

NOTABLE LOGS

1) List notable events that occurred within 15 minutes.

index="notable"|table source severity | sort severity

splunk>enterpriseApps ▾Haydar Akyurek ▾998 Messages ▾Settings ▾Activity ▾Help ▾Find

SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

New Search

Save As ▾Create Table ViewClose

index="notable"|table source severity | sort severity

Last 15 minutes ▾

Q

✓ 3 events (10/8/25 9:33:20.000 AM to 10/8/25 9:48:20.000 AM)No Event Sampling ▾Job ▾▮▮▮▮▮Smart Mode ▾

EventsPatternsStatistics (3)Visualization

20 Per Page ▾FormatPreview ▾

source ▾	severity ▾
Risk - 24 Hour Risk Threshold Exceeded - Rule	critical
Risk - 24 Hour Risk Threshold Exceeded - Rule	medium
Access - Password Brute Forcing - Rule	

2) Identify notable events and their numbers within 15 minutes.

index=notable |stats count by search_name

splunk>enterpriseApps ▾Haydar Akyurek ▾998 Messages ▾Settings ▾Activity ▾Help ▾Find

SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

New Search

Save As ▾Create Table ViewClose

index=notable |stats count by search_name

Last 15 minutes ▾

Q

✓ 3 events (10/8/25 9:36:11.000 AM to 10/8/25 9:51:11.000 AM)No Event Sampling ▾Job ▾▮▮▮▮▮Smart Mode ▾

EventsPatternsStatistics (2)Visualization

20 Per Page ▾FormatPreview ▾

search_name ▾	count ▾
Access - Password Brute Forcing - Rule	1
Risk - 24 Hour Risk Threshold Exceeded - Rule	2

3) List the source IP addresses, categories, and requests involved in the "Unwanted DNS Request" event within 24 hours.

index="notable" source="Threat - Unwanted DNS Requests - Rule" | table request category src

splunk>enterpriseApps ▾Haydar Akyurek ▾998 Messages ▾Settings ▾Activity ▾Help ▾Find

SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

New Search

Save As ▾Create Table ViewClose

index="notable" source="Threat - Unwanted DNS Requests - Rule" | table request category src

Last 24 hours ▾

Q

✓ 4 events (10/7/25 9:00:00.000 AM to 10/8/25 9:53:29.000 AM)No Event Sampling ▾Job ▾▮▮▮▮▮Smart Mode ▾

EventsPatternsStatistics (4)Visualization

20 Per Page ▾FormatPreview ▾

request ▾	category ▾	src ▾
-----------	------------	-------

4) List the source and destination IP addresses involved in the "Remote Desktop Network Bruteforce" incident within 24 hours.

`index="notable" source="ESCU - Remote Desktop Network Bruteforce - Rule" | table dest src`

The screenshot shows the Splunk Enterprise interface. The search bar contains the query: `index="notable" source="ESCU - Remote Desktop Network Bruteforce - Rule" | table dest src`. The search results show 9 events from 10/7/25 9:00:00.000 AM to 10/8/25 9:57:01.000 AM. The search is in 'Statistics (9)' mode, showing 20 results per page. The table view shows columns for 'dest' and 'src'.

5) Identify source external IP addresses involved in more than 1 incident in 24 hours.

`index="notable" | stats dc(source) as olay values(source) as kurallar count by src_ip | where olay > 1`

The screenshot shows the Splunk Enterprise interface. The search bar contains the query: `index="notable" | stats dc(source) as olay values(source) as kurallar count by src_ip | where olay > 1`. The search results show 200 events from 10/7/25 9:00:00.000 AM to 10/8/25 9:58:48.000 AM. The search is in 'Statistics (2)' mode, showing 20 results per page. The table view shows columns for 'src_ip', 'olay', 'kurallar', and 'count'.