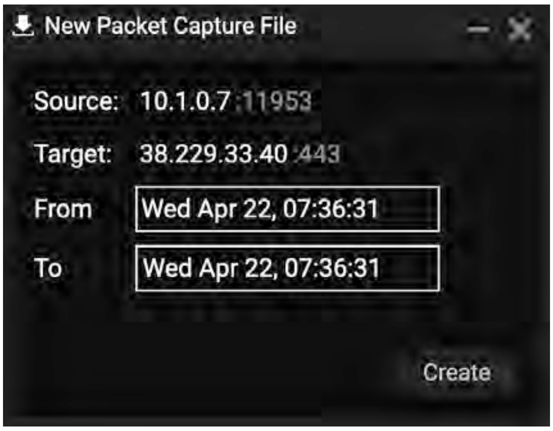
3. Alternatively, when creating a packet capture for an event, notice the **Use Connection** button.



   When clicked, it will update the **From** and **To** date and time stamps to the connection selected.

   Also the source and destination ports are specified. Click **Create**.

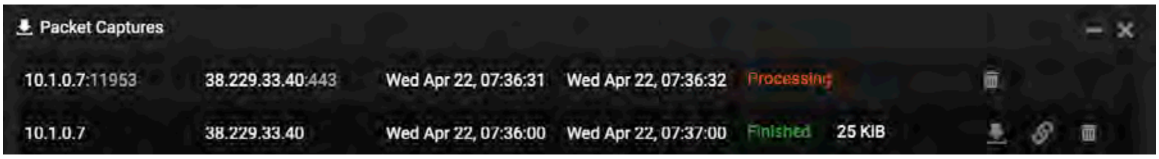
   It may take a few minutes or longer to create the packet capture file, depending on the duration selected.



Source: 10.1.0.7 :11953
Target: 38.229.33.40 :443
From Wed Apr 22, 07:36:31
To Wed Apr 22, 07:36:31

4. On the Threat Visualizer home screen, select **Menu** and choose **Packet Captures.** The newly created PCAP may be Processing.

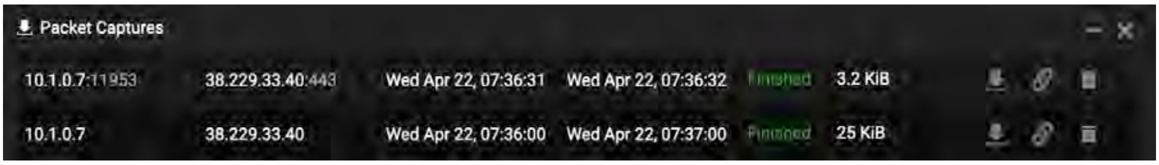
Packet Captures



Packet Captures

10.1.0.7:11953	38.229.33.40:443	Wed Apr 22, 07:36:31	Wed Apr 22, 07:36:32	Processing		
10.1.0.7	38.229.33.40	Wed Apr 22, 07:36:00	Wed Apr 22, 07:37:00	Finished	25 KiB	

5. Confirm the process has Finished and click the **View this packet capture file in the browser** link icon.



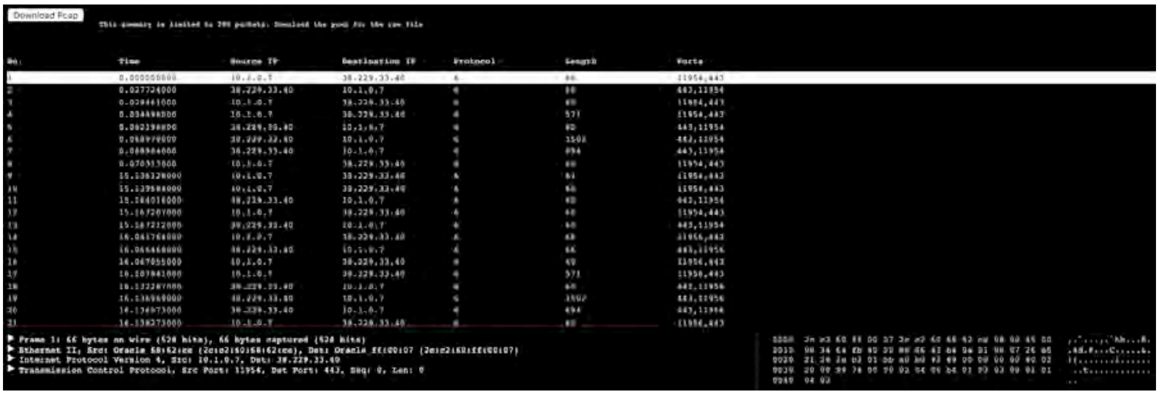
Packet Captures

10.1.0.7:11953	38.229.33.40:443	Wed Apr 22, 07:36:31	Wed Apr 22, 07:36:32	Finished	3.2 KiB
10.1.0.7	38.229.33.40	Wed Apr 22, 07:36:00	Wed Apr 22, 07:37:00	Finished	25 KiB

***Note:** The other icons show that the data can also be downloaded for viewing in another program or the packet capture can be deleted.*

6. The PCAP results will open in a new tab. The Threat Visualizer has automatically formatted the results though an application called **Darkshark**.

   The amount of PCAP data stored significantly depends on the type of network traffic monitored, but typically ranges from three to seven days. Click on the packet frames to view the full details.



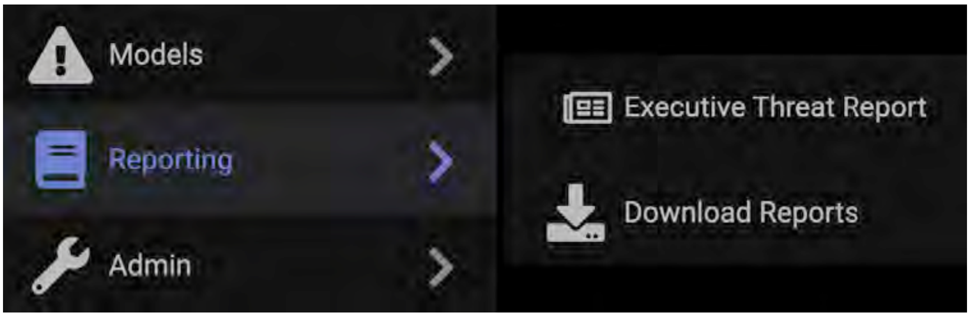
```
This summary is limited to 200 packets. Download the pcap for the raw file

No.   Time           Source IP      Destination IP   Protocol   Length   Ports
1     0.000000000    10.1.0.7       38.229.33.40     6          66       11954,443
2     0.027724000    38.229.33.40   10.1.0.7         6          66       443,11954
3     0.029461000    10.1.0.7       38.229.33.40     6          60       11954,443
4     0.034498000    10.1.0.7       38.229.33.40     6          571      11954,443
5     0.062198000    38.229.33.40   10.1.0.7         6          60       443,11954
6     0.068979000    38.229.33.40   10.1.0.7         6          1502     443,11954
7     0.068984000    38.229.33.40   10.1.0.7         6          494      443,11954
8     0.070313000    10.1.0.7       38.229.33.40     6          60       11954,443
9     15.136328000   10.1.0.7       38.229.33.40     6          54       11954,443
10    15.139588000   10.1.0.7       38.229.33.40     6          66       11956,443
11    15.184016000   38.229.33.40   10.1.0.7         6          60       443,11954
12    15.167207000   10.1.0.7       38.229.33.40     6          60       11954,443
13    15.187212000   38.229.33.40   10.1.0.7         6          60       443,11954
14    16.041764000   10.1.0.7       38.229.33.40     6          60       11956,443
15    16.066468000   38.229.33.40   10.1.0.7         6          66       443,11956
16    16.067055000   10.1.0.7       38.229.33.40     6          60       11956,443
17    16.107941000   10.1.0.7       38.229.33.40     6          571      11956,443
18    16.132287000   38.229.33.40   10.1.0.7         6          60       443,11956
19    16.136969000   38.229.33.40   10.1.0.7         6          1502     443,11956
20    16.136973000   38.229.33.40   10.1.0.7         6          494      443,11956
21    16.138273000   10.1.0.7       38.229.33.40     6          60       11956,443

▶ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▶ Ethernet II, Src: Oracle 68:62:ee (2e:e2:60:68:62:ee), Dst: Oracle ff:00:07 (2e:e2:60:ff:00:07)
▶ Internet Protocol Version 4, Src: 10.1.0.7, Dst: 38.229.33.40
▶ Transmission Control Protocol, Src Port: 11954, Dst Port: 443, Seq: 0, Len: 0

0000  2e e3 60 ff 00 07 2e e2 60 68 62 ee 08 00 45 00   [illegible]
0010  00 34 64 db 40 00 80 06 4f b4 0a 01 00 07 26 e5   [illegible]
0020  21 28 2e b2 01 bb a0 b0 f3 49 00 00 00 00 80 02   [illegible]
0030  20 00 39 78 00 00 02 04 05 b4 01 03 03 08 01 01   [illegible]
0040  04 02                                              ..
```

