LOGPOINT

Integrations

Recorded Future

V6.1.0

CONTENTS

CHAPTER

ONE

RECORDED FUTURE

Recorded Future enriches incoming logs with the threat information fetched from *Recorded Future*. You can use the enriched data in dashboards, reports and alerts to monitor and track threats. Recorded Future is also a threat intelligence source in Threat Intelligence. The Threat Intelligence process command can further enrich Recorded Future logs.

It fetches threat information of the following entities:

- IP Address
- URL
- Domain
- Hash
- Vulnerability

Recorded Future summarizes all the fetched and enriched data of the given entities in an *Intelligence Card*.

CHAPTER

TWO

INSTALLING RECORDED FUTURE

Prerequisite

- LogPoint v6.12.2 or later
- Threat Intelligence v5.0.0 or later

To install Recorded Future:

1. Download the .pak file from the *Download* section in Release Notes.
2. Go to *Settings >> System Settings* from the navigation bar and click **Applications**.
3. Click **Import**.
4. **Browse** to the downloaded .pak file.
5. Click **Upload**.

After installing Recorded Future, you can find it in *Settings >> Configurations* and in **Threat Intelligence Management** panel.

CHAPTER

THREE

UNINSTALLING RECORDED FUTURE

You must first remove Recorded Future configurations from Logpoint and then uninstall it.

To remove Recorded Future configurations:

1. Go to *Settings >> Configuration* from the navigation bar and click **Recorded Future**.
2. Click **Settings**.
3. Disable **Enable Source** and click **Submit**.

To uninstall Recorded Future:

1. Go to *Settings >> System Settings* from the navigation bar and click **Applications**.
2. Click the **Uninstall** (🗑) icon in **Actions** of Recorded Future.

CHAPTER

FOUR

CONFIGURING RECORDED FUTURE

Go to *Settings >> Configuration* from the navigation bar and click **Recorded Future**.

4.1 General Information

You can find an overview of the fetched information from *Recorded Future* in **General Information**. It displays the total number of logs enriched in **Total Records**. It also displays details of risk lists found in the fetched information. A risk list is a list of entities that have been identified as posing a potential risk to an organization. These entities may be associated with known security threats, vulnerabilities or malicious activity.

The following information is displayed on the risk list:

Column	Description
Name	Name of the entity risk lists.
Type	Type of entity.
Last Successful Fetch	Date and time on which the data was last fetched.
Status	Status if the data is fetched. It can be Fetching, Completed or Error.
Number of Records	Total number of data fetched of the entity type.

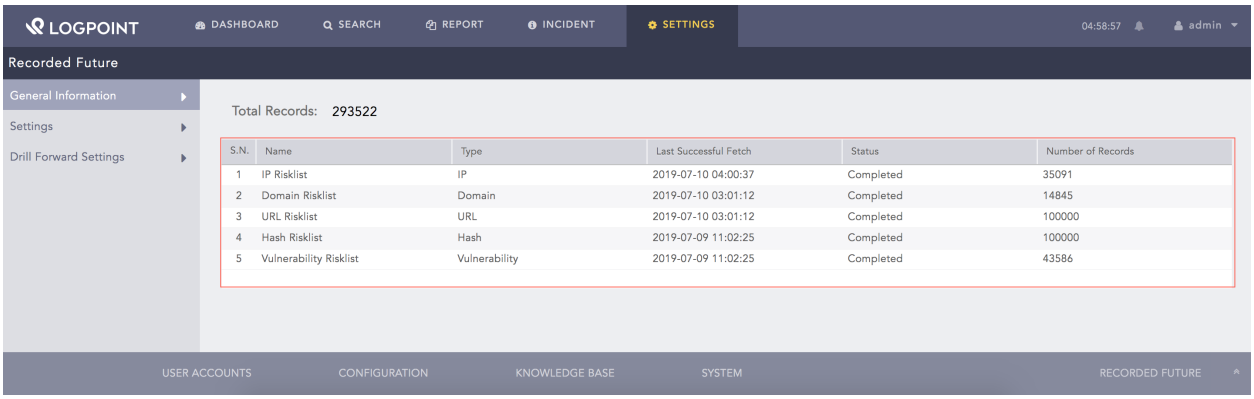

Fig. 1: General Information

All the risk lists are updated according to a particular interval and use API credits as mentioned below:

Risk List	Update Interval	Total API Credits per day
IP Address	Every one hour	120 credits
Domain	Every two hours	60 credits
URL	Every two hours	60 credits
Hash	Once a day	5 credits
Vulnerability	Once a day	5 credits

Your total API credit is 250 per day if you select all the entities.

