



---

## DarkOwl Vision User Interface Guide

Contents

Getting Started ..... 3

Searching ..... 5

Search Tools ..... 19

Search Results (Research) ..... 24

Explore: Actor ..... 34

Explore: Entity ..... 38

Explore: Leak ..... 41

Track: Your Alerts ..... 43

Track: Your DARKINT Exposure Scores ..... 45

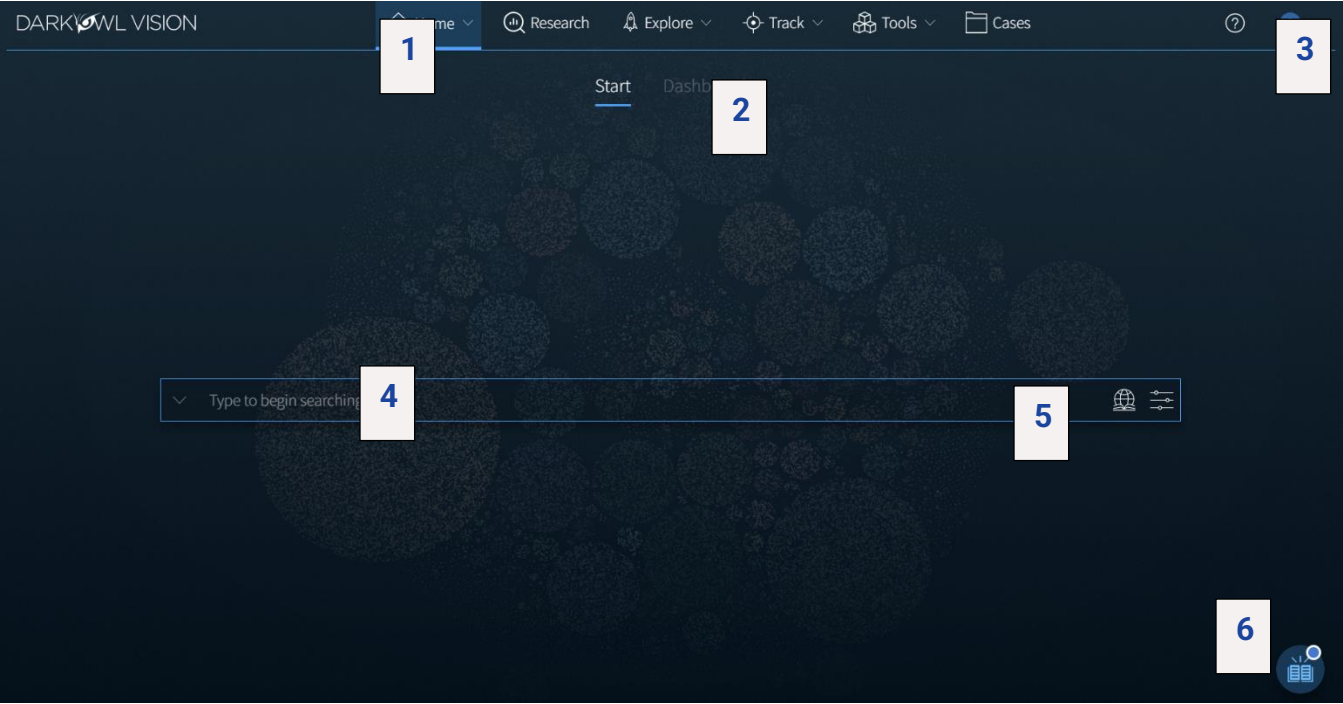
Tools: Saved Searches ..... 48

Tools: Search Blocks ..... 49




Cases..... 51

## Getting Started

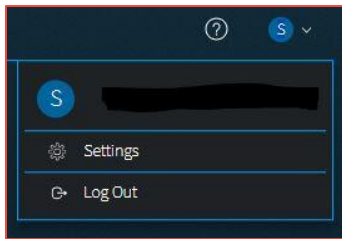
DarkOwl Vision's user-friendly User Interface has tools that enable analysts to effectively search, monitor, and receive alerts when leaked data appears on the darknet.



1. <b>Navigation Menu</b> (see below)	Navigate to <b>Research</b> to view search results; <b>Track</b> Alerts & DARKINT Exposure; <b>Explore</b> actors, entities, and leaks; manage Saved Searches and Search Blocks <b>Tools</b> ; set up <b>Cases</b> .
2. <b>Section Navigation</b>	Toggle between individual pages within a section.
3. <b>Help &amp; Account Options</b>	Link to Help resources; manage Settings (Profile, Preferences) and see Activity; or logout.
4. <b>Search Bar</b>	Type to begin searching or click on the arrow to open the Search Tools menu.
5. <b>Filters Menu</b>	Create a targeted and effective search using filters, dates, and advanced options.
6. <b>Vision UI Assistant</b>	Access onboarding and feature walkthrough guides, as well as important announcements and updates.

 Home ▾	 Research	 Explore ▾	 Track ▾	 Tools ▾	 Cases
<b>Start / Dashboard</b> pages	<b>Research</b> (search results) page	<b>Actor / Entity</b> / <b>Leak</b> pages	<b>Alerts / Exposure</b> pages	<b>Saved Searches / Search Blocks</b> pages	<b>Cases</b> page

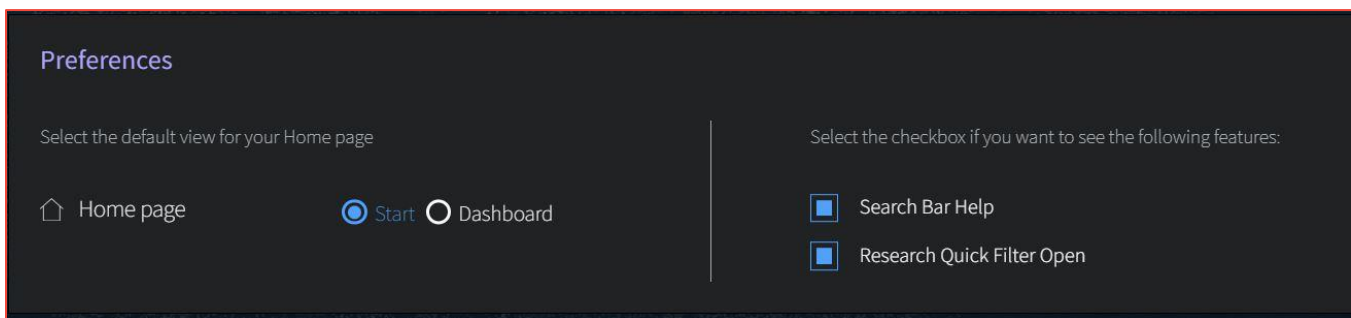
## User Settings (Profile and Activity)



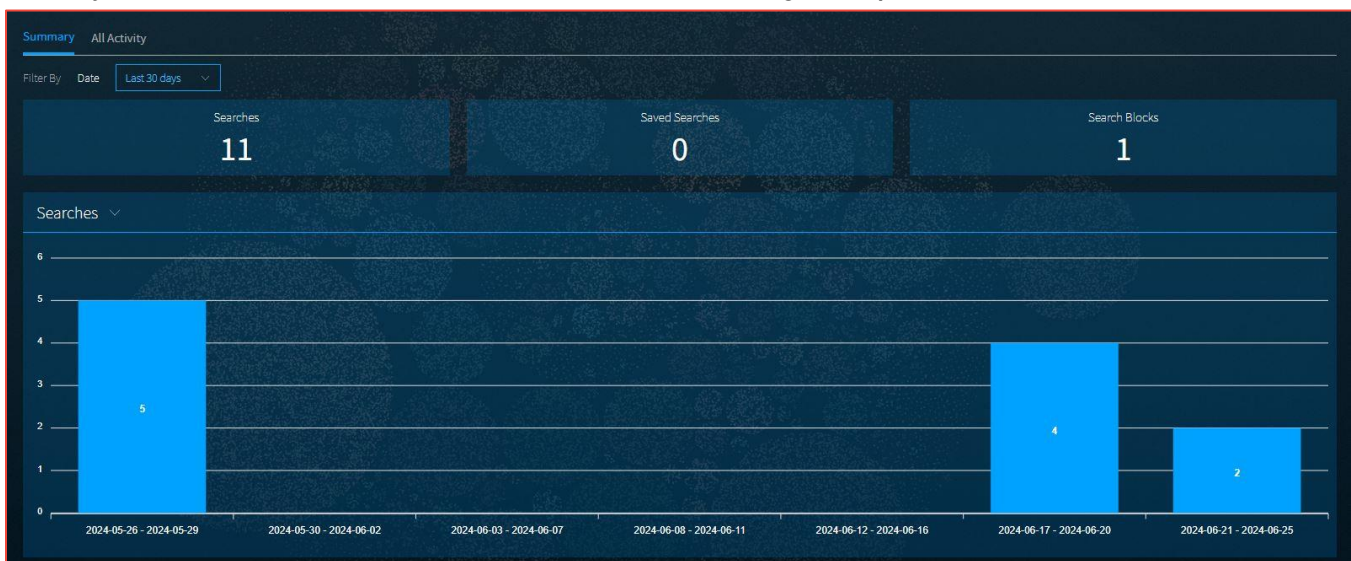
Click on the **User** icon in the upper right corner to access your Settings, which includes a Profile page and Activity page. You can also use this menu when you're ready to log out of Vision UI and end the active session.

On the **Profile** page, you can manage these options:

- *In the Basic Information section:* Optionally add your first and last name
- *In the Preferences section:* Select a default view for your Start page. This allows you to select which landing page on which you prefer to start after log in.
- *In the Preferences section:* Toggle on/off Search Bar Help prompts or the Quick Filter menu (in the Research section)



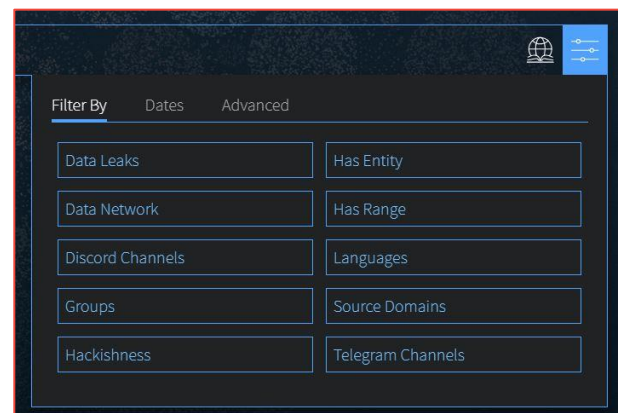
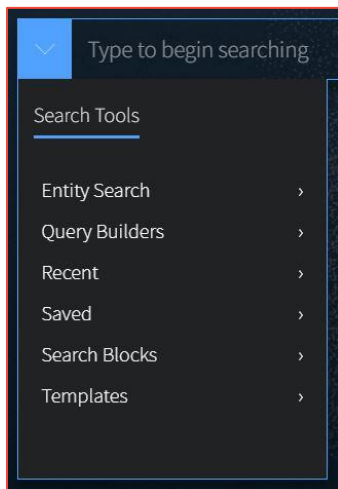
On the **Activity** page, once you start working in Vision UI, you will see a summary of recent Searches performed, Saved Searches created, or Search Blocks created. Click on the All Activity tab to see the detail of these activities, including time performed.



## Searching

### Using the Search Bar

1. The search bar works like most search engines; simply type words, phrases, numbers, or characters. The Search Techniques section goes into more detail and options for searching, but here a few quick start tips:
  - Use Boolean operators when searching more than one keyword. More Information: [Searching with Booleans](#).
  - Use straight quotations ("**Jane Doe**") to send the query as one phrase, Jane Doe.
  - Use the **exact:** search operator (**exact:fullz**) to prevent word stemming, and search for exact matches of that term. See: Stemming and Searching for Exact Terms.
2. Use the left drop-down menu to open **Search Tools**, which include these options:
  - **Entity Search:** the best way to search for Emails, CVEs, Credit Cards, Cryptocurrency Addresses, IP Addresses, and Social Security Numbers.
  - **Query Builder:** a helper for search variations or advanced formatting for commonly search items.
  - **Search Blocks:** Pre-populated keyword as well as any custom search blocks that you create, are accessible from this menu for easy access.
  - **Templates:** pre-populated search templates to help you get started quickly.
3. Once you've started searching, **Recent Searches** and **Saved Searches** will also appear in the Search Tools menu, for easy access.
4. Click on the **right Lexicon icon** to open the Lexicon and filter to (or exclude) darknet sites of interest. More information is provided in this section: [Lexicon](#).
5. Click on the **right Filter icon** to open the Filter menu. More information about these is provided in this section: [Filters](#), [Dates](#), [Advanced Search Options](#).



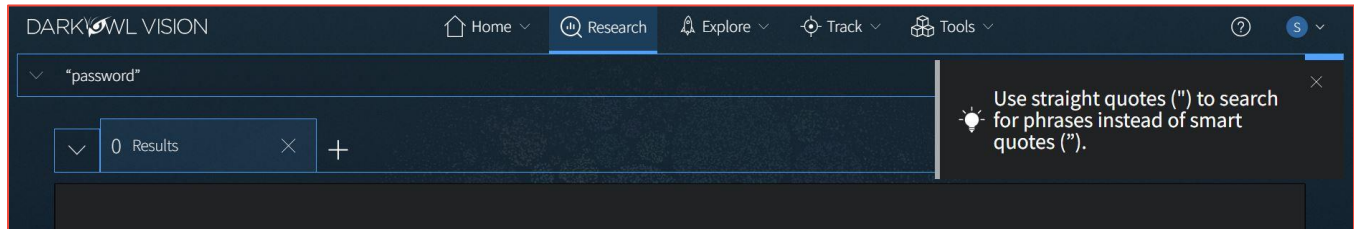
6. **Guidelines for using multiple search components in the same search:** Generally, using multiple *different* search components AND together; using multiple of the *same* search component (but different values) OR together. The only exception applies to the Free Text field, detailed below. The following are search components and their behaviors:
- **Entity Search** is a component. Note: Using two types of Entity Searches (for example, Emails and IP Addresses) in the same search would be the *same* search component with different values, and would OR together in your search. Using an Entity Search with a Filter (for example, Email Entity Search and a Groups Forum filter) would AND together in the search.
  - **Each Filter** is a component; a Network filter and a Has Entity filter are two *different* components and would AND together. Using two Network filters (for example, Network Onion, Network Telegram) would OR together in your search as they are the *same* search component with different values.
  - The **Lexicon** is a component. Note: Using two Lexicon entries in the same search would be the *same* search component with different values, and would OR together in your search. Using a Lexicon entry with another item (for example, Exploit Lexicon entry and the User Entity Search) would AND together in the search.
  - The **Free Text field** (type-in space in the search bar) is a component *but has a key difference* than the ones above—while it is a search component, each Free Text field acts independently of other Free Text fields. This means that two Free Text fields (for example, two Keyword Search Blocks) in the same search will AND together. Using keywords or clauses in the free text field with another item below would AND together in the search.

Here are examples of using different search components together:

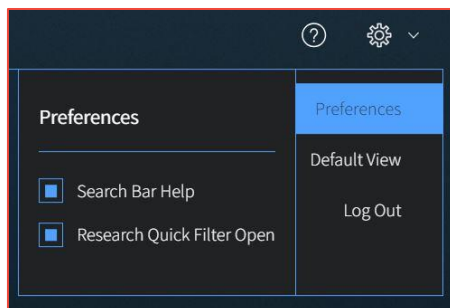
- Search Bar Free Text, Lexicon Paste Entry in the same search—AND
- Entity Search (Cryptocurrency), Search Bar Free Text in the same search—AND
- Hacking Keywords Search Block, Exclude Social Media Search Block—AND
- Lexicon Market Entry, Lexicon Forum Entry in same search—OR
- Network (Tor), Network (Discord) in the same search—OR
- Entity Search (Email), Entity Search (IP) in the same search—OR

## Search Bar Help

Search tips will appear in the upper right corner when a search could be optimized or includes a character the field doesn't recognize.



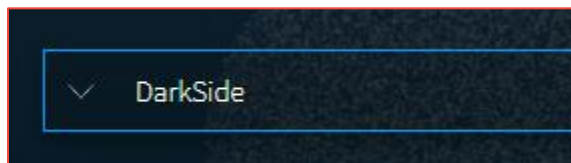
You can turn this feature off by clicking on your name in the upper right corner, selecting Preferences in the drop-down menu, and unchecking the toggle for Search Bar Help.



## Search Techniques

### Single Terms

To find any document with a specific keyword, simply put that keyword into the search bar:



### Phrase Searching

To find two or more keywords in a specific order, place the keywords within double quotes:

- "AES 256"

Without the double quotes, the search would be sent as: *AES OR 256*. This OR search is an inclusive search and may return results that only include the term AES, that only include the term 256, that include both terms but not next to each other, and that include both terms next to each other.

### Boolean Searching

Use Boolean operators **AND**, **OR**, and **NOT** to specify inclusions, alternate terms, or exclusions. (You can substitute AND, OR, and NOT with **&&**, **||**, and **!** respectively.) Keywords and field searches can be separated by any of the above in order to fine-tune your results.



- **drugs OR crime** – find documents with either 'drugs' or 'crime'
- **drugs AND crime** – find documents with both 'drugs' and 'crime'
- **DarkOwl AND (hack OR ddos OR 0day)** – find documents with DarkOwl and any one of three hacking keywords

*Note: Boolean operators must be in all caps. If they aren't in all caps, DarkOwl Vision will consider the word "and", "or", etc as keywords.*

#### Using Subqueries/Boolean Order of Operations

You can group together phrases to form subqueries, using parentheses ( ) to indicate each clause. This is especially important when both ANDs and ORs are used, to designate the correct order of operations for your subqueries.

