### Real-Time Detection

#### Overview

Real-time detection scenarios are used to perform immediate detection by correlating data collected in real-time based on patterns or conditions. For example, high-risk attacks can be detected based on specific patterns in IPS logs, or data leaks can be identified when outbound traffic exceeds a certain threshold. This corresponds to methods for threat and anomaly detection.

The following illustration depicts the operation of real-time detection scenarios. Real-time detection scenarios are applied to normalized data during the collection phase. When creating a real-time detection scenario, ensure to use the normalized field names defined by the [Log Schema](https://docs.logpresso.comnull).



Real-time detection scenarios primarily perform the following actions:

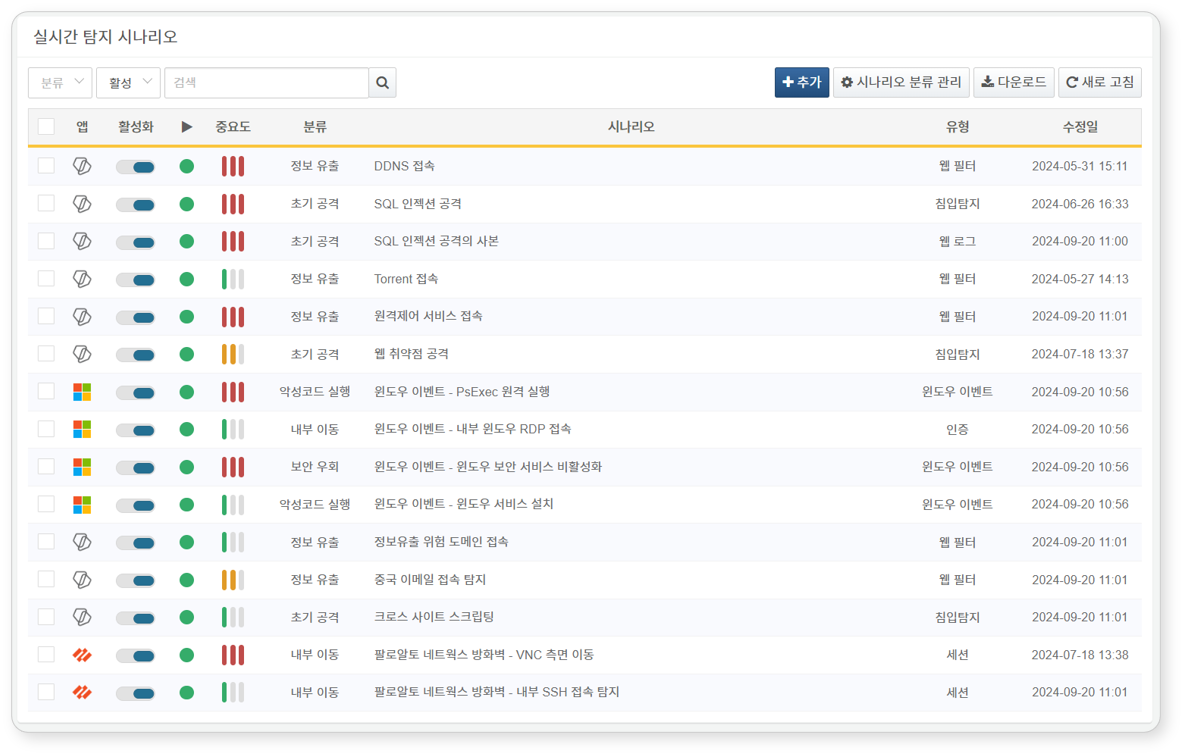
* Event Detection: Comparison of detection libraries with normalized field values
* Response Actions
* Issuing tickets and sending alerts for detected events
* Requesting explanations if the event's subject is an employee
* Registering the IP addresses related to the event in address groups
* Sending commands to integrated devices to block the corresponding traffic if necessary
* Executing playbooks

Executing playbooks is not a direct response action performed within the real-time detection scenario. However, if a playbook is created with the detection scenario specified as a trigger, response actions will be automatically executed according to the playbook upon event detection.

In most cases, real-time detection scenarios issue tickets or request explanations from event actors upon event detection. Excessive ticket issuance can increase the workload of malware analysts or security monitoring personnel, so it is necessary to minimize duplicate ticket issuance. Logpresso Sonar provides functionality to handle identical events as a single ticket based on the alert message and ticket title used during event detection, or based on duplicate criteria fields.

