CYBER ANALYST PART 1 – ADVANCED ANALYSIS

Cyber Analyst Part 1 – Advanced Analysis
Manual v2.0.1 – Darktrace v5

Table of Contents

1. Learning Objectives

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

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

- **Use fundamental techniques to confidently navigate Advanced Search**
- **Determine how much data was transmitted over a number of connections**
- **Perform effective queries and interpret network traffic in Advanced Search**
- **Effectively investigate different categories of network breaches**
- **Carry out advanced analytical processes utilizing Darktrace analytical tools**

For this course, a basic knowledge of the Threat Visualizer is assumed. This material is covered in Threat Visualizer Part 1 – Familiarization and Threat Visualizer Part 2 – Investigation. On completion of this course, it is advised that you next attend Cyber Analyst Part 2 – Model Optimization.

2. Analyst Prerequisites

By embarking on this course, it is assumed that you have attended parts 1 and 2 of the Threat Visualizer essentials course. This section reviews the basic underlying knowledge Darktrace suggests junior Cyber Security Analysts should have. This list is provided for review and the teaching of these concepts and material is outside the scope of this course.

Networking

In terms of networking, you should:

- Understand network architecture including routers, switches, subnets and VLANs
- Discern the difference between implicit/explicit proxies, NATing and routers as well as a knowledge of what happens when a source IP address is changed
- Have a knowledge of common security controls such as Firewall, SIEM, IDS/IPS and DLP
- Be aware of ICS/SCADA network structure and terminology (in depth knowledge not a necessary prerequisite)
- Recognize common processes such as file sharing, RPC, and understand how a web request/communications work
- Be able to interpret common authentication protocols, particularly Kerberos
- Possess knowledge of TCP/IP and of the most common ports/associated protocols:

Port	Protocol	Description
20/21	TCP	FTP (File Transfer Protocol)
22	TCP/UDP	SSH (Secure Shell, Secure Copy Protocol, Secure File Transfer Protocol)
23	TCP/UDP	Telnet
25	TCP/UDP	SMTP (for sending outgoing emails)
43	TCP	WHOIS function
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
88	TCP	Kerberos

110	TCP	POP3 (for receiving email)
119	TCP	NNTP (Network News Transfer Protocol)
123	UDP	Network Time Protocol (NTP)
137/138/139	TCP/UDP	NetBIOS
161/162	TCP/UDP	Simple Network Management Protocol (SNMP)
143	TCP/UDP	IMAP4 Protocol (for email service)
194	TCP	Internet Relay Chat
389	TCP/UDP	LDAP (lightweight directory access)
443	TCP	Secure HTTP over SSL (https)
445	TCP	Server Message Block (SMB) Protocol for network file sharing
465	TCP	Secure SMTP (email) using SSL
514	UDP	Syslog
636	TCP/UDP	Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
989/990	TCP/UDP	Secure FTP using SSL
993	TCP	Secure IMAP protocol over SSL (for emails)
995	TCP	POPS
1433	TCP/UDP	Microsoft SQL Server
1521	TCP	Oracle Database
3306	TCP/UDP	MariaDB/MySQL Database Server
3389	TCP	RDP (Remote Desktop Protocol)
5432	TCP	PostgreSQL Database Server
5985	TCP	WinRM (Microsoft Windows Remote Management)
5986	TCP	WinRM over HTTPS
7680	TCP	Windows 10 peer-to-peer update distribution

Malware

In terms of malware/threat knowledge, you should:

- Have knowledge of attack methods such as:
    - Domain shadowing
    - Exploit kits
    - Domain fluxing
    - Botnets
    - Spear phishing with malicious documents

- Be able to explain what an Advanced Persistent Threat (APT) is

- Have a basic knowledge of different forms of malware and the relation between exploits, downloaders, droppers, trojans, and rootkits

- Understand and perceive the difference between penetration testing, red teaming and vulnerability scanning

- Recognize what network or vulnerability scanning looks like

- Grasp what lateral movement is and recognize the signs

- Learn the kill chain phases involved in compromising a network

Research

Using prior experience from the Threat Visualizer interface, you should know:

- What is understood by Open-Source Intelligence (OSINT) and how to research IPs and domains

- How to detect and investigate unidirectional traffic

- Recognize when Darktrace is not mapping devices correctly and when Model blurring is occurring

- What the different SMB notices mean

- How ransomware works and is presented in the User Interface

- What the history field represents in Advanced Search

Security

Finally, you should have general knowledge of:

- How to maintain good Operations Security (OPSEC) by keeping your device and software up to date.

3. Advanced Search Navigation and Tips

This introductory section provides a recap of some navigation tips for Advanced Search as well as providing further details for more experienced Advanced Search users.

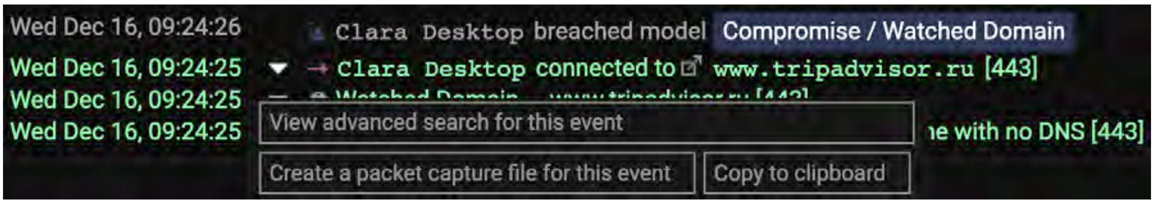
Pivoting Between Interfaces

As a wealth of information can be found in the Threat Visualizer and Advanced Search, it is useful to be able to pivot between these interfaces to investigate details of an event further.

Threat Visualizer to Advanced Search

While the Threat Visualizer's Event Log provides a significant level of visibility into a device's communications, at times there is the desire to inspect additional details of a connection, or to use it as a starting point for a broader query of the network traffic.

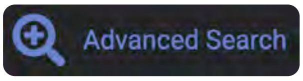
1. Select **View advanced search for this event** from the grey drop-down arrow to the left of an entry to view the same communication in Advanced Search.



```
Wed Dec 16, 09:24:26      Clara Desktop breached model Compromise / Watched Domain
Wed Dec 16, 09:24:25  ▼ → Clara Desktop connected to www.tripadvisor.ru [443]
Wed Dec 16, 09:24:25      Watched Domain  www.tripadvisor.ru [443]
Wed Dec 16, 09:24:25                                            ne with no DNS [443]
```

View advanced search for this event
Create a packet capture file for this event
Copy to clipboard

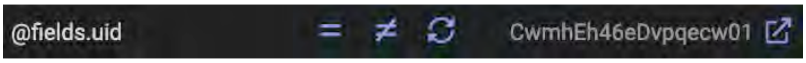
__Note:__ An unrestricted Advanced Search tab can be opened by selecting Advanced Search option from the main menu.



Advanced Search to the Threat Visualizer

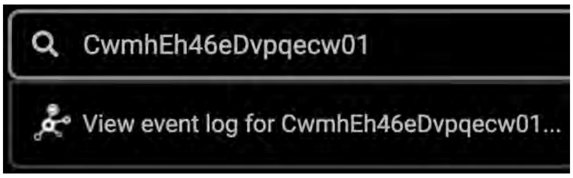
It often helps to review details of the source or destination in the Threat Visualizer. It is easy to pivot to the device in the Threat Visualizer Device View by entering the value of a corresponding connection's **uid** field into the Threat Visualizer's Omnisearch bar.

1. Copy the **uid** field value from an advanced search result.



@fields.uid = ≠ CwmhEh46eDvpqecw01

2. Paste the alphanumeric string into the **Omnisearch bar** in the Threat Visualizer.

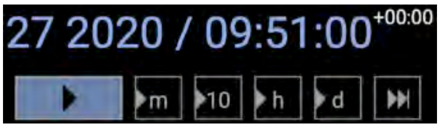


CwmhEh46eDvpqecw01

View event log for CwmhEh46eDvpqecw01...

__Note:__ Alternatively, click the link icon to the right of the field in Advanced Search to open the appropriate Event Log within Threat Visualizer in a new browser tab.

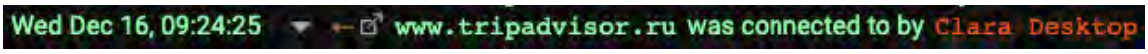
3. The Event Log will only display communications that have occurred in the two weeks prior to the visualizer time. Change the time accordingly using the buttons under the Time Selector in the top right-hand corner.



27 2020 / 09:51:00 +00:00

__Note:__ The final icon brings the visualizer to the current time, which can be useful to see real-time events from the device of interest.

4. Click on the name of the modeled device to navigate to its **Device View**. This allows for device investigation surrounding the time of the event of interest.



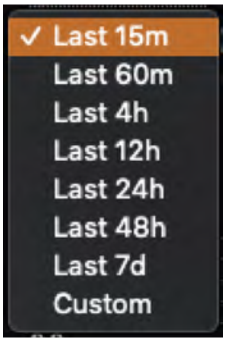
```
Wed Dec 16, 09:24:25 www.tripadvisor.ru was connected to by Clara Desktop
```

Useful Functionalities

1. Visiting Advanced Search directly from the Threat Visualizer main menu will set the time period to the **last 15 minutes**.

   Similarly, when pivoting from a connection within the Threat Visualizer to Advanced Search, the time will reflect the time period surrounding the connection UID.

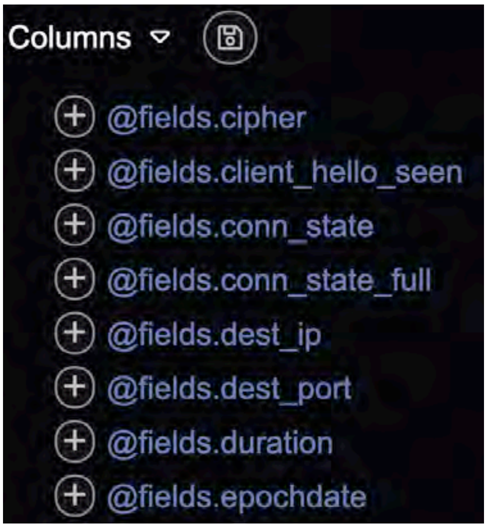
   Generally, it may be useful to expand the time period out to the **last 7 days** in order to get an understanding of events occurring over the last week.



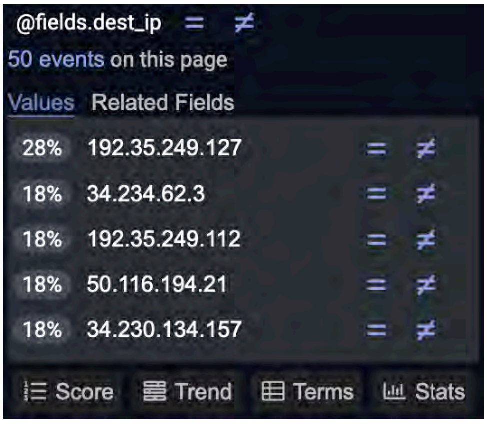
2. Notice the **Columns** list down the left-hand side of the screen. Clicking the plus to the left of any field will add that field as a column in the Advanced Search table.

   Note: *If the Columns list is hidden, click the right facing arrow under the Darktrace logo in the top left of the screen.*

3. Click the **plus or minus icon** to the left of a field to display or remove the chosen fields in the table of events, rather than just displaying the default Type and Message fields.



4. Clicking on an entry will display the field **dialog**. This shows a percentage breakdown of the chosen field for the 50 events displayed on the page and allows the user to perform statistical analysis on the results.



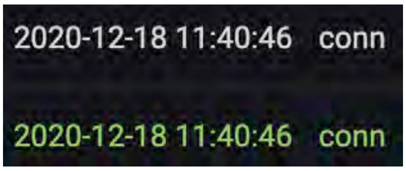
28%	192.35.249.127	=	≠
18%	34.234.62.3	=	≠
18%	192.35.249.112	=	≠
18%	50.116.194.21	=	≠
18%	34.230.134.157	=	≠

   a. Click the equals or not equals sign to filter the results on where the field exists or does not exist.

   = ≠

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

   b. With the field dialog open, click a value to **highlight events** on the current page in **green** where that result matches the field. The same process needs to be repeated per page.

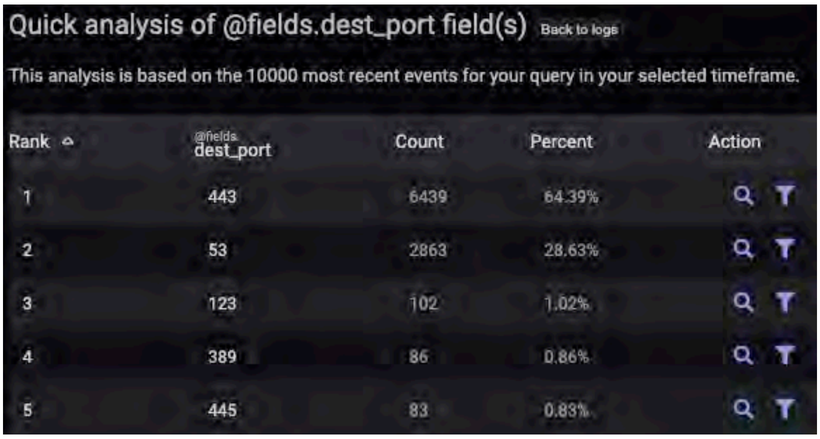


```
2020-12-18 11:40:46   conn

2020-12-18 11:40:46   conn
```

Score

c. Clicking **Score** for a chosen field will rank all the 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.



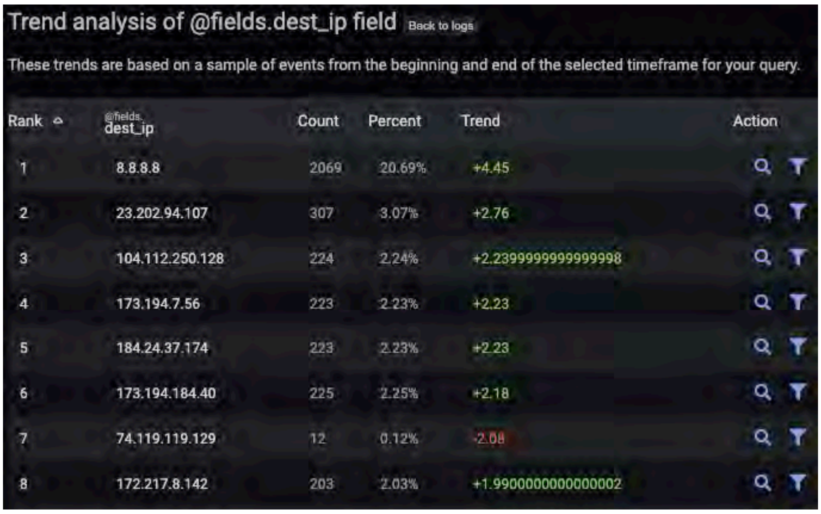
Quick analysis of @fields.dest_port field(s) Back to logs

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

Rank	@fields. dest_port	Count	Percent	Action
1	443	6439	64.39%	🔍 ▼
2	53	2863	28.63%	🔍 ▼
3	123	102	1.02%	🔍 ▼
4	389	86	0.86%	🔍 ▼
5	445	83	0.83%	🔍 ▼

Trend

d. 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 where values are denoted in **red** and **green** for decreases and increases in popularity respectively.



Trend analysis of @fields.dest_ip field Back to logs

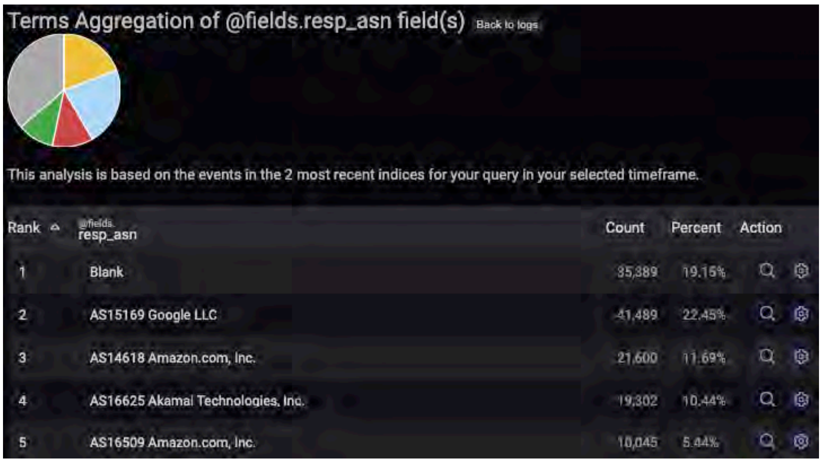
These trends are based on a sample of events from the beginning and end of the selected timeframe for your query.

Rank	@fields. dest_ip	Count	Percent	Trend	Action
1	8.8.8.8	2069	20.69%	+4.45	🔍 ▼
2	23.202.94.107	307	3.07%	+2.76	🔍 ▼
3	104.112.250.128	224	2.24%	+2.2399999999999998	🔍 ▼
4	173.194.7.56	223	2.23%	+2.23	🔍 ▼
5	184.24.37.174	223	2.23%	+2.23	🔍 ▼
6	173.194.184.40	225	2.25%	+2.18	🔍 ▼
7	74.119.119.129	12	0.12%	-2.08	🔍 ▼
8	172.217.8.142	203	2.03%	+1.9900000000000002	🔍 ▼

Terms

e. Selecting **Terms** for 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.

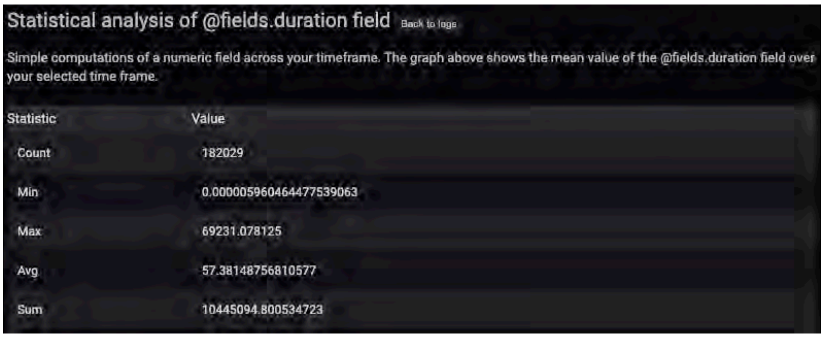


Terms Aggregation of @fields.resp_asn field(s) Back to logs

This analysis is based on the events in the 2 most recent indices for your query in your selected timeframe.

Rank	@fields. resp_asn	Count	Percent	Action
1	Blank	35,389	19.15%	🔍 ⚙
2	AS15169 Google LLC	41,489	22.45%	🔍 ⚙
3	AS14618 Amazon.com, Inc.	21,600	11.69%	🔍 ⚙
4	AS16625 Akamai Technologies, Inc.	19,302	10.44%	🔍 ⚙
5	AS16509 Amazon.com, Inc.	10,045	5.44%	🔍 ⚙

f. 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.

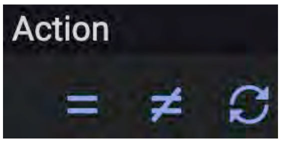


Statistical analysis of @fields.duration field Back to logs

Simple computations of a numeric field across your timeframe. The graph above shows the mean value of the @fields.duration field over your selected time frame.

Statistic	Value
Count	182029
Min	0.000005960464477539063
Max	69231.078125
Avg	57.38148756810577
Sum	10445094.800534723

5. Expand an entry by clicking on it and notice that for every field it contains, there are three icons in the **Action** column. The **equals** and **not equals symbols** will add the field to the search bar with an AND or NOT respectively; The pivoting arrows will append the source and destination IPs with the selected field.

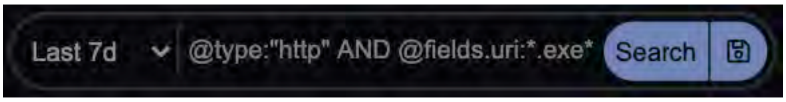


Save Options

There are multiple options within Advanced Search which allow the user the option to save queries, fields and take notes. Saving queries can allow for easy access to commonly used searches while saving fields in the Columns list can display columns of useful information in the Advanced Search table. All of these options require local storage, so this is not recommended for shared workstations.

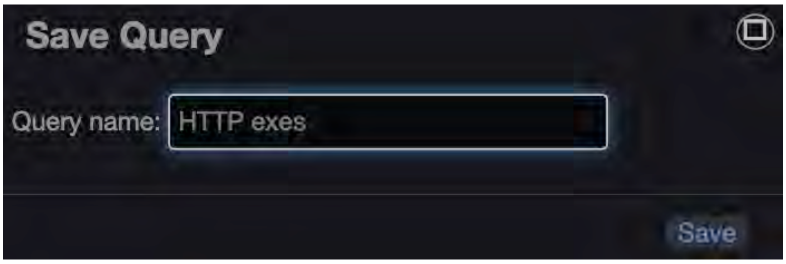
Queries

1. First, to save a query, populate it in the search bar and click the **Save icon** to the right of the bar.



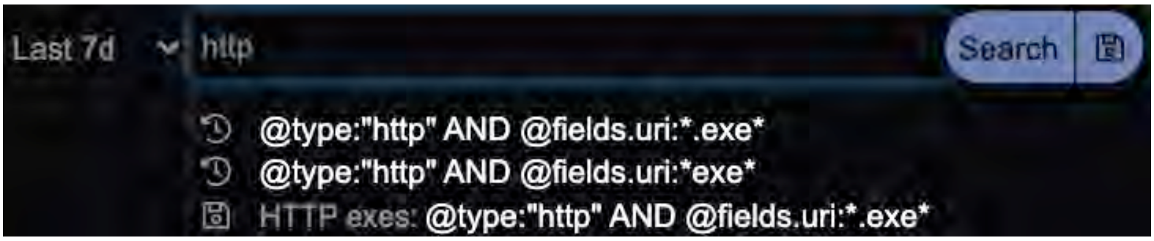
@type:"http" AND @fields.uri:*.exe*

2. Then, provide a **query name** and click **Save**.



Query name: HTTP exes

3. For future searches, **begin typing in the query name** to locate the saved query and view any historical queries that also match the criteria.



http

@type:"http" AND @fields.uri:*.exe*

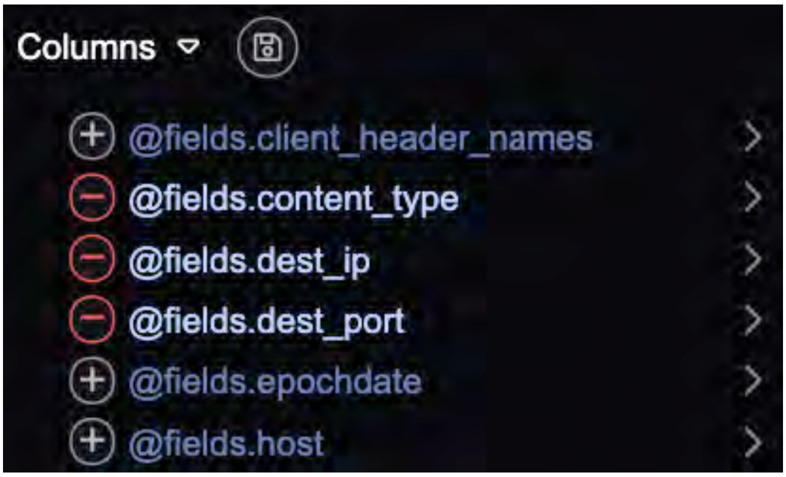
@type:"http" AND @fields.uri:*exe*

HTTP exes: @type:"http" AND @fields.uri:*.exe*

Fields

1. Navigate to the **Columns list** down the left-hand side of the interface and choose appropriate fields to display the selected headings in the table under the graph.

