BUILD EFFECTIVE MONITORS

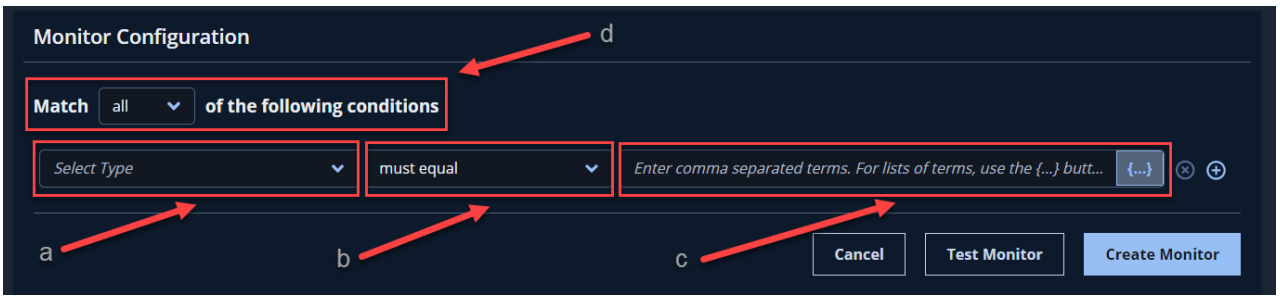
An effective monitor in Digital Threat Monitoring (DTM) is one that targets the content that's relevant to your needs, while minimizing the amount of false-positives (noise). To build effective monitors, we recommend that you first explore existing data using **Research Tools** **(https://docs.mandiant.com/home/dtm-research-tools)** to understand the types of content your target data includes. With that background, you can create the first version of your monitor and then update based on the alerts that are generated.

Each DTM Monitor Condition consists of the following:

1. A **Topic** (Select Type) that defines the set of things you would like to query for the Condition. Most of these topics are groups of entities or labels that have been extracted from the document and transformed. The two exceptions to this are the `Free Text Search` and `Lucene Text Query (Advanced)` topics which are covered in **Text Matching Topics**.
2. A Condition **Operator** such as `must equal` or `must contain`, which defines the operation to apply when searching for your Condition's values in the document.
3. The Condition **Values** (comma-separated terms or lists of terms), which are one or more values that you want to match in the document, entities, or labels. If you specify more than one value, the values in a given Condition are combined using the `OR` operator. That is, only one of the values must match.

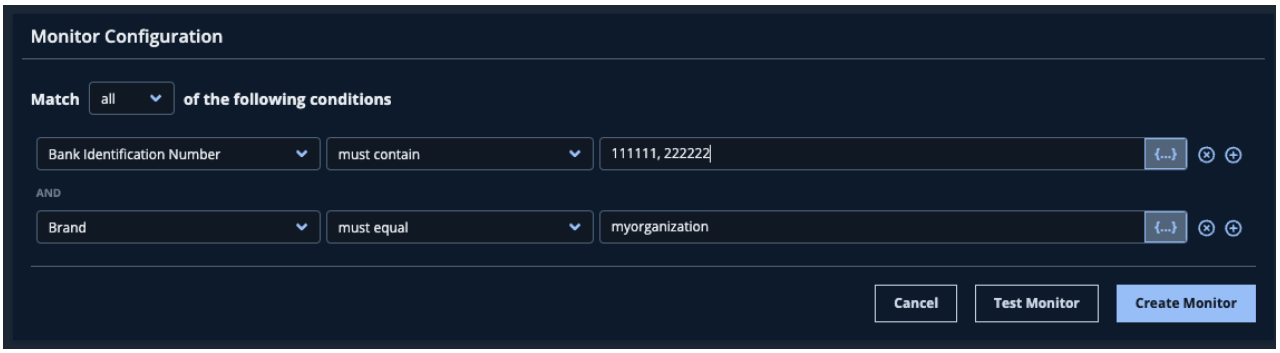
   Values are normalized before matching, and are therefore not case sensitive.

4. Each group of DTM Monitor Conditions in a Monitor is also governed by its **Conjunction** which can either be:
   - `all`: All conditions within the group must be true.
   - `any`: Any one of the conditions within the group must be true.



For example, the simple Monitor Conditions in the following screenshot will generate an alert when an ingested document contains a `Bank Identification Number` (detected entity) that contains `111111` or `222222` `AND` that same document has a `Brand` (detected entity) that equals `myorganization`.