- **DarkOwl AND (drugs OR crime)** – find documents with DarkOwl plus one of either drugs or crime
- **("AES-256" OR "AES 256") AND ("RSA-4096" OR "RSA 4096")** – find documents with one of AES-256 or AES 256 plus one of RSA-4096 or RSA 4096

#### Stemming and Searching for Exact Terms

DarkOwl Vision supports a process called stemming, which tries to reduce a word to an approximation of its stem or root form. Usually, terms are stemmed to plural/singular versions or different tenses. This means that searching will return matches on related forms of a word, unless you specify otherwise:

- **Hack** may return **Hacked, Hacker, Hacking**, in addition to **Hack**

When you want to search for a specific term, including special characters and punctuation, use the **exact:** operator to prevent word stemming:

- **exact:hack** – will return only documents containing the word hack

#### Excluding Items from a Search

Keywords can be excluded in multiple ways:

- Using the NOT Boolean operator
- Prefacing the term with a hyphen (-)
- Prefacing the term with an exclamation mark (!)

For example, the three searches below are equivalent and will find documents that contain 'DarkOwl' but not 'drugs'. Note that when excluding a keyword via hyphen or exclamation mark, it must be placed directly before the keyword with no space in between.

**(DarkOwl NOT drugs)** is the same as **(DarkOwl -drugs)** is the same as **(DarkOwl !drugs)**

You can also exclude values in other fields in the same way:



- DarkOwl NOT domain:drugs.onion
- DarkOwl -domain:drugs.onion
- DarkOwl !domain:drugs.onion

#### Searching for Entities in the Search Bar

When searching for specific entities, such as an email address or credit card number, directly in the search bar, we recommend searching with the appropriate operator. The Search Tools (in the drop-down on the left-side of the search bar) are a shortcut and automatically convert your query to the correct syntax.

- email:first.last@company.com
- ccn:111111111111111111
- cryptocurrency:15ivMrk8VzaK9TEN85XYssVbU3Yd6tLzb9
- cve:cve-2022-12345
- ipAddress:127.0.0.1\24
- ssn:123-45-6789

When searching for multiple entities, use the search operator and a Boolean OR, as follows:

- email:(first.last@company.com OR last.first@company.com)
- ccn:(111111111111111111 OR 222222222222222222)
- cve:(2022 OR cve-2021-12345)

#### Searching for both Keywords and Entities in the Search Bar

When searching for both keywords and specific entities (such as an email address or credit card number) directly in the search bar, use the following format:

- ("First Last" OR Nickname) AND email:first.last@company.com

#### Using Wildcards

Wildcards (\* or ?) are currently allowed in limited usage, in the middle or end of terms only. An asterisk (\*) is used to find zero or more unknown characters; a question mark (?) is used to find any one unknown character. Examples:

- **dar\*** – will find "dar", "dart", "darkowl", "daredevil", etc
- **d?rk** – will find "dark", "dork", "dirk", etc; will not find "drk" (however, d\*rk would)

*Note: DarkOwl Vision does not support leading wildcards. In other words, a search term cannot begin with either one of the wildcard characters.*

### Using Proximity Searches

You can find words near to each other by using quotations and selecting a maximum distance allowed: **"password hack"~2**. The maximum distance supported is 9.

### Using Pattern Matching / Regular Expressions

Lucene-based regular expressions are allowed and should be wrapped by forward slashes (/). Not all functionality you may be familiar with may be supported. Additionally:

- **These queries may time out**, particularly when searching for a high volume of unknown characters. Regex searching is computationally heavy and will result in slower, less performant searches.

To use a regular expression in Vision, place the expression between two forward slash characters:

- **/r[0-9a-zA-Z]{24,34}/** – to find results matching the pattern of a Ripple cryptocurrency address (which starts with 'r', then has anywhere between 24 to 34 alphanumeric characters)

*Note: Not all regex functionality you may be used to is supported by our system.*

### Using Special Characters

The following characters are reserved:

**+ - = && || > < ! ( ) { } [ ] ^ " ~ \* ? : \ /**

If any of the above characters are in a keyword or phrase being searched, you can escape the character with a backslash: \. For example, to search for mentions of a URL within a document, such as *https://darkowl.com/darkint-blog*, you must escape the colon, forward slashes, and hyphen, otherwise the search will return an error.

You can perform this search multiple ways:

- Escaping the special characters: `https:\\\\darkowl.com\\darkint-blog`
- Putting the whole keyword in quotes: `"https://darkowl.com/darkint-blog"`

Without escaping the special characters, this search will be interpreted as:

1. Searching within a field called 'https' (which doesn't exist)
2. An empty regular expression (/ / signifies the start and end of a regex with no content)
3. The keyword 'darkowl.com'
4. The start of a regular expression starting with 'darkint-blog'
5. No end to the regular expression (will return an error)

---

### Field Searching (Search Operators for Metadata)

Every search performed will look in one or more fields for the keyword(s) being searched. By default, the search bar will search both the 'title' and 'body' fields of documents. This means that results will be returned if the keywords you're looking for are found in either the body of the document or the title (or both). This means:

- A search of **the word 'drugs' in the search bar** is the same as
- **title:drugs OR body:drugs.**

Most searches will not require specifying a field name, since title and body are automatically searched. However, other metadata fields can be searched, including specifying only the title or body field, for example:

- title:alphabay
- hackishness:1
- domain:drugs.onion

The list of metadata fields is below. When searching within these fields, type the following search operators in the search bar, and then the query content:

- inUrl:
- contentType:
- headers.server:
- headers.last-modified:
- title: (to search within this field exclusively)
- body: (to search within this field exclusively)
- domain:
- leak:
- network:
- hackishness:

Multiple values within the same field can be searched in a number of ways. The following examples are equivalent:

- **domain:(drugs.onion OR crime.onion)** is the same as
- **domain:drugs.onion OR domain:crime.onion**

You can also look for phrases within specific fields using double quotes:

- **title:"Forum rules"**

Subqueries within fields are supported:

- **title:(darkowl AND (drugs OR crime))**

*Note: when searching using fields, there should not be a space after the ':' character.*

#### Field Searching (Search Operators for Chat Networks)

There are several search operators that can help you filter to content from Discord or Telegram servers, channels, and users.

- The **telegram:** operator filters to channels, IDs, or users from Telegram.
- The **discord:** operator filters to servers, channels, IDs, or users from Discord.
- The **user:** operator filters to usernames or user IDs from either Telegram or Discord.
- To exclude telegram, discord, or user operators: preface the search operator with a hyphen: **-telegram:"EVILX.su Leaks Chat"**

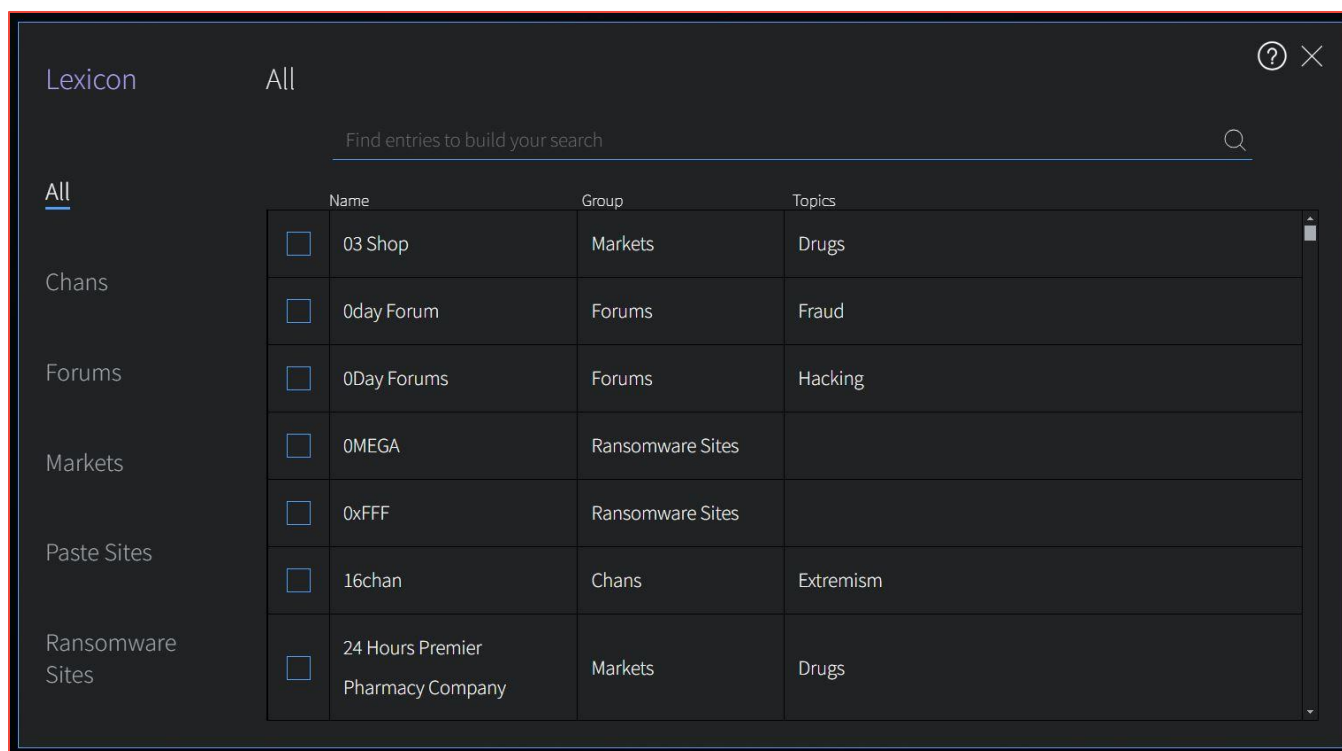
Several examples are presented below:

Search	Description
telegram:"Чат Военковов Русской Весны"	Search for content from this Telegram channel (quotations are used as it has spaces in its name)
telegram:" <b>DEMON HUB 1</b> 🐈 ~ <b>#THEDEMONNETWORK</b> "	Search for content from this Telegram channel (note quotations for spaces and special characters)
telegram:lapsus*	Search for content from any Telegram channel or username that starts with the characters <i>lapsus</i>
telegram:"-1001228309110"	Search for content from the Telegram channel with this channel ID. Include the - prefix with straight quotes.
discord:"HELLU!"	Search for content from this Discord server
discord:funny-sb	Search for content from this Discord channel
discord:tylerdurdan710	Search for content associated with username (Discord only)
user:tylerdurdan710	Search for content associated with this username on Discord or Telegram or Forums

#### Lexicon

DarkOwl Vision's Lexicon is an easy-to-use tool intended to help you find interesting content from hacking forums, marketplaces, and other darknet sites. While not an exhaustive list of sites in our data, it's a good place to get started. Make a suggestion at any time for sites you'd like us to add at: <https://www.darkowl.com/lexicon>.

Click on the **right Lexicon icon** on the Search Bar to open the Lexicon. To find an entry in the Lexicon, start typing to filter through all entries, or select a Group from the left and scroll through the section. The search field will search all columns (Name, Group, Topics).



Clicking once next to your desired entry(ies) will immediately add the entry(ies) to the search bar. **Click once to include, click twice to exclude.**



Click the > icon, or anywhere outside of the modal, to go back to the Search Bar. In the screenshot below, we've selected Dread and Exploit.in forums, which will filter results to content from only those two forums. You can run the search with just the Lexicon entries, or add more keywords to your search.

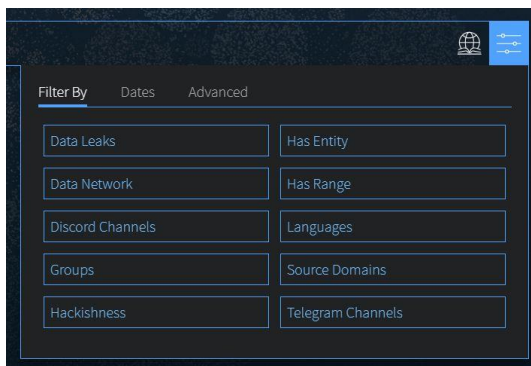


### Groups You'll Find in the Lexicon

Section	Description
<b>Chans</b>	A chan imageboard is considered a type of bulletin-board-like forum that revolves around the posting of images, often alongside text and discussion. Read more about <a href="#">Chans here</a> .
<b>Forums</b>	Forums are online places where people discuss specific topic threads; some require authentication to access.

<b>Markets</b>	Markets include both small vendor shops to big-name marketplaces; some require authentication to access. Some marketplaces have previously been taken down by law enforcement, though we may still have historical content.
<b>Paste Sites</b>	Paste sites are online temporary content-hosting applications that allows for users to share text online anonymously.
<b>Ransomware Sites</b>	Ransomware sites are domains administered by ransomware groups. It is common for these groups to post their victims, and data stolen from their victims, on these sites.

### Filters, Dates, and Advanced Search Options



Refine your search using the Filters icon on the right side of the search bar. This includes three tabs for:

#### Filters

#### Dates

#### Advanced options

### Data Leaks

Filter or exclude content from any known data leaks or breaches. **Click the box next to the desired option.** To find individual leaks, see the [Leak Explore](#) section or the Lexicon.

- For free text searching, type *leak:leakname* in the search bar
- Prefix with - to exclude, i.e. *-leak:leakname* in the search bar

### Data Network

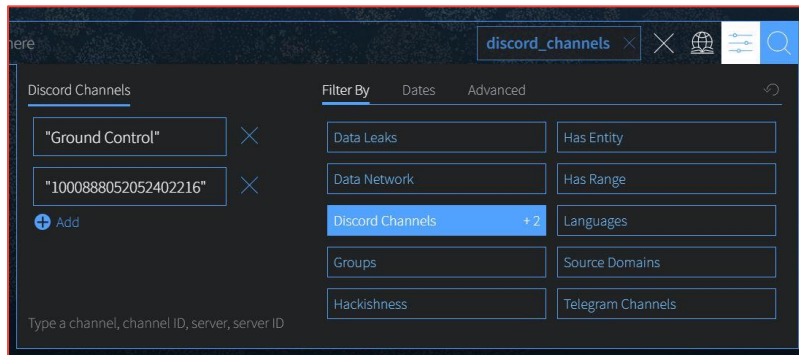
Filter to content from a particular DarkOwl data collection network. Options include: Discord, FTP, I2P, IRC, Onion, OpenNIC, Telegram, Zeronet. **Click once to include, click twice to exclude.** More information: Data Networks.

- For free text searching, type *network:networkname* in the search bar
- Prefix with - to exclude, i.e. *-network:networkname* in the search bar

### Discord Channels

Filter to content from one or more specific Discord channels or servers. Click the **Add** button, and then type either one channel name, channel ID, server name, or server ID in the box. You'll note that quotation marks are automatically applied when you start typing. You can add up to

10 channels or servers per query. You can remove previously-entered channels or servers by clicking the X next to the channel or server to remove.



- For free text searching:
  - To filter to one channel or server: Type **discord:"Ground Control"** in the search bar
  - To filter to one channel ID or server ID: Type **discord:"757762132962967624"** in the search bar
  - To filter to multiple channels/IDs: Type **discord:("757762132962967624" OR "Ground Control")**
  - To exclude discord channels or servers (free text searching only): preface the search operator with a hyphen: **-discord:"Ground Control"**

## Groups

Groups are combined filters that narrow your search to specific categories; **click to include:**

- **Authenticated Sites:** Filter to content from sites requiring credentials or challenges.
- **Blogs:** Filter to content from sites identified as blogs.
- **Chans:** Filter to content from sites identified as chan/imageboard forums.
- **Darknet:** Filter to content from the Tor, I2P, and Zeronet darknets.
- **Forums:** Filter to content from sites identified as forums.
- **Forum Posts:** Filter to content specifically from forum posts (note: the **Forums** group is will include Forum Posts, and will also include content from forum sites such as member profile pages, etc).
- **Markets:** Filter to content from sites identified as marketplaces or vendor shops.
- **Ransomware:** Filter to content from known ransomware data leak sites.
- **Paste Sites:** Filter to content from sites identified as paste sites.



### Hackishness

Hackishness assigns a rating to every piece of content collected, indicating the likelihood to which the information could be used for criminal activity. The lower bound of hackishness is .01 and the upper bound is 1.0; the UI shows these as percentages on search results. You can quickly filter to results with hackishness by using the slider on the Hackishness filter to select a desired hackishness threshold.

You can also filter to hackish results using hackishness: in the search bar, which supports searching as range. This means, you can narrow down to values between two parameters, inclusive or exclusive, for example:

- **hackishness:[.01 TO 1]**
- **hackishness:{.01 TO 1}**

Note the '[' and '{' characters used above. In Lucene range queries, '[' and ']' are inclusive so the first query above would return values from .01 to 1, including both .01 and 1. The second example would return values from .01 to 1 not including .01 or 1. '[' and '{' can be combined:

- **hackishness:{.5 TO 1]** (this will find values greater than .5 and up to and including 1)

### Has Entity (Credit Cards, Cryptocurrencies, CVEs, Email, IPs, Social Security Numbers)

Filter to content that have at least one selected Entity. **Click next to the Entity name to select.**

### Has Range (Credit Cards, Cryptocurrencies, CVEs, Email, IPs, Social Security Numbers)

Filter to content that have a certain number of selected Entities. This filter is helpful in finding "dumps," as many threat actors will post multiple instances of PII on a singular site or document. **Type values next to a selected Entity:** Enter a lower bound (minimum 1), upper bound (maximum 999999), or use both fields to form a range (50 to 1000).