2. Click the **Save** icon to the right of the Columns title.



⊕ @fields.client_header_names

⊖ @fields.content_type

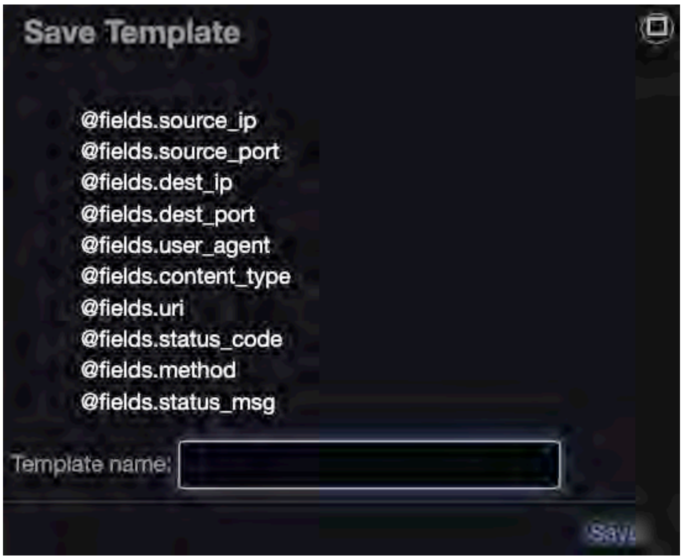
⊖ @fields.dest_ip

⊖ @fields.dest_port

⊕ @fields.epochdate

⊕ @fields.host

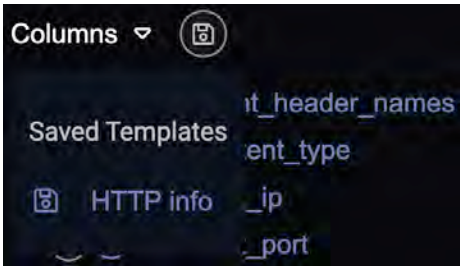
3. A new dialog will appear with all the selected fields. Confirm these are the fields to be used to define the template, **assign it a template name** and click **Save**.



@fields.source_ip
@fields.source_port
@fields.dest_ip
@fields.dest_port
@fields.user_agent
@fields.content_type
@fields.uri
@fields.status_code
@fields.method
@fields.status_msg

Template name:

4. From now on, it is possible to use the drop-down arrow located to the right of the Columns heading and select **Saved Templates** from the list.



Notepad

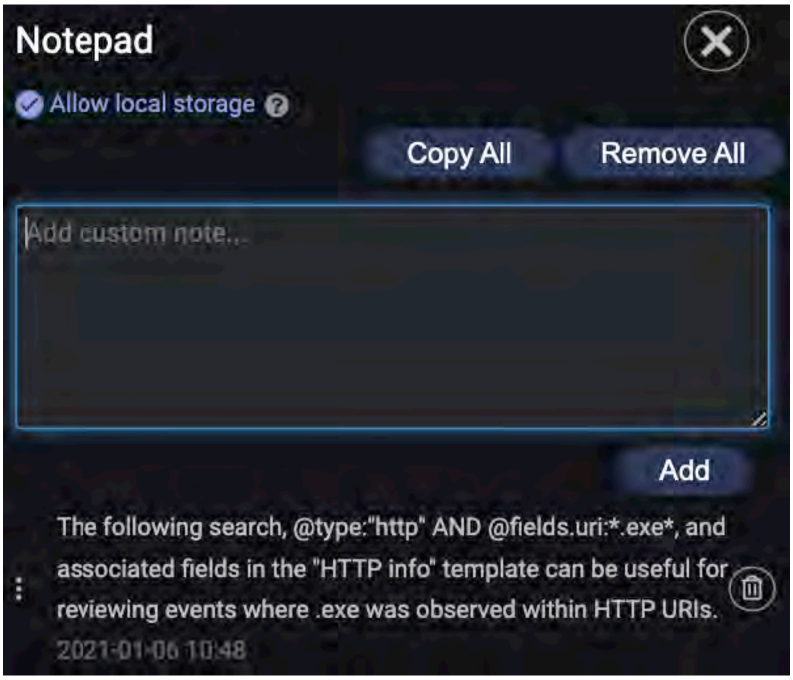
1. Click the **Notepad** button, as denoted by the **speech bubble** in the right-hand corner of the interface, to begin writing notes or reminders.

2. Begin typing in the **Add custom note** box to add notes and click **Add** once ready.

   Notes made previously will be presented under this box with the **date and time** they were created.

   All existing notes can be copied out of the Notepad function, using **Copy All**, so they can be pasted outside of the interface.

   They can be removed individually by clicking the bin icon next to a note or all notes can be deleted by clicking **Remove All**.

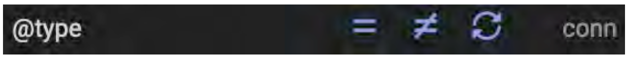


The following search, @type:"http" AND @fields.uri:*.exe*, and associated fields in the "HTTP info" template can be useful for reviewing events where .exe was observed within HTTP URIs.
2021-01-06 10:48

Determining Cumulative Data Transfer

It is straightforward to find the upload or download that has occurred over a single connection, by using the **orig_bytes** and **resp_bytes** fields respectively from the **conn** event. However, it is often useful to determine the total transfer over multiple communications, for example, a series of SSL connections between a particular source and destination IP.

1. Within the Advanced Search events, locate a **conn** event:



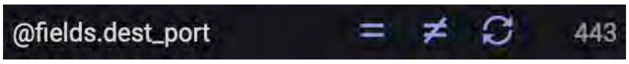
@type = ≠ ⟳ conn

@type:conn

2. As the amount of transfer between two IPs may be interesting, click the **pivot arrows** next to **@type:conn** to **view similar connections**. This will apply a query to the search bar:

@type:conn **AND (@fields.source_ip:10.0.0.1 AND @fields.dest_ip:10.1.0.1)**

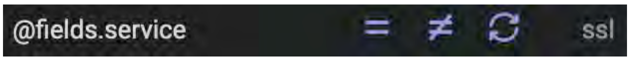
3. Click the equals sign next to @fields.destination_port to specify the **destination port** and add to the query:



@fields.dest_port = ≠ ⟳ 443

@type:conn AND (@fields.source_ip:10.0.0.1 AND @fields.dest_ip:10.1.0.1) **AND @fields.dest_port:443**

4. Alternatively (or additionally), specify the **application protocol** by clicking the equals sign next to @fields.service:

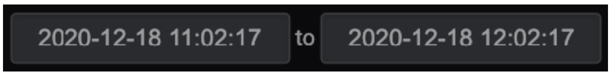


@fields.service = ≠ ⟳ ssl

@type:conn AND (@fields.source_ip:10.0.0.1 AND @fields.dest_ip:10.1.0.1) **AND @fields.service:ssl**

Note: *Searching by port number alone does not account for services accessed via non-default ports. Also, be aware that when searching by @fields.service, or any other field that is specific to a certain type of event, results for other event types may be excluded.*

5. Additional fields can also be used as needed, but these will often be sufficient to isolate a session once you have selected an **appropriate time frame**.



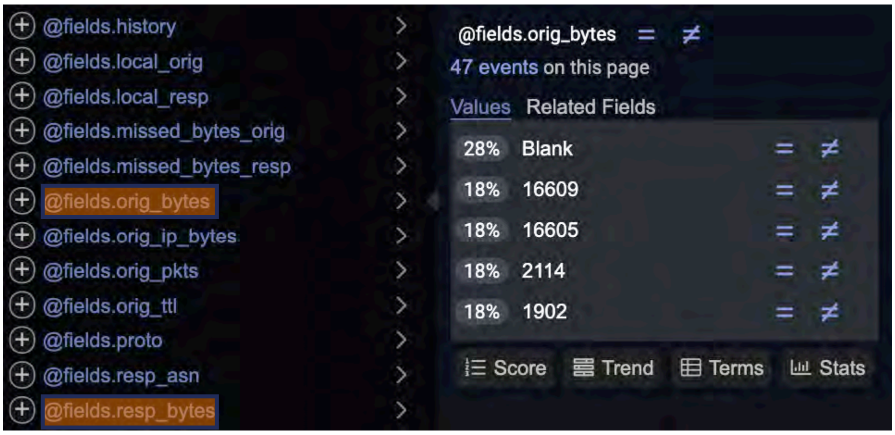
2020-12-18 11:02:17 to 2020-12-18 12:02:17

6. The **orig_bytes** and **resp_bytes** fields list the payload transfer (upload and download, respectively). If desired, adjust the query to ensure the results only include connections with non-zero upload or download.

> @type:conn AND (@fields.source_ip:10.0.0.1 AND @fields.dest_ip:10.1.0.1) AND @fields.dest_port:443 **AND @fields.orig_bytes:>0**
>
> @type:conn AND (@fields.source_ip:10.0.0.1 AND @fields.dest_ip:10.1.0.1) AND @fields.dest_port:443 **AND @fields.resp_bytes:>0**

Note: *Rather than using quotation marks around values, the greater than (>) or less than (<) symbols can be utilized to show ranges of results rather than exact matches.*

7. With the query entered, these **fields are listed on the left-hand side** of the interface (assuming a nonzero transfer has been observed over one or more of the communications).



- @fields.history
- @fields.local_orig
- @fields.local_resp
- @fields.missed_bytes_orig
- @fields.missed_bytes_resp
- @fields.orig_bytes
- @fields.orig_ip_bytes
- @fields.orig_pkts
- @fields.orig_ttl
- @fields.proto
- @fields.resp_asn
- @fields.resp_bytes

@fields.orig_bytes = ≠

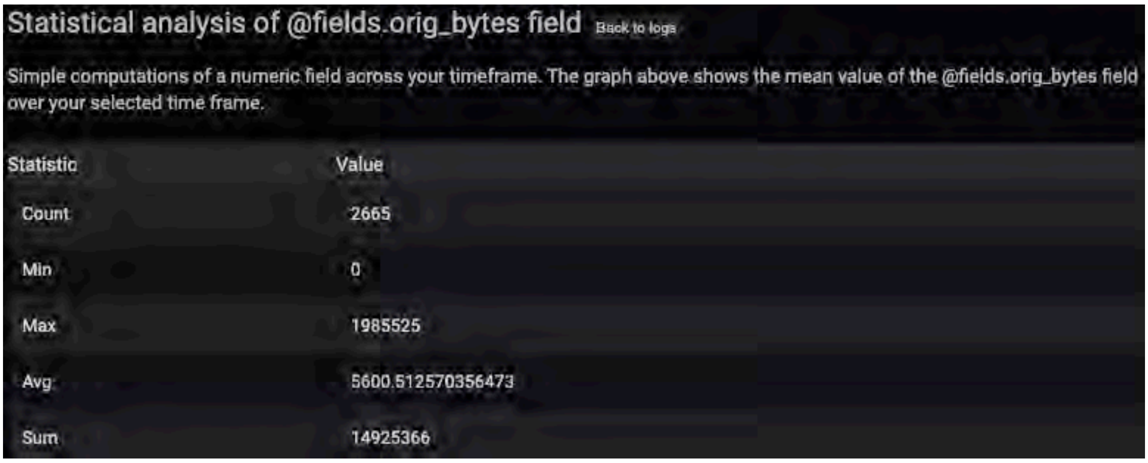
47 events on this page

Values Related Fields

28%	Blank	= ≠
18%	16609	= ≠
18%	16605	= ≠
18%	2114	= ≠
18%	1902	= ≠

8. Clicking on one of these fields opens a **dialog window** to the right presenting values for the selected field displayed on the current page of events.

9. Click the **Stats** button**.** This will provide, among other values, a **sum** representing the cumulative upload or download in bytes for the query and time frame.



Statistical analysis of @fields.orig_bytes field

Simple computations of a numeric field across your timeframe. The graph above shows the mean value of the @fields.orig_bytes field over your selected time frame.

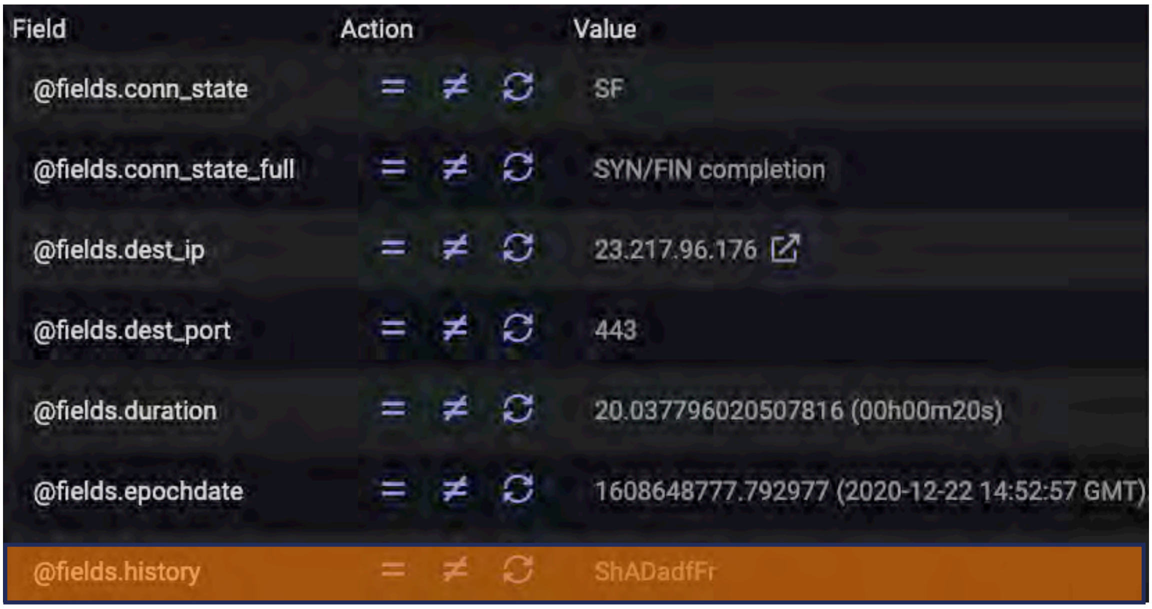
Statistic	Value
Count	2665
Min	0
Max	1985525
Avg	5600.512570356473
Sum	14925366

Note: *The count may differ from the "hits" if the query doesn't ensure the evaluated field is present in all results.*

Understanding the History Field

When reviewing **connection** events (@type:"conn") the **history** field describes the types of packets exchanged in either direction. Connections are only listed in Advanced Search upon completion. In advance of such time, one or more **conn_long** events may be listed with details of the ongoing connection.

1. In Advanced Search, review the **history** field for a TCP connection.



Field	Action	Value
@fields.conn_state	= ≠ ↻	SF
@fields.conn_state_full	= ≠ ↻	SYN/FIN completion
@fields.dest_ip	= ≠ ↻	23.217.96.176
@fields.dest_port	= ≠ ↻	443
@fields.duration	= ≠ ↻	20.037796020507816 (00h00m20s)
@fields.epochdate	= ≠ ↻	1608648777.792977 (2020-12-22 14:52:57 GMT)
@fields.history	= ≠ ↻	ShADadfFr

A successful connection typically appears as a succession of letters, e.g. **ShADadFf**.

Note: *Packets from the connection source are displayed in uppercase; those sent in response are displayed in lowercase.*

2. Use the following table to interpret the steps in the depicted transaction.

Letter	Meaning
s	a SYN without the ACK bit set
h	a SYN+ACK (“handshake”)
a	a pure ACK ("acknowledge")
d	packet(s) with payload (“data”)
f	packet with FIN bit set ("finish")
r	packet with RST bit set ("reset")
c	packet with a bad checksum
t	packet with retransmitted payload
w	packet with a zero-window advertisement
i	inconsistent packet (e.g. FIN+RST bits set)
q	multi-flag packet (SYN+FIN or SYN+RST bits set)
^	connection direction was heuristically flipped
g	Antigena Network reset packet(s)
m	a content gap was seen
t	packets with a retransmitted payload were seen
n	part of the connection was shunted (supported environments only)

a. The letter ‘**R**’ at the end of **ShADadR** indicates the source device sent a reset to close the connection.

b. A history of ‘**Dd**’ indicates data has been sent in both directions, often over UDP, as the letters representing a TCP handshake are not present. This can be confirmed via **@fields.proto**.

c. A history of ‘**^d**’ indicates the traffic direction was flipped. Analyzing the transmission from device B to device Am Darktrace heuristically determined that device A initiated communication. This typically occurs when the packets in one direction appear not to have been included in the data feed.

3. The table below gives a breakdown of potential connection states and their associated values, as seen in the history field.

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

Advanced Search Navigation Exercise

a. Practice pivoting from an event in the Threat Visualizer to its details in Advanced Search.

b. Practice pivoting from an Advanced Search log to its source device in the Threat Visualizer in two ways.

c. Use Advanced Search to determine the cumulative upload and download between two endpoints over a thirty-minute period.

d. Determine the cumulative upload and download for a series of connections specified by a Model Breach.

e. Use the score capability to view the history value for the last fifteen minutes of connectivity.

4. Investigating Threats Using Advanced Search

This section provides further details surrounding Advanced Search to facilitate efficient investigation. The search tactics covered in this course will provide the user additional skills, tools, and capabilities for research and investigation in the Darktrace Threat Visualizer. In addition, this section will also cover more ways to explore common searches and expand the understanding of common protocol results.

Searching for Externally Bound Unencrypted FTP Traffic

FTP is one example of an unencrypted protocol that, when used to communicate externally, can expose credentials, operational details, and/or internal company documents. Even if organizational policies permit the use of this application protocol, it is useful to be able to quickly locate any such cases where sensitive details are transmitted in clear text. Similar techniques can be applied for various unencrypted protocols; here FTP serves as an example.

1. FTP traffic can be searched for in multiple ways. The first method utilizes the **conn** event type as it includes the **local_resp** field, which indicates whether the destination is viewed as external. The **service** field can be used to filter results by application protocol. Use the following query to look for external FTP connections:

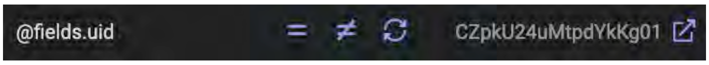
```
@fields.local_resp:false AND @fields.service:ftp
```

2. It is also possible to include failed attempts to connect to the protocols default destination port. Using the following parenthesis, search for the **FTP connections or connections on port 21**:

```
@fields.local_resp:false AND (@fields.service:ftp OR @fields.dest_port:21)
```

3. Any results of this query will be logs of type **conn** and therefore will not contain details specifically relevant to the FTP protocol. Such details are found within the **ftp** event type.

   A connection's **ftp** log can be found by searching solely for its **uid** value, using the equals icon.



@fields.uid = ≠ CZpkU24uMtpdYkKg01

4. To **view all similar connections** given a source and destination IP, use the pivot shortcut for a chosen log, e.g., destination port.

5. The **ftp** event type gives details of each command performed, including transmission of username and password and if any files were read or written.

   a. The **command** and **arg** fields detail each action taken.

   b. The PASS command will display a transmitted password as **<hidden>**, but this is a redaction. The value can be confirmed by inspecting a corresponding packet capture.

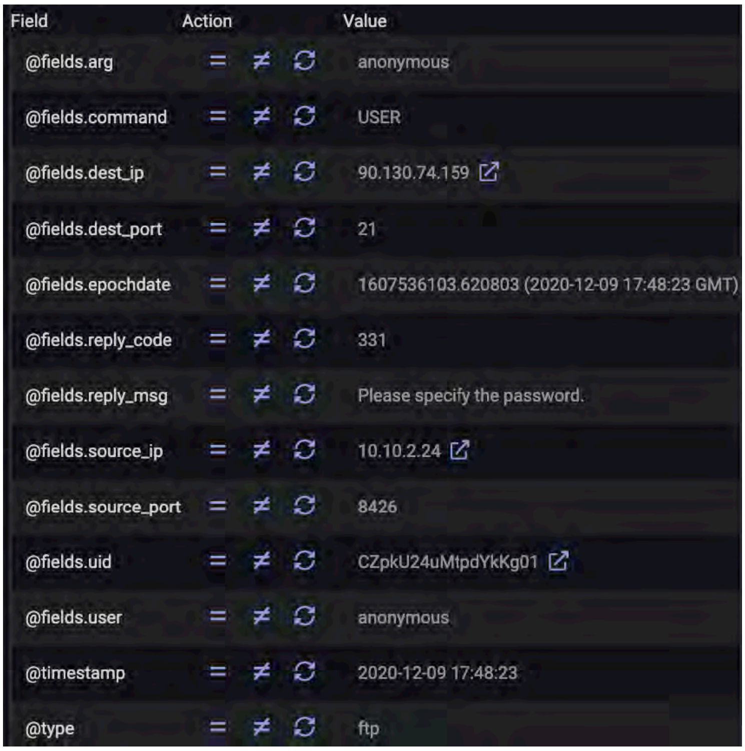
   c. The log of a STOR or RETR command includes the path to/from which a file has been written/read, which may provide insight into the nature or content of the file or service.

Reviewing the credential used for login, the destination server, and details of any additional operations performed may help ascertain the nature of the interaction and whether it is an event that needs to be addressed.

Optionally, use the **uid** or other aspects of the connection(s) to find and examine details of the internal device within the Threat Visualizer.

For a list of available FTP commands, see:

https://en.wikipedia.org/wiki/List_of_FTP_commands



Field	Action	Value
@fields.arg	= ≠ ↻	anonymous
@fields.command	= ≠ ↻	USER
@fields.dest_ip	= ≠ ↻	90.130.74.159
@fields.dest_port	= ≠ ↻	21
@fields.epochdate	= ≠ ↻	1607536103.620803 (2020-12-09 17:48:23 GMT)
@fields.reply_code	= ≠ ↻	331
@fields.reply_msg	= ≠ ↻	Please specify the password.
@fields.source_ip	= ≠ ↻	10.10.2.24
@fields.source_port	= ≠ ↻	8426
@fields.uid	= ≠ ↻	CZpkU24uMtpdYkKg01
@fields.user	= ≠ ↻	anonymous
@timestamp	= ≠ ↻	2020-12-09 17:48:23
@type	= ≠ ↻	ftp

6. If only successful external FTP events are of interest, it is possible to utilize the ftp event type directly by writing a query to search for the **@type:"ftp"** and look for any connections to IP addresses excluding any internal ranges.

```
@type:"ftp" AND NOT (@fields.dest_ip:10.* OR @fields.dest_ip:/172.<16-31>..+/
OR @fields.dest_ip:192.168.*)
```

Note: *The above syntax can be modified to include any externally owned ranges and can be applied to many Advanced Search queries.*

Try this:

Have any successful outbound FTP connections occurred in the past 7 days? Inspect the details of any operations performed and determine whether any sensitive information is likely to have been exposed.

Are there any examples of externally bound Telnet? If there has been any observed in recent history, try to determine the nature of the activity, reviewing the details present in Advanced Search and locating the internal device in the Threat Visualizer if necessary.

Confirming the Possibility of an RDP Tunnel

When a device is detected simultaneously making and receiving connections via RDP, it is advisable to inspect the times, durations, and data transfer amounts to confirm or rule out the possibility that RDP is being used to tunnel data across the device. A malicious actor may use this technique to leverage access gained on the intermediate device to move data through the network in the course of lateral movement.

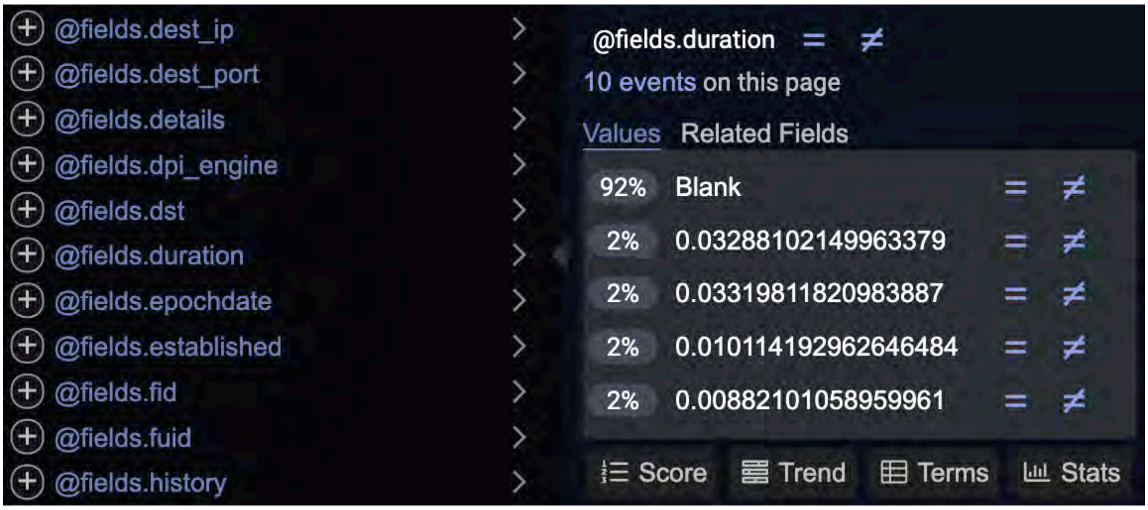
1. Narrow down the results to communications to or from a given IP address, as highlighted by a breach within the Threat Visualizer. Note the use of the **OR** operator.

```
@fields.source_ip:10.1.0.3 OR @fields.dest_ip:10.1.0.3
```

2. Specify a **destination port**. This may be preferable to using the **service** field of the **conn** event which will limit the results to that type of event. This allows for the inspection of general connection information such as time, duration, and data transfer, alongside details that are specific to the application protocol, such as an observed RDP cookie.

```
(@fields.source_ip:10.1.0.3 OR @fields.dest_ip:10.1.0.3) AND
@fields.dest_port:3389
```

3. Inspect the **timestamp** and **duration** within **conn** events in the result set. If data is being tunneled via the device, a pair of connections to and from the device, whose time periods overlap, may exhibit similar transfer amounts in the **orig_bytes** or **resp_bytes** field, signifying a tunneled upload or download.