Given that Condition values are normalized, `myorganization` will also match with `MyOrganization` and `MYORganization`, for example.



Monitors can be as broad or as targeted as you want them to be, using monitor topic conditions and text query strings. Use text query strings to create a broad search and use a monitor topic condition to target specific types and values. For example, suppose you're interested in *Malware threats against the Nike athletic apparel company* . There are two ways to approach the search:

Broad:

- Use a monitor topic condition for `Threat Type must equal Malware` . This condition ensures that your ML pipeline has identified a Malware classification in the document.
- Use a text query string for `nike` .

Targeted:

- Use a monitor topic condition for `Threat Type must equal Malware` . This condition ensures that your ML pipeline has identified a Malware classification in the document.
- Use a monitor topic condition for `Product or Brand Name must equal nike` . This condition ensures that your ML pipeline has identified a product of type `nike` .

While the broad approach produce matches for documents mentioning the Nike company, it will also potentially match on any mention of the word `nike` . For example, a document regarding Malware with the author `Jane Nike` would be included in the results, which may not be relevant resulting in a noisy monitor.

Text Matching Topics

The `Free Text Search` and `Lucene Text Query (Advanced)` topics let you match on text within the document in any arbitrary property. Usage of these topics should be treated with care, since they are effectively "grepping" the document text rather than being applied to identified entities or labels.

Free Text Search

The `Free Text Search` topic lets you specify one or more values which are then treated as keywords to find within the document. For example, using a `Free Text Search` Condition with `must contain` and the values `root` and `access` would match on any of the following: `root` , `rooted` , `root-access` , `noaccess` , `theroot.com` , `root@host.com` . While this outcome may be desirable in some scenarios, this technique can provide matches that are very broad and result in a noisy monitor without careful usage.

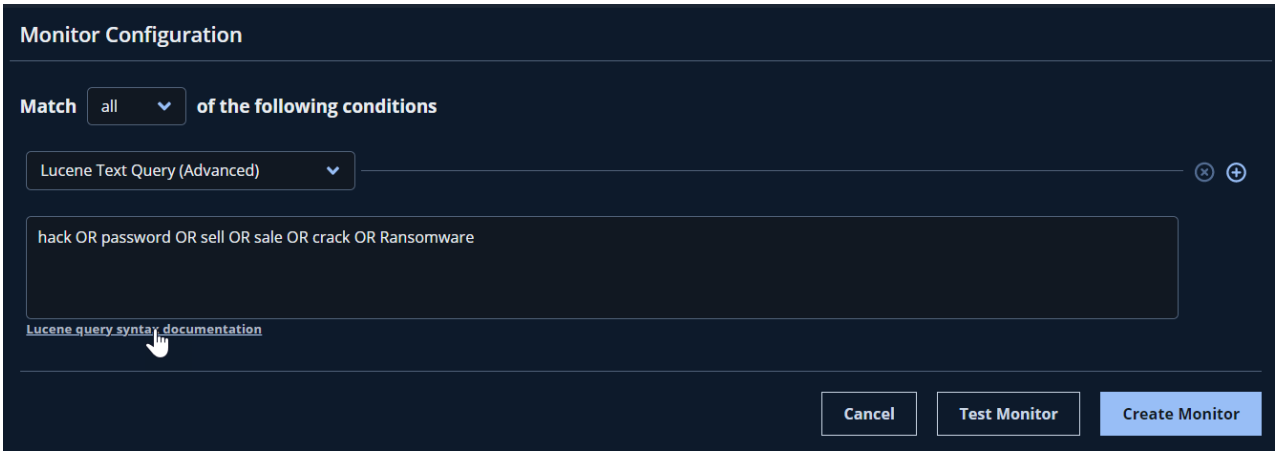
Lucene Text Query

In addition to matching Monitor Conditions, your monitors can (optionally) further search documents using a text query string as well. In this usage, the **Lucene Text Query (https://docs.mandiant.com/home/dtm-lucene-queries)** becomes part of your Monitor Conditions used to match documents as they are ingested. A query string is an **Elasticsearch Query String (https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-query-string-query.html)** (Lucene-based) that lets you:

- Perform a free text search over the entire document contents.
- Search specific **document model fields** using a JSON path-based syntax, for example `tweet_hashtags.hashtag:ransomware.`
- Use wildcards and shallow forms of **regexes (https://en.wikipedia.org/wiki/Regular_expression)**.
- Build queries using the basic syntax supported by **Elasticsearch Query String (https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-query-string-query.html)** syntax, including operators such as `AND` & `OR` .