### Language

Filter to content in a particular language. Languages are detected by DarkOwl Vision at the time of ingestion, using natural language processing. **Click once to include.**

- For free text searching, type *language:languagevalue* in the search bar

### Source Domains

Filter to content from one or more domains, or exclude a particular domain by typing a hyphen in front of the domain. Type only the domain portion in the filter box (example: **arch3rsecgjqcmjb.onion**; no need for the www or http:// prefix). Be sure to remove any trailing slashes or paths from the domain.

- For free text searching, type *domain:domain.onion* in the search bar
- Prefix with - to exclude, i.e. *-domain:domain.onion* in the search bar

## Telegram Channels

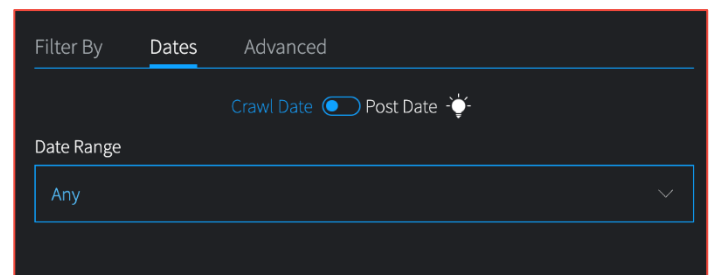
Filter to content from one or more specific Telegram channels. Click the **Add** button, and then type either one channel name or one channel ID in the box. You'll note that quotation marks are automatically applied when you start typing. You can add up to 10 channels per query. You can remove previously-entered channels by clicking the X next to the channel to remove.

*Note: when typing a channel ID, use the hyphen prefix, i.e. -1001556588508.*

- For free text searching:
  - To filter to one channel: Type **telegram:"EVILX.su Leaks Chat"** in the search bar
  - To filter to one channel ID: Type **telegram:"-1001556588508"** in the search bar
  - To filter to multiple channels/IDs: Type **telegram:("-1001556588508" OR "EVILX.su Leaks Chat")**
  - To exclude telegram channels (free text searching only): preface the search operator with a hyphen: **-telegram:"EVILX.su Leaks Chat"**

## Dates

Use the drop-down to quickly select a time range for search results, or select Custom to choose a specific start/end date.



Use the toggle to choose between filtering by **Crawl Date** or **Post Date**:

- **Crawl Date:** Filters to any content that DarkOwl collected between the specified dates.
- **Post Date:** Filters to any content that was posted between the specified dates. Filtering by Post Date will filter to results where the post date is known. Other search results will be excluded.

Dates can be searched in the search bar as a range using the following date format: YYYY-MM-DDTHH-MM-SSZ:

- **crawlDate:[2021-07-01T00:00:00Z TO 2021-07-10T23:59:59Z]**
- **published:[2021-07-01T00:00:00Z TO 2021-07-10T23:59:59Z]**

As the Date filter supports range searching, you can narrow down to values between two parameters, inclusive or exclusive, as discussed in the hackishness section. In Lucene range queries, '[' and ']' are inclusive, and '{' and '}' are exclusive.

### Advanced Options (Sort By, Show Duplicates, Empty Bodies)

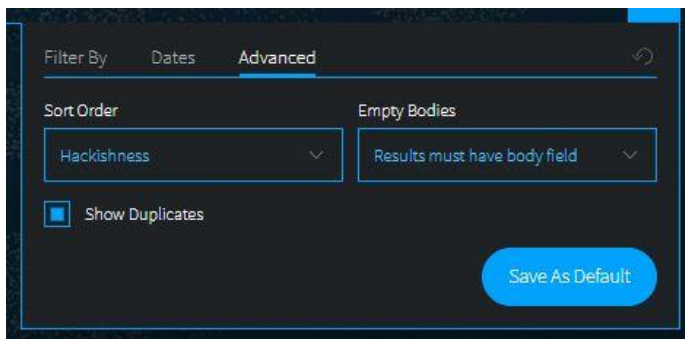
Use Advanced Options to select a Sort option, or to show all results (including similar ones).

- **Sort options.** Use the drop-down to sort your results by **Relevance** (default), **Hackishness**, **Crawl Date**, or **Post Date**.

*Note: Sort by Post Date will filter to results where the post date is known. Other search results may be excluded. Sort by Post Date is not available to be set as a Default search.*

- **De-duplicate your results.** A maximum of 20 results are returned per page. You can choose to de-duplicate similar results on a per-page basis (default) or see all results. The default is to de-duplicate results on each page; you can toggle this on or off.
- **Empty bodies.** Our collection includes documents collected that do not contain any text characters; text content is stored in the Body field. Use the drop-down to select one:
  - **Any document** (documents can include text in the body, or no text in the body)
  - **Results must have body field** (default) (to only return documents that had text content on them)
  - **Results must not have body** (to see only documents without text)

You can personalize your experience and change the above defaults. When you select a new option in any of the above settings, a button will appear to **Save as Default**. Clicking to save will remember these settings for future searches.



## Search Tools

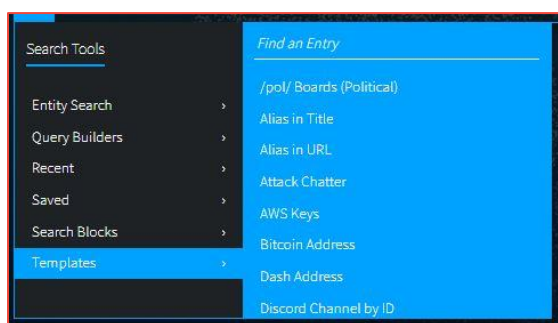
The Search Tools menu includes tools to help you create effective searches, including Entity Search, the DARKINT Lexicon, Query Builders, Search Blocks, and Templates. Once active, your Recent Searches and Saved Searches will also appear in this menu for easy access.

### Templates

Search **Templates** are a great way to get started searching our data. This list includes many example searches to help find information of interest. Click on an item in the list to populate it in the search bar

*Note: where indicated, replace the text with your information as appropriate (for example, when "organization.com" appears in the template).*

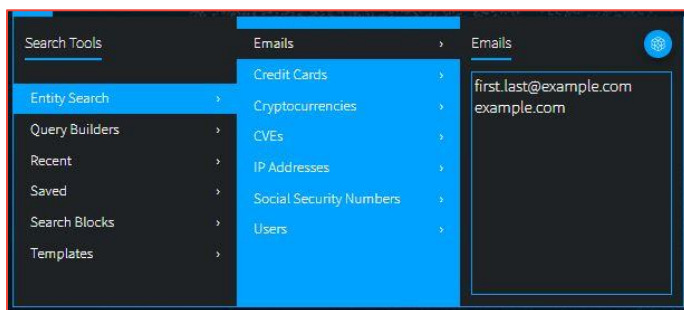
**Start typing in the Find an Entry field** to filter the list quickly.



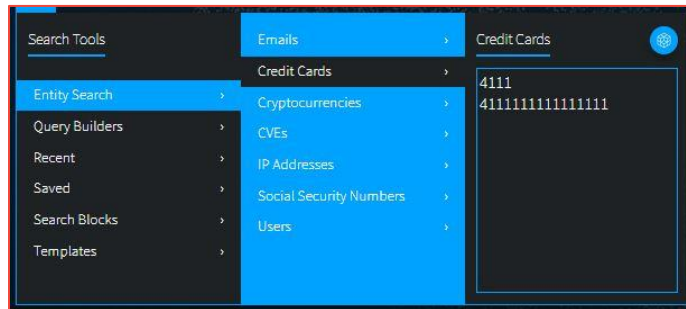
### Entity Search

**Entity Search** is the best way to search within our indexed document content for Emails, Cryptocurrency, Credit Cards, IP Addresses, and Social Security Numbers. Additionally, all Entity Searches can easily become [Search Blocks](#), with Set Up Monitors options, by clicking on the Search Block icon on the upper right. You can enter one or more values in each builder, using space, comma, or semi-colon between values. Pressing Enter will execute the search.

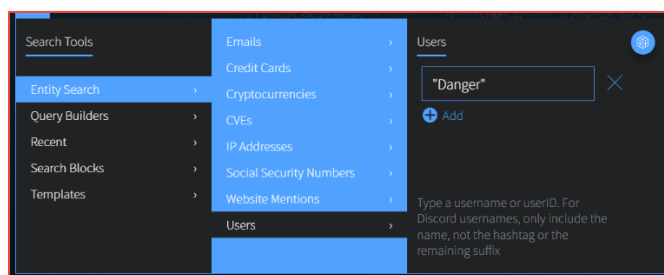
- **Emails** supports searching for individual addresses, domains, or subdomains.



- **Credit Cards** supports searching for individual addresses or BINs.

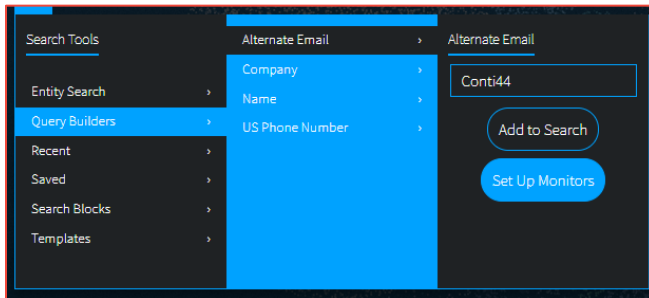


- **Cryptocurrencies** supports searching for the following types: *Bitcoin, Ethereum, Monero, Litecoin, Dash, ZCash*. The types have been validated by DarkOwl Vision. Cryptocurrency wallet types not in this list can continue to be found with regular expressions.
- **CVEs** supports searching for the following formats:
  - By full CVE-ID, i.e. *CVE-2022-12345* (finds specific known CVE)
  - By CVE-ID, i.e. *2022-12345* (finds specific known CVE, without the CVE prefix)
  - By Year only, i.e. *2022* (finds all CVEs from that year)
- **IP Addresses** supports searching for the following formats: *IPv4, IPv6/IPv6 compressed, and CIDR ranges for both IPv4 and IPv6*. *Note: When we find and extract IP addresses in the text of a document, we store them as an IP address object rather than a string (all of our other tokenized entities are strings). This allows for more search flexibility, such as searching for CIDR ranges. However, since the IP address being searched is not a string/text, they are not able to be highlighted when searching this way.*
- **Social Security Numbers** supports the following format: *123-45-6789* (with hyphens).
- **Website Mentions** supports searching for domains or URLs.
- **Users** supports searching for usernames across Discord, Telegram, and Forum sources.



## Query Builders

**Query Builders** help you format commonly searched items that either require special formatting or work best when submitted with variations, in order to make the most inclusive search to find the best results. Once you've selected the type of builder and input text in the appropriate field(s), you can either **Add to Search**, or [Set Up Monitors](#). Clicking **Add to Search** will format the query and place it in the search bar. You can continue to add filters, date ranges, or other advanced options before submitting the search.



### Types of Query Builders

- **Alternate Email:** When searching for email addresses a threat actor may be using with another provider, a trailing wildcard can be a helpful search. For example, entering the prefix of Conti44 in the Query Builder will find results for conti44[at]hotmail.com, conti44[at]hotmail.il, conti44[at]tutonota.com, and so forth. These may be potential associated or alternate email addresses run by the same person or group.
- **Company:** When searching for company mentions on the darknet, we recommend using both the company's name and domain in the same query. This query builder will construct a search to find results that have your company's name or any mentions of its domain.
- **Names:** When searching for first and last names, we recommend using a proximity search, with up to 2 words as a distance. This can help find variations such as "last, first" or "first middle last" (even when the middle name is unknown).
- **US Phone Numbers:** When searching for phone numbers, we recommend preparing a query without spaces and with spaces between number groups.

*Note: We recommend preparing searches the same way for international phone numbers; i.e. 1234567889 OR "123 456 7889".*

### Set Up Monitors

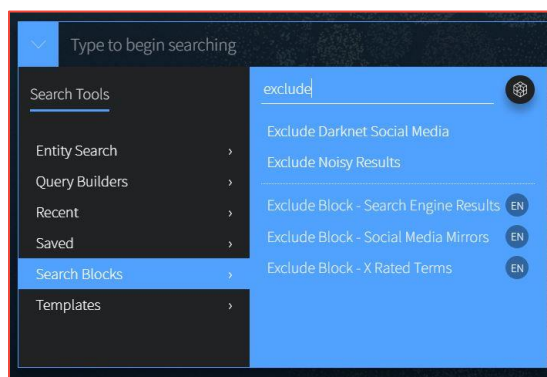
Clicking **Set Up Monitors** (from Query Builders or Entity Search Blocks) will prompt you to select pre-built searches that will automatically save and start monitoring, notifying you when new results are found. Choose the searches you'd like to create and click Confirm.

*Note: You can change any of the default settings by clicking the Edit icon by the search name.*

## Search Blocks

**Search Blocks** are reusable search components and appear in Search Tools for quick access. Use Search Blocks to create lists of commonly searched items, such as a list of company names, IPs, or domains; or create any query string that you'd like to use across multiple searches.

- You can use the same block in multiple searches, which can help save you time when you are building queries that have similar elements.
- When you update a block, all searches that use that block are automatically updated to use the new block content.



Initially you'll see a list of pre-built blocks in the Search Tools list and Search Block page, which were created by DarkOwl analysts. After you create your own search blocks, they will appear at the top of the list. Begin typing in the Find an Entry field to filter the list.

You can make search blocks in a few different ways:

1. Select **Add New Block** on the Tools: Search Blocks page.
2. On the Search Blocks page, click on the Edit icon next to a pre-built block. Make modifications and save as a new block.
3. When you are in the Entity Search, click on the block icon to convert into a new block. In addition to creating a new Search Block, Entity Search Blocks also allow you to **Set Up Monitors**.

## Saving Searches

A **Saved Search** is simply a query you'd like to run again in the future. Once saved, you can find this list of searches on the Search Tools menu. Additionally, you can **Automate this search** to apply monitoring functionality, which runs the search for you on a cadence you choose, generating **Alerts** on your dashboard if hits are found. After you run a query, the **Save Search icon** (star icon) will appear on the right side of the search bar.

Selecting that icon will open a form:

- Add a **Saved Search Nickname**.
- Select one or more **Cases** to save the search into (optional).



- *If a Case is selected:* the search will be saved directly to that Case. If you have selected the Automate this search option below, any Alerts generated will be automatically saved into that Case as well.
- *If a Case is not selected:* the search will be saved in the list within your Tools > Saved Searches page.
- Add **Categories** (optional). Categories can help you sort your searches and alerts.
- Click **Automate this search**, if you'd like to apply monitoring. If this is selected, additional options for Frequency, Criticality, and Email Notifications will appear.
- Click **Save** when complete.

Save New

Saved Search Nickname

My new saved search

Save to Case (Optional)

Threat actor tracking

Categories (Optional)

Click to Remove Category

EXECMONITOR

☒ Automate this search to monitor for new results

Run Every

24 Hours

Alert Criticality

Low

☒ Email me when this automated search finds alerts

Cancel Save

## Search Results (Research)

DarkOwl Vision collection activities are automated and continuous 24/7/365, collecting content from millions of websites daily in 52 languages. Our collection includes Tor, I2P, Zeronet darknets; encrypted chat servers, channels, and groups; certain deep web sites with transitory information, such as paste sites, forums, and FTP content; as well as high-interest closed access surface websites. Collectively, we refer to this as DARKINT™, or darknet intelligence.

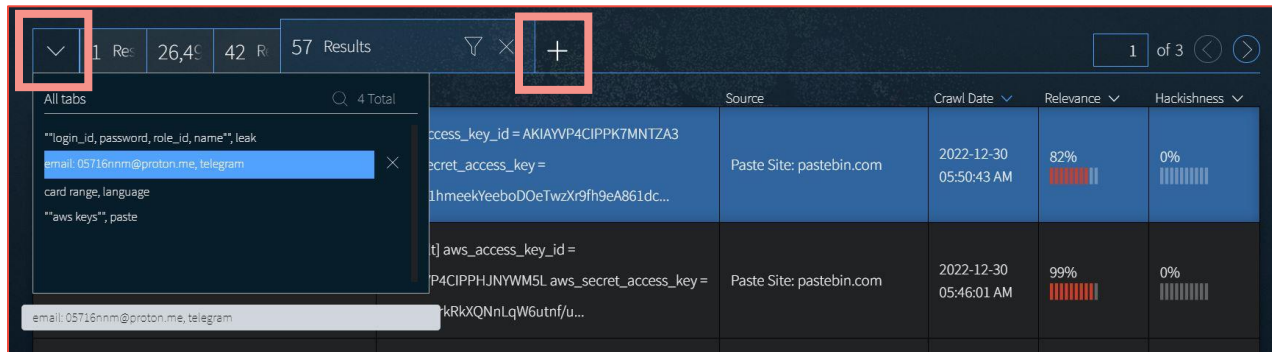
Our indexed document collection, which are the results you receive after doing a search in the Research section, is processed into the following field categories:

<b>Body field</b>	The raw text collected from the webpage/record/target.
<b>Metadata fields</b>	Fields we collect along with the body, if available, such as: domain, network, headers, leak information. Click on the Metadata and Leak view switches in Search Results to see this information.
<b>Mined fields</b>	<p>Tokenized features we mine out of the body of the result, which are currently Entities (emails, credit cards, cryptocurrencies, cves, ip addresses, ssns, website mentions) and Chat-related information (users, user IDs, servers, channels, channel IDs).</p> <p>Entities and Chat Users appear as individual View Switches in Search Results, if present in the body.</p>
<b>Processed fields</b>	Information we apply to a result from our natural language processing or machine learning, such as hackishness or language detection.

