Getting started with Cognito Recall

Overview

Cognito Recall™ from Vectra® enables incident responders to follow the chain of events from an initial threat signal – whether from Cognito Detect™, another security event or threat intelligence source – using enriched network metadata that is searchable by host name.

This document provides a quick overview of Cognito Recall, including its various capabilities to hunt and investigate using the metadata. The document also provides details about prebuilt dashboards and saved searches that provide an easy entry point to interact with the data. By default, Vectra provides three dashboards in Cognito Recall to get started using the product. These are:

- Host dashboard
- External Entity dashboard
- Network Visibility dashboard

Cognito Recall also includes saved searches that help with retrospective hunting and provides visibility into potential compliance violations. These dashboards and saved searches have been developed by the Vectra security research and professional services teams.

Host dashboard

Every detection and host in Cognito Detect has a link that allows security teams to further investigate the host in Cognito Recall by pivoting over to the Host Dashboard in Cognito Recall. The Host Dashboard provides a view of the host around the time of the latest detection events by providing details on all activity to and from the host. The link in Cognito Detect launches the host dashboard filtered on the host and the timestamp of the latest detection events. In other scenarios where the host gets flagged by another security tool, the analyst can navigate to the Host Dashboard (by clicking on Dashboard in the left navigation bar in the UI and selecting the Host Dashboard) and filter by the hostname or IP and time range to understand the behavior of the host. The dashboard provides the following about the host:

Connectivity information

Connections to external domains: All recorded connections made from the internal host to external domains. Some of the fields displayed are the domain (if applicable), destination IP, number of connections, bytes sent, and bytes received.

Internal connections: Lists all recorded connections made from hosts inside the network to other hosts inside the network.

Internal admin connections: Lists all administrative connections inside the network. The following ports/protocols are considered admin connections; ports: 22, 23, 623, 3389, 5938, 5900, 5901, 5985, 5986 and services: VNC, RDP, SSH, HTTP on port 16992, and TLS on Port 16993.

Account usage on host

Account usage on host is a critical piece of information when investigating a host. The host dashboard in Cognito Recall provides a comprehensive view by providing information about account usage on the host (to connect out) or usage of an account to connect to the host over two protocols – Kerberos and NTLM.

Internal Kerberos account usage: Lists the Kerberos account usage on the network including the number of attempts and authentication status (success/fail).

Internal NTLM account usage: Similar to Kerberos usage, this shows the accounts used to communicate to and from the host using the NT LAN Manager protocol. Fields shown include the number of authentication attempts along with the authentication status.

RPC calls

Internal RPC usage: Shows the remote procedure calls made to and from the host. Fields shown are the source host, the destination host, the account if available, the RPC endpoint, the function called and the total number of calls.

DNS data

DNS requests: Shows domain name resolution requests to and from the host. Fields shown are the DNS query made and the response along with the number of attempts.

HTTP data

HTTP destinations: Shows all HTTP destinations that the host connected to and the connection counts.

User-agent usage: Shows the different user-agents seen. Fields shown are the user-agent, the first seen timestamp, and the last seen timestamp, the total number of times that user-agent has been seen.

LDAP queries

LDAP connections: Shows LDAP usage by the host including the LDAP object that was requested, scope of the query, the query itself, and the result

External Entity dashboard

The External Entity dashboard can help you better understand the in-network devices you encounter during investigations, regardless of whether you start from Cognito Detect or third-party sources. It is recommended that this dashboard be used filtered by an external entity (and the relevant time range) to understand the connectivity to that external entity. It has four sections:

Connections from internal hosts: Lists all recorded connections made from hosts inside the network to destinations outside the network. Fields shown are the source hostname, source IP, domain name if applicable, the destination IP, the protocol, destination port, number of bytes sent to the destination, bytes received from the destination, the first seen connection time, the last seen connection time, and the number of connections that contacted an external entity – e.g. IP address, domain, user agent or URI.

Connections over time: Provides a visualization of the aggregate connection count over time.

Data transfer: Shows the aggregate amount of data sent to and from the internal host(s).

HTTP destination: Provides the HTTP requests. Fields shown are the source hostname, the source IP, the hostname request header labeled as domain, and the URI.

Network dashboard

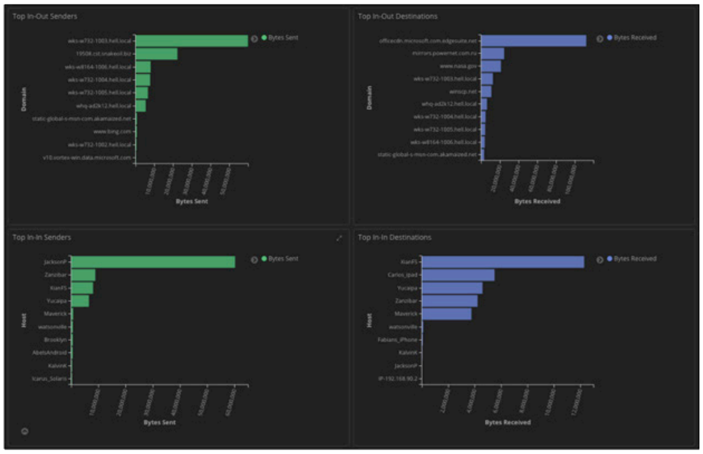
The Network dashboard shows network usage statistics. This provides visibility into various aspects of your network including:

Top in-out senders: Shows the top 10 internal hosts talking to external entities based upon the total number of bytes sent.

Top in-out destinations: Shows the top 10 external entities based upon the total number of bytes received (by internal hosts).

Top in-in senders: Shows the top 10 internal hosts talking to other internal hosts based upon the number of bytes sent.

Top in-in destinations: Shows the top 10 internal hosts talked to by other internal hosts based upon total number of bytes received.



