

Integrations

Recorded Future

V5.0.0

CONTENTS

1 RecordedFuture Application	1
1.1 Using Recorded Future 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	7
5 Search and Drill Forward	9
6 Intelligence Card	11
6.1 Overview	11
6.2 Threat Lists	14
6.3 Recent References	15
6.4 Shodan	15
7 Uninstallation	19
7.1 Uninstalling the RecordedFuture Application in LogPoint	19

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 the threat information of the following entities from *Recorded Future*:

- IP Address
- URL (Uniform Resource Locator)
- 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 Recorded Future as a threat 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 Recorded Future in LogPoint

The following steps summarize the flow of using Recorded Future in LogPoint:

1. Install the Threat Intelligence application v5.0.0 or later.
2. Install the Recorded Future application v5.0.0 or later.
3. Add Recorded Future as a threat source in the *Threat Intelligence Management* panel or the *RecordedFuture* panel.

4. Select the Recorded Future entity types to fetch the threat information and store it in LogPoint.
5. Map LogPoint fields to the Recorded Future entity types so that you can drill forward from the fields to the Intelligence Card.
6. Apply an enrichment policy with the Threat Intelligence enrichment source.
7. From the search results, drill forward and find the Intelligence Card for the mapped fields.

INSTALLATION

2.1 Prerequisites

- LogPoint v6.7.0 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 *RecordedFuture_5.0.0.pak* file.
4. Click **Upload**.

After installing the application, you can find the *RecordedFuture Drill Forward 5.0.0* and *Recorded Future Enrichment Source 5.0.0* entries under *Settings >> System >> Plugins*.

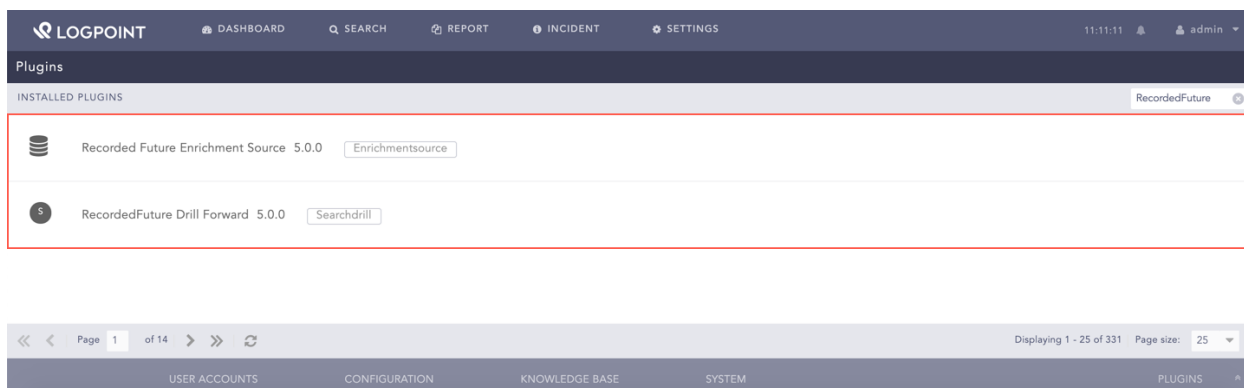


Fig. 1: Recorded Future Installed

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 source.