Alternative applications can be used to investigate the PCAP data, such as Wireshark.

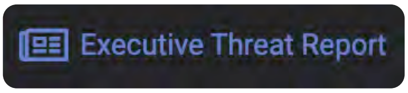
6. Executive Threat Reports

The Executive Threat Report provides an insightful professional summary of the types of model breaches discovered over a set time period.

1. On the Threat Visualizer Menu, select **Reporting** to see two further options.



2. Click **Executive Threat Report** to open a new window where reports can be generated.



   a. To create a report, confirm the **duration** or select a custom date range.

   b. The time can be converted to a given **time zone**. By default, this field will reflect the time zone in the Time Selector.

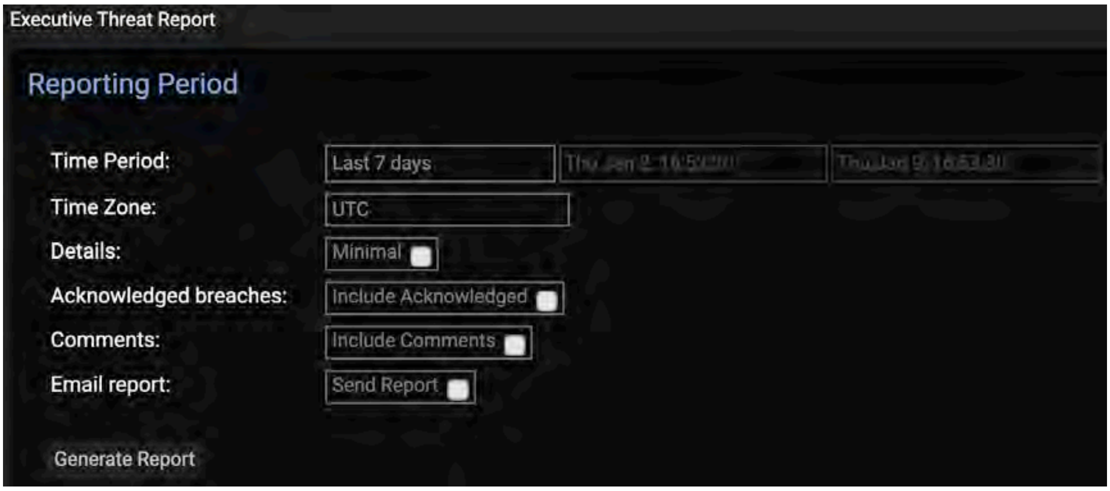
   c. For Details, it may be helpful to select **Minimal** to remove the Appendix and reduce the size of the report.

   d. If many Models breaches have been acknowledged it is recommended to enable the **Include Acknowledged** setting to build a report of all breaches.

   e. If many breaches have been commented on, these **comments** can be included.

   f. If the report is to be emailed, ticking **Send Report** will do so.

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



Time Period: Last 7 days | Thu Jan 2 16:53:30 | Thu Jan 9 16:53:30

Time Zone: UTC

Details: Minimal □

Acknowledged breaches: Include Acknowledged □

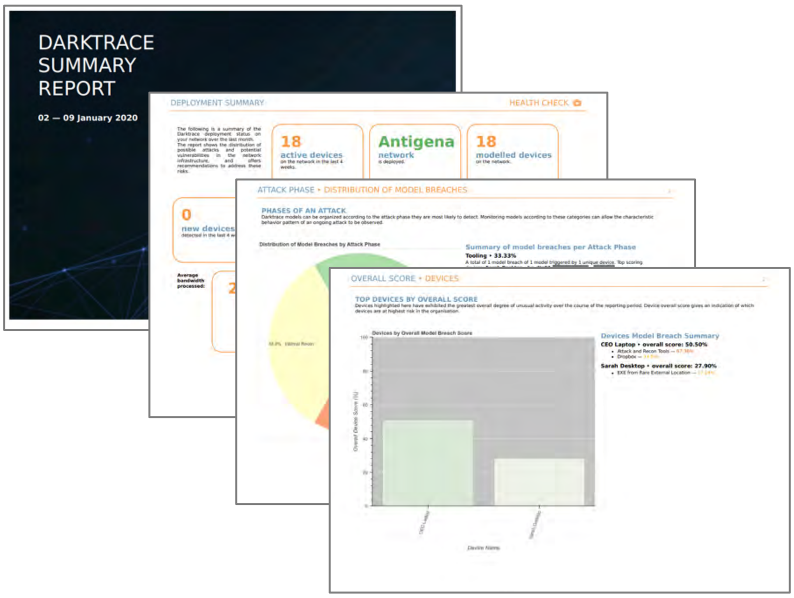
Comments: Include Comments □

Email report: Send Report □

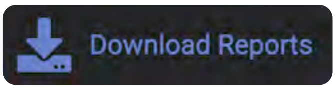
3. The report will open as a **preview** in the Executive Threat Report window.

   It can be opened as a **pdf** in a new browser tab by downloading it, an option which is obtained by clicking or hovering over the preview.

   Review the report to understand the full range of statistics covered.

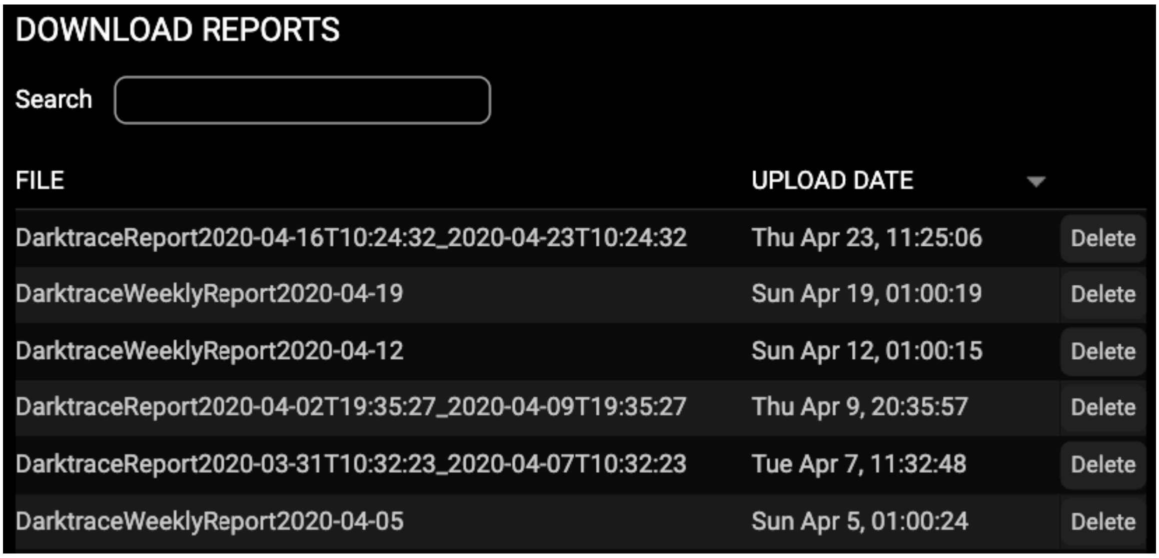

DARKTRACE SUMMARY REPORT
02 – 09 January 2020
DEPLOYMENT SUMMARY
HEALTH CHECK
18 active devices
Antigena network
18 modelled devices
0 new devices
ATTACK PHASE • DISTRIBUTION OF MODEL BREACHES
PHASES OF AN ATTACK
Summary of model breaches per Attack Phase
OVERALL SCORE • DEVICES
TOP DEVICES BY OVERALL SCORE
Devices by Overall Model Breach Score
Devices Model Breach Summary
CEO Laptop • overall score: 50.50%
Sarah Desktop • overall score: 27.90%
Device Name

4. When reports are generated, they are automatically saved. In the Threat Visualizer Menu under **Reporting**, select **Download Reports**.