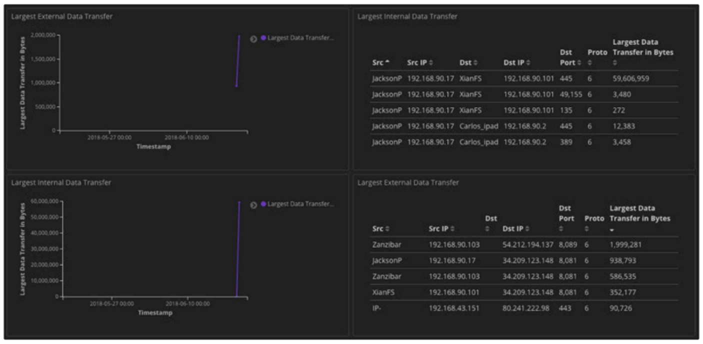
Top in-out senders, top in-out destinations, top in-in senders, and top in-in destinations

Largest external data transfer: Shows the largest amount of data leaving the network over the selected time range.

Largest internal data transfer: Shows the largest amount of data moving through the network. Fields shown are source hostname, source IP, destination hostname, destination IP, the destination port, the protocol, and the amount of data transferred in bytes.

Largest internal data transfer: Shows the largest amount of data moving through the network over the selected time range.

Largest external data transfer: Shows the largest amount of data leaving the network. Fields shown are source hostname, source IP, destination, destination IP, the destination port, the protocol, and the amount of data transferred in bytes.



Largest Internal Data Transfer

Src ▴	Src IP ⇕	Dst ⇕	Dst IP ⇕	Dst Port ⇕	Proto ⇕	Largest Data Transfer in Bytes ⇕
JacksonP	192.168.90.17	XianFS	192.168.90.101	445	6	59,606,959
JacksonP	192.168.90.17	XianFS	192.168.90.101	49,155	6	3,480
JacksonP	192.168.90.17	XianFS	192.168.90.101	135	6	272
JacksonP	192.168.90.17	Carlos_ipad	192.168.90.2	445	6	12,383
JacksonP	192.168.90.17	Carlos_ipad	192.168.90.2	389	6	3,458

Largest External Data Transfer

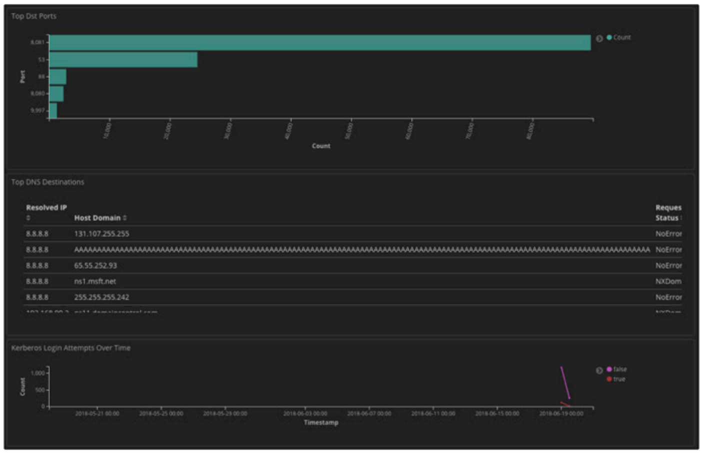
Src ⇕	Src IP ⇕	Dst ⇕	Dst IP ⇕	Dst Port ⇕	Proto ⇕	Largest Data Transfer in Bytes ▾
Zanzibar	192.168.90.103		54.212.194.137	8,089	6	1,999,281
JacksonP	192.168.90.17		34.209.123.148	8,081	6	938,793
Zanzibar	192.168.90.103		34.209.123.148	8,081	6	586,535
XianFS	192.168.90.101		34.209.123.148	8,081	6	352,177
IP-	192.168.43.151		80.241.222.98	443	6	90,726

Largest external data transfer and largest internal data transfer

Top destination ports: Shows the top five destination ports for network traffic.

Top DNS destinations: Shows the top 10 domain name requests. Fields shown are the resolved IP, the host name, the request status. Not shown in the photo but accessible by scrolling to the right is the count of requests made.

Kerberos login attempts over time: Shows the number of login attempts via Kerberos over time, with successes and failures shown separately.



Top DNS Destinations

Resolved IP	Host Domain	Reques Status
8.8.8.8	131.107.255.255	NoError
8.8.8.8	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	NoError
8.8.8.8	65.55.252.93	NoError
8.8.8.8	ns1.msft.net	NXDom
8.8.8.8	255.255.255.242	NoError

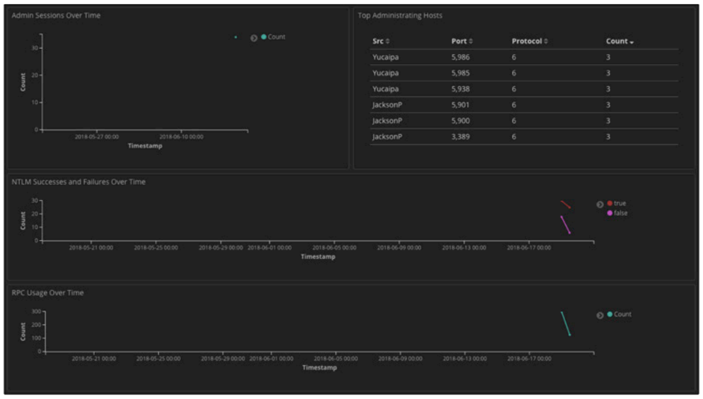
Top destination ports and top DNS destinations

Admin sessions over time: Shows the total number of admin connections over the selected time range. The following ports/protocols are considered admin connections; ports: 22, 23, 623, 3389, 5938, 5900, 5901, 5985, 5986 and services: VNC, RDP, SSH, HTTP on port 16992, and TLS on port 16993.

Top administrating hosts: Shows the top 10 hosts seen conducting administrative traffic. Fields shown are the source hostname, the port used, the protocol, and the count of connections. The following ports/protocols are considered admin connections; ports: 22, 23, 623, 3389, 5938, 5900, 5901, 5985, 5986 and services: VNC, RDP, SSH, HTTP on port 16992, and TLS on port 16993.

NTLM successes and failures over time: Shows both NTLM successes and failures over the selected time range.

RPC usage over time: Shows the total number of remote procedure calls over the selected time range.