#### Viewing/Search Real-Time Detection Scenario List

You can view or search the list of real-time detection scenarios under **Policy > Real-Time Detection**.



* **App**: App icon related to the detection scenario. Default scenarios or user-added scenarios are represented by the Logpresso icon, while scenarios from installed apps are displayed with the respective app icon.
* **Activation**: Toggle button for activating the detection scenario (: Activated, : Deactivated)
* **Status**: Status of the detection scenario based on activation settings (**Green**: Activated, **Gray**: Deactivated)
* **Importance**: Importance of the detection scenario (High/Medium/Low)
* **Classification**: Classification information applied to the scenario
* **Scenario**: Name of the detection scenario
* **Type**: Information on the [Log Schema](https://docs.logpresso.comnull) set for the detection scenario
* **Modification Date**: Date when the detection scenario was last modified (or created)

To find a specific real-time detection scenario in the list, use the search tool in the toolbar. The search tool will display real-time detection scenarios that include the entered word in the **Name**, **Description**, or **Stream Query** fields. The search tool is case-insensitive.

Activating/Deactivating Scenarios

To activate or deactivate a real-time detection scenario, click the toggle button in the activation column of the detection scenario (: Activated, : Deactivated).

Downloading the List

To save the list of real-time detection scenarios to your local PC, click **Download** in the toolbar and select the desired file format for download.

Refreshing the List

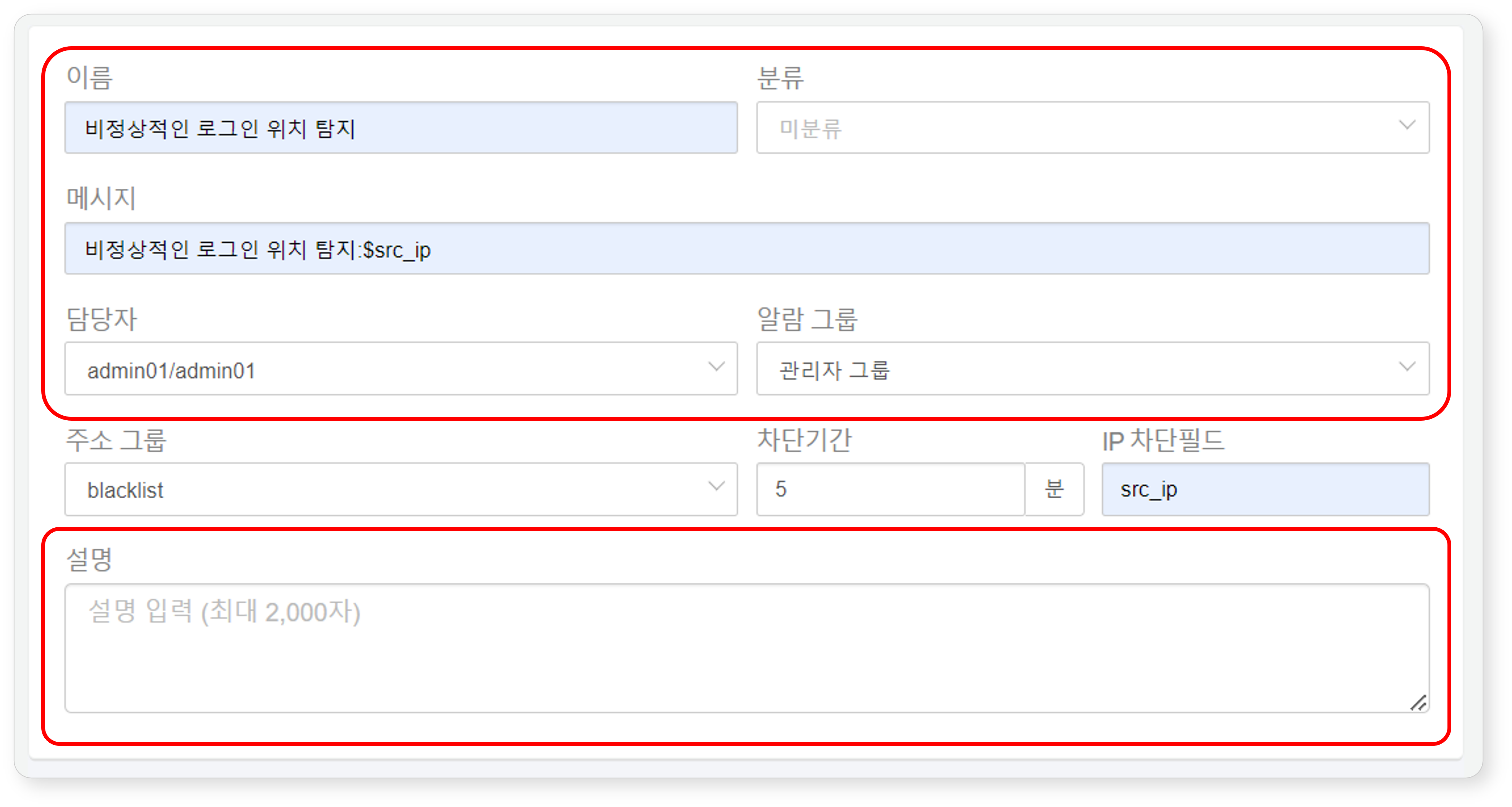
To refresh the list of real-time detection scenarios with the latest information, click **Refresh** in the toolbar.