   The Executive Threat Report which has just been generated can be found in this list. Other reports are automatically created and saved once a week and are easily recognizable as they contain **WeeklyReport** in their title.

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



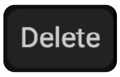
DOWNLOAD REPORTS

Search

FILE	UPLOAD DATE ▼	
DarktraceReport2020-04-16T10:24:32_2020-04-23T10:24:32	Thu Apr 23, 11:25:06	Delete
DarktraceWeeklyReport2020-04-19	Sun Apr 19, 01:00:19	Delete
DarktraceWeeklyReport2020-04-12	Sun Apr 12, 01:00:15	Delete
DarktraceReport2020-04-02T19:35:27_2020-04-09T19:35:27	Thu Apr 9, 20:35:57	Delete
DarktraceReport2020-03-31T10:32:23_2020-04-07T10:32:23	Tue Apr 7, 11:32:48	Delete
DarktraceWeeklyReport2020-04-05	Sun Apr 5, 01:00:24	Delete

   a. Click a report to **download** it.

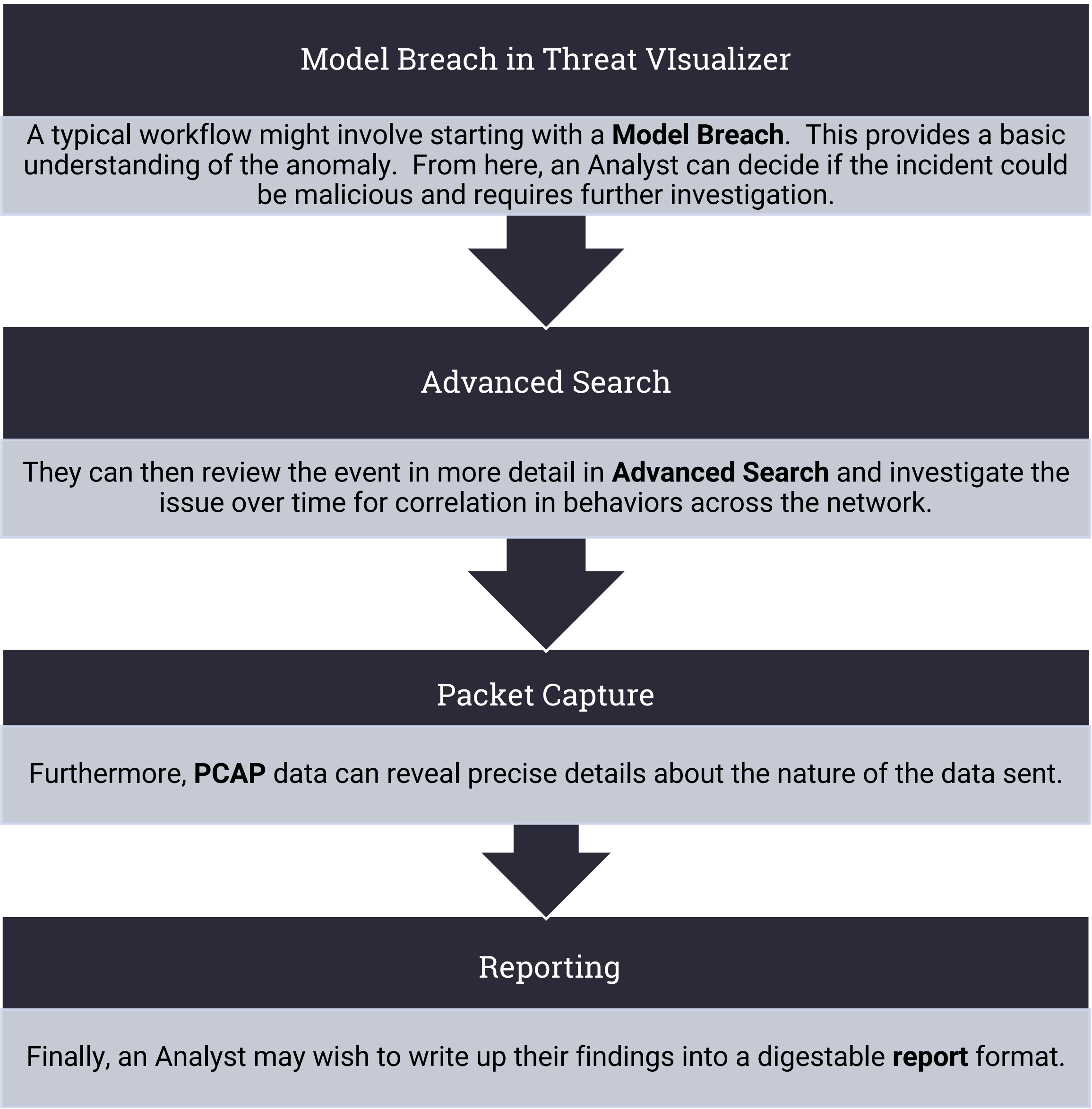
   b. Reports can also be **deleted** from this page.



   c. To find a report, utilize the Search bar at the top of the page.

7. Analyst Workflow

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



Model Breach in Threat VIsualizer

A typical workflow might involve starting with a **Model Breach**. This provides a basic understanding of the anomaly. From here, an Analyst can decide if the incident could be malicious and requires further investigation.

Advanced Search

They can then review the event in more detail in **Advanced Search** and investigate the issue over time for correlation in behaviors across the network.

Packet Capture

Furthermore, **PCAP** data can reveal precise details about the nature of the data sent.

Reporting

Finally, an Analyst may wish to write up their findings into a digestable **report** format.

Darktrace enables you to use the platform in a variety of ways, however there is no fixed recipe for how to investigate potential threats using the platform. Investigation of different types of model breaches will require different approaches.

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

1. Increase the Sensitivity Slider to include a manageable number of model breaches and focus on the most important. **60%** is a good starting point.

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

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

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

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

6. Does the device have **related anomalies** at the time or in the last 7 days?

7. Review what else the device was doing at the time in the **Device Event Log**. Try adding metrics in the graphs to get a better understanding the device's behavior. Investigate why Darktrace has provided a high score for a threat.

