LOGPOINT

Integrations

Recorded Future

*V*6.0.0

CONTENTS

1 Recorded Future Application **1**
1.1 Using RecordedFuture in LogPoint 1

2 Installation **3**
2.1 Prerequisites 3
2.2 Installing the RecordedFuture Application in LogPoint 3

3 Configuration **4**
3.1 Configuring the RecordedFuture Application in LogPoint 4
3.2 Configuring Drill Forward 5

4 General Information **8**

5 Search and Drill Forward **10**

6 Intelligence Card **12**
6.1 Overview 12
6.2 Threat Lists 16
6.3 Recent References 16
6.4 Shodan 17

7 Uninstallation **20**
7.1 Uninstalling the RecordedFuture Application in LogPoint 20

CHAPTER

ONE

RECORDED FUTURE APPLICATION

The RecordedFuture application enriches the 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.

The application fetches threat information of the following entities from *Recorded Future*:

- IP Address
- URL
- Domain
- Hash
- Vulnerability

The application summarizes all the fetched and enriched data of the given entities in an *Intelligence Card*. You can drill forward from the search results to access the Intelligence Card.

Furthermore, the application adds RecordedFuture as a threat intelligence source in the Threat Intelligence application. You can also use the Threat Intelligence process command to further enrich logs with the latest threat information.

1.1 Using RecordedFuture in LogPoint

The following steps summarize the flow of using RecordedFuture in LogPoint:

1. Install the Threat Intelligence application.
2. Install the RecordedFuture application.
3. Add RecordedFuture as a threat intelligence source in the **Threat Intelligence Management** panel or go to *Settings >> Configuration >> Recorded Future*.

4. Select the RecordedFuture entity types to fetch the threat information and store it in LogPoint.
5. Enable the **Enable Drill Forward** option.
6. Map LogPoint fields to the RecordedFuture entity types to drill forward from the fields to the Intelligence Card.
7. Apply an enrichment policy with the Threat Intelligence enrichment source.
8. From the search results, drill forward and find the Intelligence Card for the mapped fields.

CHAPTER

TWO

INSTALLATION

2.1 Prerequisites

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

2.2 Installing the RecordedFuture Application in LogPoint

1. Go to *Settings >> System >> Applications*.
2. Click **Import**.
3. **Browse** for the location of the downloaded pak file for the RecordedFuture application.
4. Click **Upload**.

After installing the application, you can find the installed plugins under *Settings >> System >> Plugins*.

CHAPTER

THREE

CONFIGURATION

3.1 Configuring the RecordedFuture Application in LogPoint

1. Go to *Settings >> Configuration >> Recorded Future*.
2. Select **Settings**.
3. Select the **Enable Source** option to activate the *Recorded Future* threat intelligence source.
4. Enter the **API Key** provided by *Recorded Future*.
5. Select the required **Entities**. The application fetches and stores data of the selected entities only.
6. Select the **Enable Proxy** option to connect to *Recorded Future* via a proxy server.
7. In the **Proxy Configuration** section:

    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**.

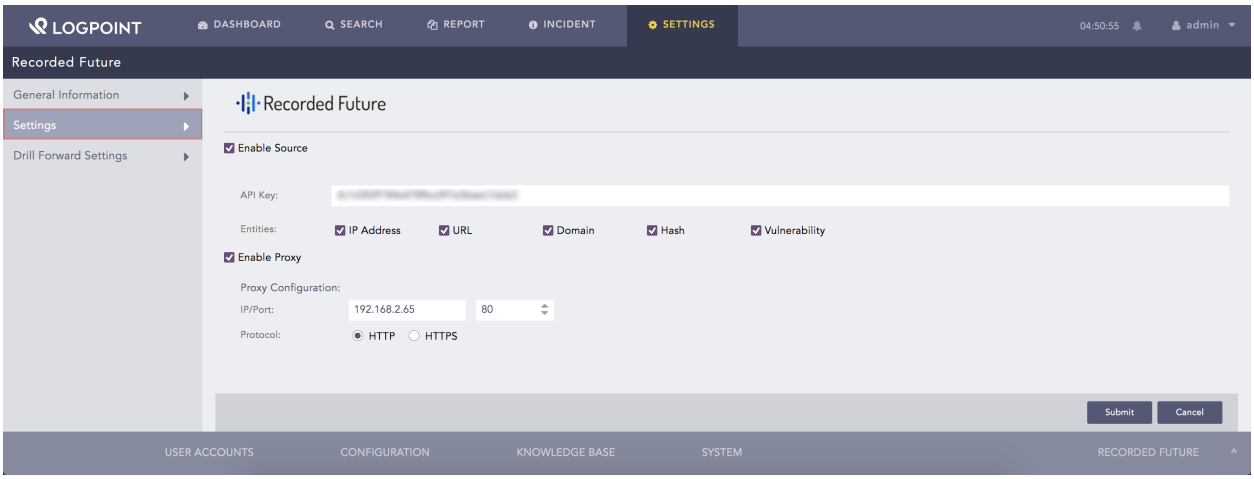

Fig. 1: Configuring Recorded Future

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

3.2 Configuring Drill Forward

The RecordedFuture application enriches the incoming logs with the threat information fetched from *Recorded Future*. You can find the enriched logs using the **Search** tab in LogPoint and can further drill forward on the enriched fields to access the *Intelligence Card*. To use the drill forward feature, you must enable the drill forward option and map the LogPoint fields with the *Recorded Future* entity type. You can only drill forward from the mapped fields.