#### Adding a Real-Time Detection Scenario

To add a real-time detection scenario:

Click **Add** in the toolbar under **Policy > Real-Time Detection**.

In the **Add Real-Time Detection Scenario** screen, configure the basic settings.



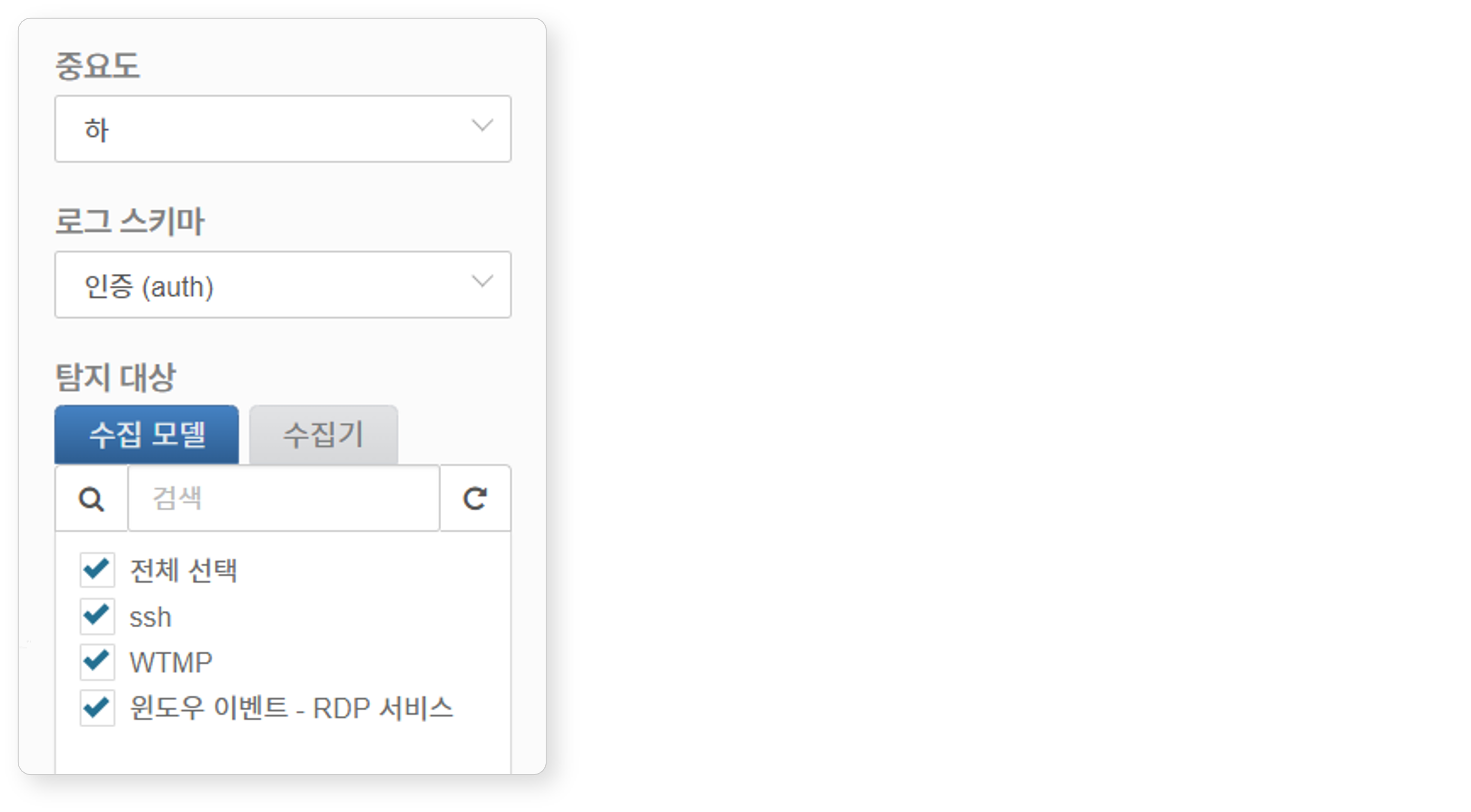
* **Name**: Unique name for the detection scenario (up to 50 characters). The name cannot be duplicated with other scenarios.
* **Classification**: Classification of the detection scenario. The classification will be displayed as **Classification** in the detection status list under **Analysis > Event Summary**. You can add or manage scenario classifications by clicking **Scenario Classification Management** in the toolbar. If not classified, no tickets will be generated.
* **Message**: Title to be assigned to the ticket upon event detection.
* Enter field names defined in the [Log Schema](https://docs.logpresso.comnull) in the format $FieldName or $FieldName$ to generate messages using field values from the logs that served as the basis for event detection (e.g., $src\_ip). If the field name contains Korean characters, be sure to use the $FieldName$ format.
* If the **Duplicate Criteria Field** is not set in **Advanced Settings**, duplicate tickets will be prevented based on the similarity of the generated message (up to 2,000 characters).
* **Assignee**: [Users](https://docs.logpresso.comnull) to whom the issued tickets will be assigned. You can select one or more accounts. If not specified, tickets will be created without an assignee.
* **Alarm Group**: [Alarm Group](https://docs.logpresso.comnull) that will receive alerts upon event detection.
* Choose the method of receiving alerts in the alarm group.
* **Description**: Detailed description of the detection scenario (up to 2,000 characters).

