



# LOGPOINT

**RecordedFuture Manual**

*Release 5.0.0*

**LogPoint**

**Feb 26, 2020**

# CONTENTS

<b>1 RecordedFuture Application</b>	<b>1</b>
1.1 Using Recorded Future in LogPoint . . . . .	1
<b>2 Installation</b>	<b>2</b>
2.1 Prerequisites . . . . .	2
2.2 Installing the RecordedFuture Application in LogPoint . . . . .	2
<b>3 Configuration</b>	<b>3</b>
3.1 Configuring the RecordedFuture Application in LogPoint . . . . .	3
3.2 Configuring Drill Forward . . . . .	4
<b>4 General Information</b>	<b>6</b>
<b>5 Search and Drill Forward</b>	<b>7</b>
<b>6 Intelligence Card</b>	<b>9</b>
6.1 Overview . . . . .	9
6.2 Threat Lists . . . . .	12
6.3 Recent References . . . . .	13
6.4 Shodan . . . . .	13
<b>7 Uninstallation</b>	<b>16</b>
7.1 Uninstalling the RecordedFuture Application in LogPoint . . . . .	16

## RECORDEDFUTURE 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* (page 9). 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*.

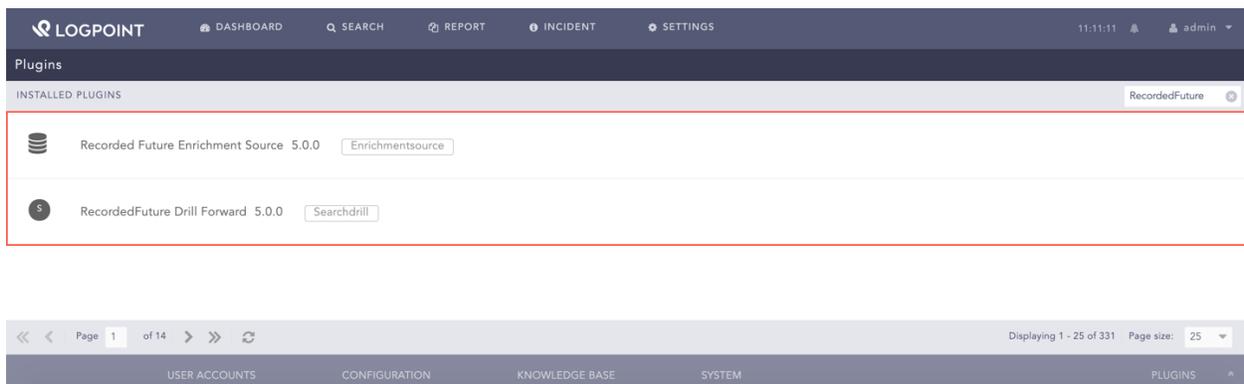


Fig. 2.1: Recorded Future Installed

## 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.

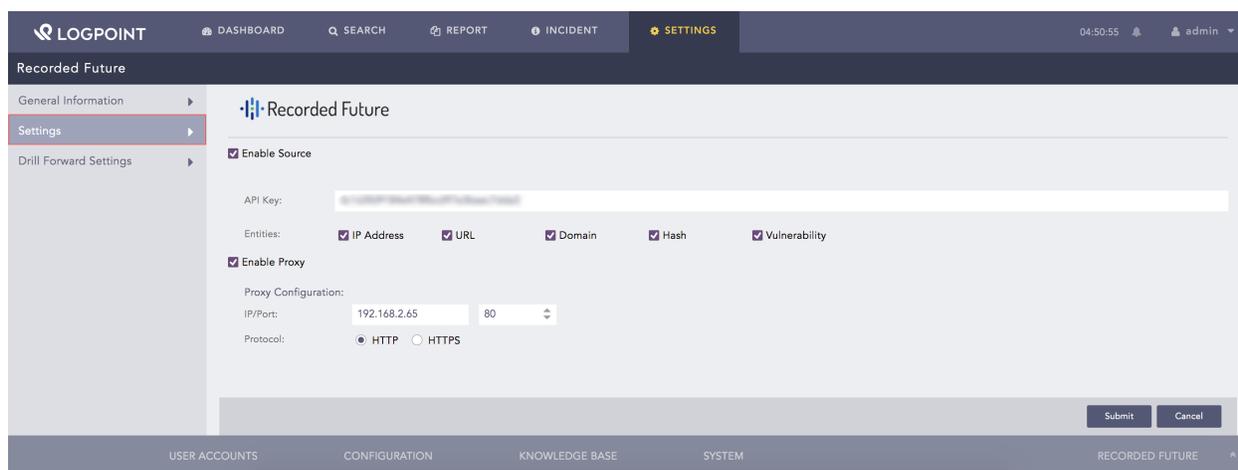


Fig. 3.1: Configuring Recorded Future

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* (page 9). 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.

The screenshot shows the Recorded Future Settings interface. The top navigation bar includes LOGPOINT, DASHBOARD, SEARCH, REPORT, INCIDENT, and SETTINGS. The user is logged in as admin. The left sidebar shows the navigation menu with 'Drill Forward Settings' selected. The main content area is titled 'Recorded Future' and contains the 'ADD NEW KEY VALUE' form. The form has a 'Type' dropdown menu set to 'Vulnerability' and a 'LogPoint Taxonomy Field' input field containing 'threat\_category'. Below the form is an 'Add' button. A table lists existing mappings:

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

At the bottom right of the form area is a 'Submit' button. The footer of the interface shows 'USER ACCOUNTS', 'CONFIGURATION', 'KNOWLEDGE BASE', 'SYSTEM', and 'RECORDED FUTURE'.

Fig. 3.2: 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

The screenshot shows the Recorded Future interface. The top navigation bar includes LOGPOINT, DASHBOARD, SEARCH, REPORT, INCIDENT, and SETTINGS. The main content area is titled 'Recorded Future' and shows 'General Information' with a total of 293522 records. A table lists the following risk lists:

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

Fig. 4.1: 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.