@fields.dest_ip
@fields.dest_port
@fields.details
@fields.dpi_engine
@fields.dst
@fields.duration
@fields.epochdate
@fields.established
@fields.fid
@fields.fuid
@fields.history

@fields.duration = ≠
10 events on this page

92%	Blank	=	≠
2%	0.03288102149963379	=	≠
2%	0.03319811820983887	=	≠
2%	0.010114192962646484	=	≠
2%	0.00882101058959961	=	≠

a. By viewing the **duration** field, it is possible to exclude all events which do not have a detected length. Select the arrow to the right of @fields.duration and click the **not equals symbol** next to the ***blank*** entry.

```
(@fields.source_ip:10.1.0.3 OR @fields.dest_ip:10.1.0.3) AND
 @fields.dest_port:3389 AND _exists_:"@fields.duration"
```

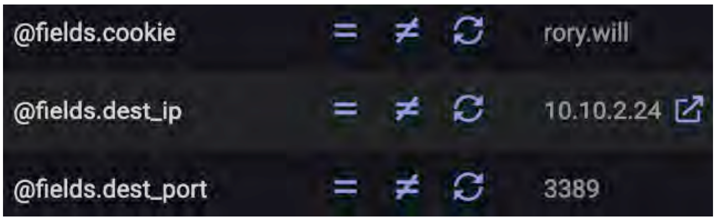
b. Expand this query further by **excluding** connections which had **no data transfer** in the origin or response bytes fields.

```
(@fields.source_ip:10.1.0.3 OR @fields.dest_ip:10.1.0.3) @fields.dest_port:3389
 AND _exists_:"@fields.duration" AND NOT (@fields.orig_bytes:"0" AND
 @fields.resp_bytes:"0")
```

c. It may also be helpful to inspect the **@fields.conn_state** and look for only connections with value of **SF**. This will conclude that the connections had a full SYN FIN completion.

Note: *These steps will limit the results to the conn type events only and the query will therefore need to be modified to remove some search terms. However, they are useful for isolating connections of interest to pivot from.*

4. You may additionally find an **RDP cookie (@fields.cookie**) in a corresponding **rdp** event, which may assist with attribution or identification of the activity.



@fields.cookie	=	≠	↻	rory.will
@fields.dest_ip	=	≠	↻	10.10.2.24
@fields.dest_port	=	≠	↻	3389

Note: *If RDP is wrapped in an encrypted protocol such as SSL, this field will not be visible.*

5. At this point the gathered information can likely be compared with expected or user-recognized activity to help **evaluate whether additional action is necessary**.

Try this:

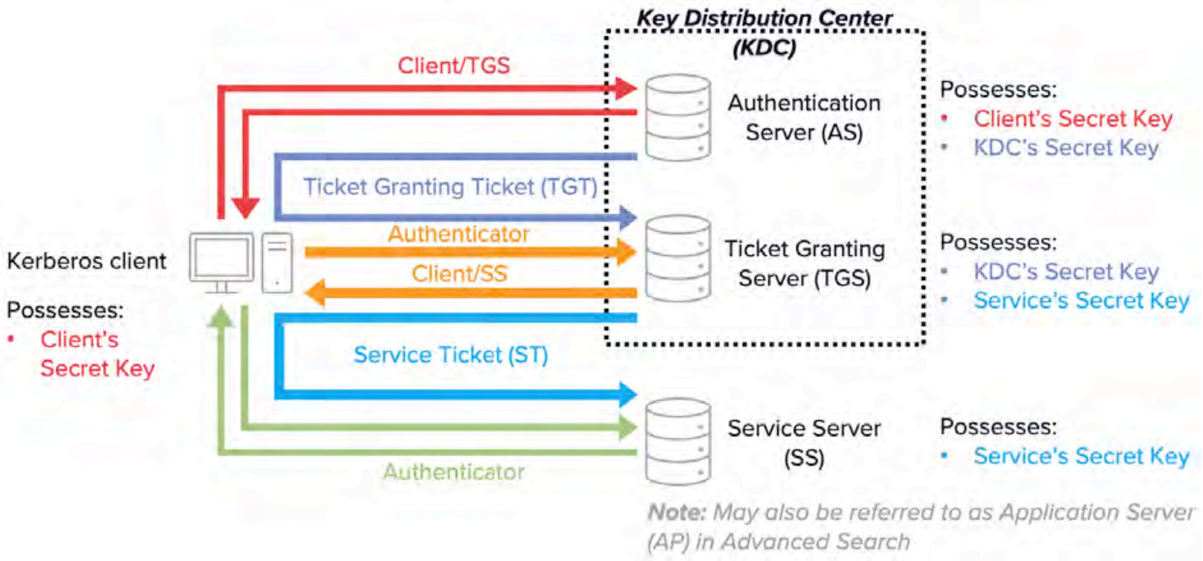
Find and review an example of RDP traffic in Advanced Search using the protocol's default port rather than specific event type. Note the different types of logs in the results and the information contained.

Perform a similar search using the rdp event type. Perform this search instead of destination port.

Create a query that includes both of the above result set. Remember the use of parentheses.

Interpreting Details of Kerberos Transactions

This section will discuss some details regarding the fields available from common Kerberos traffic. The proficient Advanced Search user will benefit from a basic understanding of the Kerberos protocol though an exhaustive description is outside the scope of this document.



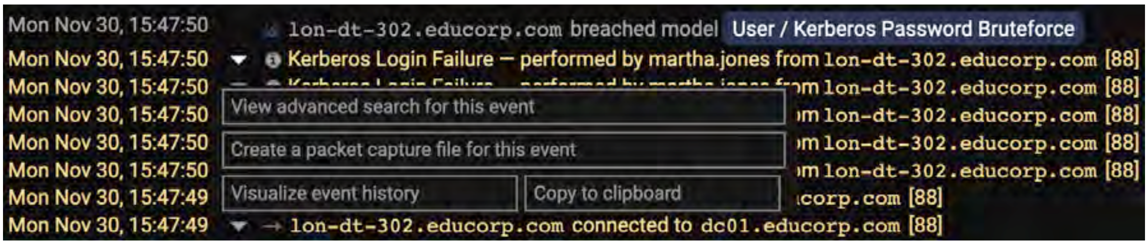
Note: May also be referred to as Application Server (AP) in Advanced Search

The **kerberos** event type is used to represent each of the three authenticating exchanges, differentiating between them using the **request_type** field. The level and type of information visible in each log depends on the exchange type; the following table explains a few of the more helpful fields.

Field	Explanation
@fields.request_type	Denotes which exchange the log describes: • Authentication server (AS): KRB_AS_REQ, KRB_AS_REP • Ticket granting server (TGS): KRB_TGS_REQ, KRB_TGS_REP • Application server access request (AP): KRB_AP_REQ, KRB_AP_REP
@fields.success	Whether or not the exchange succeeded (*true* or *false*). If missing, success or failure could not be determined from observed traffic.
@fields.client	The client principal; for a user login, *<username>@<realm>*.
@fields.service	In the AS or TGS exchange, the (principal of the) service to which the client is requesting access. Examples: • AS: *krbtgt/example.com@example.com* • TGS: *cifs/fs1.example.com@example.com*
@fields.new_ticket_service	In a successful AS or TGS exchange, contains the (principal of the) requested service, much like the **service** field.
@fields.auth_ticket_service	In the TGS or AP exchange, the (principal of the) service that granted the ticket authenticating this request. Examples: • TGS: *krbtgt/example.com@example.com* • AP: *cifs/fs1.example.com@example.com*
@fields.new_ticket_ciphertext	In a successful AS or TGS exchange, the encrypted text of the ticket received by the client.
@fields.auth_ticket_ciphertext	In a TGS or AP exchange, the encrypted text of the ticket sent by the client. Matches the **new_ticket_ciphertext** field of the preceding AS or TGS exchange.

When investigating unusual or suspicious credential use, it is important to understand that the Model Breach Event Log and Model Breach summary may only represent a portion of the overall activity; additional similar events may have occurred after detection or may not have matched the conditions of the model that breached. For a more complete understanding, review the details of relevant traffic around the time of the event.

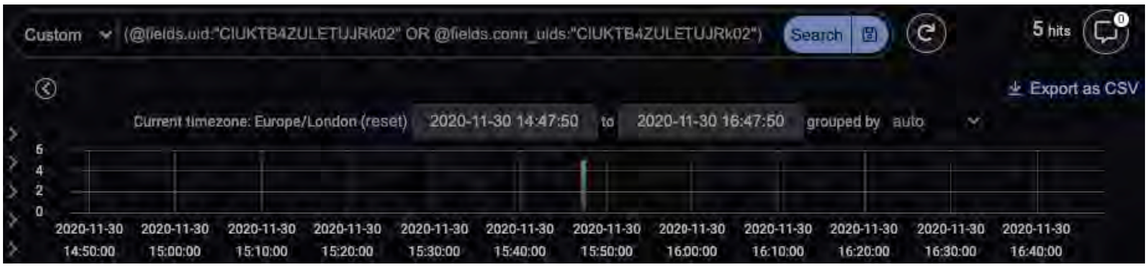
1. From a Kerberos event within a Model Breach Event Log/Device Event Log, click the **View advanced search for this event** from the drop-down menu.



```
Mon Nov 30, 15:47:50      lon-dt-302.educorp.com breached model User / Kerberos Password Bruteforce
Mon Nov 30, 15:47:50  ▼ Kerberos Login Failure — performed by martha.jones from lon-dt-302.educorp.com [88]
Mon Nov 30, 15:47:50                                                         om lon-dt-302.educorp.com [88]
Mon Nov 30, 15:47:50                                                         om lon-dt-302.educorp.com [88]
Mon Nov 30, 15:47:50                                                         om lon-dt-302.educorp.com [88]
Mon Nov 30, 15:47:50                                                         om lon-dt-302.educorp.com [88]
Mon Nov 30, 15:47:49                                                         corp.com [88]
Mon Nov 30, 15:47:49  ▼ → lon-dt-302.educorp.com connected to dc01.educorp.com [88]
```

View advanced search for this event
Create a packet capture file for this event
Visualize event history
Copy to clipboard

2. This will **set the initial time frame** to work with and will also **restrict the search results** to the chosen communication. Remove the pre-populated query in order to broaden the search and inspect the events presented in the logs.



Custom (@fields.uid:"CIUKTB4ZULETUJRk02" OR @fields.conn_uids:"CIUKTB4ZULETUJRk02")

5 hits

Current timezone: Europe/London (reset) 2020-11-30 14:47:50 to 2020-11-30 16:47:50 grouped by auto

3. The first step in authentication is the AS exchange; these events include all successful and failed domain logins. The **request_type** fields can be used to search for logs of all AS exchanges from the detected source device's IP.

@fields.source_ip:10.1.0.3 AND @fields.request_type:AS

4. Specify **krbtgt**, the **service** associated with establishing a TGS session, if the AS exchange has other uses. Using a wildcard pattern as the service field will include additional information.

@fields.source_ip:10.1.0.3 AND **(**@fields.request_type:AS AND
@fields.service:krbtgt*)

5. If the initial results are too broad, narrow the results by using additional search criteria, such as the destination IP or a specific credential.

@fields.source_ip:10.1.0.3 AND (@fields.request_type:AS AND
@fields.service:krbtgt*) **AND @fields.client:(alice@example.com
OR bob@example.com)**

6. Upon review of the search results, some attempts may be **successful**. Inspect the timing and other details of these attempts as potential indicators of possible relevance.

@fields.source_ip:10.1.0.3 AND (@fields.request_type:AS AND @fields.service:krbtgt*)
AND @fields.client:(alice@example.com OR bob@example.com) **AND
@fields.success:true**

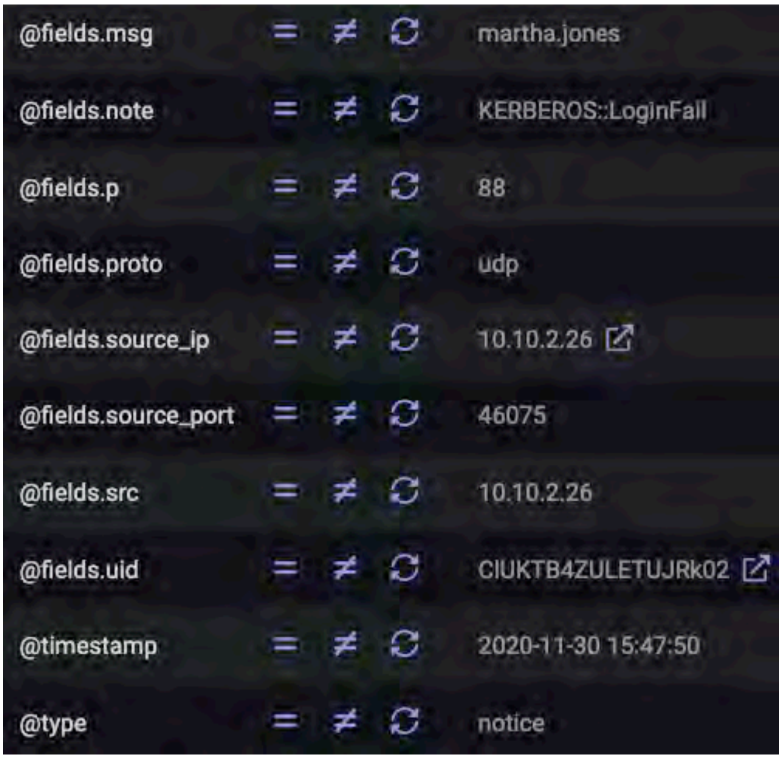
7. Modify the query to **include application requests** (request_type AP) from the source IP to determine which services, on which hosts, were requested following any unrecognized successful logins. The service authenticated in the AP exchange is listed in the *auth_ticket_service* field.

```
@fields.source_ip:10.1.0.3 AND (((@fields.request_type:AS AND
@fields.service:krbtgt*) AND @fields.client:(alice@example.com OR
bob@example.com) AND @fields.success:true) OR @fields.request_type:AP)
```

8. If one or more credentials are suspected to have been abused or compromised, remove the restriction on the source IP, broadening the search to include the use of those credentials elsewhere on the network.

```
(@fields.request_type:AS AND @fields.service:krbtgt*) AND
@fields.client:(alice@example.com OR bob@example.com)
```

9. All the fields discussed so far are **kerberos** event type specific. Advanced Search can also be filtered on the **notice** event type which will present the details in an alternative format. The **notice** event can describe a myriad of protocol and event types so would require filtering to a subset of Kerberos related notice events.



@fields.msg	martha.jones
@fields.note	KERBEROS::LoginFail
@fields.p	88
@fields.proto	udp
@fields.source_ip	10.10.2.26
@fields.source_port	46075
@fields.src	10.10.2.26
@fields.uid	CIUKTB4ZULETUJRk02
@timestamp	2020-11-30 15:47:50
@type	notice

Try this:

Create a query that will return Kerberos attempts over 24 hours. Use the request type to differentiate these from other authentication attempts.

Adjust the query to return only failed attempts and use the options in the Column list to better analyze the results. Use the Score feature to display a breakdown of the most commonly observed values for the credential (client). Restrict results to one of the listed credentials and then display a similar breakdown of the observed error messages. Further resist one of these commonly observed errors and display a breakdown of observed source IPs.

HTTP or HTTPS Bruteforcing

Repeated attempts to log into a web interface will often manifest in the form of numerous requests to the same URI, which may contain recognizable terms like "**login**", "**auth**", or similar.

URIs requested via unencrypted HTTP are visible in Advanced Search, allowing for confirmation that a single endpoint has been repeatedly requested. On the other hand, HTTPS connections will not display this detail due to them being encrypted. In the latter case, it may be possible to isolate large or unusual volumes of requests to or from a device which could be an indicator of such activity. However, it is more advisable to rely on further indicators, such as a subsequent comparison with expected or recognized activity, in order to determine the likelihood that a bruteforce login attempt has occurred.

Such instances of repeated requests may have highlighted by a Model Breach or through investigations of HTTP/HTTPS communications. In either case, it will be useful to understand how Advanced Search can help locate and interpret the details of comparatively large volumes of requests.

1. Focus on a **specific source and/or destination** to provide a more isolated set of communications for review. It may be useful to also limit the destination port and/or application protocol depending on the activity of interest.

   ```
   @fields.dest_ip:10.1.2.3 AND @type:http

   @fields.dest_ip:10.1.2.3 AND @fields.service:ssl AND @fields.dest_port:443
   ```

   Note: *The above query uses the conn type's service field rather than specifying the ssl event type as it is the conn type that contains this information.*

2. With HTTP, results can be narrowed further by **destination URI** and/or **response status code**. When isolating possible HTTPS bruteforce attempts, the relevant details are **duration** and **data transfer**, as these can help to differentiate attempted and successful logins from failed connections.

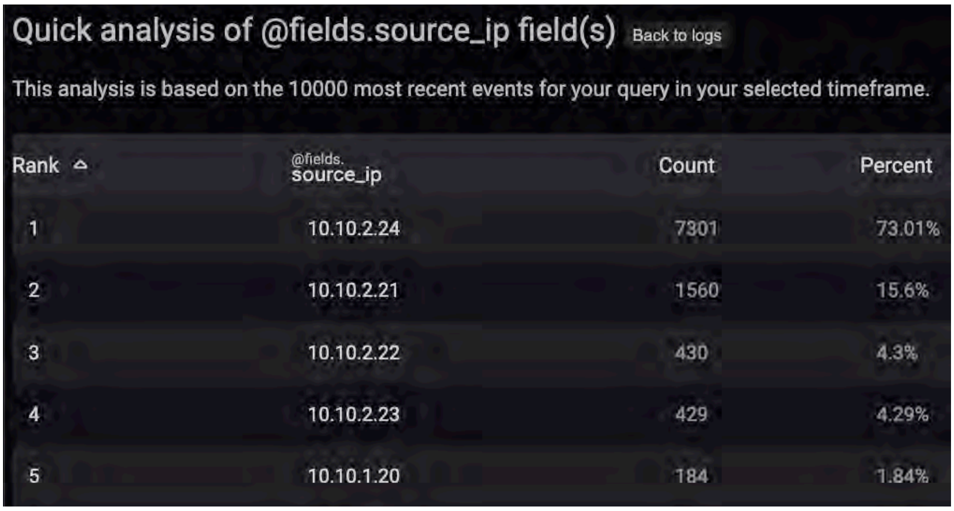
   For **HTTP**, a query could simply be altered like so:

   ```
   @fields.dest_ip:10.1.2.3 AND @type:http AND @fields.uri:"/login" AND
   @fields.status_code:401
   ```

   For **HTTPS**, the results can be narrowed to better represent possible login attempts by requiring a non-zero data transfer from the connection source, since such attempts will involve a successful TCP connection and the transmission of credentials:

   ```
   @fields.dest_ip:10.1.2.3 AND @fields.service:ssl AND @fields.dest_port:443 AND
   @fields.orig_bytes:>0
   ```

3. Rank the source IPs using the **Score** functionality to narrow down specific source addresses within a desired time frame.



Quick analysis of @fields.source_ip field(s)

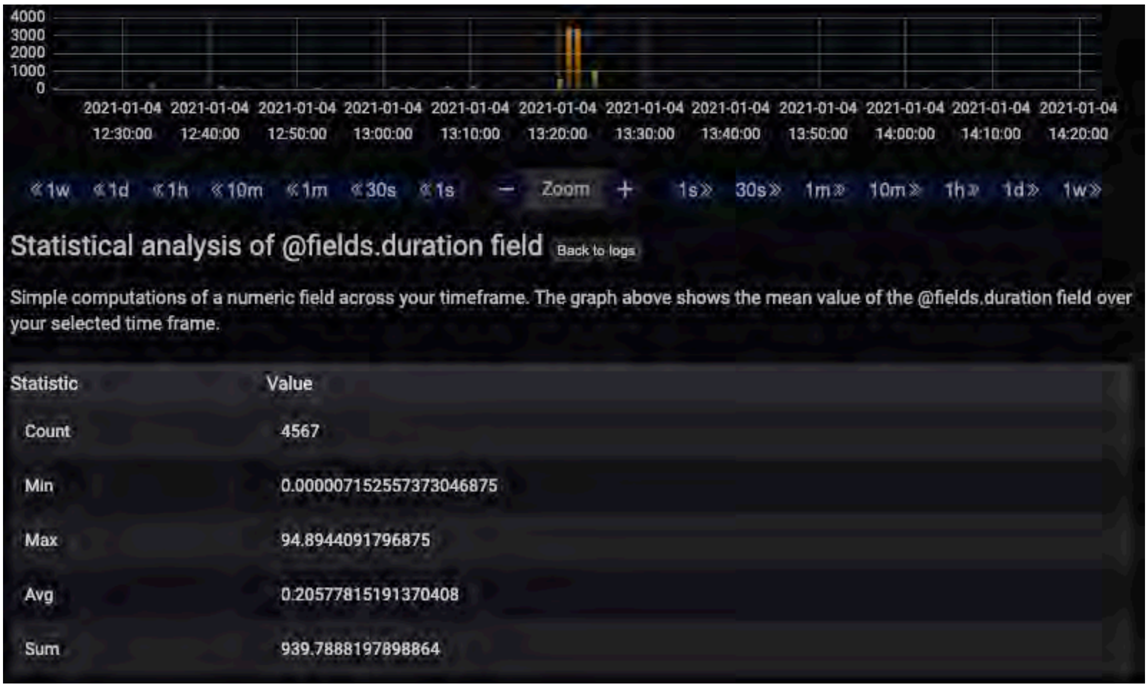
This analysis is based on the 10000 most recent events for your query in your selected timeframe.

Rank	@fields. source_ip	Count	Percent
1	10.10.2.24	7301	73.01%
2	10.10.2.21	1560	15.6%
3	10.10.2.22	430	4.3%
4	10.10.2.23	429	4.29%
5	10.10.1.20	184	1.84%

@fields.source_ip:10.4.5.6 AND @fields.dest_ip:10.1.2.3 AND @type:http AND @fields.uri:"/login" AND @fields.status_code:401

@fields.source_ip:10.4.5.6 AND @fields.dest_ip:10.1.2.3 AND @fields.service:ssl AND @fields.dest_port:443 AND @fields.orig_bytes:>0

4. Score and **Stats** can also be used to compute the average duration or transfer over multiple connections. Any number of these may support or deny the likelihood that selected SSL traffic represents brute force login attempts.



Statistical analysis of @fields.duration field

Simple computations of a numeric field across your timeframe. The graph above shows the mean value of the @fields.duration field over your selected time frame.

Statistic	Value
Count	4567
Min	0.000007152557373046875
Max	94.8944091796875
Avg	0.20577815191370408
Sum	939.7888197898864

Note: *While more rudimentary implementations of HTTPS bruteforcing may utilize one connection per attempt, multiple requests, i.e., attempts, can occur over a single connection.*

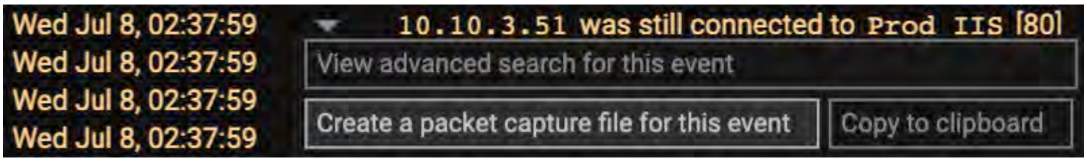
5. Once bruteforce login attempts have been likely confirmed, the next step may be to look for **successful attempts**. Narrow down the results by **differentiating a factor** such as response code, duration, or data transfer.

```
@fields.source_ip:10.4.5.6 AND @fields.dest_ip:10.1.2.3 AND @type:http AND
@fields.uri:"/login" AND NOT @fields.status_code:401

@fields.source_ip:10.4.5.6 AND @fields.dest_ip:10.1.2.3 AND @fields.service:ssl
AND @fields.dest_port:443 AND (@fields.duration:>1 OR @fields.resp_bytes:>1000)
```

6. For more **follow up investigations**, navigate to the corresponding devices in the Threat Visualizer in search of other signs of unusual activity.

   a. When investigating a HTTP Bruteforce, it is useful to **download a PCAP** of some of the connections around the time of the attempt. Considering this is a cleartext protocol, it is possible to see data which was transferred in the URI.

