

Windows LOGS

1. List the users and external IP addresses that have failed to log in to the Exchange machine security logs in the last 15 minutes.

index="wineventlog" EventCode=4625 Host=CNLEX01

| stats values(src_ip) count by user

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `index="wineventlog" EventCode=4625 Host=CNLEX01 | stats values(src_ip) count by user`. The time range is set to "Last 15 minutes". The search results show 0 events for the time range 10/6/25 10:22:37.000 AM to 10/6/25 10:37:37.000 AM. The interface includes tabs for Search, Analytics, Datasets, Reports, Alerts, and Dashboards. The search results are displayed in a table view with columns for Events, Patterns, Statistics (0), and Visualization. The message "No results found. Try expanding the time range." is visible at the bottom.

2. List users who have unsuccessfully logged in with more than one external IP address in the Exchange machine security logs in the last 15 minutes.

index="wineventlog" EventCode=4625 Host=CNLEX01

| stats dc(src_ip) as gelen values(src_ip) as ip_list by user

| where gelen > 1

| table user gelen ip_list

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `index="wineventlog" EventCode=4625 Host=CNLEX01 | stats dc(src_ip) as gelen values(src_ip) as ip_list by user | where gelen > 1 | table user gelen ip_list`. The time range is set to "Last 15 minutes". The search results show 0 events for the time range 10/6/25 10:24:34.000 AM to 10/6/25 10:39:34.000 AM. The interface includes tabs for Search, Analytics, Datasets, Reports, Alerts, and Dashboards. The search results are displayed in a table view with columns for Events, Patterns, Statistics (0), and Visualization. The message "No results found. Try expanding the time range." is visible at the bottom.

3. List successful and unsuccessful logins from the same user in the Windows security logs in the last 15 minutes.

index=wineventlog EventCode=4624 OR EventCode=4625 user!=*\$* | stats dc(user) by user

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `index=wineventlog EventCode=4624 OR EventCode=4625 user!=*$* | stats dc(user) by user`. The search is set to 'Last 15 minutes'. The results show 342 events. The interface includes a top navigation bar with 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. A 'New Search' section is visible with buttons for 'Save As', 'Create Table View', and 'Close'. The search results are displayed in a table with columns for 'user' and 'dc(user)'.

4. List users whose accounts have been locked in the Windows security logs in the last 24 hours.

index="wineventlog" EventCode=4740 | table user| dedup user

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `index="wineventlog" EventCode=4740 | table user| dedup user`. The search is set to 'Last 60 minutes'. The results show 4 events. The interface includes a top navigation bar with 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. A 'New Search' section is visible with buttons for 'Save As', 'Create Table View', and 'Close'. The search results are displayed in a table with columns for 'user' and 'dedup user'.