DarkOwl Vision User Interface Guide

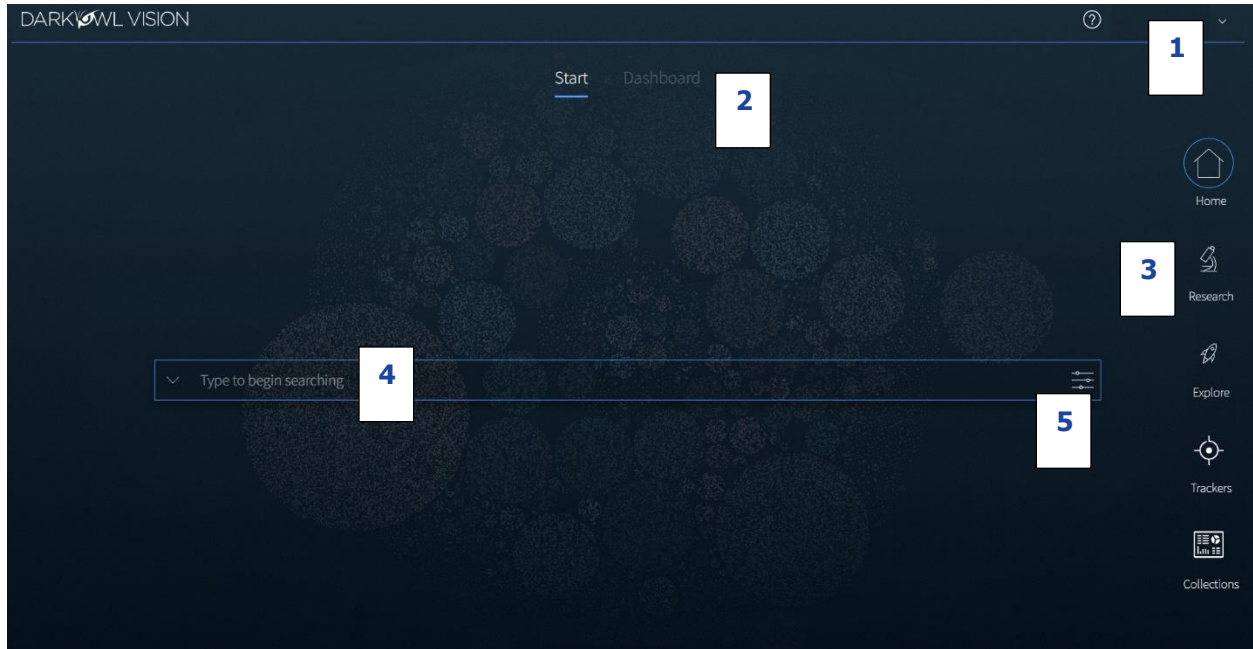## Table of Contents

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.	**Help & Account Options**	A quick link to Help resources; manage **Preferences** (Search Bar Hints, Quick Filter), **Default Views**, or logout.
2.	**Start / Dashboard Toggle**	Toggle between simple search view or your Dashboard elements.
3.	**Right Navigation Menu (see below)**	Navigate to **Research** to view search results; **Trackers** (Alerts & DARKINT Exposure); **Explore** entities; see **Collections** of Searches and Blocks.
4.	**Search Bar**	Type to begin searching or click on the arrow to open the Search Tools menu.
5.	**Filters Menu**	Create a targeted and effective search using filters, dates, and advanced options.

Home	Research	Explore	Trackers	Collections
Start / Dashboard pages	Search Results page	Entity page	Alerts / Exposure pages	Saved Searches / Search Blocks pages

Preferences and Default Views

Click on the Gear icon in the upper right corner to select Preferences to receive Search Bar Help prompts or to toggle the Quick Filter menu (in the Research section) on or off. Default Views allow you to select which page you prefer to start on within each section. For example, if you would like to log in and see the Dashboard, select the toggle for Dashboard next to Home.
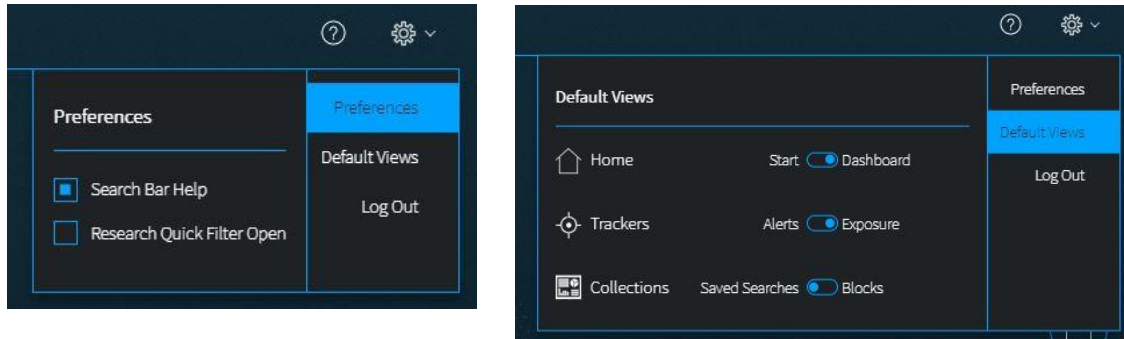
Searching

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:

   o Use Boolean operators when searching more than one keyword. See: Searching with Booleans.
   o Use quotations (**"Jane Doe"**) to send the query as one phrase, *Jane Doe*.
   o 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:
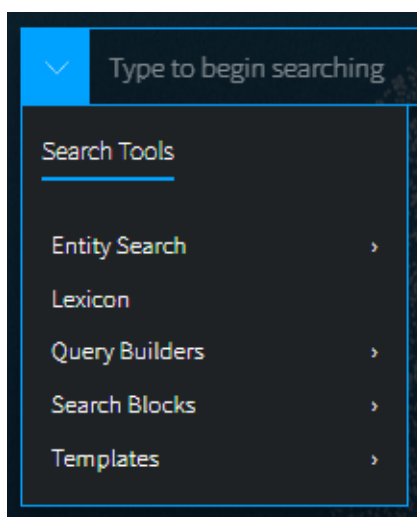
Entity Search: the best way to search for Emails, CVEs, Credit Cards, Cryptocurrency Addresses, IP Addresses, and Social Security Numbers.