Top Administrating Hosts

Src	Port	Protocol	Count
Yucaipa	5,986	6	3
Yucaipa	5,985	6	3
Yucaipa	5,938	6	3
JacksonP	5,901	6	3
JacksonP	5,900	6	3
JacksonP	3,389	6	3

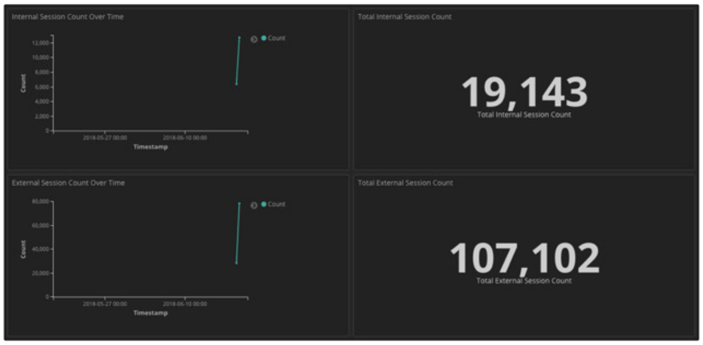
Admin sessions over time, NTLM successes and failures over time, and RPC usage over time

Internal session count over time: Shows the total number of internal to internal session counts over the selected time range.

Total internal session count: Shows the total number of internal to internal sessions counts during the search query time.

External session count over time: Shows the total number of internal to external session counts over the selected time range.

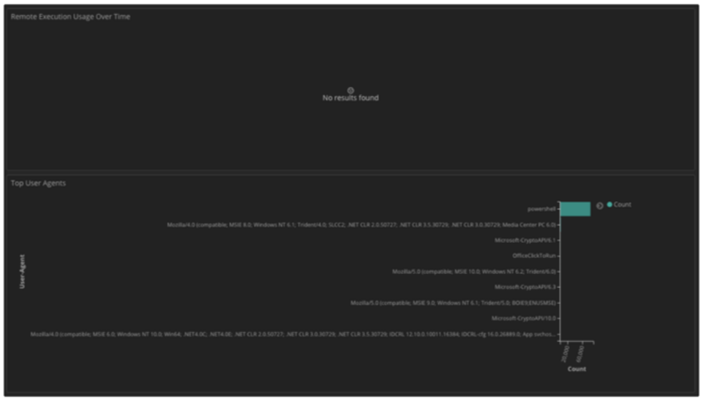
Total external sessions count: Shows the total number of internal to external sessions counts during the search query time.


Internal Session Count Over Time
12,000
10,000
8,000
6,000
4,000
2,000
0
Count
2018-05-27 00:00
2018-06-10 00:00
Timestamp
Count
Total Internal Session Count
19,143
Total Internal Session Count
External Session Count Over Time
80,000
60,000
40,000
20,000
0
Count
2018-05-27 00:00
2018-06-10 00:00
Timestamp
Count
Total External Session Count
107,102
Total External Session Count

Internal session count over time, total internal session count, external session count over time, and total external session count

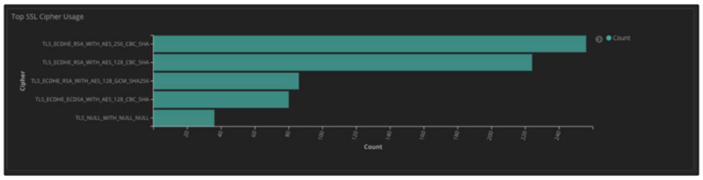
Remote execution usage over time: Shows the total number of remote execution calls over the selected time range. This image shows “No results found” because there was no remote execution during the time queried.

Top user-agents: Shows the top 10 user-agents and gives the total number of times they were seen.



Top user agents

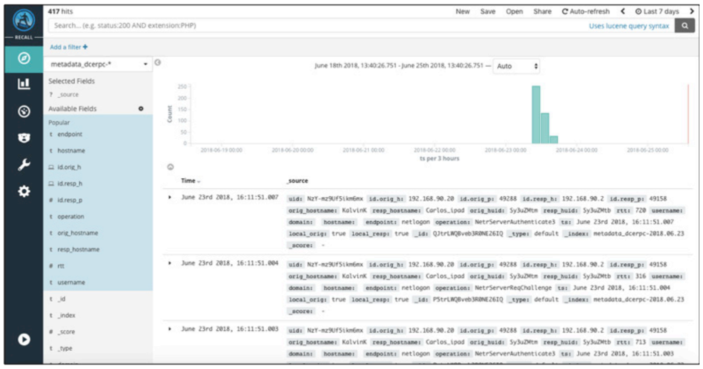
Top SSL cipher usage: Shows the top five SSL cipher suites observed.



Top SSL cipher usage

Discover

The Discover page in Cognito Recall lets analysts search all of the metadata stored in the system for incident investigation and threat hunting. The metadata itself is forwarded from the Cognito Detect platform and normalized into the Bro format. Analysts can perform searches on any attribute of any metadata stream, combine queries to form complex queries, view results, and pivot further to perform deep investigation using the metadata.



```
June 23rd 2018, 16:11:51.007  uid: NzY-mz9UfSikm6mx id.orig_h: 192.168.90.20 id.orig_p: 49288 id.resp_h: 192.168.90.2 id.resp_p: 49158
                              orig_hostname: KalvinK resp_hostname: Carlos_ipad orig_huid: Sy3uZMtm resp_huid: Sy3uZMtb rtt: 720 username:
                              domain: hostname: endpoint: netlogon operation: NetrServerAuthenticate3 ts: June 23rd 2018, 16:11:51.007
                              local_orig: true local_resp: true _id: QJtrLWQBveb3R0NE26IQ _type: default _index: metadata_dcerpc-2018.06.23
                              _score: -
June 23rd 2018, 16:11:51.004  uid: NzY-mz9UfSikm6mx id.orig_h: 192.168.90.20 id.orig_p: 49288 id.resp_h: 192.168.90.2 id.resp_p: 49158
                              orig_hostname: KalvinK resp_hostname: Carlos_ipad orig_huid: Sy3uZMtm resp_huid: Sy3uZMtb rtt: 316 username:
                              domain: hostname: endpoint: netlogon operation: NetrServerReqChallenge ts: June 23rd 2018, 16:11:51.004
                              local_orig: true local_resp: true _id: P5trLWQBveb3R0NE26IQ _type: default _index: metadata_dcerpc-2018.06.23
                              _score: -
June 23rd 2018, 16:11:51.003  uid: NzY-mz9UfSikm6mx id.orig_h: 192.168.90.20 id.orig_p: 49288 id.resp_h: 192.168.90.2 id.resp_p: 49158
                              orig_hostname: KalvinK resp_hostname: Carlos_ipad orig_huid: Sy3uZMtm resp_huid: Sy3uZMtb rtt: 713 username:
                              domain: hostname: endpoint: netlogon operation: NetrServerAuthenticate3 ts: June 23rd 2018, 16:11:51.003
```

