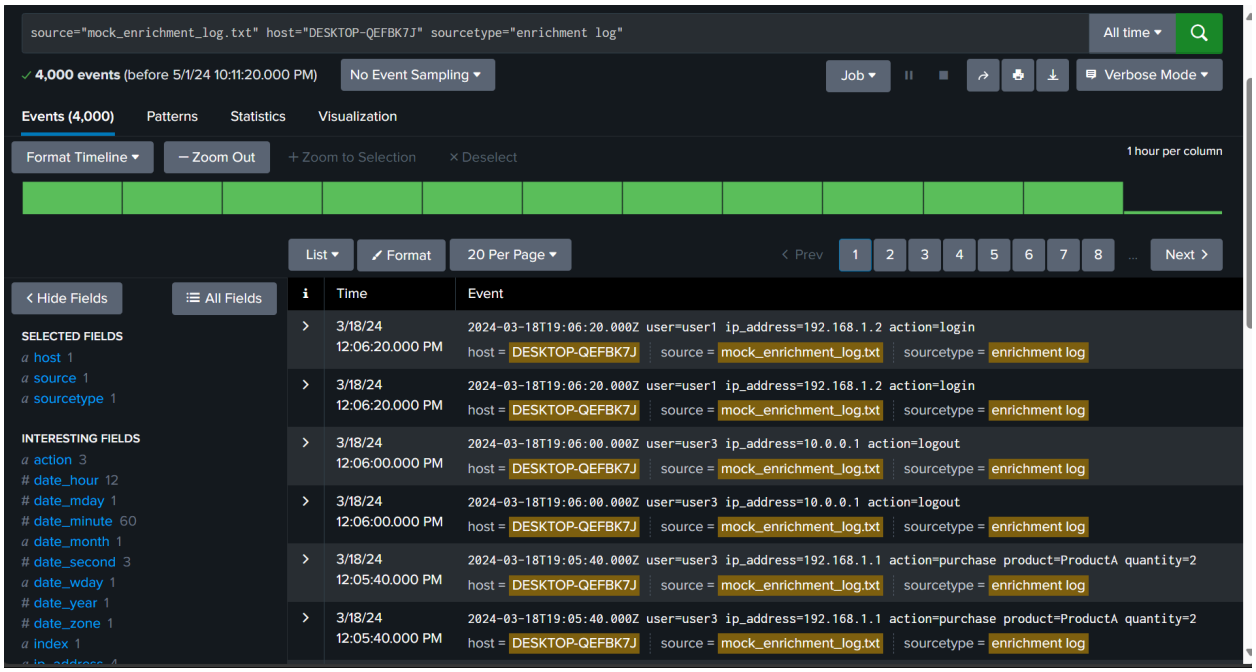
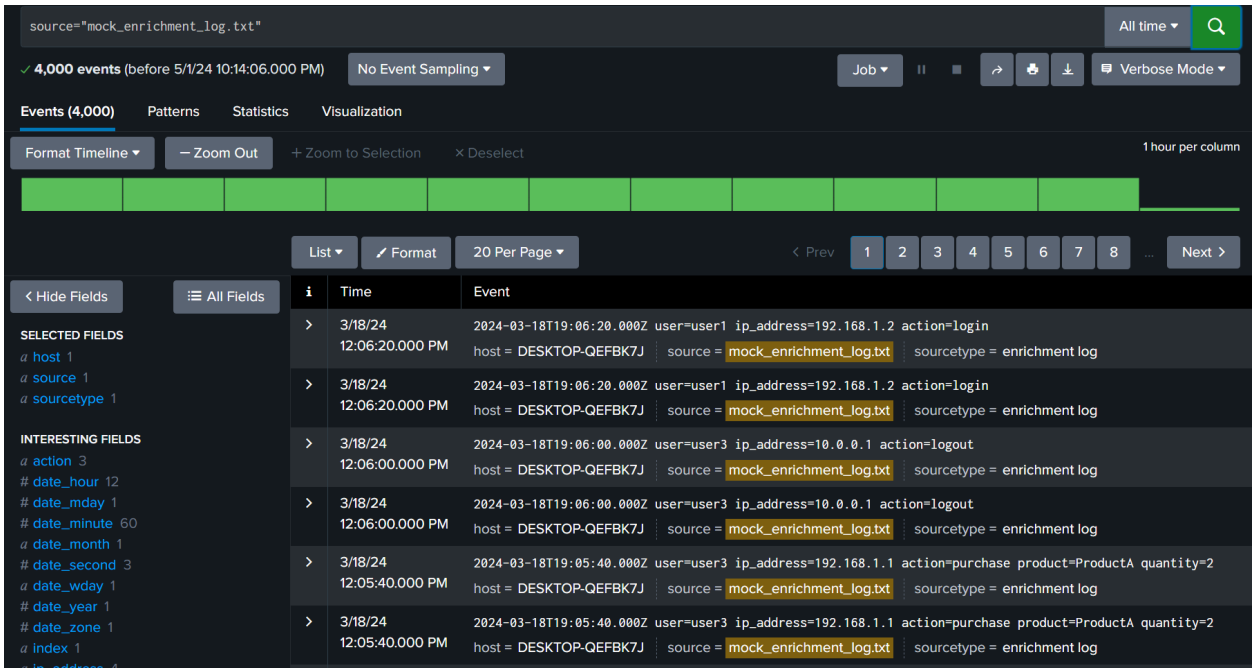
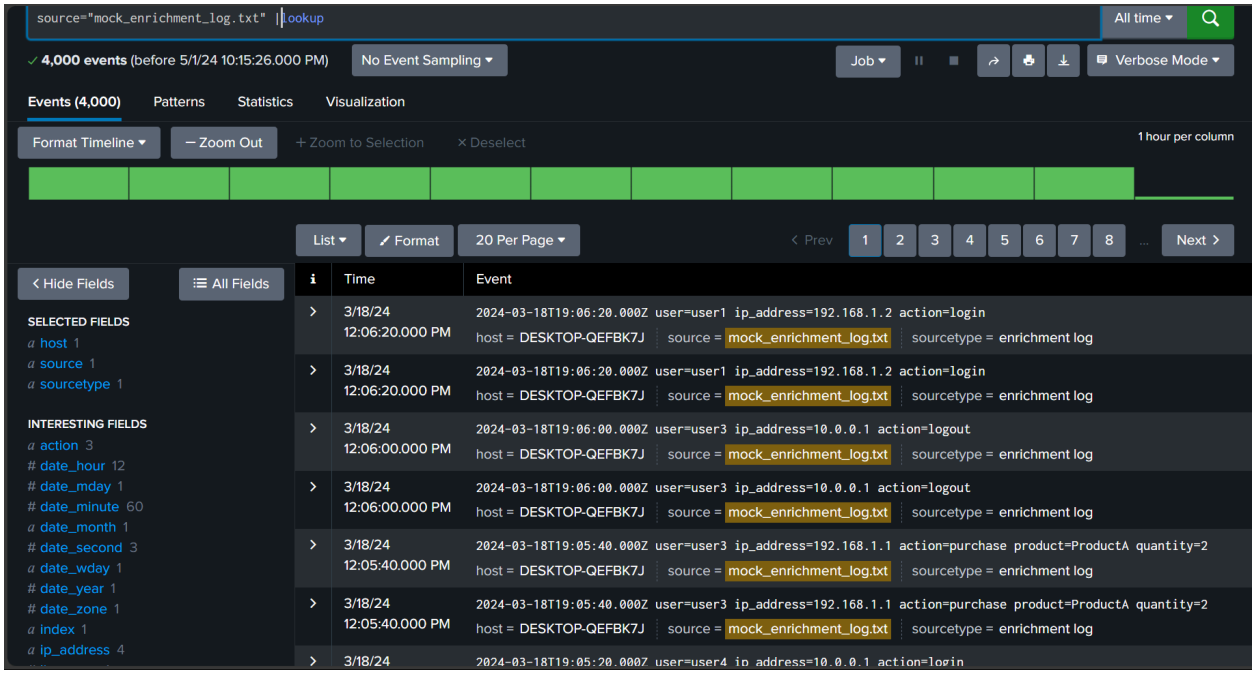
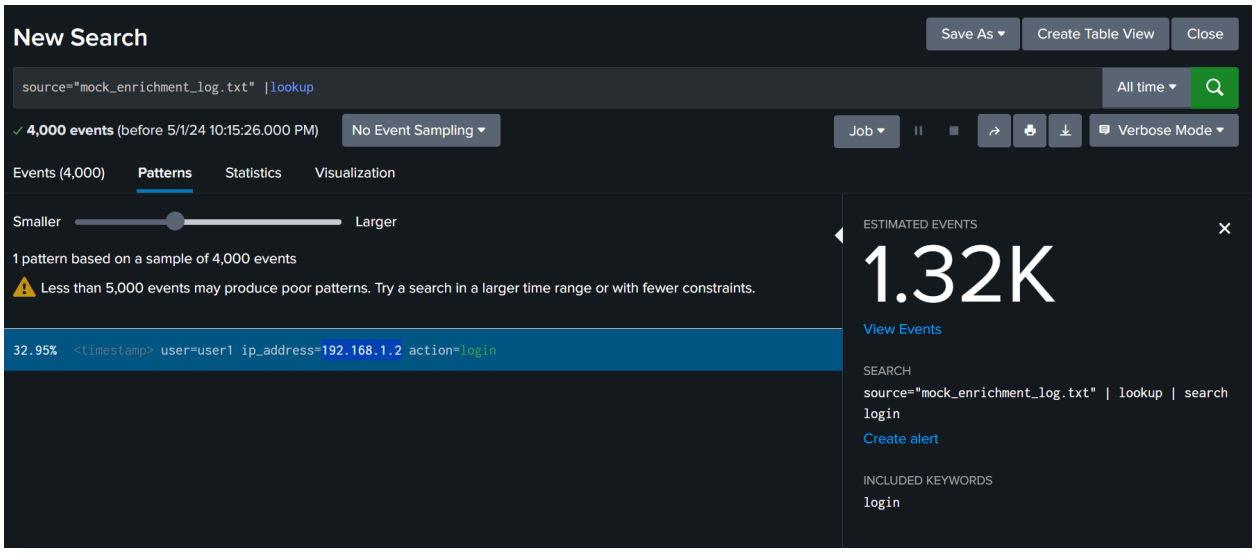
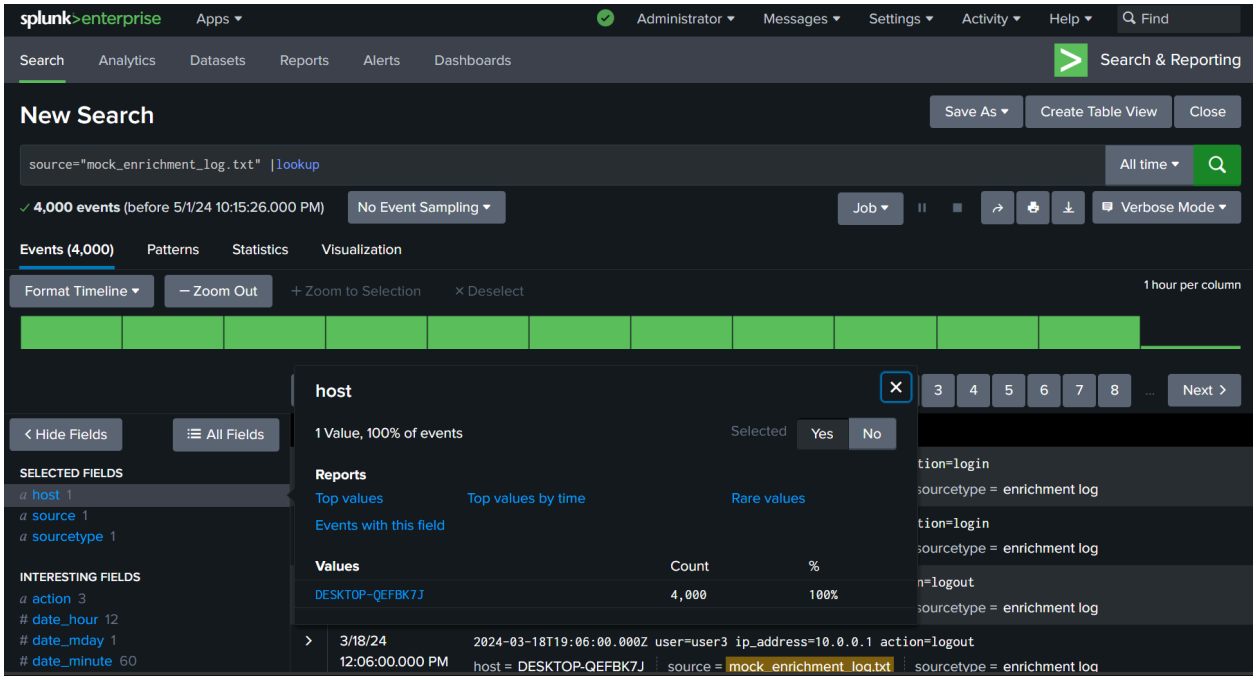
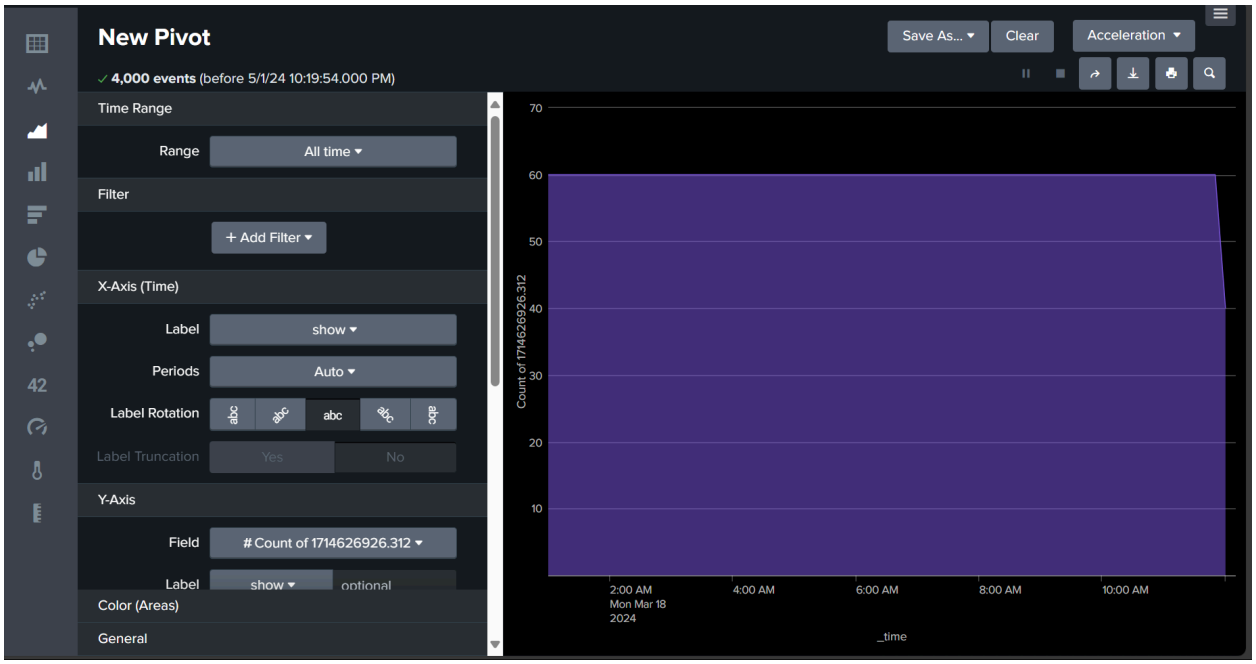

source="mock_enrichment_log.txt" host="DESKTOP-QEFBK7J" sourcetype="enrichment log"
All time
4,000 events (before 5/1/24 10:11:20.000 PM)
No Event Sampling
Job
Verbose Mode
Events (4,000)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
20 Per Page
Prev
1 2 3 4 5 6 7 8
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a action 3
date_hour 12
date_mday 1
date_minute 60
a date_month 1
date_second 3
a date_wday 1
date_year 1
date_zone 1
a index 1
Time
Event
3/18/24 12:06:20.000 PM