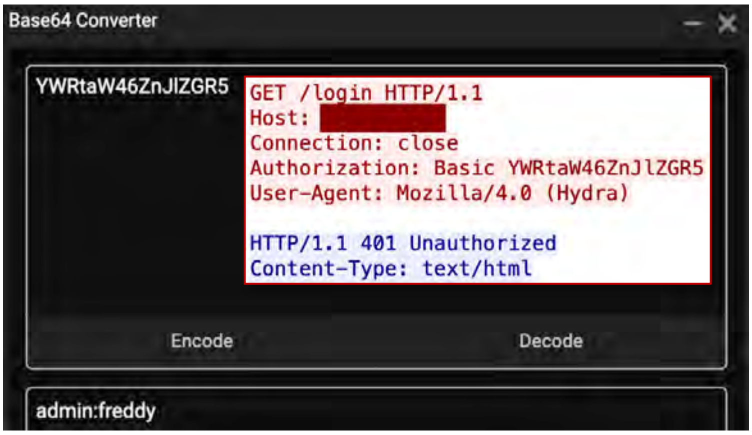


```
Wed Jul 8, 02:37:59    10.10.3.51 was still connected to Prod IIS [80]
Wed Jul 8, 02:37:59
Wed Jul 8, 02:37:59
Wed Jul 8, 02:37:59
```

View advanced search for this event
Create a packet capture file for this event
Copy to clipboard

   i. The authorization may sometimes be encoded. It may be advisable to open the Base64 Converter from the Utilities menu to enable decoding.

Copying the Authorization field from the example PCAP into the Base64 Converter and clicking Decode shows one of the **username:password** combinations attempted was admin and freddy.



YWRtaW46ZnJlZGR5

```
GET /login HTTP/1.1
Host: [redacted]
Connection: close
Authorization: Basic YWRtaW46ZnJlZGR5
User-Agent: Mozilla/4.0 (Hydra)

HTTP/1.1 401 Unauthorized
Content-Type: text/html
```

admin:freddy

__Note:__ Utilities are outlined towards the end of the manual.

Try this:

Find an example of a Model Breach highlighting possible HTTP/HTTPS bruteforcing and review the details of matching connections. Filter the Threat Tray on the AP: Bruteforce Model Tag and adjust the time frame to include at least one example. Pivot into Advanced Search to expand the query and view all related connections. Use the Stats to calculate the average duration and data transfer over the set of communication in order to determine the likelihood of bruteforcing.

Investigating SMB Enumeration

Model Breaches highlighting possible SMB enumeration are more specifically indicating a device has accessed a number of network shares for the first time in a finite time period. There are multiple ways in which the model can be triggered, each of which merits investigation if unrecognized. Such activity is commonly seen in the case of network reconnaissance.

The Model **Anomalous Connection / SMB Enumeration** is triggered by several occurrences of one of the following cases within a finite time frame, where each has the potential to be used by a malicious actor for information gathering:

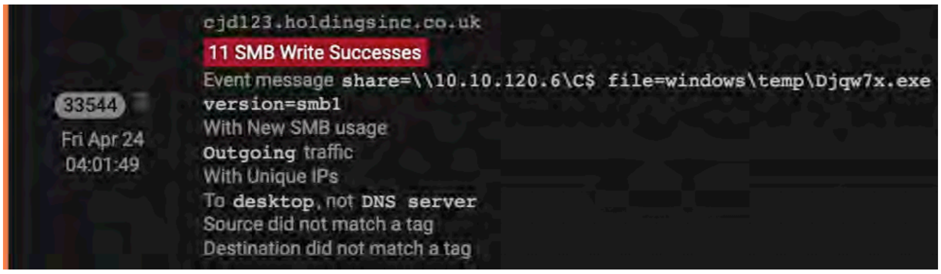
- Successful SMB writes to the Server Service Remote Protocol (*srvsvc*) on unique internal destinations' inter-process communication (*IPC$*) share. This share is also known as a null session connection and can be used to enumerate network shares and domain accounts on a destination server.

- Unusual successful anonymous SMB sessions to unique internal destinations.

- Newly-observed successful SMB writes to hidden shares, with a few exclusions.

- Newly-observed successful SMB writes as *guest* on unique internal destinations.

1. Examine the summarized information in the corresponding **Breach Log**.

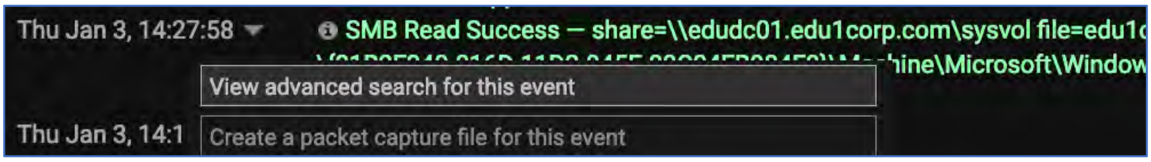


```
33544
Fri Apr 24
04:01:49

cjd123.holdingsinc.co.uk
11 SMB Write Successes
Event message share=\\10.10.120.6\C$ file=windows\temp\Djqw7x.exe
version=smb1
With New SMB usage
Outgoing traffic
With Unique IPs
To desktop, not DNS server
Source did not match a tag
Destination did not match a tag
```

   While a handful of SMB operations can trigger the Model, this is often a subset of the overall activity. Similar information can also be found in the device's Event Log and the full scope of the device's activity can be reviewed in Advanced Search.

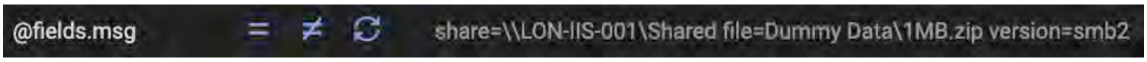
2. Choose one of the SMB operations in the **Model Breach Event Log** as a starting point, and pivot to that connection in Advanced Search.



```
Thu Jan 3, 14:27:58    SMB Read Success — share=\\edudc01.edu1corp.com\sysvol file=edu1c
                       hine\Microsoft\Window
Thu Jan 3, 14:1
```

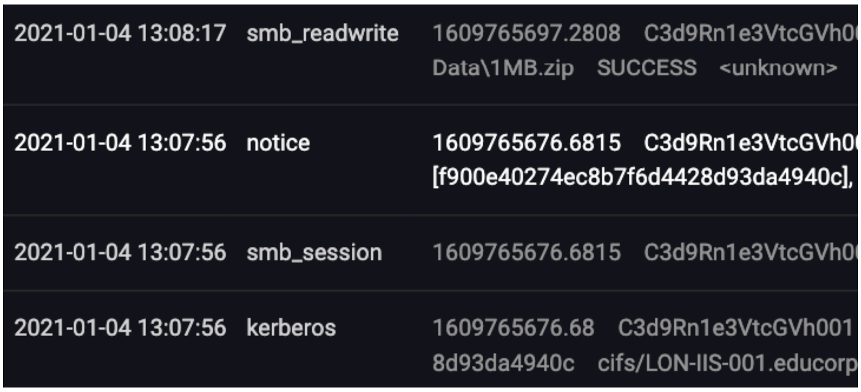
View advanced search for this event
Create a packet capture file for this event

3. The relevant **msg** field of the **notice** event corresponds to the **message** filter in the Model definition. SMB writes will often contain the destination share, filename and protocol version and the SMB session initiation will contain the username.



```
@fields.msg    share=\\LON-IIS-001\Shared file=Dummy Data\1MB.zip version=smb2
```

4. In addition to the **notice** event, corresponding **smb_session, smb_transaction**, **smb_readwrite**, or **smb_access_failure** events may also be present, each containing different types of information.



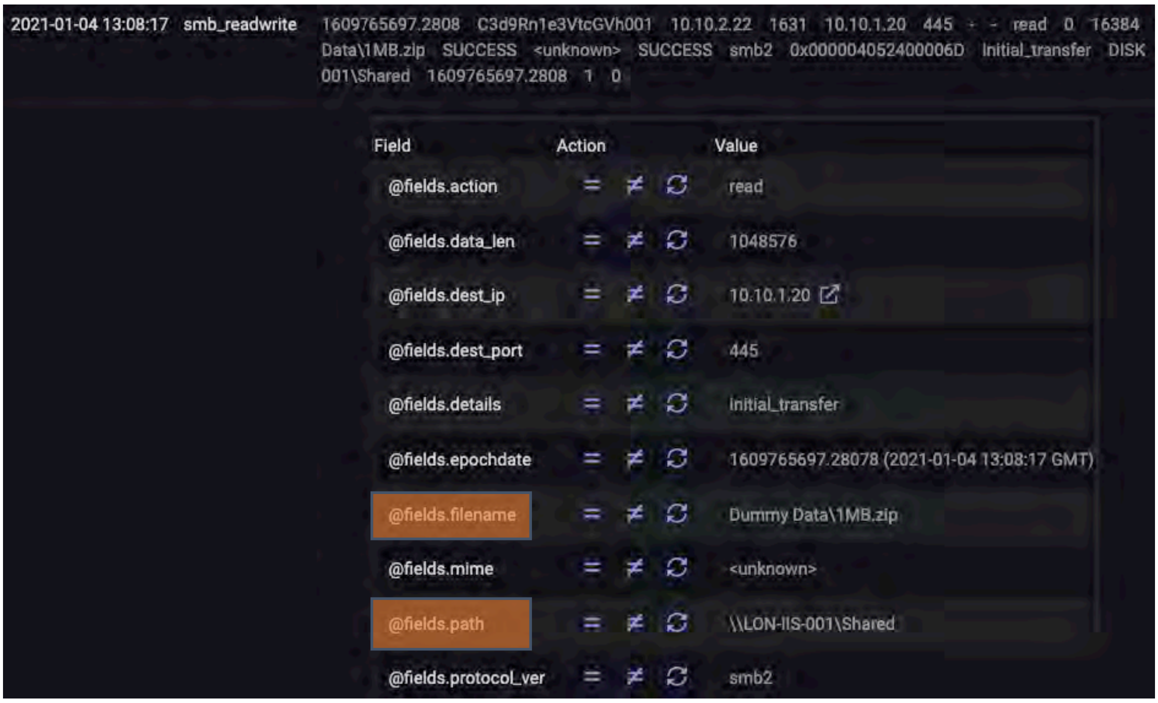
```
2021-01-04 13:08:17   smb_readwrite   1609765697.2808   C3d9Rn1e3VtcGVh0
                                      Data\1MB.zip   SUCCESS   <unknown>

2021-01-04 13:07:56   notice          1609765676.6815   C3d9Rn1e3VtcGVh0
                                      [f900e40274ec8b7f6d4428d93da4940c],

2021-01-04 13:07:56   smb_session     1609765676.6815   C3d9Rn1e3VtcGVh0

2021-01-04 13:07:56   kerberos        1609765676.68   C3d9Rn1e3VtcGVh001
                                      8d93da4940c   cifs/LON-IIS-001.educorp
```

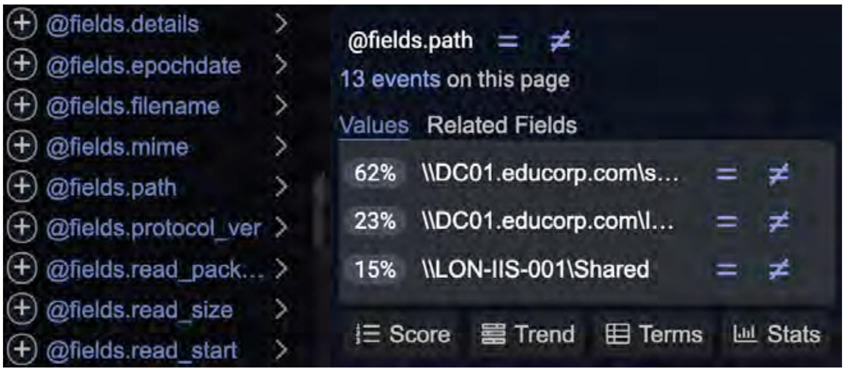
5. Reviewing these additional event types can make it easier to investigate activity as the basis for a broader query as these will separate values into fields like **filename**, **path**, or **account**.



```
2021-01-04 13:08:17   smb_readwrite   1609765697.2808   C3d9Rn1e3VtcGVh001   10.10.2.22   1631   10.10.1.20   445   -   -   read   0   16384
                                      Data\1MB.zip   SUCCESS   <unknown>   SUCCESS   smb2   0x000004052400006D   Initial_transfer   DISK
                                      001\Shared   1609765697.2808   1   0
```

Field	Action	Value
@fields.action	= ≠	read
@fields.data_len	= ≠	1048576
@fields.dest_ip	= ≠	10.10.1.20
@fields.dest_port	= ≠	445
@fields.details	= ≠	initial_transfer
@fields.epochdate	= ≠	1609765697.28078 (2021-01-04 13:08:17 GMT)
@fields.filename	= ≠	Dummy Data\1MB.zip
@fields.mime	= ≠	<unknown>
@fields.path	= ≠	\\LON-IIS-001\Shared
@fields.protocol_ver	= ≠	smb2

6. Having decided upon an appropriate common factor (e.g. filename, path or account) and time frame, use the **Score** capability to determine the various destinations of the operations of interest.



@fields.path = ≠

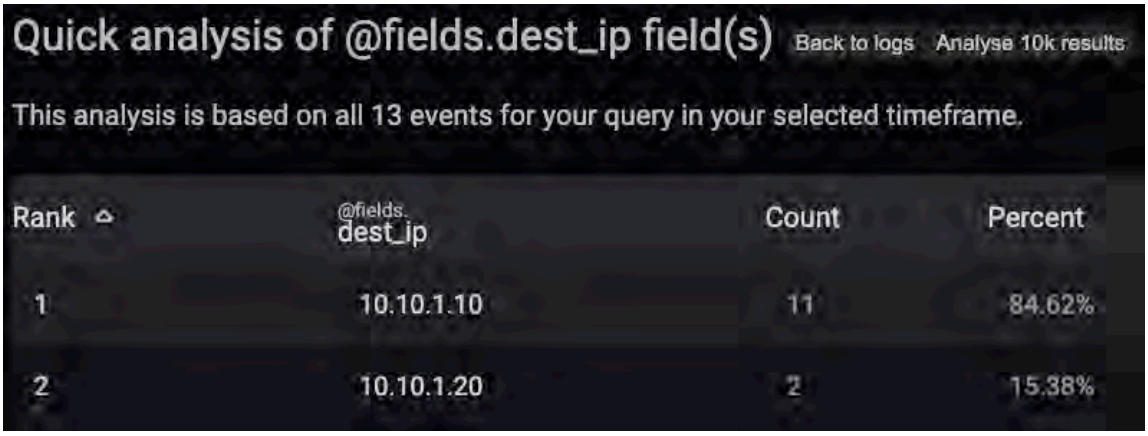
13 events on this page

Values   Related Fields

62%	\\DC01.educorp.com\s...	= ≠
23%	\\DC01.educorp.com\l...	= ≠
15%	\\LON-IIS-001\Shared	= ≠

7. Append the **account name** and score the destination to quickly highlight any areas of interest:

```
@type:smb_session AND @fields.source_ip:10.4.5.6 AND @fields.account:guest
```



Quick analysis of @fields.dest_ip field(s)

This analysis is based on all 13 events for your query in your selected timeframe.

Rank	@fields. dest_ip	Count	Percent
1	10.10.1.10	11	84.62%
2	10.10.1.20	2	15.38%

Note: *In the case of exploitable named pipes or anonymous access, it may be desirable to review policy and configuration regarding the allowance of their use.*

Try this:

Locate an Anomalous Connection / SMB Enumeration Model Breach and inspect the activity that triggered it. Adjust the time frame for the Threat Tray to find an example and compare the Model Breach Event Log to the Model definition to better understand why the breach occurred. View the activity in Advanced Search and use the Score feature to display a breakdown of commonly observed share paths, files names and destination IPs. Determine whether the listed details help correlate this with recognized SMB operations.

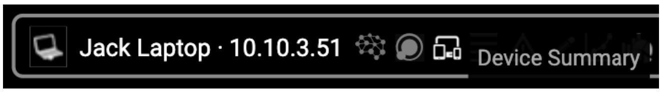
Inspecting the Details of a Network Scan

Making large numbers of communication attempts to obtain devices' addresses and/or available ports and services - also known as address and/or port scanning - is a routine part of many legitimate activities. Such activity often performed by a sanctioned vulnerability scanner, auditing service, or asset management solution. However, due to the nature of these routine services, it is easy for an unauthorized actor wishing to perform reconnaissance while remaining undetected. Thus, when a device is detected performing a port or address scan, the primary question for consideration is whether such activity is authorized.

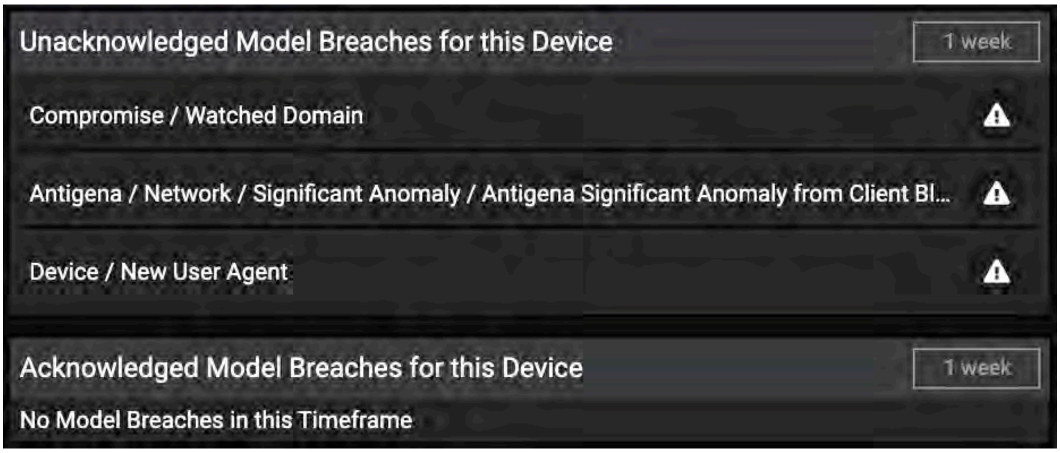
Darktrace can assist in ferreting out unauthorized network scans, as they will often be seen accompanied by a detection of unusual activity; however, a newly or infrequently performed scan may yet be legitimate.

1. When alerted to such scans, first compare them to an **existing knowledge** of authorized activity.

    a. Pivot to the device in question on the Threat Visualizer and check the **Device Summary** for a history of network scan breaches.



    i. View **unacknowledged and acknowledged breaches** for the device up to 6 months prior and see if the device consistently breaches the same Model type and if it has been recognized as legitimate activity.



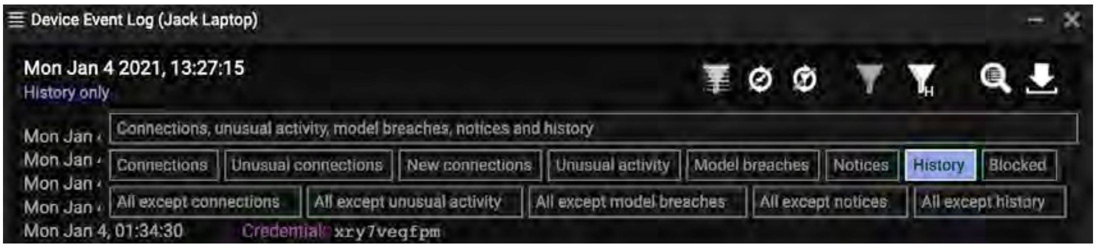
Unacknowledged Model Breaches for this Device — 1 week

- Compromise / Watched Domain
- Antigena / Network / Significant Anomaly / Antigena Significant Anomaly from Client Bl...
- Device / New User Agent

Acknowledged Model Breaches for this Device — 1 week

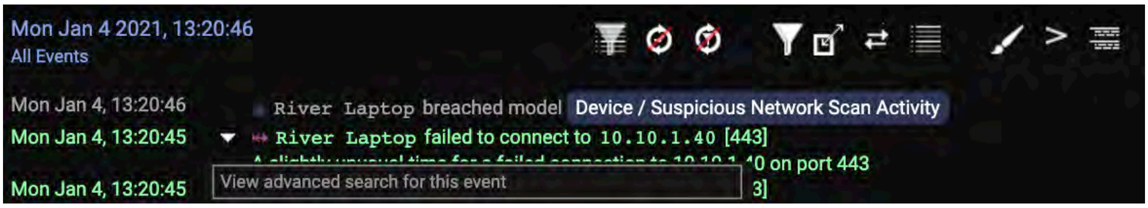
No Model Breaches in this Timeframe

    b. Look at the History within the **Device Event Log**. Does the device have any administrative or recognizable credentials associated with it? What user agents have been observed on the device?



```
Mon Jan 4 2021, 13:27:15
History only
Mon Jan
Mon Jan
Mon Jan
Mon Jan
Mon Jan 4, 01:34:30        Credential: xry7veqfpm
```

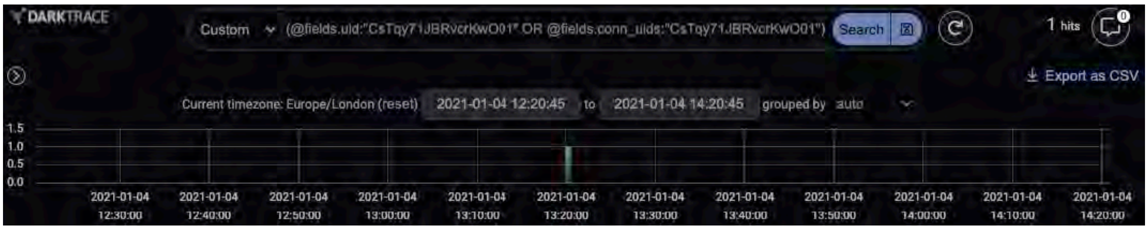
2. If the scan does not appear legitimate, or further investigation is required, pivot to **Advanced Search** from one of the connection attempts in one of the Event Logs.



Mon Jan 4 2021, 13:20:46
All Events

Mon Jan 4, 13:20:46 River Laptop breached model Device / Suspicious Network Scan Activity
Mon Jan 4, 13:20:45 River Laptop failed to connect to 10.10.1.40 [443]
'0 on port 443
Mon Jan 4, 13:20:45 3]

3. Similar to breaches of the SMB Enumeration Model, the activity in the Event Log is often a subset of a larger set of activity but is useful as a starting point. When Advanced Search opens, a **pre-populated search bar and time frame** are present.

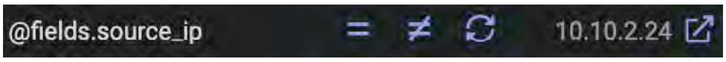


Custom (@fields.uid:"CsTqy71JBRvcrKwO01" OR @fields.conn_uids:"CsTqy71JBRvcrKwO01")

1 hits

Current timezone: Europe/London (reset) 2021-01-04 12:20:45 to 2021-01-04 14:20:45 grouped by auto

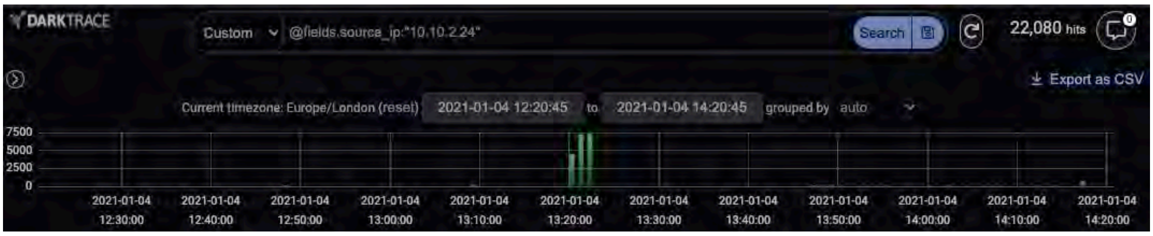
4. **Delete** the pre-populated query and click on the **equals sign** next to the source IP field.



@fields.source_ip = ≠ 10.10.2.24

```
@fields.source_ip:"10.1.2.3"
```

This will show all connectivity from the breach device over the pre-set time frame.



