knowledge17
May 7–11, 2017 • Orange County Convention Center • Orlando, FL

Lab Guide

Threat Hunting, Awareness, and Sharing with Security

Antoni Kew, Alex Yupanqui, and Scott Lewis

Default Login / Password: Knowledge17

admin / Knowledge17

Lab Sponsored by Amazon Web Services



This
Page
Intentionally
Left
Blank

Lab Goal

This lab explains how to fully take advantage of the new features in the Threat Intelligence application. This lab walks you through Active Sighting Searches and Trusted Security Circles.

Lab Logistics

Agenda

Threat Intelligence overview

Why Sighting Searches

Trusted Security Circles and use cases

Lab 1.1 Configure Log Store

Lab 1.2 Configure Threat Central

Lab 2.1 Security Incident Walkthrough

Lab 2.2 Manual Sighting Search

Lab 2.3 Review Results from Search

Lab 3.0 Trusted Security Circles Query

Lab Bonus URL Sightings Search

Lab Goal

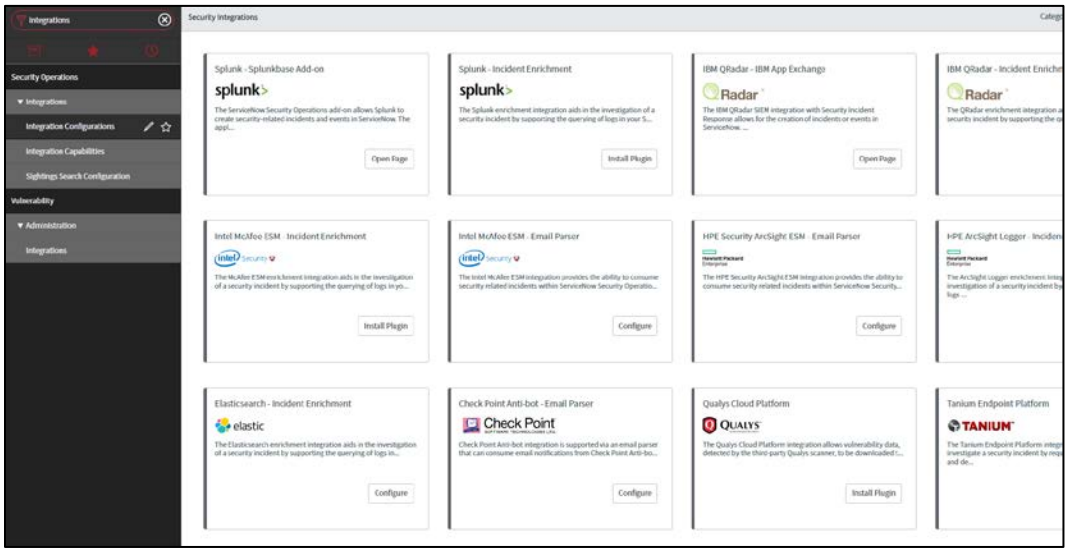
Lab 1.1
Configure Log Store(s)

Sightings Searches do exactly what they say. To do this ServiceNow needs to know where to search. ServiceNow can search in one log store or many log stores. This all depends on where you are storing logs!

For the purposes of this lab, you have an instance of ElasticSearch available to search.