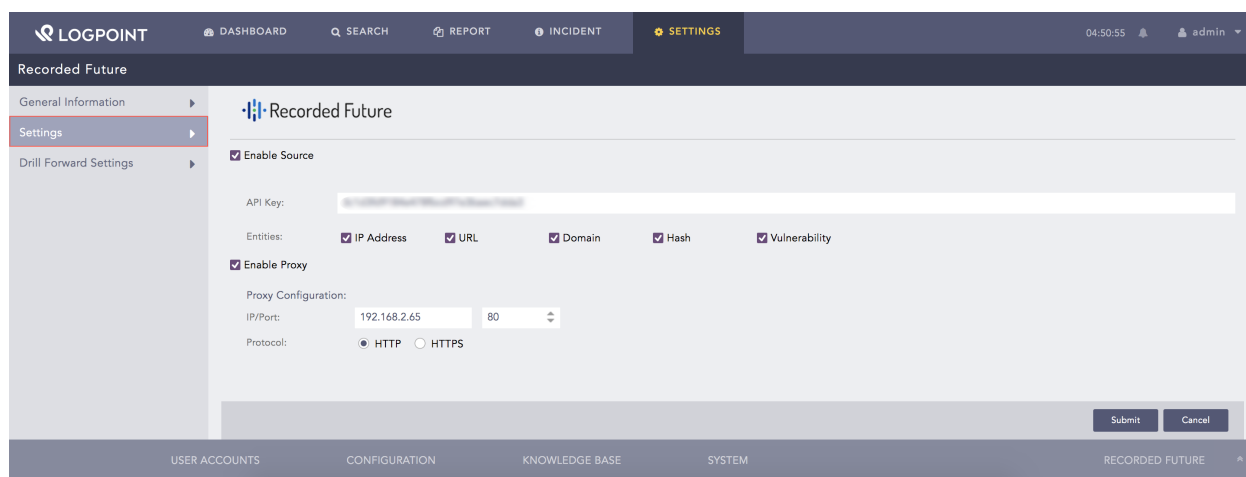


Fig. 1: Configuring Recorded Future

4. Enter the **API Key** provided by *Recorded Future*.
5. Select the required **Entities**. The application fetches and stores the 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**.

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 Recorded Future 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*. You must map the LogPoint fields with the *Recorded Future* entity type to use the drill forward feature as 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 map LogPoint fields to the *Recorded Future* entity types:

1. Go to *Settings >> Configuration >> Recorded Future*.
2. Select **Drill Forward Settings**.
3. Select the **Type** of entity from the drop-down menu.
4. Enter the **LogPoint Taxonomy Field** to map the entity type.

LOGPOINT DASHBOARD SEARCH REPORT INCIDENT SETTINGS 08:26:09 admin

Recorded Future

General Information Settings **Drill Forward Settings**

ADD NEW KEY VALUE

Type: Vulnerability

LogPoint Taxonomy Field: threat_category

Add

S.N.	LogPoint Taxonomy Field	Type	Actions
1	source_address	IP Address	
2	destination_address	IP Address	
3	ip_address	IP Address	
4	device_ip	IP Address	
5	host_address	IP Address	
6	hash	Hash	
7	hash_sha256	Hash	
8	hash_sha1	Hash	
9	domain	Domain	
10	url	URL	
11	threat	Vulnerability	

Submit

USER ACCOUNTS CONFIGURATION KNOWLEDGE BASE SYSTEM RECORDED FUTURE

Fig. 2: Mapping LogPoint Field with the Recorded Future Entity Type

5. Click **Add**.
6. Click **Submit**.

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 and 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 <i>Fetching</i> , <i>Completed</i> , or <i>Error</i>
Number of Records	Total number of records fetched according to the entity type

LOGPOINT

DASHBOARD

SEARCH

REPORT

INCIDENT

SETTINGS

04:58:57

admin

Recorded Future

General Information

Settings

Drill Forward Settings

Total Records: 293522

S.N.	Name	Type	Last Successful Fetch	Status	Number of Records
1	IP Risklist	IP	2019-07-10 04:00:37	Completed	35091
2	Domain Risklist	Domain	2019-07-10 03:01:12	Completed	14845
3	URL Risklist	URL	2019-07-10 03:01:12	Completed	100000
4	Hash Risklist	Hash	2019-07-09 11:02:25	Completed	100000
5	Vulnerability Risklist	Vulnerability	2019-07-09 11:02:25	Completed	43586

USER ACCOUNTS

CONFIGURATION

KNOWLEDGE BASE

SYSTEM

RECORDED FUTURE

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.