2024-03-18T19:06:20.000Z user=user1 ip_address=192.168.1.2 action=login
host = DESKTOP-QEFBK7J source = mock_enrichment_log.txt sourcetype = enrichment log
3/18/24 12:06:20.000 PM
2024-03-18T19:06:20.000Z user=user1 ip_address=192.168.1.2 action=login
host = DESKTOP-QEFBK7J source = mock_enrichment_log.txt sourcetype = enrichment log
3/18/24 12:06:00.000 PM
2024-03-18T19:06:00.000Z user=user3 ip_address=10.0.0.1 action=logout
host = DESKTOP-QEFBK7J source = mock_enrichment_log.txt sourcetype = enrichment log
3/18/24 12:06:00.000 PM
2024-03-18T19:06:00.000Z user=user3 ip_address=10.0.0.1 action=logout
host = DESKTOP-QEFBK7J source = mock_enrichment_log.txt sourcetype = enrichment log
3/18/24 12:05:40.000 PM
2024-03-18T19:05:40.000Z user=user3 ip_address=192.168.1.1 action=purchase product=ProductA quantity=2
host = DESKTOP-QEFBK7J source = mock_enrichment_log.txt sourcetype = enrichment log
3/18/24 12:05:40.000 PM
2024-03-18T19:05:40.000Z user=user3 ip_address=192.168.1.1 action=purchase product=ProductA quantity=2
host = DESKTOP-QEFBK7J source = mock_enrichment_log.txt sourcetype = enrichment log


source="mock_enrichment_log.txt"
All time
4,000 events (before 5/1/24 10:14:06.000 PM)
No Event Sampling
Job
Verbose Mode
Events (4,000)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
20 Per Page
Prev
1 2 3 4 5 6 7 8
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a action 3
date_hour 12
date_mday 1
date_minute 60
a date_month 1
date_second 3
a date_wday 1