4.2 Settings

You can configure *Recorded Future* from **Settings**.

1. Go to *Settings >> Configuration* from the navigation bar and click **Recorded Future**.
2. Select **Settings**.
3. **Enable Source** to activate the *Recorded Future* threat intelligence source.
4. Enter the *Recorded Future* **API Key**.

Note: To obtain the *Recorded Future* API Key:

1. Log in to the Recorded Future Portal.
2. Click the menu in the upper right and click **User Settings**.
3. Select **API Access** in **User Settings** dropdown and click **Generate New API Token**.

---

5. Select the required **Entities**. Recorded Future fetches and stores data of the selected entities only.
6. **Enable Proxy** to connect to *Recorded Future* via a proxy server.
7. In **Proxy Configuration**:
    7.1. Enter the **IP** address and the **Port** number of the proxy server.
    7.2. Select the **HTTP** or **HTTPS** protocol as required.
8. Click **Submit**.

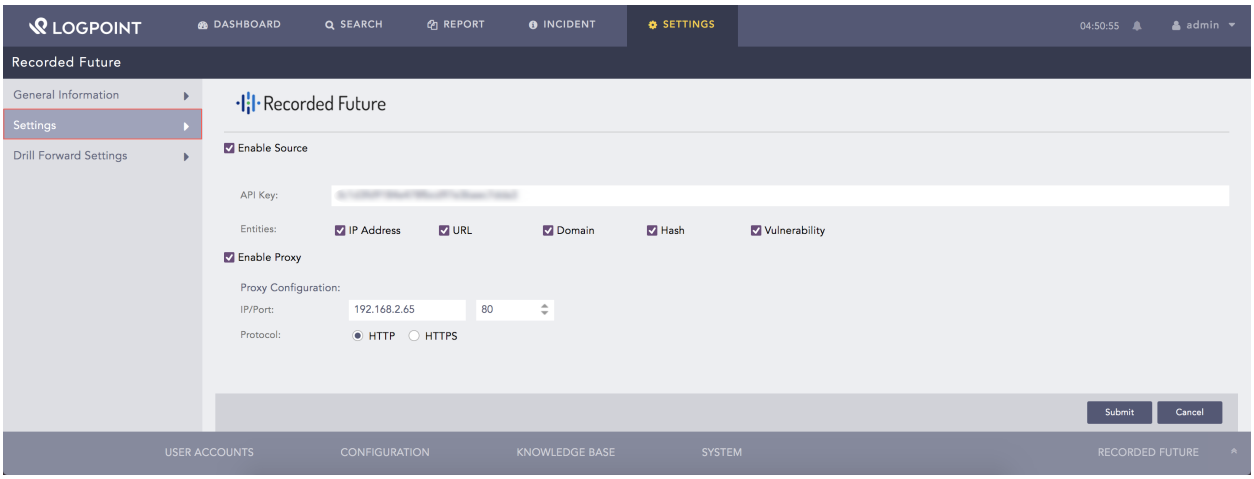

Fig. 2: Configuring Recorded Future

Note: The data fetched from *Recorded Future* is stored in the Threat Intelligence database. You must use the Threat Intelligence enrichment source while creating an enrichment policy for Recorded Future.

4.3 Drill Forward Settings

After Recorded Future enriches the incoming logs, you can further drill forward on their fields to access an *Intelligence Card*. This intelligence card summarizes all the threat information in the log. You can configure settings for the drill forward in **Drill Forward Settings**.

To configure the drill forward settings:

1. Go to *Settings >> Configuration* from the navigation bar and click **Recorded Future**.
2. Click **Drill Forward Settings**.
3. Select **Enable Drill Forward**.
4. Select the **Type** of the field from the drop-down.
5. Enter the **LogPoint Taxonomy Field** to map it with the *Recorded Future* entity type.
6. Click **Add**.
7. Click **Submit**.