SEARCH AND DRILL FORWARD

Follow these steps to drill forward on the enriched field:

1. Search for the enriched logs.

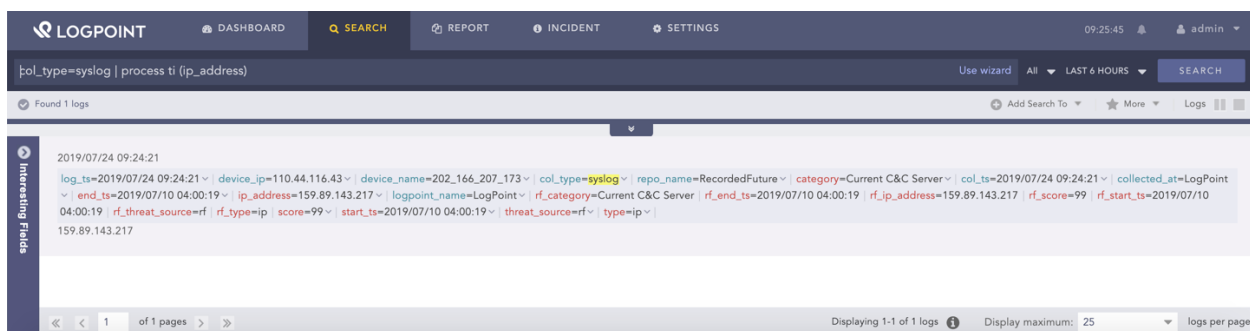


Fig. 1: Search Tab

2. Click the drop-down menu of the previously mapped field in the *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.

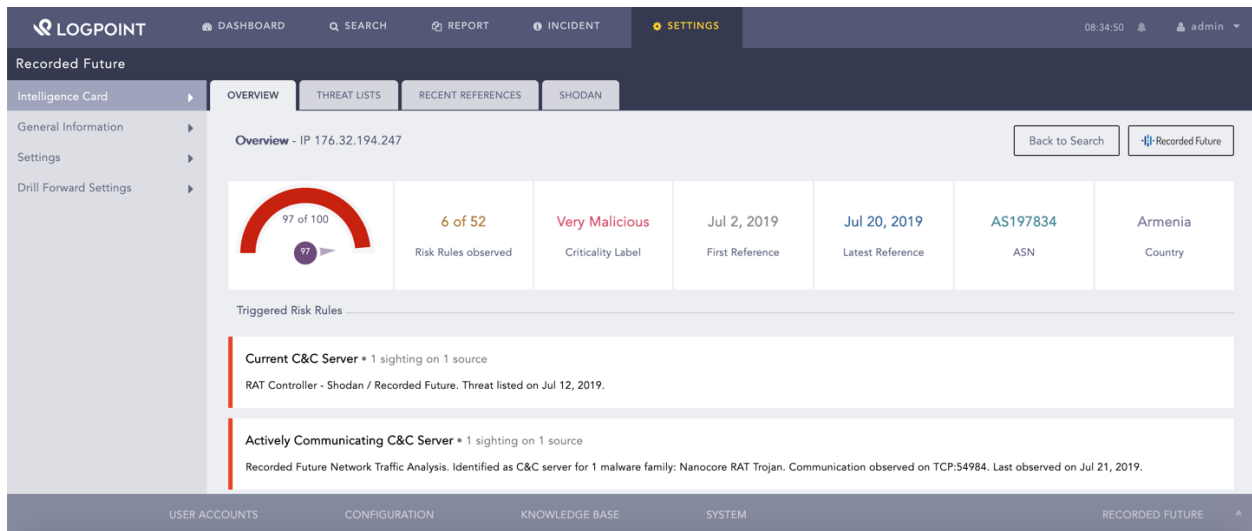


Fig. 3: Intelligence Card

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 that you have drilled forward from the search results.