Search on any attribute of any metadata stream

The metadata in Cognito Recall is divided among several streams. The stream to be used for the query should be selected via a dropdown menu. These streams are:

- DCERPC
- DHCP
- DNS
- HTTP
- iSession
- Kerberos
- LDAP
- NTML
- RDP
- SMB Files
- SMB Mapping
- SSL
- X509

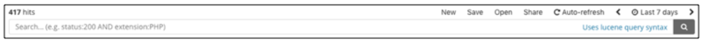
Each stream has its own collection of metadata key-value pairs. The detailed description of all attributes in every metadata stream can be found in the Cognito Recall metadata attributes document on the Vectra support portal here.

iSession provides high-level flow information, and so will be the starting point for many queries before digging deeper in a protocol-specific stream.

Discover features

When conducting investigations, it is pertinent to be able to focus only on the data of interest. There are multiple ways to do this, each with their own strengths.

Search

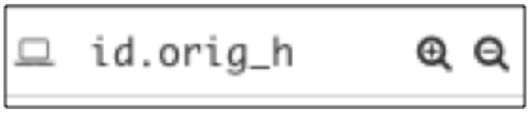


Search is the initial way to narrow down the data on the page to the entities of interest. Analysts can perform free-form search or qualified (key-value pair) search for a more targeted search.

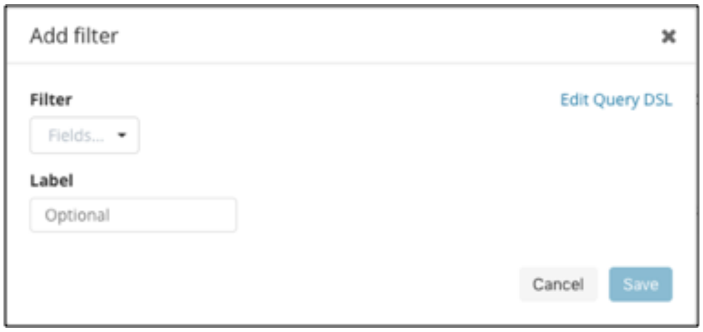
Filter

Filters apply to the search as opposed to querying all of the stored metadata. They can be applied and unapplied quickly. There are two ways to apply a filter.

The fastest and easiest way is to use the two little magnifying glasses listed next to each key. The one with the plus sign will apply that value as a filter. The magnifying glass with the minus sign will add the NOT condition and will show all values but the selected value.



The second approach is to click on the “Add a filter +” button below the search bar. A pop-up will appear that allows for creation of the filter.



Add filter ✖

Filter

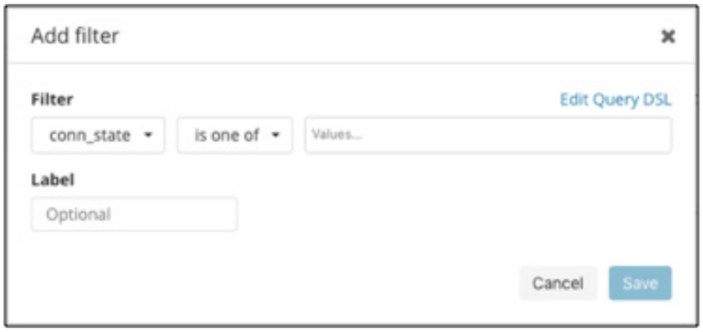
Edit Query DSL

Fields... ▾

Label

Optional

Cancel Save



Add filter ✖

Filter

Edit Query DSL

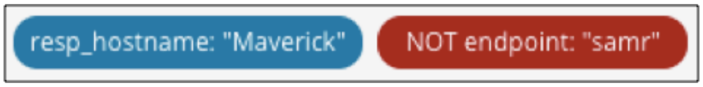
conn_state ▾ | is one of ▾ | Values...

Label

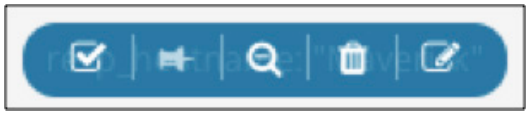
Optional

Cancel Save

Click on “Save” to apply to filter.



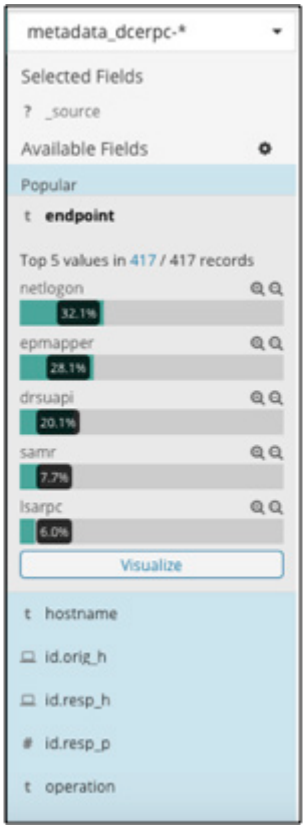
Once the filter is created, it will display as a blue pill (red if using the NOT operator). Highlighting over the pill will provide several options.