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

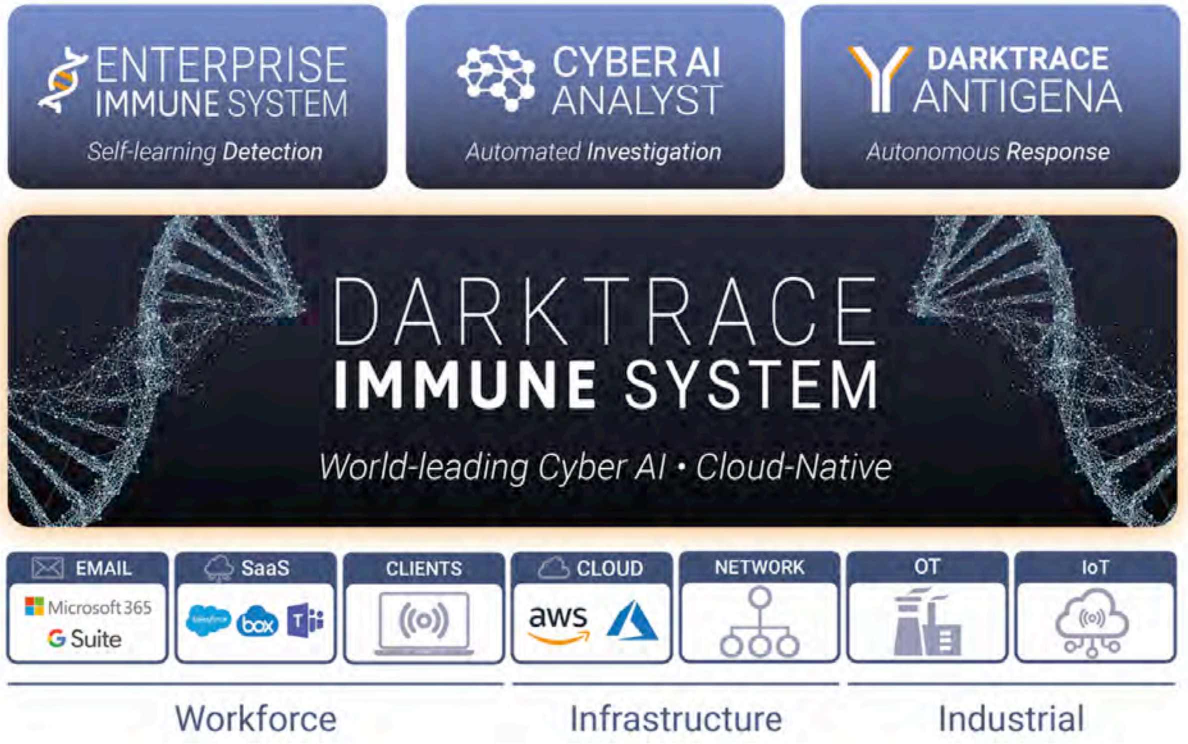
9. Use **third party resources** for open-source context regarding a suspicious domain or file (e.g. WhoIs, Virustotal, Google search or malware research organizations).

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

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

8. Additional Offerings Overview

Darktrace offers the Cyber AI platform, which is made up of the Enterprise Immune System (EIS) and Darktrace Antigena. The combination of these offerings can protect a wide range of network architectures, including industrial, cloud, hybrid and email environments.



Cloud and SaaS Connectors

Darktrace Cloud Connectors allow companies to easily extend Darktrace's visibility and detection capabilities to Cloud based offerings. This allows anomalous behaviors to be detected in real time, extending Darktrace's Enterprise Immune System defense beyond the physical enterprise network and into Cloud environments. All these potential threats from different environments can be presented in one unified view within the Threat Visualizer interface. Such incidents are also automatically investigated by the Cyber AI Analyst, meaning different events can be correlated in easy to view incidents.

There are three main network architectures to consider when using the Cloud:

- Hybrid Cloud (IaaS)
- Hybrid Cloud (SaaS)
- Cloud only (IaaS and/or SaaS)

With the Hybrid IaaS Cloud environment, Darktrace can deploy virtual probes called vSensors which capture real-time traffic in the cloud and correlate it with the rest of the business. Darktrace is also able to deploy osSensors on endpoints which feed traffic to local vSensors which, in turn, feed the relevant metadata to the Darktrace master probe in the cloud/corporate network for analysis. On top of this, AWS and Azure customers can deploy Darktrace Connectors to monitor sysadmin activity at the API level.

For Hybrid SaaS deployments, Darktrace Connectors are remotely installed on physical or cloud-based Darktrace masters/probes to interrogate the security APIs of the chosen SaaS solutions. Available SaaS connectors include Office 365, G Suite, Dropbox, Box, Salesforce, Egnyte, JumpCloud, Zoom and more. Darktrace is able to continually analyze and correlate SaaS data with network traffic from the rest of the business. All this information can be presented in the Threat Visualizer.

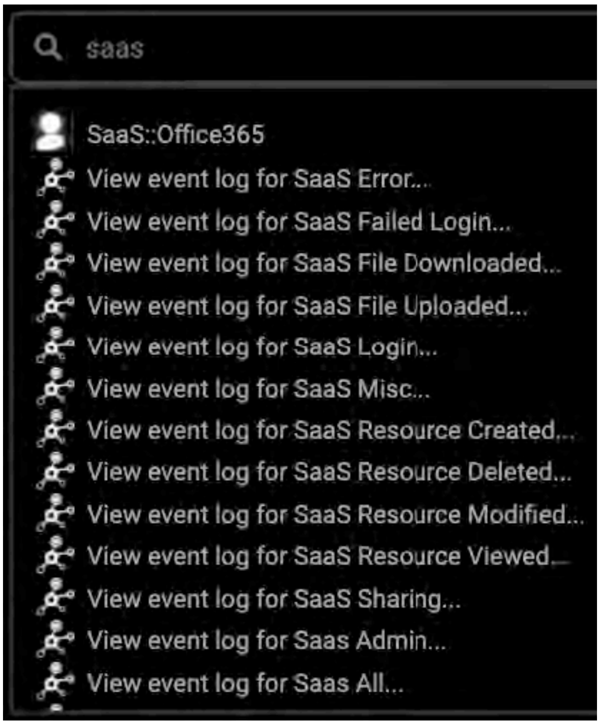
It is also possible to have Cloud Only setups which are completely built on IaaS and/or SaaS without the need for on-premise networks. In cases like this, Darktrace manages a cloud master/probe which receives traffic from sensors and connectors in the environment.

Depending on the connector which has been deployed, a variety of events can be displayed within the Threat Visualizer.

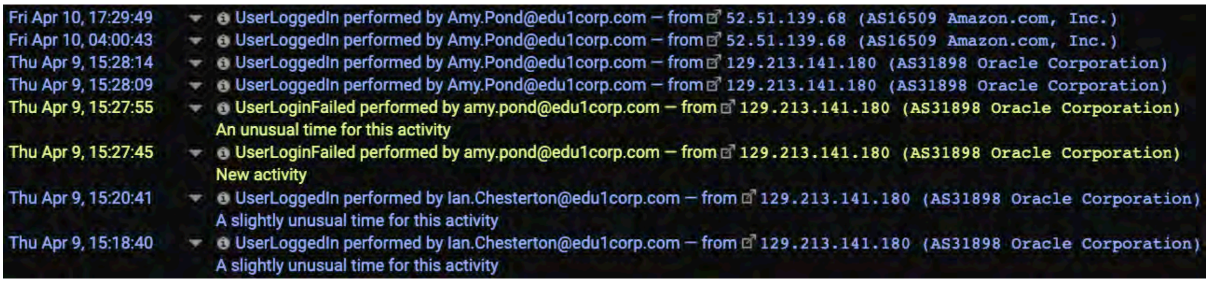
Just as with other searchable features in the Threat Visualizer, the IaaS/SaaS service can be located just as a device or user would be under normal circumstances.

Taking Office365 as an example, as seen on the right, logins, movement of files, administrative, resource-related or miscellaneous events can be observed.

As with the connections normally presented in the Threat Visualizer Event Logs, SaaS events are also displayed in a similar way.