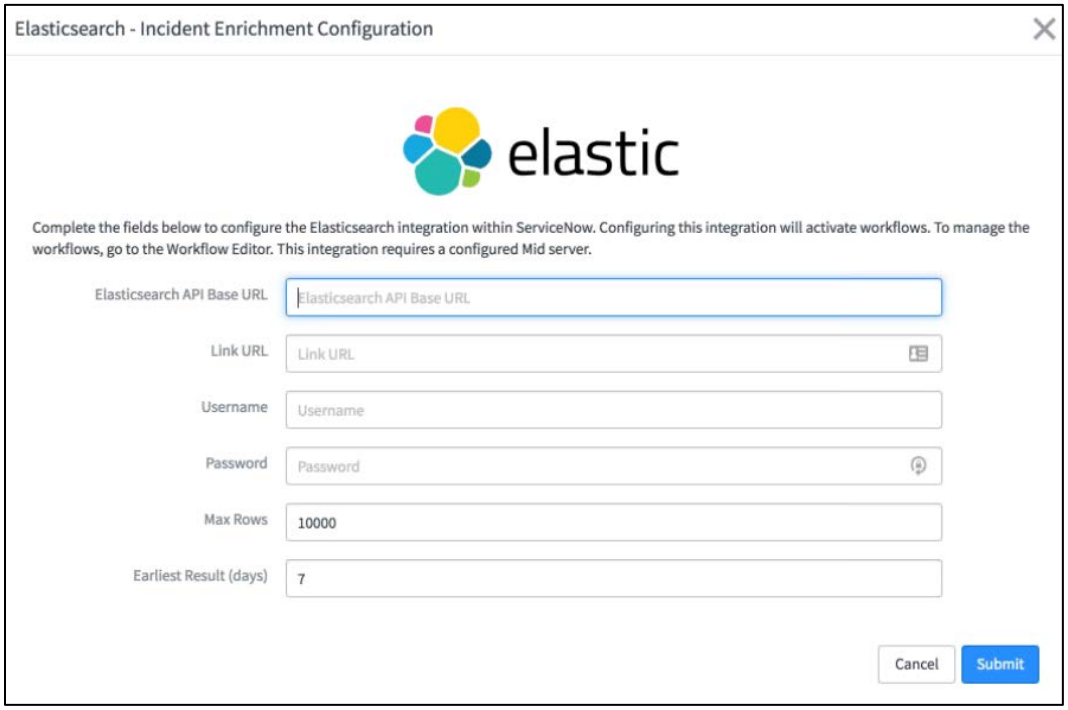
Elastic Search

1. From the **Filter Navigator** in the top-left corner of your instance search for **Integrations**.



2. From the Integration options click **Configure** for **Elastic Search**.

3. Within the **Elasticsearch - Incident Enrichment Configuration** dialogue box, **configure the fields** based on the handouts given to you by our **Friendly Lab Gurus**.



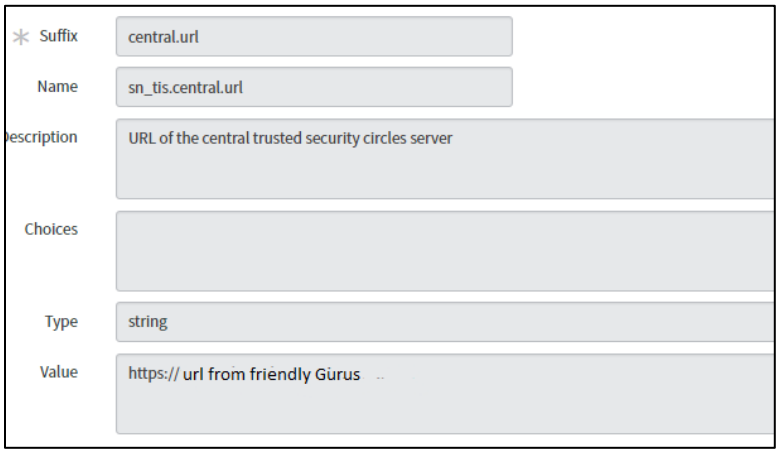
Lab Goal

This lab explains how to configure Threat Central connection.

Lab 1.2 Configure Threat Central

1. From the Filter Navigator type **sys_properties.list** to see a list view of system properties. From that view search for a system property with the name sn_tis.central.url.

2. Click **sn_tis.central.url** and from within that record update it to the value shared with you by our **Friendly Lab Gurus**.

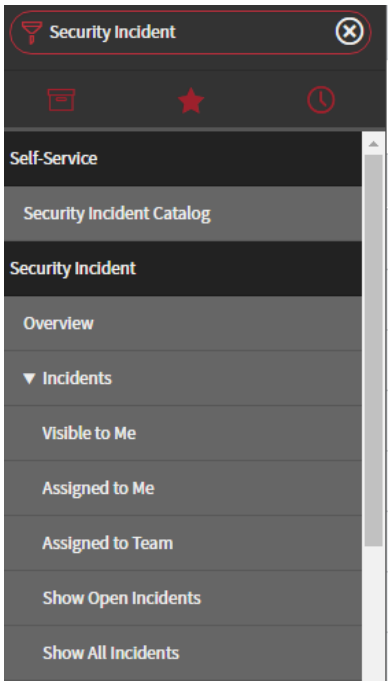


Lab Goal

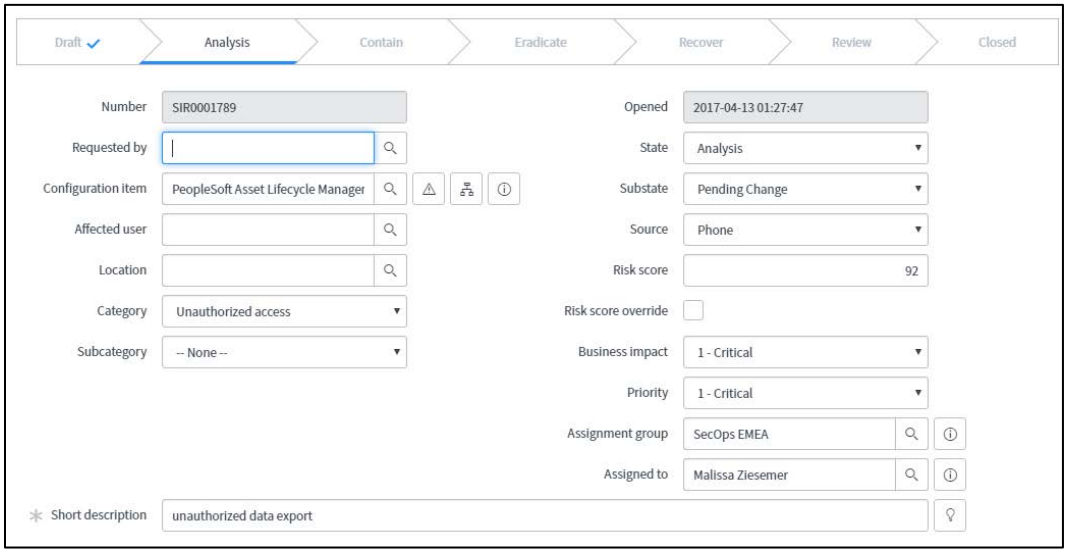
This lab explains Sighting Searches within the context of an incident.