Custom @fields.source_ip:"10.10.2.24"

22,080 hits

Current timezone: Europe/London (reset) 2021-01-04 12:20:45 to 2021-01-04 14:20:45 grouped by auto

5. Start narrowing down the query to look for all **similar connection attempts**, for example those that were unanswered or rejected.

```
@fields.source_ip:"10.1.2.3" AND @fields.history:("S" OR "Sr" OR "ShR")
```

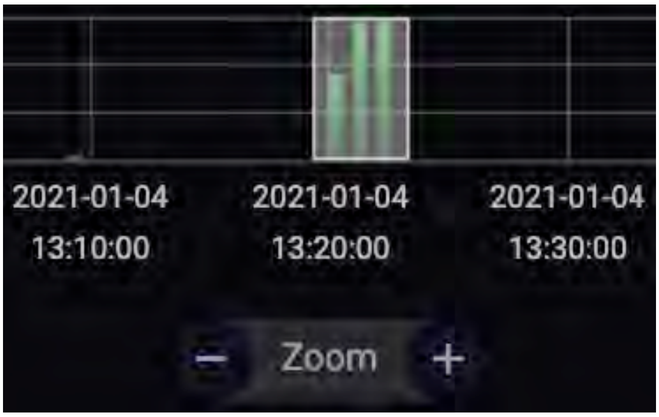
Note: *UDP connections do not have such variable history fields. The above query will therefore only be giving an overall idea of the TCP connection attempts, effectively displaying results as if the @fields.proto:tcp was appended to the query.*

6. This connectivity may also include any external attempts, but the focus of this exercise is to locate internal connectivity. Modify the query to return only connections with a **local response**.

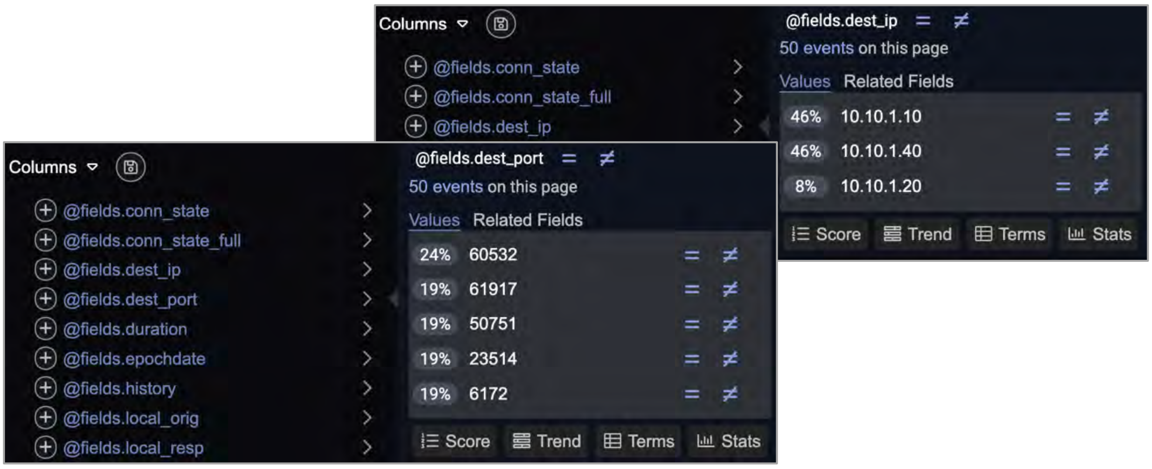
```
@fields.source_ip:"10.1.2.3" AND (@fields.history:("S" OR "Sr" OR "ShR") AND
@fields.proto:tcp AND @fields.local_resp:true)
```

7. If the time frame is not appropriate, modify as necessary. This can be done manually by **clicking and dragging** over the desired area to zoom in or selecting the appropriate **zoom buttons**.

   Note: Remember to loosen the query later and inspect the results, so as not to miss a broader set of attempts.



8. Once the query has returned the required results, it is helpful to narrow down which **addresses / ports** were probed. Use the **Score** function for the chosen field to gain an approximate understanding.



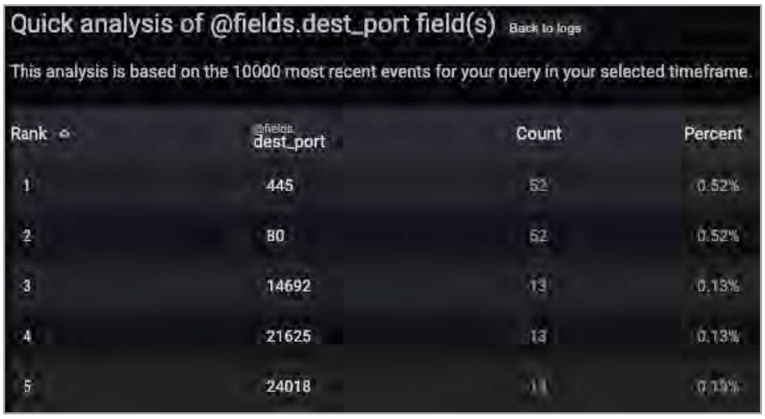
@fields.dest_ip = ≠
50 events on this page
Values Related Fields

46%	10.10.1.10
46%	10.10.1.40
8%	10.10.1.20

@fields.dest_port = ≠
50 events on this page
Values Related Fields

24%	60532
19%	61917
19%	50751
19%	23514
19%	6172

9. Such results can serve as **starting points** for new queries regarding subsequent communications from the source to these specific destination address/port combinations, as there may be follow-on activity if a potentially exploitable service was discovered.



Quick analysis of @fields.dest_port field(s)

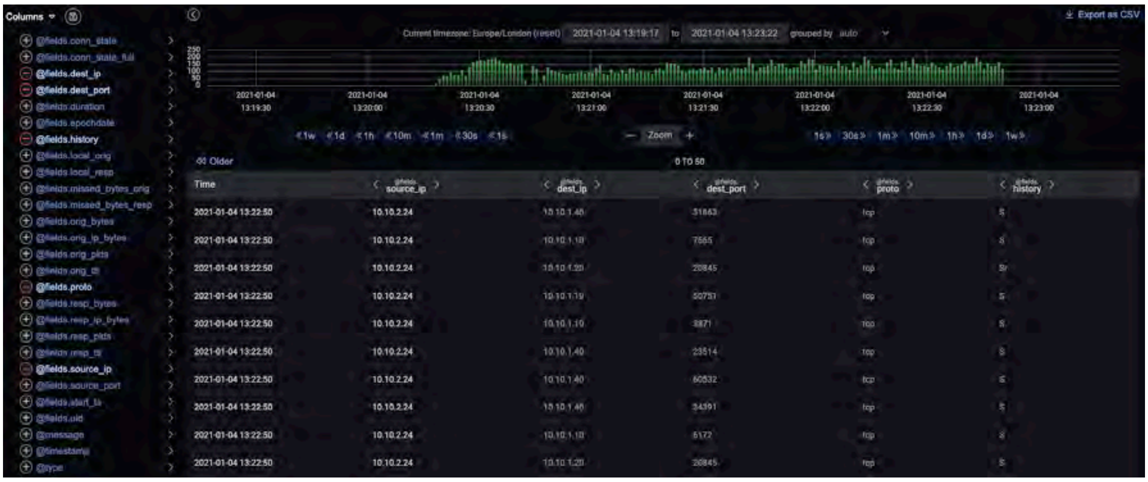
This analysis is based on the 10000 most recent events for your query in your selected timeframe.

Rank	@fields dest_port	Count	Percent
1	445	52	0.52%
2	80	52	0.52%
3	14692	13	0.13%
4	21625	13	0.13%
5	24018	11	0.11%

For example, this may highlight unencrypted protocols, e.g., HTTP, which could provide additional information such as URIs and user agents.

10. By clicking **Back to Logs**, select columns by clicking the plus icon next to a desired field to create a table.

Back to logs



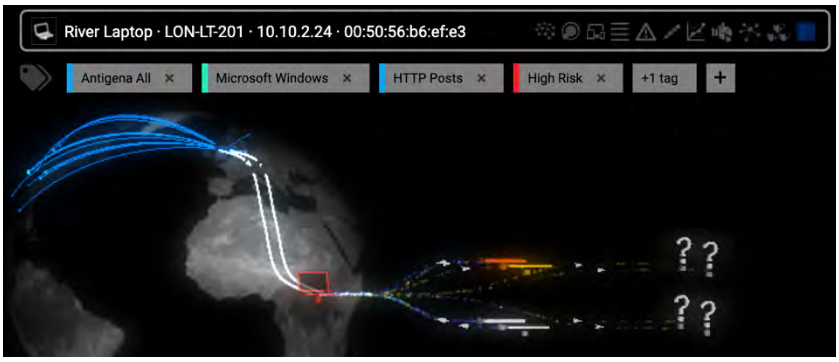
Time	@fields. source_ip	@fields. dest_ip	@fields. dest_port	@fields. proto	@fields. history
2021-01-04 13:22:50	10.10.2.24	10.10.1.46	31863	tcp	S
2021-01-04 13:22:50	10.10.2.24	10.10.1.10	7565	tcp	S
2021-01-04 13:22:50	10.10.2.24	10.10.1.20	20845	tcp	Sr
2021-01-04 13:22:50	10.10.2.24	10.10.1.19	50751	tcp	S
2021-01-04 13:22:50	10.10.2.24	10.10.1.10	3871	tcp	S
2021-01-04 13:22:50	10.10.2.24	10.10.1.40	23514	tcp	S
2021-01-04 13:22:50	10.10.2.24	10.10.1.40	60532	tcp	S
2021-01-04 13:22:50	10.10.2.24	10.10.1.46	34391	tcp	S
2021-01-04 13:22:50	10.10.2.24	10.10.1.10	5172	tcp	S
2021-01-04 13:22:50	10.10.2.24	10.10.1.20	20845	tcp	S

11. Choose to export up to 10k or 100k of the selected results in the table by clicking the **export** button in the top right of Advanced Search.

Export as CSV

This technique allows all the duplicates to be stripped in an external program or spreadsheet, allowing for the ports, for example, to be ordered into a list.

12. Return to the **Threat Visualizer** to investigate other breaches which occurred around the same time to further understand the nature of the network scan.



Try this:

Find an example Network Scanning Model Breach and use Advanced Search to determine the scope of the activity. Adjust the time frame and apply the AP: Internal Recon Model Tag to the Threat Tray to locate a scan-related breach. From a connection attempt within an Event Log, navigate to Advanced Search. Modify the query to include all communications from a breaching device and narrow it down to include unanswered (history S or D) or rejected (history of Sr or similar) connections. Not all attempts in a network scan will fail, but this technique can be approximate the overall number of attempts. Adjust the time frame to encapsulate all the scanning activity in the histogram distribution and Score the features to obtain a breakdown of destination ports and IPs.

Interpreting Records of the Use of PsExec

PsExec is a useful administrative tool which allows remote interactive command execution without prior installation on the destination device. As a result, it is often abused for lateral movement by malicious actors. It relies upon SMB for transport thus the involved file operations can be observed as long as it uses an unencrypted version of said protocol, e.g. SMBv2.

The following are file name patterns commonly accessed in the course of using PsExec to execute commands on a remote system:

- A binary file written to the destination's ADMIN$ share; a service that will receive and execute commands locally and return any output. This is normally deleted at end of use.

```
PSEXESVC.EXE
```

- Service control may be observed being accessed on the destination's IPC$ share to start the remote service.

```
svcctl
```

- Named pipe on the IPC$ share to which commands are written, as a means of delivering them to the remote service which will execute them.

```
PSEXESVC-<client-hostname>-<pid>-stdin
```

- Named pipes on the IPC$ share from which output and error messages are read.

```
PSEXESVC-<client-hostname>-<pid>-stdout
PSEXESVC-<client-hostname>-<pid>-stderr
```

1. Upon finding an instance of PsExec use, pivot to **Advanced Search**.

2. **Review** the reads, writes, transfer volumes, start time and duration of the activity overall.

3. **Compare** this with any known legitimate administrative use of PsExec by the source device.

Try this:

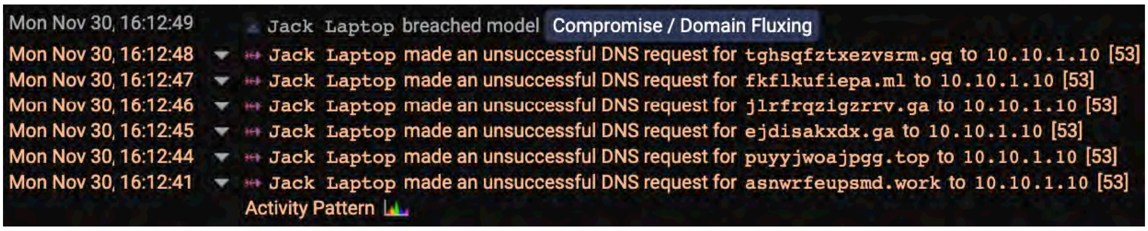
Locate an example Model Breach highlighting PsExec usage, review the details triggering the activity and compare this to the source device's expected activity. Search PsExec in the Omnisearch bar to list all the relevant Models that could breach. Adjust the Threat Tray time frame to return appropriate results. Pivot from the Model Breach Event Log to Advanced Search, expand the query to include all SMB communications between the source and destination and look for details similar to those outlined above to confirm PsExec usage.

Tracking Down Possible Domain Fluxing

Domain fluxing is a technique used by some malware in the course of establishing communications with malicious infrastructure. Instead of contacting a specific hostname or IP, the malware algorithmically generates a large number of hostnames which it queries via DNS. The attacker, knowing the algorithm used, can register a small subset of the hostnames it can generate and regularly switch between them. This makes it more difficult to prevent at the perimeter. The DNS requests themselves can be difficult to isolate as most devices make numerous DNS requests as part of normal operation.

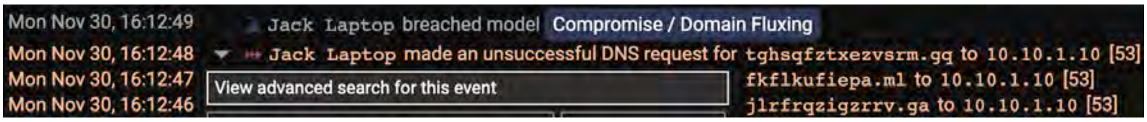
Darktrace can detect possible cases of domain fluxing by observing when a device makes several DNS queries whose requested hostnames heuristically appear to be dynamically generated.

1. Verify whether the domain fluxing which is occurring is **likely legitimate** web traffic or DNS pre-fetching. These can trigger the domain fluxing model if queried hostnames appear sufficiently likely to have been generated. Scrutinize the DNS requests presented in the **Model Breach Event Log**.



```
Mon Nov 30, 16:12:49     Jack Laptop breached model Compromise / Domain Fluxing
Mon Nov 30, 16:12:48  ▾  Jack Laptop made an unsuccessful DNS request for tghsqfztxezvsrm.gq to 10.10.1.10 [53]
Mon Nov 30, 16:12:47  ▾  Jack Laptop made an unsuccessful DNS request for fkflkufiepa.ml to 10.10.1.10 [53]
Mon Nov 30, 16:12:46  ▾  Jack Laptop made an unsuccessful DNS request for jlrfrqzigzrrv.ga to 10.10.1.10 [53]
Mon Nov 30, 16:12:45  ▾  Jack Laptop made an unsuccessful DNS request for ejdisakxdx.ga to 10.10.1.10 [53]
Mon Nov 30, 16:12:44  ▾  Jack Laptop made an unsuccessful DNS request for puyyjwoajpgg.top to 10.10.1.10 [53]
Mon Nov 30, 16:12:41  ▾  Jack Laptop made an unsuccessful DNS request for asnwrfeupsmd.work to 10.10.1.10 [53]
                         Activity Pattern
```

2. If the possibility of domain fluxing cannot easily be ruled out, inspect the DNS queries more closely in **Advanced Search**.

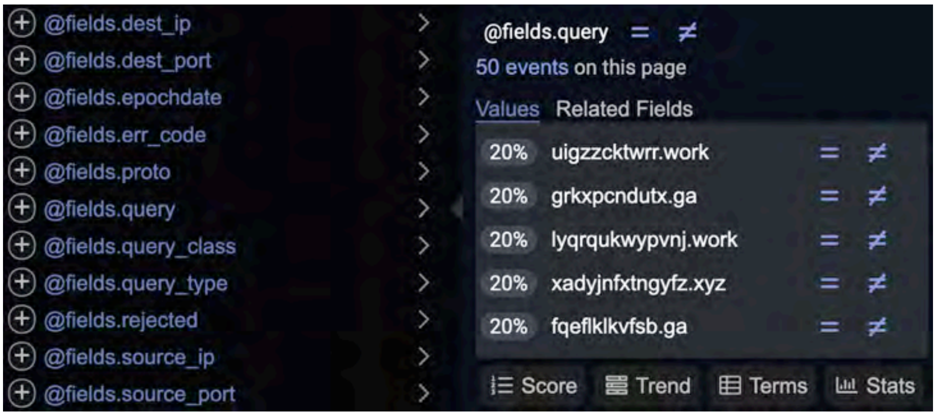


```
Mon Nov 30, 16:12:49     Jack Laptop breached model Compromise / Domain Fluxing
Mon Nov 30, 16:12:48  ▾  Jack Laptop made an unsuccessful DNS request for tghsqfztxezvsrm.gq to 10.10.1.10 [53]
Mon Nov 30, 16:12:47  View advanced search for this event     fkflkufiepa.ml to 10.10.1.10 [53]
Mon Nov 30, 16:12:46                                          jlrfrqzigzrrv.ga to 10.10.1.10 [53]
```

3. In cases of domain fluxing, a large number of DNS responses indicating a non-existent domain (where the error, or response, code **NXDOMAIN**) is common. Such activity often causes the DNS requests to fail. Alter the pre-populated query to include additional failed requests.

```
@fields.source_ip:10.1.2.3 AND @fields.err_code:NXDOMAIN
```

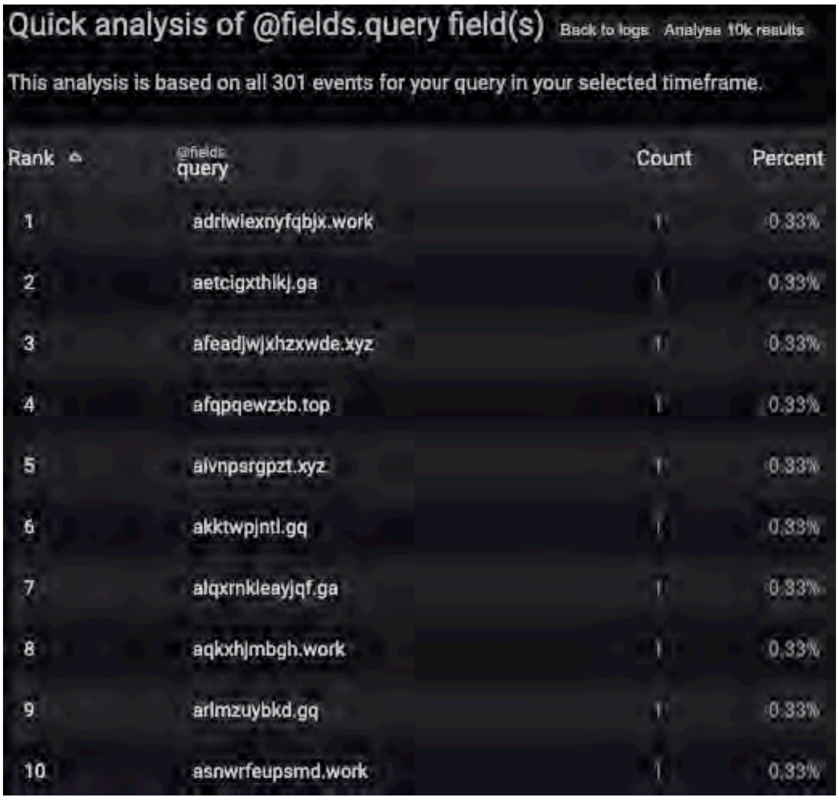
4. After making any necessary adjustments to the time frame, use the **Score** capability to view a list of unique values of the **@fields.query** field.



20%	uigzzcktwrr.work	= ≠
20%	grkxpcndutx.ga	= ≠
20%	lyqrqukwypvnj.work	= ≠
20%	xadyjnfxtngyfz.xyz	= ≠
20%	fqeflklkvfsb.ga	= ≠

5. Look for any **distinguishable traits** of hostnames that appear to have been queried as part of domain fluxing that can be isolated for further queries to check for successful resolutions.

6. If the results are diluted with commonly queried but irrelevant hostnames, exclude these from the query, perhaps with a wildcard pattern. This may span multiple iterations.


Quick analysis of @fields.query field(s)

This analysis is based on all 301 events for your query in your selected timeframe.

Rank	@fields query	Count	Percent
1	adrlwiexnyfqbjx.work	1	0.33%
2	aetcigxthikj.ga	1	0.33%
3	afeadjwjxhzxwde.xyz	1	0.33%
4	afqpqewzxb.top	1	0.33%
5	aivnpsrgpzt.xyz	1	0.33%
6	akktwpjntl.gq	1	0.33%
7	alqxrnkleayjqf.ga	1	0.33%
8	aqkxhjmbgh.work	1	0.33%
9	arlmzuybkd.gq	1	0.33%
10	asnwrfeupsmd.work	1	0.33%

```
@fields.source_ip:10.1.2.3 AND @fields.err_code:NXDOMAIN AND NOT
@fields.query:(*microsoft* OR *msft*)

@fields.source_ip:10.1.2.3 AND @fields.err_code:NXDOMAIN AND
@fields.query:/[a-z]{5,7}\.[0-9]{13,}\.net/
```

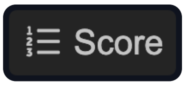
7. Once the results have been limited primarily to queries that appear related, try to determine a hostname pattern (wildcard or regex) to use in the query, instead of only looking for responses of NXDOMAIN.

```
@fields.source_ip:10.1.2.3 AND @fields.query:/[a-z]{5,7}\.[0-9]{13,}\.net/ AND NOT
@fields.err_code:NXDOMAIN
```

8. Excluding these cases from the query may help locate any **successful resolutions**. If such occurrences are located, follow up by searching for communications to the returned IP, or additional DNS resolutions that return the IP.

```
@fields.answers:*12.34.56.78* OR @fields.dest_ip:12.34.56.78
```

9. Score the **source IP address** field to locate which internal devices have been observed communicating with these external destinations so local investigations can be carried out on the machines.



Domain Fluxing "Gotchas":

1. **Google Chrome/Chromium**
   Sometimes, domain fluxing breaches will fire due to the presence of domains which contain 9-15 a-z characters will no TLD. This is a syntax used by Google Chrome/Chromium as an anti NXDOMAIN hijacking technique. When carrying out investigations, check that it is not just Chrome working out what happens to NXDOMAIN DNS requests.
   https://code.google.com/p/chromium/issues/detail?id=47262

2. **Apple devices**
   If the domains are a random series of characters, many with subdomains and some with hyphens ending **.com** (e.g., **9z3wj4ugkx1q5k4rgsir9b-8j2g.87ak3nscvd9[.]com**), this could be a process which is performed by Apple devices.

Try this:

Locate and evaluate a Compromise / Domain Fluxing Model Breach. Search for Domain Fluxing in the Omnisearch bar and adjust the Threat Tray time period as necessary. Review the Model Breach Event Log to determine whether the heuristically detected domains appear to represent domain fluxing. If the domain fluxing is apparent, use the above techniques to understand the scope of the activity. If the queries follow an isolatable pattern, use it to determine whether the DNS query was successful in obtaining an IP address. If an IP address was obtained, search for communications to that address by using the Score feature to obtain a list of source IPs.

Understanding Details of DCE/RPC in Advanced Search

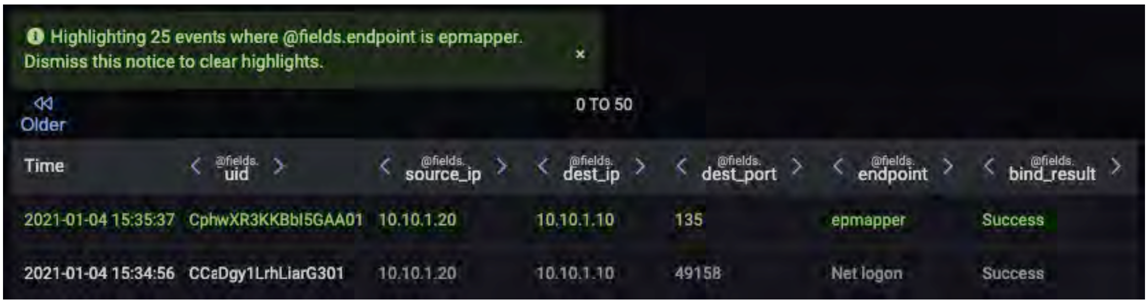
DCE/RPC is a remote procedure call system that facilitates communication among programs in a distributed environment, allowing the execution of a procedure on a remote device. DCE/RPC has legitimate uses and is heavily employed by Windows devices under normal operation, but due to the large variety and high utility of tasks that can be completed remotely using this system, it is attractive to malicious actors as a vehicle for lateral movement.

In order to trigger an operation remotely via DCE/RPC, the initiating device first needs to locate and bind to an **interface** corresponding to the desired **endpoint**, through which it can make a request to perform one or more operations. In order to locate said interface, it may first bind and issue a request to a separate interface known as the Endpoint Mapper.