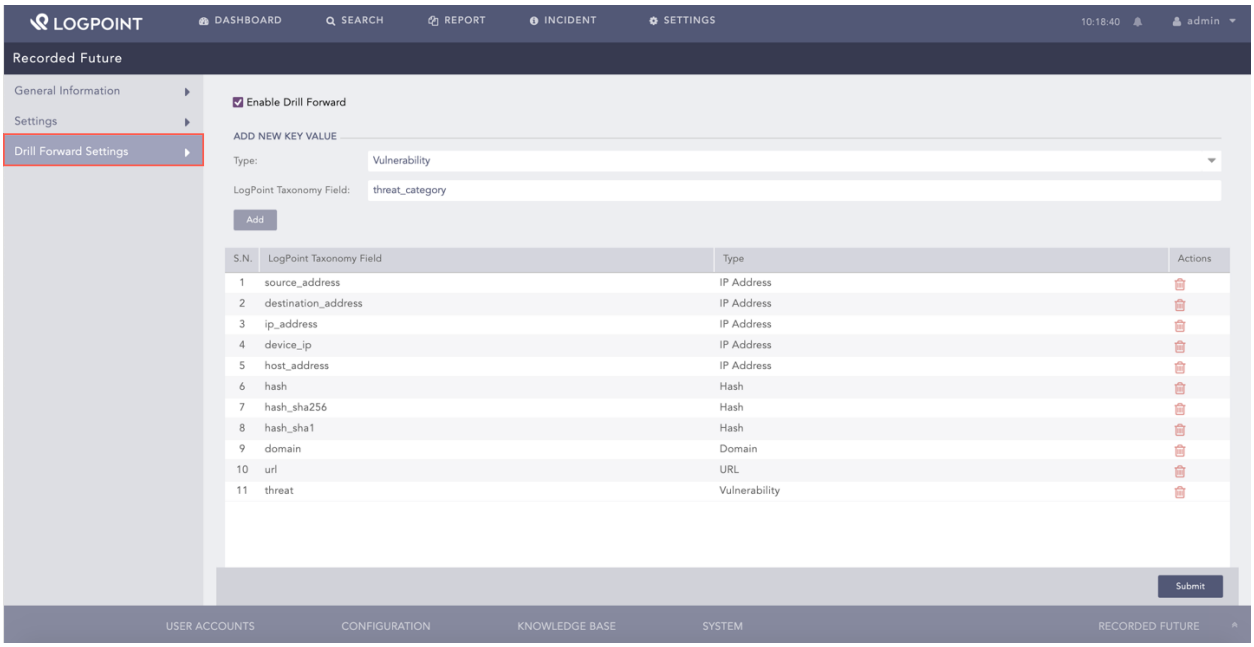

Fig. 3: Enabling Drill Forward

Recorded Future maps the following fields by default:

LogPoint Taxonomy Field	Recorded Future Entity Type
source_address	IP Address
destination_address	IP Address
ip_address	IP Address
device_ip	IP Address
host_address	IP Address
hash	Hash
hash_sha256	Hash
hash_sha1	Hash
domain	Domain
url	URL
threat	Vulnerability

CHAPTER

FIVE

INTELLIGENCE CARD

You can find the summary of the threat information fetched, enriched and analyzed by *Recorded Future* on the selected entity in **Intelligence Card**.

There are Intelligence Cards for the following entity types:

- IP Address
- URL
- Domain
- Hash
- Vulnerability

To access an intelligence card:

1. Search for the enriched logs.

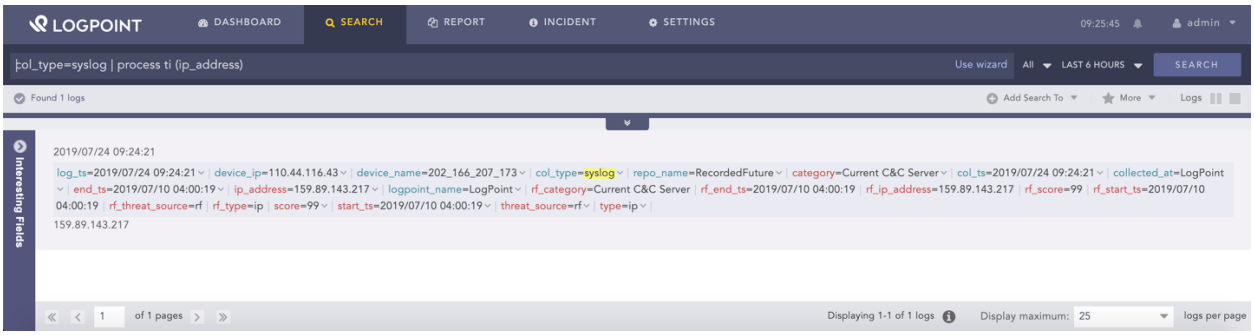

Fig. 1: Search Tab

2. Click the drop-down of the previously mapped field from *Drill Forward Settings*.

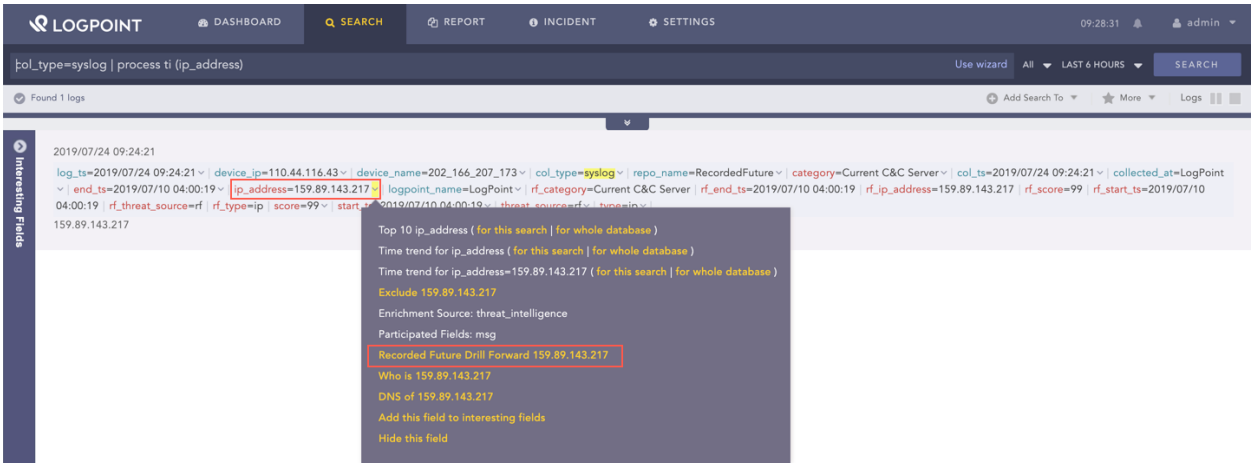

Fig. 2: Recorded Future Drill Forward

3. Click **Recorded Future Drill Forward**.

Note: Each drill forward uses 1 API credit.

Recorded Future redirects you to the **Intelligence Card**.

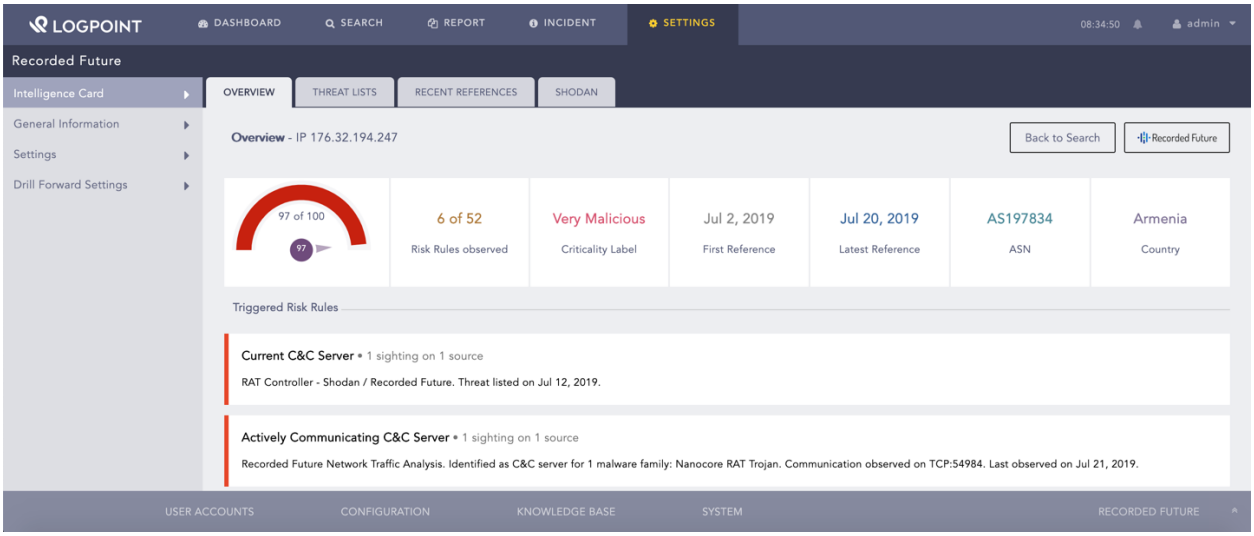

Fig. 3: Intelligence Card

5.1 Overview

You can find the risk information summary, including the *Recorded Future* risk score and triggered risk rules of the selected entity in **Overview**. Risk score is a numerical value

that represents the level of risk associated with the entity. Triggered Risk Rules are a set of automated alerts for specific types of security risks that are customized to look for risks across multiple data sources.

You can click **Back to Search** to redirect you to the search results page and **Recorded Future** to the *Recorded Future's* Intelligence card.