From left to right, the following options are available:

- Checkbox: toggle the filter on/off
- Push pin: “Pin” the filter so that it will persist across navigation to different parts of Cognito Recall (Dashboard or Discover)
- Magnifying glass: Invert the filter state
- Trash can: Delete the filter
- Paper and pencil icon: Edit the filter

The keys for that metadata stream are also readily available as part of the sidebar. Clicking on the keys in the sidebar presents the top five values for that key. Clicking on the magnifying glasses adds the key-value pair as a filter.



metadata_dcerpc-* ▾

Selected Fields

? _source

Available Fields

Popular

t **endpoint**

Top 5 values in 417 / 417 records

netlogon 32.1%

epmapper 28.1%

drsuapi 20.1%

samr 7.7%

lsarpc 6.0%

Visualize

t hostname

id.orig_h

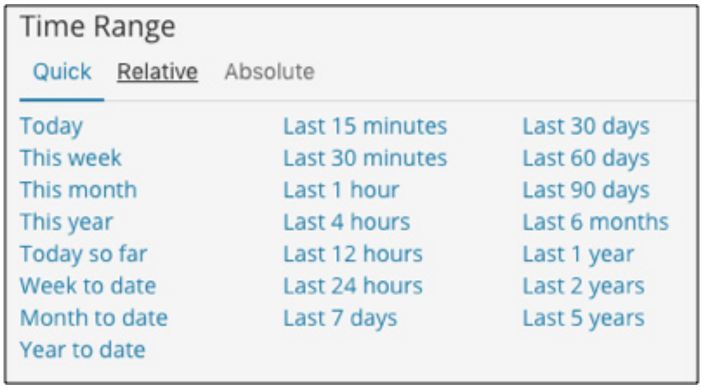
id.resp_h

id.resp_p

t operation

Time range

Cognito Recall provides flexibility for specifying the time range. The time range can be modified by clicking on the top right of the dashboard, above the search bar. The "Quick" time range is the easiest and most convenient to use. It provides a common set of time ranges based upon the current time.



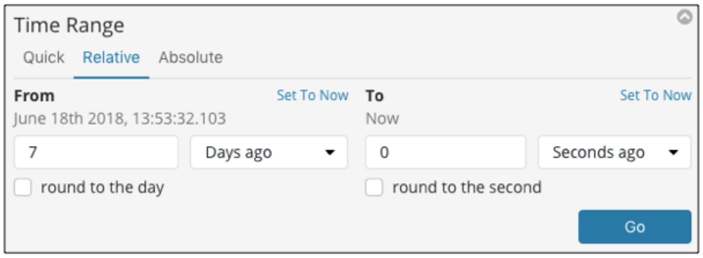
Time Range

Today
This week
This month
This year
Today so far
Week to date
Month to date
Year to date

Last 15 minutes
Last 30 minutes
Last 1 hour
Last 4 hours
Last 12 hours
Last 24 hours
Last 7 days

Last 30 days
Last 60 days
Last 90 days
Last 6 months
Last 1 year
Last 2 years
Last 5 years

The "Relative" time range allows specifying the start and end times based upon the current time.

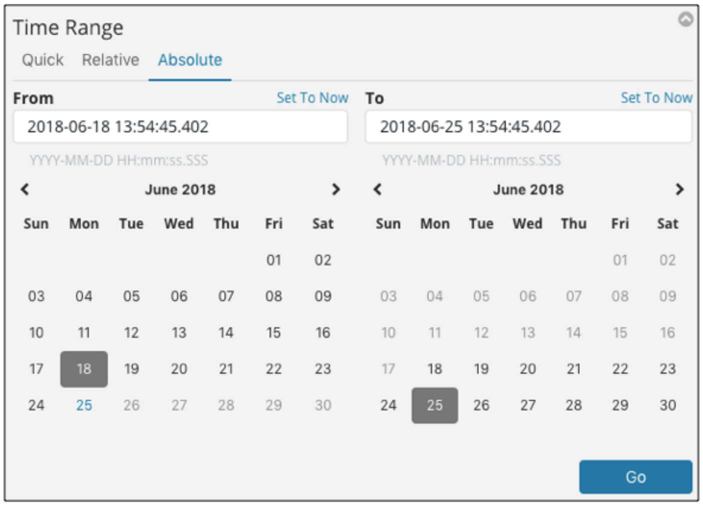


Time Range

From
June 18th 2018, 13:53:32.103
7 | Days ago
□ round to the day

To
Now
0 | Seconds ago
□ round to the second

The "Absolute" time range allows specification of a date and time for both the start and end time.



Time Range

From
2018-06-18 13:54:45.402

June 2018

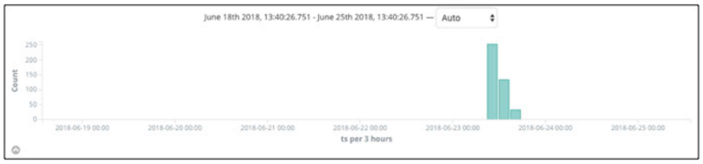
Sun	Mon	Tue	Wed	Thu	Fri	Sat
					01	02
03	04	05	06	07	08	09
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

To
2018-06-25 13:54:45.402

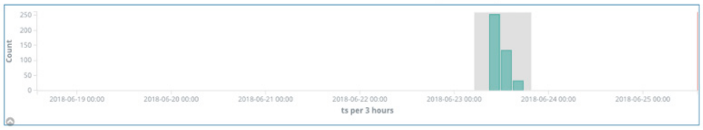
June 2018

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					01	02
03	04	05	06	07	08	09
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

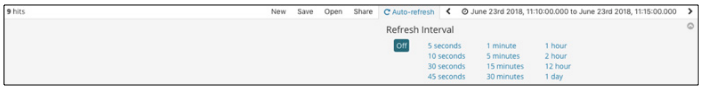
When the results are returned, a bar graph displays the number of results over time. The unit of time can be specified by clicking the dropdown.



The time range of the search results can be modified by interacting with the graph and highlighting the time range of interest.



The page can be configured to autorefresh by selecting a refresh interval from the link at the top of the page.

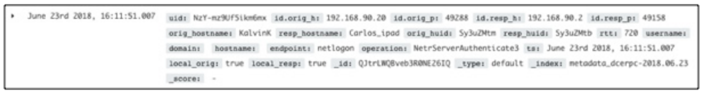


9 hits
New
Save
Open
Share
Auto-refresh
June 23rd 2018, 11:10:00.000 to June 23rd 2018, 11:15:00.000

Refresh Interval

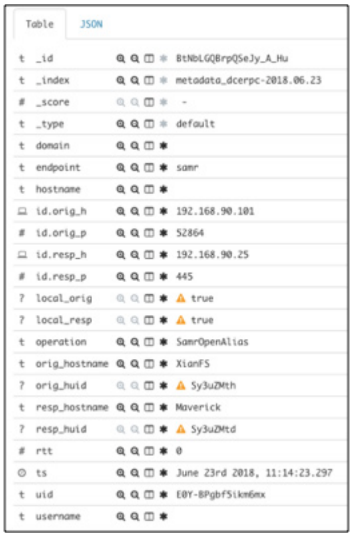
Viewing metadata records

By default, the search results provide the metadata associated with the search and filter parameters.