Lab 2.1 Security Incident Walkthrough

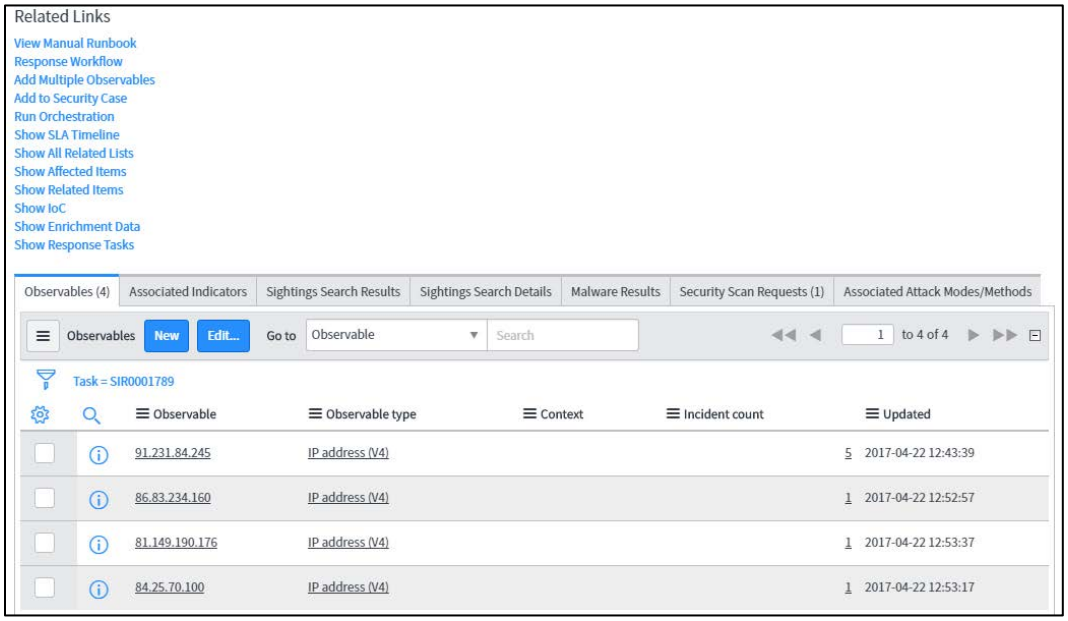
1. From the **Filter Navigator**, search for Security Incident. Find and **click Show All Incidents**.



2. From the list of open incidents, find the one listed in the handouts given to you by our **Friendly Lab Gurus** and click it.



3. From within the incident form, scroll down and **click on Show IOC**.

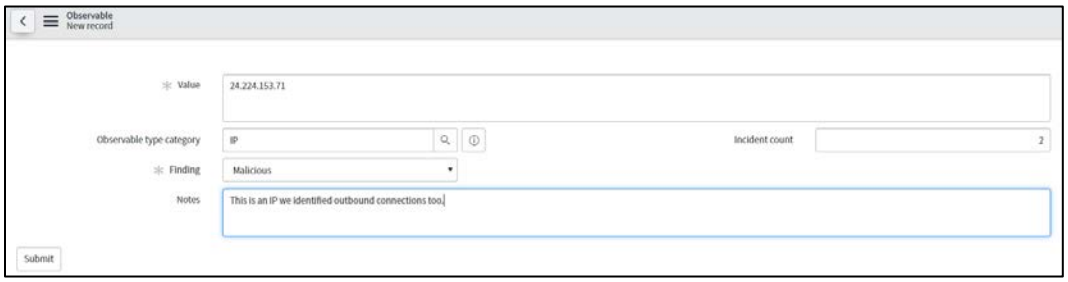


4. You can see here several observables that are associated with this incident.



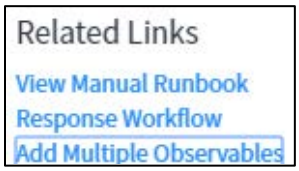
5. Add some additional observables that have been identified as part of an investigation (see your handout).