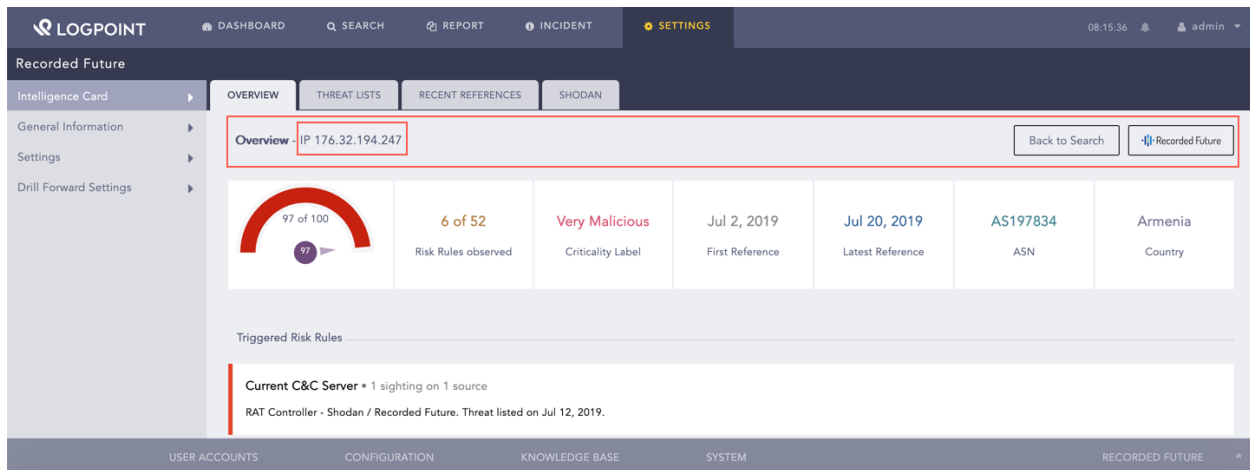


Fig. 1: Selected Entity

The **Back to Search** option redirects you to the search results page.

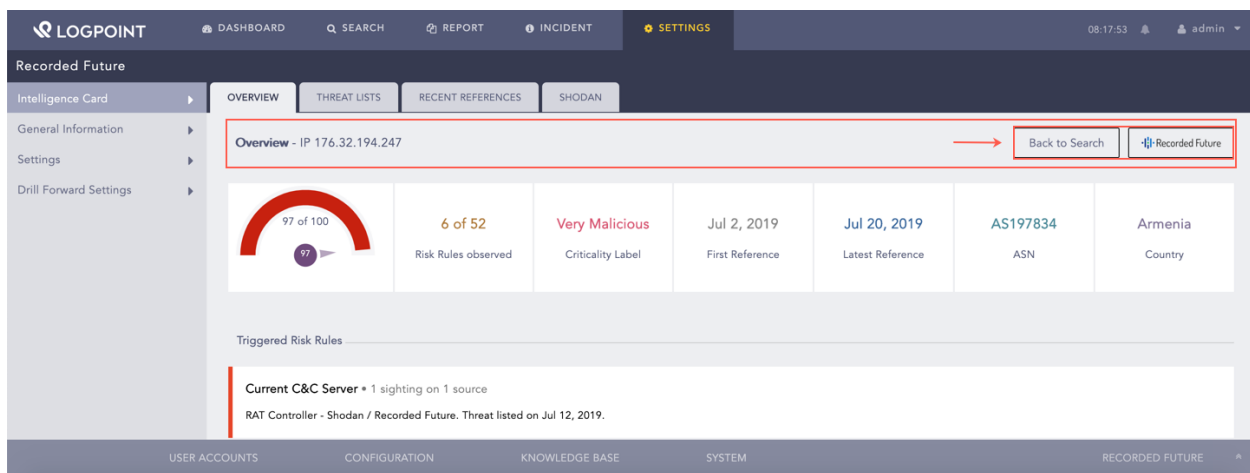


Fig. 2: Back to Search

The **Recorded Future** option redirects you to *Recorded Future's* Intelligence Card.