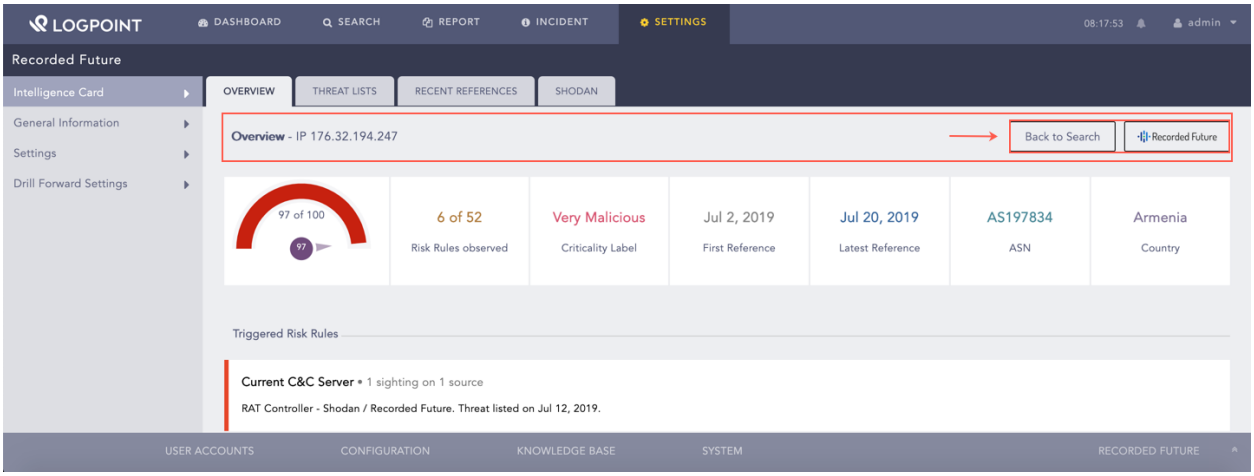

Fig. 4: Back to Search

Recorded Future generates the risk score by analyzing the level of risk on the entity. It analyzes risks based on its set of risk rules and threat lists. Each risk rule has a criticality, a criticality label and a risk score. The risk rule is color-coded by the criticality of the threat. The gauze chart is used to display the risk score of the entity.

Criticality Label	Criticality	Risk Scores	Color
Very Malicious	4	90-99	Red
Malicious	3	65-89	Red
Suspicious	2	25-64	Bright Yellow
Unusual	1	5-24	Light Gray
No current evidence of risk	0	0	Light Gray

You can find the number of triggered risk rules and their severity level in **Risk Rules observed** and **Criticality Label**. The date when the risk rule was first triggered is displayed in **First Reference**, and the date it was last triggered is displayed in **Latest Reference**. You can also find the autonomous system numbers (ASN) and the country where the threat is detected. Autonomous System Numbers (ASN) are unique identifiers of each network on the internet.

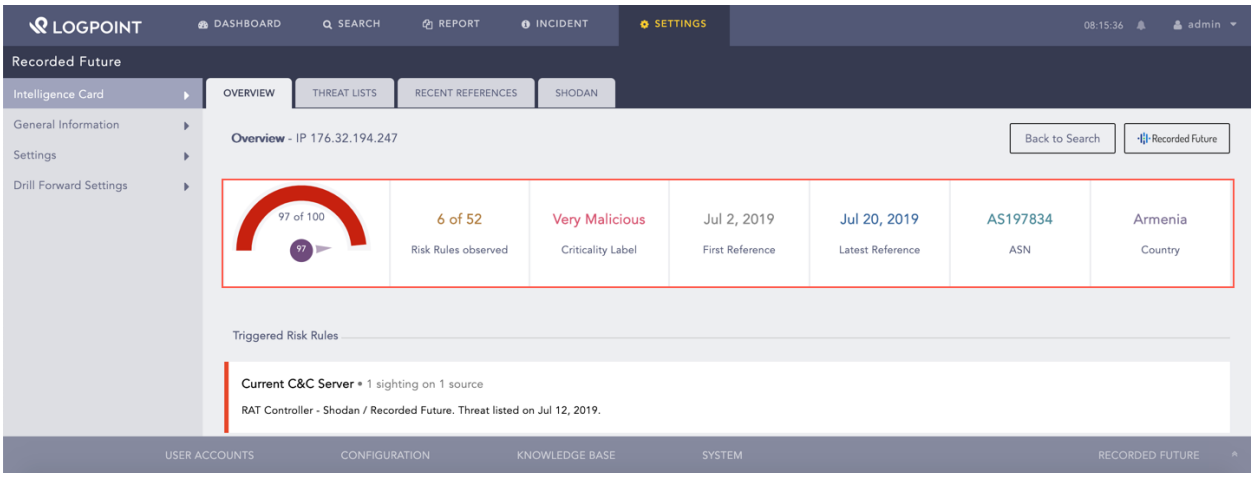

Fig. 5: Risk Score and Risk-Related Content

Recorded Future has its own set of risk rules that are triggered based on the risk rule evidence found in different sources. The sources include threat feeds, IP reputation lists, security research blogs, social media posts, paste sites, underground forums and malware analysis services. You can find the triggered risk rules and their details under **Triggered Risk Rules**.