When you do a search in the search bar from Home or Research, a maximum of 20 results are returned per page. Vision UI includes a default setting to de-duplicate results on a per-page basis. When the Show Duplicates option is off, you may receive fewer documents than the count submitted, since some of the results may not be returned. If you would like to see all results, you can change this setting in the Filter menu's [Advanced Options](#), which includes an option to toggle Show Duplicates on or off.

## Search Tabs

You can have multiple searches open, to allow for pivoting and further investigation. Click on the (+) icon to start a new search. You can go back to previous searches and results by either clicking on a specific Result tab, or using the left tab dropdown menu. You can have up to ten search inquiries open simultaneously.



## Search Result Viewer

After running a search, your result list will appear on the Research page. The list displays a summary including the title and excerpt of the result (around the first keyword match, if applicable), where the result was found, crawl date, hackishness, and relevance of the result.

Click in the Title or Excerpt columns to open the full Result Detail; click on the X to close.

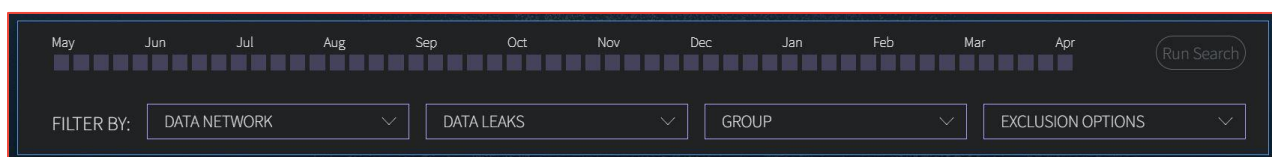
## Keyboard Shortcuts

Navigate through Search Results using these keyboard shortcuts:

Key	Description	Key	Description
<b>k</b>	next result	<b>;</b>	toggle detail pane
<b>i</b>	previous result	<b>o</b>	next page
<b>l</b>	next highlight	<b>u</b>	previous page
<b>j</b>	previous highlight		

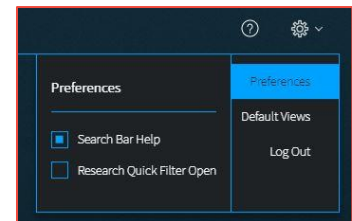
## Quick Filtering

The quick filter menu includes some of our most frequently used filters, as well as a crawl date bar, and can help refine your result set. Once selected, filters will appear in the search bar. Click the **Run Search** button to see a new result list.



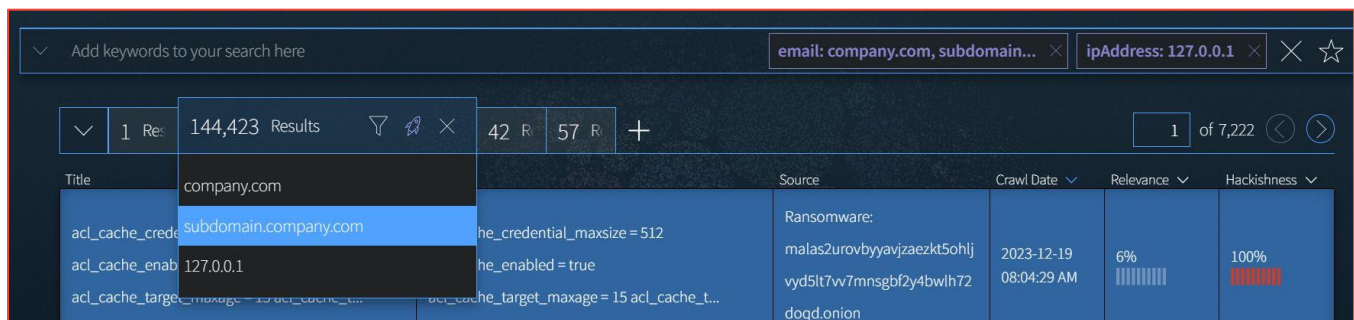
- **Crawl Date Slider.** Select a Crawl Date range within the last year, by clicking on a box to start, sliding over the date period, and clicking on an end box.
- **Filter by Data Network.** Click once to select a network; click twice to exclude a network.
- **Filter by Data Leak.** Click the box next to the option to see results from Data Leaks, or exclude results from Data Leaks.
- **Filter by Groups.** Click once to select a group; click twice to exclude a group.
- **Exclusion Options.** Click the box next to the desired option. You can add the Hackishness filter (exclude results with 0% hackishness), or select various Exclusion Search Blocks, to reduce noise in result sets.

*Note: The quick filter menu is open on the Research page by default, to help you easily work through result sets. However, this setting can be adjusted in the Preferences menu.*



### Pivot to Entity Explore

If your search included an Email, Credit Card, Cryptocurrency, or IP Address Entity Search tile, the Explore icon will appear next to the Quick Filter icon. You can use this icon to look up any of the values in the Explore: Entity section. Click the icon, then select one of the values from the drop-down.



### Viewing Individual Result Detail

Results from our index include the following elements, referenced on the screenshots below:


1. **Source** of the result and either **Crawl Date** (when we added it to our data collection) or **Post Date** (date of the forum post). Additionally, you may see these options:
  - a. If a result is a forum post, a **Post Author** will be present. You can click on this button to open a new search tab to search for other posts by the same author.
  - b. If a URL has special characters or emojis, a **Decode URL** button will be present to toggle to the decoded version, which can assist users who have the proper sandboxed environments in viewing the original source. DarkOwl Vision stores

URLs in their encoded form. Once a URL is decoded, you can toggle back to the encoded version by clicking **Encode URL**.

http://  
9F%D1%80%D0%BE%D0%B4%D0%B0%D0%BC-  
%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D1%8B.1113/#post-5243  
Crawled on 2023-06-22 08:19:24 AM [Decode URL](#)

http://  
Продам-доступы.1113/#post-5243  
Crawled on 2023-06-22 08:19:24 AM [Encode URL](#)

2. Result actions you can take.
  - a. Options to **Download** the result (.txt) or get a **Link** to return to this result later.
  - b. If a search result is a forum post, you can click **View Thread** to reconstruct the posts into the original thread. See the [View Thread](#) section.
3. If enabled for your account, you will see the **Direct to Darknet** button on eligible documents. See the [Direct to Darknet](#) section.
4. The right side will contain various [View Switches](#) to see the result, metadata, tokenized fields, and enrichment:
  - a. The **Body** is the content of the result.
  - b. **Metadata** includes where and when the result was collected. Clicking on the icon next to URI will allow you to copy the URL in a defanged format.

URI: <https://forum.> 240354/ 

  - c. If present in the Body, additional view switches will show Lists of Entities within the result (**Emails, Cards, Cryptocurrencies, CVEs, IP addresses, SSNs, Website Mentions**).
  - d. A **Chat Users** view switch will be present if the result is from Telegram or Discord with Usernames and User IDs found in the result. (The lower screenshot shows this switch active.)
  - e. [Leak Context](#) or [Site Context](#) buttons may also be present, depending on the type of search result.
5. A **Group** heading will be present if the site has a classification. Some of the classifications include: Blog, Chan, Data Sharing, Directory, File Repository, Forum, Forum Post, Market, News, Paste, Search Engine, Social Media, Ransomware. Other classifications may be added in the future. Additionally, *Authenticated Site* will be present if the site required special access, such as a login or other challenge.

http://breached.  
FRESHLY-DECLASSIFIED-DATABASES-AT-HIGH-PRICES--106677  
Posted on 2024-02-23 05:00 | [Post Author: Foxmr](#)

1

I Need freshly decrypted databases  
My price will definitely satisfy you  
As long as you are freshly decrypting the database,  
I hope you are not a second-hand dealer because I know many people  
No need to throw me a public or 1kk file and say - bro check! Take your time  
and mine!  
Looking for long-term cooperation with hackers  
100k=400\$-800\$ depends on the quality.  
Databases like 20k, 50k, 80k also like  
TG ---- @AlexAbelard

2

View Thread

3

DIRECT TO DARKNET

4

Body

Metadata

Group

Forum

5

Forum Posts

Hackishness

27%

https://telegram.me/  
Crawled on 2023-11-13 09:56:46 AM

Find an Entry

Username	User ID	
DrWebBot	161163358	...
Ju1cy_LuCy	6205236132	...

4

Body

Metadata

Chat Users

2

Hackishness

0%


### View Thread

If a search result is a forum post, you can reconstruct the original thread. Clicking on **View Thread** from a forum post search result will open up a new modal which will display the thread post-by-post in chronological order. Once in the thread view, you can paginate through the thread (if there are multiple pages) and/or change the sort direction. Clicking on the three-dot menu includes options to see post metadata, or search for all posts from that user.

**Thread: DBS bank - 13GB Transactional Database**


avatar\_air BreachForums (2023) Started on April 05, 2024 11:29 PM

16 Posts ↑↓ Oldest first

**Mitrich**


**April 06, 2024 - 1:49:00 AM**  
sample please. what is inside?

...

**maybes0me1**


**April 06, 2024 - 1:55:00 AM**  
Thank you so much man This forum account is currently banned. Ban Length: (1d, 18h, 27m remaining)  
Ban Reason: Spamming.

...

**vulture**


**April 06, 2024 - 2:17:00 AM**  
Do provide sample also on your post itself.

...



**DIRECT TO DARKNET**

Users on this page (16)  
**avatar\_air, Mitrich, maybes0me1, vulture, Shinichi, Addka72424, sunj9710, Ledgerbydatabase, BurkeVan, niuj76809, cuong89bkb, orb1t, jester9999,**

**Mitrich**

**April 06, 2024 - 1:49:00 AM**  
sample please. what is inside?

...

View Post Metadata

Search all posts by this user

### Direct to Darknet

For eligible documents, clicking **Direct to Darknet** from a search result or thread view will launch a secure sandbox environment which will take you to the original source of that document. Eligible documents include any live Onion V3 domain or clearnet domain from a DarkOwl Vision Search result. Direct to Darknet leverages the best-in-class Silo web isolation platform from Authentic8.

You can safely interact with the site content, such as to solve a captcha; downloading files from the darknet site is not supported. Some sites may require credentials; you can use your own established credentials to safely interact with the site content. Browsing is domain-locked to the site accessed from the search result. For more information, see our [FAQ document](#).

*Note: A site may not be active or online at the time you try to access it. The search result from DarkOwl Vision is persistent as it is stored by DarkOwl.*

*Note: If you use pop-up blockers, be sure to allow pop-ups from darkowl.com.*



## View Switch Actions

The View Switch for Entities (**Emails, Cards, Cryptocurrencies, CVEs, IP addresses, SSNs, Website Mentions**) or **Chat Users** will show you a list of the items that appear within the Body of the search result. Click directly on an item to jump to where that item is located in the Body.

Email : @gmail.com  
 Email Password:  
 IP Address : 50.93.226.86  
 Full Name :  
 Address:  
 City:  
 Zip:

50.93.226.86  
 66.87.177.106

*Clicking on the IP address will bring you to that location in the search result.*

Some of the View Switches include additional pivoting actions.

- For **Chat Users**, you will see a menu that allows you to quickly search for the User ID or Username. Searching for the User ID can help you find alternate usernames.
- For **CVEs**, you will see a menu that allows you to pivot to **See in Mitre**. This will open a new browser tab and read more about the CVE from Mitre's cve.org website.
- For **Emails, Cards, Cryptocurrency, and IP Addresses**, you will see a menu that allows you to quickly look up that item in Entity Explore.

Username	User ID
DRTELEGRAMMM	6204389858
emalaelama	
Free_LTC_Legit	
ghadamghadam888	
khaterekoshki	
Koshaiio	2076202260

Find an Entry

Rolexyzenltd@gmail.com

Search in Entity Explore  
 See in document

## Site Context

If a search result is from a ransomware site or forum, an additional **Site Context** View Switch will appear below the Metadata View Switch. Site Context is information from the DarkOwl analyst team that gives additional enrichment such as the Site Name and any aliases, and may include relevant dates and more. Where available, options to pivot to Actor Explore, or to pivot to search associated Telegram channels will be present.

http://3slz1.onion/

Crawled on 2022-04-27 10:15:23 AM

Site Context

Site Name	STORMOUS
Aliases	STORMOUS
First Active	2021-12-01
Context Actors	<a href="#">Stormous</a>
Telegram Channels	<a href="#">STORMOUS Ransomware</a>
Ciphers	AES+RSA

Download

Link

DIRECT TO DARKNET

Body

Metadata

Site Context

Group

Ransomware

Hackishness

0%

Leak Context

If a search result is from a data leak, an additional **Leak Context** View Switch will appear below the Metadata View Switch. Leak Context is information from the DarkOwl analyst team that gives additional enrichment regarding the leak, and may include relevant dates, content information, and target information.

Data Leak: naz.api

Crawled on 2024-01-30 08:26:08 PM

Leak Context

Search for Filetree

Download Context

Name	naz.api
Description	<p>The naz.api leak was made available on BreachForums, on January 15, 2024. According to the post, it is a 35 GB collection of public URLs, usernames and passwords. The post also notes that it was originally on xkey.info but was taken down for allegedly not being the real naz.api leak.</p> <p>Analyst Note: naz.api is one of the largest credential stuffing lists originally posted in September 9, 2023 by 0x64. According to that post, the database was created by extracting data from stealer logs, and contains over 1 billion unique records of saved logins and passwords in users' browsers. The post also notes that the original naz.api dataset was donated to 0t.rocks.</p>

Content Categories	Credit cards, Emails, Credentials
Content Specifics	Email addresses, Account information, User accounts, Device information, Passwords, IP addresses, Credit card numbers
Associations	2023, BreachForums, StealerLogs
Actor	emo
Host	i.suffer.rip
Original Post URL	<a href="http://breached.d.onion/T">http://breached.d.onion/T</a>
Post Location Type	Forum
Post Vision ID	<a href="#">a03b3f9362fbd7ba5032400315640c6cc19fb804</a>
Associated URLs	<a href="http://breached.d.onion/T">http://breached.d.onion/T</a>
Leak Classifications	StealerLogs
Leak Size Records	1 Billion Records
Leak Size Advertised	35 GB
For Sale	false
Date Available	2023-11-02

Some of the actions you can take include:

- Click **Search for Filetree** to locate and review the leak's filetree document(s) (if filetree is available). The filetree will provide a list of all of the files that were available in the leak, including files that were not indexed by DarkOwl Vision. This can help you review for non-text content that might be relevant to your investigation.
- Click **Download Context** the leak content (.txt) to include in reports or briefings, is available in active client accounts.
- Click on the **Vision Document ID** link to open the Vision document to see the original post in a new search tab. This can help investigate the source of the leak further.

The following table provides a description of fields that may appear in Leak Context. *Note: not all fields may be available or known for all leaks. Additional fields may be added in the future.*

<b>Name</b>	Name of the leak.
<b>Description</b>	A short description about the nature of the leak.
<b>Date Available</b>	Date the data was made available on the darknet or internet, if known.
<b>Date Breached</b>	Date of the leak incident or ransomware attack, if known.
<b>Content Categories</b>	High-level categories or types of content contained in this data leak. Content Category examples include: combolist, credentials, documents, messages, PII, stealerlogs, etc.
<b>Content Specifics</b>	More granular information about the compromised data in this leak. Content Specifics examples include: dates of birth, email addresses, financial documents, internal documents, ip addresses, legal documents, plaintext passwords, phone numbers, physical addresses, profile information, usernames, etc.
<b>Password Format</b>	Format of passwords found in the leak, if applicable, such as: plaintext, hashed, none, both.
<b>Password Hash Formats</b>	If the leak contains hashed passwords, this field will display what hashing algorithm is used, if known. Examples: MD5, SHA1, etc.
<b>Associations</b>	Any entity (site, organization, country, year, etc) that is associated with the data leak. Values in this field are searchable with the leak: operator.
<b>Actors</b>	Username(s) of the original poster or actor responsible or otherwise involved in leaking the data. Values in this field are searchable with the leak: operator.
<b>Attack Types</b>	The type of attack that resulted in the data leak.

<b>Targets</b>	The target organization or company where the data originated, if known. This is generally the name of the organization(s) attacked. If known, this field will optionally return Target Name, Target Domain, Target Description, and/or Target Country.
<b>Countries</b>	Country associated with the leak; for leaks related to a country without an organization Target.
<b>Hosts</b>	Site name(s) on which the original data was hosted. Values in this field are searchable with the leak: operator.
<b>Download Locations</b>	The URL where the leak was downloaded.
<b>Original Post URL</b>	The URL of the post in which the leak was initially shared.
<b>Original Telegram Channel</b>	The Telegram Channel ID in which the leak was initial shared.
<b>Post Location Type</b>	A classification of the location on which the leak was initially shared. Examples include: forum, leak site, marketplace, messaging platform, telegram, torrent, etc.
<b>Post Vision ID</b>	The document ID of the original post in the DarkOwl Vision index, if known.
<b>Associated URLs</b>	Any additional URLs that may be associated with this leak.
<b>Leak Classifications</b>	A classification of the nature of the leak. Examples include: Combolist, Cyberwar, Politically Motivated, Ransomware, Stealerlogs, etc.
<b>Leak Size Records</b>	The total number of records contained in the leak.
<b>Leak Size Actual</b>	The actual size of the leak, once downloaded.
<b>Leak Size Advertised</b>	The advertised size of the leak, from the original post.
<b>Completeness</b>	In some cases, partial or sample data is leaked by an actor. This field will display <i>Partial</i> if it is known that the leak dataset is not complete.
<b>For Sale?</b>	In some cases, leak data is offered for sale prior to being released on the darknet by an actor. This field indicates whether the leak content was ever offered for sale, if known.  <i>Note: DarkOwl adheres to a strict collections policy guided by CCIPS best practices, and we do not purchase leak data or facilitate criminal activity.</i>
<b>Filetree</b>	The name of the filetree document in DarkOwl Vision. Values in this field are searchable with the leak: operator.
<b>Public Reporting</b>	Any URLs, dates, or notes related to public reporting about this leak.
<b>Media Reporting</b>	Any URLs, dates, or notes related to media reporting about this leak.