To manage the attacker's IP address or anomalous actor's IP address separately during event detection, or to relay address group information to firewalls, IPS, etc., configure the following items.



* **Address Group**: [Address Group](https://docs.logpresso.comnull) to which the value (IP address) of the field designated as the **IP Block Field** will be added.
* **Block Duration**: Duration (in minutes) for which the IP address added to the **Address Group** will be retained. If the specified block duration elapses, the IP address will be automatically deleted from the address group. If not specified, it will be retained permanently in the address group (range: 1-100,000,000).
* **IP Block Field**: Field name of the IP address to be added to the address group during event detection. Enter the names of IP address-related fields defined in the log schema (e.g., src\_ip, dst\_ip) (up to 50 characters).
* For settings related to blocking integration with third-party information protection systems, refer to 'System > Response Targets'.

Set the importance of detected events and the collection model or logger to which the real-time detection scenario will be applied.



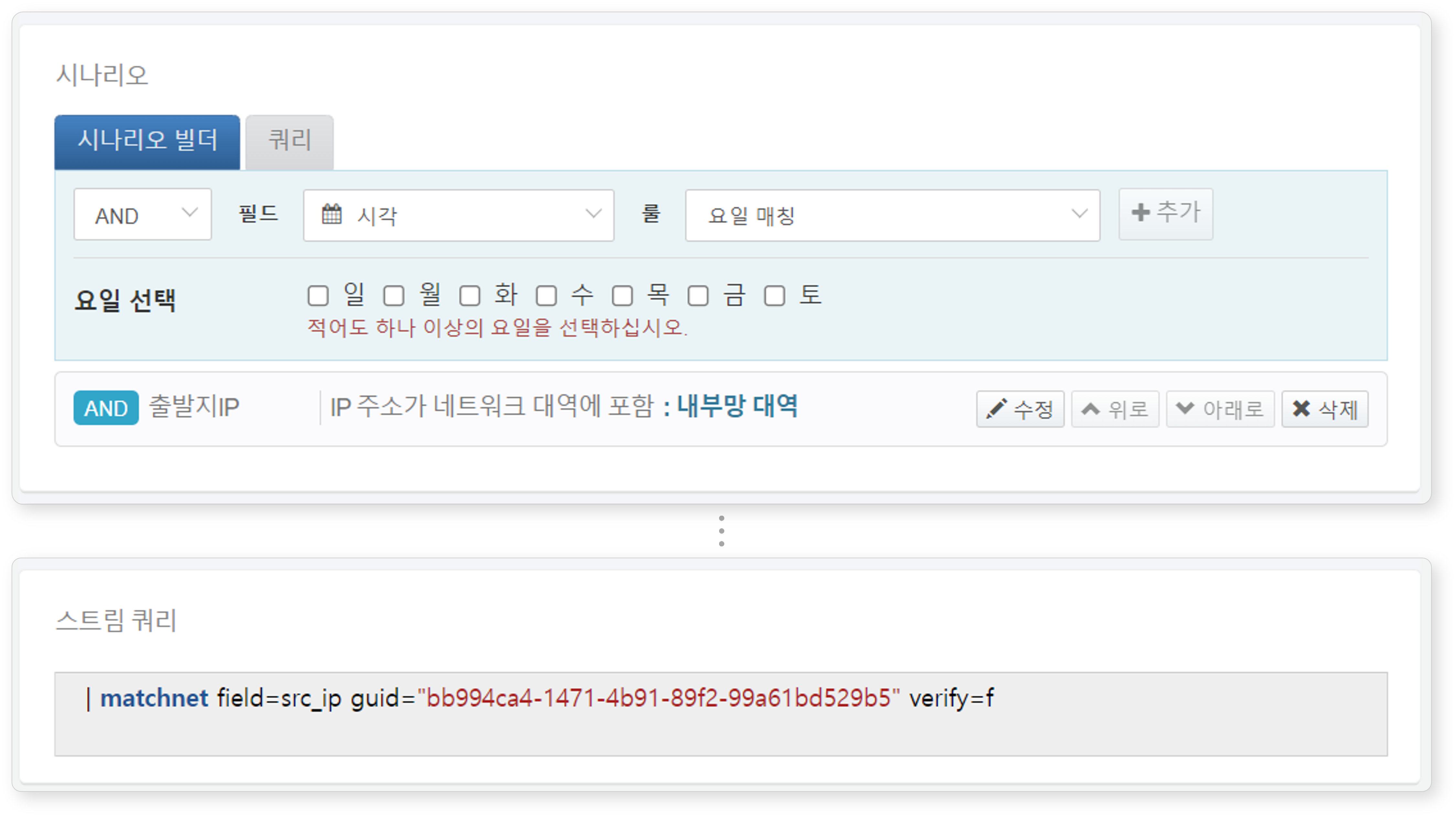
* **Importance**: Importance of the detected event (High, Medium, Low)
* **Log Schema**: Select the log schema to be applied to the detection scenario. The items available in the scenario builder will be determined by the log schema.
* **Detection Target**: Select the data collection model or logger to which the detection scenario will be applied from the list. You cannot select both a collection model and a logger simultaneously. Choose either a collection model or a logger. The detection target list will only show collection models and loggers that reference the selected **Log Schema**.

If the collection model only has "Original" normalization rules, it will not appear in the detection target list as there are no referenced log schemas. Ensure to define normalization rules that reference the log schema when setting up the collection model.

Create the threat detection scenario. You can use the **Scenario Builder** or directly input query statements in the **Query** field to create the detection scenario. For detailed explanations of the scenario builder, refer to [Rules and Parameters by Field Type](https://docs.logpresso.comnull).

A scenario consists of at least one rule, and the rules are applied in the order they appear in the list. When data is collected through the **Detection Target** selected in step 4, comparisons will be performed in the order of the rules. The subsequent rule will only execute if the preceding rule is satisfied. The order of rule execution can impact system performance, so it is advisable to set simple and quick conditions in the upper rules to filter out unrelated logs as much as possible.

If you input an incorrect or unexecutable query statement (e.g., specifying a non-existent address group or pattern group), you will not be able to add detection rules.