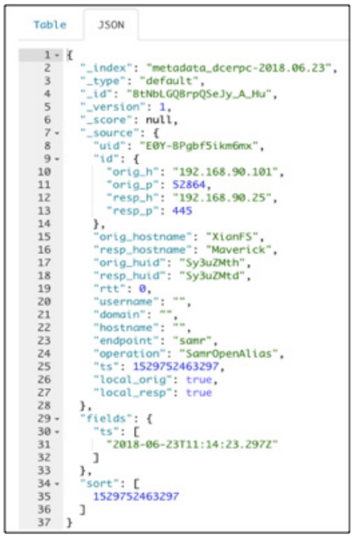


```
▸ June 23rd 2018, 16:11:51.007   uid: NzY-mz9UfSikm6mx id.orig_h: 192.168.90.20 id.orig_p: 49288 id.resp_h: 192.168.90.2 id.resp_p: 49158
                                 orig_hostname: KalvinK resp_hostname: Carlos_ipad orig_huid: Sy3uZMtm resp_huid: Sy3uZMtb rtt: 720 username:
                                 domain:  hostname:  endpoint: netlogon operation: NetrServerAuthenticate3 ts: June 23rd 2018, 16:11:51.007
                                 local_orig: true local_resp: true _id: QJtrLWQ8veb3R0NE26IQ _type: default _index: metadata_dcerpc-2018.06.23
                                 _score: -
```

The results can be expanded to see the key-value pairs in a table or in JSON format.

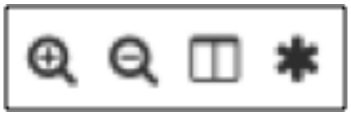


t	_id	BtNbLGQBrpQSeJy_A_Hu
t	_index	metadata_dcerpc-2018.06.23
#	_score	-
t	_type	default
t	domain	
t	endpoint	samr
t	hostname	
🖳	id.orig_h	192.168.90.101
#	id.orig_p	52864
🖳	id.resp_h	192.168.90.25
#	id.resp_p	445
?	local_orig	⚠ true
?	local_resp	⚠ true
t	operation	SamrOpenAlias
t	orig_hostname	XianFS
?	orig_huid	⚠ Sy3uZMth
t	resp_hostname	Maverick
?	resp_huid	⚠ Sy3uZMtd
#	rtt	0
⏲	ts	June 23rd 2018, 11:14:23.297
t	uid	E0Y-BPgbf5ikm6mx
t	username	



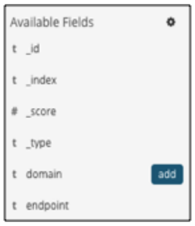
```
{
  "_index": "metadata_dcerpc-2018.06.23",
  "_type": "default",
  "_id": "BtNbLGQBrpQSeJy_A_Hu",
  "_version": 1,
  "_score": null,
  "_source": {
    "uid": "E0Y-BPgbf5ikm6mx",
    "id": {
      "orig_h": "192.168.90.101",
      "orig_p": 52864,
      "resp_h": "192.168.90.25",
      "resp_p": 445
    },
    "orig_hostname": "XianFS",
    "resp_hostname": "Maverick",
    "orig_huid": "Sy3uZMth",
    "resp_huid": "Sy3uZMtd",
    "rtt": 0,
    "username": "",
    "domain": "",
    "hostname": "",
    "endpoint": "samr",
    "operation": "SamrOpenAlias",
    "ts": 1529752463297,
    "local_orig": true,
    "local_resp": true
  },
  "fields": {
    "ts": [
      "2018-06-23T11:14:23.297Z"
    ]
  },
  "sort": [
    1529752463297
  ]
}
```

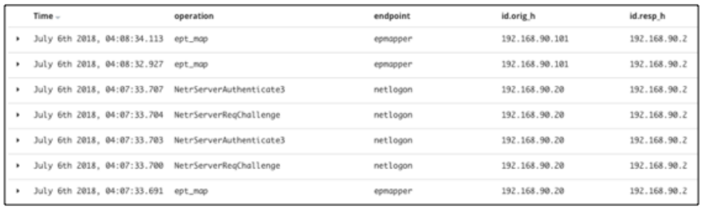
Each metadata attribute has four icons next to it. The magnifying glasses to add a value to a filter, the table icon that toggles the key as a column in the table, and an asterisk to add a "field present" filter that requires the field to exist in the result.



Building tables

Columns can be added to the table by clicking on the "add" button that appears on hovering over a key name on the sidebar. Cognito Recall will also provide the common fields selected for the stream. The columns can be rearranged by clicking the arrows or removed by clicking the "x."





	Time	operation	endpoint	id.orig_h	id.resp_h
▸	July 6th 2018, 04:08:34.113	ept_map	epmapper	192.168.90.101	192.168.90.2
▸	July 6th 2018, 04:08:32.927	ept_map	epmapper	192.168.90.101	192.168.90.2
▸	July 6th 2018, 04:07:33.707	NetrServerAuthenticate3	netlogon	192.168.90.20	192.168.90.2
▸	July 6th 2018, 04:07:33.704	NetrServerReqChallenge	netlogon	192.168.90.20	192.168.90.2
▸	July 6th 2018, 04:07:33.703	NetrServerAuthenticate3	netlogon	192.168.90.20	192.168.90.2
▸	July 6th 2018, 04:07:33.700	NetrServerReqChallenge	netlogon	192.168.90.20	192.168.90.2
▸	July 6th 2018, 04:07:33.691	ept_map	epmapper	192.168.90.20	192.168.90.2

Saving and sharing searches

The Discover page allows for saving, sharing and opening searches using menu options on the top right of the page. "New" will clear the search and filter conditions and create a new search. "Save" can be used to name the search and save it for future usage. "Open" allows opening of one of the saved searches. "Share" provides a link that allows for sharing either a saved search or a snapshot of the current search. The next section describes some default saved searches available in the product.