## Explore: Actor

The **Actor Explore** page provides analyst-curated information about Threat Actors. Our actor database focuses on state-sponsored actors, actors focusing on cybercrime, ransomware groups, access brokers, exploit brokers and buyers, or critical infrastructure attackers. The actor information will continue to grow as we add more content and hear from our customers. If you know of a new threat actor that should be included – please let us know!

To get started, navigate to the Explore section, and select Actor from the top menu. This will bring you to a landing page of Actor baseball cards.

- Use the < > icons to page through the list.
- Use the left options to filter and sort the actor list.
- Click on a baseball card, or search for an actor using the lookup bar at the top, to go to the actor's detail page. You can look up actors by name, alias, CVE, or industry.

The screenshot displays the 'Actor Explore' interface. At the top, there are tabs for 'Actor', 'Entity', and 'Leak'. Below the tabs, a search bar prompts 'Find an actor by Name, Alias, CVE, or Industry'. A 'Compare' button is visible on the right. On the left, a 'View Actors By' sidebar lists filters: Country Targeted, CVEs, Industries, Origin, Sophistication, Specialization, Sort By, and Sort Direction. The main area shows three actor cards:

Actor Name	Sophistication	Origin	Years Active	First Seen	Status	Aliases	Specialization
Sqlety	Intermediate	Unknown	< 1	Aug 2, 2023	Active	Sqlety	Initial Access Broker
ShinyHunters	Advanced	Unknown	1	Mar 22, 2020	Active	White Dev 100, fs0c131y, Shiny Hunters, ShinyHunters	Ransomware
LockBit Group	Innovator	Unknown	4	Sep 3, 2019	Active	LockBit, LockBit Gang, LockBit Group, UNC2758, BITWISE SPIDER, GOLD MYSTIC, DEV-0396, Water Selkie, LockBitSupp, legasov, Storm-0396	Ransomware

Once you select an actor, you will go to that actor's detail page, opened to the Dossier.

## APT28

Group

FIRST SEEN  
Dec 31, 2003

Active

SOPHISTICATION

ORIGIN

Strategic

RU - Russia

SPECIALIZATION  
Espionage

Dossier

Targets - 76

Tools - 30

CVEs - 40

### Dossier

#### ALIASES

Select one or more of these aliases to research.

SednitSwallowtailGTsSSGroup 74GRU Unit 26165Blue Athena

SectorC01APT28SofacyPawn StormFROZENLAKESENAKEMACKEREL

ITG05Threat Group-4127UAC-0028BlueDeltaForest Blizzard

IRON TWILIGHT85th Main Special Service CenterSTRONTIUM

Fighting UrsaTG-4127APT 28Tsar TeamZebrocyFancy Bear

Search AllSearch Selected

#### STIX THREAT ACTOR TYPE

Nation-State, Spy

#### KEY POINTS

APT28 is a Russian state-sponsored threat group active since at least 2007. The threat group steals internal data from high-profile organizations of interest for the Russian government and sometimes leaks the data online with fabricated personas.

An actor entry may include the following tabs: **Dossier**, **Darknet Fingerprint**, **Targets**, **Tools**, or **CVEs**. Click on the name of the tab to navigate to that section; continue reading for more detail about the information contained within each tab.

Dossier

Darknet Fingerprint

Targets - 49

Tools - 10

CVEs - 4

Information included within the **Dossier** page may include any of the following:

<b>Aliases</b>	All Aliases by which the Actor is known. Click on an Alias to search within Vision for matches.
<b>Origin</b>	The country in which the Actor operates, if known.
<b>First Seen</b>	The date the Actor was first known to be active.
<b>Last Seen</b>	The date the Actor was last known to be active.
<b>Sophistication</b>	The level of sophistication at which the Actor operates, using STIX Threat Actor Sophistication Vocabulary: <i>none, minimal, intermediate, advanced, expert, innovator, strategic</i> .
<b>Specialization</b>	A categorization of the type of activity or area in which the Actor is known to participate. These values may include: <i>Cyber Crime, Data Exfiltration, Espionage</i> ,



	<i>Exploit Developer, Exploit Seller, Financial Crime, Hacker, Hacktivist, ICS Attacks, Initial Access Broker, Intellectual Theft, Phishing, Ransomware, Social Engineering.</i>
<b>Size</b>	Identification of whether the Actor is an individual entity, a group, or unknown size.
<b>Key Points</b>	A brief narrative description. This section may also include any known <b>Law Enforcement Activity</b> , if applicable.
<b>Stix Threat Actor Type</b>	A categorization of the type of Actor, using STIX Threat Actor Type vocabulary: <i>activist, competitor, crime-syndicate, criminal, hacker, insider-accidental, insider-disgruntled, nation-state, sensationalist, spy, terrorist.</i>
<b>Contact Details</b>	<ul style="list-style-type: none"> <li>• <b>Email</b> addresses that have been associated with the Actor.</li> <li>• <b>Tox</b> IDs that have been associated with the Actor. Tox is a peer-to-peer instant messaging platform.</li> <li>• <b>Jabber</b> addresses that have been associated with the Actor. Jabber uses the XMPP protocol.</li> <li>• <b>Telegram accounts</b> that have been associated with the Actor.</li> <li>• <b>Discord accounts</b> that have been associated with the Actor.</li> </ul>
<b>Cryptocurrency</b>	<b>Bitcoin, Ethereum, or Monero</b> wallets that have been associated with the Actor.

Information included within the **Darknet Footprint** tab may include any of the following:

<b>Operations</b>	<p>Places on the darknet or messaging platforms that are known to be run by the actor. Click on the <b>Search</b> button to begin researching within a channel or domain.</p> <ul style="list-style-type: none"> <li>• <b>Channels:</b> Telegram or Discord channels the Actor is known to operate or administer.</li> <li>• <b>Domains:</b> Darknet or other websites the Actor is known to operate or administer.</li> </ul>
<b>Data Leaks</b>	Data leaks or breaches within the DarkOwl Vision dataset the Actor is known to have leaked. Click on the <b>Search</b> button to begin researching within a data leak.
<b>Presence</b>	A list of Forums and/or Markets on which the Actor has been observed.

Information included within the **Targets, Tools, and CVEs** pages includes:

<b>Targets</b>	Industries and Organizations (or type of organizations) the Actor is known to have previously attacked. Clicking on a target will show other Actors in our database that have targeted the same industry or organization.
<b>Tools</b>	A list of known software Tools the Actor has used to carry out attacks. Clicking on a tool will show other Actors in our database that have used the same tool, and



	have an option to <b>Compare</b> them. The Compare functionality will show the timelines of each actor, as well as collisions in profile data.
<b>CVEs</b>	<p>A list of known CVEs (Common Vulnerabilities and Exposures) the Actor has used to carry out attacks. Clicking on a CVE will show other Actors in our database that have exploited the same CVE, and have the option to <b>Compare</b> them.</p> <p>Additionally, you can use the three dot drop-down menu to:</p> <ul style="list-style-type: none"><li>• <b>Search in Vision</b> to begin researching a CVE within the DarkOwl Vision dataset.</li><li>• <b>See in Mitre</b> to open a new browser tab and read more about the CVE from Mitre’s cve.org website.</li></ul>

### CVEs

Click on a CVE to learn more.

1 CVE-2021-35464

2 CVE-2015-2291

See in Research

See in Mitre

Compare

Actors Using CVEs

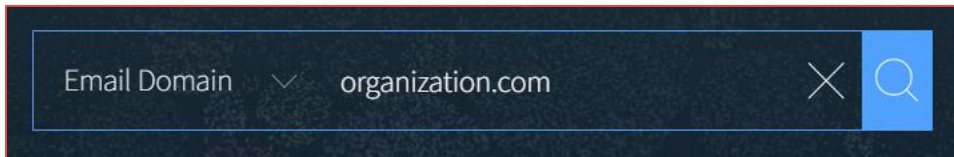
Gold Melody >

Oktapus >

## Explore: Entity

The **Entity Explore** page allows you to look up six Entity types (**Email Domain, Email Address, Credit Card, Bank Identification Number, IP Address, or Cryptocurrency**) and view information about that entity in our overall dataset.

To get started, use the drop-down to select a type of Entity, and then type the specific value in the look up bar. You can decide to click the search icon at this point, or you can use the Filter menu to apply additional parameters before you submit the query.



Once you do a look up, you will see the first page of results. *If there are more results, the left arrow will be active; click the left arrow to see the previous page.* The screen will display several sections:

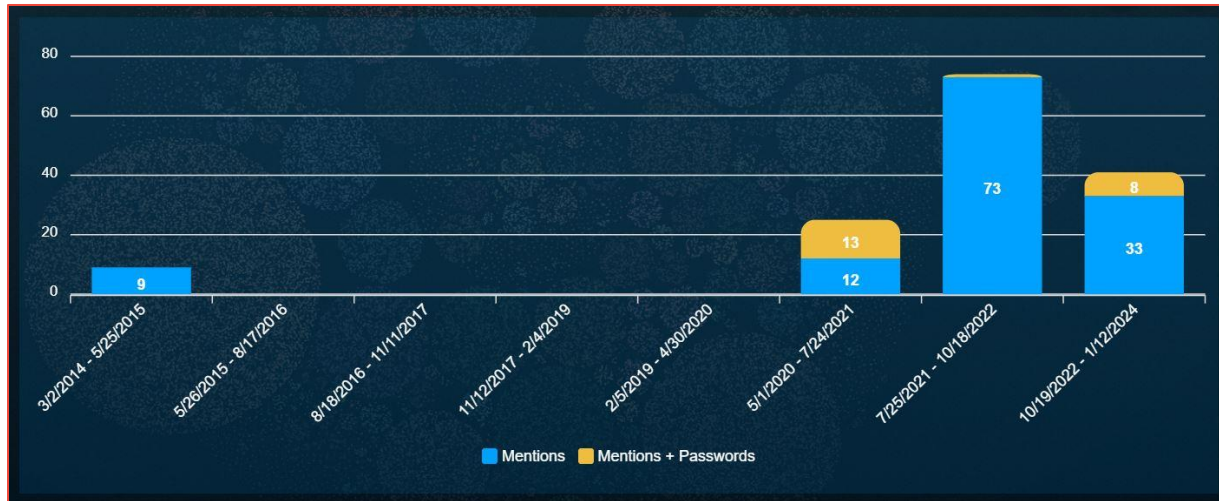
- Date Range, Total and Unique results found during Date Range
- Timeline of result set found during Date Range
- Summary information for the result set
- Itemized entity result list

### Timeline

The **Timeline** will plot mentions of that entity found in our dataset over time. BIN, Credit Card, Email Address, and Email Domain display Stacked Bars, to indicate whether the entity was a 'mention only' (blue) or a 'mention + details' or 'mention + password' (yellow).

- **For BINs and Credit Cards**, the yellow part of the bar indicates the card was found with either a CVV or expiration date.
- **For Email Addresses and Email Domains**, the yellow part of the bar indicates the email address was found with a password (either plaintext or hashed).

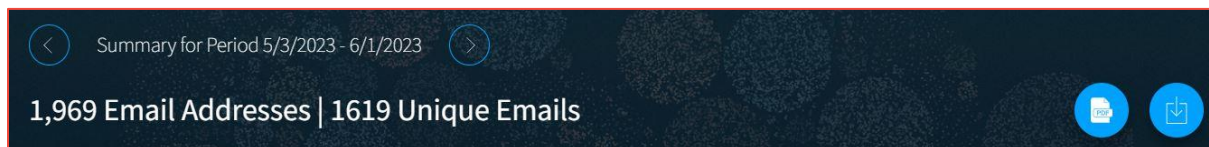
If there are more than one page of results, you can use the left Arrow action button to see previous results. *If the left Arrow is not active, there are no additional results.*



You can click on any of the bars on the Timeline to filter to that result set. You'll note when you do, the bottom of the page updates its information for just that result set shown. Click the Clear Filter button to reset to the original result set at any time.

### Action Buttons

- **Left Arrow:** See the previous page (reporting period) of results; *if this arrow is not active, it means there are no additional results*
- **Right Arrow:** See the next page (reporting period) of results
- **Download PDF:** Download a PDF report of the reporting period results; *available for Email Domain and Email Address entity types*
- **Download CSV:** Download a list of results; *available in active client accounts*
- **Reset:** Clears any filters selected and shows all results within the reporting period



### Summary Information

This section will show boxes with various result set facets. Most items in these boxes act as can be selected as filters, to narrow your result set list below. Note: if there are more than 10 items, you can scroll to see the full list. All entity types will show the following summaries:

- **Sources:** The breakdown of results found within each network and/or data leak content.




Some types have additional summaries, as indicated below.

- **Card Details:** (BIN and Credit Cards) Shows the breakdown of unexpired cards, cards with cvv and/or exp date, and cards without details.
- **Data Leaks:** (Email Address and Email Domain) Shows the breakdown of emails found by individual data leak.
- **Password Details:** (Email Address and Email Domain) Shows the breakdown of emails found with plaintext password, with hashed password, and without password.
- **Password List:** (Email Address) Shows a list of all plaintext passwords in the result set.

Password Details		Data Leaks		Sources	
With Plaintext Passwords	294	250k USA SSN with Bank Information	9	Data Leaks	2,034
With Hashed Passwords	0	2896 LOGS REDLINE STEALER	5	Cleartnet/Deep Web	2
Without Passwords	1,744	600 Dumps - 145Gb / 2022-2023	2	Onion	2
		929K ComboList	6		
		Blueocean	2		

Entity Result List

This is a list of itemized results, based on any filters you have applied. You can click on the (1) left arrow to see metadata collected with the entity, or (2) `See Full Result` icon to go to the Research section to go to the original document from our indexed document collection.

Crawl Date	Email	Password	Type	See Full Result
> 10/7/2024	[redacted]@cisco.com	[redacted]	plain	 2
> 10/7/2024	[redacted]@cisco.com	[redacted]	plain	
> 10/7/2024	[redacted]@cisco.com	[redacted]	plain	

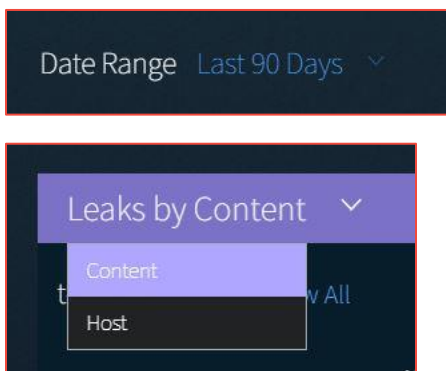
## Explore: Leak

The **Leak Explore** page allows you to search for and view analyst-curated information about the data leaks or breaches included in the DarkOwl Vision dataset. To get started looking up leaks, you can start typing in the Search Bar, or you can use the Filter options on the left to View Leaks by Attack Type, Content, or Countries.

### All Leaks

The charts at the top of the page provide information about the leak dataset overall, including the volume of leaks, recently added leaks, leaks by country, and leaks by content. Clicking on **View All Charts** will bring you to an expanded visualization section showing *Leaks by Content*, *Leaks by Host*, and *Leaks by Country*.

- Use the drop-down to change the time period shown in the charts.
- Toggle between *Leaks by Content* and *Leaks by Host*, by selecting the drop-down on the top chart.



### Individual Leaks

Clicking on an individual leak on the table will bring you to the detail page for that leak. This provides information from the DarkOwl analyst team that gives additional enrichment regarding the leak, and may include relevant dates, content information, and target information. It includes the same fields as the Leak Context feature, which is available on leak search results. Individual leaks also include actions, which include:

- Viewing the filetree in the Research section, if available
- Viewing the data in the Research section
- Downloading the Leak Context for this leak
- Clipping a link to this leak entry
- Pivoting to the Actor Explore page, if an Actor entry is available
- Pivoting to the original post or Telegram channel, if available

HostAfrica.co.za

Names

Email addresses

Account information

User accounts

Phone numbers

IP addresses

Company Names

HostAfrica

ZA - South Africa

Medusa Team, zxcv16

Jan 19, 2024

Summary

View File Tree

View Leak Data

Date Added: 2024-01-19 | Date Breached: 2023-05-23 | Date Available: 2023-09-10

Associations:

Medusa

2023

OSINT without borders

South Africa

HostAfrica

Nullified

Ransomware

hostafrika.co.za

Data purported to be from Host Africa was posted on Nullified, a hacking forum, on September 10th, 2023. According to the post, HostAfrica is a data service provider headquartered in Cape Town, South Africa. Data exposed includes names, company names, email addresses, and other associated account information. Analyst Note: A high level review of the data indicates that the leak also includes customer information from Kenya, Mozambique, Tanzania, and Uganda. Analyst Note 2: The password for the file is listed as OSINT\_without\_borders, indicating the source of the leak is the OSINT without borders team. This team is known to announce content from the Medusa Ransomware Group. Review of the Medusa Blog resulted in a victim page for HostAfrica from May 13, 2023, supporting this data leak is a repost from the original ransomware victim page on the Medusa Blog.

