### Threat Intelligence

#### Overview

Logpresso supports effective responses to the latest and known threats through the Logpresso CTI (Cyber Threat Intelligence) service. This service collects, analyzes, and shares various up-to-date threat information, enabling organizations to quickly identify and respond to cyber threats.

Logpresso CTI

Upon installing Logpresso Sonar, a list of Logpresso CTI feeds is provided.

|  |  |  |  |
| --- | --- | --- | --- |
| Name | STR\_FEED\* | Type | Description |
| Logpresso CTI IP | logpresso\_cti\_ip | IP | Information on malicious IP addresses related to cyber attacks |
| Logpresso CTI Domain | logpresso\_cti\_domain | DOMAIN | Information on malicious domain addresses such as malware distribution sites and C&C servers |
| Logpresso CTI URL | logpresso\_cti\_url | URL | Information on Logpresso CTI URL indicators |
| Logpresso CTI MD5 | logpresso\_cti\_md5 | MD5 | Logpresso CTI MD5 hash indicator feed |
| Logpresso CTI SHA1 | logpresso\_cti\_sha1 | SHA1 | Logpresso CTI SHA1 hash indicator feed |
| Logpresso CTI SHA256 | logpresso\_cti\_sha256 | SHA256 | Logpresso CTI SHA256 hash indicator feed |

\* **STR\_FEED** refers to the name=STR\_FEED option described in the [matchfeed command documentation](https://docs.logpresso.comnull).

To utilize Logpresso CTI:

A subscription contract is required for Logpresso CTI feeds. Paid subscriptions provide real-time feeds, while free subscriptions offer feeds with a 90-day delay.

Configure your network security policy to allow Logpresso Sonar to connect to the Logpresso CTI service (https://cti.logpresso.com). The CTI provided by the app also requires a connection to the service provider's service address.

To use the Logpresso CTI service on the Logpresso platform, you must set up a connect profile for the Logpresso CTI server. For instructions on setting up a connect profile, refer to [Connect Profiles](https://docs.logpresso.comnull).

CTI Provided by Apps

Apps such as [S2W Quaxar](https://logpresso.store/ko/apps/quaxar) available in the Logpresso Store provide threat intelligence. Upon installation, these apps will offer CTI feeds in the threat intelligence list. In this case, please contact the respective CTI service provider for service usage inquiries.

#### Viewing/Search Threat Intelligence Feeds

You can view or search for the latest types of threat information under **Policy > Threat Intelligence**.



* **Activation**: Toggle button for activating threat intelligence (: Activated, : Deactivated)
* **Type**: Types of information provided by threat intelligence
* **IP**: Malicious IP addresses, primarily used to identify the source of attacks or command and control servers.
* **DOMAIN**: Malicious domain addresses, used to identify phishing sites or malware distribution sites.
* **MD5, SHA1, SHA256**: Hash values of normal/malicious files, used for file integrity verification and malicious file identification.
* **URL**: Threat information of malicious web URLs, used to block links to malicious websites involved in malware distribution or phishing attempts.
* **EMAIL**: Information on compromised email addresses.
* **Name**: Name of the CTI feed.
* **Description**: Description of the CTI feed.
* **Last Updated**: Date and time of the most recent update to the threat intelligence.

To find specific threat intelligence in the threat intelligence list, use the search tool in the toolbar. The search tool will display threat intelligence feeds that include the entered term in the **Name**. The search tool is case-insensitive.

Downloading the List

To download the threat intelligence list as a file to your local PC, click **Download** in the toolbar and select your desired file format.

Refreshing the List

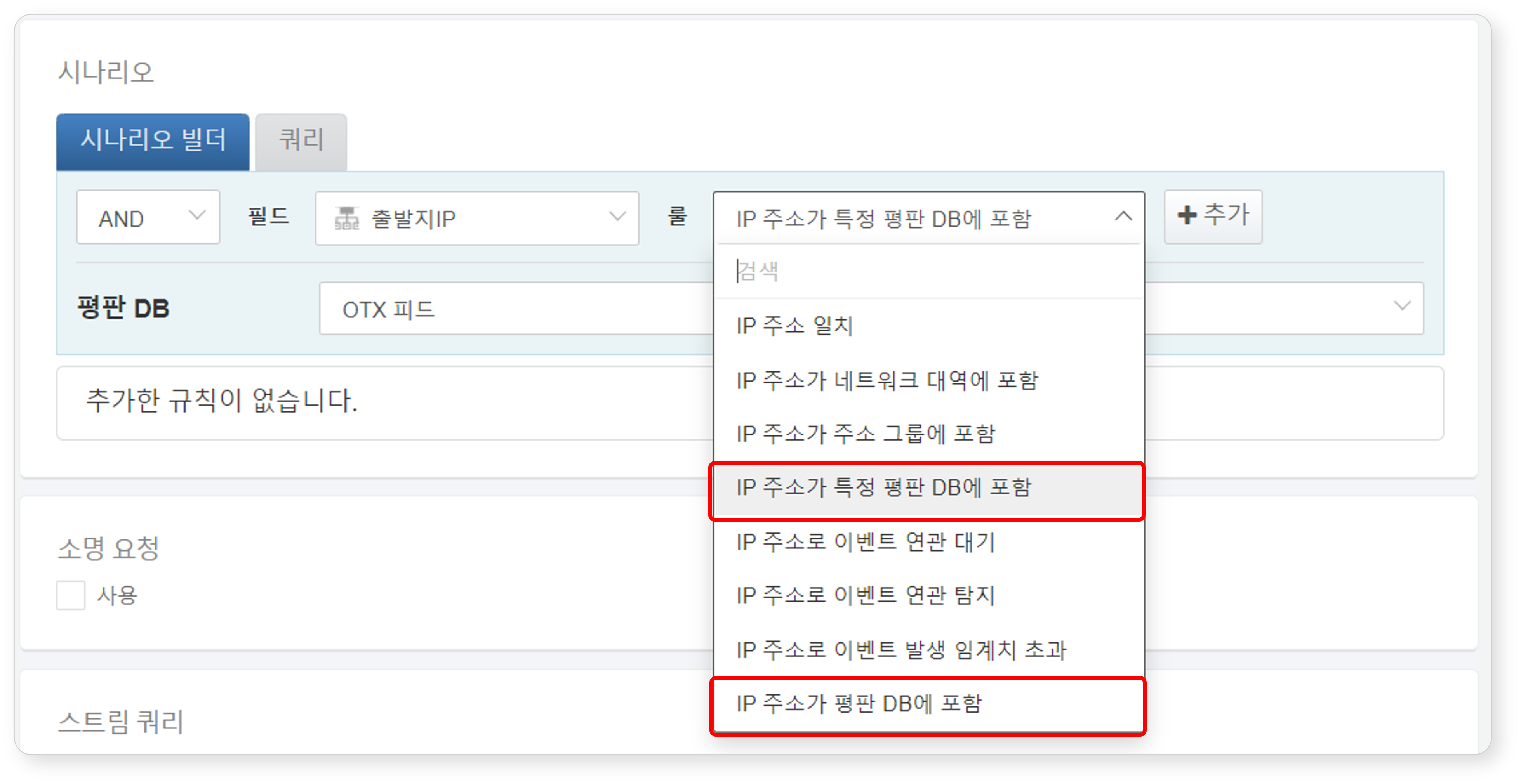
To refresh the threat intelligence list with the latest information, click **Refresh** in the toolbar.

#### Utilizing Threat Intelligence

The functionalities that utilize threat intelligence are as follows.

Scenario Builder

In **Policy > Real-Time Detection**, you can utilize threat intelligence when adding or modifying detection scenarios using the scenario builder.



The following summarizes the threat intelligence feed-related content available by input field type in the scenario builder. For more details, refer to [Field Type Rules and Parameters](https://docs.logpresso.comnull).

**IP**

|  |  |  |  |
| --- | --- | --- | --- |
| Rule | Parameter | Input Range | Description |
| IP address included in a specific reputation DB | Reputation DB | CTI feed selection | Filters field values included in the specified reputation DB |
| IP address included in reputation DB | - | - | Filters field values that have been included in any threat intelligence at least once |

**MD5/SHA1/SHA256**

|  |  |  |  |
| --- | --- | --- | --- |
| Rule | Parameter | Input Range | Description |
| Matches target hash value | Hash | Up to 255 characters | Filters field values that match the hash value |
| Included in reputation DB | - | - | Filters field values that have been included in any threat intelligence at least once |
| Included in a specific reputation DB | Reputation DB | CTI feed selection | Filters field values included in the specified reputation DB |

**URL**

|  |  |  |  |
| --- | --- | --- | --- |
| Rule | Parameter | Input Range | Description |
| URL included in reputation DB | - | - | Filters field values included in the reputation DB |
| URL included in a specific reputation DB | Reputation DB | CTI feed selection | Filters field values included in the specified reputation DB |

**DOMAIN**

|  |  |  |  |
| --- | --- | --- | --- |
| Rule | Parameter | Input Range | Description |
| DOMAIN included in reputation DB | - | - | Filters field values included in the reputation DB |
| DOMAIN included in a specific reputation DB | Reputation DB | CTI feed selection | Filters field values included in the specified reputation DB |

Query

In **Policy > Real-Time Detection** or **Policy > Batch Detection**, you can utilize threat intelligence when adding or modifying detection scenarios using the [matchfeed](https://docs.logpresso.comnull) command or the [matchfeed()](https://docs.logpresso.comnull) function. Additionally, remember that you can use threat intelligence wherever there is a feature for entering query statements.