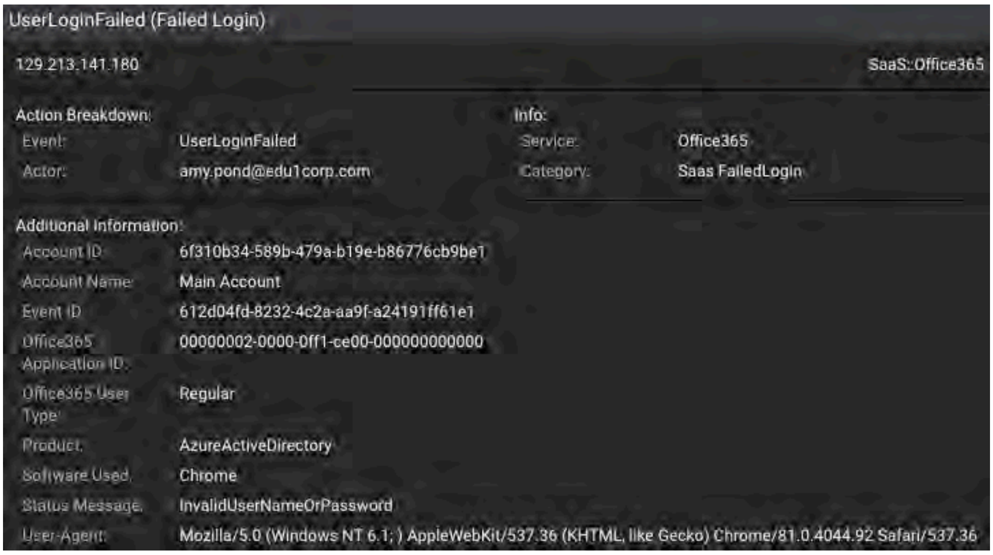

saas
SaaS::Office365
View event log for SaaS Error...
View event log for SaaS Failed Login...
View event log for SaaS File Downloaded...
View event log for SaaS File Uploaded...
View event log for SaaS Login...
View event log for SaaS Misc...
View event log for SaaS Resource Created...
View event log for SaaS Resource Deleted...
View event log for SaaS Resource Modified...
View event log for SaaS Resource Viewed...
View event log for SaaS Sharing...
View event log for Saas Admin...
View event log for Saas All...

In the Event Logs, the user which performed the action, the action that was performed and the location from which this occurred are presented in easy to read formats. Furthermore, notices obtained from the Machine Learning alert the end user of Darktrace to new or unusual times for activity.



```
Fri Apr 10, 17:29:49   UserLoggedIn performed by Amy.Pond@edu1corp.com — from 52.51.139.68 (AS16509 Amazon.com, Inc.)
Fri Apr 10, 04:00:43   UserLoggedIn performed by Amy.Pond@edu1corp.com — from 52.51.139.68 (AS16509 Amazon.com, Inc.)
Thu Apr 9, 15:28:14    UserLoggedIn performed by Amy.Pond@edu1corp.com — from 129.213.141.180 (AS31898 Oracle Corporation)
Thu Apr 9, 15:28:09    UserLoggedIn performed by Amy.Pond@edu1corp.com — from 129.213.141.180 (AS31898 Oracle Corporation)
Thu Apr 9, 15:27:55    UserLoginFailed performed by amy.pond@edu1corp.com — from 129.213.141.180 (AS31898 Oracle Corporation)
                       An unusual time for this activity
Thu Apr 9, 15:27:45    UserLoginFailed performed by amy.pond@edu1corp.com — from 129.213.141.180 (AS31898 Oracle Corporation)
                       New activity
Thu Apr 9, 15:20:41    UserLoggedIn performed by Ian.Chesterton@edu1corp.com — from 129.213.141.180 (AS31898 Oracle Corporation)
                       A slightly unusual time for this activity
Thu Apr 9, 15:18:40    UserLoggedIn performed by Ian.Chesterton@edu1corp.com — from 129.213.141.180 (AS31898 Oracle Corporation)
                       A slightly unusual time for this activity
```

By hovering over the tooltip icon for each categorized event, the dialogs show which user and service can be attributed to it as well as a plethora of associated information.



UserLoginFailed (Failed Login)

129.213.141.180 SaaS::Office365

Action Breakdown:

Event:	UserLoginFailed
Actor:	amy.pond@edu1corp.com

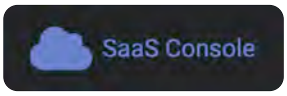
Info:

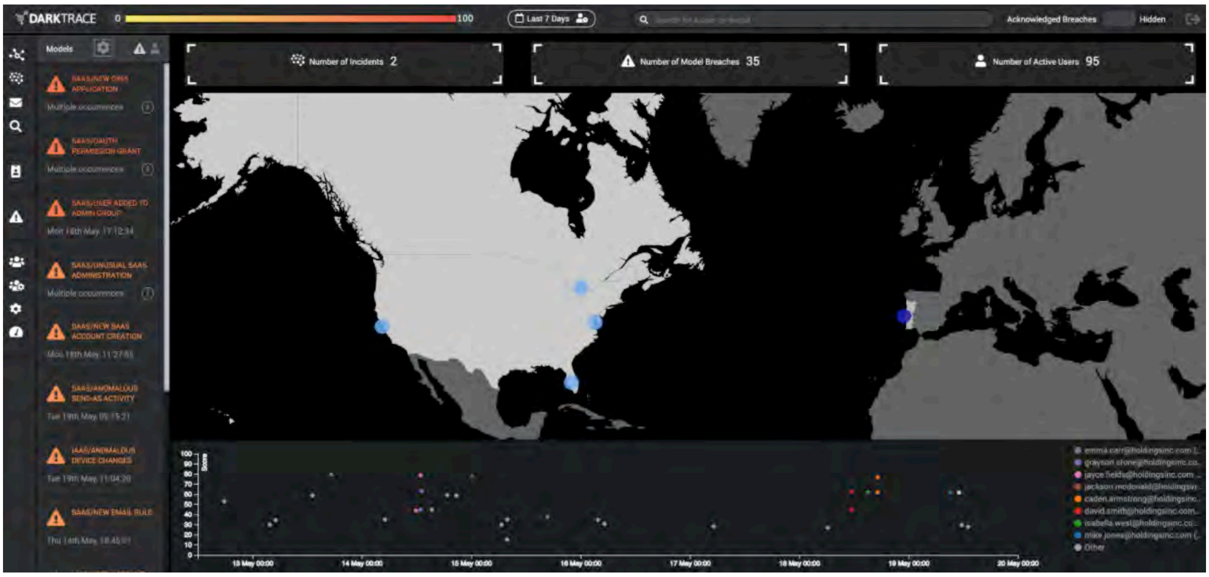
Service:	Office365
Category:	Saas FailedLogin

Additional Information:

Account ID:	6f310b34-589b-479a-b19e-b86776cb9be1
Account Name:	Main Account
Event ID:	612d04fd-8232-4c2a-aa9f-a24191ff61e1
Office365 Application ID:	00000002-0000-0ff1-ce00-000000000000
Office365 User Type:	Regular
Product:	AzureActiveDirectory
Software Used:	Chrome
Status Message:	InvalidUserNameOrPassword
User-Agent:	Mozilla/5.0 (Windows NT 6.1;) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.92 Safari/537.36

Information is not only presented within the Threat Visualizer Interface. With a SaaS connector, it is possible to view all the SaaS only related content by navigating to the SaaS Console through the main menu.




DARKTRACE
0
100
Last 7 Days
Acknowledged Breaches
Hidden
Models
SAAS/NEW OWS APPLICATION
Multiple occurrences
SAAS/OAUTH PERMISSION GRANT
Multiple occurrences
SAAS/USER ADDED TO ADMIN GROUP
Mon 18th May, 17:12:34
SAAS/UNUSUAL SAAS ADMINISTRATION
Multiple occurrences
SAAS/NEW SAAS ACCOUNT CREATION
Mon 18th May, 11:27:51
SAAS/ANOMALOUS SEND-AS ACTIVITY
Tue 19th May, 09:15:21
IAAS/ANOMALOUS DEVICE CHANGES
Tue 19th May, 11:04:20
SAAS/NEW EMAIL RULE
Thu 14th May, 18:45:01
Number of Incidents 2
Number of Model Breaches 35
Number of Active Users 95
Score
100
90
80
70
60
50
40
30
20
10
0
13 May 00:00
14 May 00:00
15 May 00:00
16 May 00:00
17 May 00:00
18 May 00:00
19 May 00:00
20 May 00:00
emma.carr@holdingsinc.com (...
grayson.stone@holdingsinc.co...
jayce.fields@holdingsinc.com ...
jackson.mcdonald@holdingsin...
caden.armstrong@holdingsinc...
david.smith@holdingsinc.com...
isabella.west@holdingsinc.co...
mike.jones@holdingsinc.com (...
Other

Antigena

Darktrace Antigena it the world's first Autonomous Response solution which can provide a helping hand when security teams are overwhelmed or not around. Darktrace Antigena can generate real-time, targeted, surgical, and proportionate responses when threatening incidents arise in network and email environments. This is crucial for defending against machine-speed attacks such as ransomware, giving security teams time to catch up without threats interrupting daily business operations.