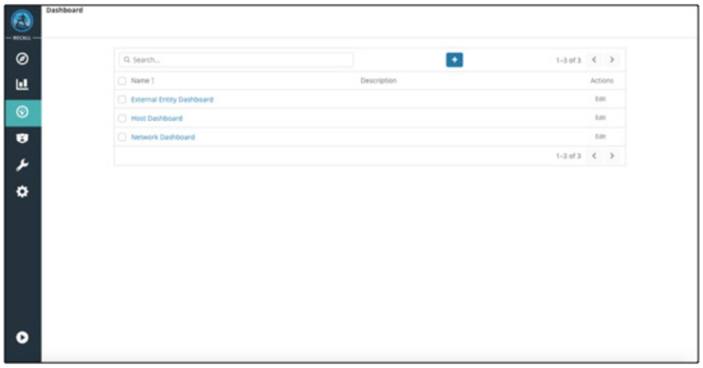
Vectra-provided saved searches

Cognito Recall includes a list of searches curated by Vectra security research to look for compliance violations, such as weak crypto ciphers, potentially harmful file downloads, and the use of unencrypted FTP and telnet. Further, saved searches are also curated for known IoCs, ranging from ransomware worms to advanced attackers and more. The following table contains a selected list of saved searches along with their descriptions. Any of these searches can be executed and the results analyzed for retrospective hunting of attacker TTPs or checking compliance posture.

Saved Search	Description
Cognito - Compliance - HTTP - Older Versions of Mozilla	Finds HTTP sessions with user-agents that advertises older versions of Mozilla.
Cognito - Compliance - HTTP - Potential Unencrypted Web Administration	Finds all web sessions for administration activity that is over clear text. To improve security posture and minimize attack surface, administration should be secured especially if they are critical servers.
Cognito - Compliance - isession - Time Wasting Sites	Finds all hosts consuming media content such as Netflix, Gaming, YouTube or Twitch over excessive periods of time. This can be classified as fraud, waste and abuse and can have a negative impact on the network infrastructure and/or productivity.
Cognito - Compliance - isession - Unencrypted FTP and Telnet	Finds all instances where clear FTP or Telnet is being used. This greatly increases the risk of exposing credentials in the clear.
Cognito - Compliance - RDP - Unencrypted RDP	Finds all hosts using RDP but are not using an encrypted keyboard. Clear keyboards expand the attack surface inside the organization.
Cognito - Compliance - SSL - Weak Server Cipher Usage	Finds all SSL/TLS sessions where my servers are using weak ciphers. It is important to check the SSL configuration being used to avoid putting in place cryptographic support which could be easily defeated.
Cognito - Compliance - SSL - Weak Client Cipher Usage	Finds all SSL/TLS sessions where the client is using weak ciphers. It is important to check the SSL configuration being used to avoid putting in place cryptographic support which could be easily defeated.
Cognito - PUP - HTTP - Potentially Harmful File Download	Finds all file downloads of risky file types (ex. .msi, .swf, .exe). Better understand your risk by file download activity.
Cognito - TTP - DNS - Bad Rabbit Domains	Finds all queries for known domains associated with Bad Rabbit – https://securelist.com/bad-rabbit-ransomware/82851/
Cognito - TTP - DNS - Parked Domains	Finds all queries for domains resolving to localhost or are not owned by Google but resolve to Google. It is not uncommon for attackers to park domain when they are not actively using it.
Cognito - TTP - DNS - Wannacry Ransomware Domain	Finds all queries for known domains associated with the Wannacry ransomware – https://www.secureworks.com/research/wcry-ransomware-analysis and https://community.spiceworks.com/topic/1994631-known-wannacry-file-extensions-start-blocking
Cognito - TTP - HTTP - Hancitor Infection with Azorult and Zeus Panda Banker Known Domains	Finds all HTTP sessions involving known domains of Hancitor's Azorult and Zeus Panda attacks – http://malware-traffic-analysis.net/2018/07/19/index2.html
Cognito - TTP - HTTP - Hidden Cobra Campaign Delta Charlie Attack Known IPs	Finds all HTTP sessions involving known domains of Hidden Cobra's Delta Charlie attack – https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity
Cognito - TTP - HTTP - Hidden Cobra Campaign TYPEFRAME Known IPs	Finds all HTTP sessions involving known domains of Hidden Cobra's TYPEFRAME attack – https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity
Cognito - TTP - HTTP - Kovter Trojan Known URI Elements	Finds all HTTP sessions involving known domains of Kovter trojan – https://www.malware-traffic-analysis.net/2017/04/19/index.html
Cognito - TTP - HTTP - Xorist Ransomware Known Domain	Finds all HTTP sessions involving known domains of the Xorist ransomware – https://www.malware-traffic-analysis.net/2018/05/08/index2.html
Cognito - TTP - SMB Files - Bad Rabbit Known Usernames	Finds all SMB fileshare transactions using usernames known to be used with Bad Rabbit – https://securelist.com/bad-rabbit-ransomware/82851/
Cognito - TTP - SMB Files - GANDCRAB Known Ransom Extensions	Finds all SMB transactions involving known GRANDCRAB file extensions – http://malware-traffic-analysis.net/2018/04/10/index.html
Cognito - TTP - SMB Files - GANDCRAB Known Ransom Note	Finds all SMB transactions involving the known GRANDCRAB ransom note – http://malware-traffic-analysis.net/2018/04/10/index.html
Cognito - TTP - SMB Files - Wannacry Known Ransom Extensions	Finds all SMB transactions involving the known Wannacry file extensions – https://www.secureworks.com/research/wcry-ransomware-analysis and https://community.spiceworks.com/topic/1994631-known-wannacry-file-extensions-start-blocking
Cognito - TTP - SMB Files - Wannacry Known Ransom Note	Finds all SMB transactions involving the known Wannacry ransom note – https://www.secureworks.com/research/wcry-ransomware-analysis and https://community.spiceworks.com/topic/1994631-known-wannacry-file-extensions-start-blocking
Cognito - TTP - SMB Files - Xorist Known Ransom Note	Finds all SMB transations involving the known Xorist ransom note – https://www.malware-traffic-analysis.net/2018/05/08/index2.html

Dashboards

Analysts can create their own custom dashboards in Cognito Recall if they so desire. Dashboards in Cognito Recall are a collection of searches and visualizations on a single page. These searches may be displayed in table format, with the data laid out in rows and columns or it may be displayed in a number of visualizations.