1. Review **@type:"dce_rpc"** events in Advanced Search. Discern what protocol (direct TCP or UDP, SMB, HTTP, HTTPS) is being used from the destination port used to access Endpoint Mapper. This activity can also be confirmed by inspecting the packet capture.

2. Review the endpoint used and the operation requested so the tasks performed can be tracked to a certain degree even in cases where the command's low-level contents are encrypted.

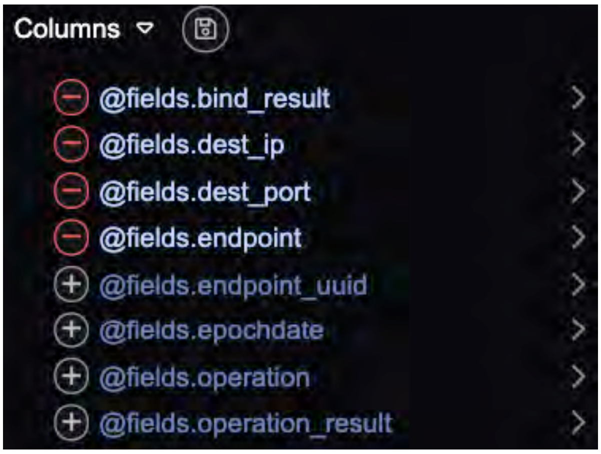
3. Utilize the **@fields.endpoint** dialog window to locate events where the endpoint matches the result epmapper. Clicking this result will highlight matching events in **green**. Endpoint Mapper can be used to map and bind two endpoints, such as drsuapi and Net logon and subsequent operations requested via those endpoints.


Highlighting 25 events where @fields.endpoint is epmapper.
Dismiss this notice to clear highlights.

Time	@fields.uid	@fields.source_ip	@fields.dest_ip	@fields.dest_port	@fields.endpoint	@fields.bind_result
2021-01-04 15:35:37	CphwXR3KKBbI5GAA01	10.10.1.20	10.10.1.10	135	epmapper	Success
2021-01-04 15:34:56	CCaDgy1LrhLiarG301	10.10.1.20	10.10.1.10	49158	Net logon	Success

__Note:__ Clicking the plus symbol to the left of the fields in the Columns list will display different headings in the Advanced Search event table.

Doing so can make it easier for an end user to locate particular pieces of relevant information rather than using the expanded view of each entry.



4. Examples of **endpoints** that may be accessed in the course of lateral movement are presented to the right and can be found in the **operation** field.

   A more comprehensive list for review can be obtained by using the Score function to better evaluate whether they are authorized and expected from the source device.

atsvc: Task scheduling
svcctl: Service Control Management
iWbemService: Access to WMI Services
winreg: Windows Registry
eventlog: Event Logs

Try this:

Find and review examples of DCE/RPC usage in Advanced Search. Note the endpoint, operation and success status of each.

Narrow the search results to failed bind attempts and review any obvious trends such as consistent repeated or large numbers of failures in a short time. Make use of the Score feature to find common sources, destinations, endpoints or operations. Compare a group of results to expected business functions to evaluate whether the behaviour represents misconfigurations or unauthorized activity.

Locating Clients Using External DNS

Permitting client devices to communicate directly with external DNS servers exposes an organization to security risks as discussed in a 2015 US-CERT advisory post (https://www.us-cert.gov/ncas/alerts/TA15-240A) and may additionally present a compliance issue. Thus, it is helpful to know whether this is occurring, and if so, which clients are involved and need correcting. This can be done in Advanced Search with a few clicks.

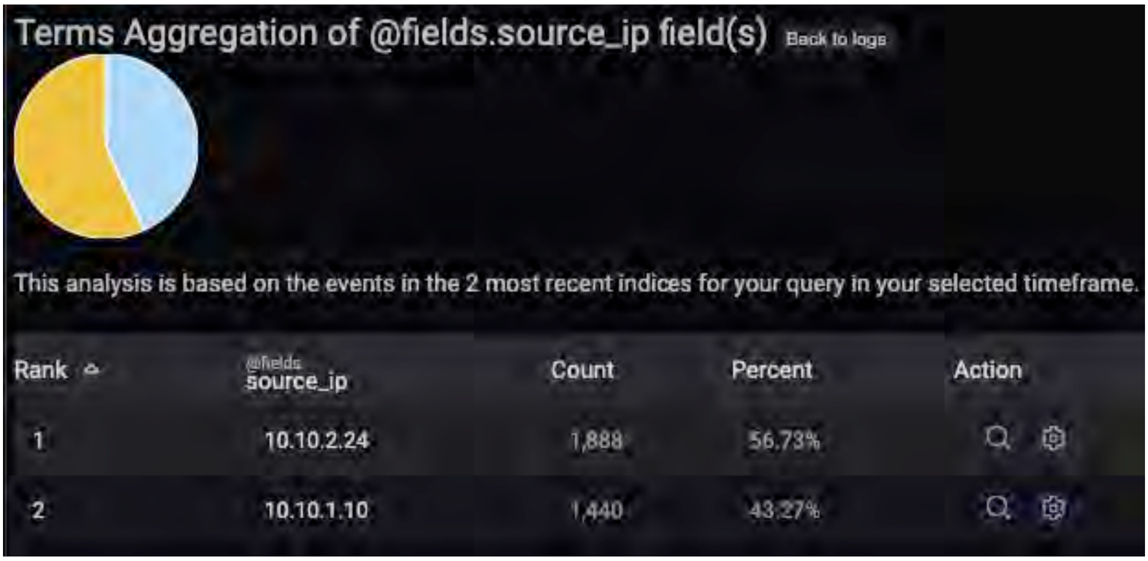
1. The initial query should restrict the results to DNS traffic only. Though there is a dns type event, only the conn type contains fields that distinguish between internal and external endpoints, thus the results should be narrowed using its **service** field.

```
@fields.service:dns
```

2. The only relevant results are those whose destination (responder) is considered external. Add in another field to filter the results.

```
@fields.service:dns AND @fields.local_resp:false
```

3. Use the **Terms** feature with the **source_ip** field to view a distribution of the top contributing source addresses.



Terms Aggregation of @fields.source_ip field(s)

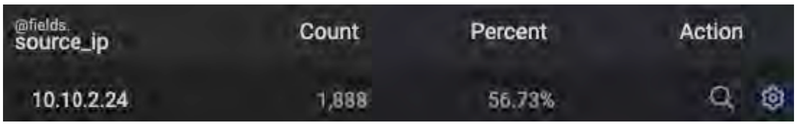
This analysis is based on the events in the 2 most recent indices for your query in your selected timeframe.

Rank	@fields source_ip	Count	Percent	Action
1	10.10.2.24	1,888	56.73%	
2	10.10.1.10	1,440	43.27%	

4. Adjust the query as needed to exclude internal DNS servers, as their external forwarding of requests will tend to eclipse other source devices.

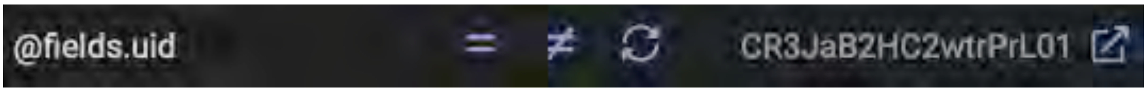
```
@fields.service:dns AND @fields.local_resp:false AND NOT
@fields.source_ip:(10.0.0.1 OR 10.0.0.2)
```

5. To identify a source beyond its IP address, add it as a term in your query by clicking the **magnifying glass** at the end of the row.



@fields. source_ip	Count	Percent	Action
10.10.2.24	1,888	56.73%	

6. Pivot on one of the source IP's communications using the link icon in the **UID** field to view the offending device Threat Visualizer.



@fields.uid = ≠ CR3JaB2HC2wtrPrL01

Try this:

As detailed above, use Advanced Search to list the IPs of the network clients most frequently observed directly accessing external DNS. For each of the top 3 sources, use the UID of one of the communications to navigate to the source device in the Threat Visualizer. Consider whether this is authorized activity.

Pinpointing External SMB Communications

The SMB protocol, having been designed exclusively for use over a private network, may present attackers with opportunities for infiltration, exfiltration, or exploitation when exposed to the open Internet. In addition to the clear increase in attack surface for third parties interested in reading or altering the contents of company file servers, a variety of exploits specifically target the protocol. One such example is the NSA's leaked EternalBlue exploit. This leverages a vulnerability in unpatched systems using SMBv1 and has been employed by a variety of widespread malware including the ransomware campaigns commonly known as WannaCry, Petya, and BadRabbit.

Even in cases where all systems are fully updated and use the latest versions of the protocol, further exploits may be developed, providing sufficient reason to disallow its unprotected use over public networks. Any such communication allowed inbound from the Internet to a network device - or outbound directly over the Internet to a remote organizational resource - represents, at best, potentially increased exposure; At worst, it may represent a glaring vulnerability that threatens the network's operational integrity. Darktrace has defined multiple Models capable of detecting the use of protocols, usually preserved for internal use, being used externally.

1. Navigate to Advanced Search, specify a time frame and use a query to search for all connections which use the **SMB service**. This can be achieved with a pattern that will include various versions of the protocol, as well as its use in combination with various authentication mechanisms/protocols.

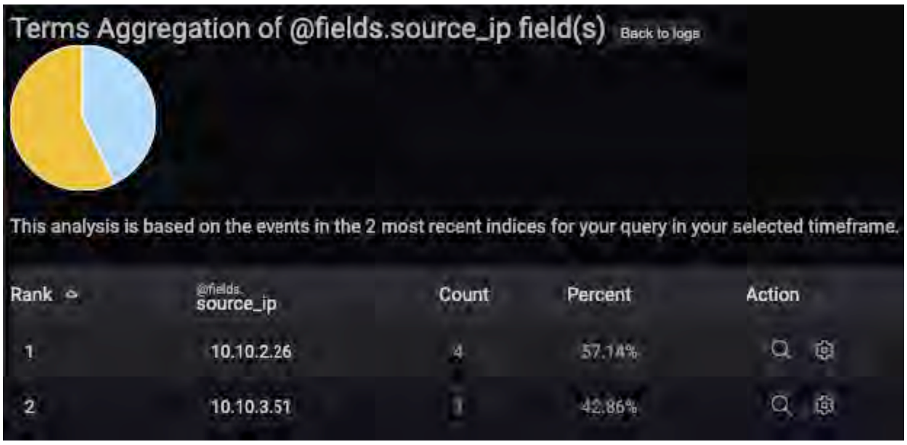
   ```
   @fields.service:*smb*
   ```

   Note: *The above syntax will exclude failed connection attempts as it is only populated when an application protocol is recognized in use over a successfully established connection. To view failed connection attempts, use @fields.dest_port.*

2. To further restrict your results to connections with an external originator or responder, append the following.

   ```
   @fields.service:*smb* (@fields.local_orig:false OR @fields.local_resp:false)
   ```

3. Use the **Terms** capability to see the distribution of involved internal (and external) IPs, or simply to adjust to a smaller time frame.



This analysis is based on the events in the 2 most recent indices for your query in your selected timeframe.

Rank	@fields. source_ip	Count	Percent	Action
1	10.10.2.26	4	57.14%	🔍 ⚙
2	10.10.3.51	3	42.86%	🔍 ⚙

4. Upon finding a case of interest, shift to a query that **specifies the source and/or destination IP** in order to more closely inspect the relevant communications.

   Note: *Even failed SMB connection attempts may represent a vulnerability if such attempts are being allowed across the network perimeter or are initiated by company devices.*

Try this:

Use Advanced Search to locate any and all external inbound/outbound SMB traffic from the network over the last 7 days. Utilize the service field so as not to include failed connection attempts.

Perform a similar search targeting failed connection attempts to port 445. These are represented by conn events with no listed service. Confirm that the results only include failed connections which commonly list a history of S (unanswered SYN packet) and Sr (a SYN packet rejected with a RST packet).

Additional Advanced Search Tactics

Advanced Search includes a number of simple but powerful shortcuts to facilitate writing queries. Try out the following examples:

1. Find file transfers of a **specific MIME type**:

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

   Using the above syntax, locate all PDF files downloaded in the past 24 hours. Which PDF file has been accessed the most?

2. Regular expression syntax can be used between two forward slashes in an Advanced Search query. Use the following to specify a range of IPs that does not divide nicely on an octet boundary:

   ```
   @fields.dest_ip:/172\.<16-31>\..*/
   ```

   The above pattern matches all IPs in the 172.16.0.0/12 range.

   Note: *Regex syntax is outside the scope of this document. The pipe and parentheses (|) cannot be used as Advanced Search uses Apache Lucene syntax. The available regex syntax, in combination with logical operators and wildcard matching, is sufficient for the majority of practical use.*

   Using a combination of wildcard pattern matching, regular expressions, and logical operators, write a query that specifically returns inbound external connections, i.e., those from IPs not found in the RFC 1918 ranges below:

   - *10.0.0.0 – 10.255.255.255*
   - *172.16.0.0 – 172.31.255.255*
   - *192.168.0.0 – 192.168.255.255*

3. Use the **orig_cc** or **resp_cc** fields in the **conn** event type in combination with country codes for external sources or destination IP addresses:

   ```
   @fields.resp_cc:"RU"
   ```

   Use the Score option for orig_cc to review country codes of inbound communications in the last 15 minutes.

4. The following query can be used to limit search results to the **unidirectional traffic** from one IP range to another, useful when diagnosing or troubleshooting this issue:

```
@fields.source_ip:10.0.* AND @fields.dest_ip:10.1.* AND ((@fields.orig_pkts:>0
AND @fields.resp_pkts:0) OR (@fields.orig_pkts:0 AND @fields.resp_pkts: >0)) AND
NOT @fields.history:S
```

5. **Parentheses** can be used to create shorter queries. The following query:

```
@fields.source_ip:10.10.4.3 OR @fields.source_ip:10.10.4.4 OR
@fields.source_ip:10.10.4.7
```

can be shortened to:

```
@fields.source_ip:(10.10.4.3 OR 10.10.4.4 OR 10.10.4.7)
```

6. Additionally, when **no operator exists** between two terms, **AND** is assumed. Shorten queries by omitting the AND operator, so the following:

```
@fields.source_ip:10.10.4.3 AND @fields.dest_ip:10.10.4.4
```

can be shortened to:

```
@fields.source_ip:10.10.4.3 @fields.dest_ip:10.10.4.4
```

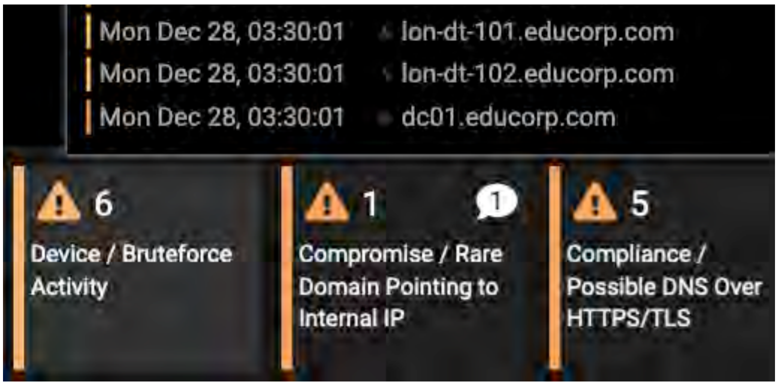
7. Use the **exact match (“ ”)** in a specific field, to detect, for example, the use of a weak cipher suite:

```
@fields.cipher:"SSLv20_CK_RC4_128_WITH_MD5"
```

5. Model Breaches

As a best practice, when reviewing Model Breaches over a set coverage period, it is advisable to first perform a cursory inspection of the full set of Model Breaches. The amount of time devoted to inspecting each individual Model Breach in this phase will vary depending on the number of Model Breaches that have occurred over the chosen coverage period but will invariably be much less than the time required for a full, in depth investigation. Instead a brief triage or inspection of the basic details of each Model Breach, taking note of those which may merit further investigation can be a more effective use of time.

1. With the Threat Tray organized and time period set, view the breaches caused. **Hovering over** any of these breaches will display which devices caused the Model to fire and at what time. This can be a good indicator of whether the device commonly breaches the same Model.



Mon Dec 28, 03:30:01 lon-dt-101.educorp.com
Mon Dec 28, 03:30:01 lon-dt-102.educorp.com
Mon Dec 28, 03:30:01 dc01.educorp.com

⚠ 6 Device / Bruteforce Activity

⚠ 1 Compromise / Rare Domain Pointing to Internal IP

⚠ 5 Compliance / Possible DNS Over HTTPS/TLS

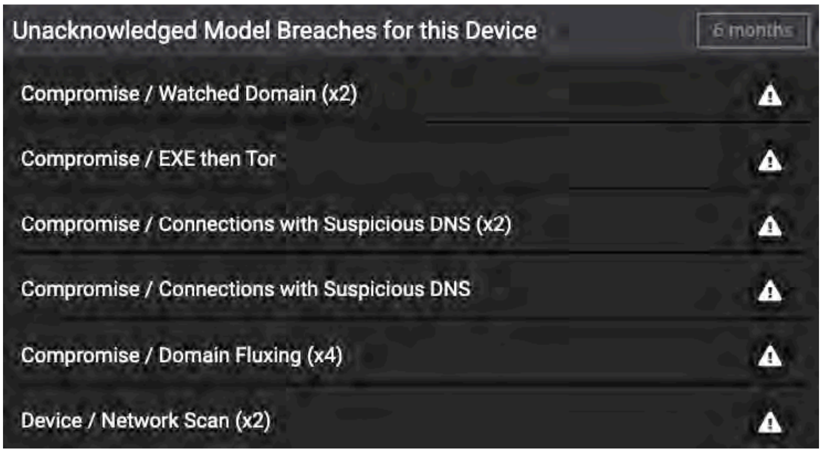
2. First of all, when opening the Breach Log, check which device caused the Model Breach. Click the **device name** to populate it in the **Omnisearch bar**.

dc01.educorp.com

   a. Click on the **Device Summary** icon to the right of the device name in the Omnisearch bar.

   b. Within the Device Summary, scroll down to locate the **historical Model Breaches for this Device**.

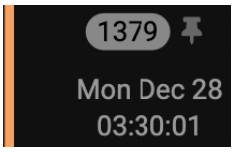
   Change the time period for the Unacknowledged or Acknowledged breaches from 1 week to **6 months** and see if the device regularly breaches the same Model and at what interval. If a device routinely performs legitimate actions, it may not require further investigation.



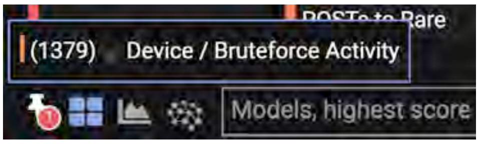
Unacknowledged Model Breaches for this Device — 6 months

Compromise / Watched Domain (x2) ⚠
Compromise / EXE then Tor ⚠
Compromise / Connections with Suspicious DNS (x2) ⚠
Compromise / Connections with Suspicious DNS ⚠
Compromise / Domain Fluxing (x4) ⚠
Device / Network Scan (x2) ⚠

3. For any Model Breach that appears worthy of investigating further, note its unique identifying number called the **Model Breach ID** within the Breach Log.

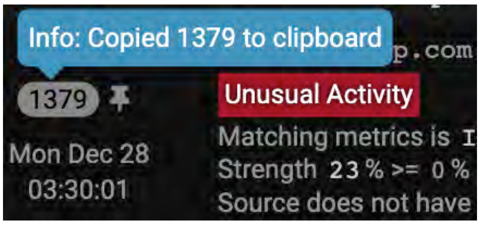


   a. This breach can be **temporarily pinned**. It can be found in the lower left corner of the Threat Tray for further investigation as long as the Threat Visualizer remains logged in.



   b. By directly clicking the number, the Model Breach ID can be **copied to the clipboard** so can be easily pasted into a URL of the form:

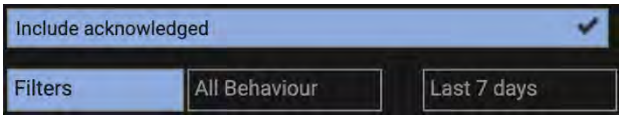
   https://<darktrace>/#modelbreach/<breachID>



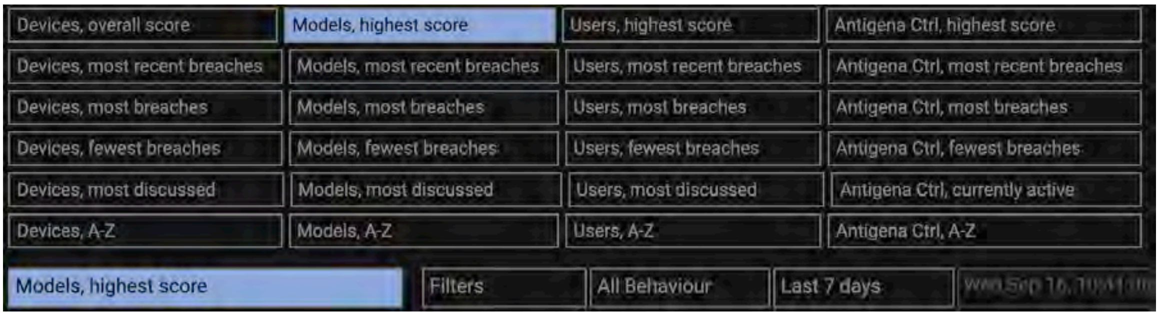
   c. The above URL can also be obtained by clicking the **clipboard icon**. This will also copy all the relevant metadata presented in the Breach Log.

4. If a Model Breach clearly requires no further action as the detected activity is recognized or benign, **acknowledge** the breach to hide it.

   Note: *These hidden breaches can be presented in the Threat Tray again by clicking the Include Acknowledged filter.*



5. Consider **sorting or filtering** the Threat Tray into the detected categories to revisit the narrowed down Model Breaches in order of urgency or priority.



6. Not all malicious activity is blaringly obvious, so take note of **weak indicators** whilst proceeding through an investigation, as it is often the combination of these indicators that will provide a sense of the likely benign or malicious nature of an event.

7. Click **Discuss this model breach with other analysts.**

   Comments can be added to a Model Breach to indicate:

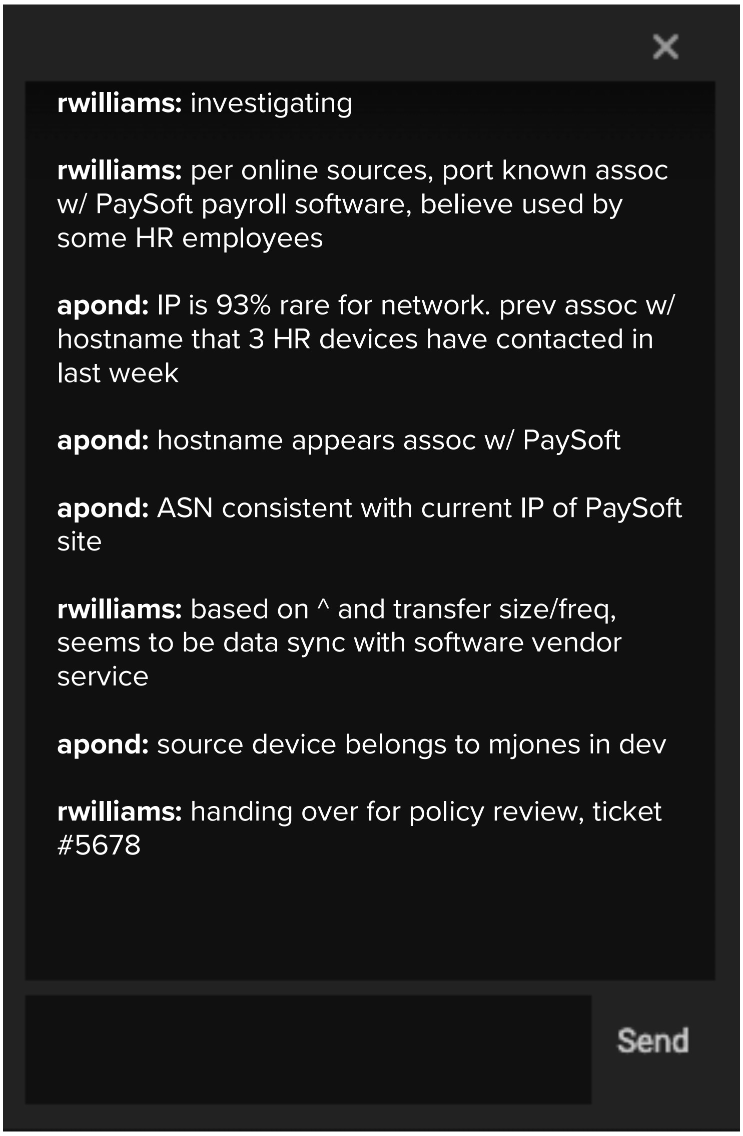
   a. That it is being investigated, to avoid overlapping efforts

   b. As weak indicators or details of potential interest are discovered

   c. If the nature of the activity has been determined to some degree of confidence and why

      Once comments have been made, the icon will change.