Lexicon: curated lists of commonly searched items and different areas of content in our database.

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.

Once you've started searching, **Recent Searches** and **Saved Searches** will also appear in the Search Tools menu, for easy access.

3. Click on the right Filter menu to refine your search, create targeted queries, and select options. More information about these is provided in this section: Filters, Dates, Advanced Search Options.

4. **Guidelines for using multiple search components (Filters, Lexicon entries, and free text) in the same search.** Generally, using multiple *different* search components AND together; using multiple of the *same* search component (but different values) OR together:

   a. Lexicon Market, Lexicon Exploit in same search—AND
   b. Lexicon Actor, Lexicon Actor in the same search—OR
   c. Network (Tor), Network (Discord) in the same search—OR
   d. Entity Search, Search Bar Free Txt in the same search—AND

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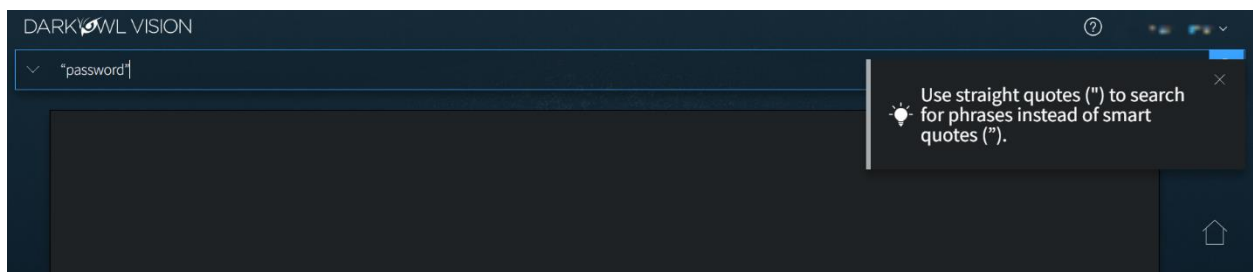
You can turn this feature off by clicking on your name in the upper right corner, selecting Preferences in the drop-down menu, and unchecking the toggle for Search Bar Help.
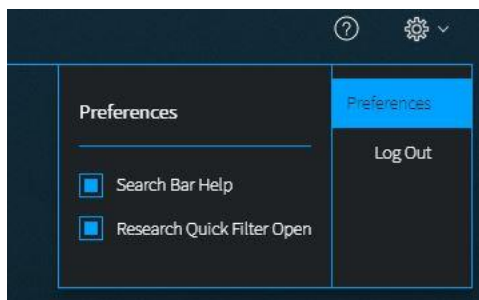
Search Techniques

Single Terms

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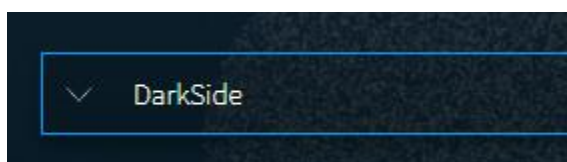
Phrase Searching

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 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 and 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 and 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:11111111111111111
- 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:(11111111111111111 OR 2222222222222222222)
- 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. (*****) is used to find *zero or more* unknown characters; (**?**) 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)

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 in proximity to each other by using quotations and selecting a maximum distance allowed: **"password hack"~2**. We support a maximum distance of 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:

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

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

- Searching within a field called 'https' (which doesn't exist) for:
  - An empty regular expression (// signifies the start and end of a regex with no content)
  - The keyword 'darkowl.com'
  - The start of a regular expression starting with 'darkint-blog'
  - 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). For example, a search of just **the word '*drugs*' in the search bar** is equivalent to: ***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 in addition to title and body, 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)**
- **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 allows you to filter to channels, IDs, or users collected from Telegram.
- The **discord:** operator allows you to filter to servers, channels, IDs, or users collected from Discord.
- The **user:** operator allows you to filter to usernames or user IDs *from either Telegram or Discord.*

Several examples are presented below:

Search	Description
telegram:"Чат Военкоров Русской Весны"	Search for content from this Telegram channel (that has spaces in its name)
telegram:"*DEMON HUB* 1 😈 ~ *#THEDEMONNETWORK*"	Search for content from this Telegram channel (that has spaces and special characters in its name)
telegram:lapsus*	Search for content from any Telegram channel or username that starts with lapsus
telegram:	
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 on Discord only
user:tylerdurdan710	Search for content associated with this username on either Discord or Telegram

Filters, Dates, and Advanced Search Options
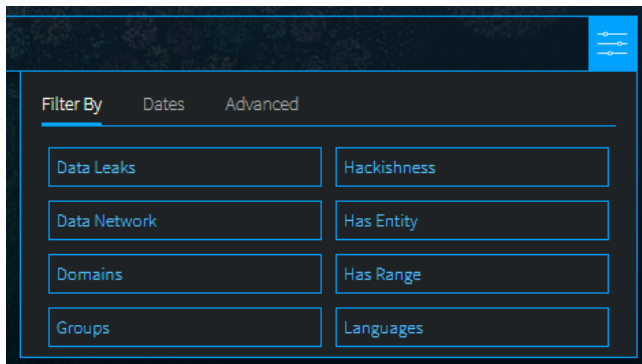
Refine your search using the Filters icon on the right side of the search bar. This includes three tabs for:

Filters

Dates

Advanced options

Data Leaks

Filter to content from known breaches or other leak data, tagged by name in DarkOwl Vision. See the Lexicon for descriptions of the Data Leaks in this list. Type or scroll to find the desired Data Leak. ***Click once to include, click twice to exclude***.