6. Click **New** and enter an **observable**.



7. Click **Submit**.

8. You can also use **Add Multiple Observables**.

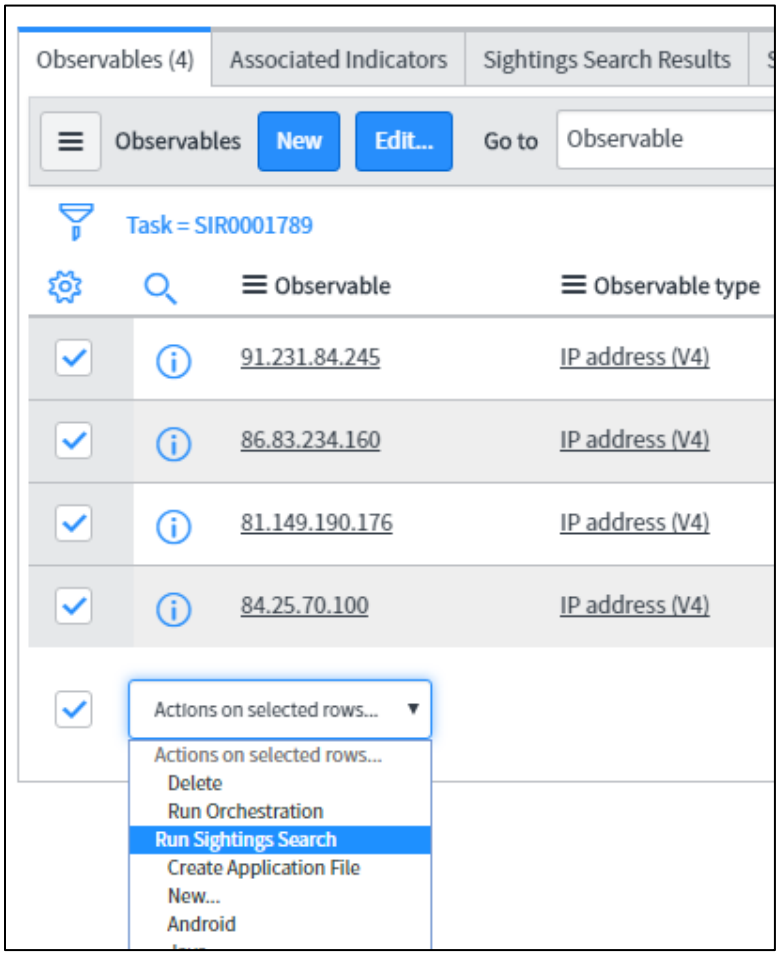


Lab Goal

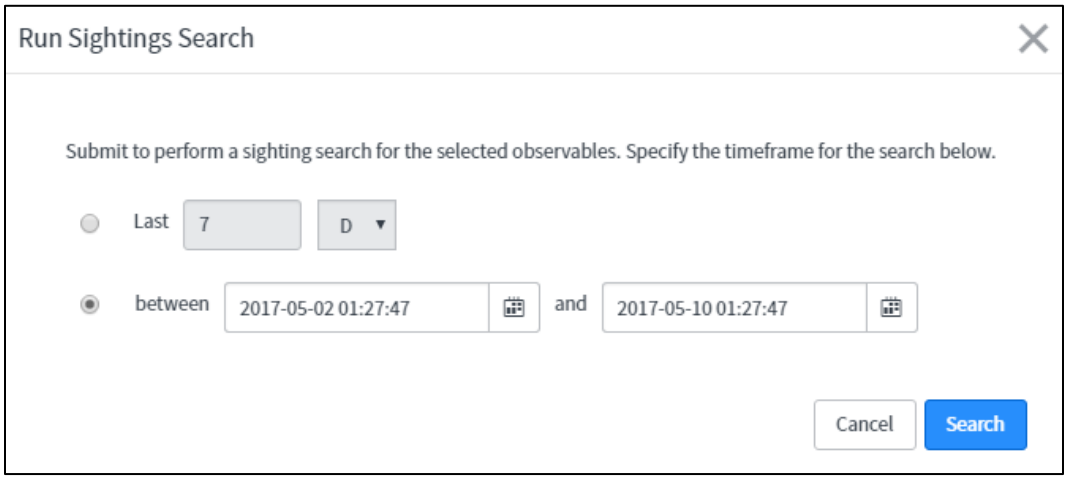
Lab 2.2 Manual Sighting Search

This lab explains how to **manually trigger** a search for these **Observables** by **selecting each observable.**

1. From the **Actions Button, Click Run Sighting Search**.



2. **Choose** a date range of the **last 7 days** or so and click **Submit**.

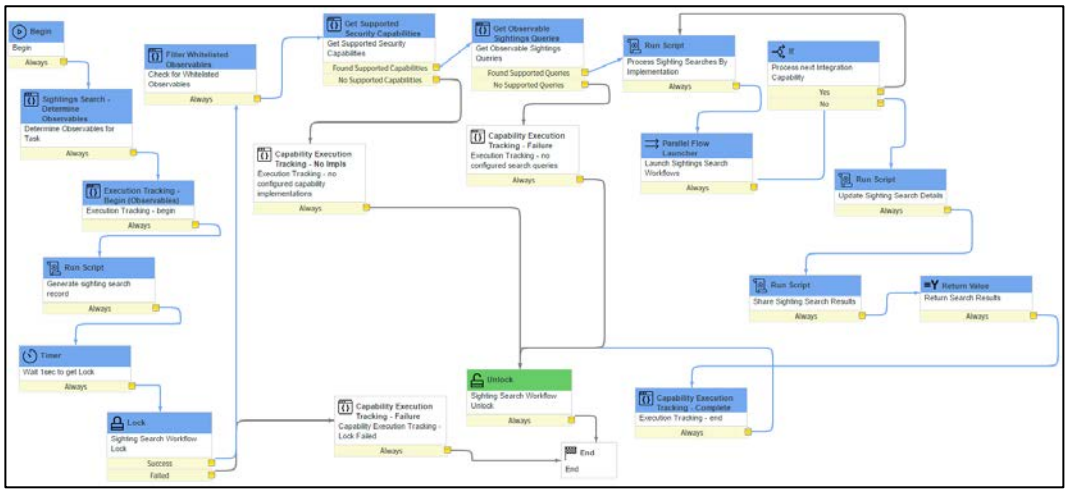


3. This action triggers a workflow, which in turn triggers an Active Sightings Search within your configured log store(s).

