nput Settings

ptionally set additional input parameters for this data input as follows:

lost

/hen the Splunk platform indexes data, each event receives a ıost" value. The host value should be the name of the machine om which the event originates. The type of input you choose etermines the available configuration options. Learn More

- (•) Constant value
- ( ) Regular expression on path
- ( ) Segment in path

Host field value: KshitijGupta

ıdex

he Splunk platform stores incoming data as events in the elected index. Consider using a "sandbox" index as a estination if you have problems determining a source type for our data. A sandbox index lets you troubleshoot your onfiguration without impacting production indexes. You can lways change this setting later. Learn More

Index: Default ▾ Create a new index

AQ

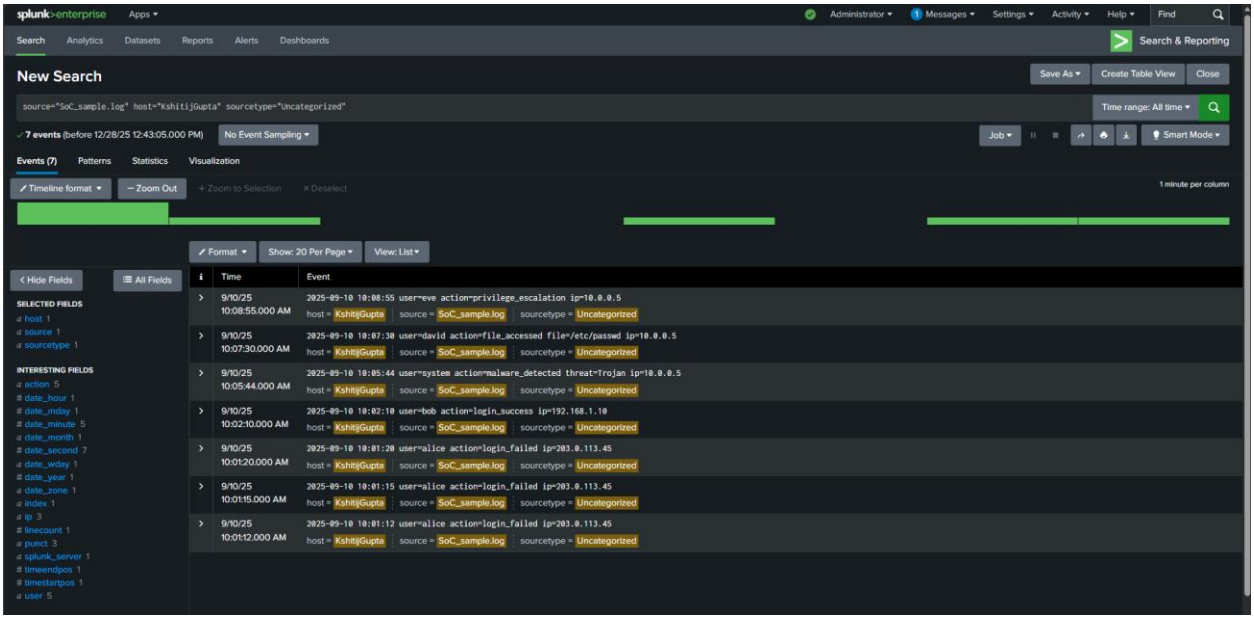
How do indexes work?

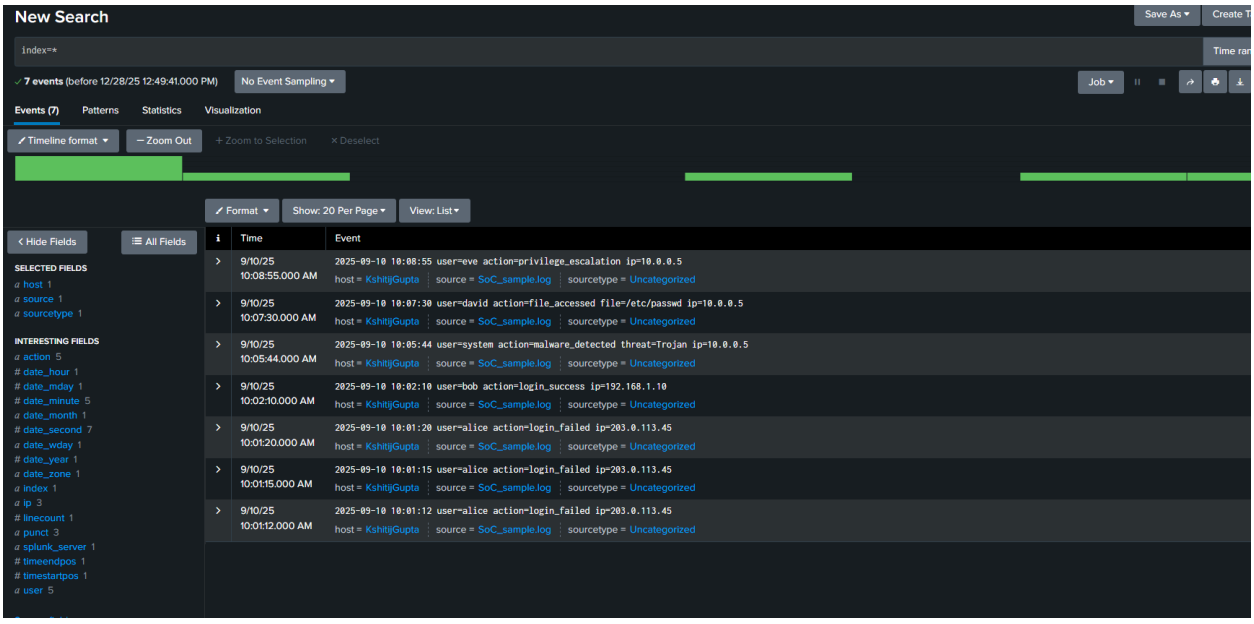
How do I know when to create or use multiple indexes?