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

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, prefixing with - to exclude.

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 (such as, **arch3rsecgjqcmjb.onion**; no need for the www or http:// prefix) in the filter box. Be sure to remove any trailing slashes or paths from the domain.

- For free text searching, type *domain:domain.com* in the search bar, prefixing with - to exclude.

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 other challenges.
- *Blogs:* Filter to content from sites identified as blogs.
- *Chans:* Filter to content from a curated set of chan/imageboard forums selected by our analysts.
- *Darknet:* Filter to content from the Tor, I2P, and Zeronet darknets.
- *Forums:* Filter to content from sites identified as forums.
- *Markets:* Filter to content from sites identified as darknet marketplaces or vendor shops.
- *Ransomware:* Filter to content from known ransomware sites.
- *Paste Sites:* Filter to content from a curated set of paste sites selected by our analysts.

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]**

The above 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, prefixing with - to exclude.

Dates

Use the drop-down to quickly select a time range for search results, or select *Custom* to choose a specific start/end date.
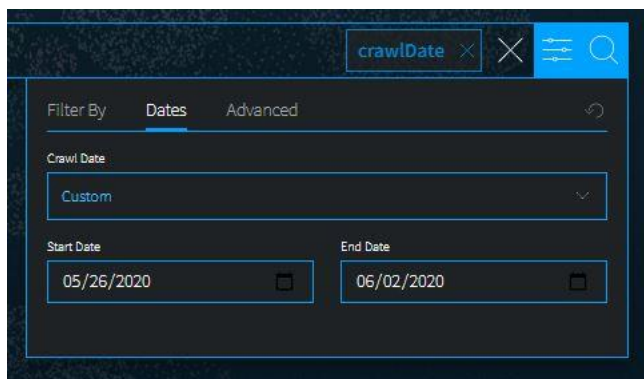
Crawl dates can be searched in the search bar as a range using the following date format: YYYY-MM-DDTHH-MM-SSZ:

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

As crawlDate 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 Similar, Empty Bodies)

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

- **Sort options.** Use the drop-down to sort your results by **_Relevance_** (default), By **_Hackishness_**, By **_Crawl Date_**
- **De-duplicate your results.** You can choose to de-duplicate your result sets or see all results, including similar results. The default is to de-duplicate result sets; 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 Any document (documents can include text in the body, or no text in the body); Results must have body field (to only return documents that had text content on them); or Results must not have body (to see only documents without text).

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 a description to populate in the search bar; if 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.
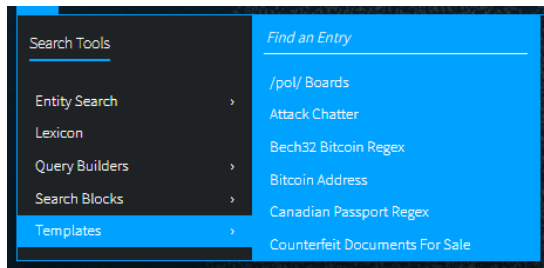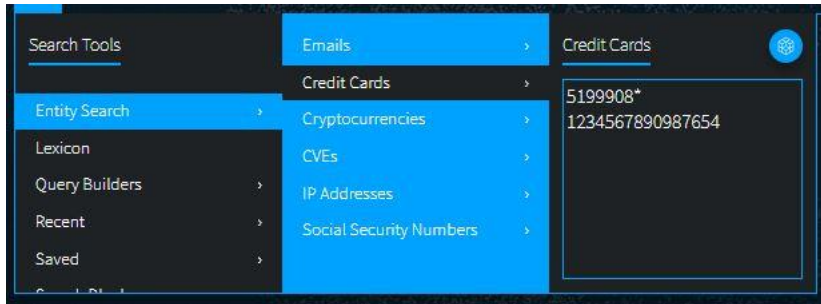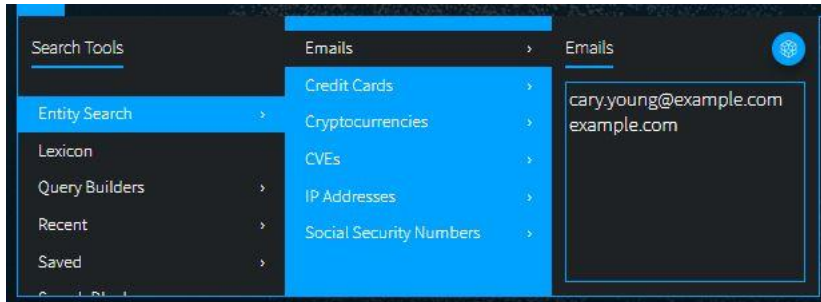

Entity Search

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, using the CVE prefix)
    - 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*.
- **Social Security Numbers** supports the following format: *123-45-6789* (with hyphens).

A note about IP entities. 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.

Lexicon

The **DARKINT Search Lexicon** includes curated lists of commonly searched keywords, domains, or data leaks, intended to help you find interesting content within our data collection. While not an exhaustive list of items in our data, it's a good place to get started. The Lexicon continues to grow as we add more content and hear from our customers. If you know of a new threat actor or darknet marketplace that's not in our list – please let us know about it at https://www.darkowl.com/lexicon.

