### Pattern Groups

#### Overview

Pattern Groups support the management of patterns by topic and their incorporation into detection policies. For instance, they can be used to identify vulnerability scans based on IPS log rules or signature names, or to group specific types of attacks such as SQL injection.

Logpresso Sonar operates using the Aho-Corasick algorithm, enabling the simultaneous detection of thousands of keywords, similar to a network intrusion prevention system (IPS). It compares the input string against all keywords belonging to the pattern group at once, and subsequently executes validation expressions sequentially for the patterns selected by the keywords, ultimately detecting events that match the patterns.

Example Patterns

|  |  |  |  |
| --- | --- | --- | --- |
| # | Pattern Name | Pattern (Required): Primary Fast Detection | Validation Expression (Optional): Secondary Filter |
| 1 | xp\_cmdshell | "sp\_addextendedproc" and "xp\_cmdshell" |  |
| 2 | zb\_now\_connect | "REMOTE\_ADDR" and ("fputs" or "fwrite") | path == "lib.php" |

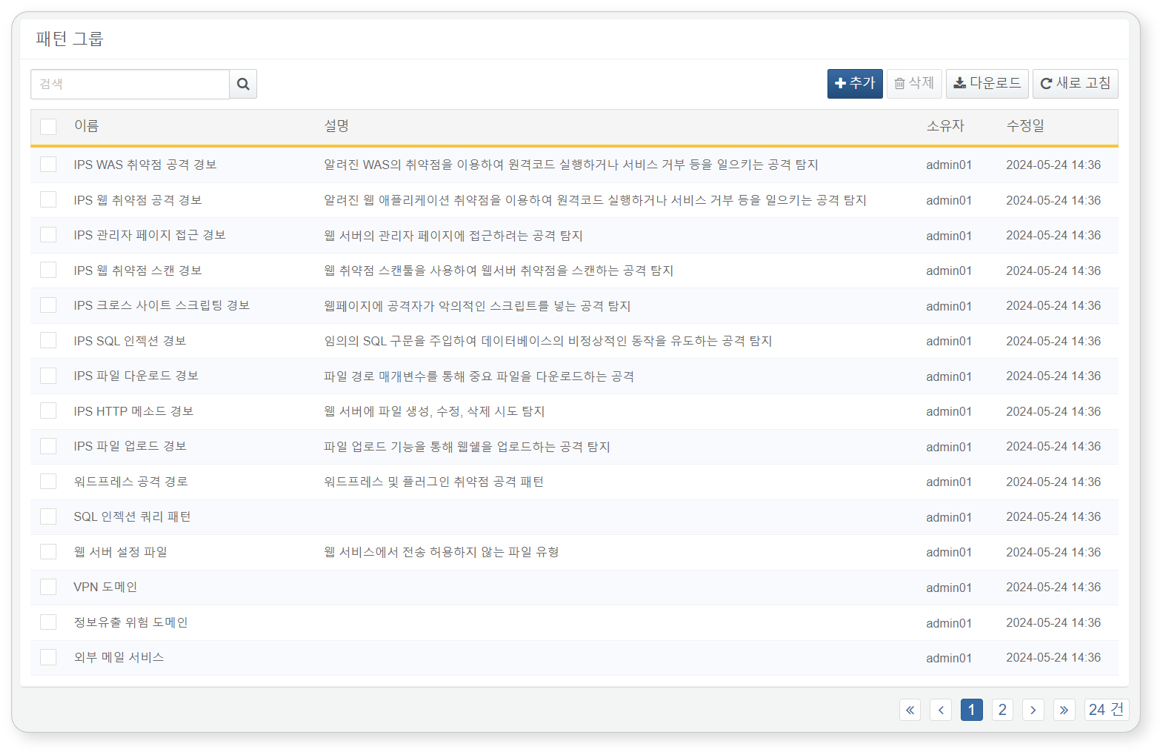
Patterns consist of string patterns and Boolean validation expressions, with the validation expression being optional.

In the first pattern **xp\_cmdshell**, sp\_addextendedproc and xp\_cmdshell are commands frequently used in Microsoft SQL Server. An attacker can use SQL injection to register the xp\_cmdshell command via sp\_addextendedproc, allowing them to execute system commands and perform malicious actions. This pattern is an example created without a validation expression.

The second pattern **zb\_now\_connect** detects an attack that executes arbitrary code lib.php remotely using [ZeroBoard 4.1 pl7 - 'now\_connect()' Remote Code Execution](https://www.exploit-db.com/exploits/9590). This pattern checks whether both the strings fputs or fwrite and REMOTE\_ADDR are found in the input field, and then verifies if the path field value matches the string lib.php.