date_year 1
date_zone 1
a index 1
Time
Event
3/18/24 12:06:20.000 PM
2024-03-18T19:06:20.000Z user=user1 ip_address=192.168.1.2 action=login
host = DESKTOP-QEFBK7J source = mock_enrichment_log.txt sourcetype = enrichment log
3/18/24 12:06:20.000 PM
2024-03-18T19:06:20.000Z user=user1 ip_address=192.168.1.2 action=login
host = DESKTOP-QEFBK7J source = mock_enrichment_log.txt sourcetype = enrichment log
3/18/24 12:06:00.000 PM
2024-03-18T19:06:00.000Z user=user3 ip_address=10.0.0.1 action=logout
host = DESKTOP-QEFBK7J source = mock_enrichment_log.txt sourcetype = enrichment log
3/18/24 12:06:00.000 PM
2024-03-18T19:06:00.000Z user=user3 ip_address=10.0.0.1 action=logout
host = DESKTOP-QEFBK7J source = mock_enrichment_log.txt sourcetype = enrichment log
3/18/24 12:05:40.000 PM
2024-03-18T19:05:40.000Z user=user3 ip_address=192.168.1.1 action=purchase product=ProductA quantity=2
host = DESKTOP-QEFBK7J source = mock_enrichment_log.txt sourcetype = enrichment log
3/18/24 12:05:40.000 PM
2024-03-18T19:05:40.000Z user=user3 ip_address=192.168.1.1 action=purchase product=ProductA quantity=2
host = DESKTOP-QEFBK7J source = mock_enrichment_log.txt sourcetype = enrichment log


source="mock_enrichment_log.txt" |lookup
All time
4,000 events (before 5/1/24 10:15:26.000 PM)
No Event Sampling
Job
Verbose Mode
Events (4,000)
Patterns
Statistics
Visualization
Format Timeline
– Zoom Out
+ Zoom to Selection
× Deselect
1 hour per column
List
Format
20 Per Page
Prev
1 2 3 4 5 6 7 8 ...