To use the Lexicon, pick a topic on the left, then filter or scroll to find entries of interest. Selecting the box next to your desired entry(ies) will immediately add the entry(ies) to the search bar.

Topics You'll Find in the Lexicon

Section	Search Component	Description
Actors	Free Text query string	Use the Actor lexicon to find actor names mentioned within search results. Actors are malicious individuals or groups that carry out targeted attacks or campaigns, with motives ranging from political hactivism to cybercrime. Many of the actors in the Lexicon come from this list from MITRE.
		Note: with the Actor and Vendor lexicons, it may be helpful to use additional search terms to reduce false positive results with Actor names that are also common words, such as (HACK CRACK FULLZ EXFILTRATION DDOS).

| Data Leaks	Filter: Leak	Use the Data Leaks lexicon to find search results from known breaches or other leak data that are tagged by name in our data. A description of each breach is included.
Exploits	Free Text query string	Use the Exploits lexicon to find exploit names mentioned within search results. Exploits are software tools designed to capitalize on flaws in a computer system, typically for malicious purposes. Examples: trojans, malware, viruses, RATs, ransomware, botnets.
Forums	Filter: Domain	Use the Forums lexicon to find search results from known darknet and deep web forms. Forums are online places where people discuss specific topic threads. Some require authentication to access. Forums that are associated with specific markets and/or vendor reviews are indicated.
Markets	Filter: Domain	Use the Markets lexicon to find search results from known darknet market domains and vendor shops. Content includes both small, vendor-owned markets, to big-name marketplaces such as Hydra and Empire. Some marketplaces have previously been taken down by law enforcement, though our data collection may still have historical content.
Ransomware Services	Filter: Domain	Use the Ransomware Services lexicon to find search results from domains administered by ransomware gangs. Each entry includes a description of when the gang was first active, associates and affiliates, and encryption cipher used.
Vendors	Free Text query string	Use the Vendors lexicon to find vendor names mentioned within search results. Vendors are sellers of goods or services on darknet marketplaces or forums. Each vendor in the Lexicon includes markets or forums where the vendor is active.

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 (see descriptions below) and input text in the appropriate field(s), you can either **Add to Search**, or **Set Up Monitors**.

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 finds 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.

- **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).
- **Websites:** When searching for domain/URL mentions within the body of a document, we recommend this format to find variations that start with https://, or www, or any path.
- **US Phone Numbers:** When searching for phone numbers, we recommend preparing a query without spaces and with spaces between number groups. (We recommend preparing searches the same way for any phone numbers; i.e. *1234567889 OR "123 456 7889"*).

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.
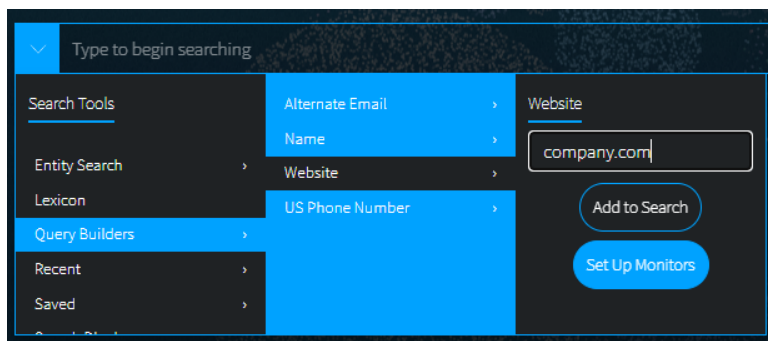

Set Up Monitors

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 next to 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. Additionally, when you update a block, all searches that use that block are automatically updated to use the new block content.
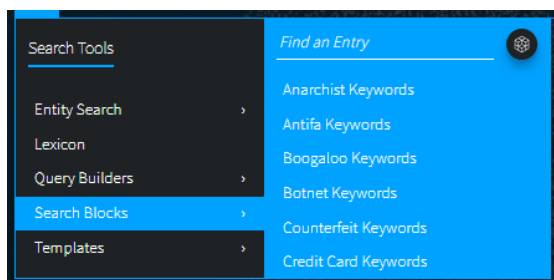
Initially you'll see a list of pre-built blocks in the Search Tools list and Search Block page, which were created by DarkOwl analysts. After you create your own search blocks, they will appear at the top of the list. Begin typing in the Find an Entry field to filter the list.

You can make search blocks in a few different ways:

- Select **Create a New Block** on the Collections: Search Blocks page.
- On the Search Blocks page, click on the Edit icon next to a pre-built block. Make modifications and save as a new block.
- 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**.
- Add **Categories**, if desired. 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.

Search Results

DarkOwl Vision collection activities are automated and continuous 24/7/365, collecting content from millions of websites daily in 52 languages. Currently, 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:

Body field	The raw text collected from the webpage/record/target.
Metadata fields	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.
Mined fields	Tokenized entities we mine out of the body of the result, which are currently Entities (*emails, credit cards, cryptocurrencies, cves, ip addresses, ssns*) and Chat-related information (*users, user IDs, servers, channels, channel IDs*). Entities and Chat Users appear as individual View Switches in Search Results, if present in the body.

Processed fields   Information we apply to a result from our natural language processing or machine learning, such as *hackishness* or *language* detection.

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 on the Expand icon, or anywhere in the Title or Excerpt columns, to open the full Result Detail; click again to close the Result Detail.

