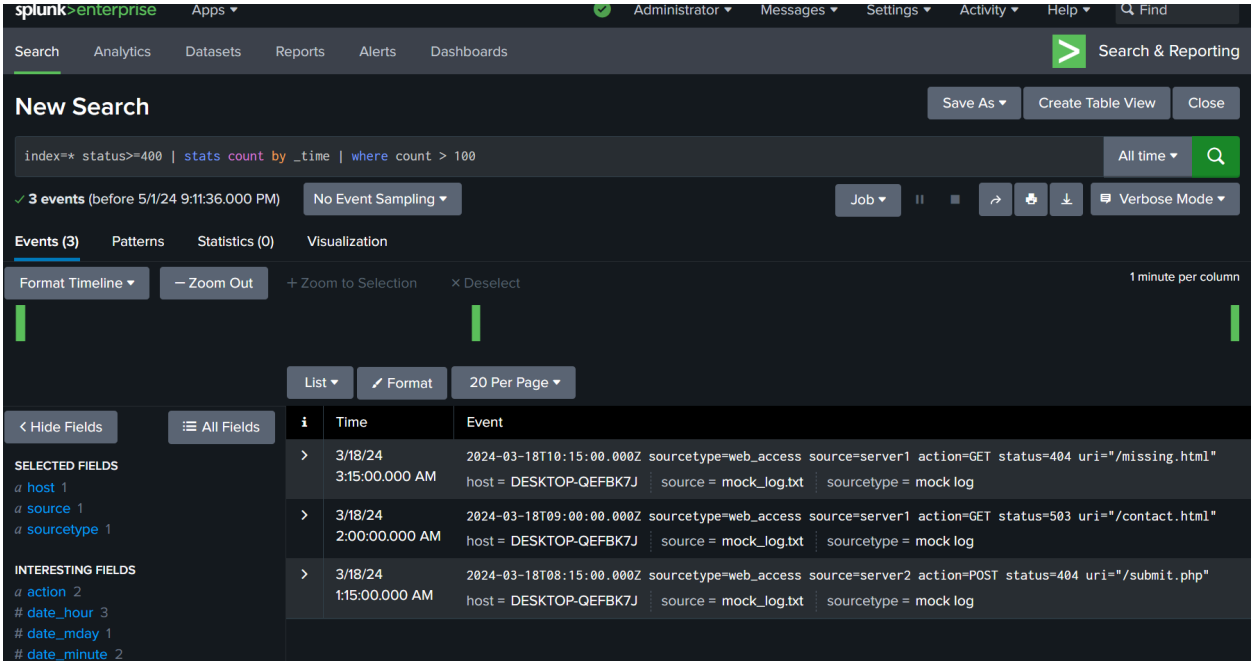
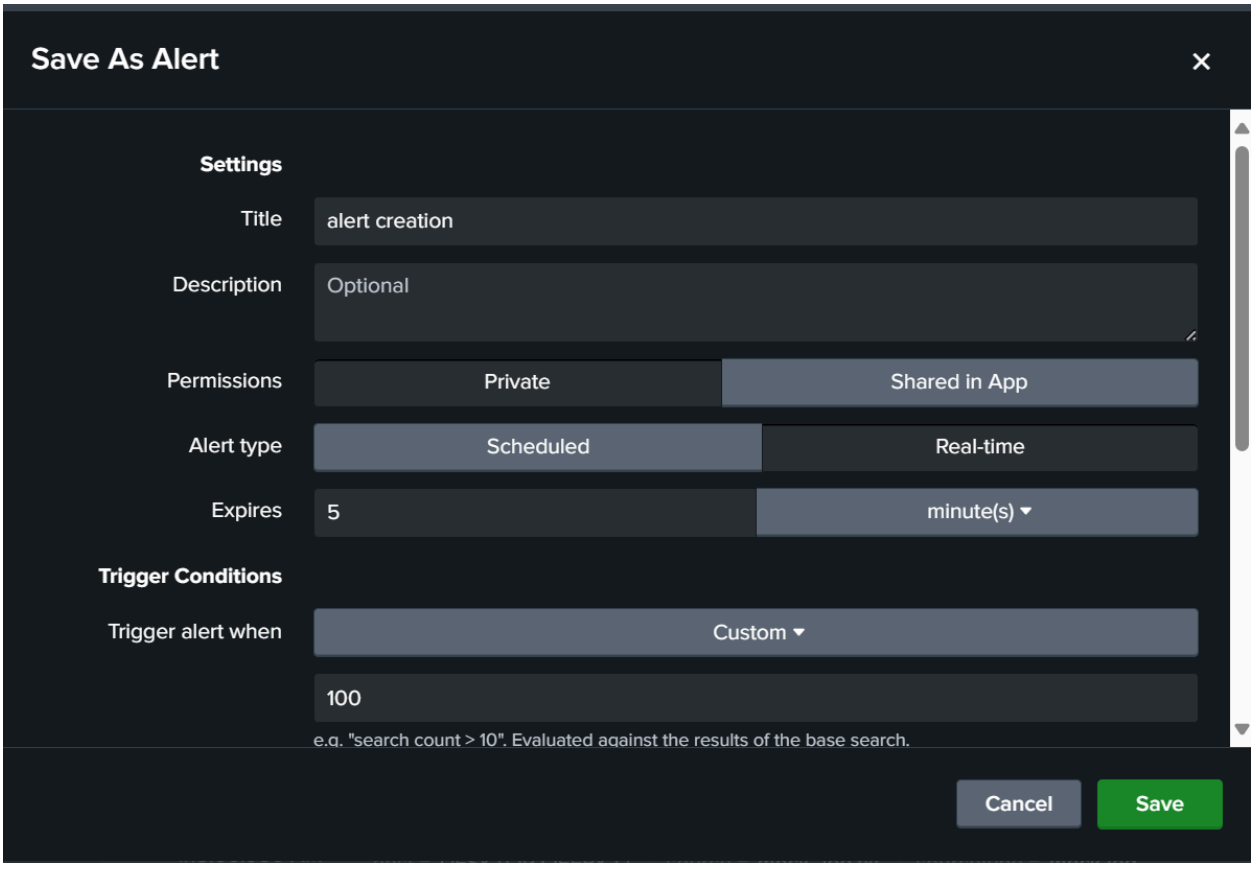