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a action 3
date_hour 12
date_mday 1
date_minute 60
a date_month 1
date_second 3
a date_wday 1
date_year 1
date_zone 1
a index 1
a ip_address 4
Time
Event
3/18/24 12:06:20.000 PM
2024-03-18T19:06:20.000Z user=user1 ip_address=192.168.1.2 action=login
host = DESKTOP-QEFBK7J source = mock_enrichment_log.txt sourcetype = enrichment log
3/18/24 12:06:20.000 PM
2024-03-18T19:06:20.000Z user=user1 ip_address=192.168.1.2 action=login
host = DESKTOP-QEFBK7J source = mock_enrichment_log.txt sourcetype = enrichment log
3/18/24 12:06:00.000 PM
2024-03-18T19:06:00.000Z user=user3 ip_address=10.0.0.1 action=logout
host = DESKTOP-QEFBK7J source = mock_enrichment_log.txt sourcetype = enrichment log
3/18/24 12:06:00.000 PM
2024-03-18T19:06:00.000Z user=user3 ip_address=10.0.0.1 action=logout
host = DESKTOP-QEFBK7J source = mock_enrichment_log.txt sourcetype = enrichment log
3/18/24 12:05:40.000 PM
2024-03-18T19:05:40.000Z user=user3 ip_address=192.168.1.1 action=purchase product=ProductA quantity=2
host = DESKTOP-QEFBK7J source = mock_enrichment_log.txt sourcetype = enrichment log
3/18/24 12:05:40.000 PM
2024-03-18T19:05:40.000Z user=user3 ip_address=192.168.1.1 action=purchase product=ProductA quantity=2
host = DESKTOP-QEFBK7J source = mock_enrichment_log.txt sourcetype = enrichment log
3/18/24
2024-03-18T19:05:20.000Z user=user4 ip_address=10.0.0.1 action=login


New Search
Save As
Create Table View
Close
source="mock_enrichment_log.txt" |lookup
All time
4,000 events (before 5/1/24 10:15:26.000 PM)
No Event Sampling
Job
Verbose Mode
Events (4,000)
Patterns
Statistics
Visualization
Smaller
Larger
1 pattern based on a sample of 4,000 events
Less than 5,000 events may produce poor patterns. Try a search in a larger time range or with fewer constraints.
32.95% <timestamp> user=user1 ip_address=192.168.1.2 action=login
ESTIMATED EVENTS
1.32K
View Events
SEARCH
source="mock_enrichment_log.txt" | lookup | search login
Create alert
INCLUDED KEYWORDS
login


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="mock_enrichment_log.txt" |lookup
All time
4,000 events (before 5/1/24 10:15:26.000 PM)
No Event Sampling
Job
Verbose Mode
Events (4,000)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
host
1 Value, 100% of events
Selected
Yes
No
Reports
Top values
Top values by time
Rare values
Events with this field
Values
Count
%
DESKTOP-QEFBK7J
4,000
100%
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
action 3
date_hour 12
date_mday 1
date_minute 60
Next
3/18/24
12:06:00.000 PM
2024-03-18T19:06:00.000Z user=user3 ip_address=10.0.0.1 action=logout
host = DESKTOP-QEFBK7J
source = mock_enrichment_log.txt
sourcetype = enrichment log


New Pivot
Save As...
Clear
Acceleration
4,000 events (before 5/1/24 10:19:54.000 PM)
Time Range
Range
All time
Filter
+ Add Filter
X-Axis (Time)
Label
show
Periods
Auto
Label Rotation
Label Truncation
Yes
No
Y-Axis
Field
Count of 1714626926.312
Label
optional
Color (Areas)
General
Count of 1714626926.312
70
60
50
40
30
20
10
2:00 AM
Mon Mar 18
2024
4:00 AM
6:00 AM
8:00 AM
10:00 AM
_time