Keyboard Shortcuts

Navigate through Search Results using these keyboard shortcuts:

Key	Description
k	next result
i	previous result
l	next highlight

j	previous highlight
;	toggle detail pane
o	next page
u	previous page

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. *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.
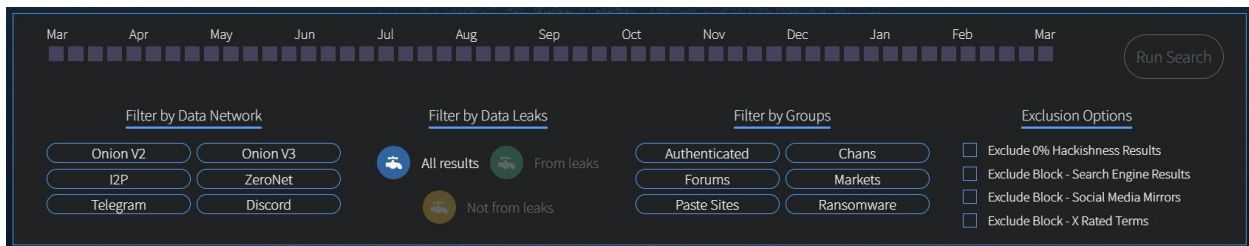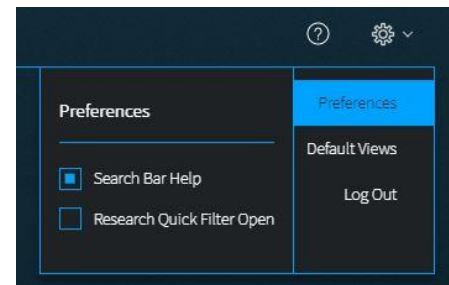
- **Crawl Date Slider.** Select a Crawl Date range within the last year, by clicking on a box to start, sliding over the date period, and clicking on an end box.
- **Filter by Data Network.** Click once to select a network; click twice to exclude a network.
- **Filter by Data Leak.**
  - Select *From leaks* to see only results from Data Leaks
  - Select *Not from leaks* to exclude results from Data Leaks
- **Filter by Groups.** Click once to select a group; click twice to exclude a group.

- **Exclusion Options.** Click to add the Hackishness filter (exclude results with 0% hackishness), or select Exclusion Search Blocks created by DarkOwl analysts, to reduce noise in result sets.

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.
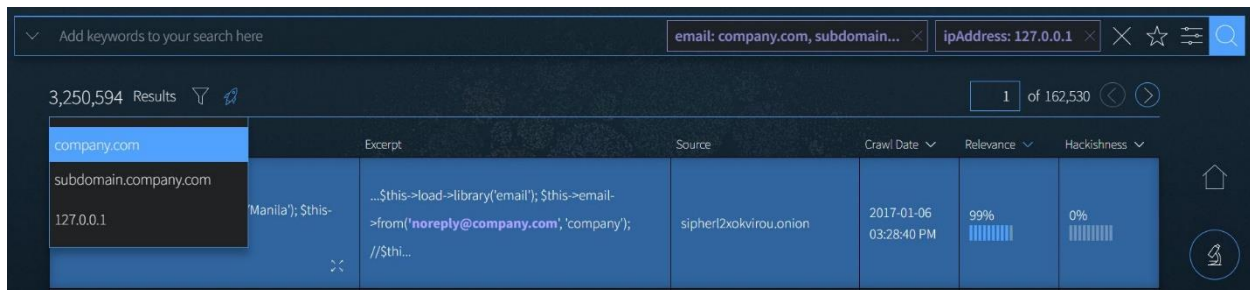
Viewing Individual Result Detail

1. **Source** of the result and when we added it to our data collection.
2. Options to **Download** the result or get a **Link** to return to this result later.
3. The right side will contain various View Switches to see the result, metadata, and various tokenized fields:
   a. The **Body** is the content of the result.
   b. **Metadata** includes where and when the result was collected.
   c. If present in the Body, additional view switches will show **Lists of Entities** within the result (Emails, Cryptocurrencies, Cards, CVEs, IP addresses, SSNs).
   d. **Leak Info** will be present if the result is from a data leak.
   e. **Chat Users** 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.)
4. A Group tag will be present if the result is from one of these types of sites: Chan, Forum, Market, Paste, or Ransomware.

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.

All entity types have Filter options to select a date range; some types have additional options, as indicated in the table below.

Entity Type	Filter Option
Bank Identification Number and Credit Card	**Card Details:** Filter to cards that were found with a CVV, with an Exp Date, or Both CVV and Exp Date
Email Address and Email Domain	**Password Options:** Filter to emails that were found with Plaintext or Hashed passwords

Once you do a look up, you will see the first page of results, and can click the left arrow to see more. The screen will display several sections:

- Timeline, Number of Entities, and Action Buttons
- 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 1 page of results, you can use the left Arrow action button to see previous results. If the left Arrow does not appear, there are no more results.
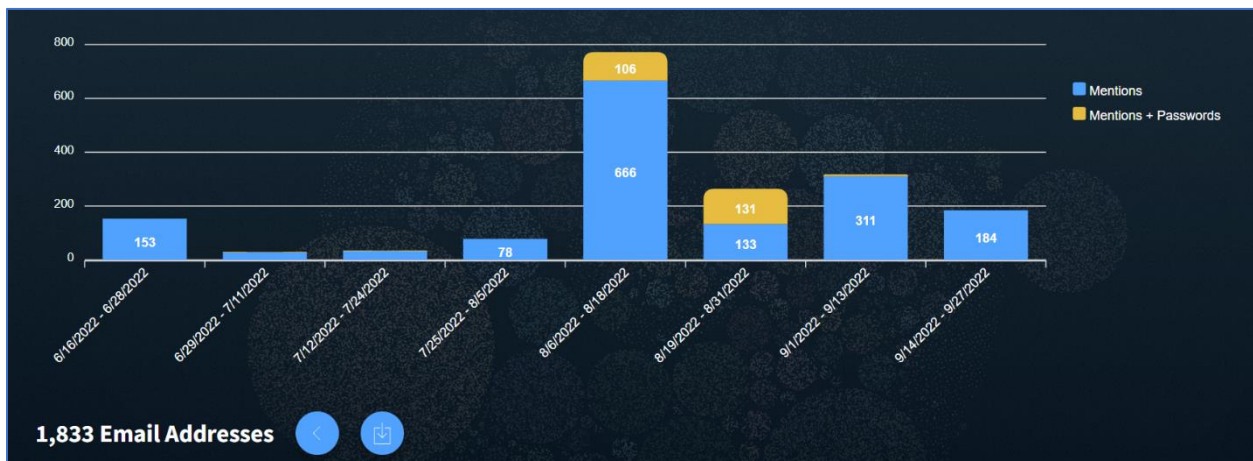
You can click on any of the bars on the Timeline to filter to that result set. You'll note when you do, the bottom of the page updates its information for just that result set shown. Click the *Clear Filter* button to reset to the original result set at any time.