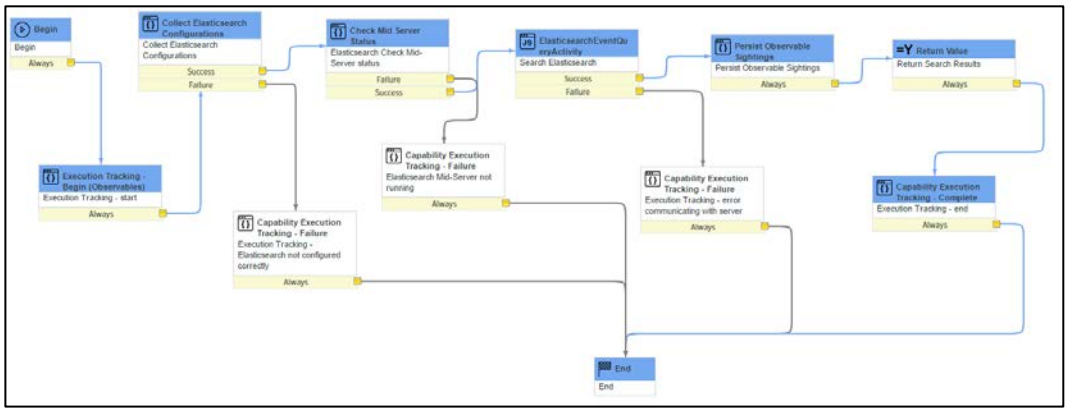
4. To review the workflows, click **Response Workflow**.



Security Operations Integration – Sightings Search



Security Operations – Elasticsearch Sightings Search

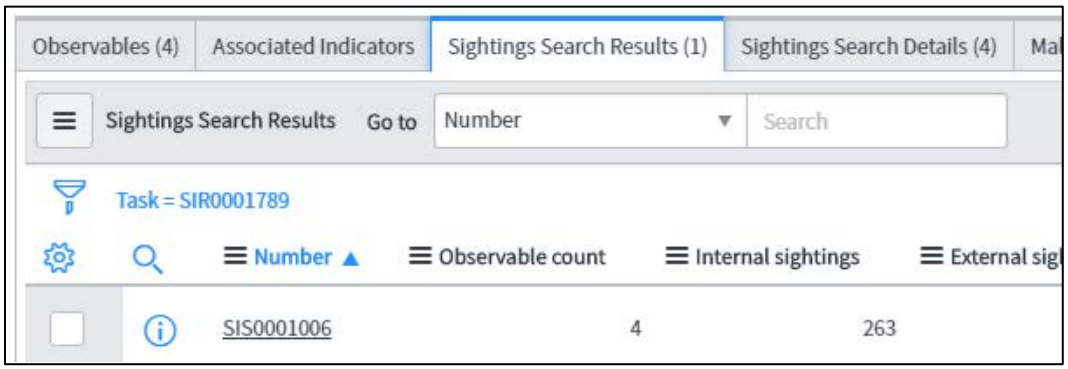


Lab Goal

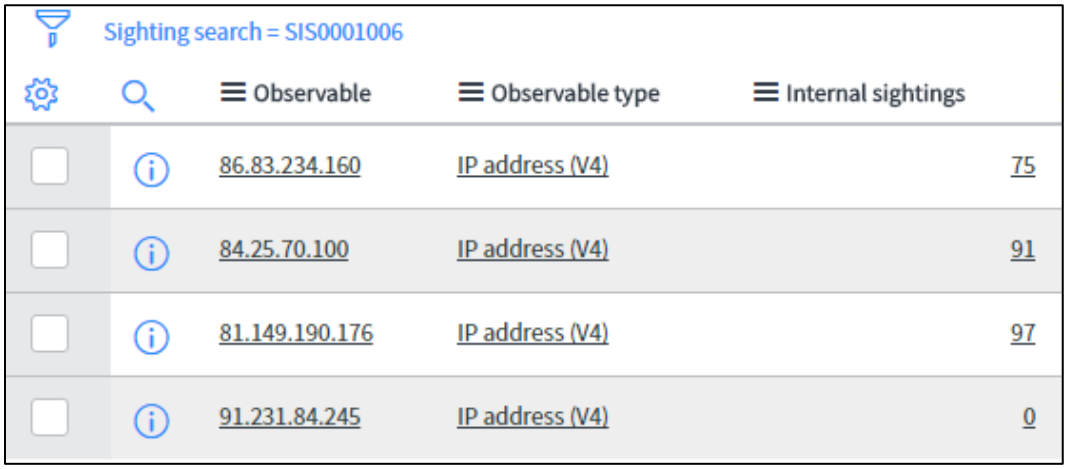
This lab explores the outcome from the Active Sightings Search.