6.1.2 Risk Score and Risk-Related Content

Recorded Future generates a risk score and specific risk-related content 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

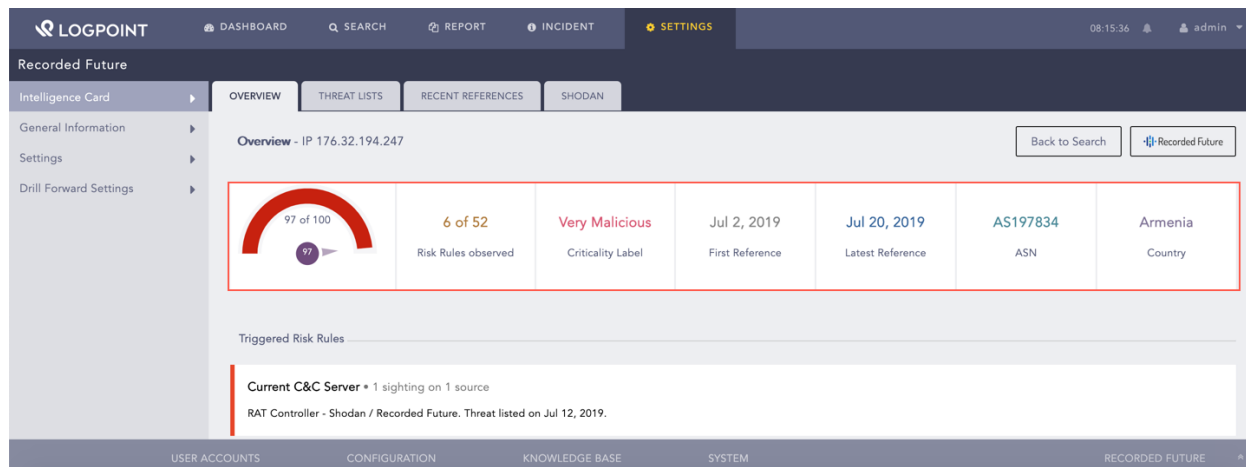


Fig. 3: Risk Score and Risk-Related Content

The gauge 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.

6.1.3 Triggered Risk Rules

Recorded Future has its own set of risk rules that are triggered on the basis of 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.

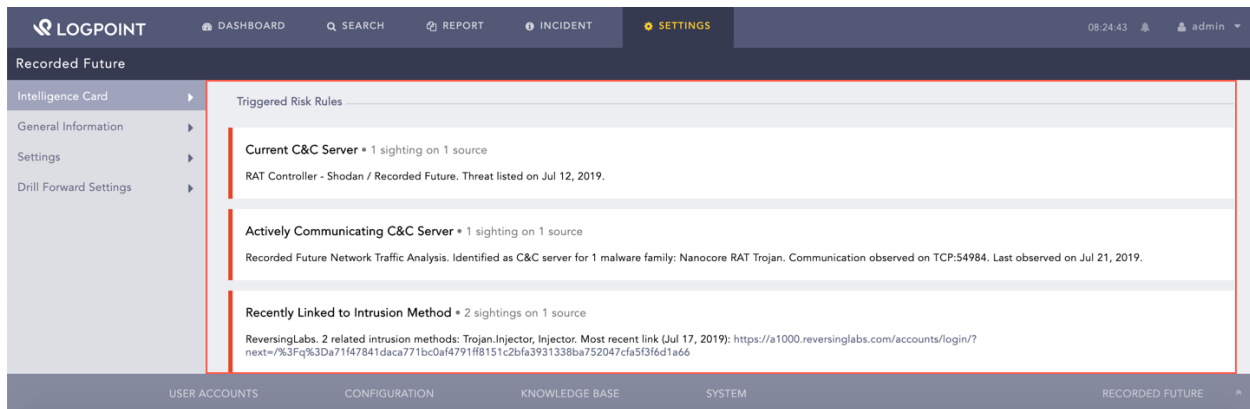


Fig. 4: Triggered Risk Rules

6.2 Threat Lists

The Threat Lists tab consists of the 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**.