Country

ZA - South Africa

Actors

Medusa Team , zxcv16

Attack Type

Ransomware

Hosts

PixelDrain.com

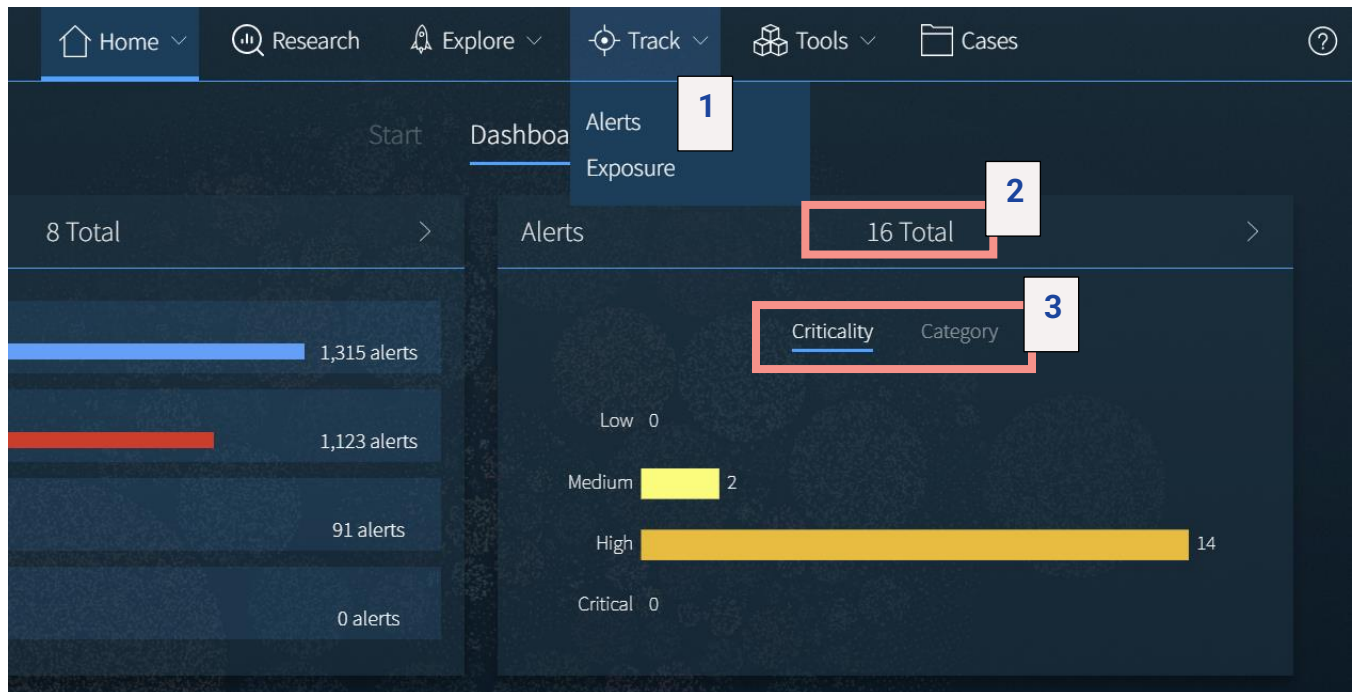
DarkOwl Vision User Interface Guide | 26 November 2024 | VERSION v3

42



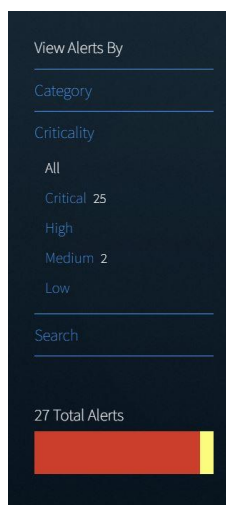
## Track: Your Alerts

Access your **Track: Alerts** page from the top navigation (1), or the Alerts widget on the Dashboard. Alerts are results found by your automated saved searches. Your Alerts dashboard will display the total number of active Critical, High, Medium, and Low results (2). If you have created categories, you can toggle the view to display by Criticality or Category (3).



## Alerts Page and Viewing Alerts

The Alerts page will display your result list. Each entry will include an excerpt from the result (around the first keyword match, if applicable), the location where the result was found, the Saved Search name, the Alert date, hackishness, and relevance of the result.



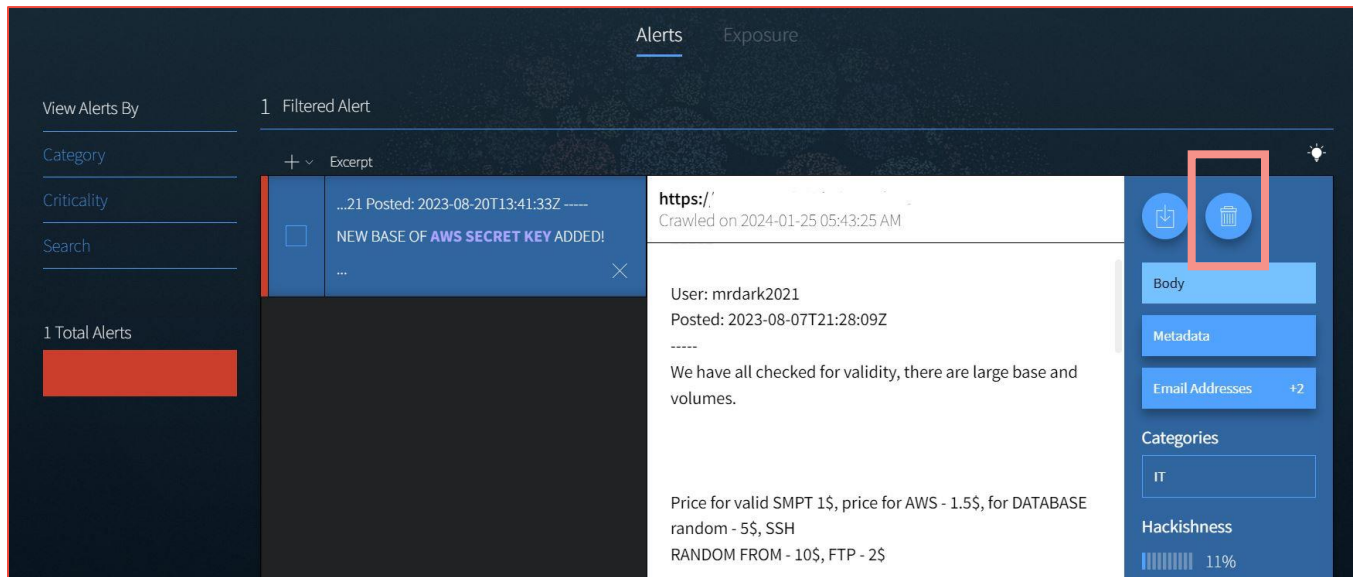
Use the Filter By menu on the left to view Alerts **by Category, by Criticality, or by Search Name.**



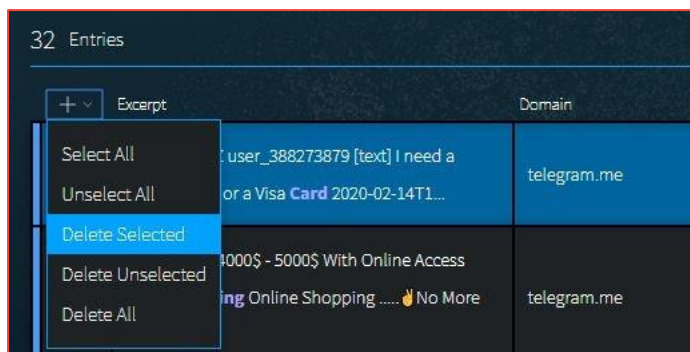
## Deleting Alerts

Once alerts are reviewed and no longer needed, you can delete them from your result set. You can delete alerts in several ways:

- **Delete an individual alert** from the Result detail: Click the **Trash icon** in the upper right corner of the alert result, then confirming on the modal.



- **Delete Selected alerts** (one or more): Check the boxes in the Alert list next to the alerts you want to delete. Then use the Action drop-down list and choose *Deleted Selected*.



*Note: You may experience a browser delay when deleting multiple alerts, or alerts large in size.*

- **Delete Unselected alerts** (one or more): Check the box next to the alerts you want to keep. Then use the Action drop-down list and choose *Deleted Unselected*.
- **Delete All alerts** (bulk), using the Action drop-down list, and confirming on the modal.

## Track: Your DARKINT Exposure Scores

**DARKINT Exposure** tracks your organization's DARKINT score over time, based on the quantity, quality, and freshness of exposed data. Scores are generated with privacy-compliant data points, requiring only a website and email domain to calculate. Increasing scores may correlate to heightened risk profiles. Tracking scores over time, changes can indicate progress in hardening security, or alert to the presence of breaches or data leaks.

Access your **DARKINT Exposure** page from the Track menu, or from the Dashboard widget.

### The DARKINT Score Formula

The algorithm focuses on specific DARKINT sources for unique matches on an organization's website and email domains, and adjust the results based on hackishness. Hackishness is the most critical input to the score, as it eliminates uninteresting content hits. We find it critical to differentiate between overall hits and hackish hits; simply because a piece of information is found on the darknet does not necessarily make it problematic to an organization.

Recent results within the last 90 days are given the most weight, as recent breaches or data leaks containing an organization's proprietary information are often more useful to hackers, and potentially haven't yet been mitigated. *Note: Scores are logarithmic, meaning every point reflects almost triple the profile of a single point less.*

$$\text{DARKINT SCORE} = H_{90}(\ln \text{RDS} + \ln \text{RTS}) + H_{\text{ATR}}(\ln \text{ATR})$$

- $H_{90}$  = Hackishness of last 90 days results
- $H_{\text{ATR}}$  = Hackishness of all time Data Leak results
- RDS = # results from Darknet Sites
- RTS = # results from Transitory Sites
- ATR = # results from all time Data Leak results

### Setting Up a Score

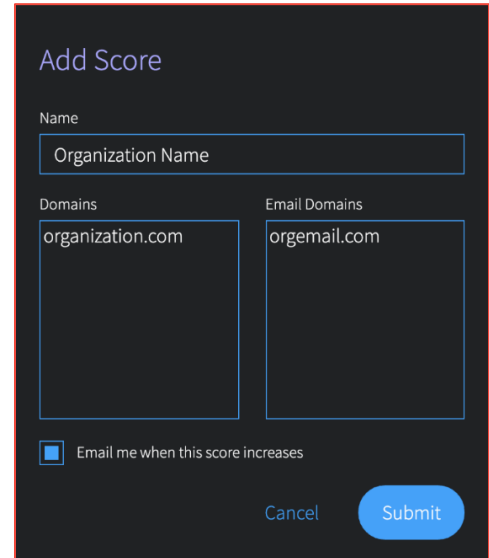


Create a score by clicking on the **+** icon on the left side of the table.

In the Add Score modal:

1. Type the Name that will be displayed in your score list.
2. Add one or more domains and subdomains, if any.
3. Add one or more email domains and subdomains. Only the domain portion is required; the @ symbol is not necessary.
4. If desired, check the box to receive email notifications when your score increases.
5. Click Submit.

At initial setup, scores will be generated for the previous month, and will continue to generate weekly.



The 'Add Score' modal form is displayed. It has a title 'Add Score' in blue. Below the title is a 'Name' field with a placeholder 'Organization Name'. Underneath are two columns: 'Domains' and 'Email Domains'. The 'Domains' field contains 'organization.com' and the 'Email Domains' field contains 'orgemail.com'. At the bottom left is a checkbox labeled 'Email me when this score increases'. At the bottom right are 'Cancel' and 'Submit' buttons.

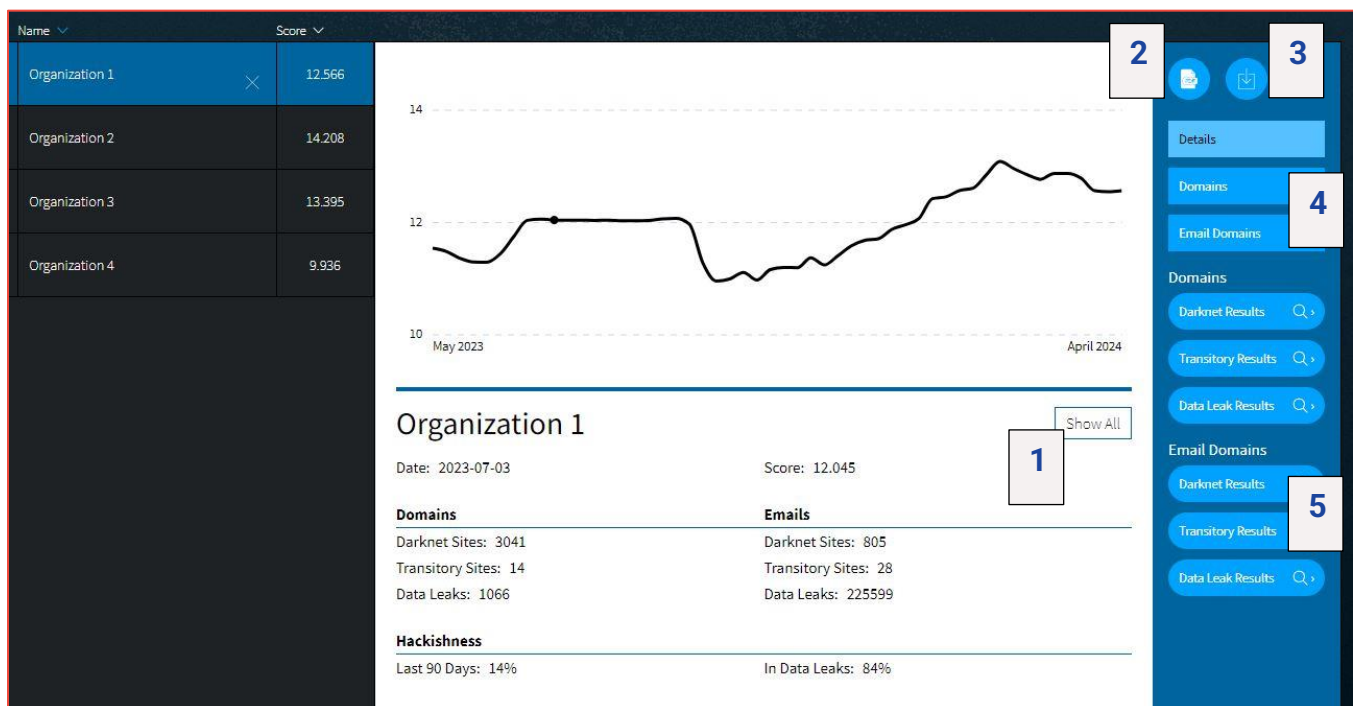
### Viewing Scores

Once you have set up scores, you will see them in the main table. For each score, the main table displays the current score, when it was last run, the change from the previous score run, as well as a trend line. Click on any row in the table see details for that entry.

+ ▾	Name ▾	Score ▾	Change	Trend	Last Run
<input type="checkbox"/>	Organization 1	4.770	▼ -0.026		2021-11-12
<input type="checkbox"/>	Organization 2	5.051	▲ 0.257		2021-11-12

Within the score detail view, hovering over the different points on the visualization will display the score inputs below the visualization.

1. Select the **Show All** button to compare the current organization with others that are set up.
2. Click the **Report** icon to generate a PDF Exposure Score Report.
3. Click the **Download** icon to download a CSV of all the scores and associated inputs that were generated for this organization.
4. Click the *Domain* and *Email Domain* buttons to see the inputs used in the formula.
5. Click the search buttons below Domains or Email Domains to see the underlying results that generated the score.



## Tools: Saved Searches

Access your **Saved Searches** page from the Tools menu. Click on a Name to open the Search Detail. Here, you can:

1. Change the name or categories associated with the search
2. Enable/disable automated searching
3. Adjust the run frequency or desired criticality of Alerts from the search
4. Run the search, or make edits to the search (see next section: Editing a Saved Search)
5. View Alerts from the search (if any)

The screenshot shows the 'Search' detail page for a saved search named 'CCNs on Telegram'. The interface includes a left sidebar with a list of saved searches: Bitcoin Regex, CCNs on Telegram (selected), Cisco Emails, CVE Exploit Mentions, and IRC Channel Mentions. The main area contains fields for 'Name' (CCNs on Telegram) and 'Categories'. Below these are checkboxes for 'Automate search' and 'Email me when this search finds alerts'. The 'Interval' section has buttons for 6 Hours, 12 Hours, 24 Hours, and Week. The 'Criticality' section has buttons for Low, Medium, High, and Critical. On the right, there are buttons for 'Run Search', 'Edit Search', and 'Alerts', along with 'Last Run' and 'Next Run' timestamps. Numbered callouts indicate: 1. Name field, 2. Automate search checkbox, 3. Interval buttons, 4. Run Search button, and 5. Alerts button.