Action Buttons

The Action Buttons appear next to the number of entities, and include:

- **Left Arrow:** See the previous time period of results
- **Right Arrow:** See the next time period of results
- **Download:** Download a list of results as CSV
- **Clear Filters:** Resets any filters selected

Action Buttons will only appear when the action is available (i.e. if no filters have been selected, the Clear Filters button will not appear). *Note: The download action is available to active client accounts.*

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:

- **Summary for Period** [Date to Date]: Shows the date range for the result set shown, with the number of total results. For BIN and Email Domains, also displays the number of unique results.
- **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.

Entity Result List

This is a list of itemized results, based on any filters you have applied. You can click on the `See Full Result` icon to go to the Research section to see the whole page from our indexed document collection.

Trackers: Your Alerts

Access your **Alerts page** from the Trackers right navigation icon, or from the Alerts Dashboard.

Alerts are results found by your automated saved searches. Your Alerts dashboard (1) will display the number of active Critical, High, Medium, and Low results. If you have created categories, you can toggle the view to display by Criticality or Category (2). You can also get to your Alerts directly from the Trackers right navigation icon (3).
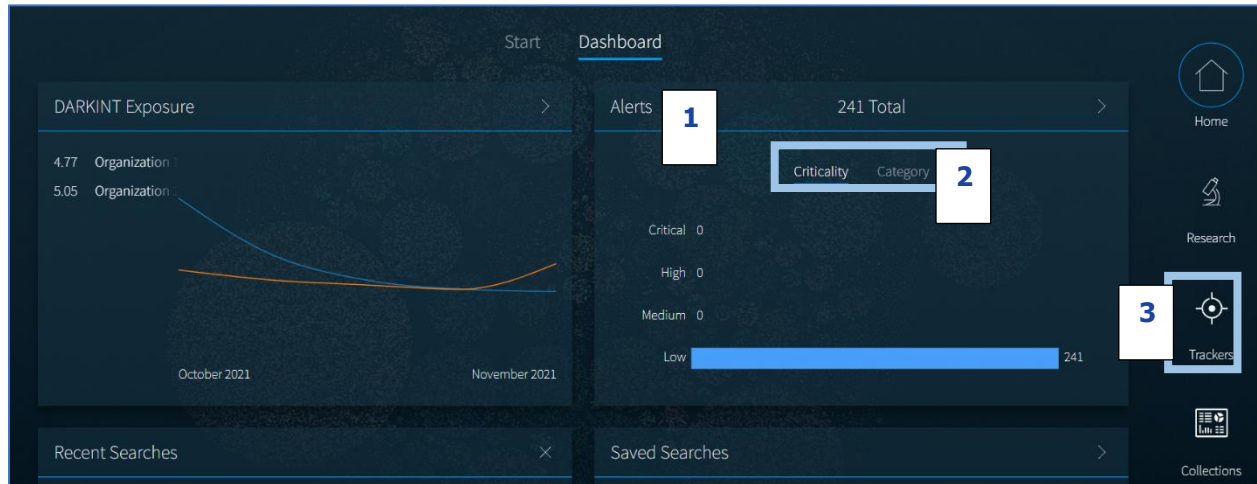
Alerts Page and Viewing Alerts

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_**.
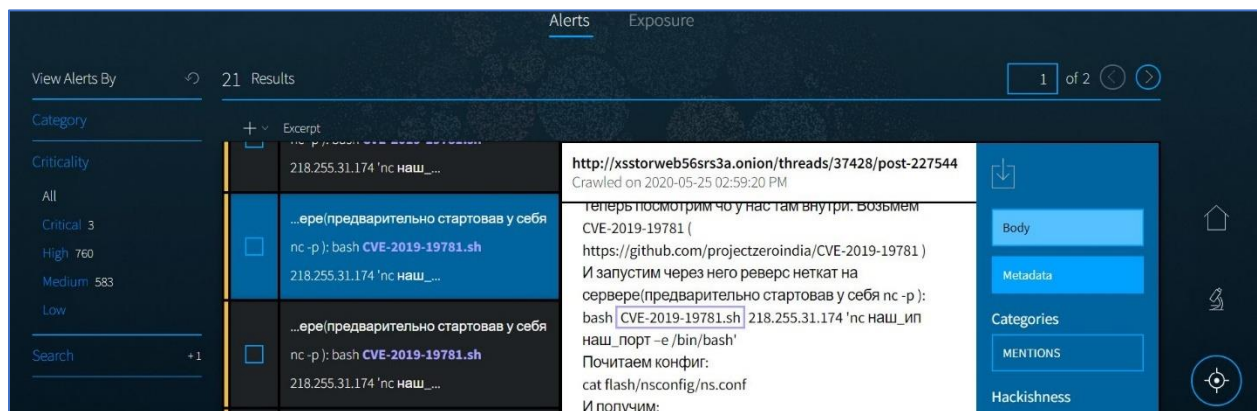
Deleting Alerts