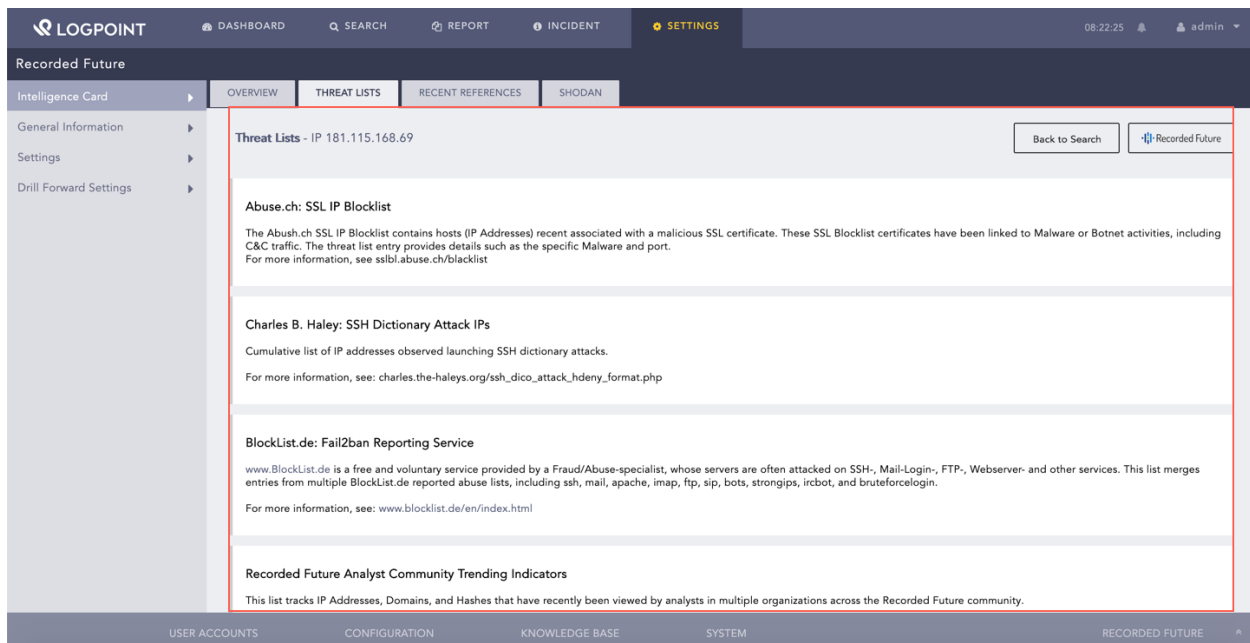


Fig. 5: Threat Lists

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

LOGPOINT DASHBOARD SEARCH REPORT INCIDENT SETTINGS 08:28:08 admin

Recorded Future

Intelligence Card OVERVIEW THREAT LISTS RECENT REFERENCES SHODAN

General Information Settings Drill Forward Settings

Recent References - IP 176.32.194.247 Back to Search Recorded Future

Type:	Most Recent
Title:	ReversingLabs scan for SHA-256 a71f47841daca771bc0af4791f8151c2bfa3931338ba752047cfa5f3f6d1a66
Source:	ReversingLabs
Published:	2019-07-17T04:13:19.000Z
Fragment:	Trojan.Injector on 2019-07-19T20:14:39 : TCP Destinations: address: 192.168.2.73 port: 54095 address: 192.168.2.73 port: 62139 address: 192.168.2.73 port: 49164 address: 192.168.2.73 port: 51957 address: 192.168.2.73 port: 49159 address: 192.168.2.73 port: 63361 address: 192.168.2.73 port: 49170 address: 8.8.8.8 port: 53 address: 176.32.194.247 port: 54984 address: 192.168.2.73 port: 49166 .
Url:	https://a1000.reversinglabs.com/accounts/login/?next=/%3Fq%3Da71f47841daca771bc0af4791f8151c2bfa3931338ba752047cfa5f3f6d1a66