#### Viewing/Search Pattern Group List

You can view or search the list of pattern groups in **Policies > Pattern Groups**.



* **Name**: Unique name of the pattern group
* **Description**: Description of the pattern group
* **Owner**: User account that added the pattern group
* **Modification Date**: Date the pattern group was created or last modified

To find a specific pattern group in the list, use the search tool in the toolbar. The search tool will display pattern groups that include the entered word in the **Name**, **Description**, **Pattern Name**, **Pattern**, or **Validation Expression** fields. The search tool is case-insensitive.

Downloading the List

To download the pattern group list as a file to your local PC, click **Download** in the toolbar.

Refreshing the List

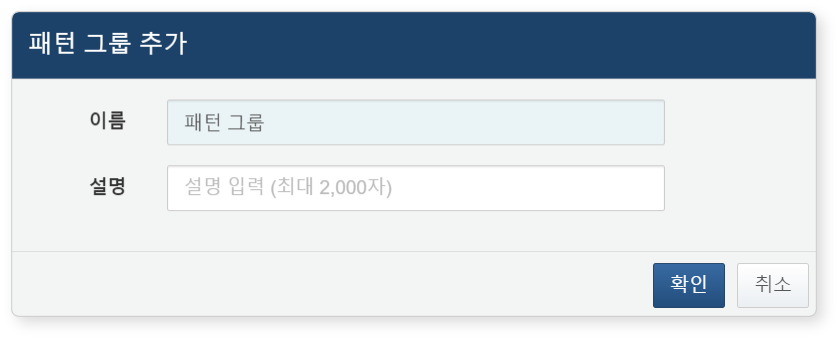
To refresh the pattern group list with the latest information, click **Refresh** in the toolbar.

#### Adding a Pattern Group

To add a pattern group:

Click **Add** in the toolbar under **Policies > Pattern Groups**.

When the **Add Pattern Group** dialog appears, enter the following items and click **OK**.



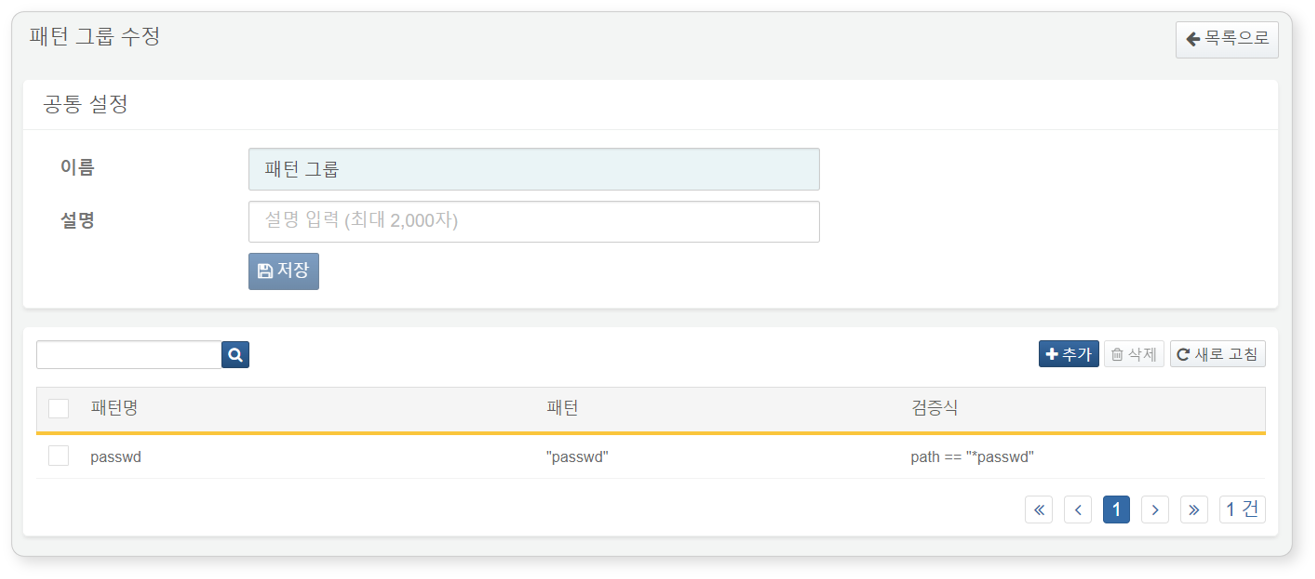
* **Name**: Name of the pattern group (up to 50 characters)
* **Description**: Detailed description of the pattern group (up to 2,000 characters)

#### Modifying a Pattern Group

To modify a pattern group:

Click the name of the pattern group you wish to modify in the [Pattern Group List](https://docs.logpresso.comnull).