Lab 2.3 Review Results From Search

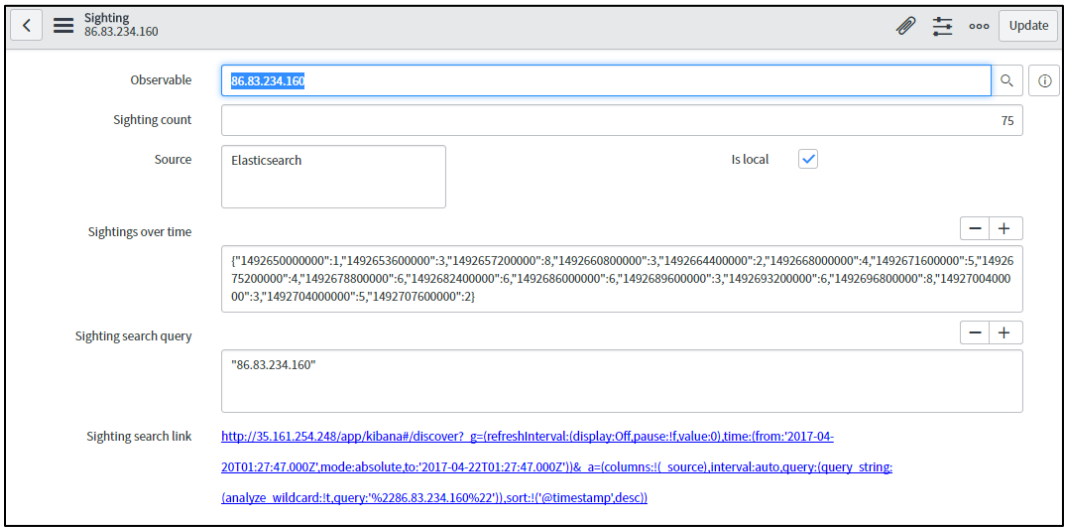
1. From within the Incident record, click the **Sighting Search Results** tab.



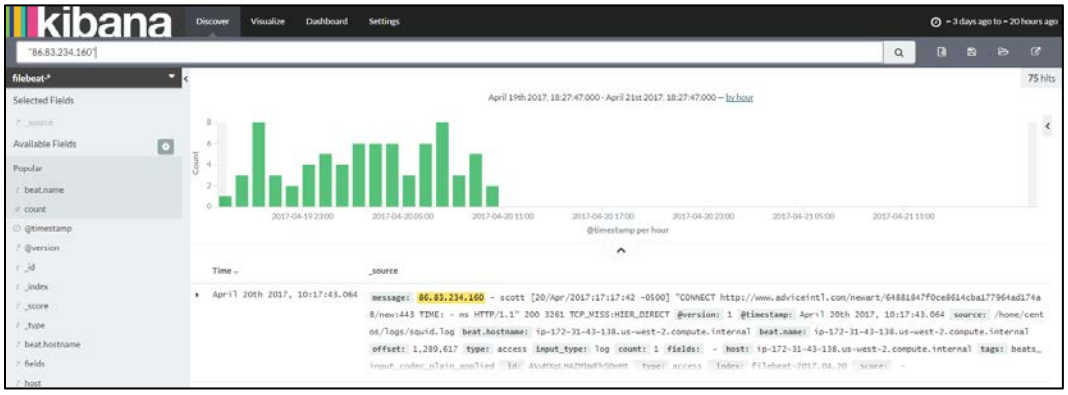
2. Click **Sighting search** to navigate to the Sightings Search Details view. From this view, you can see if the **Observables** that were search for had internal sightings.



3. **Click** one of the **Observables internal sightings count** to view the results.



4. Click **Sighting Search link** to review the source of the logs in the SIEM.

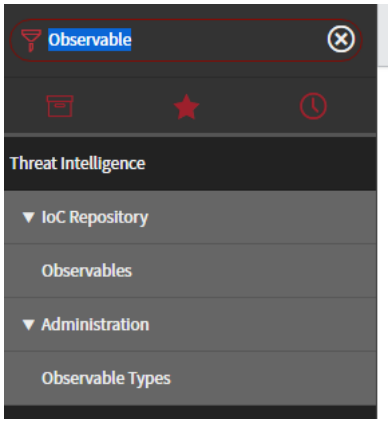


Lab Goal

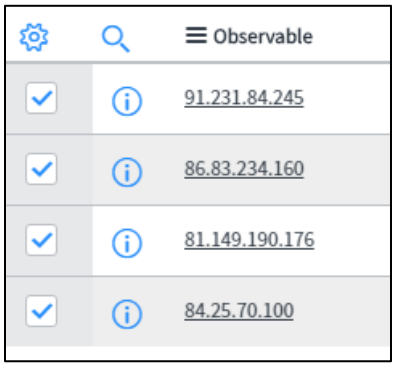
This lab explains how to share observables from an Incident with a **Trusted Security Circle** to get additional context.