Type:	Recent Info Sec
Title:	ReversingLabs scan for SHA-256 a71f47841daca771bc0af4791f8151c2bfa3931338ba752047cfa5f3f6d1a66
Source:	ReversingLabs
Published:	2019-07-17T04:13:19.000Z
Fragment:	Trojan.Injector on 2019-07-19T20:14:39 : TCP Destinations: address: 192.168.2.73 port: 54095 address: 192.168.2.73 port: 62139 address: 192.168.2.73 port: 49164 address: 192.168.2.73 port: 51957 address: 192.168.2.73 port: 49159 address: 192.168.2.73 port: 63361 address: 192.168.2.73 port: 49170 address: 8.8.8.8 port: 53 address: 176.32.194.247 port: 54984 address: 192.168.2.73 port: 49166 .
Url:	https://a1000.reversinglabs.com/accounts/login/?next=/%3Fq%3Da71f47841daca771bc0af4791f8151c2bfa3931338ba752047cfa5f3f6d1a66

USER ACCOUNTS CONFIGURATION KNOWLEDGE BASE SYSTEM RECORDED FUTURE

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 in a map.

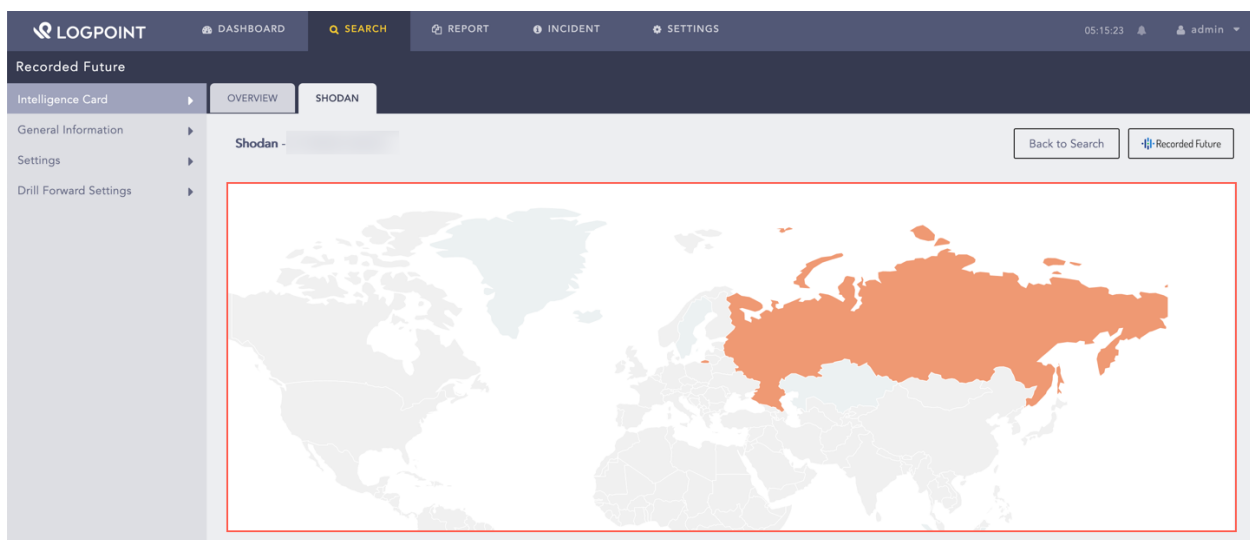


Fig. 7: Map

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

The screenshot displays the Recorded Future web application interface. The top navigation bar includes the Logpoint logo and tabs for DASHBOARD, SEARCH, REPORT, INCIDENT, and SETTINGS (which is highlighted). The right side of the header shows the time 08:32:12 and the user 'admin'. Below the header, the 'Recorded Future' section is active. On the left, a sidebar contains 'Intelligence Card' and its sub-items: 'General Information', 'Settings', and 'Drill Forward Settings'. The main content area shows the 'General Information' tab selected, displaying a table of enriched data for an IP address. The data includes location (Armenia, Yerevan), coordinates, organization (Interactive TV LLC), and open ports (53, 500). Below the table, there are sections for 'Tags' (vpn, malware) and 'Ports' (53, 500). The bottom of the interface features a navigation bar with links to USER ACCOUNTS, CONFIGURATION, KNOWLEDGE BASE, SYSTEM, and RECORDED FUTURE.