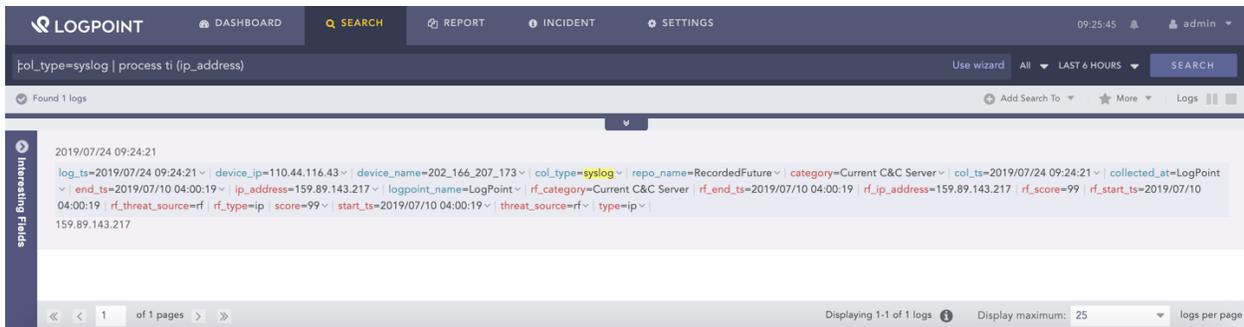


Fig. 5.1: Search Tab

2. Click the drop-down menu of the previously mapped field in the *Configuring Drill Forward* (page 4).

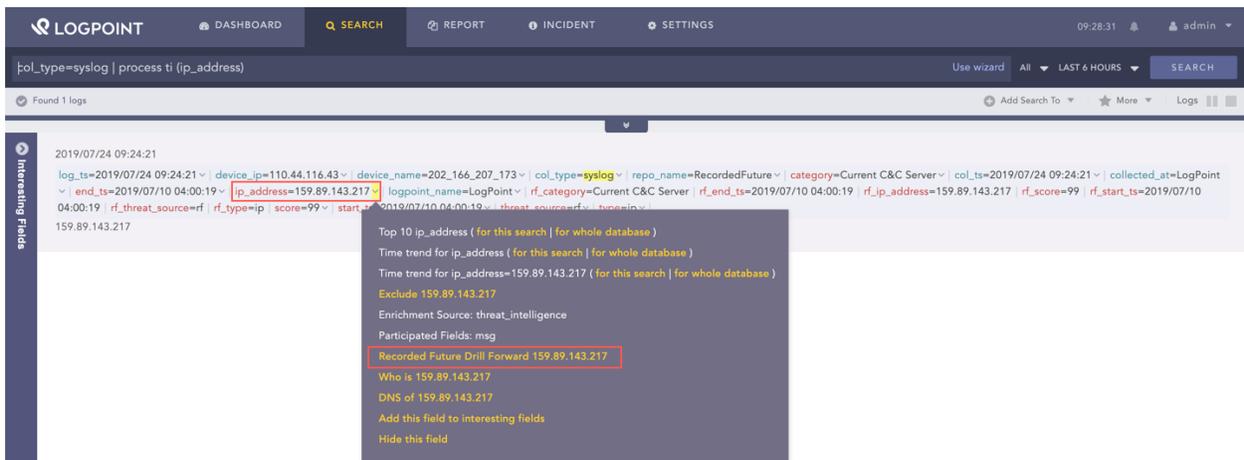


Fig. 5.2: Recorded Future Drill Forward

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

**Note:** Each drill forward uses 1 API credit.

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

The screenshot shows the Recorded Future interface. At the top, there is a navigation bar with 'LOGPOINT' and menu items: DASHBOARD, SEARCH, REPORT, INCIDENT, and SETTINGS. The user is logged in as 'admin' at 08:34:50. Below the navigation bar, the 'Recorded Future' section is active, with a sub-menu for 'Intelligence Card' containing 'OVERVIEW', 'THREAT LISTS', 'RECENT REFERENCES', and 'SHODAN'. The 'OVERVIEW' tab is selected, showing details for IP 176.32.194.247. A 'Back to Search' button and a 'Recorded Future' icon are visible. The main content area displays a progress indicator (97 of 100), '6 of 52 Risk Rules observed', a 'Very Malicious' criticality label, and a table of references. Below this, two sections describe triggered risk rules: 'Current C&C Server' and 'Actively Communicating C&C Server'. The bottom of the page features a footer with 'USER ACCOUNTS', 'CONFIGURATION', 'KNOWLEDGE BASE', 'SYSTEM', and 'RECORDED FUTURE'.

97 of 100	6 of 52	Very Malicious	Jul 2, 2019	Jul 20, 2019	AS197834	Armenia
	Risk Rules observed	Criticality Label	First Reference	Latest Reference	ASN	Country

Triggered Risk Rules

**Current C&C Server** • 1 sighting on 1 source  
RAT Controller - Shodan / Recorded Future. Threat listed on Jul 12, 2019.

**Actively Communicating C&C Server** • 1 sighting on 1 source  
Recorded Future Network Traffic Analysis. Identified as C&C server for 1 malware family: Nanocore RAT Trojan. Communication observed on TCP:54984. Last observed on Jul 21, 2019.

Fig. 5.3: 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.