> If any of the terms you're searching for include any special characters such as periods, commas, or dashes, the term should be enclosed in double quotes. For example rather than `acme.com` you should use `"acme.com"` , rather than using `i-sight` use `"i-sight"` .

If specified, the query string is matched only after your monitor topic conditions have matched. In other words, it's a way to refine your search further once your topic conditions have been met.



Document Model Search Paths

Using a text query string lets you query specific model paths of your documents. Targeting specific paths in the model can be useful to target very specific values in the document. However, all text paths in documents can be searched without specifying model search paths. For example, if you use a text query string of `hack OR password` both `hack` and `password` will be searched for in all text paths of documents.

When specifying model search paths in the query string, the format is a dotted notation where each value in the path is the property name in the document. For example, if you want to search for a specific hashtag value in a `tweet` document, the following path can be used: `tweet_hashtags.hashtag` , which specifies the document path to search is the `hashtag` property of the `tweet_hashtags` object in a tweet document.

To understand which paths exist, you must look at the **Schemas** in the **API specification** (see **Monitor fields documentation (https://docs.mandiant.com/home/dtm-monitor-fields)**). There you will find the document types that correspond to the models. The following top-level models are currently being supported in DTM:

- `account_discovery`
- `document_analysis`
- `domain_discovery`
- `email_analysis`
- `forum_post`

- `message`
- `paste`
- `shop_listing`
- `tweet`
- `web_content_publish`

> When using document model paths in your query string, ensure that your monitor topic conditions are that set up to only match on the respective document type. For example, to search on the content of Forum Posts, you would add a Monitor topic condition **`Search Collection Type`** **`must equal`** **`forum_post`**. This ensures that when your query string is used to search the document, results will always be of type `forum_post`.

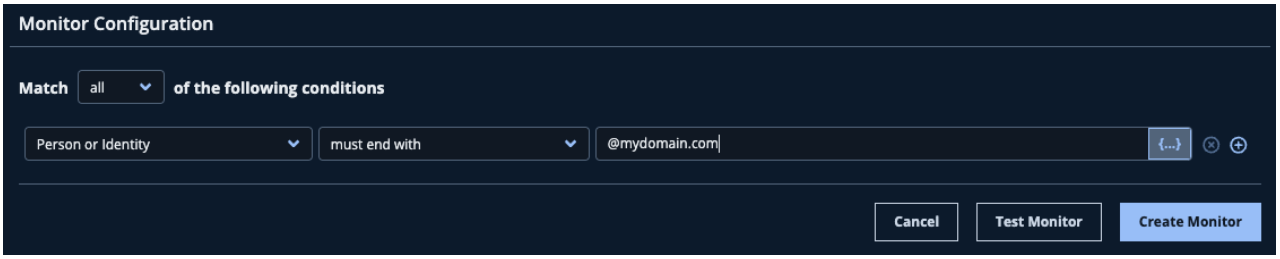
Example Monitors

Filenames

Suppose you want your Monitor to alert anytime a document mentions the filename `my_sensitive_file1` or `my_sensistive_file2`. The following Monitor Conditions depict how you might approach defining this Monitor. Notice that the conjunction used is `any`, so either of the Conditions can match in order to return a result. Both the `Filenames & Paths` and the `Network Information` topics are used here because the filenames could be detected as a file system path, or in the path of a URL. This Monitor Configuration captures either of those scenarios.