The application 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

Follow these steps to use the drill forward feature:

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

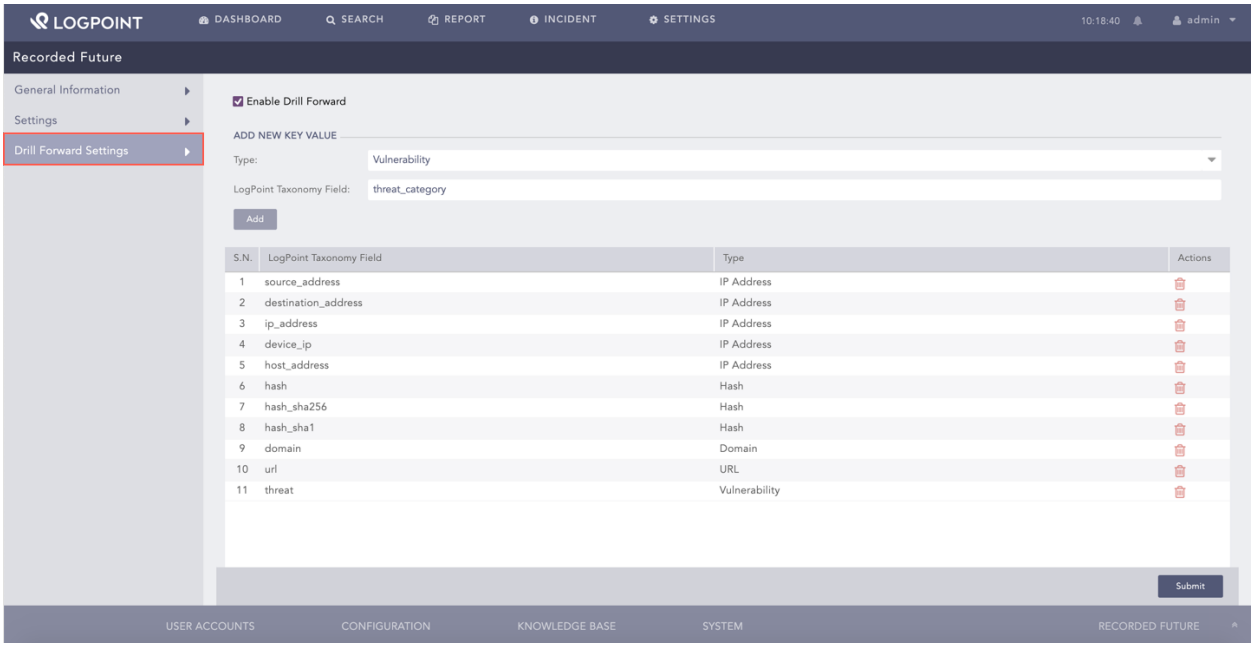

Fig. 2: Enabling Drill Forward

CHAPTER

FOUR

GENERAL INFORMATION

The **General Information** page gives an overview of the fetched information from *Recorded Future*. The page consists of risk lists of the entities.

It also displays the following information on a table:

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 of the data fetch. It can be Fetching, Completed, or Error
Number of Records	Total number of records fetched according to the entity type

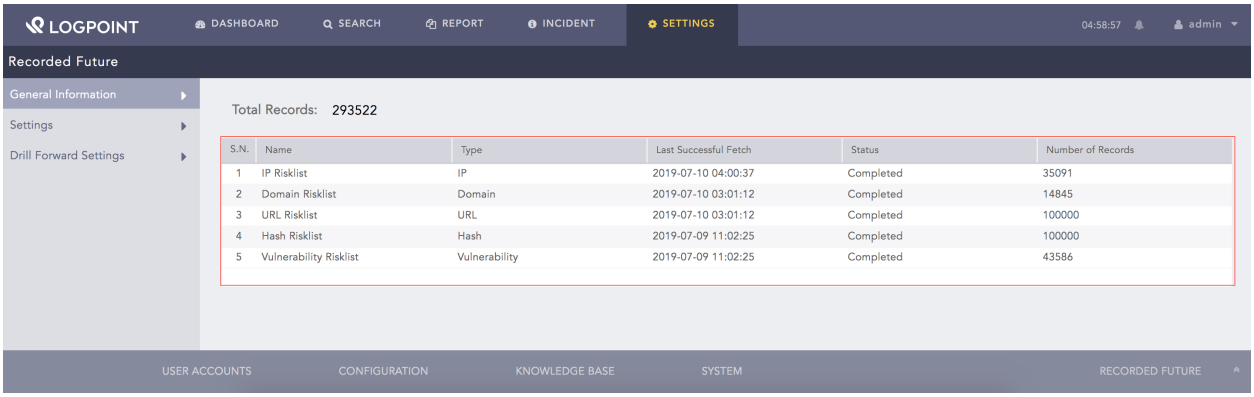

Fig. 1: General Information

All the risk lists are updated in a particular interval and use certain 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.