The screenshot shows the Recorded Future interface. At the top, there is a navigation bar with 'LOGPOINT' and various menu items: DASHBOARD, SEARCH, REPORT, INCIDENT, and SETTINGS. The user is logged in as 'admin' at 08:15:36. Below the navigation bar, the 'Recorded Future' header is visible. The main content area is titled 'Intelligence Card' and has tabs for OVERVIEW, THREAT LISTS, RECENT REFERENCES, and SHODAN. The 'OVERVIEW' tab is selected, showing the entity 'IP 176.32.194.247'. A 'Back to Search' button and a 'Recorded Future' logo are also present. The overview section displays several key metrics: a risk score of 97 (out of 100) represented by a red arc; 6 of 52 risk rules observed; a 'Very Malicious' criticality label; a first reference on Jul 2, 2019; a latest reference on Jul 20, 2019; an ASN of AS197834; and a country of Armenia. Below this, a section titled 'Triggered Risk Rules' shows one rule: 'Current C&C Server' with 1 sighting on 1 source, and 'RAT Controller - Shodan / Recorded Future. Threat listed on Jul 12, 2019.' The bottom of the interface has a footer with 'USER ACCOUNTS', 'CONFIGURATION', 'KNOWLEDGE BASE', 'SYSTEM', and 'RECORDED FUTURE'.