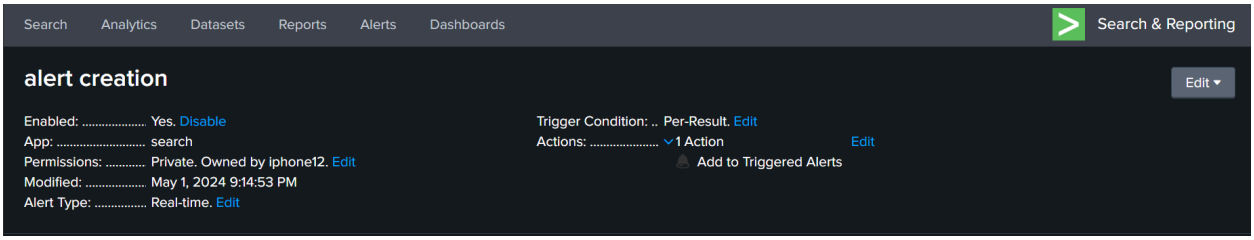
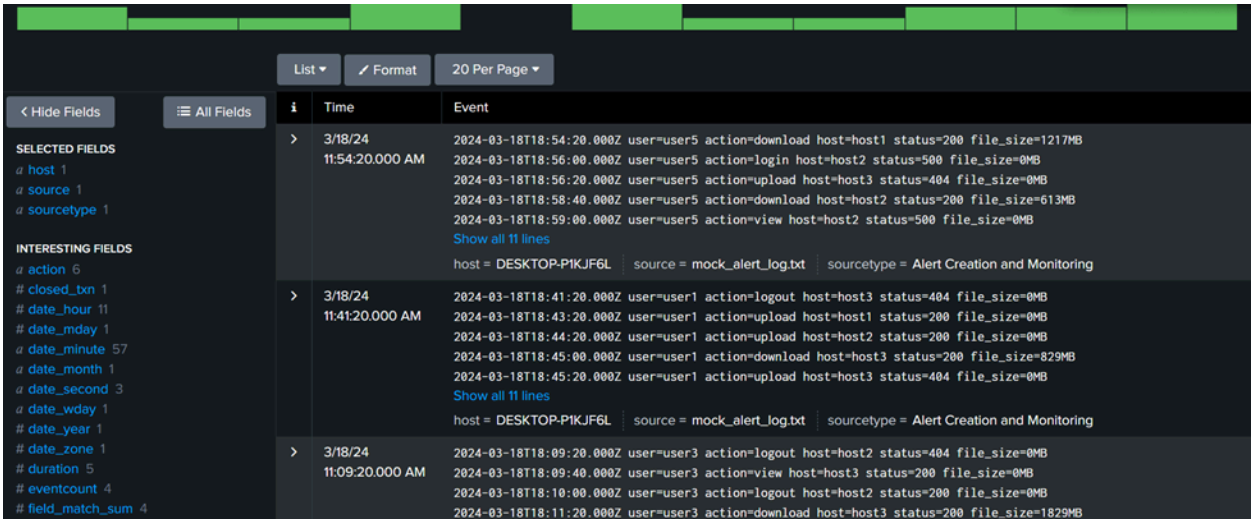
1.)