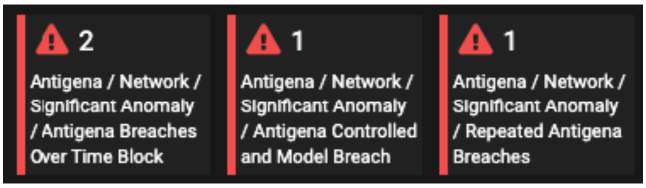
Antigena Network and Antigena Cloud

Antigena Network delivers 24/7 Autonomous Response AI across the physical and cloud enterprise networks. Like a digital antibody, Antigena can generate responses to external and insider threats, accounts takeovers and critical misconfigurations.

Within seconds of detecting a threat, Antigena can enforce the normal 'pattern of life' for users, devices and containers without relying on prior assumptions or manually input known threats. Considering Antigena Cloud is a cloud-native solution, it analyzes behaviors across diverse cloud platforms. Antigena Network can also integrate with firewalls and network devices if appropriate.

Antigena understands the severity of a threat and will only interrupt threatening activity while sustaining normal operations. It can issue a range of actions depending on what is appropriate, including interrupting unusual connections and stopping unusually large amounts of data being sent.

Antigena breaches are displayed in the Threat Visualizer in the same ways as EIS Models. These can be clicked on to open up the Model Breach Event Log.



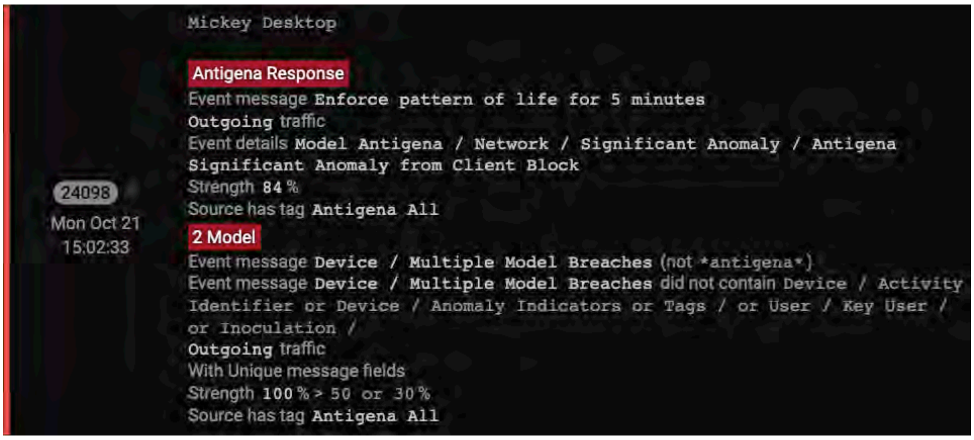
2
Antigena / Network / Significant Anomaly / Antigena Breaches Over Time Block

1
Antigena / Network / Significant Anomaly / Antigena Controlled and Model Breach

1
Antigena / Network / Significant Anomaly / Repeated Antigena Breaches

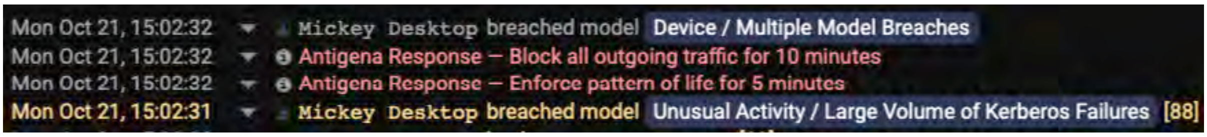
Lots of useful metadata is presented in the Breach Log.

The breaches can still be analyzed using the same workflow.



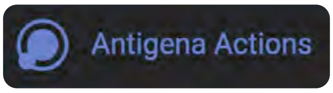
```
24098
Mon Oct 21
15:02:33

Mickey Desktop

Antigena Response
Event message Enforce pattern of life for 5 minutes
Outgoing traffic
Event details Model Antigena / Network / Significant Anomaly / Antigena
Significant Anomaly from Client Block
Strength 84 %
Source has tag Antigena All
2 Model
Event message Device / Multiple Model Breaches (not *antigena*)
Event message Device / Multiple Model Breaches did not contain Device / Activity
Identifier or Device / Anomaly Indicators or Tags / or User / Key User /
or Inoculation /
Outgoing traffic
With Unique message fields
Strength 100 % > 50 or 30 %
Source has tag Antigena All
```

Clicking on a Model Breach Event Log opens up the connectivity prior to the Antigena response, including any Models that were breached. In the case below, the device's pattern of life was enforced for 5 minutes and all outgoing traffic was blocked for 10 minutes.

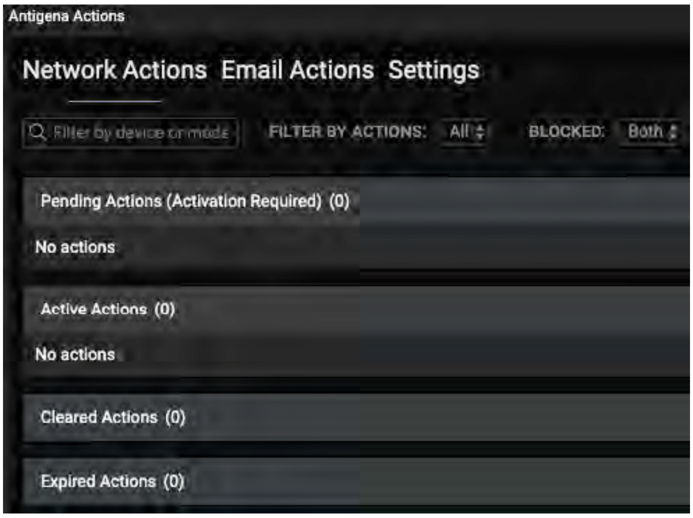


```
Mon Oct 21, 15:02:32   Mickey Desktop breached model Device / Multiple Model Breaches
Mon Oct 21, 15:02:32   Antigena Response – Block all outgoing traffic for 10 minutes
Mon Oct 21, 15:02:32   Antigena Response – Enforce pattern of life for 5 minutes
Mon Oct 21, 15:02:31   Mickey Desktop breached model Unusual Activity / Large Volume of Kerberos Failures [88]
```

All the Antigena Actions that have been taken can be observed from the Antigena Actions section in the main menu of the Threat Visualizer.



Clicking this opens up a new window that shows pending, active, cleared and expired actions that have been taken with the network environment.



Pending Actions (Activation Required) (0)

No actions

Active Actions (0)

No actions

Cleared Actions (0)

Expired Actions (0)

Antigena Email

Email security is an increasingly important field. More than 90% of malware today originates from the inbox, but 98% of attacks in the inbox contained no malware. Antigena Email applies the self-learning Autonomous Response to dynamic email environments, analyzing the flow of inbound, outbound and internal email traffic.

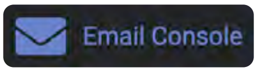
Antigena Email learns the pattern of life for every user and correspondent and its understanding can be strengthened by the traffic observed in the Enterprise Immune system. It can quickly detect malicious and anomalous emails and interrupt the delivery, so it does not reach the intended recipient.