Fig. 6.1: Selected Entity

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

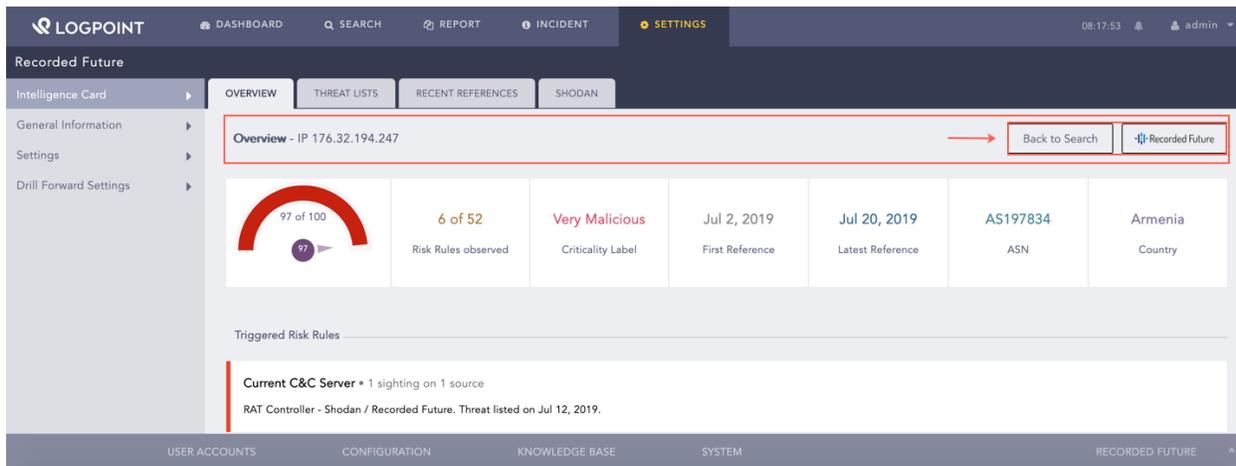


Fig. 6.2: Back to Search

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

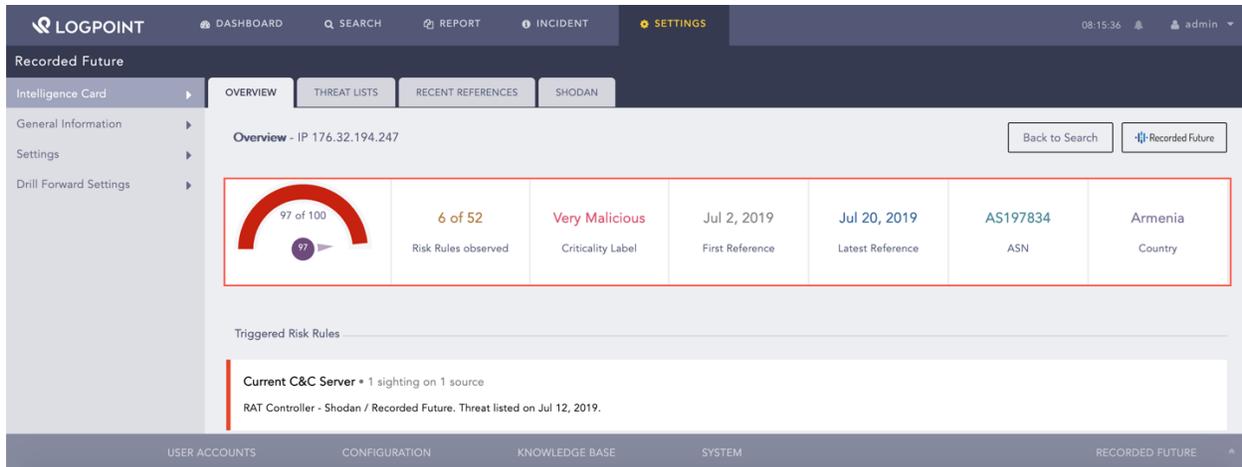


Fig. 6.3: Risk Score and Risk-Related Content

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.

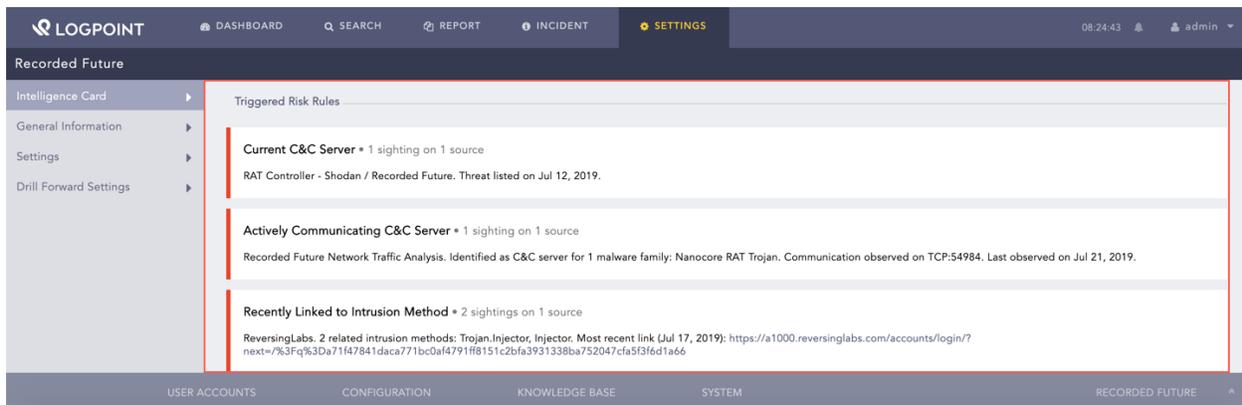


Fig. 6.4: Triggered Risk Rules

## 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**.

The screenshot shows the Recorded Future web interface. At the top, there is a navigation bar with the LOGPOINT logo and menu items: DASHBOARD, SEARCH, REPORT, INCIDENT, and SETTINGS. The user is logged in as 'admin' at 08:22:25. Below the navigation bar, the 'Recorded Future' section is active, with tabs for OVERVIEW, THREAT LISTS, RECENT REFERENCES, and SHODAN. The 'THREAT LISTS' tab is selected, showing a list of threat lists for the IP address 181.115.168.69. The list includes:

- Abuse.ch: SSL IP Blocklist**  
The Abuse.ch SSL IP Blocklist contains hosts (IP Addresses) recent associated with a malicious SSL certificate. These SSL Blocklist certificates have been linked to Malware or Botnet activities, including C&C traffic. The threat list entry provides details such as the specific Malware and port.  
For more information, see [sslb.abuse.ch/blacklist](https://sslb.abuse.ch/blacklist)
- Charles B. Haley: SSH Dictionary Attack IPs**  
Cumulative list of IP addresses observed launching SSH dictionary attacks.  
For more information, see: [charles.the-haleys.org/ssh\\_dico\\_attack\\_hdeny\\_format.php](https://charles.the-haleys.org/ssh_dico_attack_hdeny_format.php)
- BlockList.de: Fail2ban Reporting Service**  
[www.BlockList.de](https://www.BlockList.de) is a free and voluntary service provided by a Fraud/Abuse-specialist, whose servers are often attacked on SSH-, Mail-Login-, FTP-, Webserver- and other services. This list merges entries from multiple BlockList.de reported abuse lists, including ssh, mail, apache, imap, ftp, sip, bots, strongips, ircbot, and bruteforcelogin.  
For more information, see: [www.blocklist.de/en/index.html](https://www.blocklist.de/en/index.html)
- Recorded Future Analyst Community Trending Indicators**  
This list tracks IP Addresses, Domains, and Hashes that have recently been viewed by analysts in multiple organizations across the Recorded Future community.

At the bottom of the interface, there is a footer with navigation links: USER ACCOUNTS, CONFIGURATION, KNOWLEDGE BASE, SYSTEM, and RECORDED FUTURE.

Fig. 6.5: 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

The screenshot displays the Recorded Future interface. At the top, there is a navigation bar with 'LOGPOINT' and several menu items: 'DASHBOARD', 'SEARCH', 'REPORT', 'INCIDENT', and 'SETTINGS'. The user is logged in as 'admin' at 08:28:08. Below the navigation bar, the 'Recorded Future' header is visible. The main content area is titled 'Recent References - IP 176.32.194.247'. On the left, there is a sidebar with 'Intelligence Card' and 'General Information', 'Settings', and 'Drill Forward Settings'. The main content area shows two entries under 'Recent References'. Each entry has the following fields: Type, Title, Source, Published, Fragment, and Uri. The entries are identical, showing a 'Most Recent' and 'Recent Info Sec' type, both from 'ReversingLabs' with a scan for SHA-256. The fragment details a Trojan.Injector scan with various IP addresses and ports.

Field	Value
Type	Most Recent
Title	ReversingLabs scan for SHA-256 a71f47841daca771bc0a4791f8151c2bfa3931338ba752047cfa5f3f6d1a66
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 .
Uri	https://a1000.reversinglabs.com/accounts/login/?next=/%3Fq%3Da71f47841daca771bc0a4791f8151c2bfa3931338ba752047cfa5f3f6d1a66
Type	Recent Info Sec
Title	ReversingLabs scan for SHA-256 a71f47841daca771bc0a4791f8151c2bfa3931338ba752047cfa5f3f6d1a66
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 .
Uri	https://a1000.reversinglabs.com/accounts/login/?next=/%3Fq%3Da71f47841daca771bc0a4791f8151c2bfa3931338ba752047cfa5f3f6d1a66

Fig. 6.6: 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.

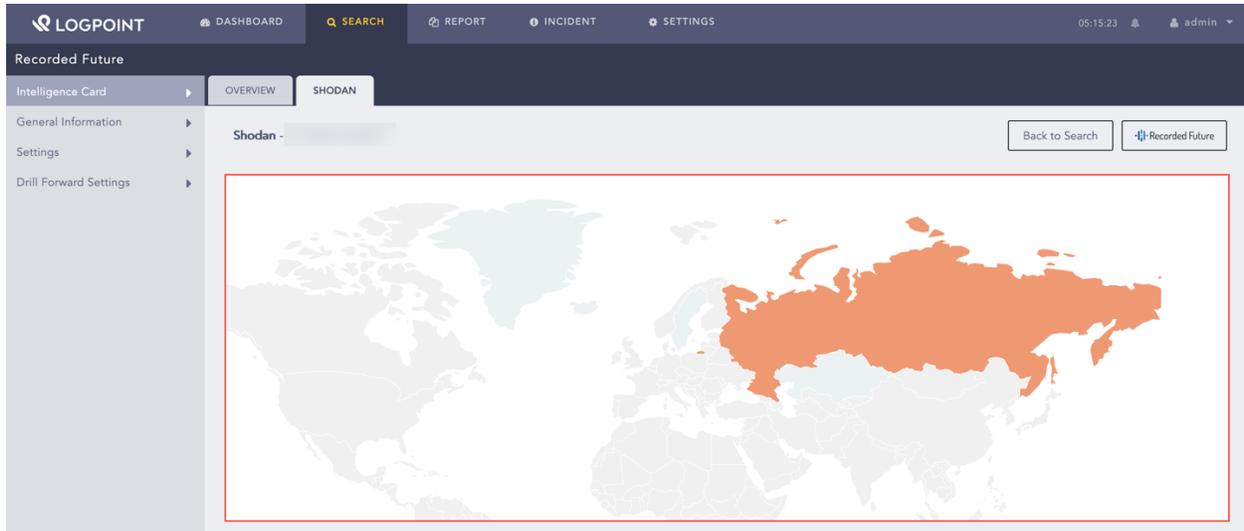


Fig. 6.7: Map

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

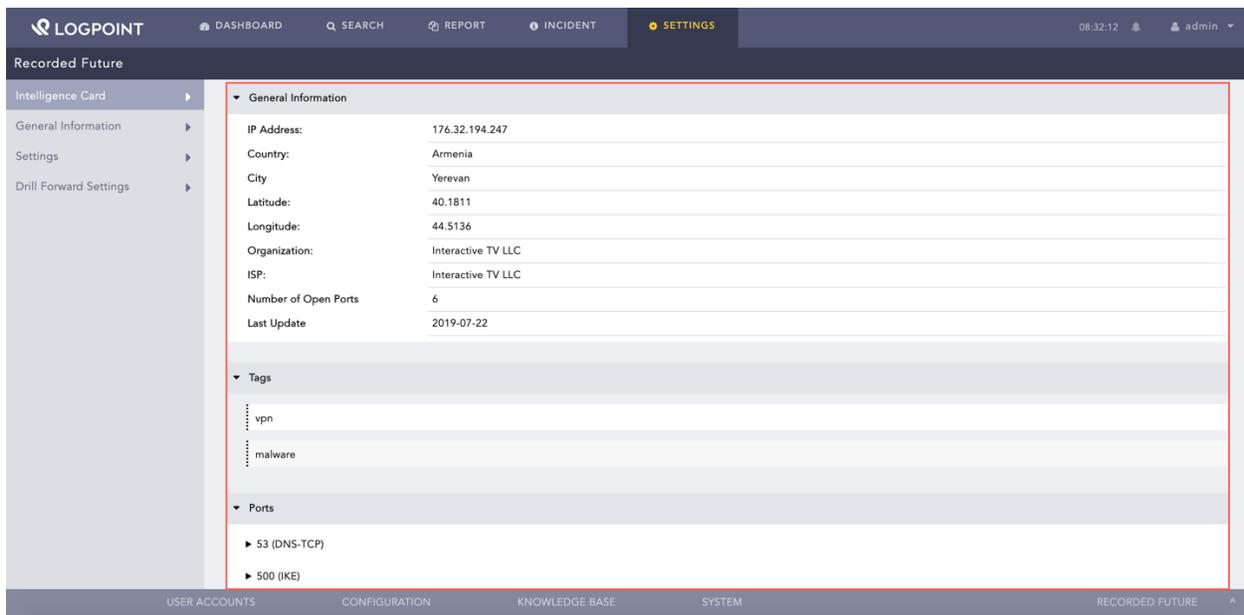
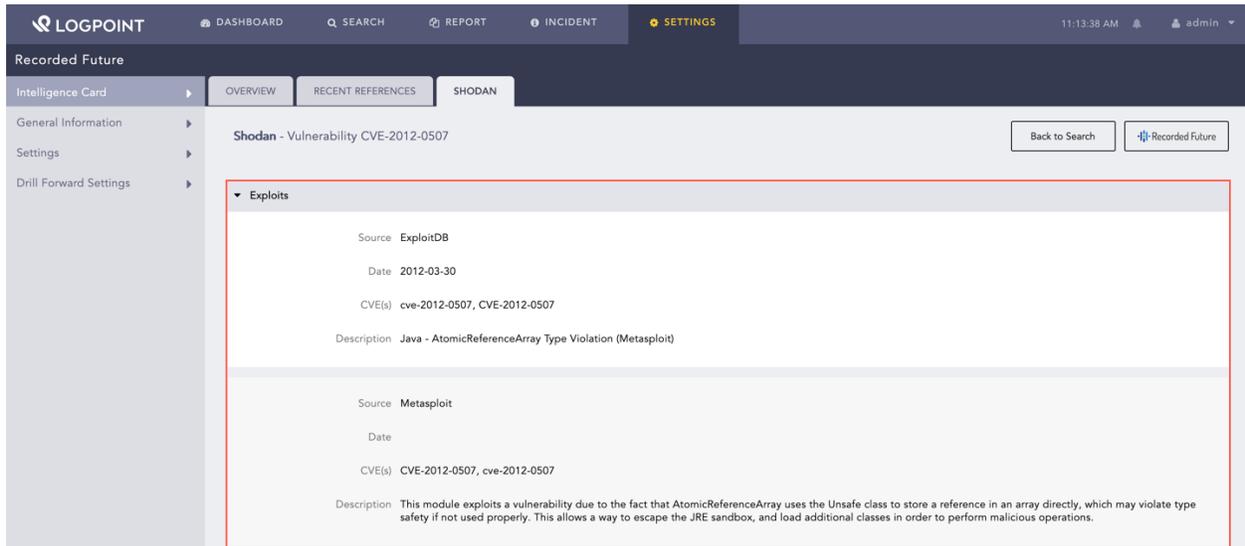


Fig. 6.8: Enriched Data for IP Address

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 displays the RecordedFuture interface. The top navigation bar includes the LOGPOINT logo and menu items: 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 'Intelligence Card' for 'Shodan - Vulnerability CVE-2012-0507'. The 'SHODAN' tab is active. The 'Exploits' section is expanded, showing two entries:

- Source:** ExploitDB
- Date:** 2012-03-30
- CVE(s):** cve-2012-0507, CVE-2012-0507
- Description:** Java - AtomicReferenceArray Type Violation (Metasploit)

- Source:** Metasploit
- Date:**
- CVE(s):** CVE-2012-0507, cve-2012-0507
- 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. 6.9: 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.

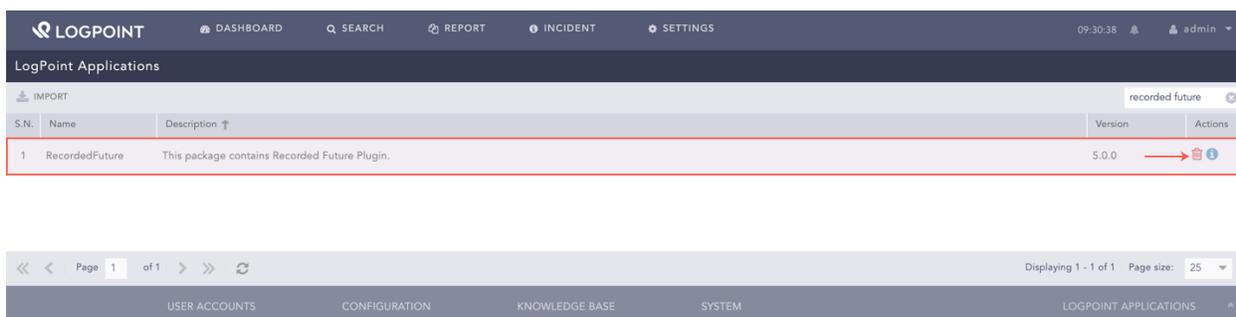


Fig. 7.1: Uninstalling RecordedFuture

---

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

---