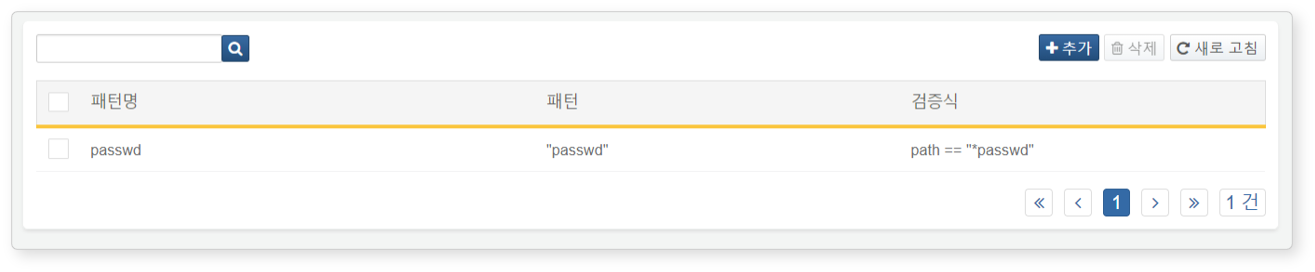
In the **Modify Pattern Group** screen, edit the information and click **Save**.



Viewing/Search Patterns

You can view or search registered patterns in the [Modify Pattern Group](https://docs.logpresso.comnull) screen.

Check the pattern list in the **Modify Pattern Group** screen.



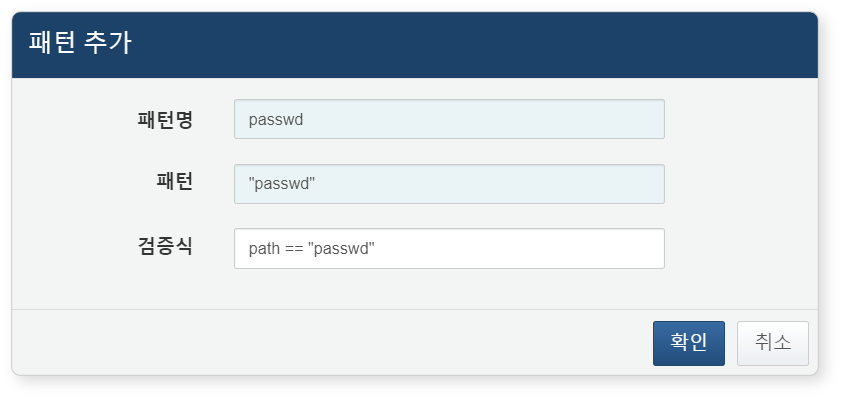
* **Pattern Name**: Name of the registered pattern
* **Pattern**: Pattern string to be detected
* **Validation Expression**: Additional validation and search conditions

Adding a Pattern

To add a pattern item to a pattern group:

Click **Add** in the toolbar on the [Modify Pattern Group](https://docs.logpresso.comnull) screen.

When the **Add Pattern** dialog appears, enter the pattern to be registered and click **OK**.



* **Pattern Name**: Unique name of the pattern to be registered (up to 1,000 characters)
* **Pattern**: Enter the string to search in the field enclosed in double quotes ("). Multiple keywords can be entered using combinations of and and or (minimum 3 characters including spaces, maximum 1,000 characters)
* **Validation Expression**: Conditions for additional validation and search in the detected data when the pattern entered in the pattern item is detected (up to 1,000 characters)
* The validation expression consists of the "Field" to search, the "Condition" (either == or !=), and the "Value" string (e.g., path == "lib.php").

|  |  |  |
| --- | --- | --- |
| Target Field | Condition | Value |
| path | == | "lib.php" |

* Wildcards (\*) can be used at the beginning or end of the "Value".
* The validation expression can be omitted.

Modifying a Pattern

To modify a registered pattern in a pattern group:

Click the name of the pattern you wish to modify in the [Modify Pattern Group](https://docs.logpresso.comnull) screen.

When the **Modify Pattern** dialog appears, edit the information and click **OK**.

Deleting a Pattern

To delete a registered pattern in a pattern group:

Select the checkbox of the pattern group row you wish to delete in the [Modify Pattern Group](https://docs.logpresso.comnull) screen.

Click **Delete** in the toolbar.