Email Addresses

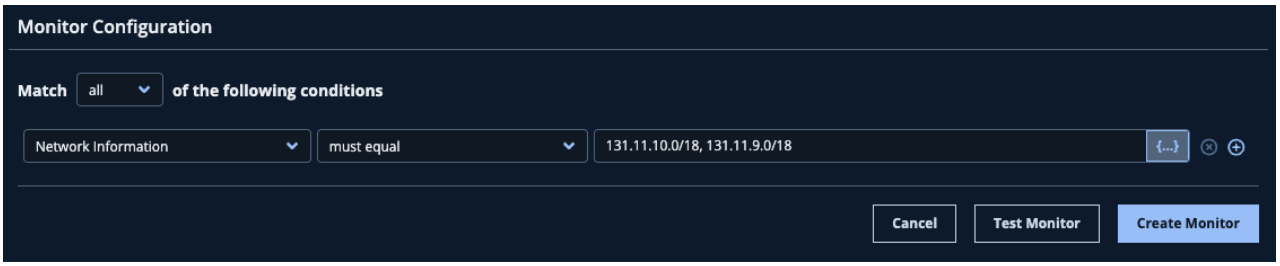
Finding email address leaks can be easily accomplished using a Monitor with a single condition. As shown in the **Monitor fields documentation (https://docs.mandiant.com/home/dtm-monitor-fields)**, email addresses are searched using the `Person or Identity` topic. If you want to match on any email addresses that contain your email domain (say `mydomain.com`), you can simply check this topic for any values that end with `@mydomain.com`. This will cover any usernames within the domain. If you wanted to alert on specific user email addresses, you could instead use the `must equal` operator and then provide a list of the full email addresses you want to target.



IP Addresses

Suppose you want to alert on any content that mentions an IP address in your internal networks within your two CIDR

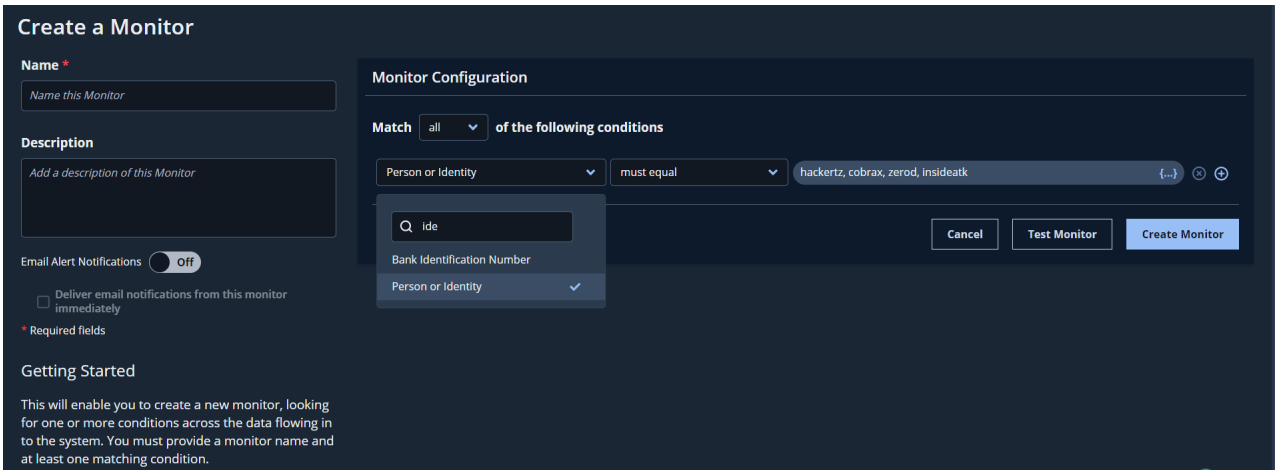
blocks `131.11.10.0/18` and `131.11.9.0/18`. You can accomplish this by simply using the CIDR block notation in a `Network Information` Topic Condition as shown in the following screenshot. DTM understands CIDR blocks and can ensure it matches anytime an IP address is found within the given CIDRs.



Target A Group Of Users

Your organization was recently attacked and while investigating this attack you've identified the following list of internet handles as being involved in the attack: `hackerz`, `cobrax`, `zerod`, `insideatk`. You want to create a monitor that will alert you of any new information that may be related to any of these handles.