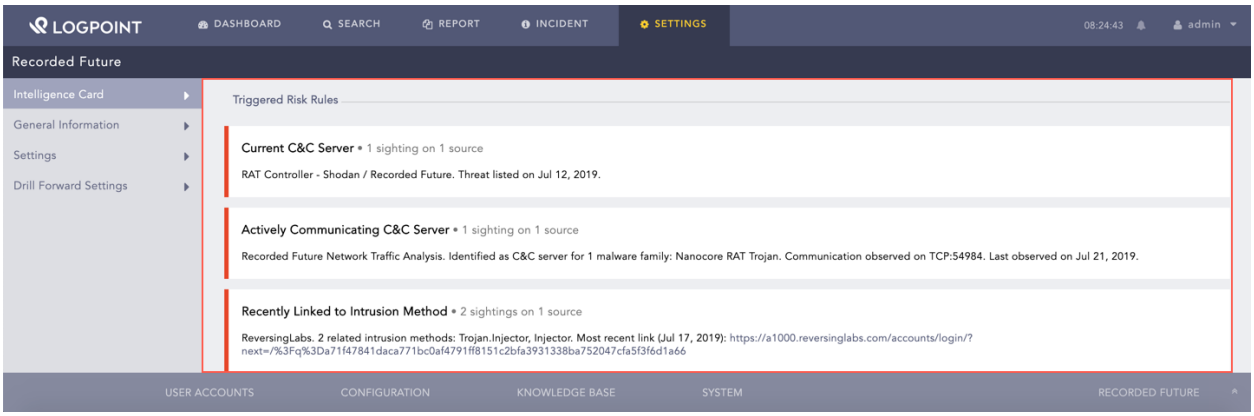

Fig. 6: Triggered Risk Rules

5.2 Threat Lists

You can find the threat lists for the selected entity in **Threat Lists**. It is a collection of information and analysis about specific cyber threats, such as malware, phishing campaigns and vulnerabilities.