## Editing a Saved Search

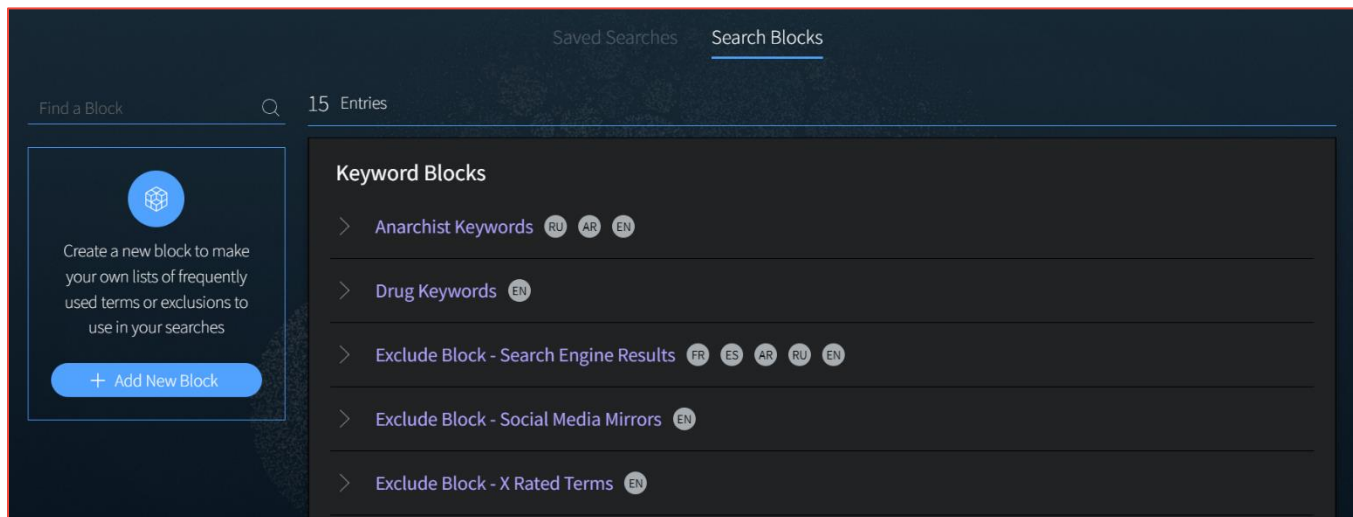
From the Saved Searches page, choose the search you'd like to adjust, then click **Edit Search**. This will bring you to the Research page, with your current search pre-populated in the search bar. From here, you can make changes to your search, updating filters, adding keywords, etc. Once you have made adjustments, run the search.

The **Saved Search icon** (star icon) will appear, this time with a Replace option for the search you're updating. Click **Replace** to confirm.

The screenshot shows a 'Replace' dialog box. At the top, there are icons for a star (Saved Search icon), a globe, and a search icon. Below the icons, there are two tabs: 'Save New' and 'Replace' (selected). The main area of the dialog has a text input field containing 'My new saved search'. At the bottom, there are two buttons: 'Cancel' and 'Replace'.

## Tools: Search Blocks

This page allows you to manage your Search Blocks library. Pre-built blocks include curated keyword lists, as well as blocks that help you exclude terms; any of these pre-built blocks can be modified to make a new customized Search Block with terms you select.



### Creating a Search Block

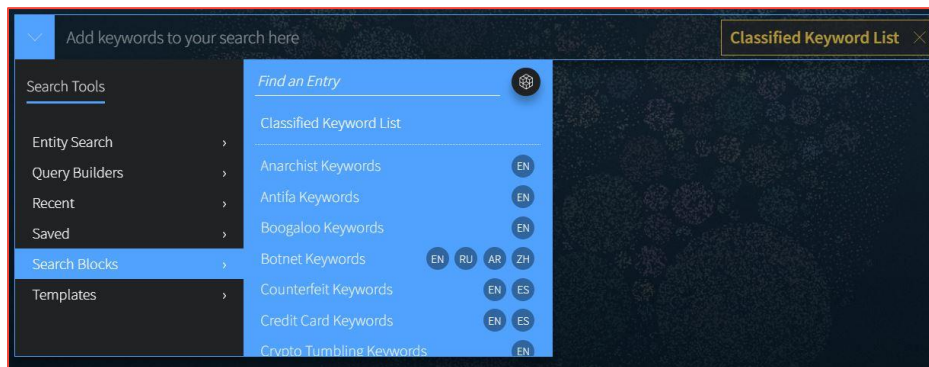
1. Click **Add New Block**.
2. Open the Select a Block Type drop-down, and choose one of:
  - **Free Text:** Accepts the same inputs and formatting (Booleans, operators, etc) as accepted on the search bar. Credit Cards can be lists of individual credit card numbers or BINs. *Note: When entering BINs, use a trailing wildcard after the first six numerical digits.*
  - **Cryptocurrencies:** Enter cryptocurrency addresses. Supported types include Bitcoin, Ethereum, Monero, Litecoin, Dash, ZCash.
  - **CVEs:** Enter full CVE-ID numbers, CVE-ID numbers, or CVE years.
  - **Emails:** Enter email addresses, email domains (without the @ portion), or email subdomains.
  - **IP Addresses:** Enter IPv4, IPv6/IPv6 compressed, or CIDR ranges for IPv4 and IPv6.
  - **Social Security Numbers:** Enter SSN input using hyphens (i.e. 123-45-6789).

- **Source Domains:** This type of Block allows you to filter or exclude content that was collected from selected domains. *Note: Use Website Mentions (below) to find domain or URL mentions within documents.*
- **Website Mentions:** Enter a list of domains or URLs.
- **Users:** This type of Block allows you to find posts or discussion from users of interest. *Note: This type matches content within Forum, Discord, and Telegram sources. To find mentions of Usernames, use the Free Text search block.*

3. Next, input your desired Block Content.

4. Finally, give the Block a Nickname and click **Submit**.

Once created, your block will now be accessible through the **Search Tools > Search Blocks**. Click on the block to add it to your query on the search bar.



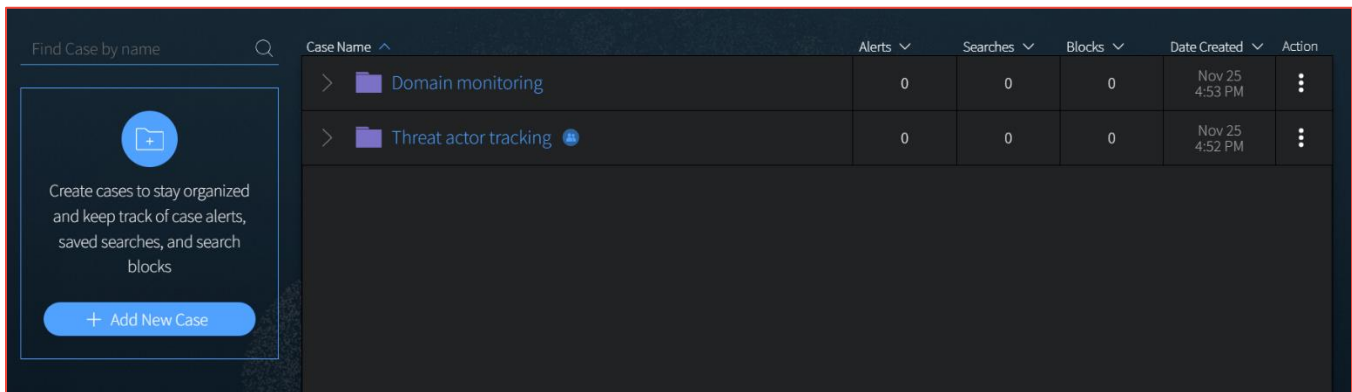
## Managing Search Blocks

- **Viewing the Content of a Search Block:** On the Search Blocks page, use the arrow to show/hide your search block content.
- **Copying and Modifying a Pre-built Search Block:** On the Search Blocks page, click the Copy icon next to the desired block. Make your revisions directly in the Block Content field, update the Block Nickname, and click Submit. This block will now appear as a new block.
- **Editing a Search Block:** On the Search Blocks page, click the Edit icon next to the desired block. Make your revisions and click Submit. If this block is used in automated searches, the next time the search runs, it will use the new block content you've specified.
- **Deleting a Search Block:** On the Search Blocks page, click the Delete icon next to the desired block. If this block is not used in any current searches, click Delete to confirm. If this block is used in saved searches, you will be prompted to go to the Saved Searches page to edit these searches to remove the block(s). Otherwise, click Delete Block and Searches to confirm.



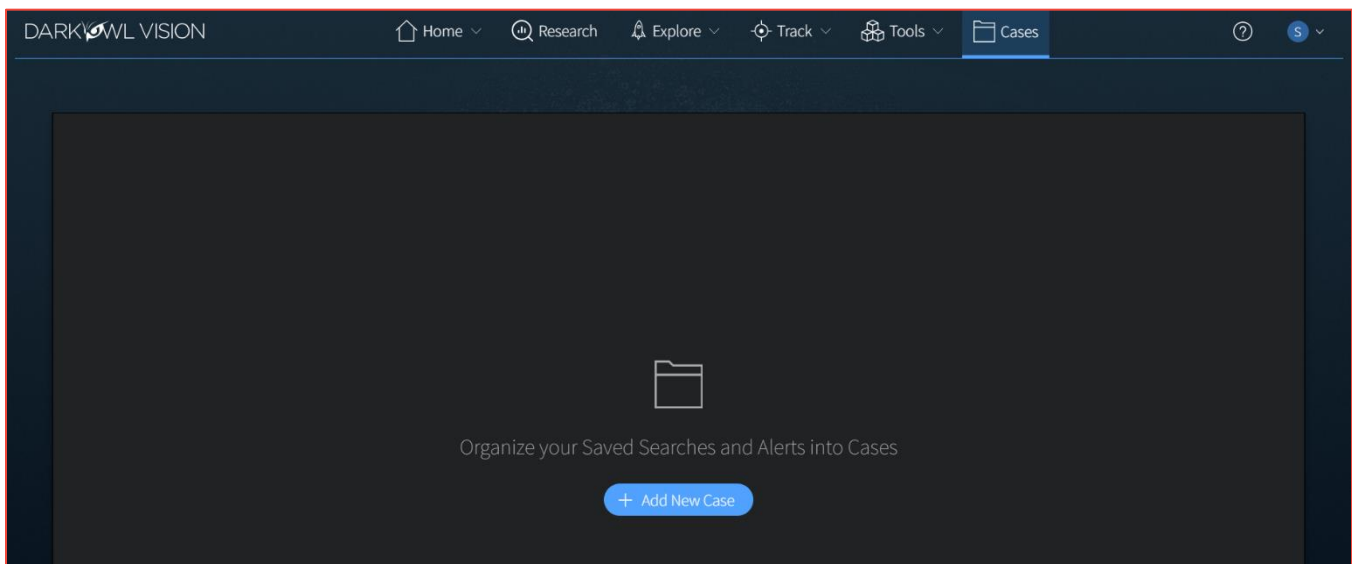
## Cases

Cases are a way to organize projects and work collaboratively in DarkOwl Vision UI. They can help you keep track of a specific topic or assignment you're working on, including all related alerts, saved searches, and search blocks. You can set up Cases for yourself, or invite other Vision UI users from your organization to work on Cases with you. When a Case is shared, you'll see a Team icon next to the Case name in your main list.

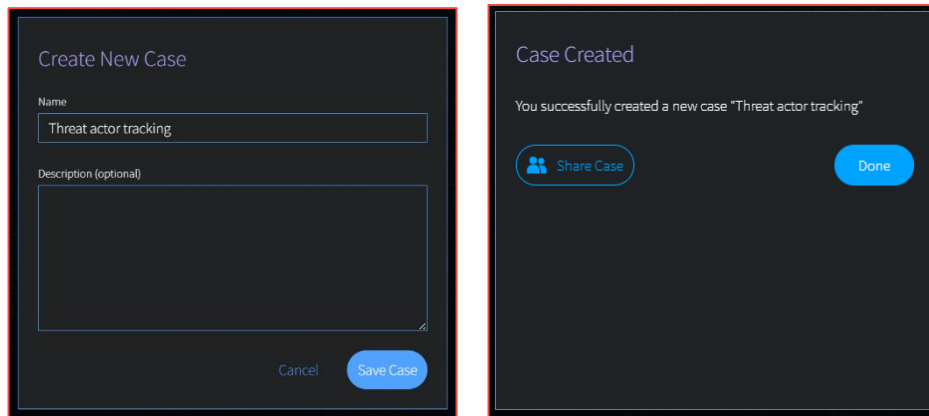


### Creating a Case

1. To get started, navigate to the Cases section, and click on Add New Case. (Once you've added a Case, the button will appear on the left side of the screen, as in the screenshot in the above section.)



2. On the **Create New Case** modal, give your Case a name, so you can easily navigate back to it. You can optionally add a description for the case; you can always update the name or description at a later time. Once you're ready to continue, click **Save Case**. A Case Created modal will appear.



3. If this is your own Case, click **Done**. If you'd like to collaborate with another Vision UI user in your organization, click the **Share Case** button on the confirmation modal. You can always add members to the Case later. See the [Adding and Managing Case Members](#) section for step-by-step instructions on how to add members to a Case.
4. Once you've created a Case, you can start adding Saved Searches (or, optionally, Search Blocks) into it. Any subsequent Alerts generated from the Saved Searches within the Case will automatically appear in the case, in the Case Alerts tab. See the [Case Detail Page](#) section for step-by-step instructions on how to add Saved Searches into a Case.
5. **Case Navigation buttons** will help you quickly toggle between Cases. Click BACK to return to the main Case page. Previous Case and Next Case navigation will appear when you've set up multiple cases, enabling you to quickly switch between Case details.

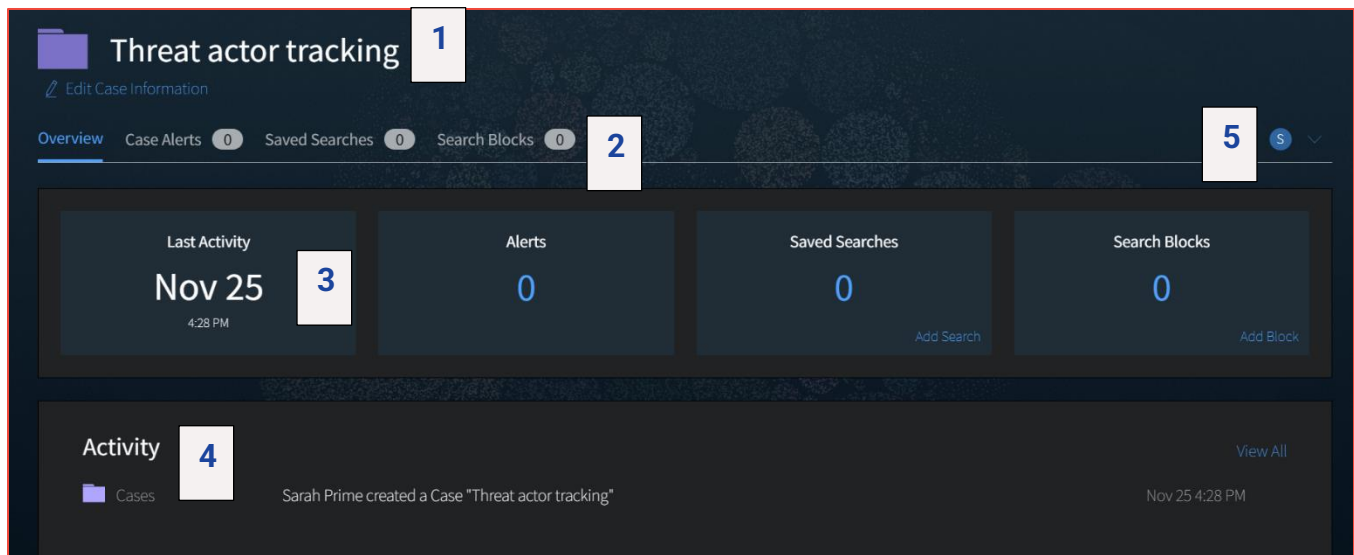


## Case Detail Page

Let's look at the elements within a Case:

1. **Case Masthead:** This will show the Case Name, as well as a Description, if you've added one. You can always update this information by clicking Add Description or the Edit button, which appears once you've input description text.
2. **Case Tabs:** Overview (default), Case Alerts, Saved Searches, Search Blocks. These tabs allow you to toggle between the different items in your Case.
3. **Summary panel:** The boxes will display the Last Activity date, number of Case Alerts, number of Searches, and number of Search Blocks associated with the Case. The Alerts, Searches, and Blocks boxes are hyperlinked to bring you directly to those sections.

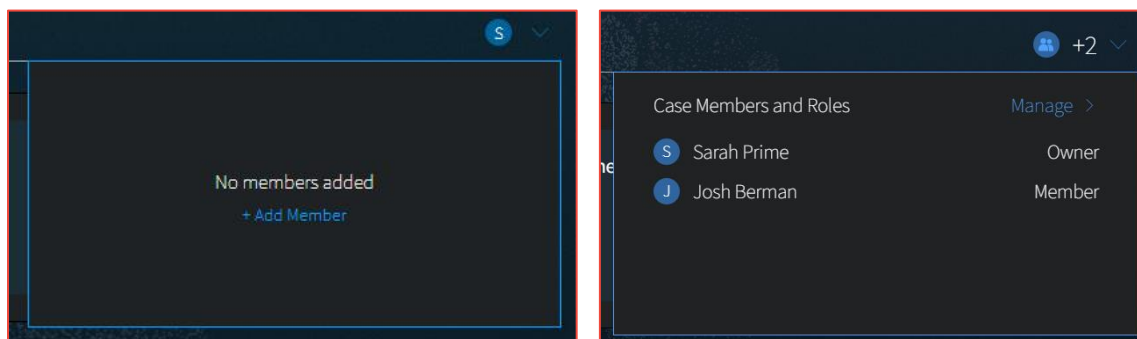
4. **Activity panel:** This section will show recent activity related to the Case. Click the View All link to see all activity related to the Case.
5. **Case Members and Roles:** This drop-down will show who is working on the Case, and allow you to add, remove, or modify member status. When a case is not shared, you will see your personal icon; when it is shared, you will see the Team icon and the number of people collaborating on the Case.