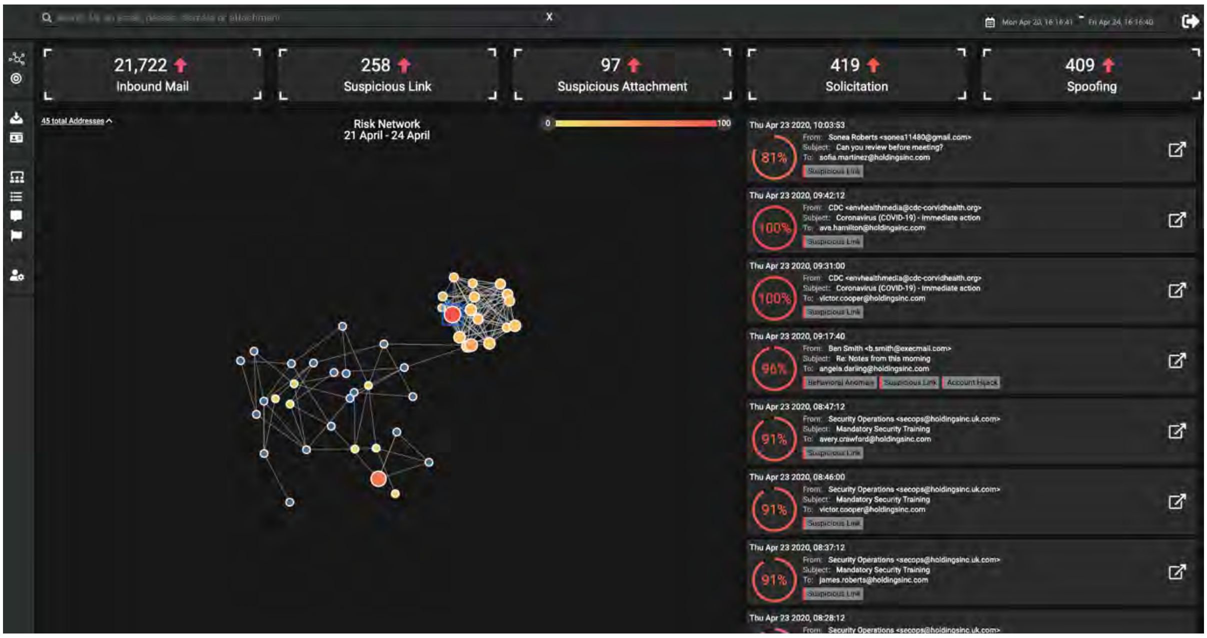
Antigena Email can stop a range of attacks, including:

- Advanced spear phishing
- Social engineering and impersonation
- Supply chain account takeover
- Business Email Compromise (BEC)
- Internal account hijack
- External data loss
- Unknown malware and ransomware

The Antigena Email system can distinguish between legitimate communication and that which has malicious intent and will therefore action "bad" emails while still letting through the "good".

The Antigena Email Console can be accessed from the Threat Visualizer main menu. Upon clicking, the Email Console will be opened in a new tab.





21,722 Inbound Mail

258 Suspicious Link

97 Suspicious Attachment

419 Solicitation

409 Spoofing

Risk Network
21 April - 24 April

Thu Apr 23 2020, 10:03:53
81%
From: Sonea Roberts <sonea11480@gmail.com>
Subject: Can you review before meeting?
To: sofia.martinez@holdingsinc.com
Suspicious Link

Thu Apr 23 2020, 09:42:12
100%
From: CDC <envhealthmedia@cdc-corvidhealth.org>
Subject: Coronavirus (COVID-19) - Immediate action
To: ave.hamilton@holdingsinc.com
Suspicious Link

Thu Apr 23 2020, 09:31:00
100%
From: CDC <envhealthmedia@cdc-corvidhealth.org>
Subject: Coronavirus (COVID-19) - Immediate action
To: victor.cooper@holdingsinc.com
Suspicious Link

Thu Apr 23 2020, 09:17:40
96%
From: Ben Smith <b.smith@execmail.com>
Subject: Re: Notes from this morning
To: angela.darling@holdingsinc.com
Behavioral Anomaly Suspicious Link Account Hijack

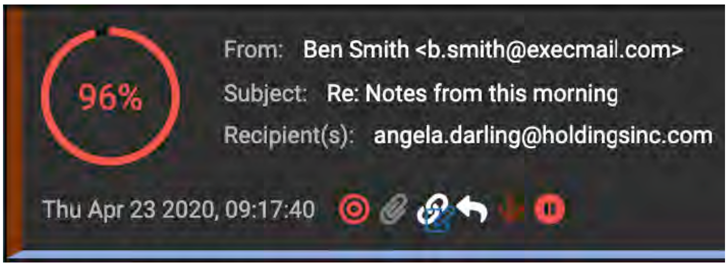
Thu Apr 23 2020, 08:47:12
91%
From: Security Operations <secops@holdingsinc.uk.com>
Subject: Mandatory Security Training
To: avery.crawford@holdingsinc.com
Suspicious Link

Thu Apr 23 2020, 08:46:00
91%
From: Security Operations <secops@holdingsinc.uk.com>
Subject: Mandatory Security Training
To: victor.cooper@holdingsinc.com
Suspicious Link

Thu Apr 23 2020, 08:37:12
91%
From: Security Operations <secops@holdingsinc.uk.com>
Subject: Mandatory Security Training
To: james.roberts@holdingsinc.com
Suspicious Link

Thu Apr 23 2020, 08:28:12
From: Security Operations <secops@holdingsinc.uk.com>

The Dashboard view gives an at-a-glance overview of changes in trends of malicious mailflow, the most targeted at-risk users and critical emails exhibiting signs of malicious intent.



96%

From: Ben Smith <b.smith@execmail.com>

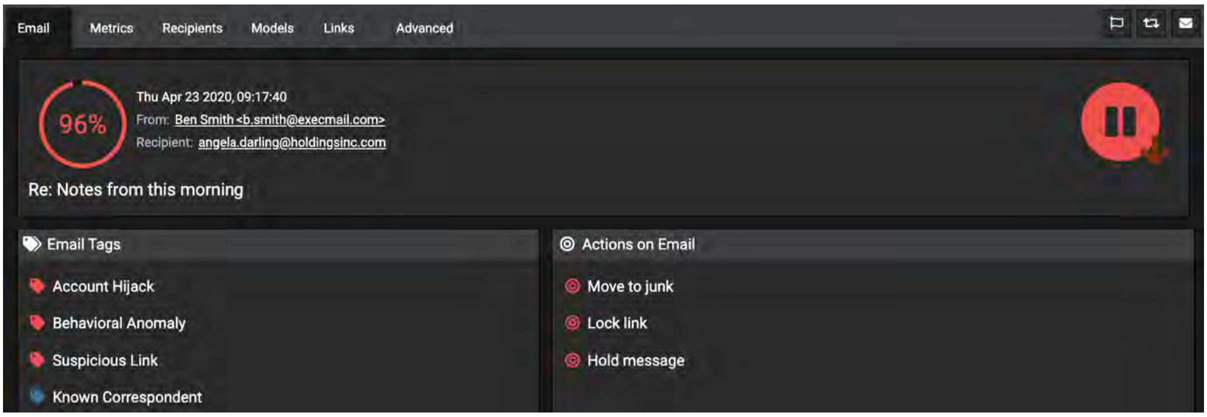
Subject: Re: Notes from this morning

Recipient(s): angela.darling@holdingsinc.com

Thu Apr 23 2020, 09:17:40

Emails are represented by their metadata, including who the email is from/to, the subject and the send time. Each email is assigned an anomaly score and has a range of quick view icons. These can assist triaging emails and understanding how they've been actioned.

Clicking on individual emails opens up more detailed information which can provide context. Emails can be investigated and manually actioned from the Email Console.