General Information	
IP Address:	176.32.194.247
Country:	Armenia
City:	Yerevan
Latitude:	40.1811
Longitude:	44.5136
Organization:	Interactive TV LLC
ISP:	Interactive TV LLC
Number of Open Ports	6
Last Update	2019-07-22

Tags

- vpn
- malware

Ports

- 53 (DNS-TCP)
- 500 (IKE)

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.

The screenshot shows the Recorded Future web interface. The top navigation bar includes LOGPOINT, DASHBOARD, SEARCH, REPORT, INCIDENT, and SETTINGS. The user is logged in as 'admin' at 11:13:38 AM. The main content area is titled 'Recorded Future' and shows the 'Shodan - Vulnerability CVE-2012-0507' page. The left sidebar has a menu with 'Intelligence Card', 'General Information', 'Settings', and 'Drill Forward Settings'. The main content area has tabs for 'OVERVIEW', 'RECENT REFERENCES', and 'SHODAN'. The 'SHODAN' tab is active, showing a list of exploits. The first exploit is from ExploitDB, dated 2012-03-30, with CVE(s) cve-2012-0507, CVE-2012-0507, and a description: 'Java - AtomicReferenceArray Type Violation (Metasploit)'. The second exploit is from Metasploit, dated 2012-03-30, with CVE(s) CVE-2012-0507, cve-2012-0507, and a description: 'This module exploits a vulnerability due to the fact that AtomicReferenceArray uses the Unsafe class to store a reference in an array directly, which may violate type safety if not used properly. This allows a way to escape the JRE sandbox, and load additional classes in order to perform malicious operations.'

Fig. 9: Enriched Data for Vulnerability

UNINSTALLATION

7.1 Uninstalling the RecordedFuture Application in LogPoint

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

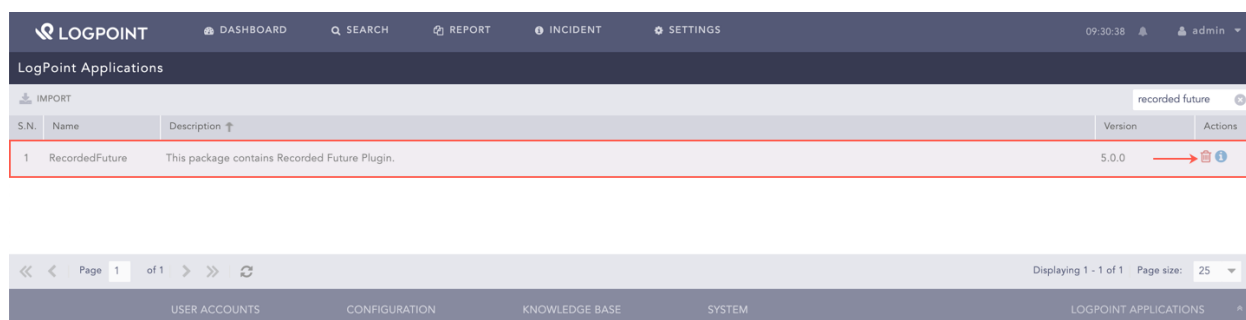


Fig. 1: Uninstalling RecordedFuture

Note: You must disable the Recorded Future threat source before uninstalling the application.