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
index=* status>=400 | stats count by _time | where count > 100
All time
3 events (before 5/1/24 9:11:36.000 PM)
No Event Sampling
Job
Verbose Mode
Events (3)
Patterns
Statistics (0)
Visualization
Format Timeline
– Zoom Out
+ Zoom to Selection
× Deselect
1 minute per column
List
Format
20 Per Page
Hide Fields
All Fields
Time
Event
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a action 2
date_hour 3
date_mday 1
date_minute 2
3/18/24 3:15:00.000 AM
2024-03-18T10:15:00.000Z sourcetype=web_access source=server1 action=GET status=404 uri="/missing.html"
host = DESKTOP-QEFBK7J source = mock_log.txt sourcetype = mock log
3/18/24 2:00:00.000 AM
2024-03-18T09:00:00.000Z sourcetype=web_access source=server1 action=GET status=503 uri="/contact.html"
host = DESKTOP-QEFBK7J source = mock_log.txt sourcetype = mock log
3/18/24 1:15:00.000 AM
2024-03-18T08:15:00.000Z sourcetype=web_access source=server2 action=POST status=404 uri="/submit.php"
host = DESKTOP-QEFBK7J source = mock_log.txt sourcetype = mock log


Save As Alert
Settings
Title
alert creation
Description
Optional
Permissions
Private
Shared in App
Alert type
Scheduled
Real-time
Expires
5
minute(s)
Trigger Conditions
Trigger alert when
Custom
100
e.g. "search count > 10". Evaluated against the results of the base search.
Cancel
Save



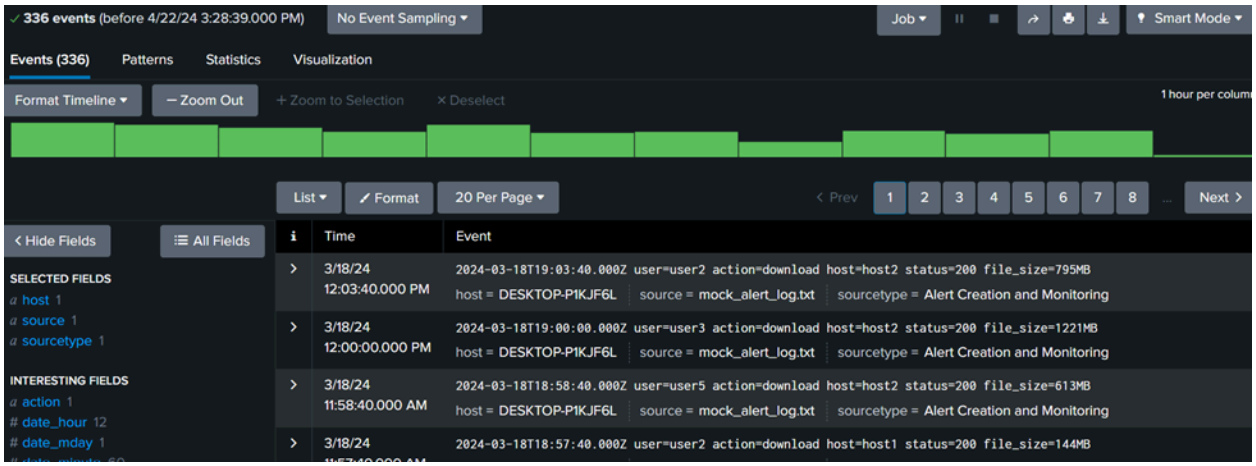
2.)



3.)

This alert greatly enhances operational security by pointing out possible efforts at data exfiltration. It makes quick action to stop possible data breaches possible by identifying very big data transfers, hence improving data security. By enabling early data protection and quick incident response, it also adds to operational efficiency.

Organizations may improve their operational security and efficiency by putting these warnings into practice and proactively identifying and handling any security events and operational abnormalities.


336 events (before 4/22/24 3:28:39.000 PM)
No Event Sampling
Job
Smart Mode
Events (336)
Patterns
Statistics
Visualization
Format Timeline
– Zoom Out
+ Zoom to Selection
× Deselect
1 hour per colum
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 1
date_hour 12
date_mday 1
Time
Event
3/18/24 12:03:40.000 PM
2024-03-18T19:03:40.000Z user=user2 action=download host=host2 status=200 file_size=795MB
host = DESKTOP-P1KJF6L source = mock_alert_log.txt sourcetype = Alert Creation and Monitoring
3/18/24 12:00:00.000 PM
2024-03-18T19:00:00.000Z user=user3 action=download host=host2 status=200 file_size=1221MB
host = DESKTOP-P1KJF6L source = mock_alert_log.txt sourcetype = Alert Creation and Monitoring
3/18/24 11:58:40.000 AM
2024-03-18T18:58:40.000Z user=user5 action=download host=host2 status=200 file_size=613MB
host = DESKTOP-P1KJF6L source = mock_alert_log.txt sourcetype = Alert Creation and Monitoring
3/18/24
2024-03-18T18:57:40.000Z user=user2 action=download host=host1 status=200 file_size=144MB