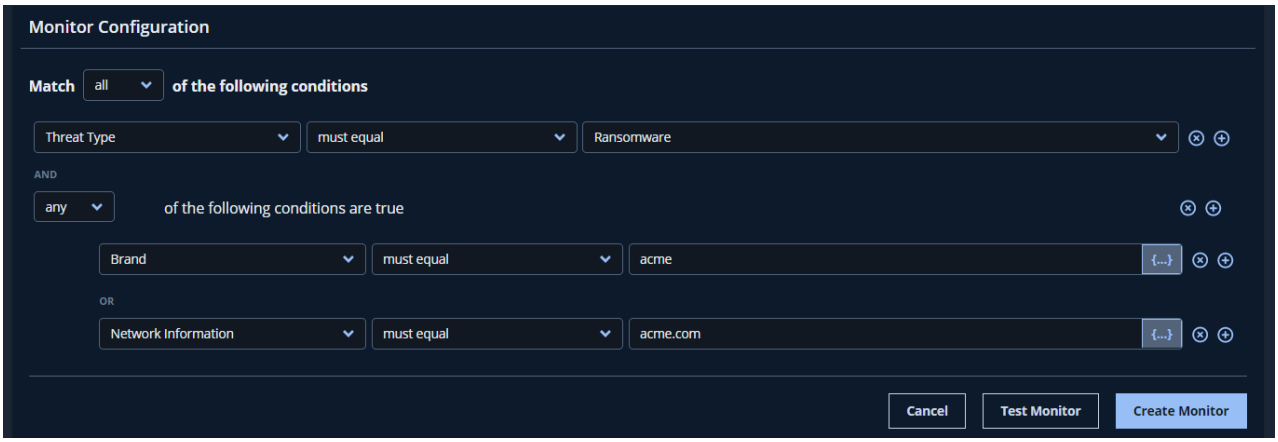
This monitor is very simple; it's a single `Person or Identity` `must equal` condition with the list of handles to match on as shown in the following screenshot:



Target Ransomware for Organization or Domain

You want to be alerted for potential Ransomware associated with your organization `acme` or your domain `acme.com`.

This is another simple monitor that uses a nested condition group to search for the organization `acme` or the domain `acme.com` when identified a `Threat Type` of `Ransomware`:

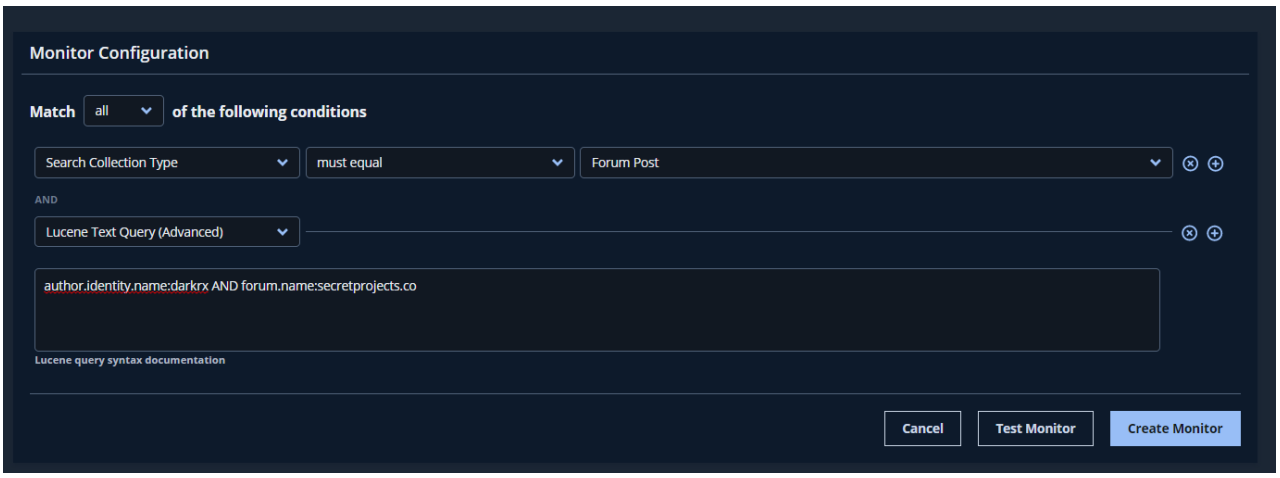


For a list of available Threat Types, see the Threat Type Description in **DTM Monitor & Research Tools Fields (https://docs.mandiant.com/home/dtm-monitor-fields)**.