Once alerts are reviewed and no longer needed, you can delete them from your result set. Select a set of results by checking the box(es), and then use the Action drop-down list. The drop-down list also gives a bulk option to Delete All alerts.
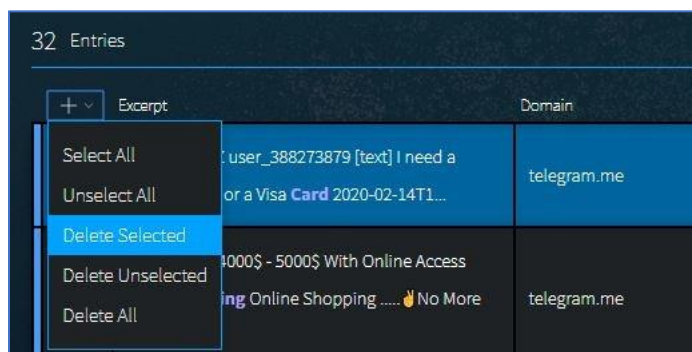
Note: You may experience a browser delay when deleting multiple alerts, or alerts that are large in size.

Trackers: 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 **Trackers: DARKINT Exposure** page from the Trackers right navigation icon, or from the Dashboard. The Dashboard gives an at-a-glance view of all organizations you have set up. Click on an organization name to access more detail on the **Trackers: DARKINT Exposure** page.

On the **Trackers: DARKINT Exposure** page, 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 an Exposure Score Report for the latest score.
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 buttons below Domains or Email Domains to see the results that generated the score.

Setting Up a Score

Create a score by clicking on the + icon on the **Trackers: DARKINT Exposure** page.
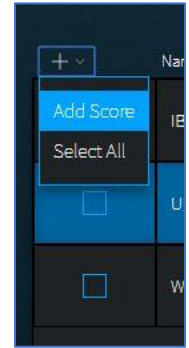
1. Type the Name that will be displayed in your score list.
2. Add one or more domains and subdomains, if any.
3. Add one or more email domains and subdomains. Only the domain portion is required; the @ symbol is not necessary.
4. If desired, check the box to receive email notifications when your score increases.
5. Click **Submit.**

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

+ ∨	Name ∨	Score ∨	Change	Trend	Last Run
☐	Organization 1	4.770	▼ -0.026		2021-11-12
☐	Organization 2	5.051	▲ 0.257		2021-11-12

The DARKINT Score Formula

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

H_{90} = Hackishness of last 90 days results

H_{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

Scores are logarithmic, meaning every point reflects almost triple the profile of a single point less.

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.

Collections: Your Saved Searches

Access your **Saved Searches page** from the Collections right navigation icon. 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 (more information: Editing a Saved Search)
5. View Alerts from the search (if any)
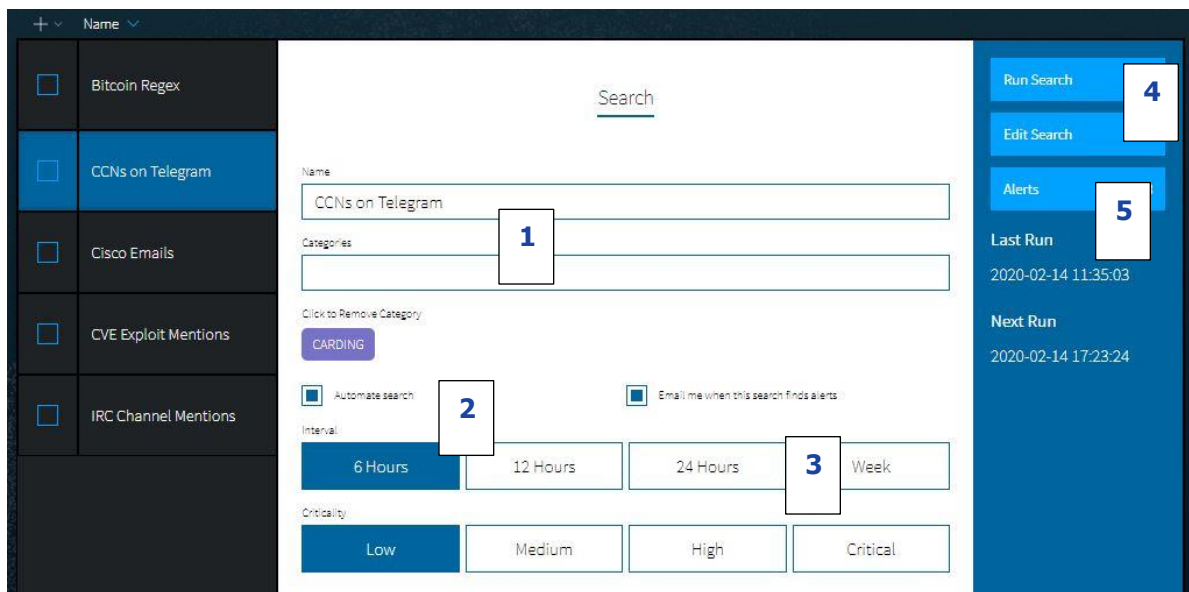
Editing a Saved Search