      While this level of detail is not always necessary it can help organize findings and serve as a future reminder, potentially saving time in the long run.



rwilliams: investigating

rwilliams: per online sources, port known assoc w/ PaySoft payroll software, believe used by some HR employees

apond: IP is 93% rare for network. prev assoc w/ hostname that 3 HR devices have contacted in last week

apond: hostname appears assoc w/ PaySoft

apond: ASN consistent with current IP of PaySoft site

rwilliams: based on ^ and transfer size/freq, seems to be data sync with software vendor service

apond: source device belongs to mjones in dev

rwilliams: handing over for policy review, ticket #5678

8. Once the investigation is complete and a brief comment has been made, **acknowledg**e the Model Breach.

   a. If multiple breaches are investigated at the same time, click the **acknowledge all** button.

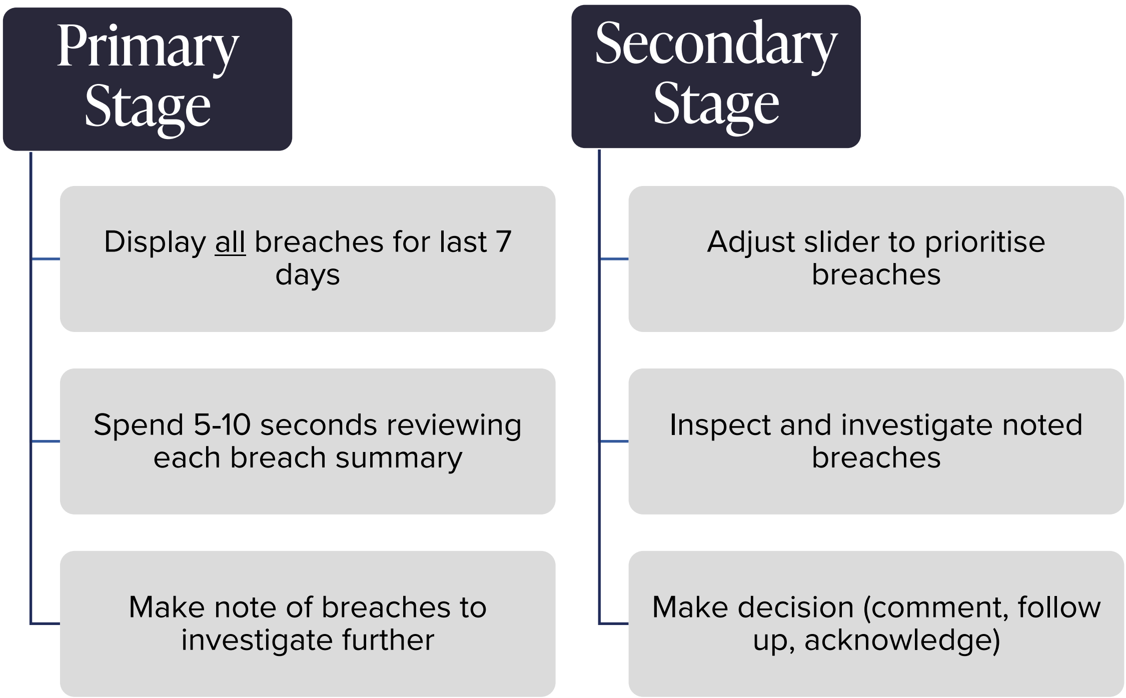
   b. To append a comment to breaches in bulk, click the **acknowledge all and leave a comment** button.

9. If a particular category of benign activity repeatedly causing Model Breaches, consider **tuning the Model** to exclude these cases.

   This can be done by editing the Model directly or by adding a device to the Model's **Exclude List** by clicking the ignore future breaches of the chosen Model for the selected device in from a Breach Log window.

10. Models can be classified into three categories: **anomalous activity**, **compliance**, and **compromise**. Although overlap exists between these categories, they are not intended to neatly divide, but rather for familiarization and directing investigations of Model Breaches.

In summary, these steps can be split into two main stages. Try following the workflow below within the Threat Visualizer:



Primary Stage
Display all breaches for last 7 days
Spend 5-10 seconds reviewing each breach summary
Make note of breaches to investigate further
Secondary Stage
Adjust slider to prioritise breaches
Inspect and investigate noted breaches
Make decision (comment, follow up, acknowledge)

Anomalous Activity

The "anomalous activity" category can be defined as including all events that are in some way unusual, whether this presents as an **unusual activity event**. This could be due to a device's deviation from its normal patterns of life, communications with a rare external endpoint, first-time access to a particular network share, or first-time use of a certain port or protocol.

Examples of such Models include, but are not limited to:

- Anomalous Connection / **Data Sent to New Domain**
- Anomalous Connection / **Multiple Connections to New External TCP Port**
- Device / **Sustained UDP Increase**
- Compromise / **UDP to Multiple Rare External Hosts**
- Compliance / **SSH to Rare External Destination**
- Anomalous Connection / **Unusual Internal RDP**
- Anomalous File / **Anomalous Octet Stream**
- Anomalous Connection / **Lots of New Connections**

Communications that are anomalous for one or more reasons may turn out to be recognized or expected upon review. The initial goal should be to correlate such events to known and/or legitimate activity. Once it has been confirmed that the activity is legitimate, investigation of the incident can be completed. Simply acknowledge the incident and end move on to the next Model Breach. A useful workflow may be:

1. **Compare** activity with that of approved applications / known operations.

2. **Research known uses of the port and/or protocol** and evaluate whether the observed activity appears to be in line with one of these uses.

3. Consider the device's **role** on the network.

    a. Is the device recognized and is its role known? If not:

        i. Look through the **Device Summary** which includes a breakdown of top ports used/served and endpoints communicated with over the last 4 weeks.

        ii. Look through the **Device Event Log** and filter on History to obtain observed credentials, user agents and changes in IP/subnet/hostname/MAC.

    b. Does the device's role **justify** or explain the observed activity?

        i. Can this instance be confirmed, perhaps via reproduction; or if appropriate, through discussion with the user?

    c. **Compare** the activity with what has previously been detected or observed.

        i. Check the **Device Breach Log** over a long period to find whether similar activity on the device has previously triggered Model Breaches. Do the same with the **Model Breach Log** to look for similar historical cases network-wide. If found:

- Were some of these cases found to represent legitimate activity? Check the Model Breaches for comments and/or **consult records** kept by the organization.

- Is the activity being **investigated** consistent with these cases?

ii. If the event involves one or more unrecognized external endpoints, use the **External Sites Summary** to find which other devices have communicated with the IP and/or hostname in the past week.

iii. If one or more metrics of the device's traffic were highlighted as unusual, use the **Graph** to review metric values over a longer time period.

- Graph the metric over the last **few weeks** to get a sense of how the metric compares to recent history.

- Navigate to another device with a similar role; review the same graph for the similar device to find whether a **similar pattern** has been observed.

Compliance

Events that fall into the “compliance” category tend to indicate the use of software, protocols, or technologies that may not be approved under an organization's network policy, or their use in circumstances that are generally not approved. The significance of such Model Breaches can be organization dependent so organizations may choose to alter existing or create additional Models to more closely reflect their compliance policies. Many Darktrace users find the built-in compliance Models sufficient as they are based upon a number of commonly restricted or disallowed behaviors and technologies.

Examples of such models include, but are not limited to:

- Compliance / **External Telnet**
- Compliance / **Outbound RDP**
- Compliance / **Remote Management Tool on Server**

When presented with a "compliance" Model Breach, the following workflow may assist with understanding:

1. The first item on the agenda is to **understand what the Model is detecting**; if it is not clear from the Model name, the Model definition will assist with this task. Furthermore, the Model Editor will also outline which conditions need to be detected in order to breach.

2. When the Model is understood, consider the following questions:

   a. Is the activity **against policy** and if not, should it be?

   b. Does the activity **violate one or more compliance regulations** for the organization?

   c. Is the activity **actionable** or worthy of **reporting**?

   d. Should such events be **logged** for future reference or auditing?

   e. Does the Model outline any **unknown issues**?

3. **Verify** what activity was detected by comparing the Model definition to the Model Breach Event Log or inspect the traffic in **Advanced Search** or **packet captures**.

4. If alerts continuously breach for the same Model and the detected activity is not relevant to the organization, **deactivate** the Model to remove numerous Model Breaches.

5. If certain activity is exempt but alerts are still desirable, **Model optimization** may be preferable. Apply Tags or change thresholds to assign a lower the breach priority.

Compromise

The “compromise” category includes those Models intended to detect specific methods of attack or abuse. These Models have significant overlap with the “anomalous activity” category, as many of them incorporate Darktrace's understanding of normal versus unusual activity, so as not to rely on any individual signature. Examples in this category include:

- Compromise / **EXE then Tor**
- Compromise / **New User Agent and POST**
- Compromise / **Excessive POSTs to Root**
- Compromise / **Domain Fluxing**
- Compromise / **HTTP Beaconing to Rare Destination**
- Compromise / **Beacon to Young Endpoint**
- Compromise / **SSL to DynDNS**
- Compromise / **Suspicious External Event Combination**
- Compromise / **Sustained SSL or HTTP Increase**

A Model Breach in the “compromise” category indicates that observed traffic matches a set of conditions describing a particular attack which is outlined in Model definition. While the workflow for this type of Model is very similar to the Anomalous Activity workflow, the following steps may be useful:

1. Look at the **Model Name**. This should quickly communication the nature of the activity.

2. Check the **Model definition** to see what the breach has highlighted and why.

    a. While the conditions are loosely defined to ensure unusual events are not missed, the conditions may point out important components to look at in the Threat Visualizer. For example, an external endpoint may need to exceed a rarity score in order for the Model to breach.

3. **Research the described attack technique** for more information in order to evaluate the detected activity.

4. **Compare** activity observed with that of approved applications / known organizational operations.

5. **Research known uses of the port and/or protocol** and evaluate whether the observed activity appears to be in line with either legitimate or potentially malicious activities.

6. Carry out investigations on any endpoints involved:

    a. Check the **External Sites Summary**.

        i. Have any **other devices** been observed connecting to this endpoint?

        ii. **When** did these devices start connecting?

        iii. Is it possible that the devices are all infected with the **same malware**?

b. Use **OSINT** and sandboxed environments to research any rare external endpoints.

   i. Are they known to be **linked with malicious activity**?

   ii. Upon visiting such endpoints, do they spawn any **unusual processes**?

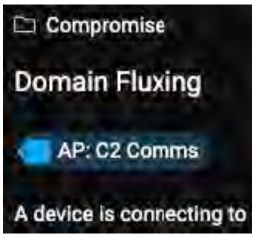
6. Targeted Threat Hunting

This section will explore examples demonstrating benefits of categorization through the use of device and model tags, device type, and device priority. In addition to applying these categories manually, they can be applied in a more automated fashion through the use of model actions. This document assumes introductory knowledge of the Tags and the Model Editor, as covered in the Threat Visualizer training.

The following Darktrace-defined tags, when applied to a model, indicate that it can detect some form of the corresponding **attack phase (AP)**:

- AP: Bruteforce
- AP: C2 Comms
- AP: Egress
- AP: Exploit
- AP: Internal Recon
- AP: Lateral Movement
- AP: Scanning
- AP: Tooling

1. The above **Attack Phases** can be viewed beside the **Model Tags** section when reviewing a Model in the **Model Editor**. Once a Model has been tagged either manually or automatically, they can be filtered within the Threat Visualizer.



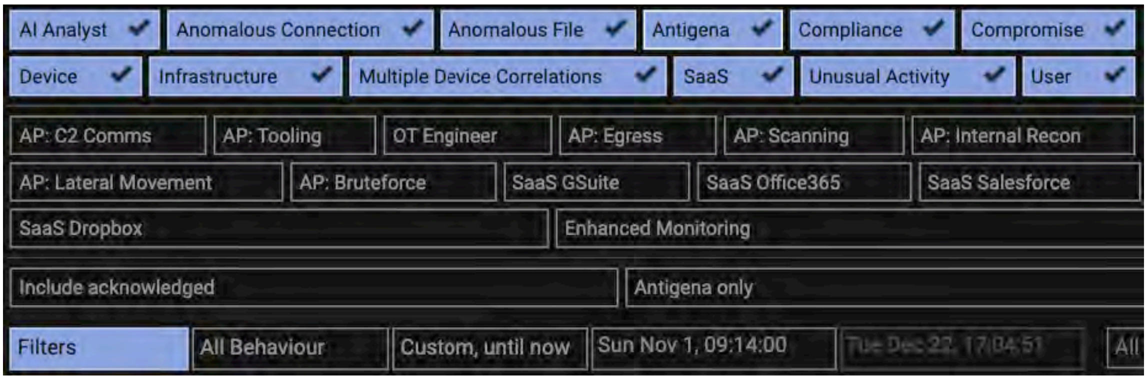
Compromise

Domain Fluxing

AP: C2 Comms

A device is connecting to

2. The **Threat Tray** can be filtered by Attack Phase, allowing breaches of tagged Models to be displayed or hidden. Selecting the Attack Phase allows specific categories of activity to be investigated which can be useful in the case of a suspected or known compromise.



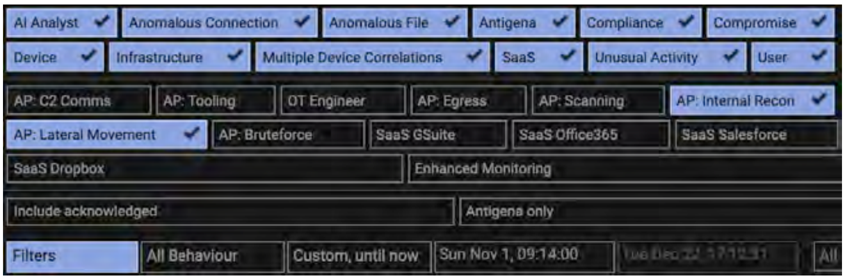
3. Apply **custom Tags** to Models to allow grouping into categories for the purpose of filtering the Threat Tray. For example, tagging a Model by which user created it, or which team should be concerned with triaging or resolving an issue can be useful for dividing up Model Breaches by SOC tier levels.

Try this:

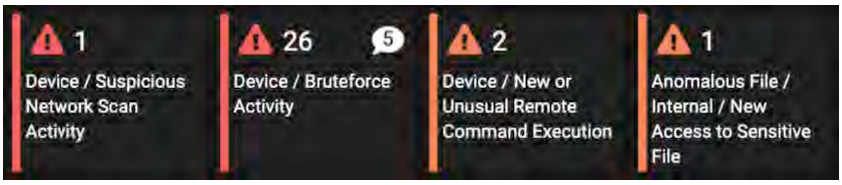
Create a Tag to be applied to custom Models. Apply this Tag to any existing Models that have been created by members of the organization.

Example Workflow: Threat Hunting Through Categorization

1. Filter the Threat Tray to only display Model Breaches that might indicate the occurrence of **Internal Recon** or **Lateral Movement**.



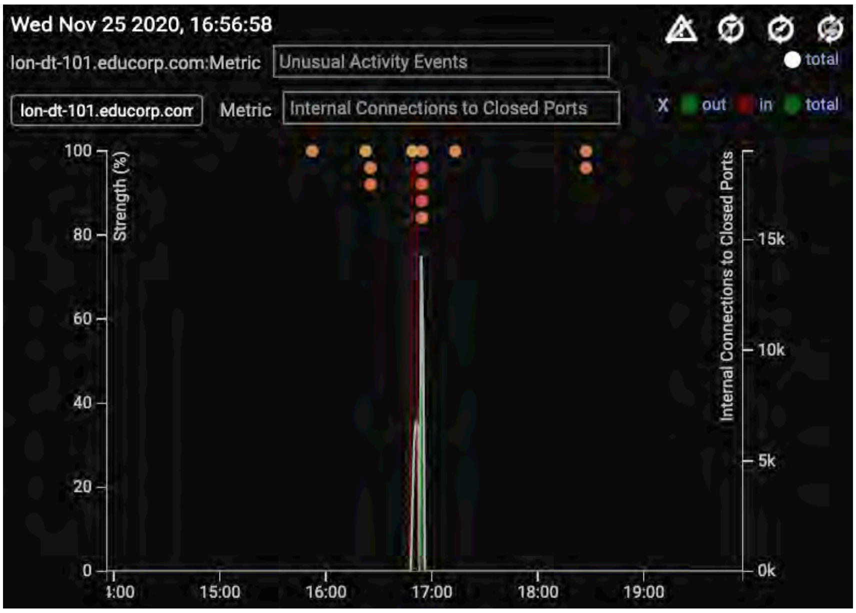
2. Review these **filtered Model Breaches** and compare each instance to the role and expected behavior of the involved devices.



1
Device / Suspicious Network Scan Activity
26
5
Device / Bruteforce Activity
2
Device / New or Unusual Remote Command Execution
1
Anomalous File / Internal / New Access to Sensitive File

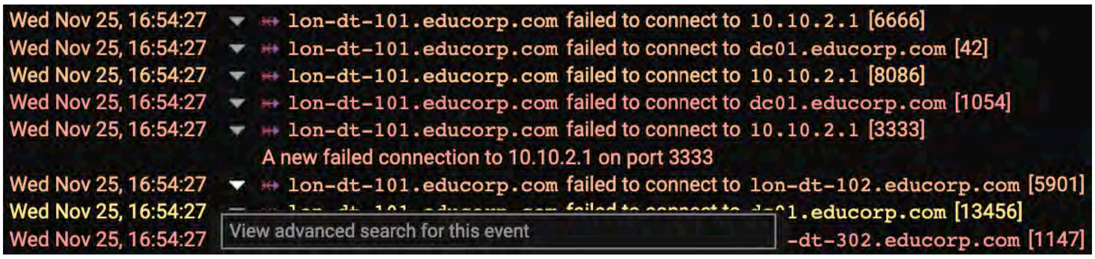
   a. For example, with the network scan, it may be useful to open a graph and **plot some metrics**.

   b. It may be beneficial to look at the **historical connectivity** to see if there are any other spikes indicating routine scanning.



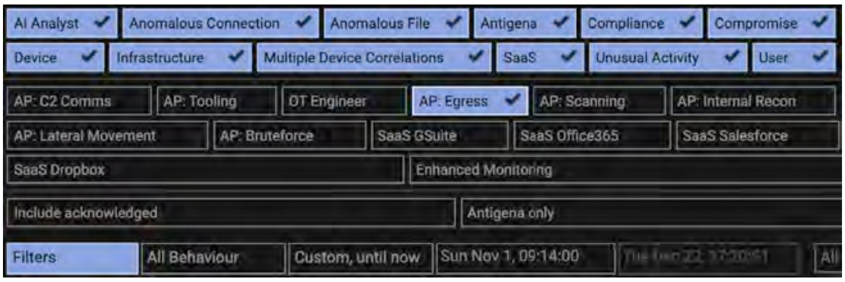
   c. Look at the **other Model Breaches** which occurred around the same time in the Device Breach Log.

   d. Pivot to **Advanced Search** from the **Event Logs** to investigate the connectivity.



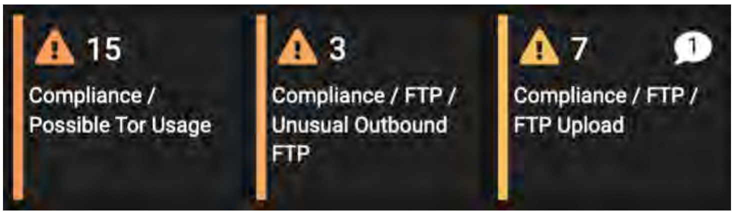
```
Wed Nov 25, 16:54:27   lon-dt-101.educorp.com failed to connect to 10.10.2.1 [6666]
Wed Nov 25, 16:54:27   lon-dt-101.educorp.com failed to connect to dc01.educorp.com [42]
Wed Nov 25, 16:54:27   lon-dt-101.educorp.com failed to connect to 10.10.2.1 [8086]
Wed Nov 25, 16:54:27   lon-dt-101.educorp.com failed to connect to dc01.educorp.com [1054]
Wed Nov 25, 16:54:27   lon-dt-101.educorp.com failed to connect to 10.10.2.1 [3333]
                       A new failed connection to 10.10.2.1 on port 3333
Wed Nov 25, 16:54:27   lon-dt-101.educorp.com failed to connect to lon-dt-102.educorp.com [5901]
Wed Nov 25, 16:54:27   lon-dt-101.educorp.com failed to connect to dc01.educorp.com [13456]
Wed Nov 25, 16:54:27   View advanced search for this event               -dt-302.educorp.com [1147]
```

3. Adjust the Threat Tray filters again by holding shift and **clicking AP: Egress** to remove the two pre-selected filters.



AI Analyst ✓ | Anomalous Connection ✓ | Anomalous File ✓ | Antigena ✓ | Compliance ✓ | Compromise ✓
Device ✓ | Infrastructure ✓ | Multiple Device Correlations ✓ | SaaS ✓ | Unusual Activity ✓ | User ✓
AP: C2 Comms | AP: Tooling | OT Engineer | AP: Egress ✓ | AP: Scanning | AP: Internal Recon
AP: Lateral Movement | AP: Bruteforce | SaaS GSuite | SaaS Office365 | SaaS Salesforce
SaaS Dropbox | Enhanced Monitoring
Include acknowledged | Antigena only
Filters | All Behaviour | Custom, until now | Sun Nov 1, 09:14:00 | Tue Dec 22, 17:20:51 | All

4. **Review the data egress Model Breaches** and confirm whether they are recognized.



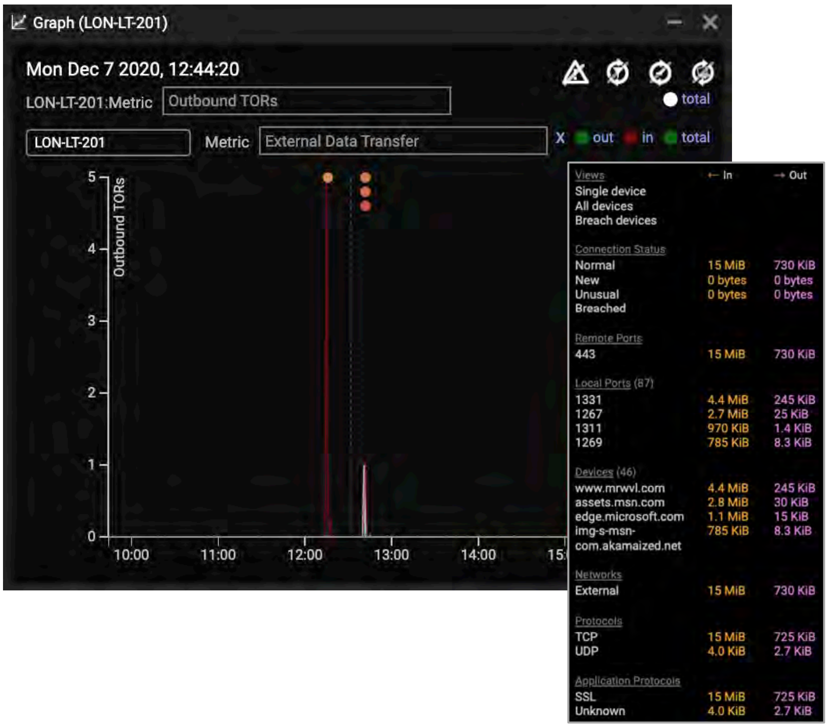
15 Compliance / Possible Tor Usage

3 Compliance / FTP / Unusual Outbound FTP

7 Compliance / FTP / FTP Upload

a. Taking the Tor Usage Model as an example, open up a **graph** and view the **external data transfer** occurring at the time of the outbound Tor.

Apply filters to the graph by utilizing the pane down the right-hand side of the Threat Visualizer.



