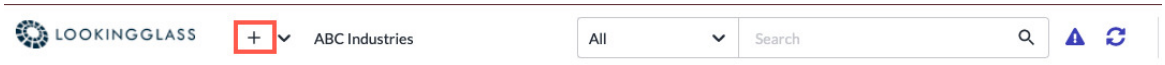
scoutPRIME - Workflow: Creating Your First Collection

Steps for creating a new collection

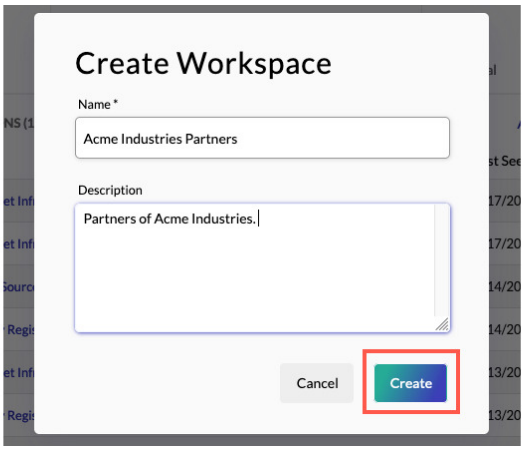
Written by Dolores M. Bernal
Updated over a week ago

To get you started with using scoutPRIME this workflow example will take you from creating a Workspace, to adding and saving your first Collection. Let's go!

1. To create a new workspace, click on the + sign on the very top navigation bar, next to the current workspace's name.



2. Next, give your workspace a unique **Name** and a **Description**. When you're are finished, click **Create**.

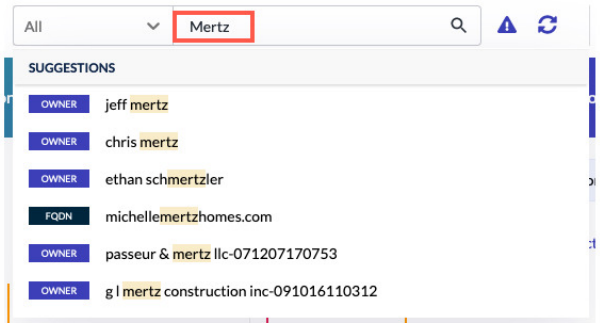


Great! You've created a new workspace - a clean environment where you can start running queries, analyzing elements, and adding or creating collections.

3. Now, we'll create a collection from search, so the first thing you need to do is run a query on an entity that's in your supply chain or is a third-party vendor.

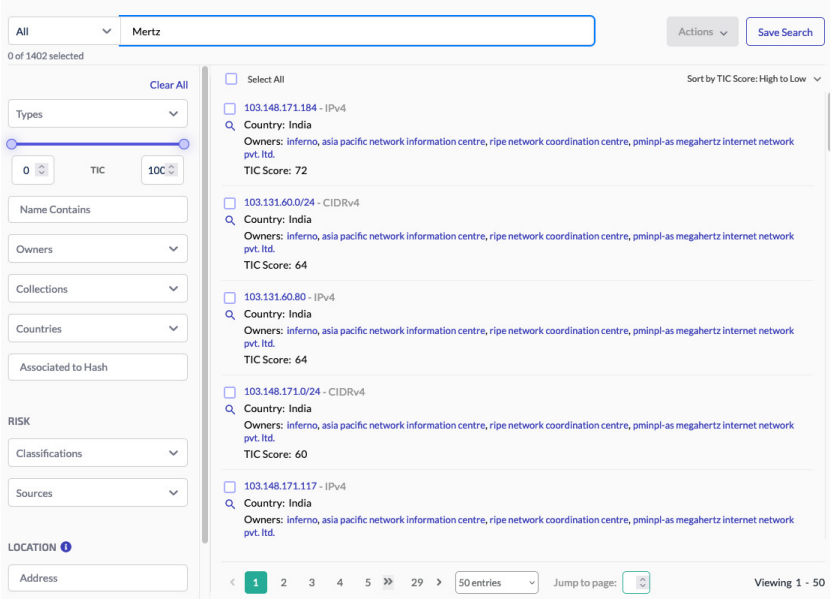
For this example, let's look into a transportation company called "Mertz," which moves goods for Acme Industries.

With **All** pre-selected for us in **Search**, type in the name of the transportation company.



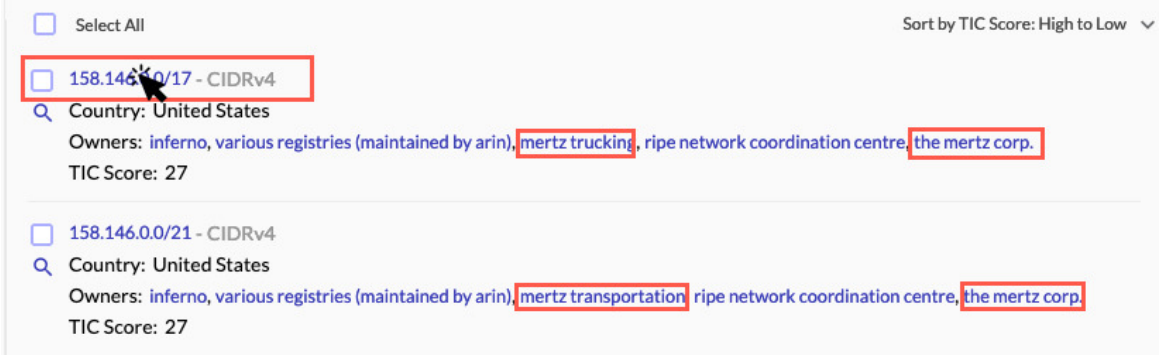
NOTE: scoutPRIME will make suggestions for your search query. If the exact entity name is not listed you can ignore the suggestions and just press **Enter** or click on the looking glass to continue with your search.

4. Search results will populate on the next page. You can scroll up or down the page until you find the entity you are looking for.

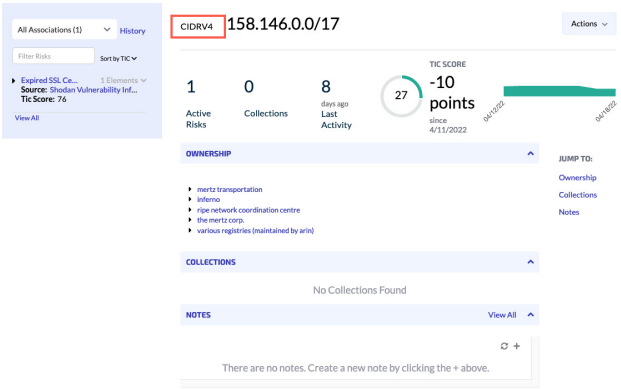


You can also use the filters on the left side of the page to help narrow down results. In this example, we'll use the **Countries** filter since the company we're interested in is headquartered in the United States.

5. Two results peak our interest because they have the name of the entity we're looking for in them. Let's drill down on the first one to examine it further.



6. Notice that the result opened up in the **Elements Details** page, this is because the result is a CIDRv4 element -- the IPv4 address is 158.146.0.0 with a subnet mask of 17.



The **Element Details** page provides us with the following information:

Statistics showing the number of **Active Risks** the element carries, also how many of our collections contain this CIDR, and how many days ago this element experienced any type of activity.

- **TIC Score** - The level of risk the element carries based on scoutPRIME's algorithm. Plus, a graph showing points when the TIC score changed since there was activity.

- **Associations** - Any Threats and Vulnerabilities listed on the left panel in blue.| -

- **Ownership** - Current or past registrant information.

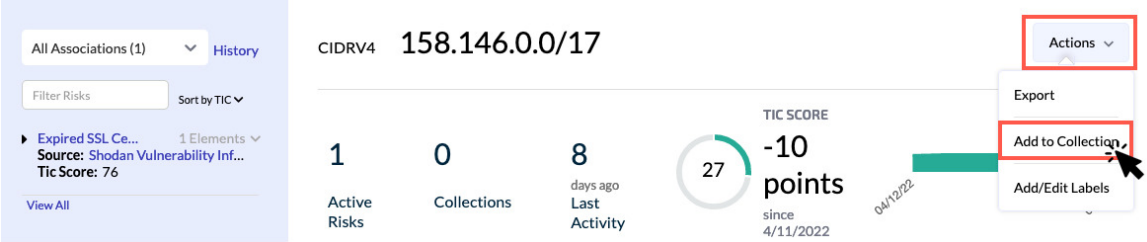
- Any **Collections** that the IP address is a member of.

- Any **Notes** from you or others in your team about the element.

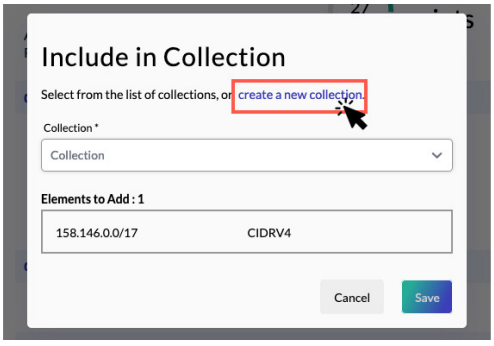
7. Since what's on the **Element Details** page is very important information about the company, we can either go ahead and explore more elements on the page such as the ones under **Ownership** or, the **Association** on the left side panel in blue: "Expired SSL Certificate."

For this example, we'll create a collection from here.

Click on **Actions** near the top right corner of the page, and select **Add to Collection** from the drop-down menu.

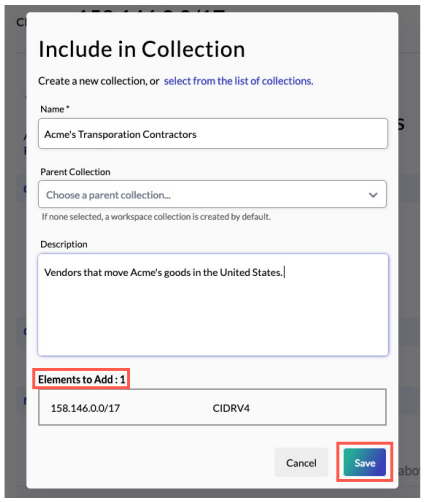


8. The **Include in Collection** window will open - you can choose to add an element to an existing collection, but for this example we'll click to **create a new collection**.

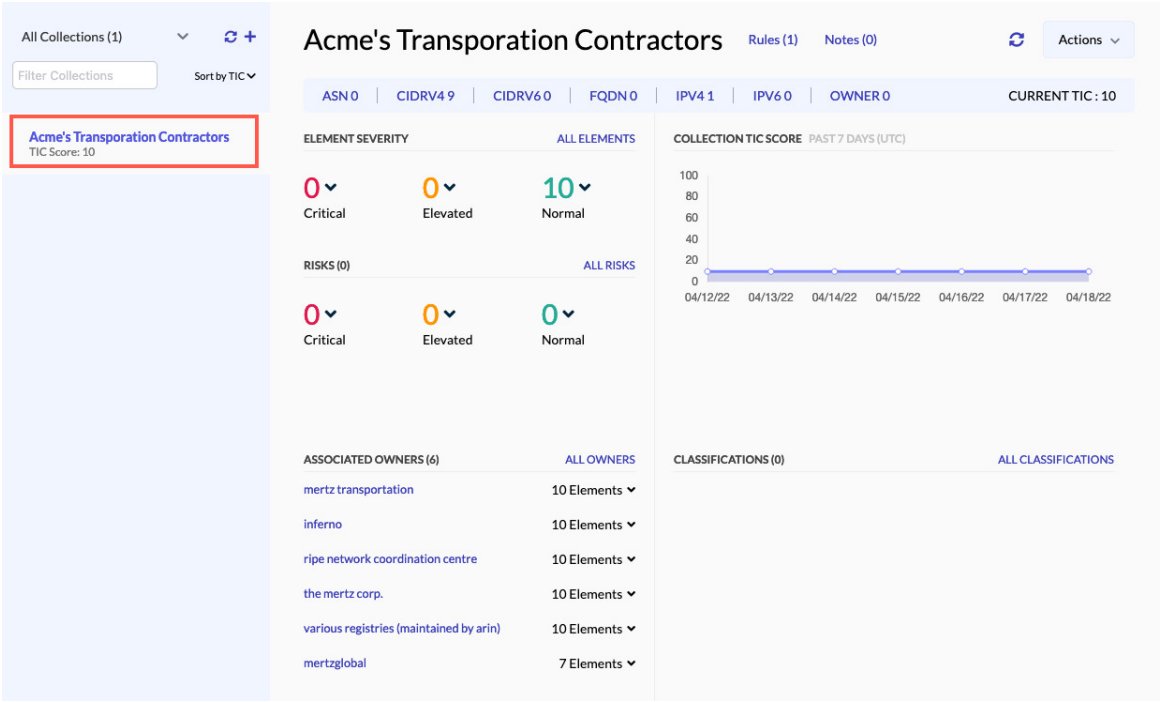


9. Give the collection a **Name** and a **Description**. If you want this to be a nested collection, you can choose a **Parent Collection** for it.