* **Scenario Builder**: An editor for detection rules consisting of **Conditions**, **Fields**, and **Rules**. After selecting all rules, click **Add** to register the rules in the rule list. You can register more than one rule.
* **Condition**: Condition for applying the rule (AND, NOT, default: AND). The next rule will be applied when the result of the data and rule comparison is true.
* **AND**: True if matched
* **NOT**: True if not matched
* **Field**: Field defined in the log schema to be compared with the **Rule**.
* **Rule**: Rule to be applied to the **Field**. The appropriate rule list will be displayed based on the **Field**.
* **Query**: Input the query statement (up to 10,000 characters) to directly add filter rules.
* **Stream Query**: Displays the filter rules input in the **Scenario Builder** or **Query** as a stream query statement.

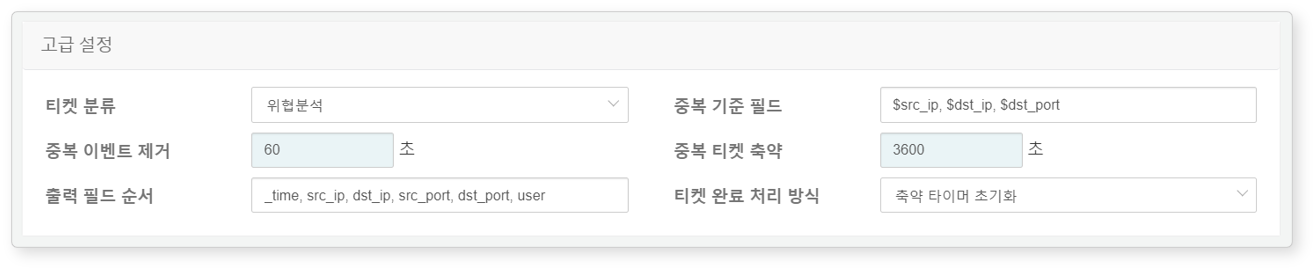
If the detected event is related to employees in the organization, you can request explanations from the respective employees.



* **Explanation Request**: Whether to use explanation requests (default: disabled).
* **Explanation Target Field**: Field containing the employee ID information of the explanation target.
* When a threat is detected, an automatic explanation request email will be sent to the employee mapped to that employee ID. In this case, employee information (employee ID, account, email) must be configured in **Policy > Employees**.
* **Classification**: Classification of the explanation. If necessary, click **Response > Explanations** and then **Manage Explanation Classifications** to add settings.
* **Secondary Reviewer**: Secondary reviewer for the explanation (if not set, defaults to "Department Head"). For information on primary and secondary reviewers, refer to [Explanations](https://docs.logpresso.comnull).
* **Deadline**: Deadline for processing the explanation (default: 7 days). Once the deadline has passed, the explanation target cannot submit an explanation.
* **Remarks**: Additional content to be included in the explanation request email. The entered content will be inserted at the position of the text macro $user\_note in the email/SMS template body. If you input field names defined in the schema in the macro format $FieldName, they will be replaced with field values. You can check the remarks in the detailed explanation content under **Response > Explanations** (up to 10,000 characters).

To request an explanation, a field named "emp\_key" is required. If this field is not present, click on the query in step 5, create the emp\_key field, and write a query statement that can map it to user accounts or IP addresses.

To issue a ticket upon event detection, configure the **Advanced Settings** items.



* **Ticket Classification**: [Ticket Classification](https://docs.logpresso.comnull) necessary for distinguishing tickets during security monitoring operations (default: not selected).
* To ensure that tickets are automatically generated upon event detection, you must specify a ticket classification. The ticket generation can also be determined by playbooks that operate based on events. Do not use this item if you want to determine ticket generation in the playbook.
* **Duplicate Criteria Field**: Enter the name of the field to be used as the basis for ticket duplication checks in macro format like $FieldName, separated by commas (range: up to 2,000 characters). If not set, it will be judged based on the **Message** string.
* For example, if the message item is set to "C&C server access: $src\_ip -> $dst\_ip" but you want to avoid generating multiple events or tickets for accessing different C&C servers from the same host, set the duplication criteria key to '$src\_ip'.
* **Ignore Duplicate Events**: Duration (default: 0, range: 0 to 86,400 seconds) to ignore duplicate events when the same event occurs consecutively after ticket issuance.
* When "0": Operates according to the **Duplicate Ticket Reduction** setting.
* When not "0": Ignores the same event for the specified duration and does not use it as supporting material for that ticket.
* **Duplicate Ticket Reduction**: Duration (default: 3,600, range: 0 to 86,400 seconds) during which, if the same event occurs after ticket issuance, it will not issue a new ticket but will only add supporting material and occurrence count to the already issued ticket.
* When "0": A new ticket is created every time the event occurs with the same title.
* When not "0": Records supporting material and occurrence count in the existing ticket for the specified duration.
* **Output Field Order**: Order of log data fields to be displayed in the supporting material of the ticket. Enter field names in the order they should be displayed, separated by commas (range: up to 2,000 characters; excluding special characters and pipe symbols).
* **Ticket Completion Handling Method**: Setting for how to handle tickets with **Duplicate Ticket Reduction** after they are completed (default: reset reduction timer).
* **Maintain Reduction Timer**: Even if the ticket is completed, if the same threat event occurs before the duplicate ticket reduction time expires, it will record supporting material and occurrence count in the completed ticket.
* **Reset Reduction Timer**: When the ticket is completed, it will be considered that the duplicate ticket reduction time has also expired, and a new ticket will be issued if the same threat event occurs.

Click **Confirm** to complete adding the real-time detection scenario. The real-time detection scenario will be activated immediately upon addition.

Rules and Parameters by Field Type

The scenario builder allows you to set rule items based on field types from the [Log Schema](https://docs.logpresso.comnull). The rules and parameters available in the scenario builder depend on the data type of the field, as follows:

**STRING**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rule | Parameter | Input Range | Load | Description |
| Matches Target String | Comparison String | Up to 255 characters | Low | Filters field values using the comparison string |
| Contains Target String | Containing String | Up to 255 characters | Low | Filters field values that contain the string |
| Signature Pattern Detection | Comparison Signature Group | Select Signature Group | Medium | Filters field values using signatures |

**BOOL**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rule | Parameter | Input Range | Load | Description |
| True or False | Comparison | Select True or False | Low | Filters field values that are true/false |

**SHORT/INT/LONG/DOUBLE**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rule | Parameter | Input Range | Load | Description |
| Matches Target Value | Comparison Value | -9007199254740991 to 9007199254740991 | Low | Filters fields with matching values |
| Value Range | Start, End | -9007199254740991 to 9007199254740991 | Low | Filters field values within the range |
| Greater Than Target Value | Comparison Value | -9007199254740991 to 9007199254740991 | Low | Filters field values greater than the value |
| Greater Than or Equal To Target Value | Comparison Value | -9007199254740991 to 9007199254740991 | Low | Filters field values greater than or equal to the value |
| Less Than Target Value | Comparison Value | -9007199254740991 to 9007199254740991 | Low | Filters field values less than the value |
| Less Than or Equal To Target Value | Comparison Value | -9007199254740991 to 9007199254740991 | Low | Filters field values less than or equal to the value |

**DATE**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rule | Parameter | Input Range | Load | Description |
| Day Matching | Day Selection | Multiple selection of Sun/Mon/Tue/Wed/Thu/Fri/Sat | Low | Filters data generated on specified days |
| Weekend Matching | - | - | Low | Filters data generated on weekends |
| Weekday Matching | - | - | Low | Filters data generated on weekdays |
| Time Range | Start Time, End Time | 0 to 23 hours | Low | Filters data generated during specified hours |

**COUNTRY**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rule | Parameter | Input Range | Load | Description |
| Matches Country Code | Comparison Country Code | Select Country | Low | Filters field values matching the country code |

**PORT**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rule | Parameter | Input Range | Load | Description |
| Matches Port Number | Comparison Port | 0 to 65535 | Low | Filters field values matching the port number |
| Included in Port Group | Comparison Port Group | Select Port Group | Low | Filters field values included in the port group |

**IP**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rule | Parameter | Input Range | Load | Description |
| Matches IP Address | Comparison IP | IPv4 format address | Low | Filters field values matching the comparison IP |
| Included in Network Range | Comparison Network Range | Select Network Range | Low | Filters field values included in the network range |
| Included in Address Group | Comparison Address Group | Select Address Group | Low | Filters |