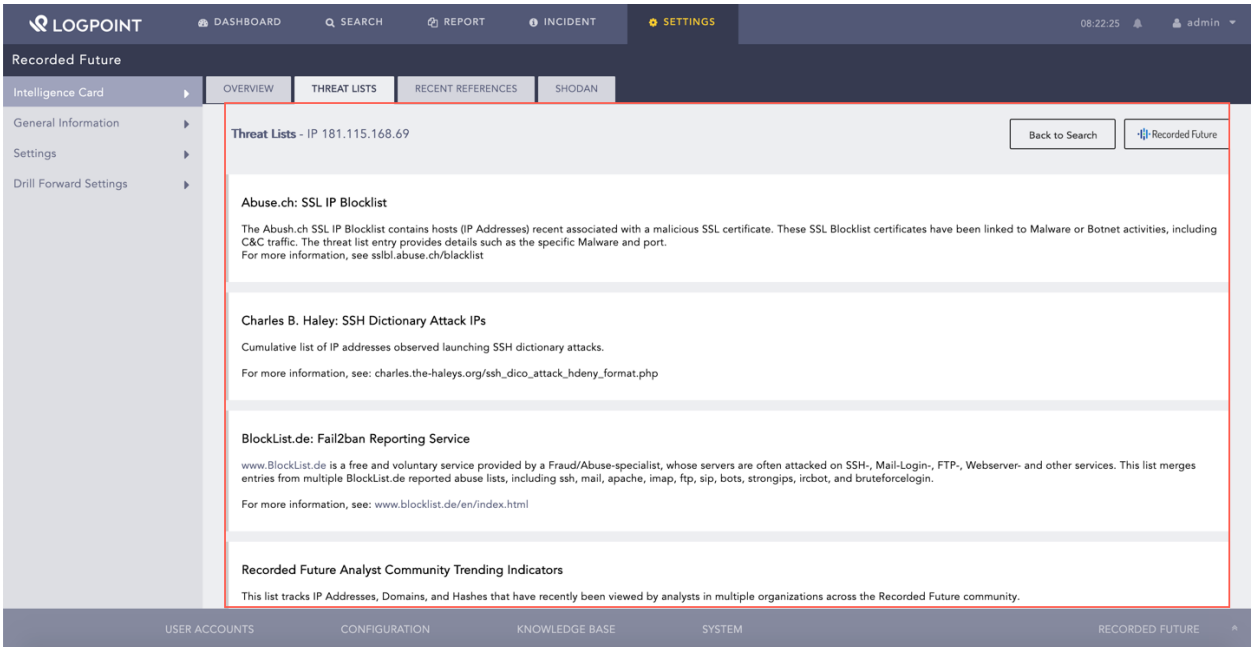

Fig. 7: Threat Lists

5.3 Recent References

You can find the recent mentions of the selected entity in various sources including but not limited to News, Blogs, Social Media and Dark Web in **Recent References**.

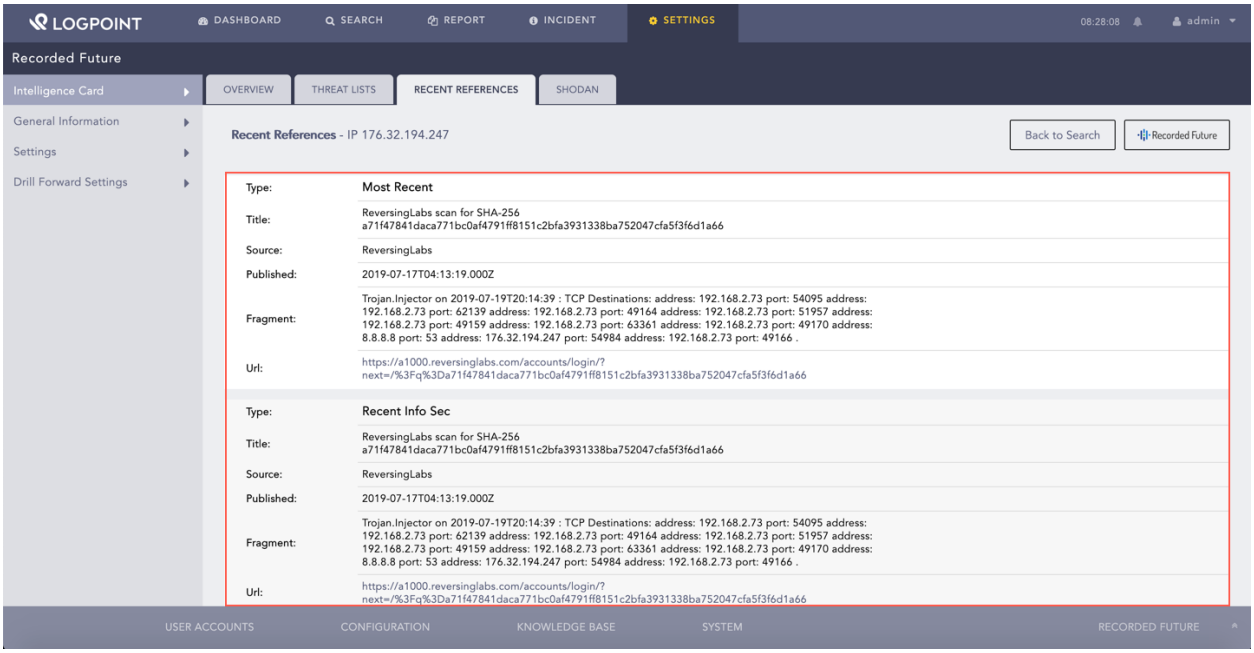

Fig. 8: Recent References

5.4 Shodan

Shodan is a search engine for internet-connected devices that enriches the IP Address and Vulnerability Intelligence Cards with its fetched data. Shodan enriches the Vulnerability Intelligence Card with fetched data from the Exploit Database. You can find the enriched data in **Exploits**.