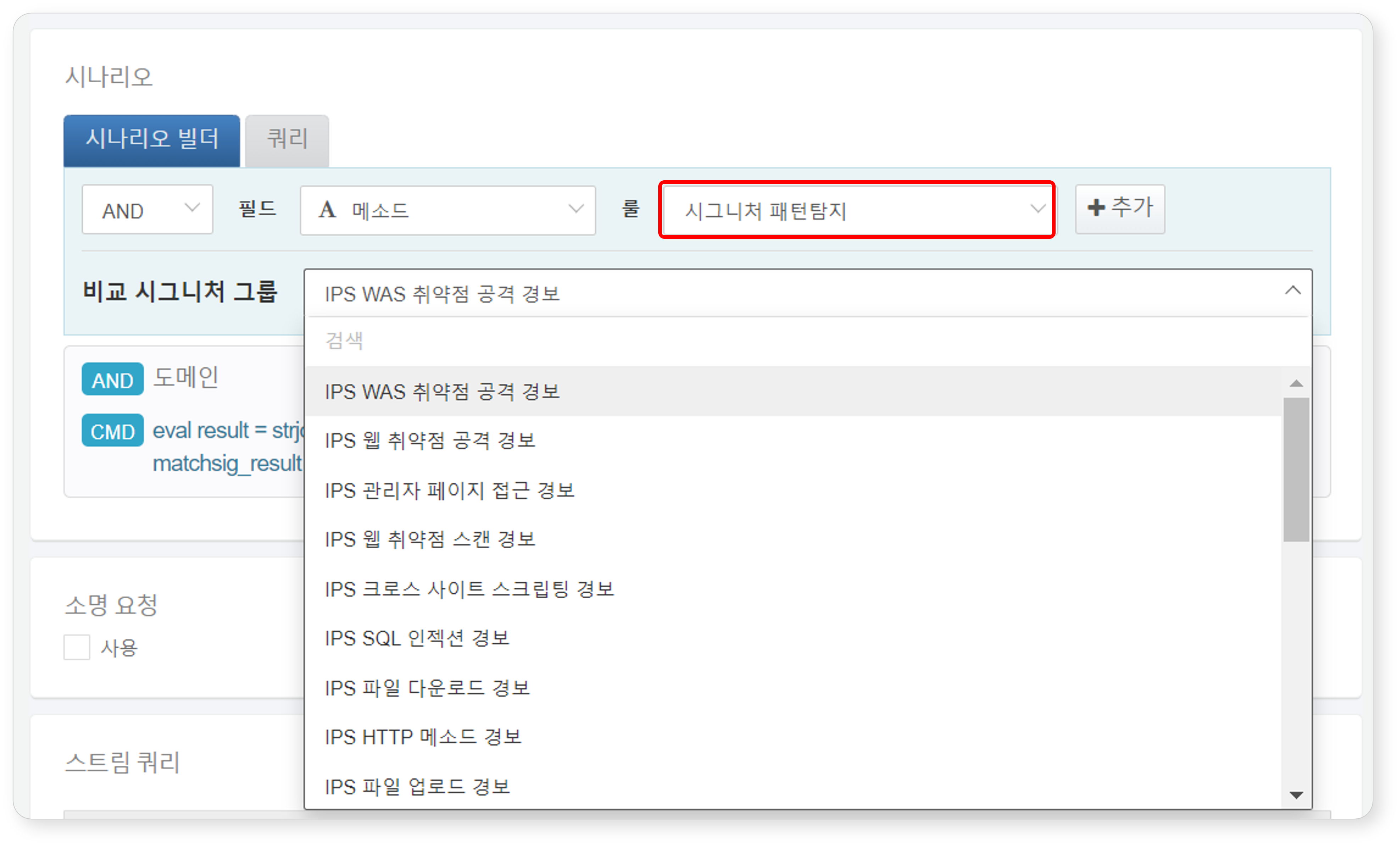
In the **Delete Pattern** dialog, review the list of patterns to be deleted and click **Delete**. Click **Cancel** if you do not wish to delete.

#### Utilizing Pattern Groups

Pattern Groups can be used in the following ways:

Scenario Builder

In **Policies > Real-Time Detection**, you can utilize pattern groups when adding or modifying detection scenarios using the Scenario Builder.



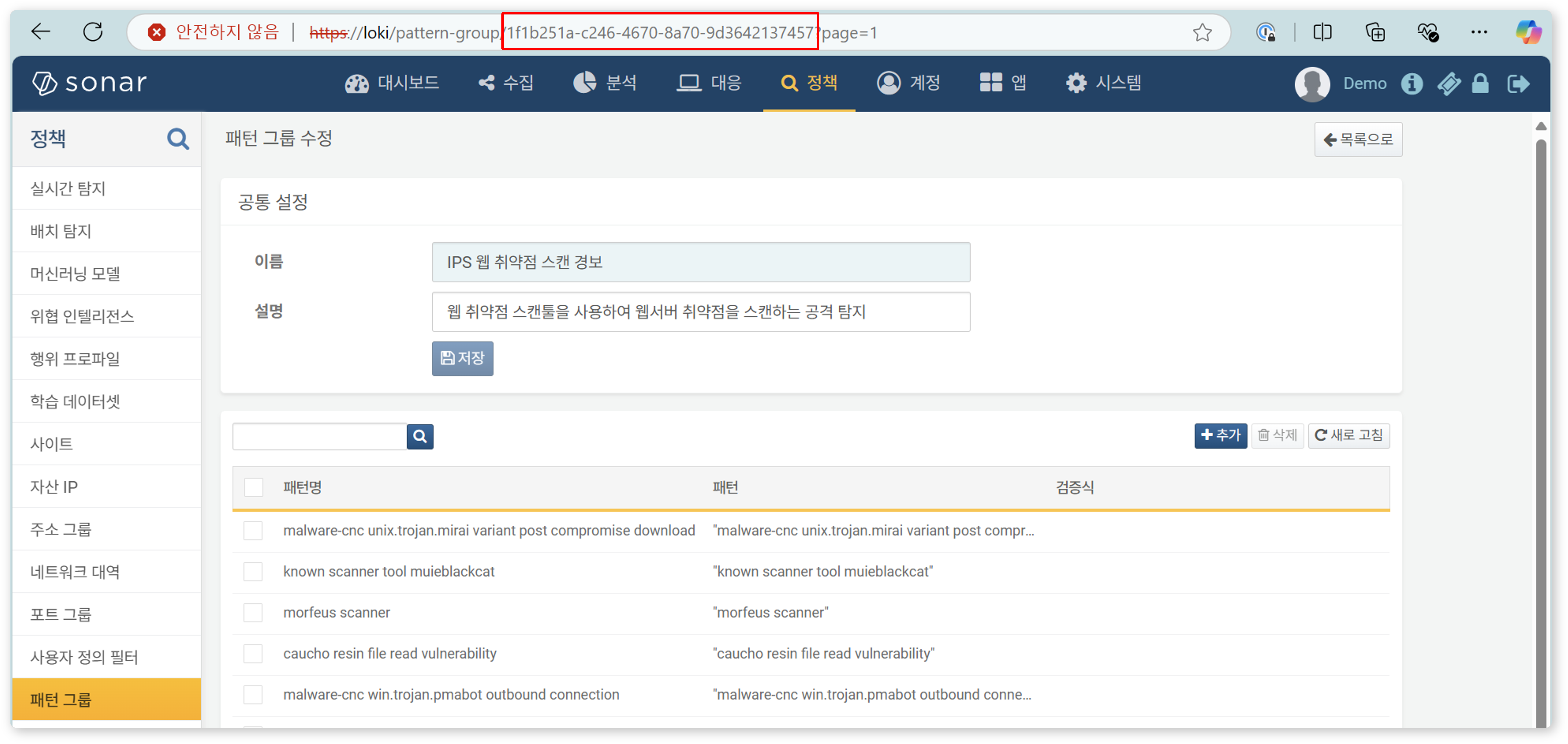
The following summarizes the pattern group-related content that can be used when the input field type is **STRING** in the Scenario Builder. For more details, refer to [Rules and Parameters by Field Type](https://docs.logpresso.comnull).

|  |  |  |  |
| --- | --- | --- | --- |
| Rule | Parameter | Input Range | Description |
| Signature Pattern Detection | Comparison Signature Group | Select Signature Group | Filters field values that match the signature |

Query

You can utilize pattern groups when adding or modifying detection scenarios in **Policies > Real-Time Detection** or **Policies > Batch Detection** using the [matchsig](https://docs.logpresso.comnull) command or the [matchsig()](https://docs.logpresso.comnull) function. Remember that you can use pattern groups wherever you can input query statements.

To use the mstchsig command or mstchsig() function, you need to know the GUID of the pattern group. The GUID can be found in the address bar of your web browser.



#### Deleting a Pattern Group

To delete a pattern group:

Select the checkbox of the pattern group row you wish to delete in the pattern group list.

Click **Delete** in the toolbar.

In the **Delete Pattern Group** dialog, review the list of pattern groups to be deleted and click **Delete**. Click **Cancel** if you do not wish to delete.

Be cautious when deleting a pattern group referenced in real-time detection or batch detection scenarios, as it may cause the detection scenarios to not function as intended.