

## Email LOGS

1. Identify external email addresses that have sent emails to CNL users in the last 15 minutes.

```
index="msexchange" sourcetype="MSExchange:2013:MessageTracking" sender!=*company_email* | table sender | dedup sender
```

The screenshot shows the Splunk Enterprise interface. The search bar contains the query: `index="msexchange" sourcetype="MSExchange:2013:MessageTracking" sender!=*cybernowlabs.com|table sender|dedup sender`. The search is filtered for the last 15 minutes. The results show 373 events. The 'Statistics' tab is selected, showing 26 statistics. The 'sender' field is highlighted in the table view.

2. Identify external email addresses that have sent emails to more than one CNL user in the last 15 minutes.

```
index="msexchange" sourcetype="MSExchange:2013:MessageTracking" sender!=*cybernowlabs.com| stats dc(recipient) as gelen by sender | where gelen > 1
```

The screenshot shows the Splunk Enterprise interface. The search bar contains the query: `index="msexchange" sourcetype="MSExchange:2013:MessageTracking" sender!=*cybernowlabs.com| stats dc(recipient) as gelen by sender | where gelen > 1`. The search is filtered for the last 15 minutes. The results show 108 events. The 'Statistics' tab is selected, showing 5 statistics. The 'sender' and 'gelen' fields are highlighted in the table view.

3. Identify external email addresses and email subjects that have sent emails to more than one CNL user in the last 15 minutes.

```
index="msexchange" sourcetype="MSExchange:2013:MessageTracking" sender!=*cybernowlabs.com| stats dc(recipient) as gelen by sender message_subject | where gelen > 1 |table sender message_subject
```

splunk>enterprise

Apps

Haydar Akyurek

998 Messages

Settings

Activity

Help

Find

Search

Analytics

Datasets

Reports

Alerts

Dashboards

Search & Reporting

New Search

Save As

Create Table View

Close

index="msexchange" sourcetype="MSExchange:2013:MessageTracking" sender!=""cybernowlabs.com" stats dc(recipient) as gelen by sender message\_subject | where gelen > 1 |table sender message\_subject

Last 15 minutes

Q

108 events (10/6/25 10:10:56.000 AM to 10/6/25 10:25:56.000 AM)

No Event Sampling

Job

II

Smart Mode

Events

Patterns

Statistics (5)

Visualization

20 Per Page

Format

Preview

sender

message\_subject