Lab 3.0 Trusted Security Circles Query

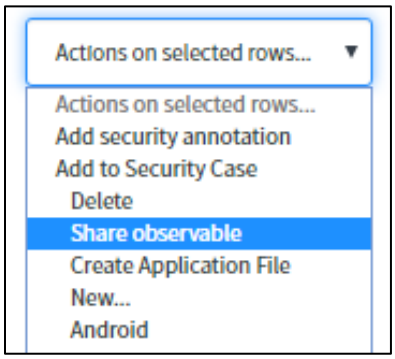
1. From the **Filter Navigator**, search for **Observable**. Find and click **Observables**.



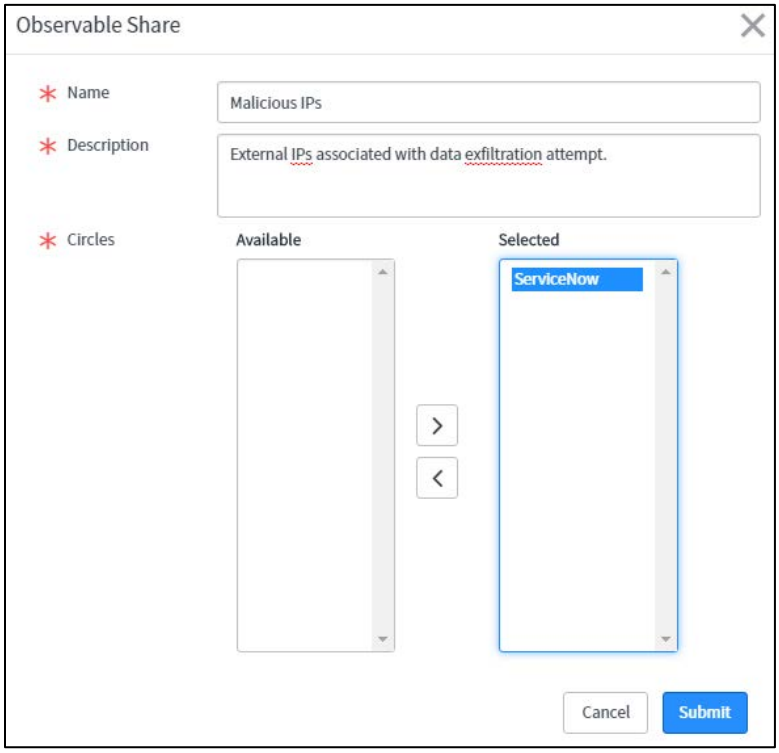
2. From the list view, click **Actions** and select **Share Observables**.



3. Click **Actions** and select **Share Observables**.



4. In the **Observable Share Window**, choose a name to give the sharing action, a description, and then choose which **Trusted Security Circle** to share with.