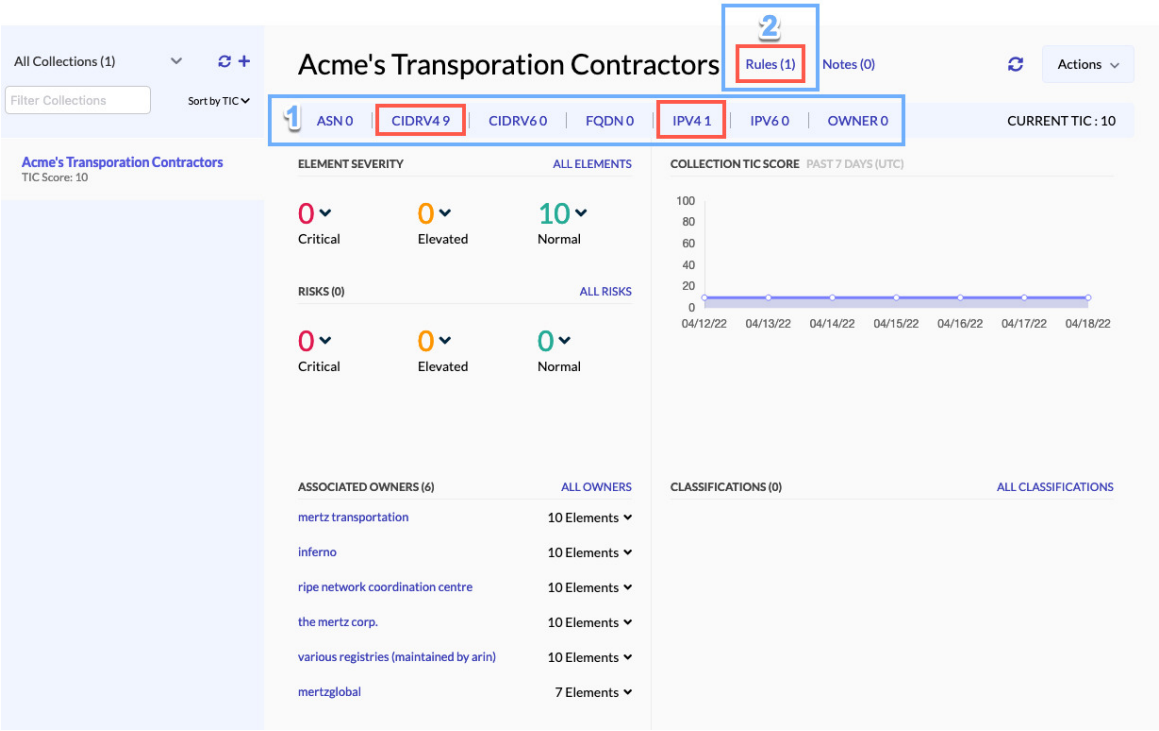
For this example, we'll just click **Save**.



10. You should receive confirmation that your collection was created and that one element has been added to it. To check if the action was successful, navigate to **Collection Management** and see if the collection name appears on the left panel in blue.



In addition, the **Collection Management** page will provide you with the following information:

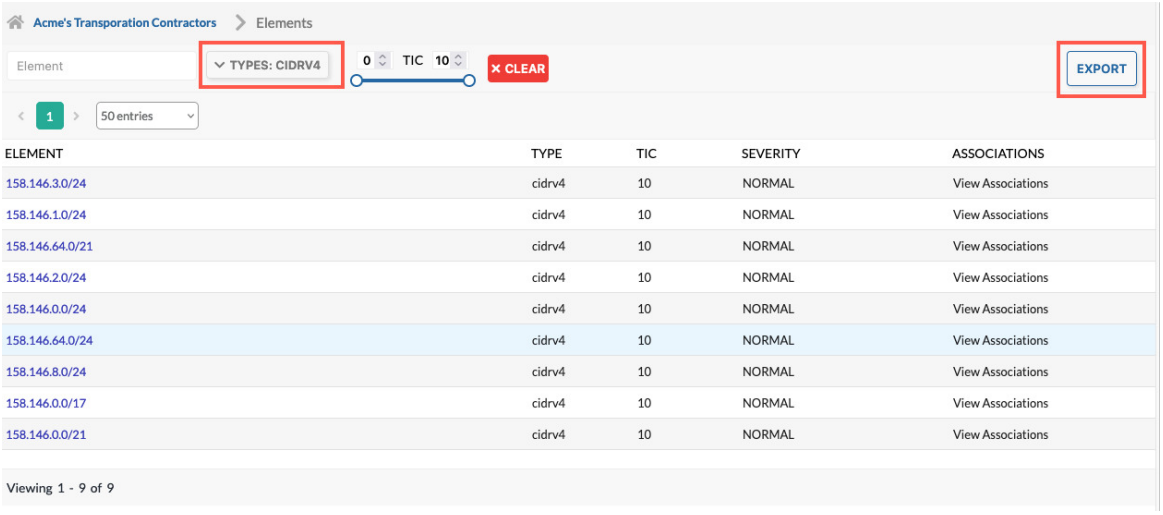


#1. How many elements are in your collection and what types. For example, in the above screen capture there is a **9** next to the **CIDRV4** element type. This means that there are nine other CIDRV4 elements that are members of this collection. The CIDRs were added from the **Ownership** list in the screen capture for Step 6.

Note also that there is **1** in parenthesis next to the **IPv4** element type. This is because the IPv4 address is part of the CIDRV4 element: **158.146.0.0**/17

#2. The is a **1** in parenthesis under **Rules**. This means that so far there is only one rule for this collection and that is to add this CIDR type elements to it. You can edit rules to include other types of elements to the collection.
11. Let's dig a little deeper and examine the CIDRs in the collection. Click on **CIDRV4** in the elements section.

12. Another page will open within the **Collection Management** feature. This page will list the nine CIDRs that are members of the collection with their corresponding **TIC scores**, **Severity** levels, and **Associations** (Threats and Vulnerabilities that the element carries).



From this page you can also choose to add more elements of the same type or different by clicking on the **TYPES** drop-down. You can also filter elements by their TIC score by using the slider. And, you can click on **Export** to download the list to your computer or workstation.

Workflow Example Summary

The biggest takeaway from following a workflow like this one is that you can very easily create a collection simply by running a query and drilling in on elements of interest.

Another, it's that relative to the millions of other CIDRs on the Internet, the company in this example had a CIDR with a very low TIC score (10), which is considered the system's default TIC score.

So, does this all mean that our fictional company, "Mertz," is a safe company to do business with? Well, it's probably too early to tell. Remember that in the background, scoutPRIME continues to work, ingesting thousands of pieces of information everyday. It's important to check the health of the elements in your collections regularly to be sure that an entity in your supply chain doesn't have rising TIC scores.

To stay on top of your collections, you can set up notifications that can alert you to changing TIC scores. To learn more about creating notifications, click here.

You also use the **Collection Health** feature to quickly view if the criticality level of your collections is rising or not.

Related Content

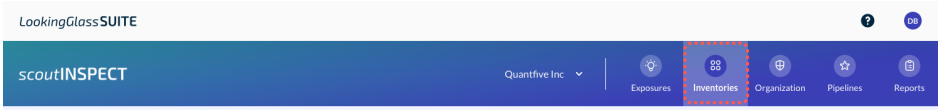
- Supported Browsers
- Login
  - Log In
  - Password Reset
  - Log Out
- Other Settings
  - Accessing Administrator Features
  - Viewing the TIC Configuration
  - Accessing Online Help
  - Sending User Feedback to LookingGlass Cyber

scoutPRIME User Documentation Table of Contents

scoutINSPECT - Inventories

Written by Dolores M. Bernal
Updated over a week ago

Inventories Overview



The **Inventories** page shows all the raw data that scoutINSPECT has collected through active scanning, these include all your:

- IP addresses (IPv4 and IPv6)
- Domain names
- DNS records
- Network records
- Cloud storage buckets
- Cloud computing services
- Security certificates

The graphs and charts on the dashboard provide snapshots of how many of your assets have been identified, assigned tags, who owns them, changes to your inventory, and more.

Inventories help analysts see the assets, keep track of them, and get more details about what software (services) each is using.

NEXT:

- My Inventory Tracker
- Total Inventory and Total Owners
- Inventories Per Owner
- Inventories Per Tag
- Top Inventory Changes
- My Inventory Table
  - Editing and Updating Items in My Inventory Table

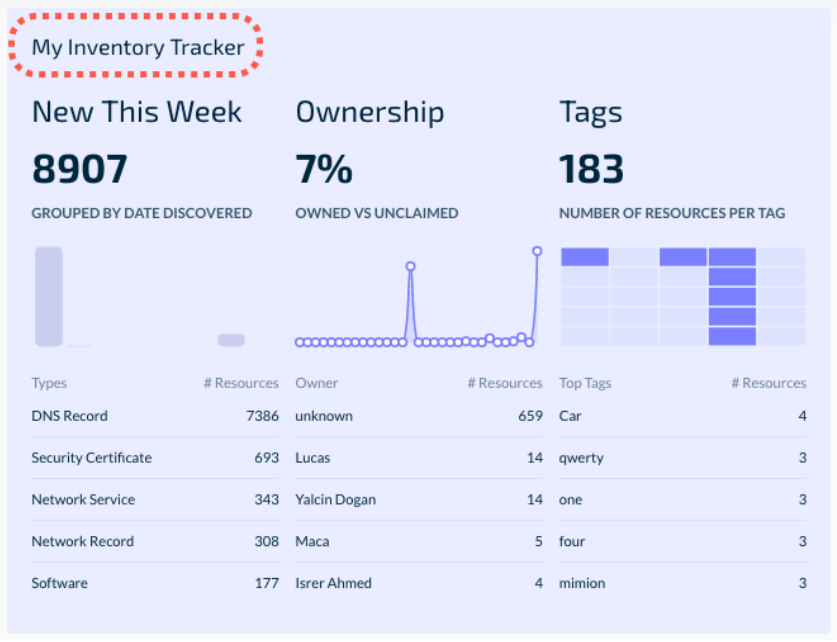
My Inventory Tracker

My Inventory Tracker offers three different views for tracking items in your inventory over the past **7 days**, including:

- **New This Week** - Shows how many different types of assets were discovered during the week.

- **Ownership** - Shows how many of the assets now have owners (analysts or other persons) versus how many lack ownership. **NOTE**: The ideal percentage number here should be "100%" meaning that all your assets have been owned.

- **Tags** - Assets that were discovered and have been assigned tags such as, "Finance Server," "Company ABC domain name," "ABC vendor," etc.



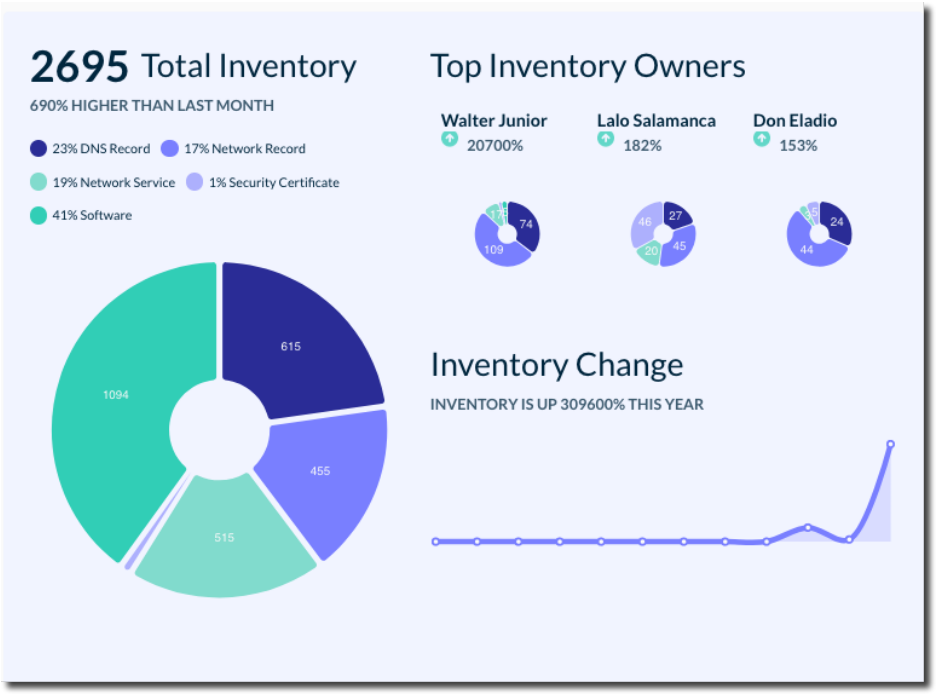
Total Inventory and Total Owners

This section contains three inventory views:

Total Inventory - The total number of assets (e.g., DNS records, security certificates, network services: IPs, domains, etc.) in the inventory over the last **30 days**.

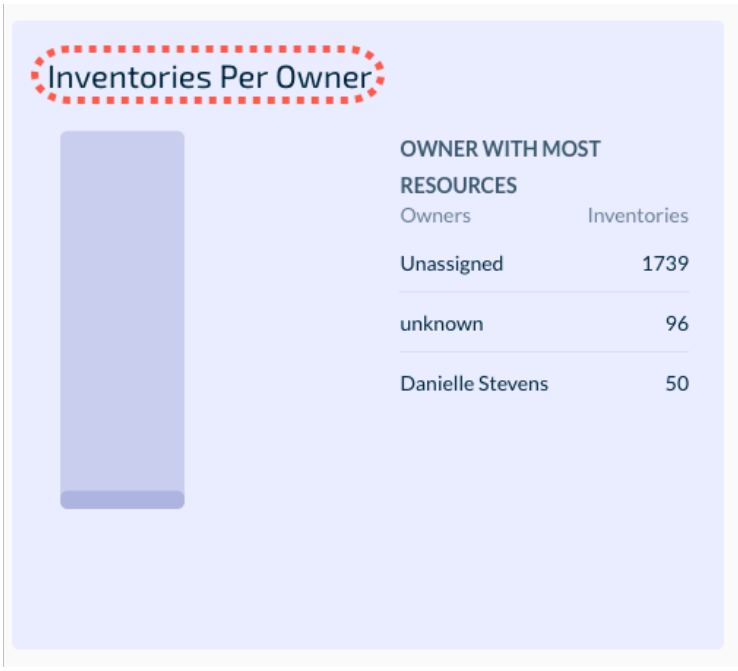
Top Inventory Owners - Who in your team owns the most assets.

Inventory Change - How the inventory has changed over the past **12 months**.



Inventories Per Owner

Inventories Per Owner provides you with a view of who in your team **currently** owns assets, as well as the names of the owners with the most assets. Assets that are not owned will display as "Unassigned."



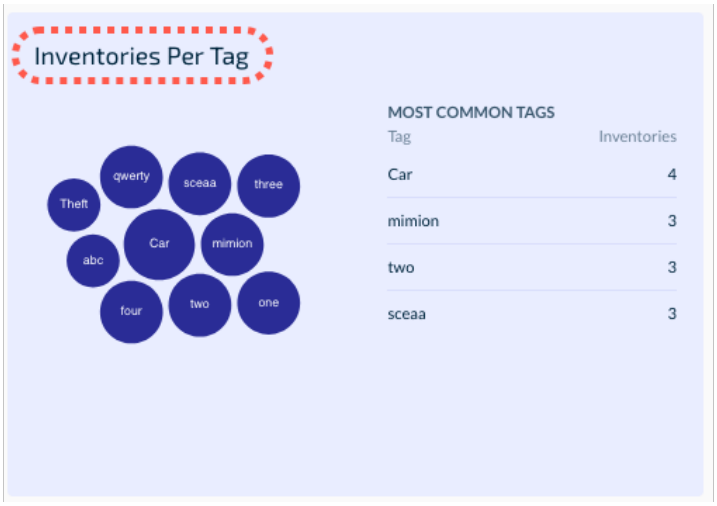
Inventories Per Tag

Inventories Per Tag graphically shows and a **current** list your tagged assets.

Tagging is when an asset is discovered then given a label to identity what it is.

For example, an IP could be tagged as "Finance Server," meaning that IP belongs to a server that handles finance data.

This section also offers how many assets have been tagged.

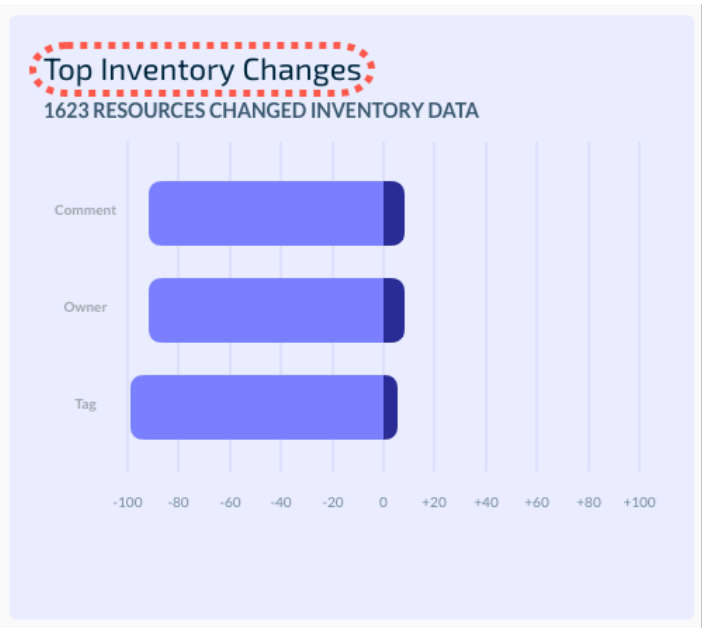


Top Inventory Changes

Top Inventory Changes shows a bar graph that informs you how assets in your inventory have changed **since discovery**.

For example, how many assets now have comments, are owned, and have been assigned tags.

Ideally, you want the bars in this graph to be on the positive side (e.g., +40, +80). When the bars are light blue and on the negative side (e.g., -40, -80), it is not considered good cyber hygiene, meaning that there are a lot of assets that need your attention and action. These assets have to be assigned owners, be tagged, and have comments in their respective Asset Details page.



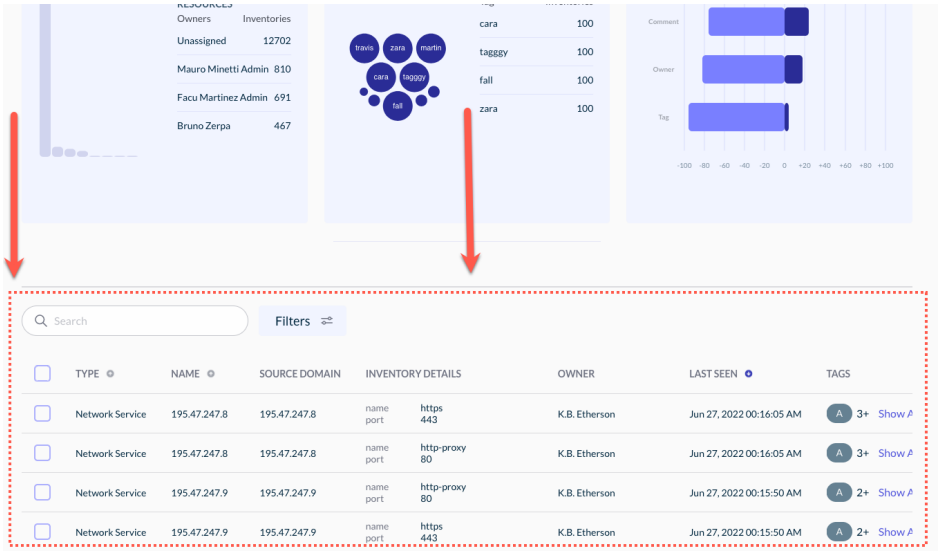
My Inventory Table

The second half of the **Inventories** page shows a table listing the assets in your inventory. The table offers information on asset **Type**, **Name**, **Source Domain**, **Inventory Details**, **Owner**, date of **Last Seen**, and **Tags**.

- **Type** - Asset types can include: Software, Network Service, DNS Record, etc.
- **Name** - The name of the asset can be represented by an IP address or the name of a software/service (e.g., Apache, Telnet, etc.).
- **Source Domain** - A domain linked to particular exposure or inventory. It can also be a subdomain of a seed domain.
- **Inventory Details** - Pertinent details about the asset in the inventory. The types of

details will vary from asset to asset.

- **Owner** - Who in the team owns the asset.
- **Last Seen** - When the issue was last updated.
- **Tags** - Labels used to identity assets (e.g., "Finance Server," "Application Server," "Main domain name," etc.).



Editing and Updating Items in My Inventory Table

You can edit or update the **Owner** of the asset. To do this, simply hover your mouse on the desired item, then click on the **pencil** icon that appears on the right.

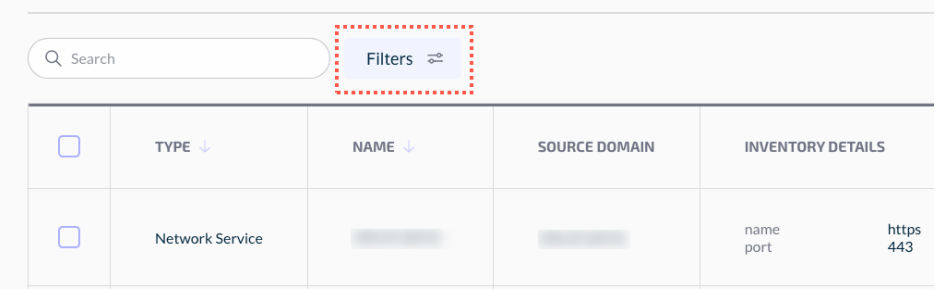
Filter Items in My Inventory Table

The My Inventory table allows you to use filters to quickly find assets by type, owner, and tag.

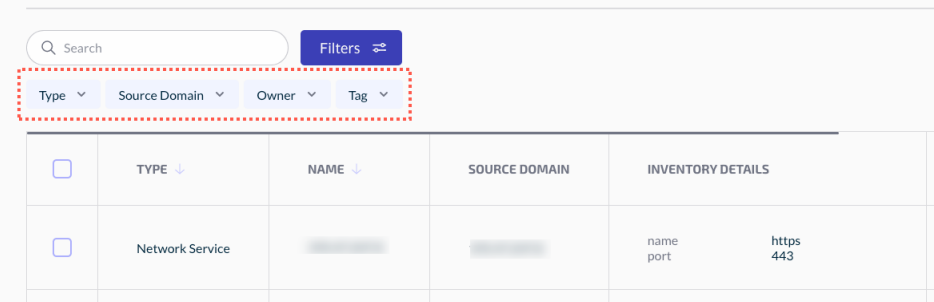
Here are a few ways to filter or sort the items on the table:

Using the Filter Field

On the My Inventory table, look for the **Filter** field and type in a keyword (i.e., an asset's IP address, domain name, or a service name, port number, exposure name, etc.). Then, click **Filter**.



You may also choose from pre-selected filters using the **Filters** drop-down menus by clicking on the Filter button.

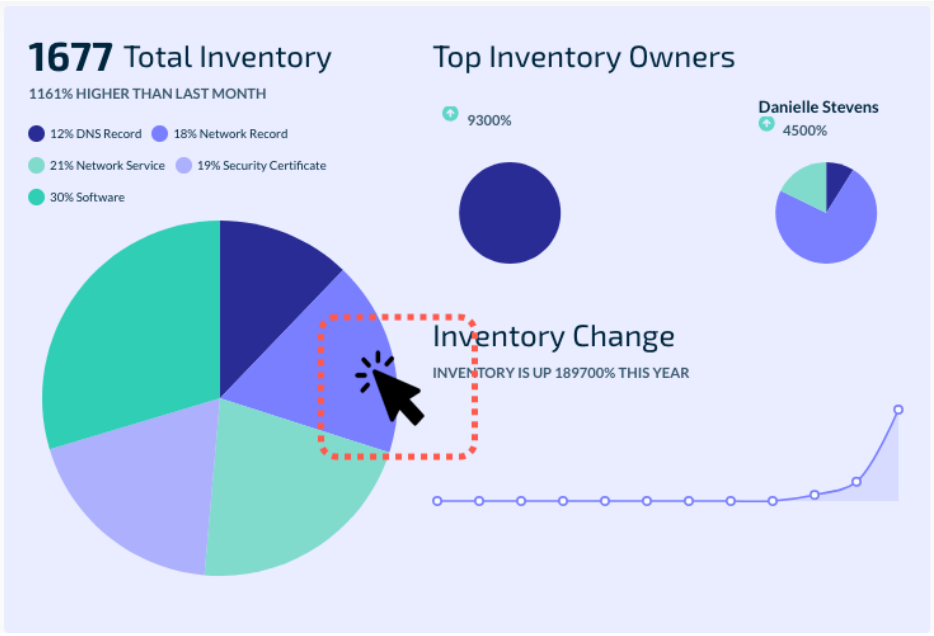


Here you can filter by:

- **Type**
- **Source domain**
- **Owner**
- **And, tag** (e.g., "finance server," "mail server," etc.)

Clicking on a Graph

You can also filter items on the table by clicking on any of the graphs on the first half of the page.



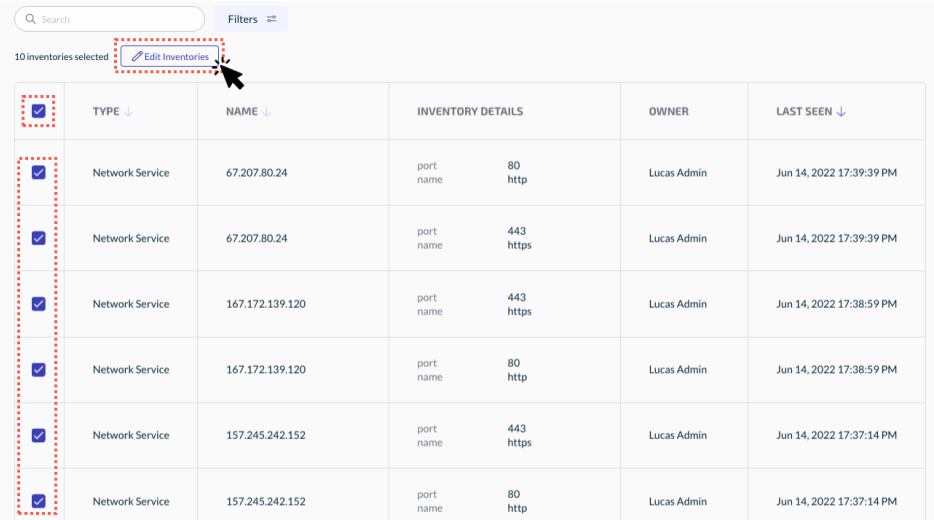
The second half of the page will display the filter that was applied when you clicked on the graph. The table will also be sorted based on what was clicked.

My Inventory Table Bulk Actions

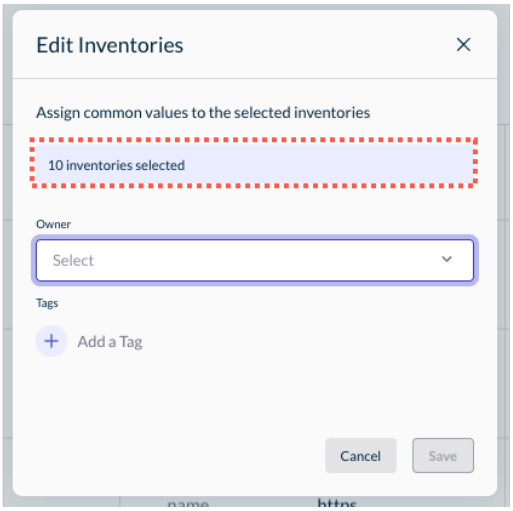
You can change the **Owner** for multiple assets at the same time on the inventory table. You can also add or remove tags (e.g., "finance server, "mail server," etc.) in bulk. To do this, follow the steps below.

Steps

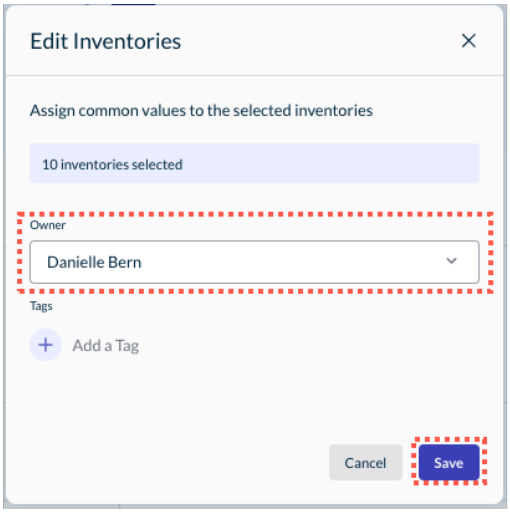
1. On the inventory table, first select multiple assets you'd like to edit in bulk, then click on **Edit Inventories**.



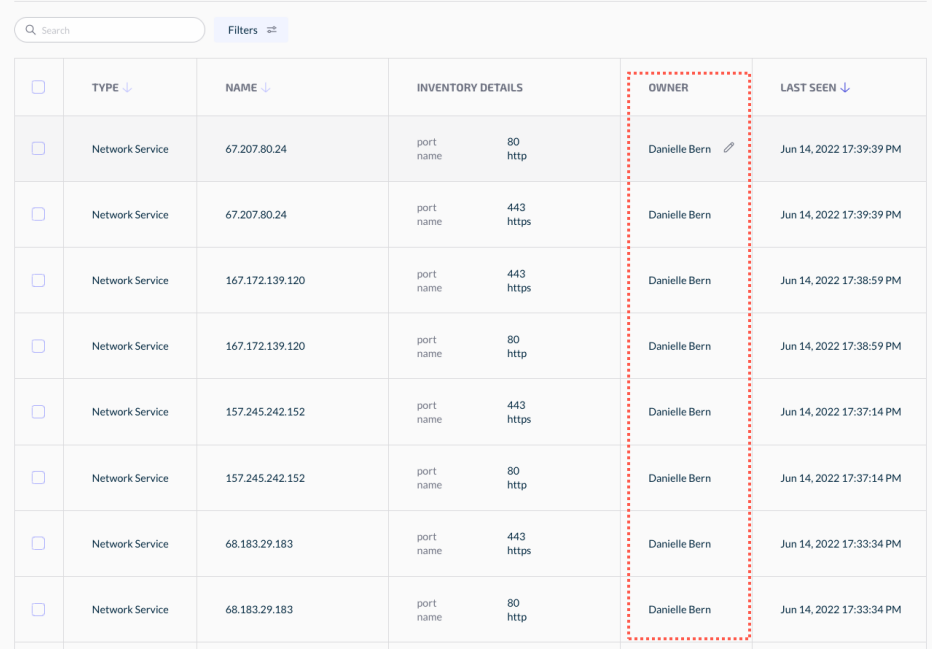
2. The **Edit Inventories** dialog box will display and show you the number of items you selected on the table which will be modified/edited.



3. In this example, we will change the **Owner** of the selected assets on the table. We click on **Save** when we are finished.

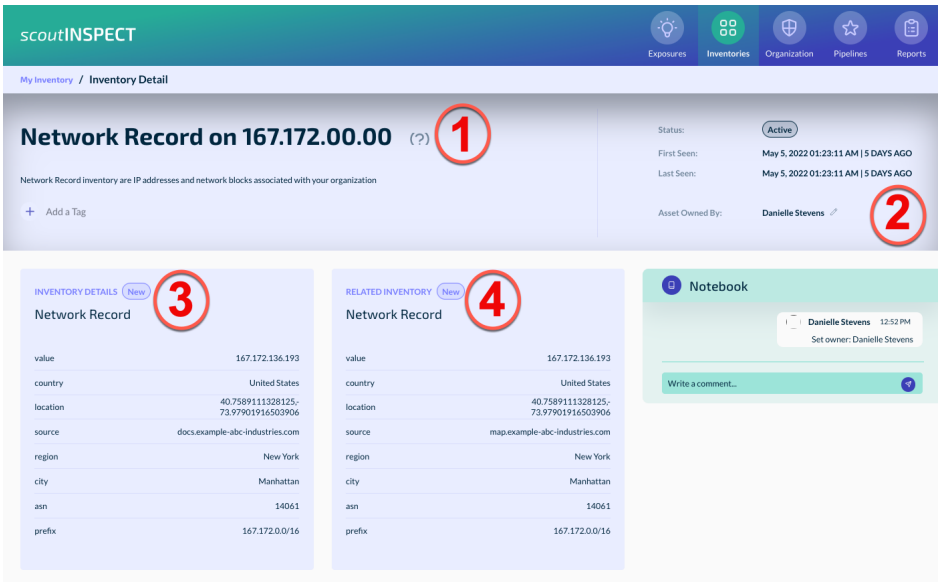


The table should now reflect the changes made on the assets that were selected.



My Inventory Details

When you click on the name of an asset from the Inventory table, a page will load with details about the asset.



#1. This section shows the asset name. Below is background information about the what the asset is or other details. You can add a tag for the asset here as well.

#2. This section contains details about the asset's status (e.g., Active, Inactive), date the asset was discovered, date the asset was last modified, and its owner. Depending on the type, the page will display boxes with information about the

asset's:
#3. Inventory Details - Provides information about the type of asset, including the software version (if any), category, description, source (IP address), raw, vendor, website (if applicable), cpe, product, etc.

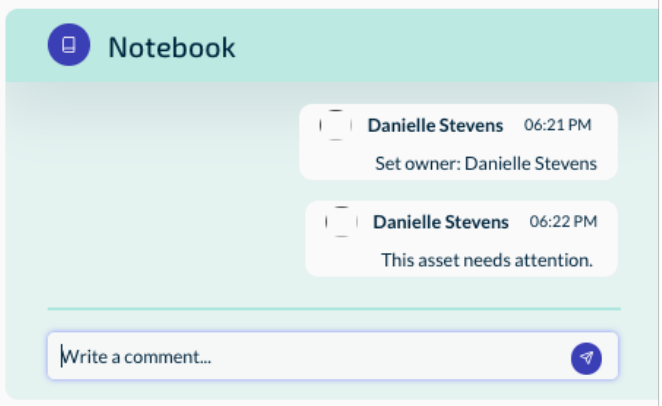
#4. Related Inventory - Provides information about any other assets in the inventory that are related to the asset (e.g., Network Services, DNS Record, etc.) Depending on the asset type, this box can contain details on the software version (if any), ip_str, name (e.g., http), cpe, OS type, port number, etc.

NOTE: You may have several **Related Inventory** records about an asset on the page.

Notebook

My Inventory includes a section called **Notebook** where analysts can write comments or ask questions about the asset.

Furthermore, when the asset is assigned an owner, **Notebook** will record the activity and add it as a comment (e.g., "Set owner: Jane Dully.")



---

scoutINSPECT User Documentation Table of Contents

Did this answer your question?

scoutTHREAT - Workflow Example: Creating Your First Threat Actor Object

Workflow for creating a Threat Actor object

Written by Dolores M. Bernal
Updated over a week ago

This workflow example consists of two parts: Using scoutTHREAT and Using TICE.
Following all the steps from the two parts will provide you with a good, first experience of what's possible when using these tools.

PART 1: Using scoutTHREAT

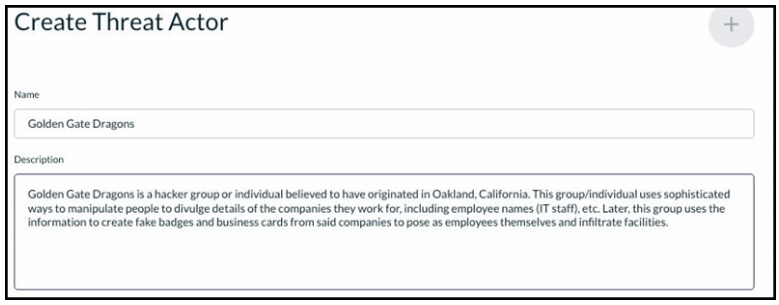
A lot of your cyber threat intelligence work will be spent creating and updating Threat Actor profile objects. Below are the basic steps for getting started with creating your first object.

Before you begin you must ensure scoutTHREAT has been configured correctly and that an Identity has been created for you and/or your organization. For steps on creating an Identity, see Workflow Example: Adding and Identity Object.

Once an Identity has been created, you can add a new Threat Actor profile. Follow these basic steps:

1. To add a Threat Actor Object, navigate to **Intelligence**, then click on **Threat Actor**.
2. If any exist, a list of Threat Actor objects will load with the item **Name, Type**, date **Created** and **Modified**.
3. Click on **Create New** on the top right side of the page.

4. Enter a **Name** and **Description** for your **Threat Actor** object profile.



5. On the right panel of the page, select the **Confidence** level you have about this Threat Actor. Choose a number from 1 to 10, 1 being the highest level.

6. Then, select the Threat Actor **Type** from the drop-down menu (e.g., hacker, competitor, nation-state, etc.).

7. Click on the empty field under **Aliases** to add alternative names used to identify this Threat Actor. Type the name of the alias then click on **Create**.

8. Next, you can choose from the drop-down menu the level of **Sophistication** the Threat Actor has when it comes to the skill, specific knowledge, special training, or expertise to perform an attack.

9. A Threat Actor can play many **Roles** such as agent, author, etc. Choose from the drop-down the role your Threat Actor object generally plays.

10. Next, choose the Threat Actor's **Resource Level** from the drop-down menu. This can include the organizational level at which this Threat Actor typically works, which in turn determines the resources available they can use in an attack.

11. Under **Primary motivation**, you can select the primary reason, motivation, or purpose behind this Threat Actor. The motivation is why the Threat Actor wishes to achieve the goal (what they are trying to achieve).

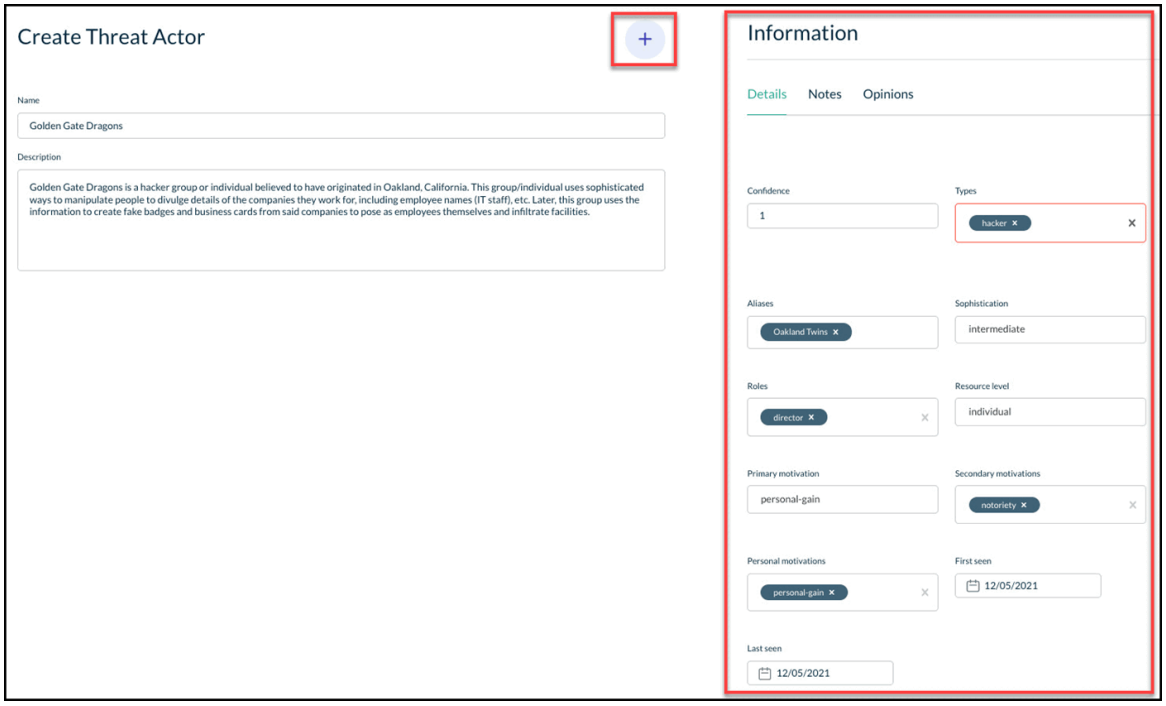
For example, a Threat Actor with a goal to disrupt the finance sector in a country might be motivated by ideological hatred of capitalism.

12. You can also add the Threat Actor's **Secondary motivation**. This property specifies the secondary reasons, motivations, or purposes behind this Threat Actor.

13. Next, you can select the Threat Actor's possible **Personal motivations**. This can include notoriety, revenge, coercion, personal-gain, and others.

14. It is optional to add dates for when the Campaign was **First seen** and **Last seen**. To add dates, click on **Select Date** fields to choose from the calendar.

15. Click on the + in the center of the page to save the information.



You can also add Notes, Opinions, Checklists, and Relationships to the profile. For more detailed steps, see Audit, Notes, & Opinions.

After creating the Threat Actor object you can receive and gather intelligence data from the TICE cloud.

PART 2: Using TICE

Before you log in to the **Threat Intelligence Collaboration Environment (TICE)** module to view intelligence data from the cloud, you must first create and trigger a Threat Query for the Threat Actor profile.

A Threat Query is a saved search for finding Threat Actor names, Malware names, etc. in the system. For more information, see Threat Queries.
1. On scoutTHREAT, navigate to **Search**.

2. Next, type in the name of the Threat Actor in the search box.

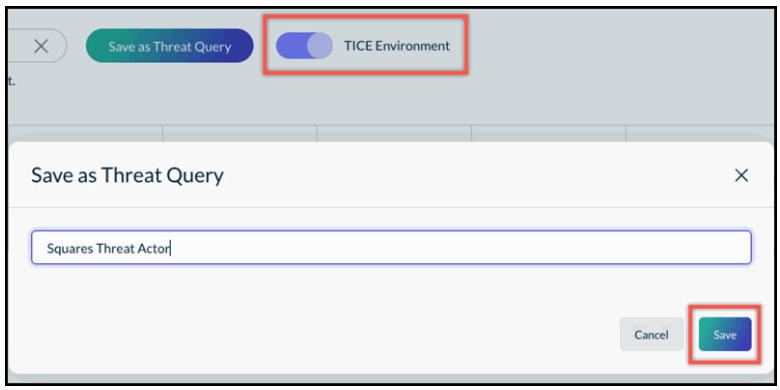
3. Checkmark the Threat Actor box under **Filters**, then click **search**.

Since this is your first time using scoutTHREAT, it is likely that you will not get

any results for your Threat Actor.
4. Next, enable **TICE Environment** by clicking on the slide button.

5. Click **Save as Threat Query** on the top right side of the page.

NOTE: You can still save your search even if no results were returned.6. A pop-up window will be displayed asking you to enter a name for your **Threat Query**. When you are done, click **OK**.



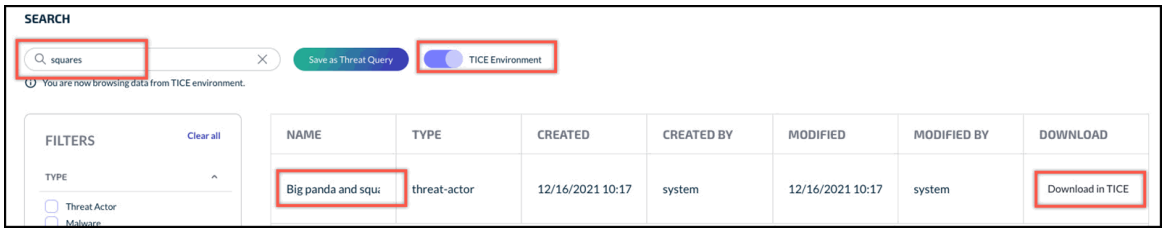
7. Next, confirm your threat query was saved by navigating to **Workflow** then to **Threat Queries**.

8. Click on the **TICE Environment** slide button.

9. Look for the Threat Query you had saved on the list and click on **Run Now** in the **Actions** column to trigger it.

10. After waiting about 15 minutes, you can go back to **Search**, click on **TICE Environment,** then run another search.

11. If any intelligence was found in the cloud it will now appear in the search results. Click on **Download in TICE**.



12. Next, log in to the TICE Module and navigate to the **Validation** page to look for the item(s) you clicked to download during your search.

13. To download the data item(s) to your scoutTHREAT system, you must follow the validation process to **Approve** or **Reject** the item.

14. Click on **Review** and ensure the destination of the data is **scoutTHREAT**.

15. If all the information on the page looks good to you, click **Approve**.

Once you have downloaded intelligence data from the TICE Module, it will populate various areas of scoutTHREAT depending on the intelligence type.

For example, if you approved and downloaded a Threat Actor item, you will now see that object in your scoutTHREAT system.

For more information on using TICE, see The Threat Intelligence Collaboration Environment (TICE).

In Brief

Related Content

- Supported Browsers
- Logging in

scoutTHREAT User Documentation Table of Contents

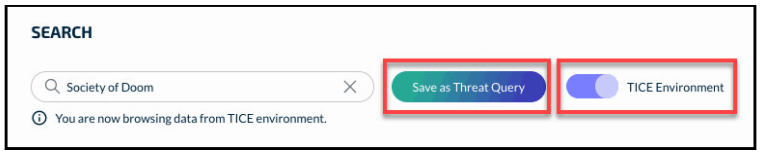
scoutTHREAT - TICE Workflow Example

Written by Dolores M. Bernal
Updated over a week ago

Let's imagine a scenario where the evening news reports a cyber attack by a Threat Actor called *Society of Doom* which targets organizations in your sector. As an analyst, you would want to gather as much information as possible about this hacker group.

1. Start by doing a search on scoutTHREAT to look for already existing data about the group in your system or with TICE Environment enabled.

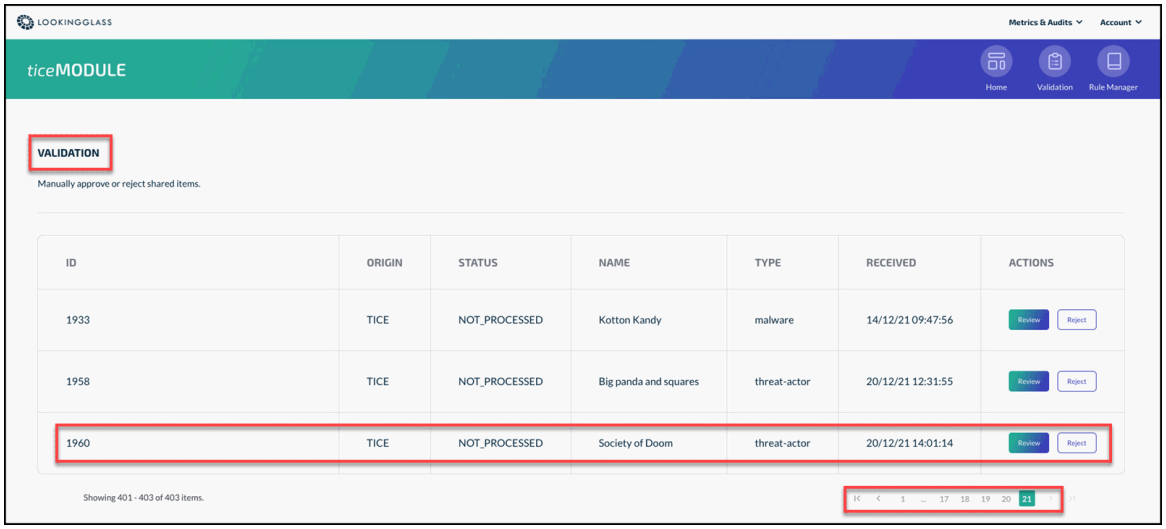
2. If few or no results return on the subject, you can save the search as a Threat Query.



3. After saving the Threat Query, you can navigate to **Workflows -> Threat Queries** and click on **Run Now** from the list. Once triggered, the Threat Query cues TICE to start pulling data from the cloud about the group.

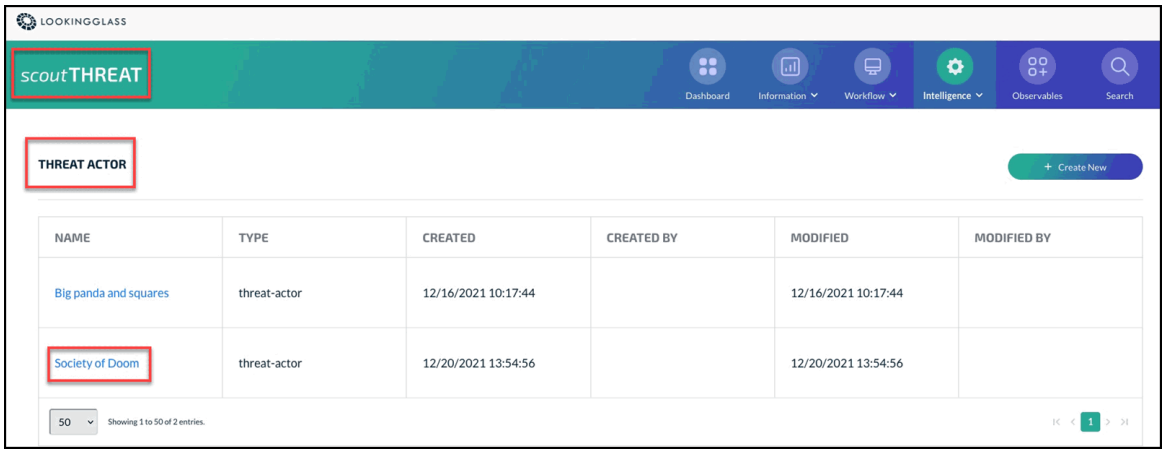
4. Next, you would want to log in to the TICE Module to check if any intelligence data about **Society of Doom** has been shared with you by the landlord and tenants.

NOTE: Intelligence items are listed from oldest to newest, so make sure you use the pagination arrows to navigate to the last page to check for new results.
If any results about the hacker group are on the **Validation** list, you can click on **Review** to view the information.

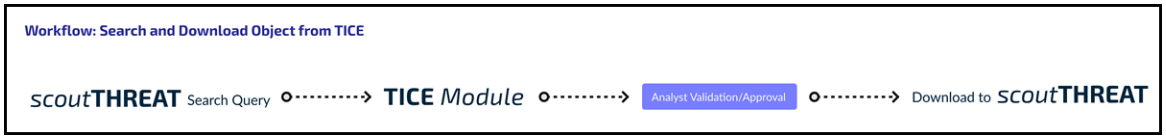


5. When you click **Review** you will see information about the intelligence data item that interests you. If you would like the item to download to scoutTHREAT click **Approve**.

6. Now, go back to scoutTHREAT and navigate to the Threat Actors page. The item you downloaded from TICE should now appear on the list.



In Brief



Related Content

- The Threat Intelligence Collaboration Environment (TICE)
- TICE Login
- The TICE Homepage
- The TICE Module Validation Process
- Validating Intelligence Items
  - Updating scoutTHREAT Objects with New TICE Information
  - Validating and Adding New TICE Intelligence to scoutTHREAT
- Sharing to TICE
- Steps for Sharing Intelligence to TICE
- The TICE Rule Manager
  - Adding Rules with Rule Builder
  - Adding Rules Manually
  - JXEL for Creating Rule Conditions
- Metrics and Audits

scoutTHREAT User Documentation Table of Contents

Did this answer your question?

scoutPRIME - Product FAQs

Answers to customer most frequently asked questions.

Written by Dolores M. Bernal
Updated over a week ago

At LookingGlass Cyber we want to make sure you get answers to important product questions so you can use scoutPRIME as efficiently and effectively as possible.

Below are frequently asked questions from customers about scoutPRIME features and functionalities. We hope that this information can help you accomplish your security goals and mission.

Feel free to also submit your questions at, support@lookingglasscyber.com.

TIC and TIC Score FAQs

Q. What is TIC?

A. The Threat Indicator Confidence (TIC) Score is a comprehensive, multi-dimensional score that measures the likelihood that a network element has been compromised, is vulnerable to compromise, or is a likely target for future compromise. The algorithm for TIC factors network proximity, multi-source corroboration, impact of compromise, and time of observed compromise.

This powerful algorithm by design brings together multiple dimensions of analysis into a single score from 00-100. Factors include:
· Trustworthiness of the intelligence source
· Risk and presence of compromise
· Impact of compromise
· Class of compromise
· Network relationship to compromise
· Corroboration of observation
· Volume of compromises
· Time since observed compromise

Using the TIC score, and any associated intelligence that goes with it, can help you better analyze risk.

scoutPRIME provides a TIC Score for:

- Elements (IPs, FQDNs, CIDRs, and ASNs)
- Overall collection health
- Threats
- Vulnerabilities

Q. How is TIC derived?

A. Each network element, collection, threat, and vulnerability is assigned a system-generated TIC score. Scores are calculated differently for each (refer to the table below).

Type	Score Calculation Summary
IPv4, IPv6	Composite score based on all associated ASNs, FQDNs, Threats, and Vulnerabilities
FQDN	Composite score based on all associated ASNs, IPs, Threats, and Vulnerabilities
ASN	Composite score based on all associated CIDRs, IPs, FQDNs, Threats, and Vulnerabilities
CIDRs	Composite score based on all associated ASNs, IPs, FQDNs, Threats, and Vulnerabilities
Threats	Composite score based on the source, criticality, and classification
Vulnerability	Composite score based on the source, criticality, and classification
Collections	Composite score based on all elements in the collection, including associated IP addresses (v4 and v6), CIDRs, ASNs, FQDNs, Threats, and Vulnerabilities

Q. Why do TIC scores fluctuate?

A. TIC scores can increase if new observed threat data associated with elements, threats, and vulnerabilities from our many sources is ingested by the system. scoutPRIME will use a sophisticated algorithm to sum up the risk into a single number value.

After two weeks, if associations are deemed inactive they become Historical. This will change the TIC score, otherwise the the score will remain constant.

Q. What are the TIC levels?

A. The system assigns scores ranging from 1-100 that categorizes the current threat risks associated with various system elements. Higher numeric values indicate a greater threat potential.

Severity	Range
Default	Score: 10
Critical	Score: 75-100
Elevated	Score: 50-74
Normal	Score: 1-49

Assigning a Score of Zero

When a score of zero is assigned to a threat, this tells the system not to include this in the calculations or the composite score. To get the system to ignore a threat, set the Criticality property score to zero, and the threat is no longer able to apply influence to any elements automatically.

Q. Why is "10" the base score?

A. The default TIC score is 10. Scores greater than 10 indicate increasing levels of risk.
Scores below 10 indicate positive assertions of risk reduction due to mitigation actions taken. There are currently no data sources providing a TIC score less than 10.

A score of 10 also means that the system hasn't registered anything necessarily positive or negative about the element, collection, etc.

Threats & Vulnerabilities FAQs

Q. Does scoutPRIME have active threats and historical threats, or just active ones?

A. scoutPRIME has historical and active threats. If you go to a specific element you can view historical threats for that element. Searching works for active threats, but you can include historical details using the API.

For more on this, click here.

Q. How long does the system keep historical threats?

A. The default set of time is six months.

Q. Which data objects are available in scoutPRIME?

A. scoutPRIME's rich data, includes the following types of objects/digital assets and elements:

- IP addresses (v4 and v6)
- FQDNs
- CIDRs (v4 and v6)
- DNS records
- WHOIS information
- File hashes
- Threats
- Vulnerabilities
- Owners
- Countries
- GeoLocations
- Enumeration details
- Security Certificates
- Notes

Data/Data Feeds FAQs

Q. How often to data feeds update?

A. We collect a vast set of propriety, commercial, and open source data sets on a continuous basis. While each data set is unique, the underlying data will typically update within a day.

Q. What types of metadata are in scoutPRIME?

A. The volume and set of metadata is massive. Here's a sampling of common metadata:

- First and last seen date
- DNS history
- WHOIS details
- GeoLocations
- File hashes
- Product information (if applicable)
- Host enumeration
- Ownership details

- Notes

Q. In what format(s) can I access and export the data?

A. Comma-separated values (CSV) and JSON. You can also create reports which generates PDF files.

Q. Is the data mapped in some industry standard, such as MITRE ATT&CK or Lockheed Martin Kill Chain or some other industry standard?

A. scoutPRIME data can be transformed into STIX v1.x, v2.x, or MITRE ATT&CK. If you are interested, please reach out to our customer services team at support@lookingglasscyber.com.

Q. Is the data available via a TAXII server?

A. Currently, LookingGlass is exploring making data available through a TAXII server to customers. For more information about this please contact, support@lookingglasscyber.com.

Collections FAQs

Q. What is a collection?

A. A collection is a set of elements that defines the attack surface of an organization, entity, or system, along with any additional information that may be available.

The elements that may be included in a collection include:

- Owners
- ASNs
- CIDRv4, CIDRv6
- FQDNs
- IPv4 and IPv6 addresses

For more about Collections, click here.

You may also find our Key Terms article useful, click here.

Q. How do I build a collection?

A. You can build an "empty" collection (without doing a search first), or you can build a collection from search results. You can also create nested collections (children collections).

For a complete workflow on how to build an empty collection, click here.
For a complete workflow on how to build a collection from search results, click here.

Q. What are nested collections?

A. Nested collections are "children collections" belonging to a "parent" or main collection and can be very useful for organizing or categorizing your data into sub groups. You can nest up to three children collections.

In addition, parent collections with children have a more accurate TIC score. This is because scores "aggregate up" in a collection, meaning that the scores of children collections help derive the score of the parent collection.

For a workflow on how to create nested collections, click here.

Q. Recommended/best practices to build a collection?

A. The recommended best practices are:

- Give your collection a clear, specific name to help you identify it. Avoid using names like "Collection One," "Collection from yesterday," etc.
- Give your collection a description so that you or others in your team can know and understand what it is.
- Set up notifications for each collection that way you can spot and keep track on any suspicious activity. For information on how to set up notifications, click here.
- Take advantage of using nested collections if it will help keep your work more organized.

Q. How do I know how "complete" my collection is? ("*Did I get*

everything?")

A. Some techniques for ensuring you have a complete collection include:

- Favoring owners - These are dynamic and pull into the collection all CIDRs and IPs.
- Review DNS records on owned assets.
- Check the organization's primary domains.
- Run owner-based searches to find additional owned assets.
- Check with the organization in question (where applicable).
- Ensure you have collection groups in workspaces. Each workspace should have its own clear purpose and mission.

Using scoutPRIME FAQs

Q. What can I search for in the Search bar?

A. You can do many types of powerful searches in scoutPRIME and get back lots of enriched data.

Below are descriptions of what each of the four filters in the Search bar's drop-down menu can help you find:

- **All** - Allows you to conduct a standard search for an online asset/element. You can search by domain name (FQDN), IP address (IPV4 or IPV6), CIDR4 and CIDR6, ASN, and Owner.

- **Map** - Allows you to see the geolocation(s) of the online asset.

- **Reverse Whois** - Allows you to search for domains by the name, address, telephone number, email address or geolocation of the registrant listed in current or historical Whois records.

- **Associated Risks** - Lists any Threats and Vulnerabilities associated with an online asset/element.

To learn more about using scoutPRIME's search features, click here.

Q. What are common workflows?

A. The scoutPRIME User Documentation provides you with several common

workflows that you guide on how to perform many important tasks.

One of the most common workflows on scoutPRIME is on how to create a collection - click here to learn more.

Another workflow is on how to create notifications or alerts for your collections - click here to learn more.

If you are looking for a workflow on how to conduct a search, you can find it here.

You can browse through the user documentation for more workflows and other helpful steps to maximize your use of scoutPRIME's powerful features.

Q. What are typical/standard use-cases of scoutPRIME?

A. scoutPRIME is widely used by customers to monitor the digital assets of their organization and/or vendors in their supply chain.

The platform's enriched data can inform analysts about potential cyber hazards and threats and vulnerabilities that their or another organization's digital assets could be facing.

scoutPRIME's TIC score also provides insight into the growing or decreasing risk of collected digital assets. This allows analysts to take action and mitigate risk, including third-party risk.

Q. Does scoutPRIME allow me to monitor cloud service and Internet service providers?

A. You can use scoutPRIME to monitor the digital assets of any entity, including companies that do business with you such as cloud service and Internet service providers.

Please note that the platform conducts only passive scanning of digital assets, therefore the data you receive from entities is already in the public domain.

Q. How do you associate network assets to owners?

A. Networks are associated to owners through the ASN registration.

Q. Is there a way “non-technical” users can craft automated queries for recurring analysis requests and/or integrations?

A. Users need to feel comfortable writing queries and making HTTP requests, therefore technical knowledge is needed.

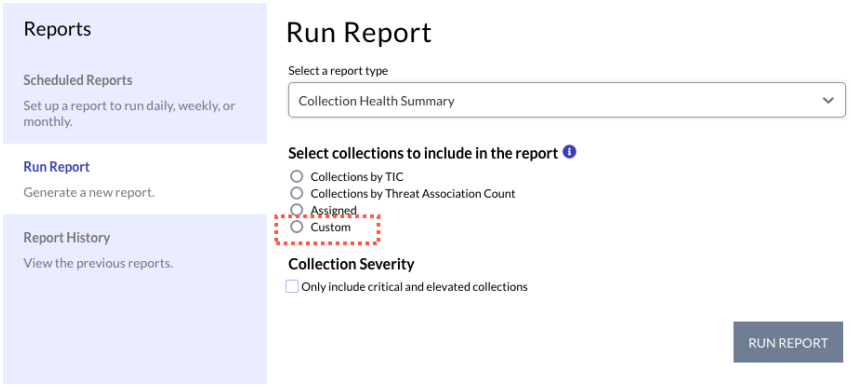
Q. Does scoutPRIME have reporting?

A. Yes, you can generate many types of reports on scoutPRIME. For more details, refer to this article.

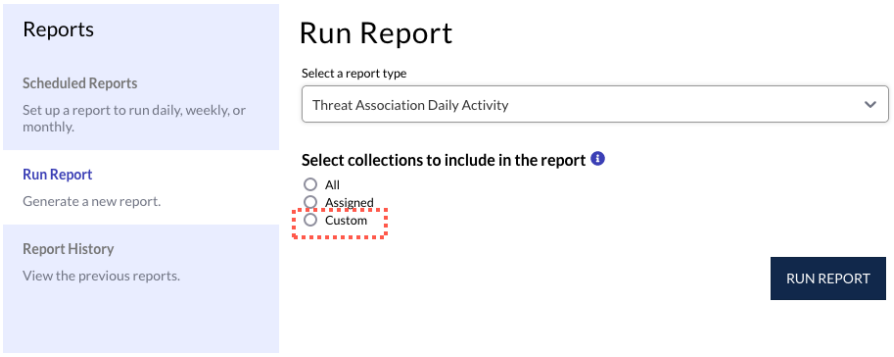
Q. Can I create “custom” reports?

A. Yes, you are able to run custom reports for:

Collection Health Summary



And, for **Threat Association Daily Activity.**



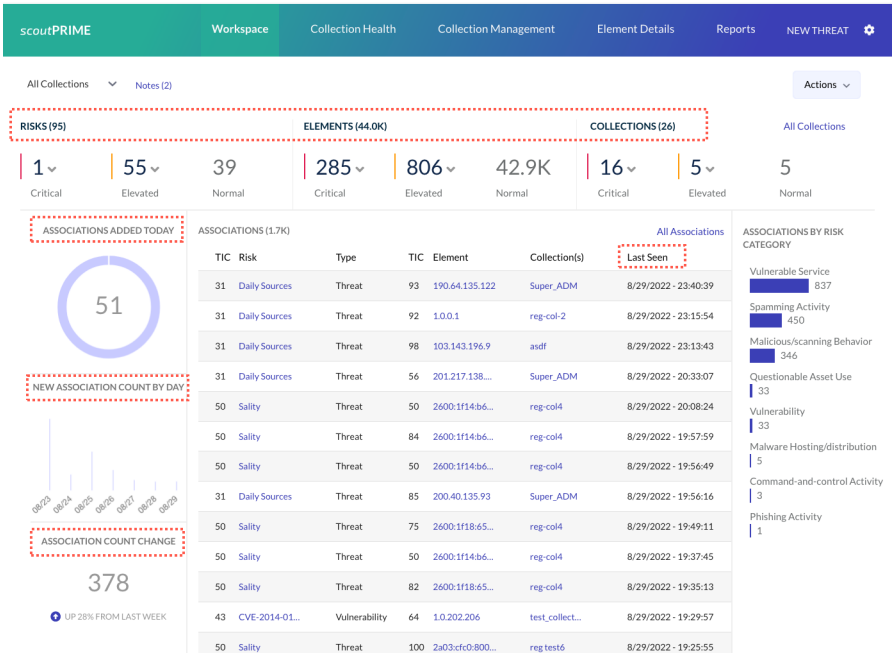
For more details, click here.

Q. Can I see my “most recent” risk information?

A. Yes, scoutPRIME has a **Dashboard** that provides you with snapshots of your workspace collections with recent TIC scores and the latest associations (threats and vulnerabilities), etc.

Recent information you will find on the Dashboard, includes:

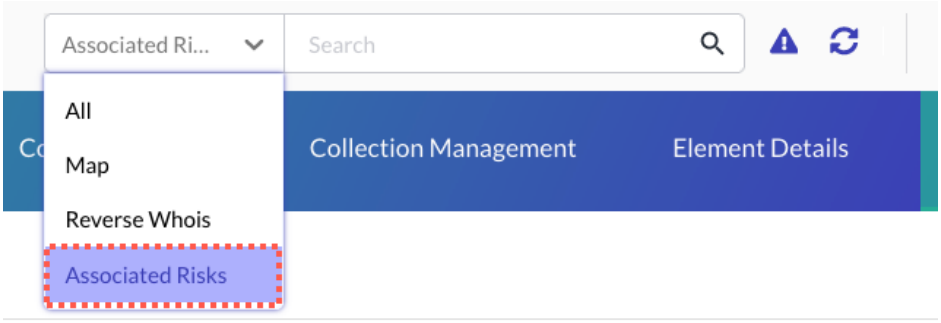
- Associations Added Today
- New Association Count by Day
- Association Count Change
- Criticality of Risks, Elements, and Collections
- And, more.



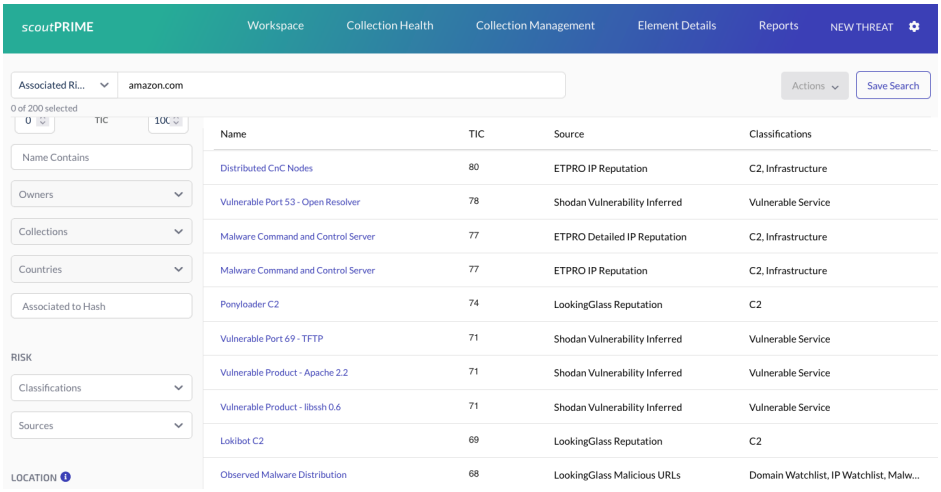
For more on this, see the article for The Dashboard.

Q. How do I find network assets associated with a CVE/vulnerability?

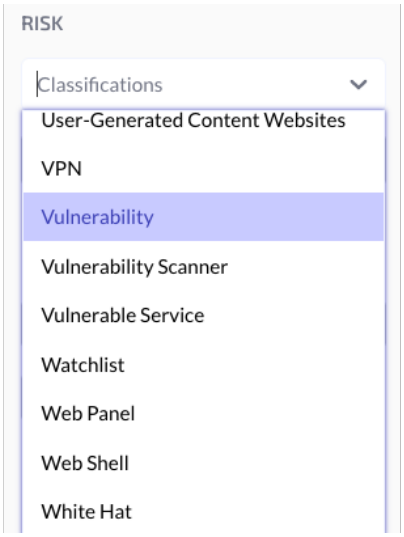
A. First, do a query or search for the element/network asset using the **Associated Risks** filter.



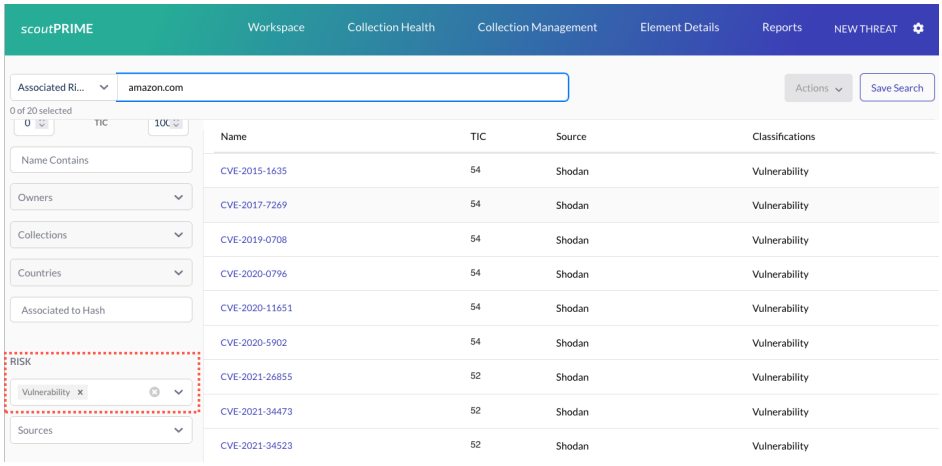
The results page will list any risks for the network element you entered in your search.



You can narrow down your search results by using the **Risk** filter on the left panel of the page. Choose **Vulnerability**.



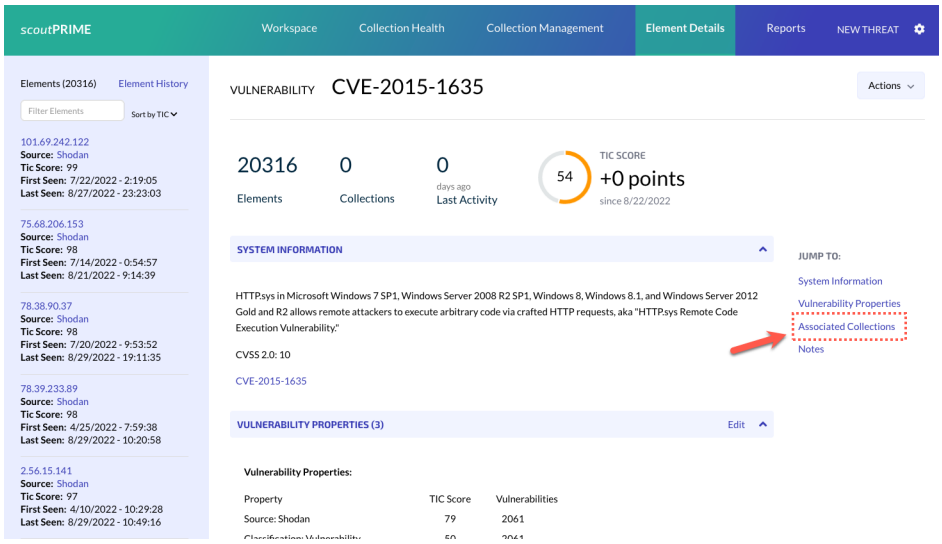
Finally, with the filter applied, scoutPRIME will load only vulnerabilities (if any) on the results page.



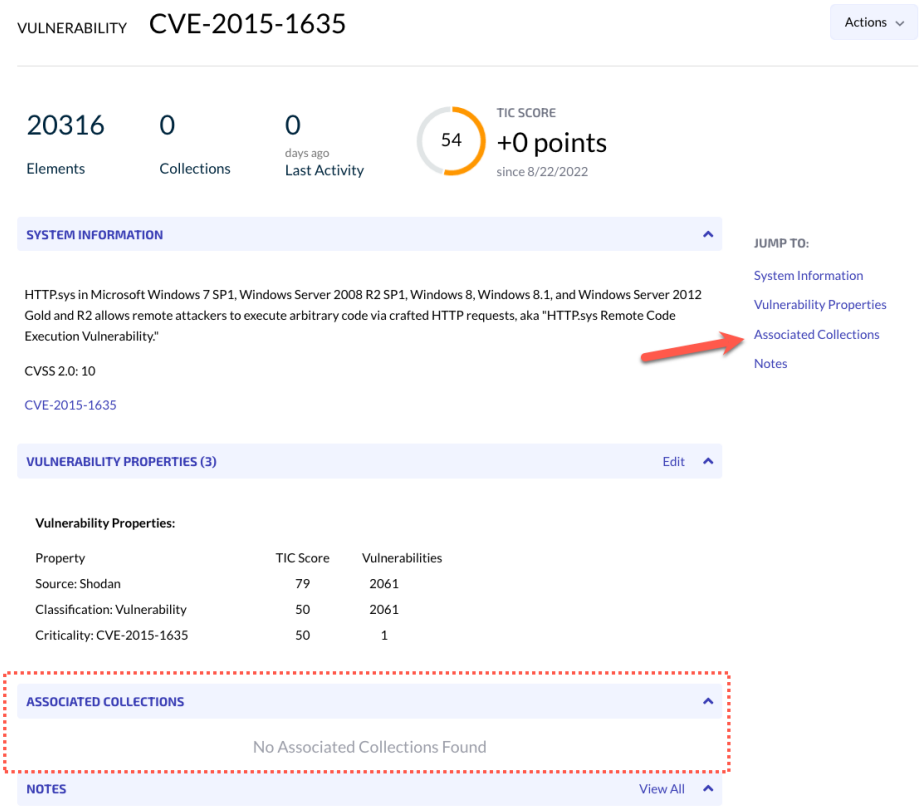
These are the CVE/vulnerabilities associated with the network asset.

Q. How do I determine if any of those network assets associated with a CVE are mine or in a collection I built?

A. When you click on a CVE/vulnerability listed on a search results page, its details will display on the **Element Details** section. To determine if the vulnerability is in any of your collections, click on **Associated Collections**.



If the CVE/vulnerability is in a collection you built, the system will list it under the **Associated Collections** section of the page.



Q. There are a lot of indicators in the platform, so for example, how do I know which malware indicators are the ones delivering the malware/attacking, and which indicators are the ones where someone has been infected by malware?

A. There are “keywords” in the indicators and within the enrichment fields that LookingGlass adds to the data sources scoutPRIME is aggregating and correlating.

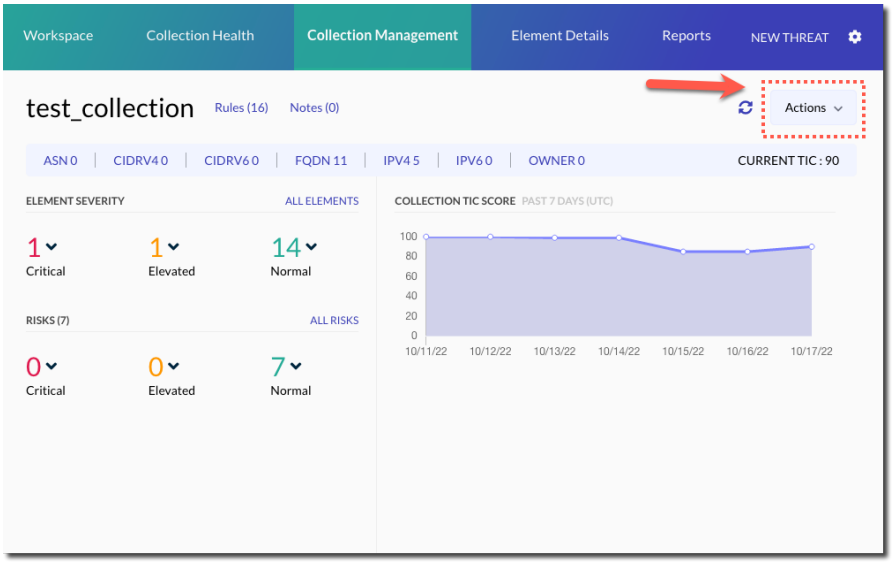
These keywords indicate to the user which indicators, and their related IoCs, are “attacker infrastructure” vs. “victim/infected infrastructure.” By leveraging these pieces of information, the scoutPRIME user can discern which indicators and IoCs should be used for network log correlation or deployment to a firewall vs. which indicators and IoCs should be used for incident response, vulnerability management/patching, or target/victim notification.

Q. How do I extract all indicators or elements associated with a specific threat?

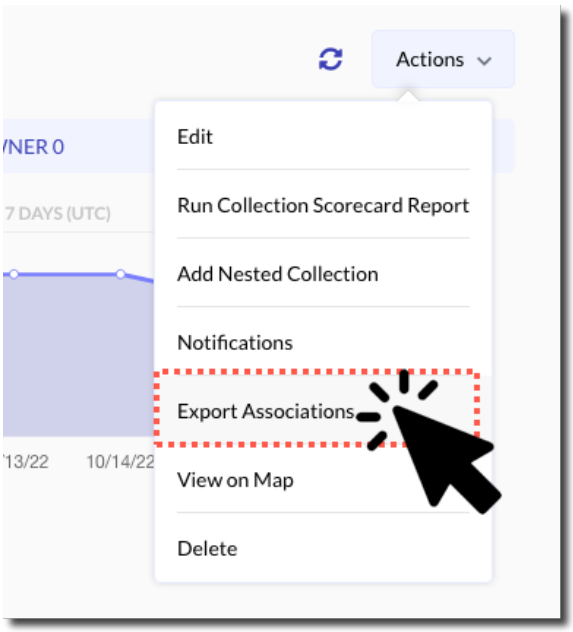
A. To extract all indicators or elements from a collection, follow these steps:

1. Go to the collection you want to extract the elements from. The collection will open in the **Collection Management** section.

2. Then, click **Actions** on the right side of the screen.



3. From the drop-down menu, click **Export Associations**.



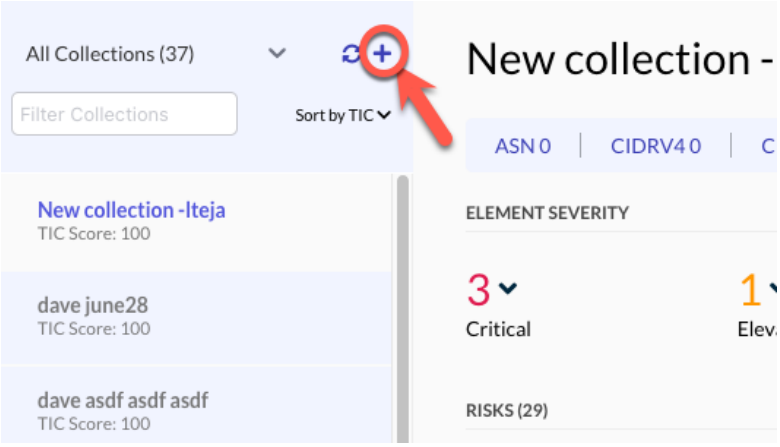
Associations will be downloaded to your system as a CSV file.

Q. I have an organization's network footprint. How do I create a collection to monitor it?

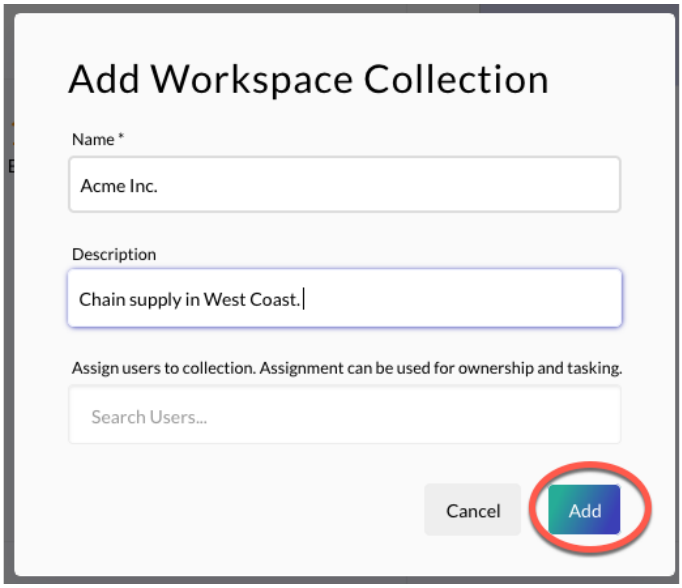
A. You can create collections with network elements that you import from your workstation. Once the data is ingested, you can monitor the elements. In addition, scoutPRIME provides TIC scores for the collection and what you've added to it.

To add your own data to a collection, follow these steps:

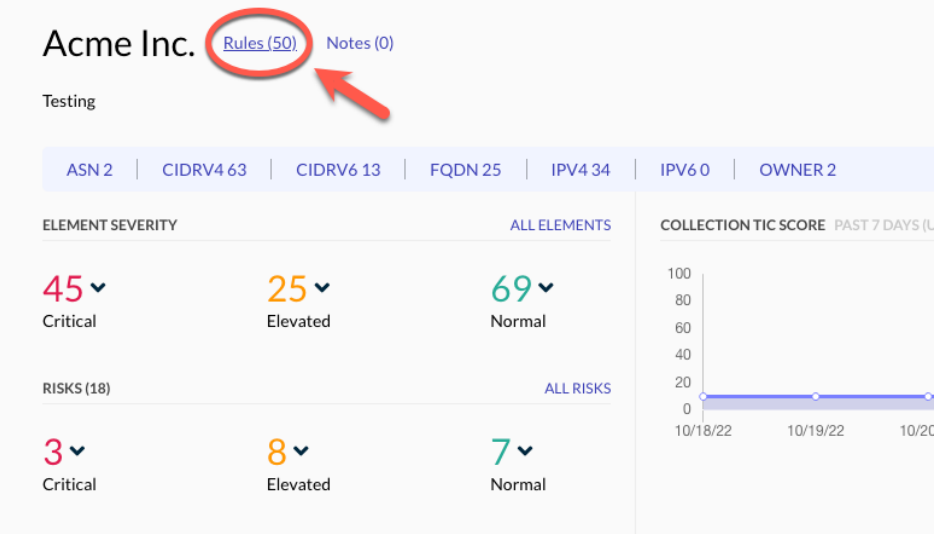
1. Create a new collection by clicking the plus sign on the top left side of the **Collections** panel.



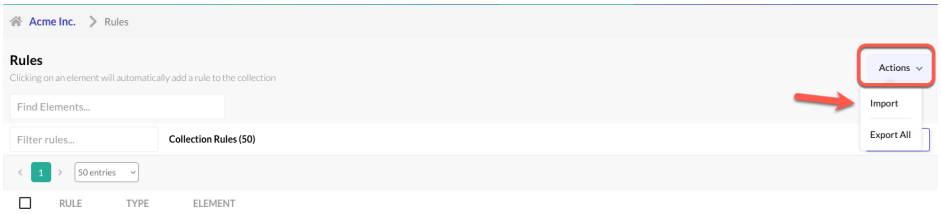
2. Give your collection a **Name**, **Description**, **Assign users** (optional), then click **Add**.



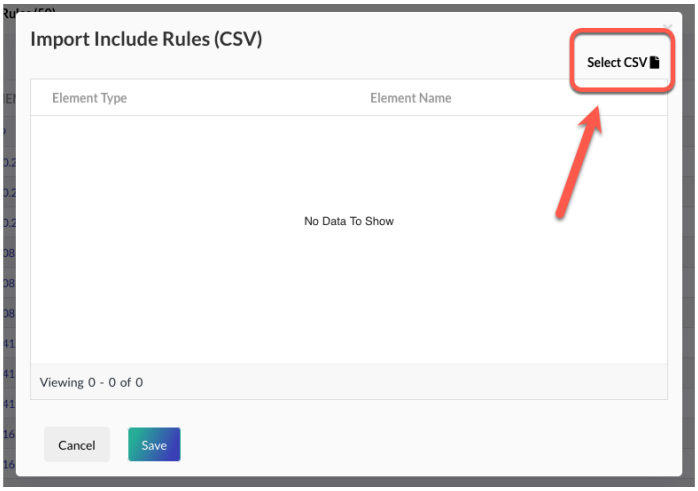
3. Next, near the top of the collection name, click **Rules**.



4. On the Rules page, click **Actions**, then select **Import** from the drop-down menu.



5. In the dialog box, click **Select CSV** to begin the importing process.



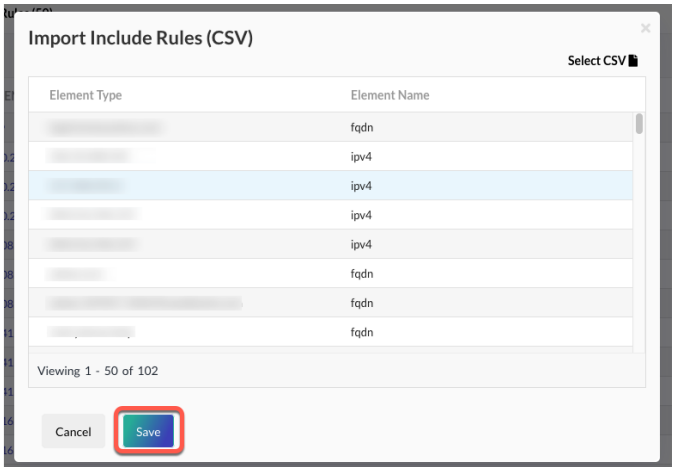
IMPORTANT: Your CSV file must have a header row with: element type ("Element Type") and the element name ("Element Name"). The items should be separated by commas.

Sample formatting:

Element Type, Element Name
asn,39981

cidrv4,10.1.0.0/24
fqdn,www.google.com
ipv4,172.16.254.1

6. After selecting the CSV file, the dialog box will display your data under the **Element Type** and **Element Name** columns. Click **Save** to finish importing.

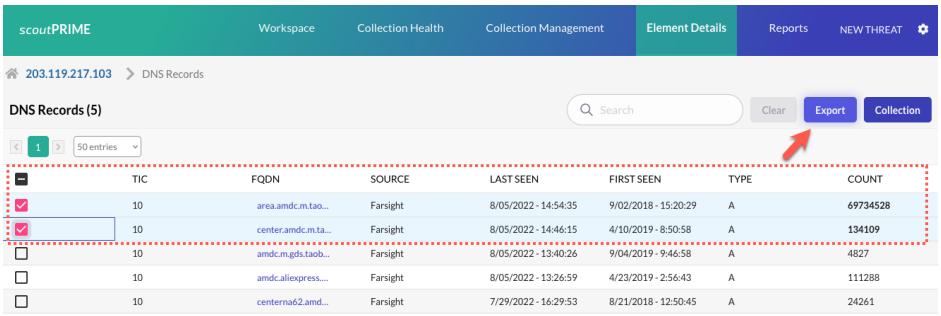


Q. How do I integrate scoutPRIME to a SIEM, SOAR, TIP, ticketing system, firewall, IDS, or IPS?

A. Our support team can provide you with scripts you can utilize to integrate the scoutPRIME API with third-party platforms, such as Splunk, Sentinel, etc. For more information, send an email to: support@lookingglasscyber.com.

Q. How do I export data?

A. You can export elements or rules (e.g., DNS records, IP addresses, etc.) as well as associations (threats and vulnerabilities) whenever you see the option to **Export** on a page. See example below. When you choose to export data, it will typically be in CSV or PDF format.



For a workflow on how to export element details, click here.

Ask Us!

If you'd like to submit a question, send an email to: support@lookingglasscyber.com. We'll get back to you as soon as possible.

scoutPRIME User Documentation Table of Contents