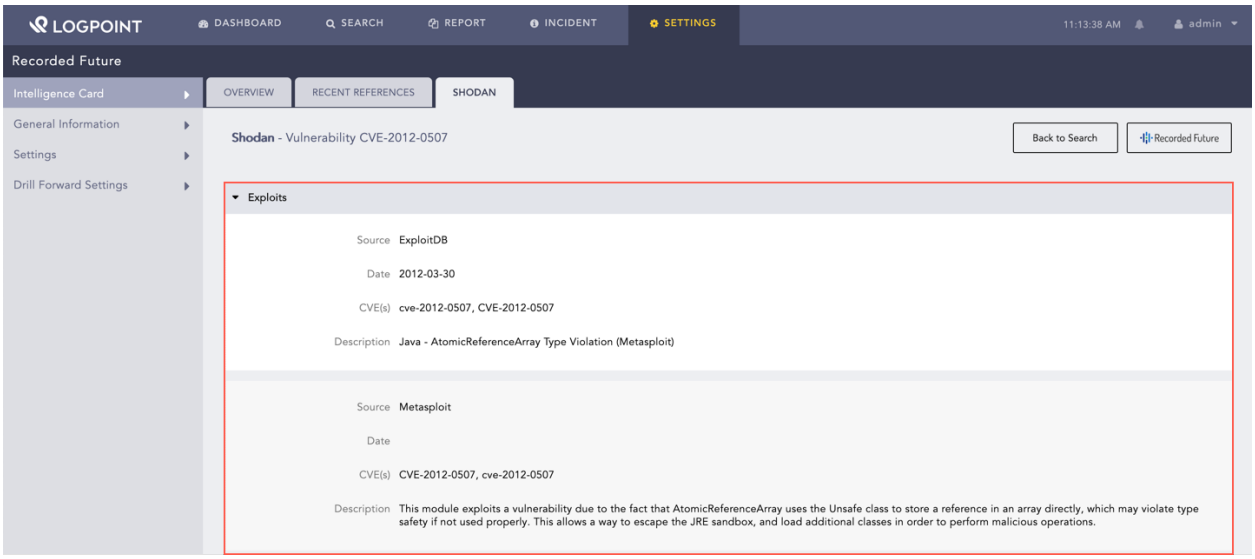

Fig. 9: Enriched Data for Vulnerability

Shodan enriches the IP Address Intelligence Card with the following data:

- Country
- Organization
- Operating system
- ISP
- Last update date
- Autonomous system number (ASN)
- Known vulnerabilities
- Device use tags
- Ports

You can find the geographic location of the IP address on a map and further enriched data in **General Information**, **Tags** and **Ports**.

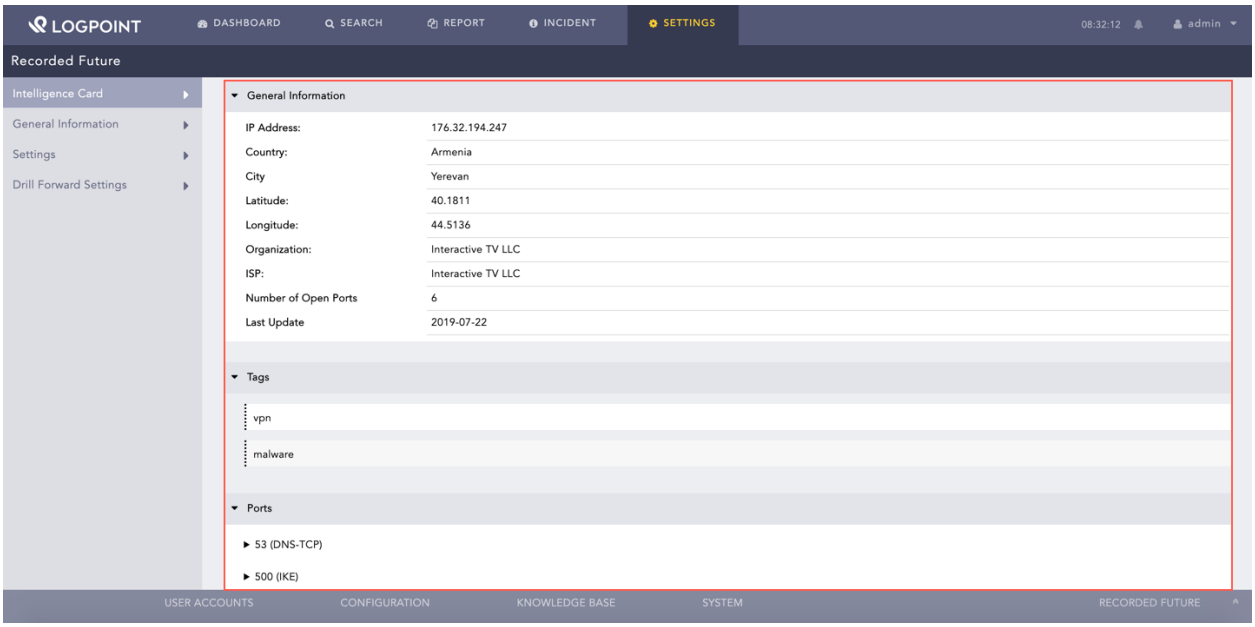

Fig. 10: Enriched Data for IP Address