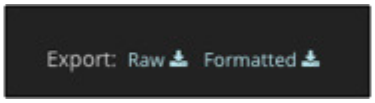


□ Name ↑	Description	Actions
□ External Entity Dashboard		Edit
□ Host Dashboard		Edit
□ Network Dashboard		Edit

Dashboard features

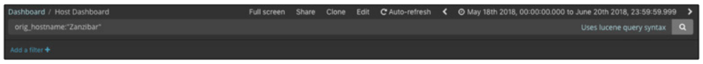
Export

The bottom of the table provides two buttons that allows for export of the data in the visualization in two different formats. The export functionality is extremely useful when the results have to be downloaded and shared amongst team members or with other teams.



Search

Just like the discover page, search can be utilized to narrow down the data on the dashboard to the specific criteria of the search. The link to pivot into Cognito Recall from a host or detection in Cognito Detect automatically filters the dashboard by the hostname and time window based on the latest timestamp of the detection.



Dashboard / Host Dashboard
Full screen
Share
Clone
Edit
Auto-refresh
‹
May 18th 2018, 00:00:00.000 to June 20th 2018, 23:59:59.999
›
Uses lucene query syntax
Add a filter +

orig_hostname:"Zanzibar"

Filter

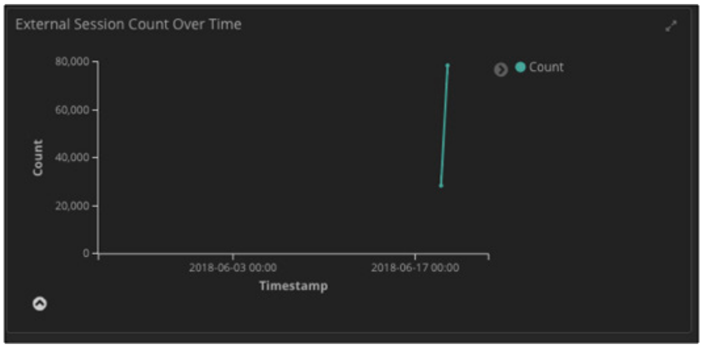
Filter operation on the dashboard is similar to the Discover section described above. Filters apply to search as opposed to querying all the stored metadata. They can be applied and unapplied quickly.

Time range

The time range for the query can be modified by clicking on the top right of the dashboard, above the search bar. This is similar to the time range selection on the Discover page.

Visualization to table

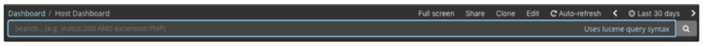
The arrow at the bottom left of the visualization converts the data into a data table format, useful for exporting results for use in reports.



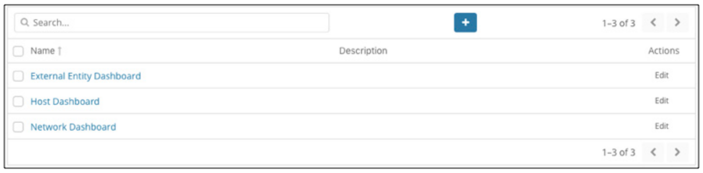
Creating custom dashboards

There are multiple ways in which analysts can create custom dashboards:

1) Start from an existing dashboard and make a copy using the "Clone" option.

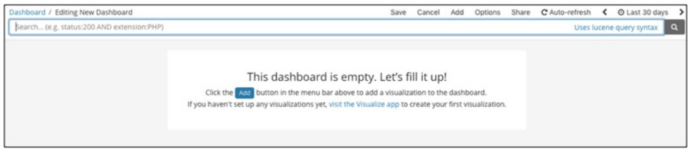


2) Create a new dashboard by clicking on the blue plus button on the main dashboard page.



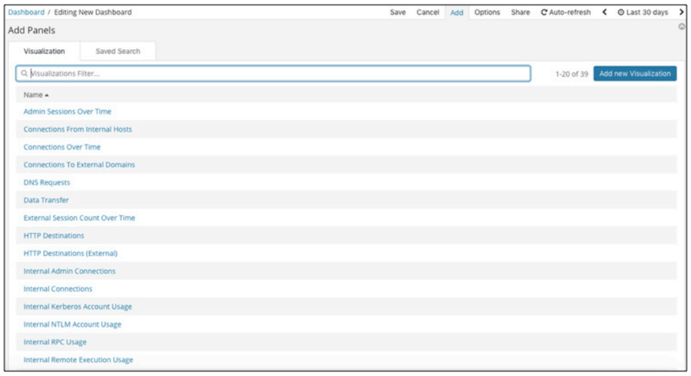
□ Name ↑	Description	Actions
□ External Entity Dashboard		Edit
□ Host Dashboard		Edit
□ Network Dashboard		Edit

Creating a new dashboard results in a blank canvas. To save a dashboard, click the save link above the search bar. To add items to the dashboard, click on the blue “Add” button or the “Add” link above the search bar.


Dashboard / Editing New Dashboard
Save
Cancel
Add
Options
Share
Auto-refresh
Last 30 days
Search... (e.g. status:200 AND extension:PHP)
Uses lucene query syntax

This dashboard is empty. Let’s fill it up!

Click the Add button in the menu bar above to add a visualization to the dashboard.
If you haven't set up any visualizations yet, visit the Visualize app to create your first visualization.



Name ▲
Admin Sessions Over Time
Connections From Internal Hosts
Connections Over Time
Connections To External Domains
DNS Requests
Data Transfer
External Session Count Over Time
HTTP Destinations
HTTP Destinations (External)
Internal Admin Connections
Internal Connections
Internal Kerberos Account Usage
Internal NTLM Account Usage
Internal RPC Usage
Internal Remote Execution Usage

Upon creation, a list of saved visualizations and searches are presented that can be added to the dashboard by simply clicking on the links. New visualizations can also be created by clicking on the blue “Add new Visualization” button.

VECTRA®
Security that thinks.®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai