Correlation Analysis Process

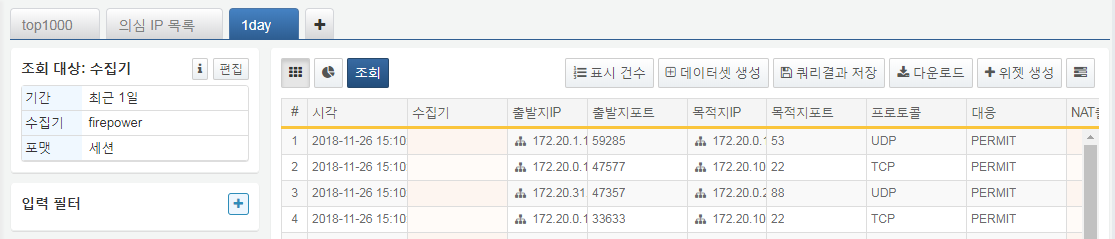
Stage 1

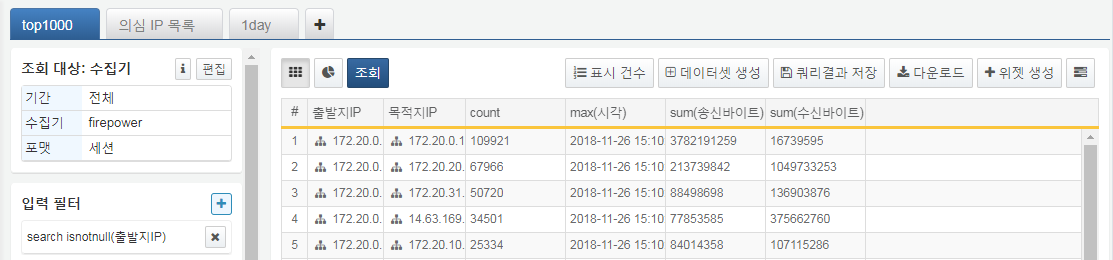
Data Preparation

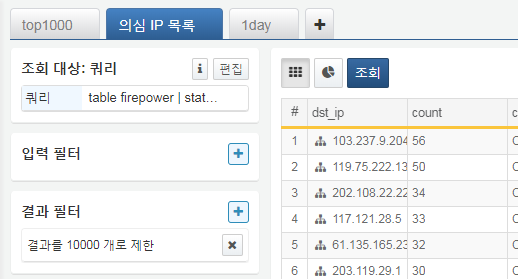
To conduct correlation analysis, at least two tabs must be opened in the pivot view, and data for analysis should be prepared in each tab. If necessary, the tab name can be changed or the tab can be deleted by clicking the button on the right side of the tab.

In the example below, three tabs have been prepared:

* **1day tab**: Firewall data entered in the last day (data for analysis)
* **top1000 tab**: The top 1000 source IP-destination IP pairs with the highest network traffic (comparison data 1)
* **Suspicious IP List tab**: A list of suspected IPs (comparison data 2)





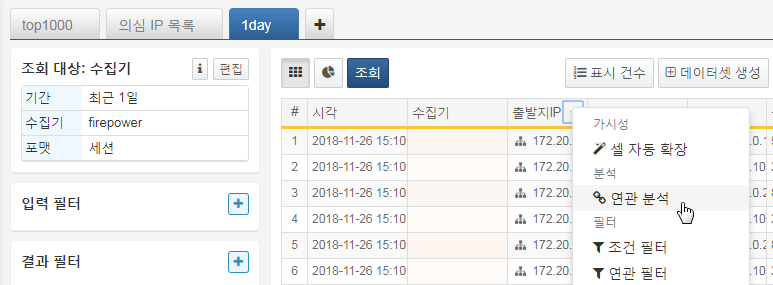


Stage 2

Adding Correlation Analysis

To proceed with correlation analysis, click on the column header in the data results window and select the correlation analysis menu.

In this example, correlation analysis is conducted on the source IP in the 1day tab.

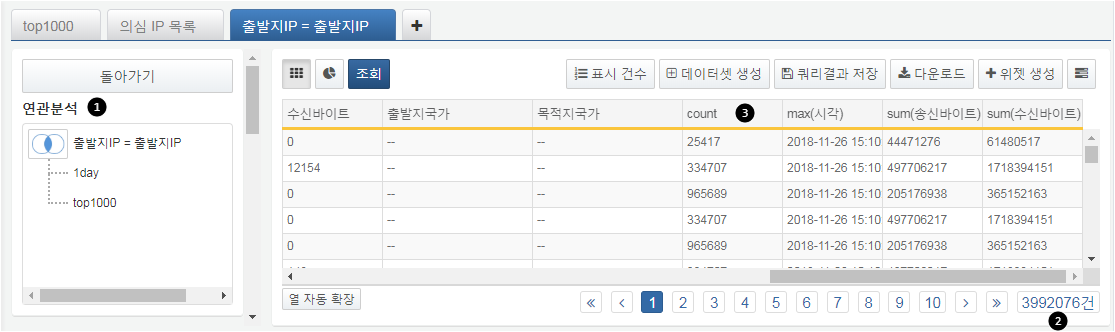


In the correlation analysis menu, settings for the correlation analysis can be entered.

In this example, a correlation analysis is added using the source IP field from the top1000 tab with an Inner join type.



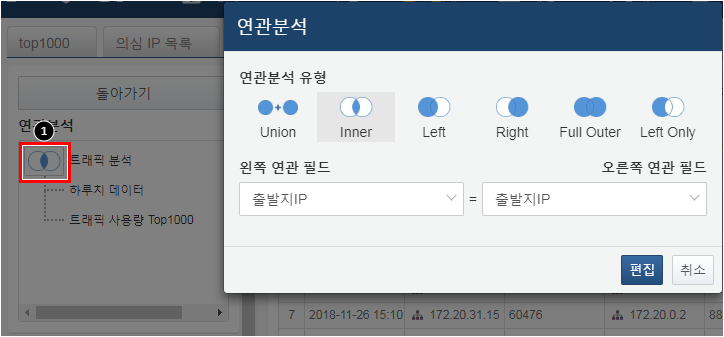
When adding correlation analysis with the above conditions, the screen changes as follows. First, the query target menu in the upper left changes to the correlation analysis menu (1), and the current correlation analysis information is displayed. Since an Inner join was performed, only the mapped data is output, resulting in a reduced output count (2). Additionally, new columns that did not previously exist, such as count, sum (sent bytes), and sum (received bytes) (3), have been added.



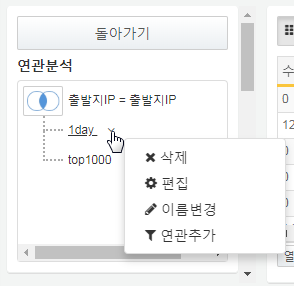
Stage 3

Modifying Correlation Analysis

In the correlation analysis menu, clicking on the correlation analysis type (Venn diagram icon 1) allows for changes to the correlation analysis type and correlation fields.



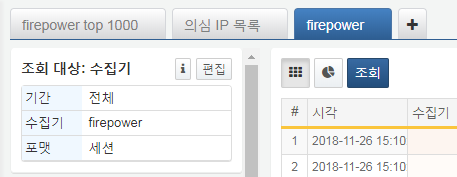
When clicking on the correlation analysis or tab in the correlation analysis menu, a context menu appears. Clicking on each tab will display options for delete, edit, rename, and add correlation, while clicking on the correlation analysis name will show options for delete, rename, and add correlation.



* **Delete**: Deletes the selected tab or correlation analysis. Upon deletion, it reverts to the state prior to the application of the correlation analysis.
* **Edit**: Edits the data in the selected tab. Modifications can be made to the data source, filters, aggregations, etc.
* **Rename**: Changes the name displayed in the correlation analysis menu.
* **Add Correlation**: Adds a new correlation analysis.

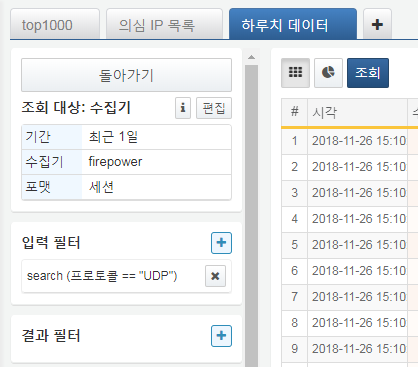
**Delete**

When a correlation analysis is deleted, that specific correlation analysis is removed. If a tab is deleted, any correlation analyses using that tab will also be deleted.



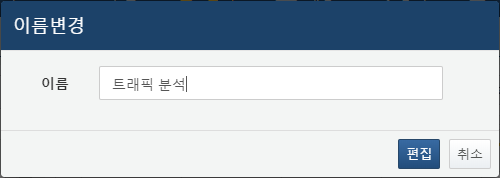
**Edit**

Selecting edit allows you to enter the corresponding data tab and modify the settings. You can change the data type and query period, adjust filter settings, or modify aggregation fields. Once editing is complete, press the Back button to return to the correlation analysis screen.

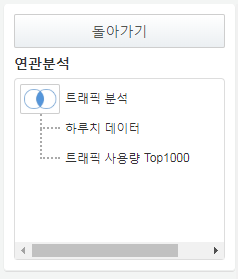


**Rename**

You can rename the correlation analysis and data tab to facilitate data analysis tasks. Clicking rename will bring up a rename window as shown below.



Enter the new name and press the edit button to apply the name in the correlation analysis screen.



**Add Correlation**

You can add correlation analysis. In the add correlation analysis window, set the tab to be used, the correlation analysis type, and the correlation fields. For more details, refer to the next stage, **Applying Additional Correlation Analysis**.



Stage 4

Applying Additional Correlation Analysis

Correlation analysis can be continuously applied. After a correlation analysis has been applied, if you wish to apply another correlation analysis, you can click on the column header as in Stage 2 to add correlation analysis from the context menu, or use the add correlation option from the correlation analysis context menu in Stage 3.

In the example below, an additional correlation analysis is added to the destination IP field in the 1day tab, mapping it to the dst\_ip field in the Suspicious IP List tab.



When a correlation analysis is added, the newly added correlation analysis will be displayed on the correlation analysis screen as shown below.