CHAPTER

FIVE

SEARCH AND DRILL FORWARD

Follow these steps to drill forward on the enriched field:

1. Search for the enriched logs.

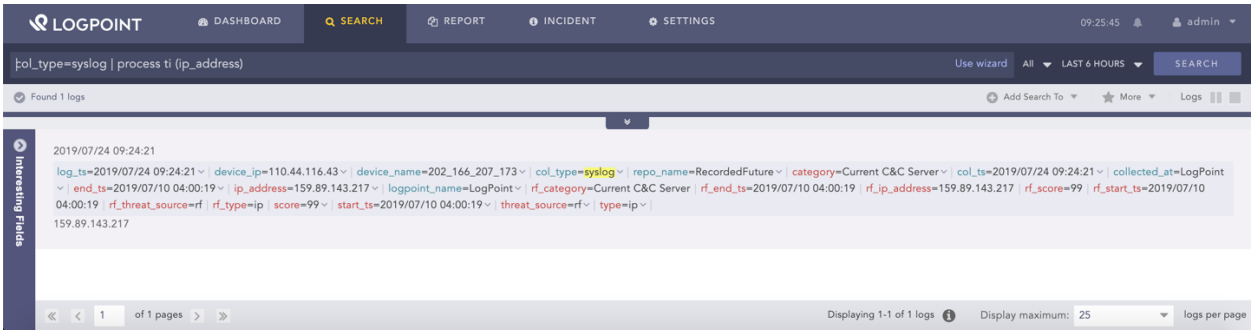

Fig. 1: Search Tab

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

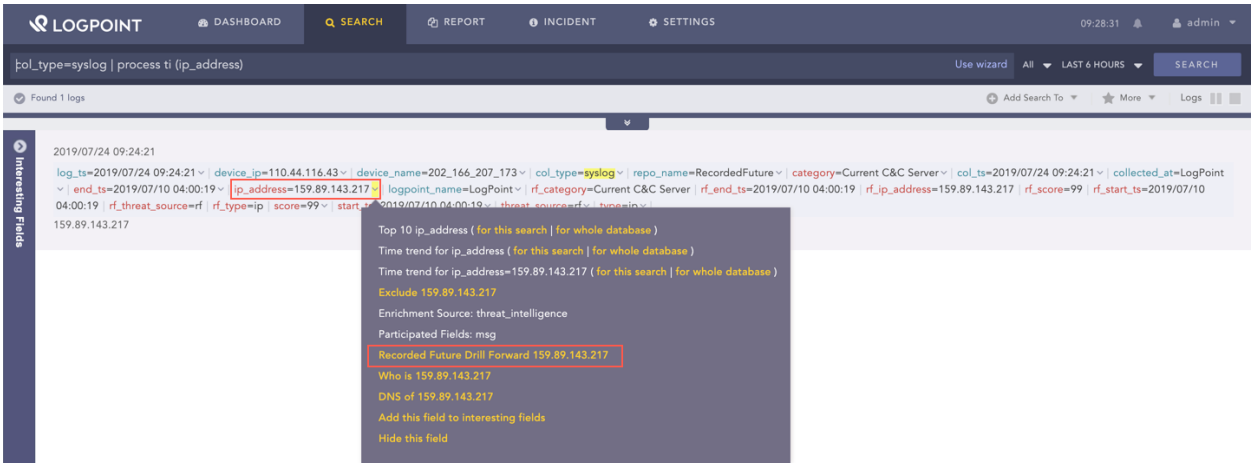

Fig. 2: Recorded Future Drill Forward

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

Note: Each drill forward uses 1 API credit.

The application redirects you to the **Intelligence Card** page.