Track posts by a specific author on a specific forum

You want to follow any forum post created by the internet handle `darkrx` on the forum site called `secretprojects.co`

Since you only want to target forum posts by a specific author, and on a specific forum site, you need to leverage the document path syntax in your text query string `autor.identity.name:darkrx AND forum.name:secretprojects.co` as shown in the following screenshot:



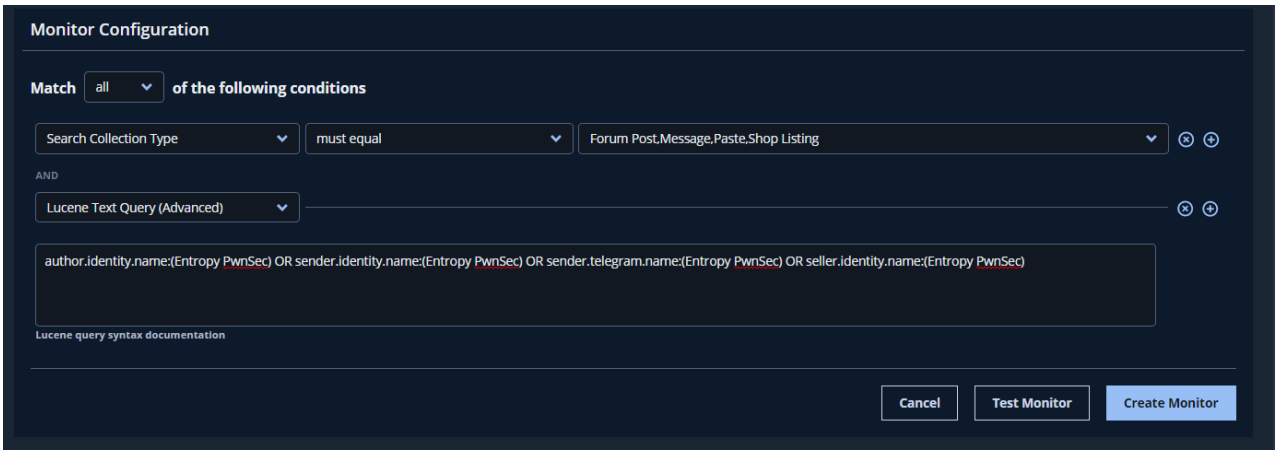
For a list of available Collection Types, see the Search Collection Type Description in **DTM Monitor & Research Tools Fields (https://docs.mandiant.com/home/dtm-monitor-fields)**.

Track Contents Posted by Specific Handle Names in the Deep and Dark Web

You want to track contents posted by specific handle names in the deep and dark web. Here you can use Lucene to target author specific fields of documents with the following query:

```
author.identity.name:(Entropy PwnSec) OR sender.identity.name:(Entropy PwnSec) OR sender.telegram.name:(Entropy PwnSec) OR seller.identity.name:(Entropy PwnSec)
```

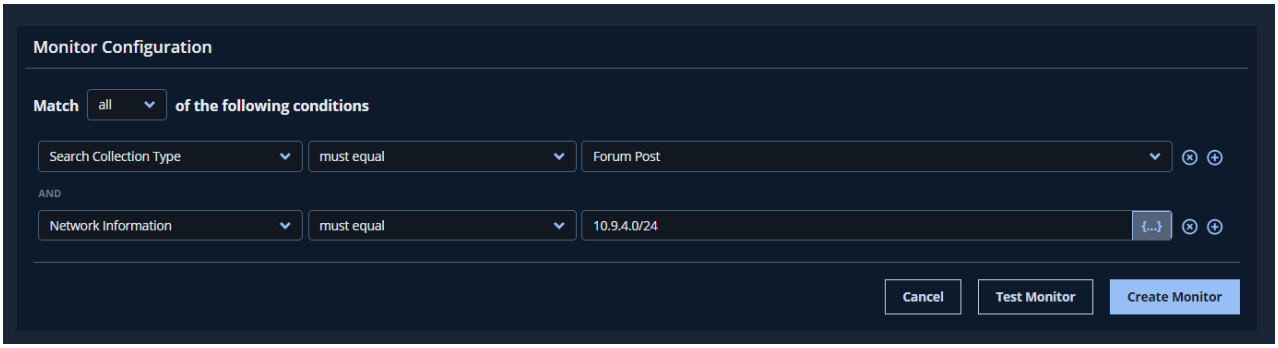
This query includes all author-related JSON paths for the document types that you're targeting by setting the **Search Collection Type** to the appropriate document types. It will match when any of those author paths include either of your actor/handle names. The final monitor configured is shown in the following screenshot:



Watch Forum Posts of IP Addresses in a Network Segment

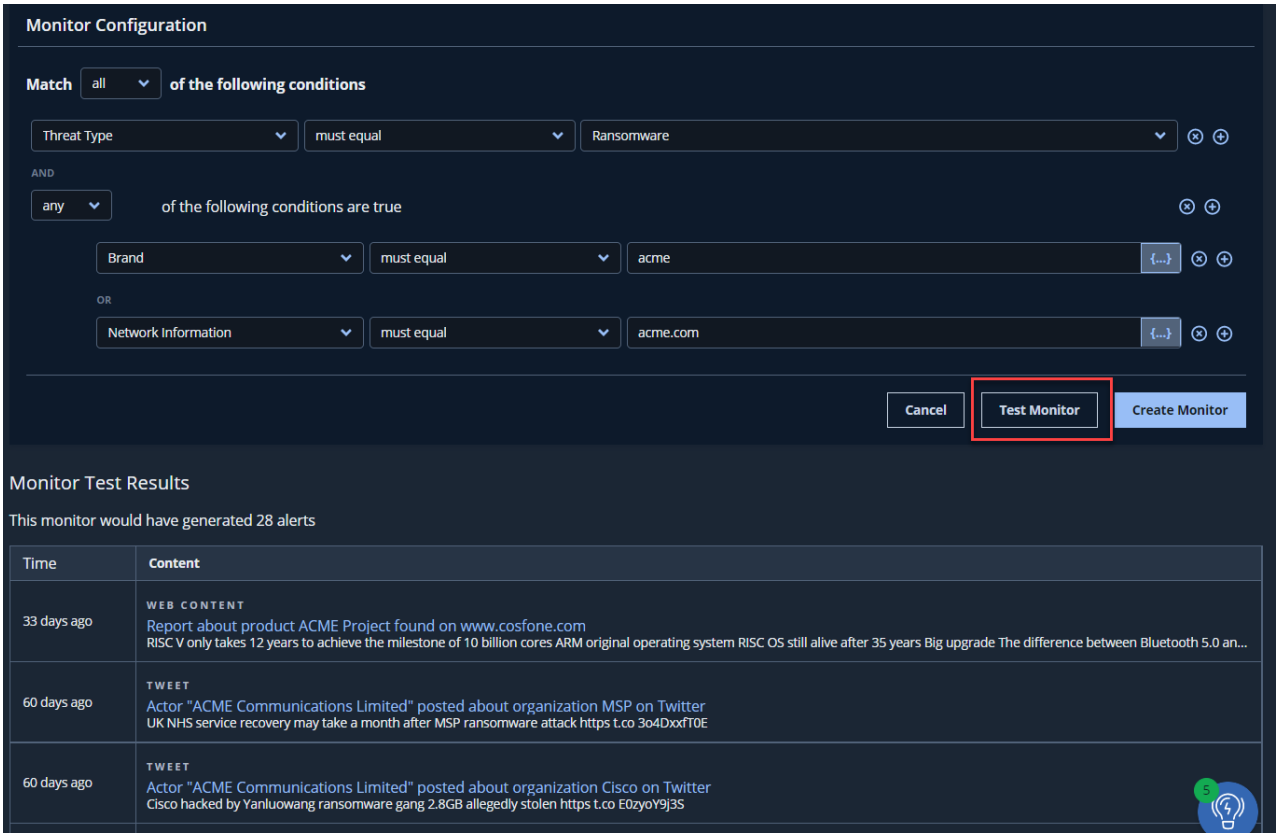
You have reason to believe one or more of your public-facing services/hosts has been compromised on your public-facing network. For demonstration purposes we'll use the non-routable network `10.9.4.0/24`. You want to create a monitor to watch all Forum Posts for any mentions of IP addresses in that network segment.

This is another simple monitor that leverages the ability to specify a network CIDR as an IPv4 address as shown in the following screenshot. Any IP address in the specified CIDR will trigger a match.



Test a Monitor

Once you create a monitor, you can test by selecting the **Test Monitor** button.



Note the following caveats:

- While testing a monitor: The `must contain` & `must not contain` may not work correctly using this feature. Test queries are limited to 200 monitors.
- Due to privacy and legal concerns, Test Monitor does not pull back Compromised Credentials documents.
- Test Monitor doesn't search partial domain names.