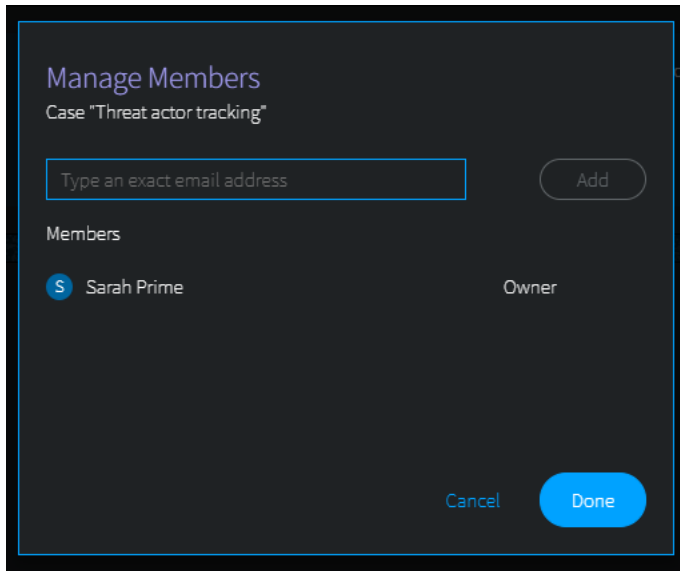
### Adding and Managing Case Members

You can opt to collaborate on Cases with another Vision UI user in your organization. Once a Case is shared, anyone with access to the Case can add, edit, or delete items in a case. This allows you to work together on keyword lists, share searches, and jointly manage a shared set of Alerts. You can click Share Case when you first set up a Case, or click on the drop-down next to the personal (or team) icon on the right side of the screen (5 in the above screenshot).

1. Click the drop-down, and then click Add Member or Manage, if members have been added.



2. This will open the Manage Members modal.



3. Type an exact email address of the person within your organization that you'd like to add to the Case, and then click **Add**.
4. When you're finished adding members, click **Done**.

#### Case Roles: Case Owner and Case Members

Each Case must have an Owner, and can only have one Owner. Anyone with access to the Case (Owner or Members) can add, edit, or delete items in a Case, including Alerts, searches, or search blocks. There are only a few functional differences between a Case Owner and Case Member. Differences include:

- Only the Case Owner can promote another member of the Case to be a Case Owner. When this happens, the Case Owner becomes a Case Member.
- The Case Owner cannot remove themselves from a Case. To do this, the Case Owner must promote another Case Member to Case Owner. Then, as a Case Member, they can remove themselves from the Case.

	Case Owner	Case Member
Add searches or search blocks into a Case	X	X
Edit searches or search blocks within a Case	X	X
Delete Alerts, searches, or search blocks within a Case	X	X
Add Case Members to a Case	X	X
Designate a Case Owner	X	
Remove yourself from a Case		X

## Viewing and Managing Case Alerts

The Case Alerts page will display all results discovered from the automated Saved Searches within that Case. Case Alerts look and function exactly as Alerts on the Track > Alerts page; the only difference is that a Case Alert was generated from a Case Saved Search, and is organized into the Case automatically.

The screenshot shows the 'Threat actor tracking' interface. At the top, there's a header with 'Threat actor tracking' and a '+ Add Description' link. Below this, a navigation bar shows 'Overview', 'Case Alerts' (with 16 items), 'Saved Searches' (with 1 item), and 'Search Blocks' (with 0 items). The main content area is titled '16 Filtered Alerts'. On the left, there's a 'View Alerts By' menu with options for 'Category', 'Criticality', and 'Search'. The main table displays three alerts, each with a checkbox, a description, source, Hackishness score, alert date, category, criticality, and a search link.

Category	Criticality	Search	Excerpt	Source	Hackishness	Alert Date	Category	Criticality	Search
		Activity on Telegram	المقتل وسيم عيسى (Type: channel) Members: 34,924 ID: -1001467206666 Username: @wassim_syria) De...	Telegram Channel: المقتل وسيم عيسى	0%	2024-10-08 08:45:03 AM	CHAT	Medium	Activity on Telegram
		Activity on Telegram	tw中華民國vn越南緬甸 (Type: group) Members: 5,179 ID: -1001217223738 Username: @buybypassport) Descri...	Telegram Channel: tw中華民國vn越南緬甸	0%	2024-10-08 08:45:03 AM	CHAT	Medium	Activity on Telegram
		Activity on Telegram	Ziyaettin - Power Proofs (Type: channel) Members: 2,088 ID: -1001621040985 Username: @powerproofsz...	Telegram Channel: Ziyaettin - Power Proofs	0%	2024-10-08 08:45:03 AM	CHAT	Medium	Activity on Telegram

Use the Filter By menu on the left to view Alerts **by Category, by Criticality, or by Search Name.** Once alerts are reviewed and no longer needed, you can delete them from your result set.

## Adding a Saved Search into a Case

You can add Saved Searches into a Case using one of two methods:

- Create a new Saved Search and save it directly into a Case
- Copy an existing Saved Search into a Case

Once a search is associated to a Case, it will appear in the Case's Saved Search tab. Any subsequent Alerts generated from that Case Saved Search will appear in the Case Alerts tab.

### Create a New Saved Search and save in a Case

On the search bar, when you create a Saved Search, you can add it directly to a Case. After you run a query, the **Save Search icon** (star icon) will appear on the right side of the search bar.

Selecting that icon will open a form:

- Add a **Saved Search Nickname**.
- Select one or more **Cases** to save the search into (optional).
  - *If a Case is selected:* the search will be saved directly to that Case. If you have selected the Automate this search option below, any Alerts generated will be automatically saved into that Case as well.
  - *If a Case is not selected:* the search will be saved in the list within your Tools > Saved Searches page.
- Add **Categories** (optional). Categories can help you sort your searches and alerts.
- Click **Automate this search**, if you'd like to apply monitoring. If this is selected, additional options for Frequency, Criticality, and Email Notifications will appear.
- Click **Save** when complete.

### Copy an Existing Saved Search into a Case

You can copy a previously created Saved Search (appearing in your Tools > Saved Search list) into a Case. This will create a new version of the Saved Search in the Case; the original version will remain in your Tools > Saved Search list unless you opt to delete it. Additionally, any Search Blocks that are contained within the Saved Search will also be copied into the Case automatically.

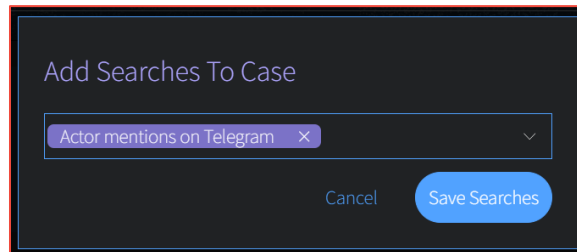
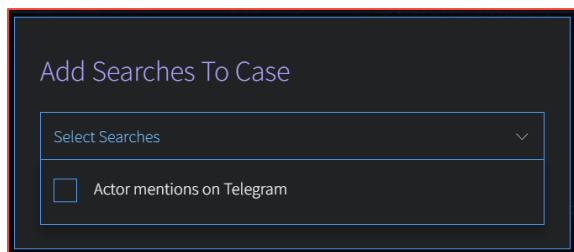
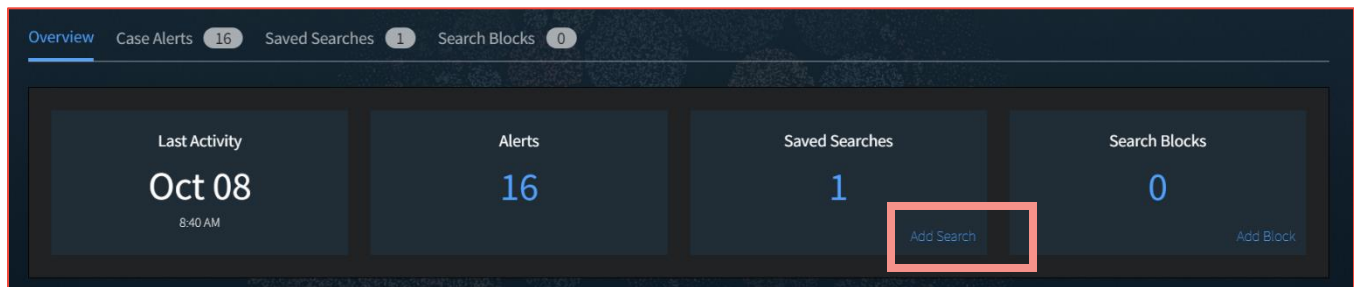
There are several ways to copy an existing Saved Search into a case:

- When you're on the Case Overview page, you can select the Add Search button.
- When you're in the Tools > Saved Searches page, you can select the Action menu next to any search to Add to Case.
- Once you have added a Case Saved Search, you can copy it into Another Case.

**From the Case Overview page:** In the Saved Search box on the Case Overview page, click on Add Search.

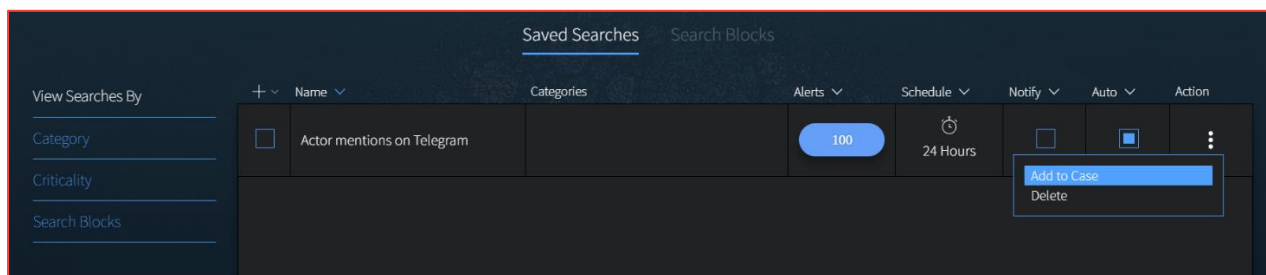
1. This will bring up a modal that includes a list of all searches from your Tools > Saved Search page
2. Select the search(es) you'd like to copy into this Case
3. Click Save Searches

*Note: After you've finished adding searches, if you only want to keep the Case version of a search, we recommend going to the Tools > Saved Search page and deleting the original search(es).*



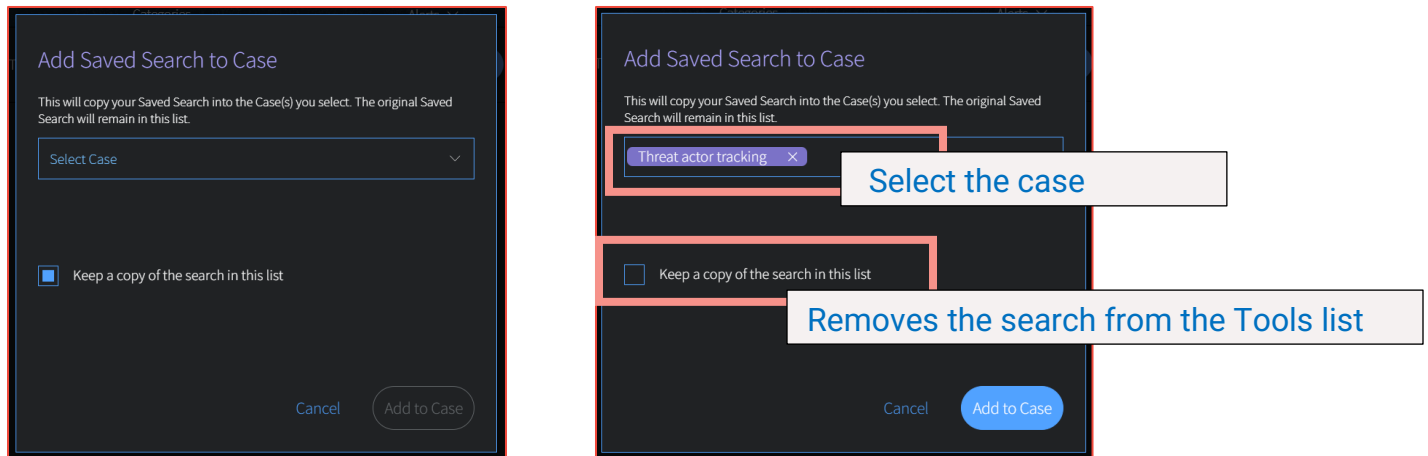
**From the Tools > Saved Searches page:** Navigate to the Tools > Saved Searches page and find the search you would like to copy into your Case.

1. Click on the Action button on the right side of the table:



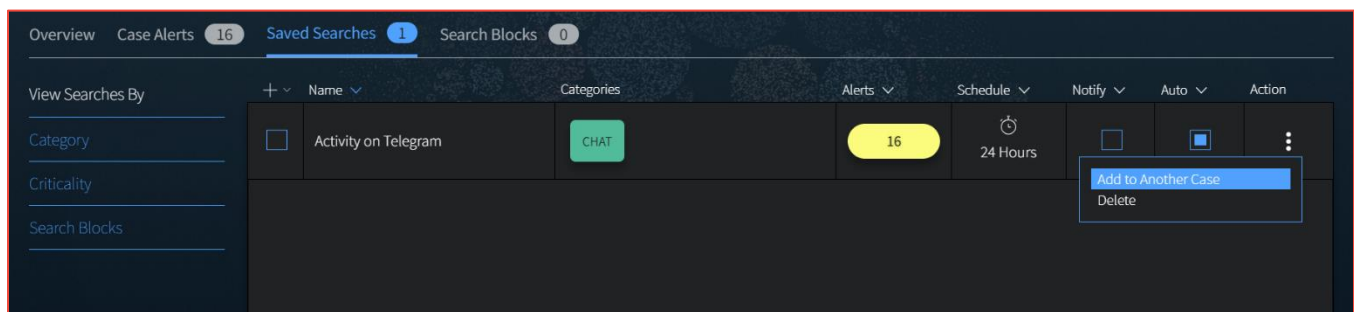
2. Select **Add to Case**, which will bring up the Add Saved Search to Case modal. Use the drop-down to Select the Case(s) you'd like to copy the search into. If you only want to keep the new copy of the search – the Case search – you can uncheck the box. This will delete the original search from this list automatically.





3. Click Add to Case. This will bring up a confirmation modal, indicating that your search has been saved successfully to the Case(s) you chose.

**From the Case Saved Search page:** Once you have added a Saved Search to a Case, you can add it to another Case. The workflow is the same as the previous section.

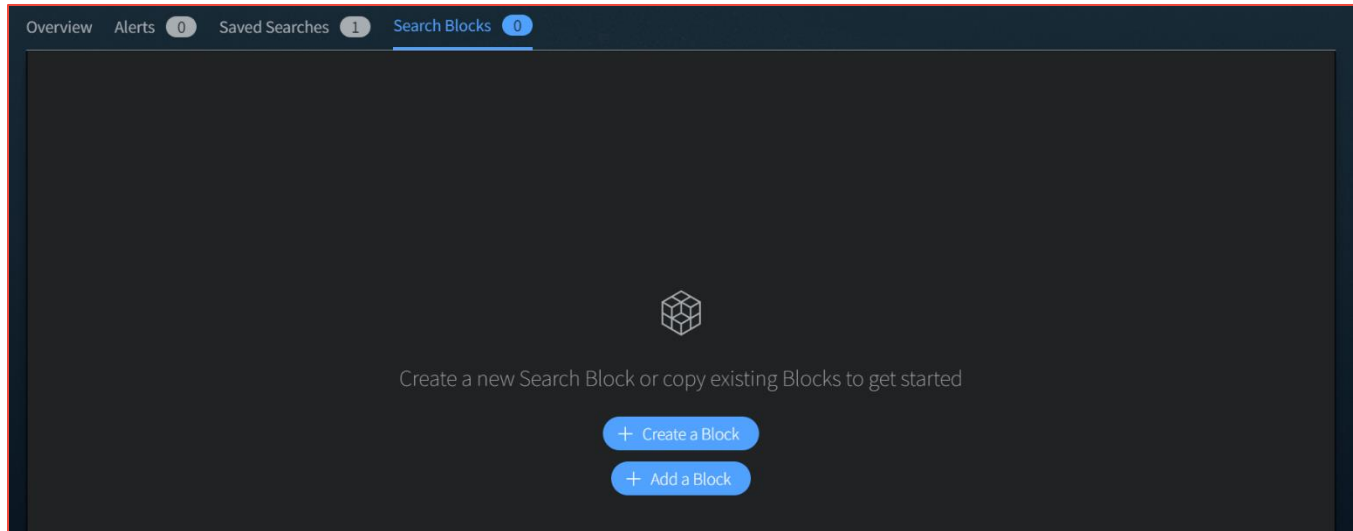


### Adding a Search Block into a Case

When you copy an existing Saved Search that contains a Search Block into a Case, that Search Block will automatically be copied into the Case. If needed, you can create Search Blocks within a Case, or copy existing personal search blocks into Cases.

### Create a new Search Block within a Case

Open the desired Case, and navigate to the Search Blocks tab. Click Create a Block. This will open the same Create a Block workflow that exists in Vision UI; the only difference is that upon saving, it will save specifically to this Case.



### Copy an Existing Search Block into a Case

There are several ways to copy an existing Search Block into a case:

- When you copy an existing Saved Search that contains a Search Block into a Case, that Search Block will automatically be copied into the Case.
- When you're on the Case Overview page, you can select the Add Block button.
- When you're in the Tools > Search Blocks page, you can select the Action menu next to any personal search block and Add to Case.
- Once you have added a Case Search Block, you can copy that search into Another Case.