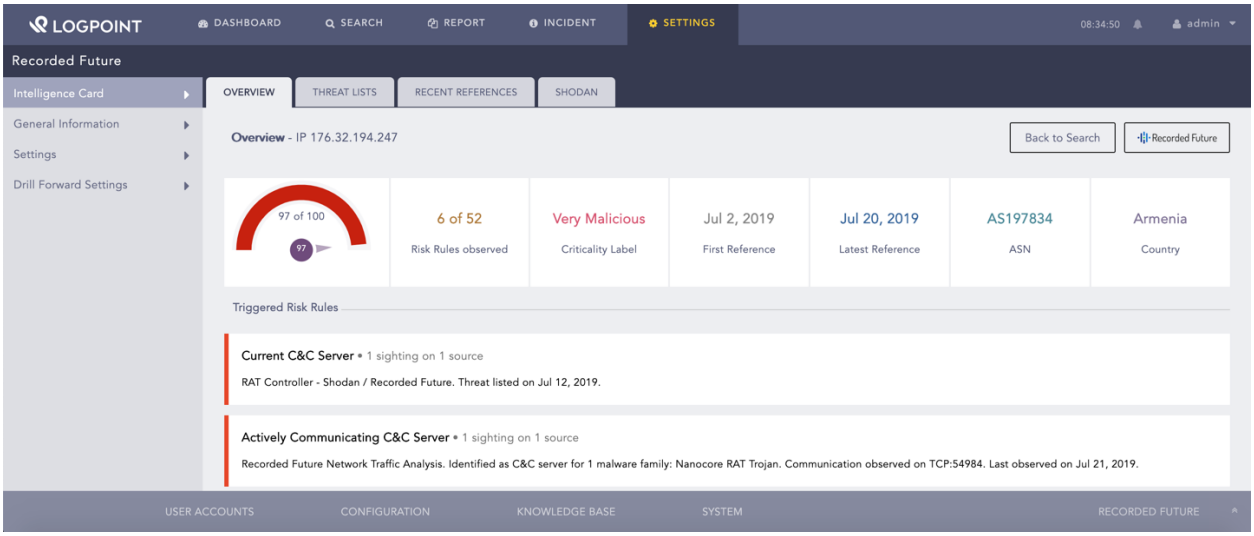

Fig. 3: Intelligence Card

CHAPTER

SIX

INTELLIGENCE CARD

The **Intelligence Card** page summarizes all the threat information fetched and analyzed by *Recorded Future* on the selected entity.

You can find the Intelligence Cards of the following entity types:

- IP Address
- URL
- Domain
- Hash
- Vulnerability

The following section describes the components found in the **Intelligence Card** page.

6.1 Overview

The **Overview** tab summarizes the risk information, including *Recorded Future* risk score and triggered risk rules of the selected entity.

6.1.1 Heading

The top of the **Overview** tab displays the entity you drilled forwarded from the search results.

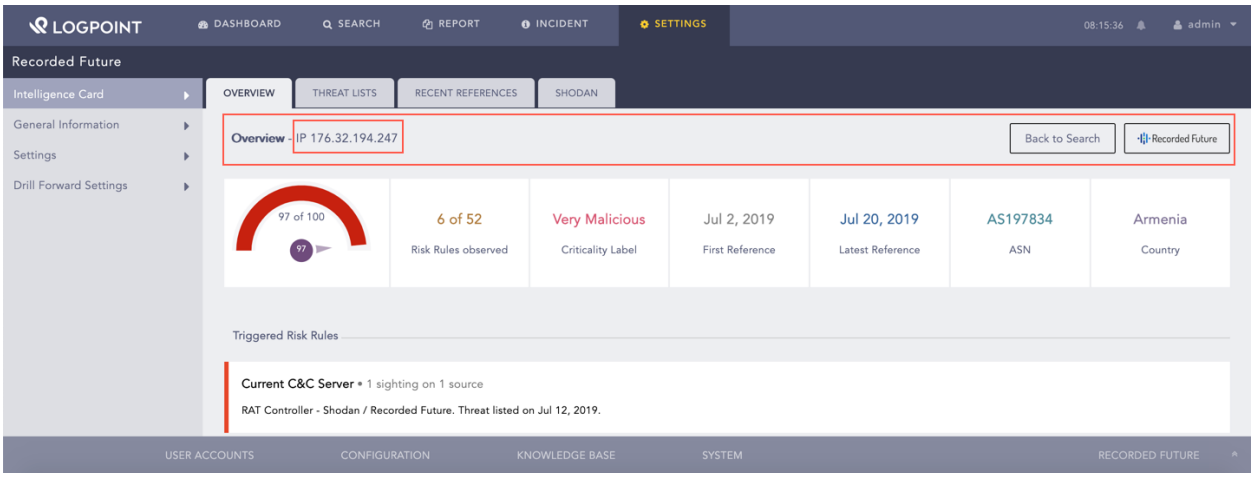

Fig. 1: Selected Entity

The **Back to Search** option redirects you to the search results page, and the **Recorded Future** option redirects you to *Recorded Future's* Intelligence Card.