Graph (LON-LT-201)

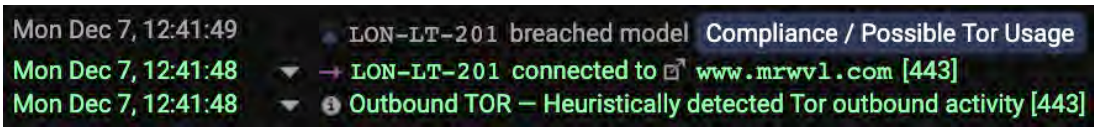
Mon Dec 7 2020, 12:44:20

LON-LT-201:Metric Outbound TORs

LON-LT-201 Metric External Data Transfer

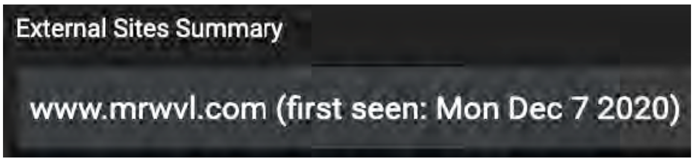
Views	← In	→ Out
Single device		
All devices		
Breach devices		
Connection Status		
Normal	15 MiB	730 KiB
New	0 bytes	0 bytes
Unusual	0 bytes	0 bytes
Breached		
Remote Ports		
443	15 MiB	730 KiB
Local Ports (87)		
1331	4.4 MiB	245 KiB
1267	2.7 MiB	25 KiB
1311	970 KiB	1.4 KiB
1269	785 KiB	8.3 KiB
Devices (46)		
www.mrwvl.com	4.4 MiB	245 KiB
assets.msn.com	2.8 MiB	30 KiB
edge.microsoft.com	1.1 MiB	15 KiB
img-s-msn-com.akamaized.net	785 KiB	8.3 KiB
Networks		
External	15 MiB	730 KiB
Protocols		
TCP	15 MiB	725 KiB
UDP	4.0 KiB	2.7 KiB
Application Protocols		
SSL	15 MiB	725 KiB
Unknown	4.0 KiB	2.7 KiB

b. Look at the **Model Breach Event Log** to view the connectivity.



```
Mon Dec 7, 12:41:49     LON-LT-201 breached model Compliance / Possible Tor Usage
Mon Dec 7, 12:41:48  ▾  → LON-LT-201 connected to www.mrwvl.com [443]
Mon Dec 7, 12:41:48  ▾  Outbound TOR — Heuristically detected Tor outbound activity [443]
```

c. View the **External Sites Summary** to see when the endpoint was first connected to and if any other devices have connected to it.



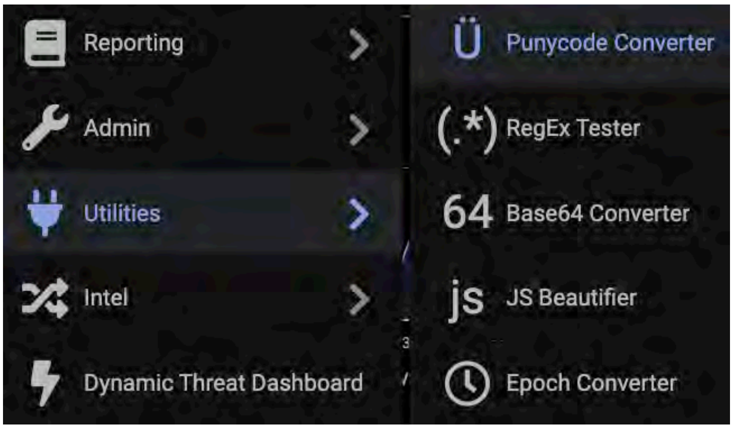
External Sites Summary

www.mrwvl.com (first seen: Mon Dec 7 2020)

7. Utilities

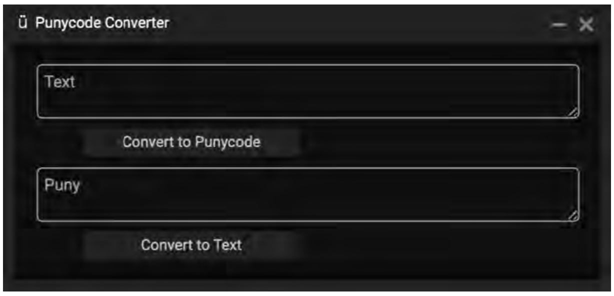
There are five useful additional tools located in the main menu under Utilities. These are:

- Punycode Converter
- RegEx Tester
- Base64 Converter
- JS Beautifier
- Epoch Converter



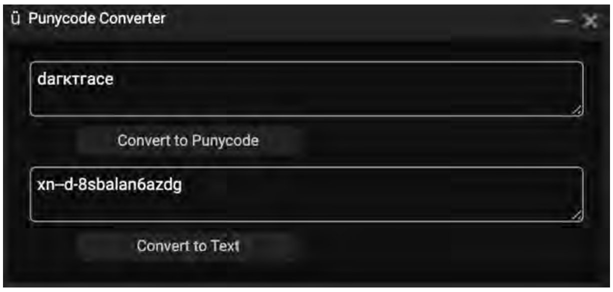
Punycode Converter

1. On the Threat Visualizer home screen, select **Menu** > **Utilities** > **Punycode Converter**. Punycode converts Unicode characters to ASCII. The converter can be used to encode/decode internationalized domain names (IDN) which can assist in understanding foreign domains.



2. There are multiple use cases for the Punycode Converter:

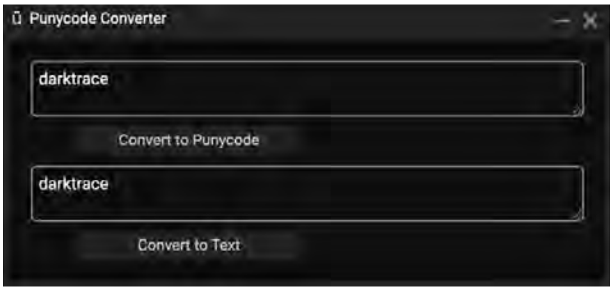
   a. In the example to the right, cyrillic characters have been used to type the word “**darктrace**”, which resembles Darktrace. Such techniques may be used to trick users into visiting spoofed domains. Converting this to Punycode shows a string that does not look like Darktrace at all in English characters.



darктrace

xn–d-8sbalan6azdg

   In comparison, using an English keyboard to type in “**darktrace**” and converting this to Punycode returns an identical string.



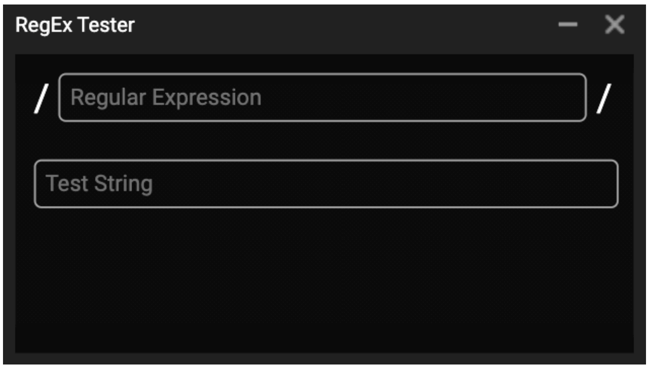
darktrace

darktrace

   b. Alternatively, if a domain in a Model Breach Event Log is presented in Punycode because the original domain contains non English characters, it is easy to convert the Punycode into a more readable text format by clicking **Convert to Text**.

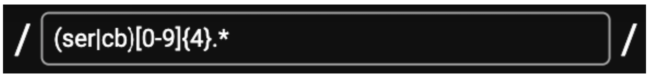
RegEx Tester

1. On the Threat Visualizer home screen, select **Menu** > **Utilities** > **RegEx Tester**.



2. Enter a regular expression in the first text field. The following will check for a valid device name:

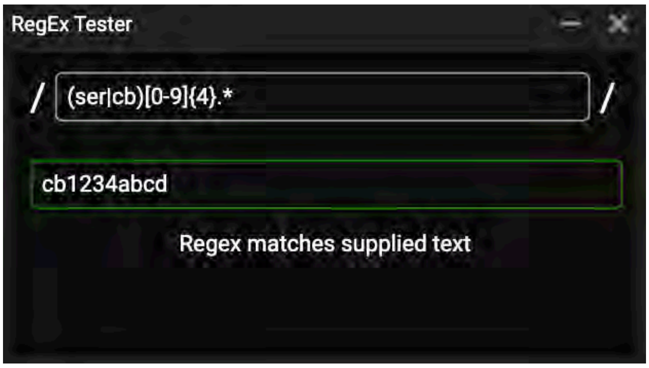
   (ser|cb)[0-9]{4}.*



/ (ser|cb)[0-9]{4}.* /

   This checks for hostnames that begin with ser or cb followed by 4 numbers between 0 and 9. The . acts as a wildcard that checks for any additional characters.*

3. Enter a valid URL and click out of the text field box. If the border around the text field turns **green** and a “Regex matches supplied text” message is displayed, the regular expression is **valid**.

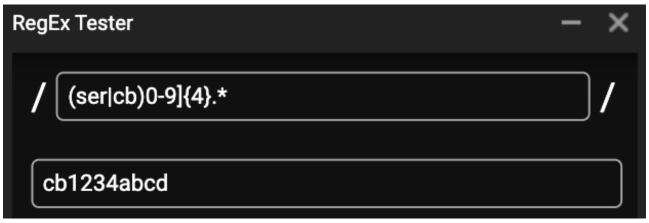


/ (ser|cb)[0-9]{4}.* /

cb1234abcd

Regex matches supplied text

4. Inserting an **invalid** regular expression, such as one with unbalanced brackets, will make the text field border color turn **white**.

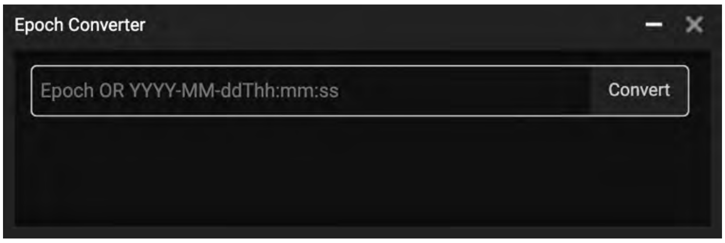


/ (ser|cb)0-9]{4}.* /

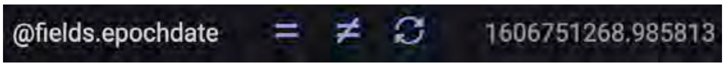
cb1234abcd

Epoch Converter

1. Open the **Epoch Converter** by choosing Utilities under the main menu.

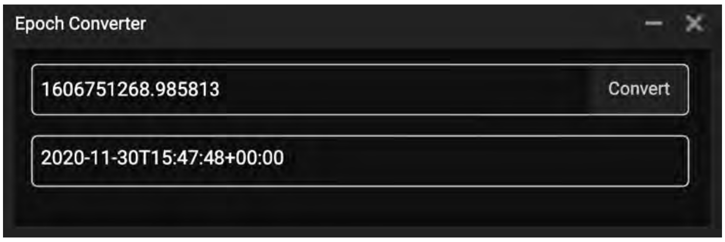


2. **Epoch dates** can be found in **Advanced Search** (@fields.epochdate), **API calls** or external **URIs**.



@fields.epochdate = ≠ 1606751268.985813

3. **Convert** dates into/from the epoch format (i.e. the number of seconds since 1st January 1970) into/from normal time.



1606751268.985813

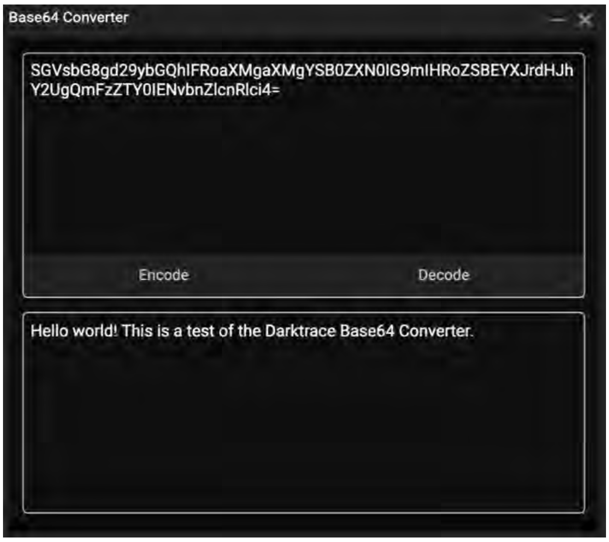
2020-11-30T15:47:48+00:00

Base64 Converter

1. On the Threat Visualizer, select **Base64 Converter** from Utilities in the Main Menu.

2. Paste Base64 encoded text into the top box and click **Decode** to convert into plain text which will be printed in the lower box. This can be useful for encoded information observed in PCAPs.

3. Alternatively, paste or type plain text into the top box and click **Encode** to present Base64 encoded text in the lower box.



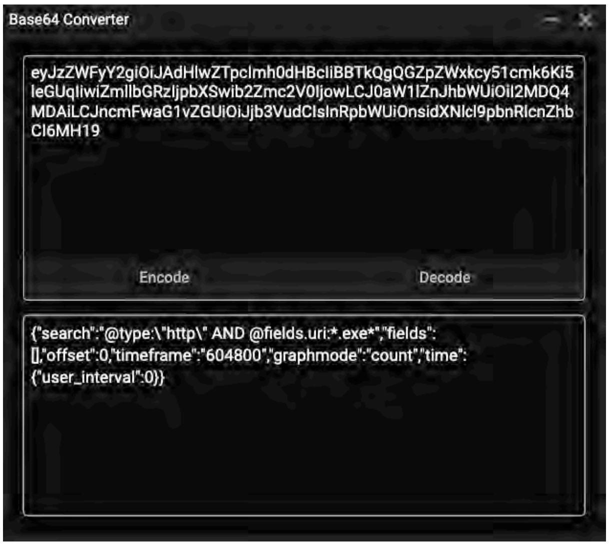
SGVsbG8gd29ybGQhIFRoaXMgaXMgYSB0ZXN0IG9mIHRoZSBEYXJrdHJhY2UgQmFzZTY0IENvbnZlcnRlci4=

Hello world! This is a test of the Darktrace Base64 Converter.

Application:

Advanced Search data can be queried and exported in JSON format. Every Advanced Search query is represented by a Base64 encoded string located in the URI. Paste the details following the # in the URI into the Base64 Converter and Decode to return the JSON response.

https://<servername>/advancedsearch/#eyJzZWFyY2giOiJAdHlwZTpclmh0dHBcliBBTkQgQGZpZWxkcy51cmk6Ki5leGUqliwiZmllbGRzljpbXSwib2Zmc2V0ljowLCJ0aW1lZnJhbWUiOil2MDQ4MDAiLCJncmFwaG1vZGUiOiJjb3VudClsInRpbWUiOnsidXNlcl9pbnRlcnZhbCI6MH19

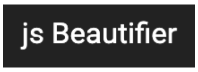


eyJzZWFyY2giOiJAdHlwZTpclmh0dHBcliBBTkQgQGZpZWxkcy51cmk6Ki5leGUqliwiZmllbGRzljpbXSwib2Zmc2V0ljowLCJ0aW1lZnJhbWUiOil2MDQ4MDAiLCJncmFwaG1vZGUiOiJjb3VudClsInRpbWUiOnsidXNlcl9pbnRlcnZhbCI6MH19

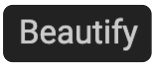
{"search":"@type:\"http\" AND @fields.uri:*.exe*","fields":[],"offset":0,"timeframe":"604800","graphmode":"count","time":{"user_interval":0}}

JS Beautifier

1. Navigate to the **JS Beautifier** via the main menu under Utilities.



2. Copy obfuscated JavaScript into the box and click **Beautify** to turn it into clean, well-formatted code. This can be particularly useful when investigating a compromised website which contains obfuscated JavaScript.



8. Learning Outcomes

Thank you for completing the Part 1 of the Cyber Analyst course. We hope this has given you the confidence to successfully utilize Advanced Search.

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

□	**I can use fundamental techniques to confidently navigate Advanced Search**
□	**I am able to determine how much data was transmitted over a number of connections**
□	**I know how to perform effective queries and interpret network traffic in Advanced Search**
□	**I can effectively investigate different categories of network breaches**
□	**I can successfully carry out advanced analytical processes utilizing Darktrace analytical tools**

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

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

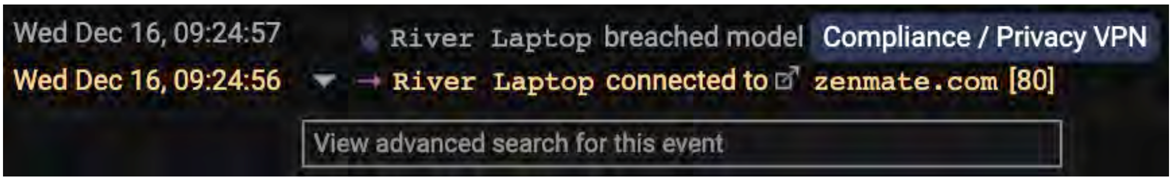
When contacting support, please make sure you provide as much detail as possible.

9. Cheat Sheet

Advanced Search Navigation Exercise

a. Practice pivoting from an event in the Threat Visualizer to its details in Advanced Search.

__Click the downwards facing arrow to the left of an event in the Threat Visualizer and select View Advanced Search for this event.__



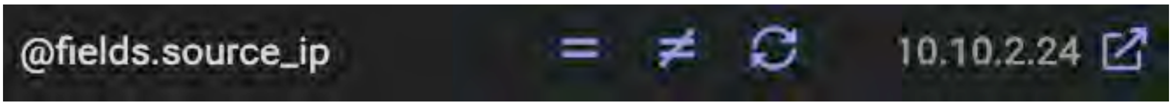
Wed Dec 16, 09:24:57 River Laptop breached model Compliance / Privacy VPN

Wed Dec 16, 09:24:56 → River Laptop connected to zenmate.com [80]

View advanced search for this event

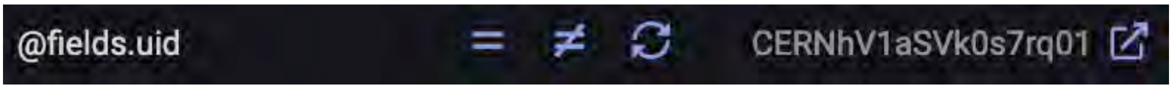
b. Practice pivoting from an Advanced Search log to its source device in the Threat Visualizer in two ways.

__First, locate the Source IP field in Advanced Search. Either copy/paste the IP address into the Omnisearch bar or click the icon to the right of the IP address to automatically populate the device in the Threat Visualizer.__



@fields.source_ip = ≠ 10.10.2.24

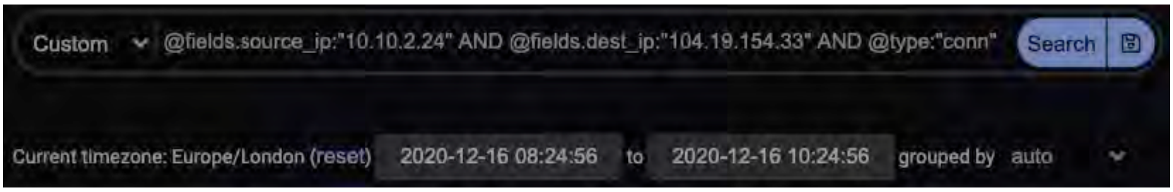
__Alternatively, locate the connection UID field. Again, either copy/paste or click the icon to populate the Omnisearch bar with the connection UID. From the Threat Visualizer, it is then possible to locate the source device.__



@fields.uid = ≠ CERNhV1aSVk0s7rq01

c. Use Advanced Search to determine the cumulative upload and download between two endpoints over a thirty-minute period.

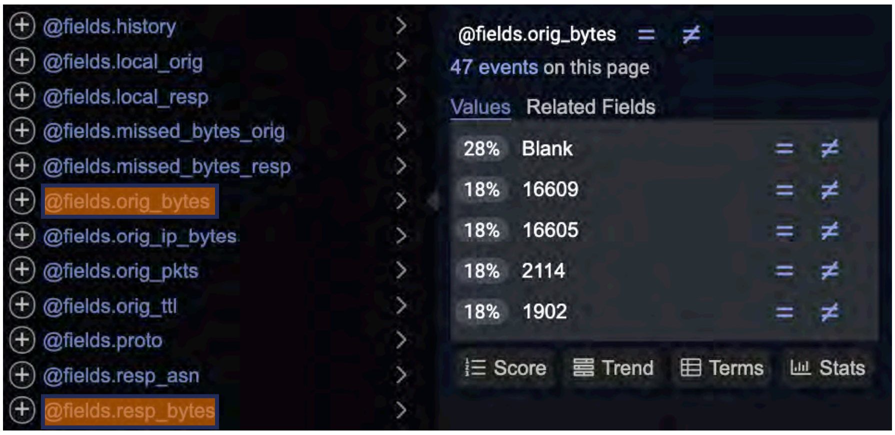
__Pivot on the conn field to append the source and destination with the connection type to the search bar. Optionally, narrow down the connectivity to a port or protocol. Set the time period to thirty minutes using the time frame above the graph.__



Custom @fields.source_ip:"10.10.2.24" AND @fields.dest_ip:"104.19.154.33" AND @type:"conn" Search

Current timezone: Europe/London (reset) 2020-12-16 08:24:56 to 2020-12-16 10:24:56 grouped by auto

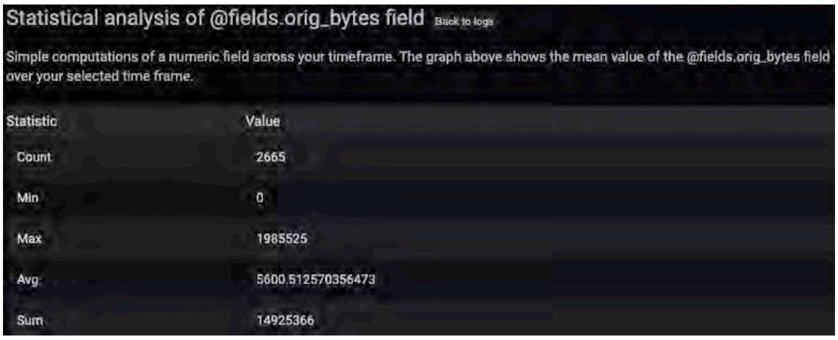
Inspect the orig_bytes and resp_bytes fields to view the uploads and downloads for the connection. For each field, select it to open the dialog and click Stats.



47 events on this page

28%	Blank	= ≠
18%	16609	= ≠
18%	16605	= ≠
18%	2114	= ≠
18%	1902	= ≠

This will provide a sum representing the cumulative upload or download in bytes for the query over the set time frame of half an hour.



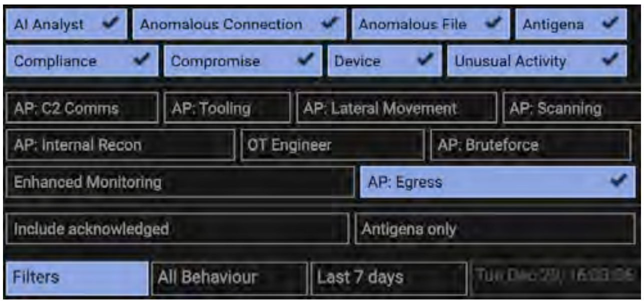
Statistical analysis of @fields.orig_bytes field

Simple computations of a numeric field across your timeframe. The graph above shows the mean value of the @fields.orig_bytes field over your selected time frame.

Statistic	Value
Count	2665
Min	0
Max	1985525
Avg	5600.512570356473
Sum	14925366

d. Determine the cumulative upload and download for a series of connections specified by a Model Breach.

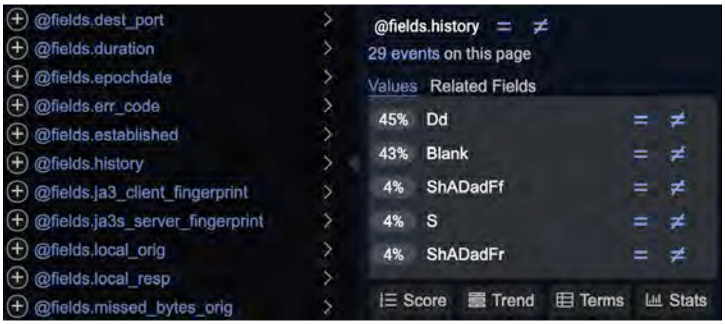
Select an appropriate Model, for example one with an AP: Egress tag, from the Threat Tray in the Threat Visualizer. Open the Model Breach Event Log and click View Advanced Search to filter beside the event data.



Once Advanced Search has opened, locate the conn event and click the equals sign next to the @type field – this limits the event information to the connections only. Follow the same process as outlined above to determine the cumulative uploads and downloads.

e. Use the score capability to view the history value for the last fifteen minutes of connectivity.

Set the frame is set to the Last 15m, as indicated to the left of the search bar. From the Columns list down the left of Advanced Search, locate @fields.history and click Score in the dialog. Review the results in the Quick Analysis table.



29 events on this page

45%	Dd	= ≠
43%	Blank	= ≠
4%	ShADadFf	= ≠
4%	S	= ≠
4%	ShADadFr	= ≠