From the Searches page in your Collections, 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.
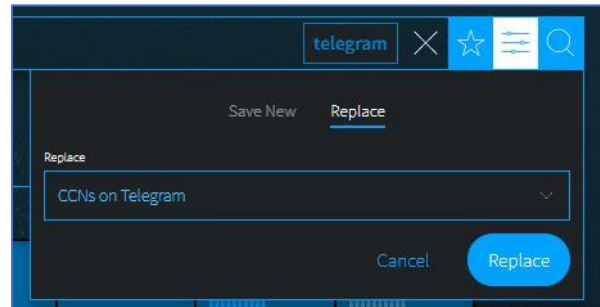
Collections: Your Search Blocks

You can manage your library of Search Blocks on the **Search Blocks page**. 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.
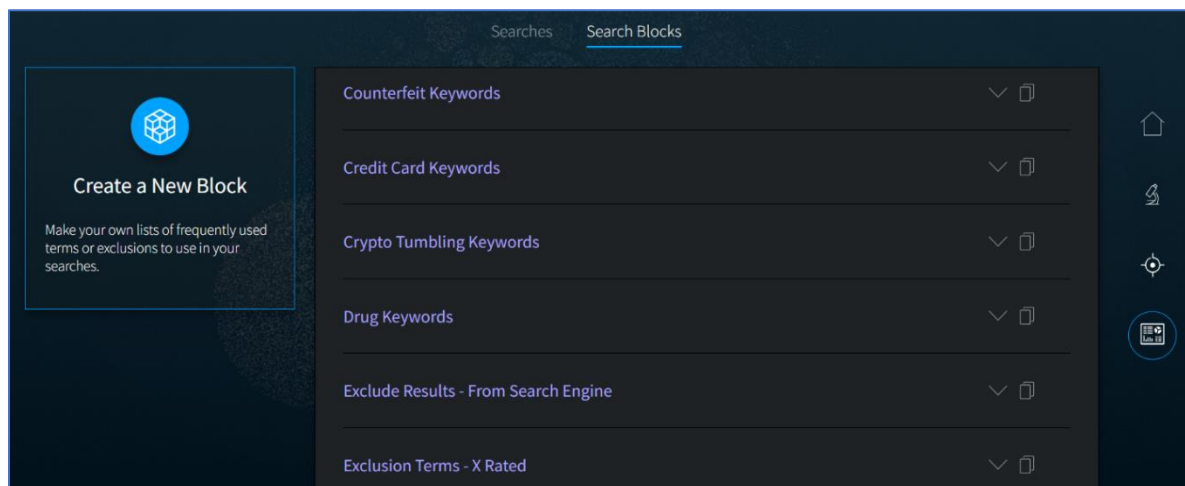
Creating a Search Block

1. Click **Create a 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. When entering BINs, use a trailing wildcard after the first six numerical digits.
- **Cryptocurrencies** can be lists of cryptocurrency wallet addresses. Supported types include *Bitcoin, Ethereum, Monero, Litecoin, Dash, ZCash.*
- **CVEs** can be lists of full CVE-ID numbers, CVE-ID numbers, or CVE years.
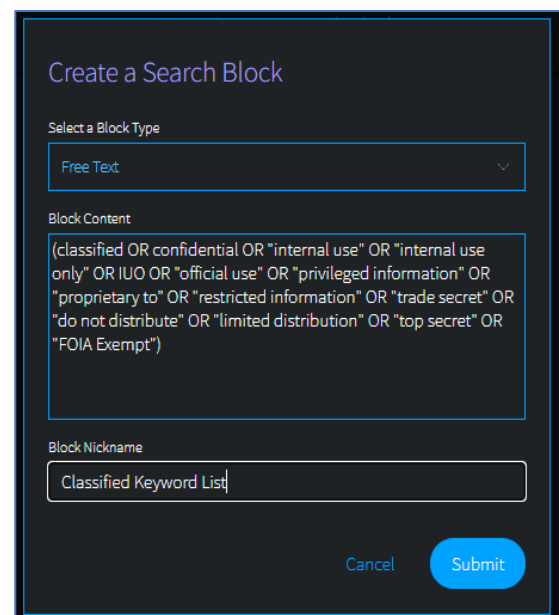
- **Domains** allow you to *filter to content from selected domains*. Use the Free Text Block Type to search for domain mentions.
- **Emails** can be lists of email addresses, email domains (without the @ portion), or email subdomains.
- **IPs** can be lists of IP addresses. We support the following types: *IPv4, IPv6/IPv6 compressed, CIDR ranges for both IPv4 and IPv6*.
- **Social Security Numbers** should be input using hyphens (i.e. 123-45-6789).

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.
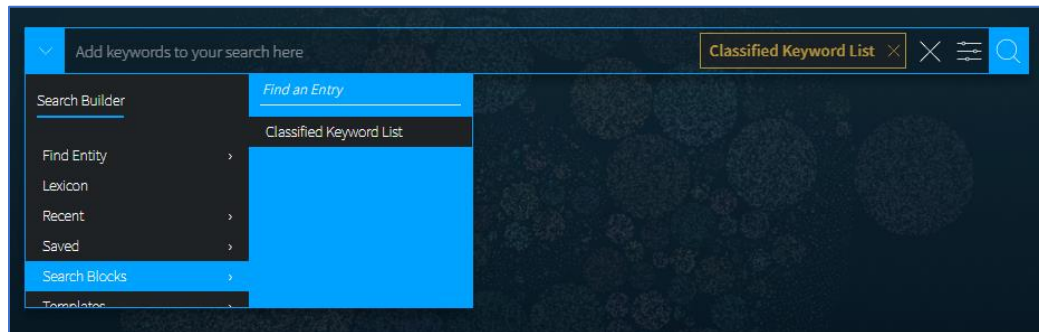
Managing Search Blocks

- **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.