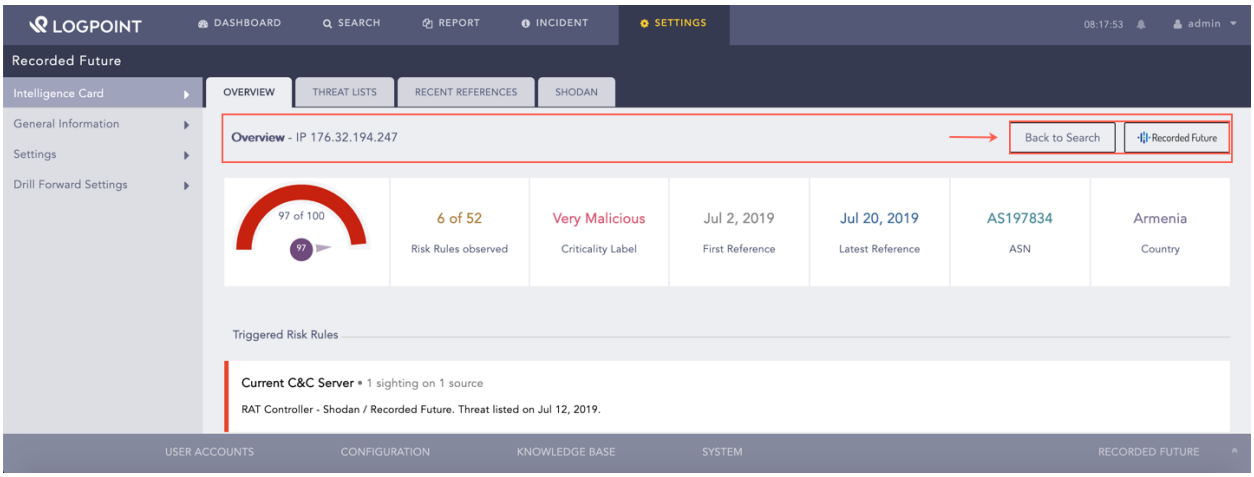

Fig. 2: Back to Search

6.1.2 Risk Score and Risk-Related Content

Recorded Future generates a risk score of the specific risk-related content. It generates the score by analyzing the level of risk on the threat information gathered from various sources. It analyzes risks based on its own 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.

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

The gauze chart displays the risk score of the entity.

The **Risk Rules observed** widget displays the number of triggered risk rules.

The **Criticality Label** widget displays the severity level of the risk rule.

The **First Reference** widget displays the earliest report, and the **Latest Reference** widget displays the most recent report for the selected field.

The **ASN** widget displays the autonomous system numbers (ASN), which is a unique identifier of each network on the internet.

The **Country** widget displays the country from where the threat is reported.

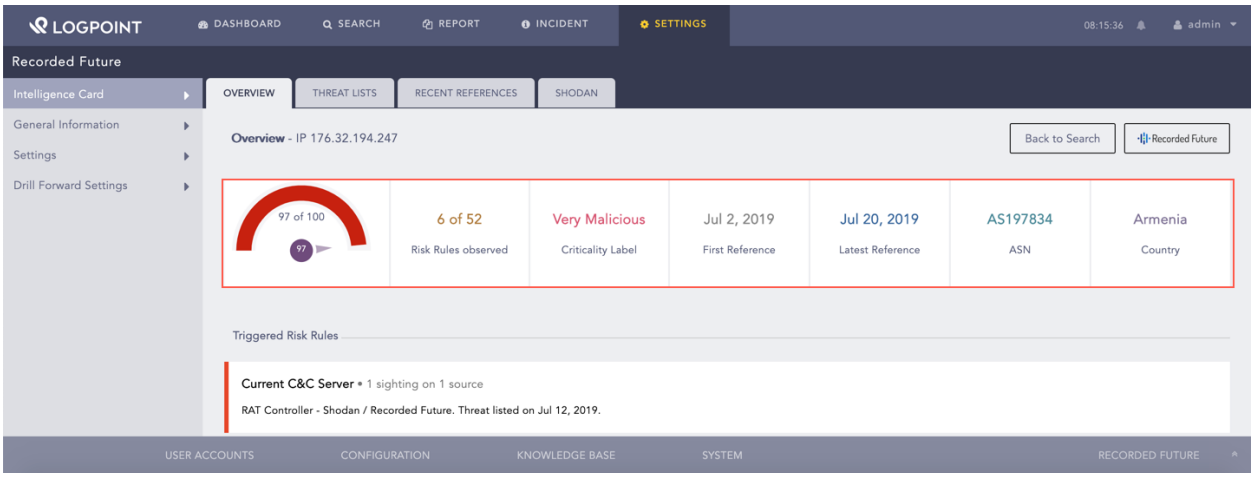

Fig. 3: Risk Score and Risk-Related Content

6.1.3 Triggered Risk Rules

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 and 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 the **Triggered Risk Rules** section.