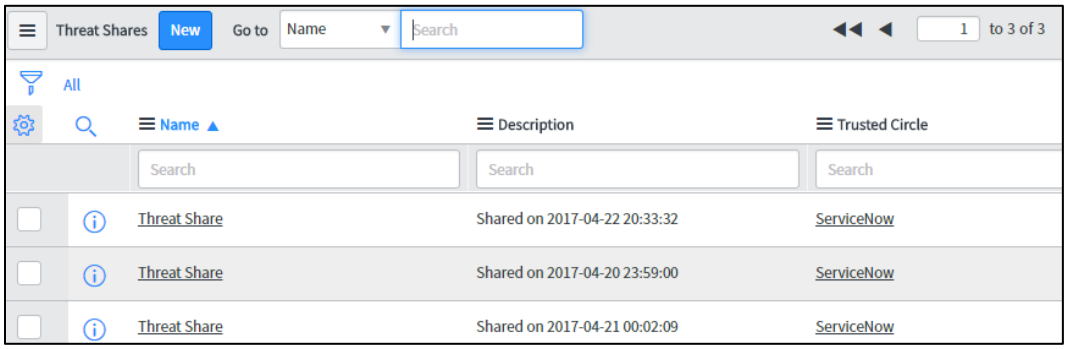


5. Click **Submit**.

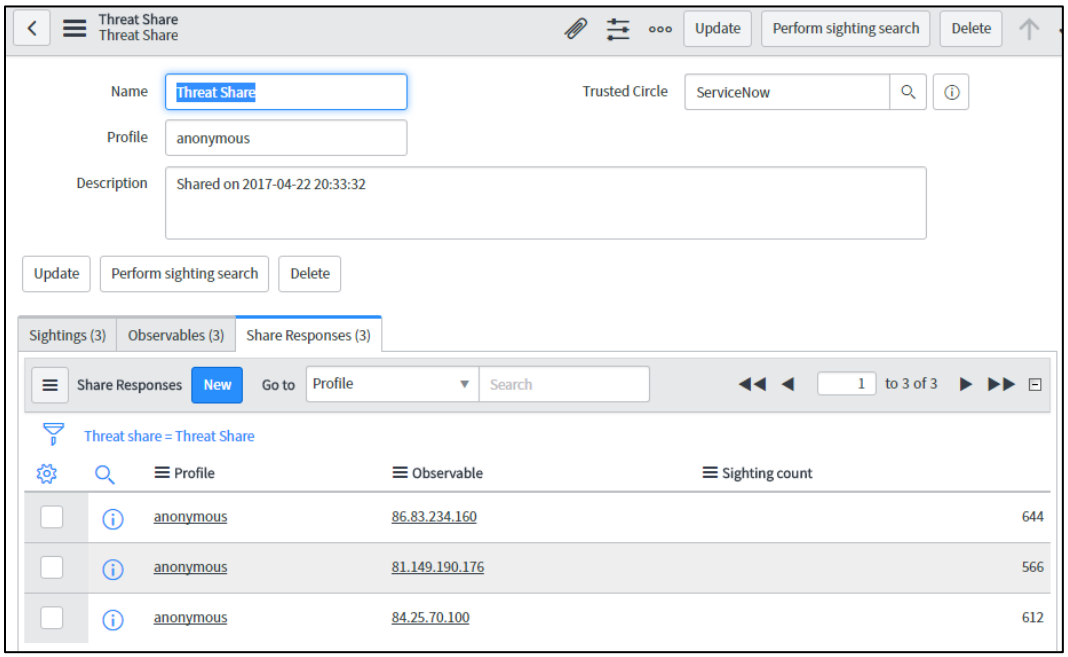
6. To review the Trusted Security Circle Threat Share, search in the Filter Navigator for **Threat Shares**. The responses from other members of the circle may not be immediate, so please be patient.



7. From the **Threat Shares** list view, select your Share.



8. From the **Threat Share Responses,** you can review the **responses** from members of the Trusted Security Share.



Congratulations! You've completed the Threat Hunting, Awareness, and Sharing with Security Lab. Please feel free to ask the **Friendly Lab Gurus** any additional questions you may have.

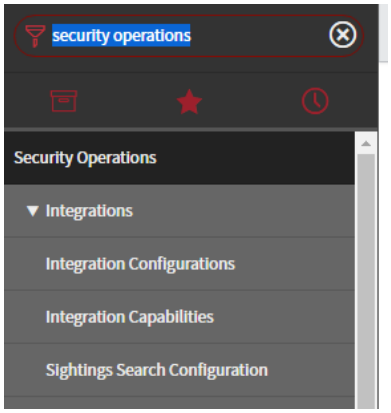
Bonus Lab Goal

Bonus Lab URL Sighting Search

This lab explains how to configure Sighting Search.

Sighting Search can search for any number of observable types. Typically, these would be IP, URL, Hash, etc. For the previous labs, we used IPs. Let's configure Observable type URL.

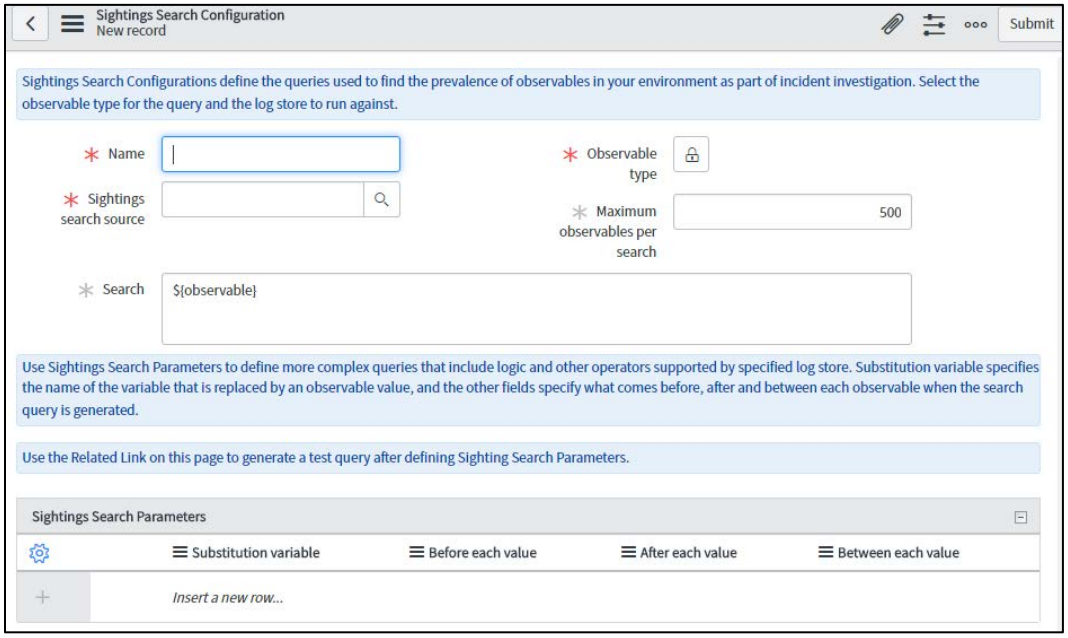
1. From the Filter Navigator, find **Security Operations** and click **Sightings Search Configuration**.



2. Click on **Default Search for IPs** to review the configuration for IP observables.



3. After returning to the Sighting Search Configurations page, click **New** to add a search for observable type URL.



4. Click **Submit**. Now you can search for URL observables too!