96%

Thu Apr 23 2020, 09:17:40

From: Ben Smith <b.smith@execmail.com>

Recipient: angela.darling@holdingsinc.com

Re: Notes from this morning

Email Tags

- Account Hijack
- Behavioral Anomaly
- Suspicious Link
- Known Correspondent

Actions on Email

- Move to junk
- Lock link
- Hold message

Darktrace Services

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

Proactive Threat Notifications

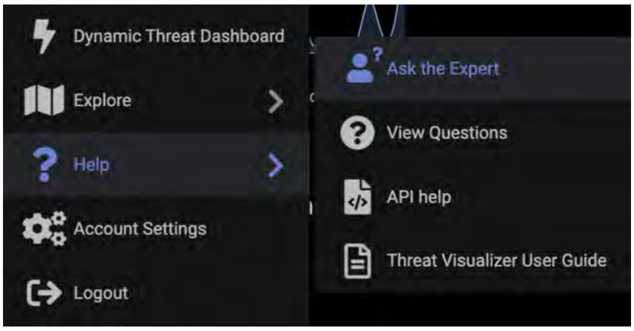
The Proactive Threat Notifications are part of Darktrace's round-the-clock SOC, which is comprised of expert analysts located around the globe, covering all time zones. If you have call-home enabled and you are signed up for this service, Darktrace analysts will review any breaches in your Threat Visualizer that fall under the Enhanced Monitoring category. They will consequently notify you if they find anything significantly suspicious via email, text or a phone call. Darktrace can offer real time advice and assistance to help you tackle live attacks.

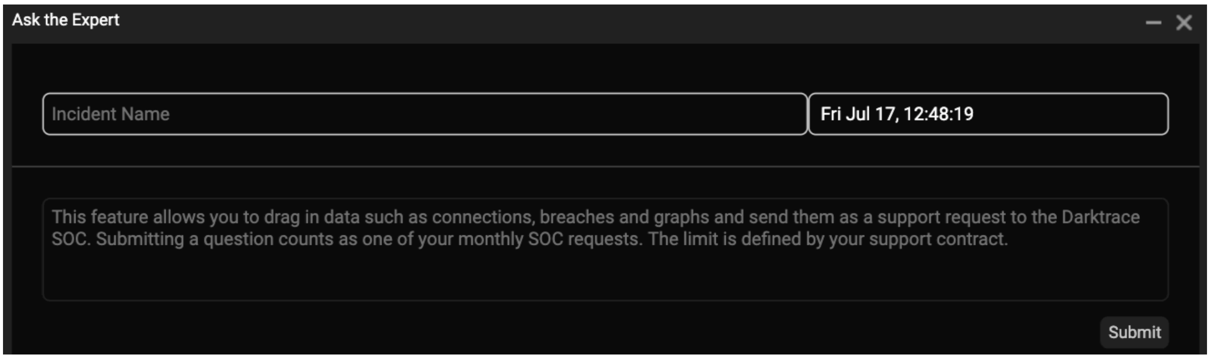
These PTNs, provided by one of our analysts, will include a short summary of the threat in question, the breach device and the Model Breach ID, effectively arming you with the appropriate knowledge before investigating the breach in your Threat Visualizer Interface.

Ask the Expert

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

To access this feature, navigate down to Help in the Threat Visualizer main menu and select Ask the Expert from the submenu. Doing so will open up a window, allowing you to type in information which will be sent to our cyber security experts.





Fri Jul 17, 12:48:19

This feature allows you to drag in data such as connections, breaches and graphs and send them as a support request to the Darktrace SOC. Submitting a question counts as one of your monthly SOC requests. The limit is defined by your support contract.

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

9. Learning Outcomes

Thank you for completing Part 2 of the Threat Visualizer course. We hope this has given you the confidence to investigate a variety of aspects within your deployment.

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

□	**I am able to appreciate the benefits of AI Analyst**
□	**I understand the uses for Tags and be able to apply them to Devices**
□	**I can perform basic queries in Advanced Search**
□	**I can create packet captures and perform packet inspection**
□	**I am able to generate reports of network activity**
□	**I am able to successfully follow the Analyst Workflow**
□	**I am aware of additional offerings from Darktrace**

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.

10. Cheat Sheet

Advanced Search Exercises

a. Were there any SSL queries to eBay in the last 60 mins?

@type:"ssl" AND @fields.server_name:*ebay*

b. Find all SSH and RDP connectivity originating from your device in the last 7 days. (If your machine is not on the network select a different host).

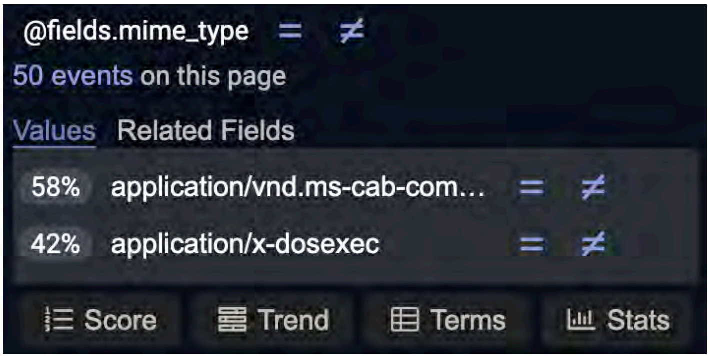
(@type:"ssh" OR @type:"rdp") AND @fields.source_ip:"<your IP>"

c. Find the SHA1 hashes of all the EXE files in the last 48hrs. Remember the side filters will change depending what you search for.

Begin by searching for all SHA1 or MIME types:

@fields.sha1:* OR @fields.mime_type:*

It is also useful to view the breakdown of MIME types:



@fields.mime_type = ≠

50 events on this page

58% application/vnd.ms-cab-com... = ≠

42% application/x-dosexec = ≠

Then review the appropriate filters to search for:

@type:"files_identified" AND @fields.mime_type:"application/x-dosexec"

d. Return the failed Kerberos Type events over the last 7 days.

@type:"kerberos" AND @fields.success:"false"

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

Locate a connection and search *@fields.uid:"<connection_uid>"*

Or use the drop-down menu for a connection within the Threat Visualizer and select "View Advanced Search for this event".

f. Find the user agent and the method of the last HTTP request sent by your machine. (If your machine is not on the network, select a different host).

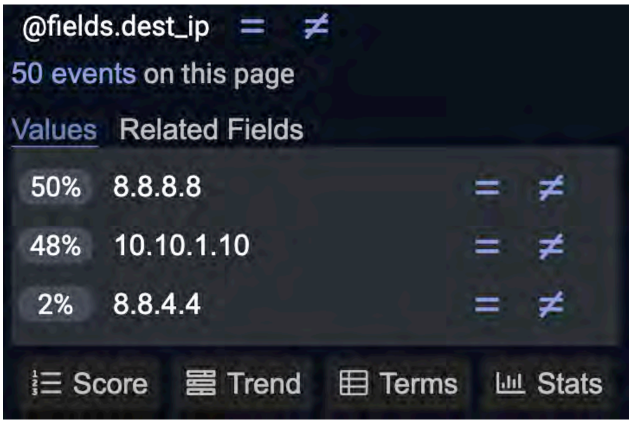
@fields.source_ip:<your IP> AND @type:"http"

g. Locate all internal DNS servers.

Use *@type:"dns"*. However this could show both internal and external DNS servers.

View the results of @fields.dest_ip:

This displays both internal servers, as well the external Google DNS.



@fields.dest_ip = ≠

50 events on this page

50%	8.8.8.8	=	≠
48%	10.10.1.10	=	≠
2%	8.8.4.4	=	≠

To exclude external domains, you could restrict all destination IP addresses (@fields.dest_ip:10.*, 192.168... or 172...), but this would result in a long query string.

An easy way is searching for the local_resp field value:

@fields.local_resp:"true"

This does not check for a response. It just examines the addresses of connections to check if they are internal

h. Find connections to external IP addresses which use the FTP protocol.

***@type:"ftp" AND @fields.local_resp:"false"* will not work because the local_resp value is not returned by the FTP type field.**

Instead use:

@fields.service:"ftp" AND @fields.local_resp:"false"