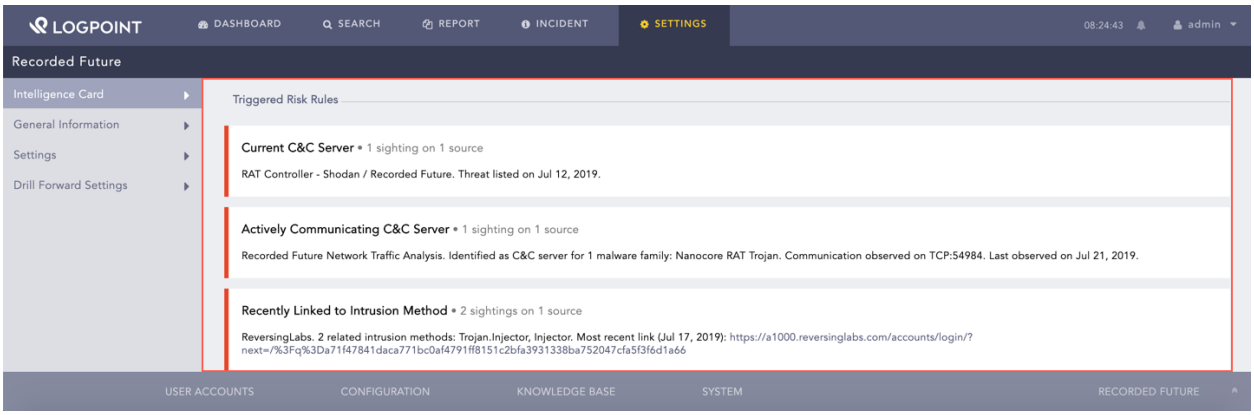

Fig. 4: Triggered Risk Rules

6.2 Threat Lists

The **Threat Lists** tab consists of the threat lists created by *Recorded Future*. It creates the list by analyzing its threat intelligence and collection of threat lists and the whitelists published in the external community. You can find the threat lists for the selected entity under **Threat Lists**.

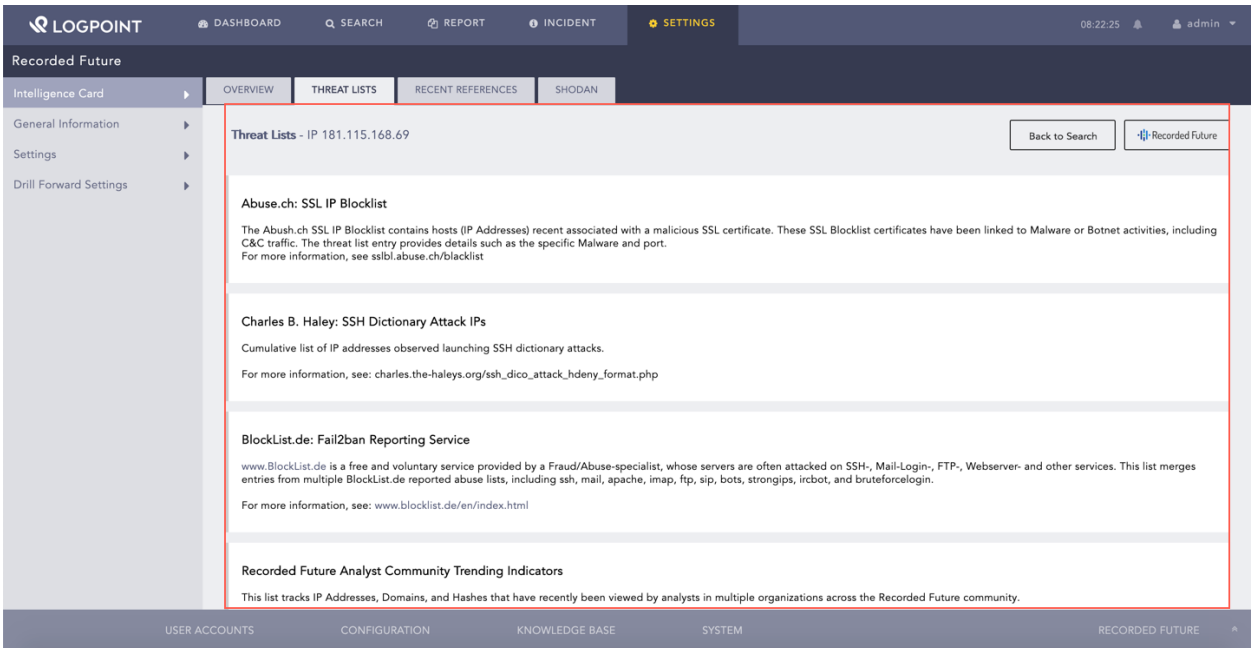

Fig. 5: Threat Lists

6.3 Recent References

The **Recent References** tab consists of entity references in external sources. These sources include cyber events, paste sites, social media, information security sources, underground forums, and dark web sources. The **Recent References** section displays the following information for each reference:

- Type
- Title
- Source
- Published
- Fragment
- URL

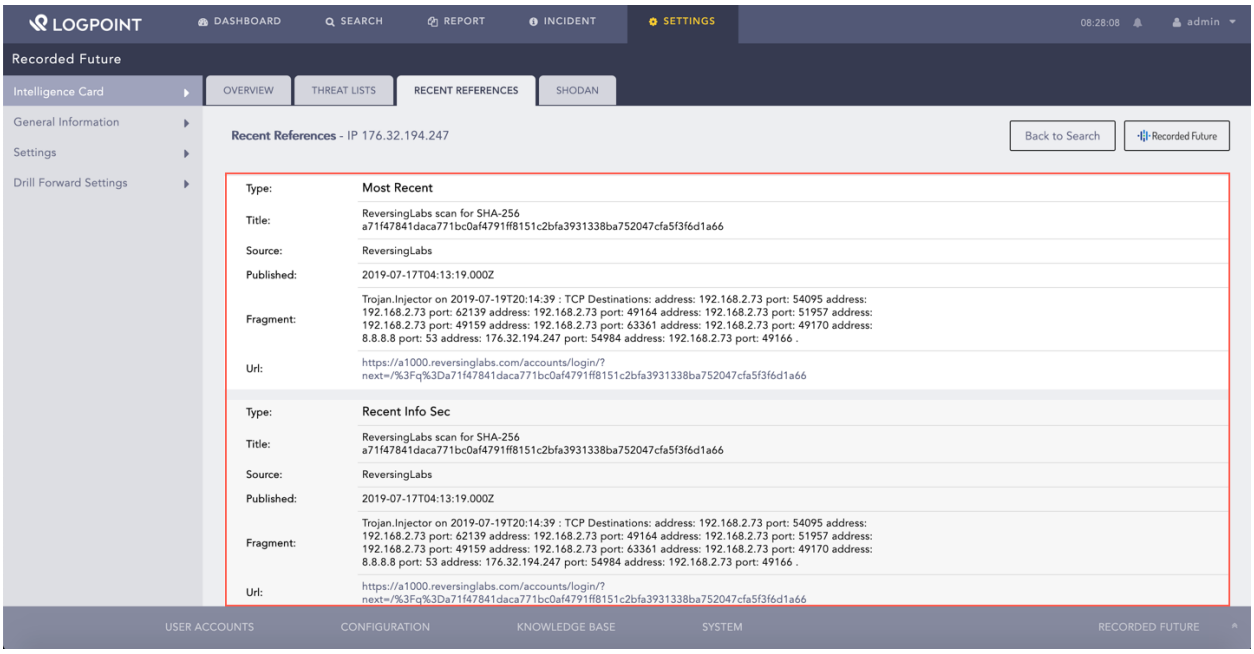

Fig. 6: Recent References

6.4 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 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

Shodan also displays the geographic location of an IP address on a map.

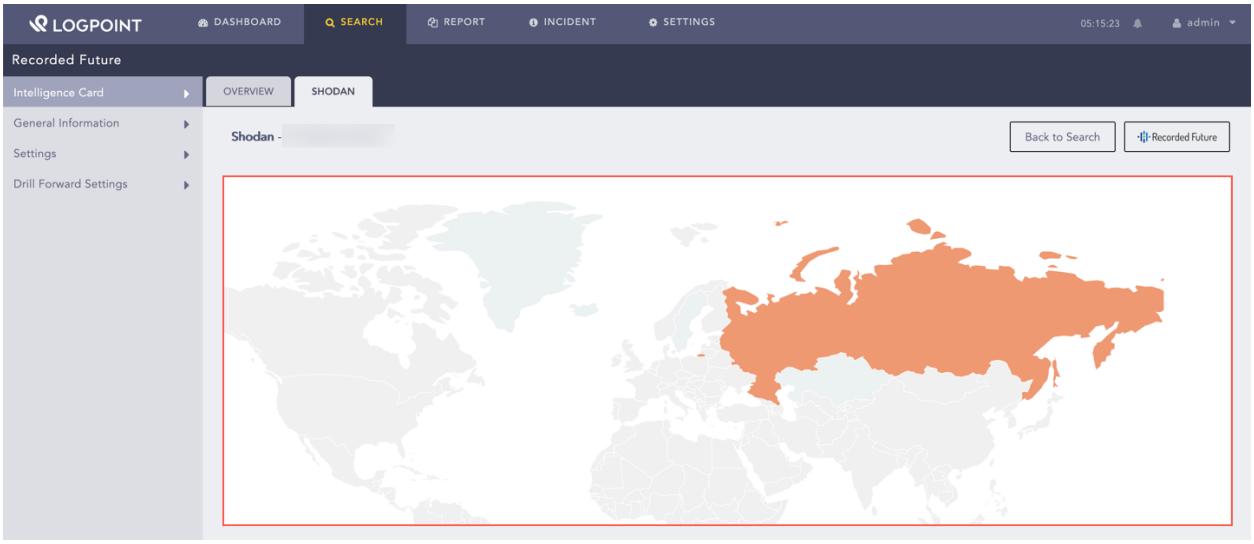

Fig. 7: Map

You can find the enriched data for the IP address under **General Information**, **Tags**, and **Ports**.

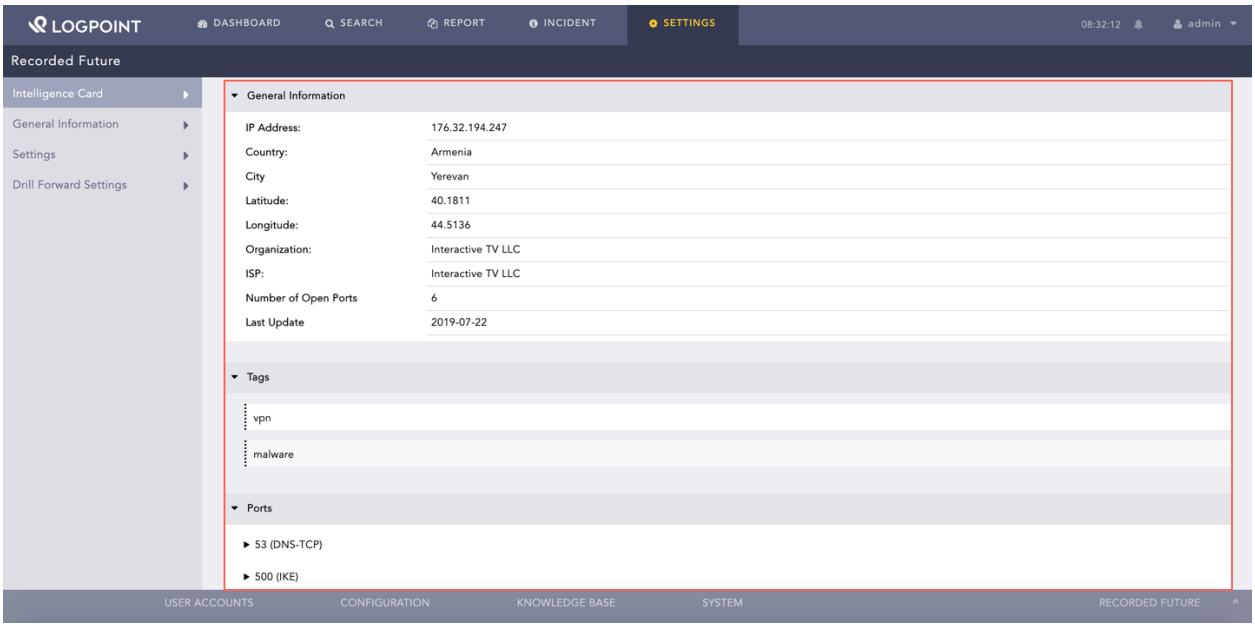

Fig. 8: Enriched Data for IP Address

Shodan enriches the Vulnerability Intelligence Card with fetched data from the Exploit Database. You can find the enriched data under the **Exploits** section.

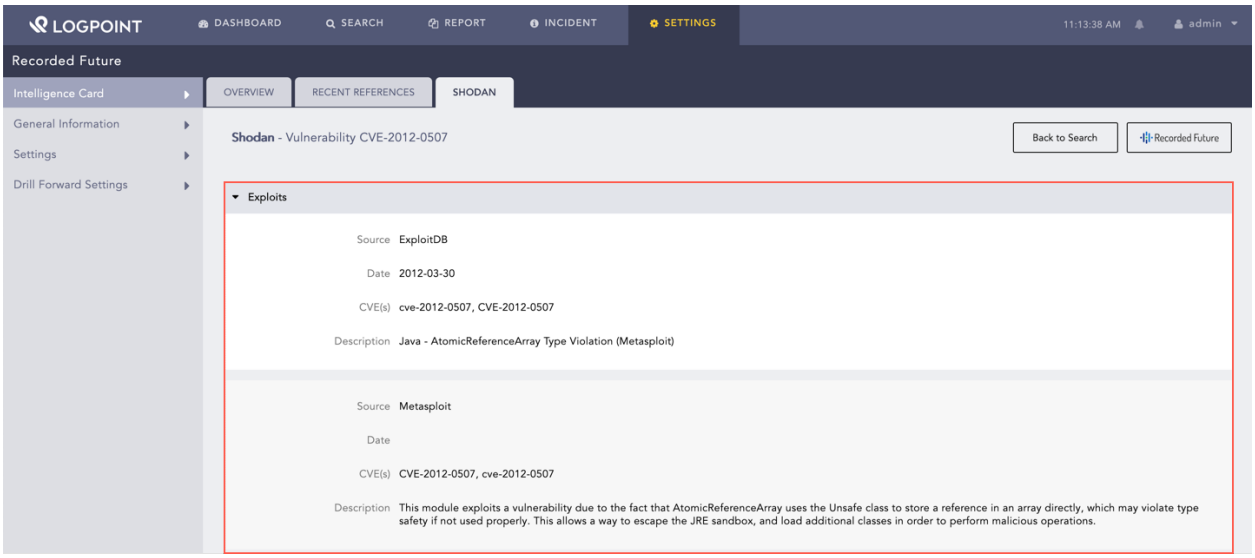

Fig. 9: Enriched Data for Vulnerability

CHAPTER

SEVEN

UNINSTALLATION

7.1 Uninstalling the RecordedFuture Application in LogPoint

1. Go to *Settings >> System >> Applications*.
2. Click the **Uninstall** (🗑) icon from the **Actions** column.

Note: You must disable the RecordedFuture threat intelligence source before uninstalling the application.