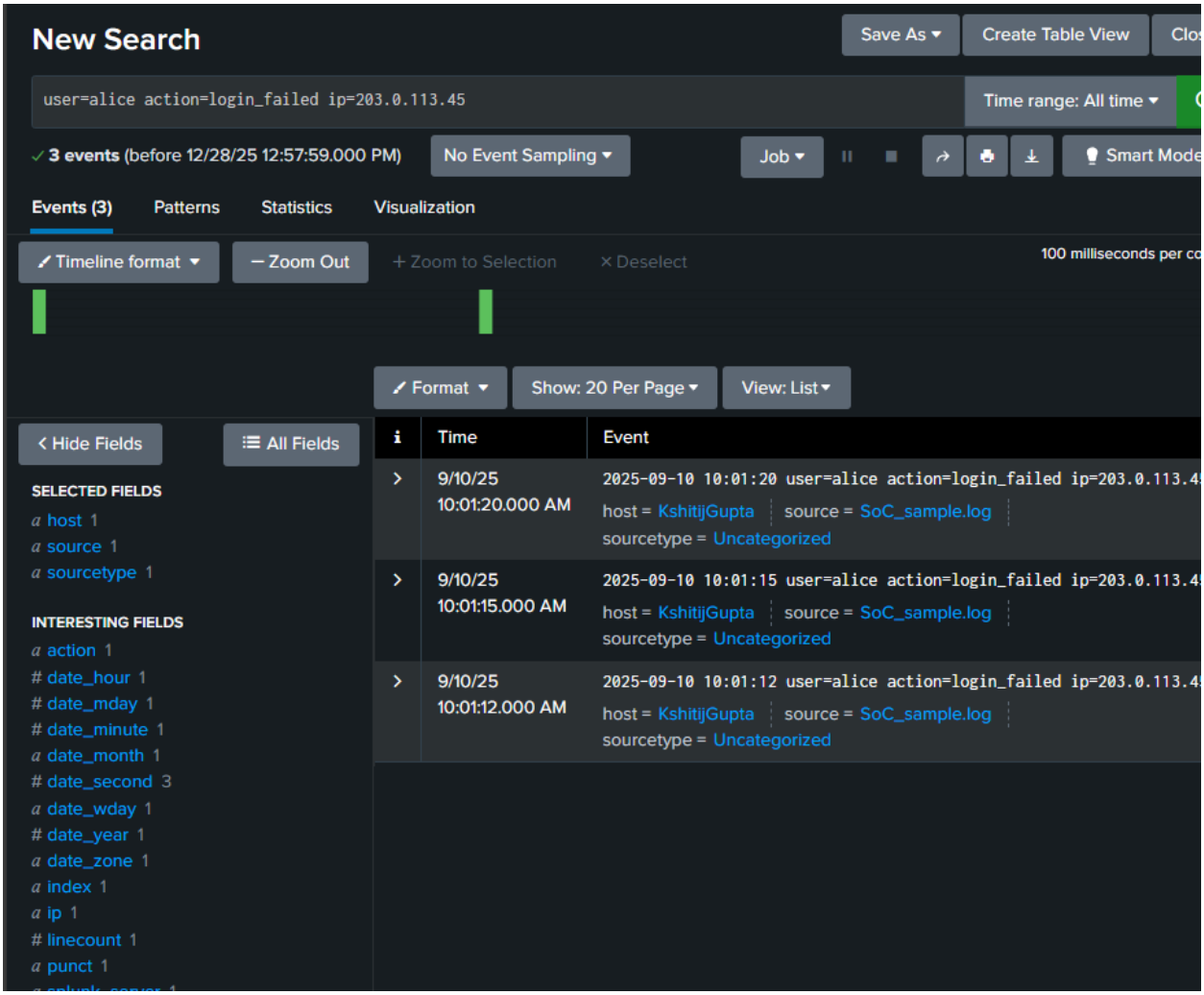
Add Data — Select Source — Set Source Type — Input Settings — Review — Done — < Back — Submit >

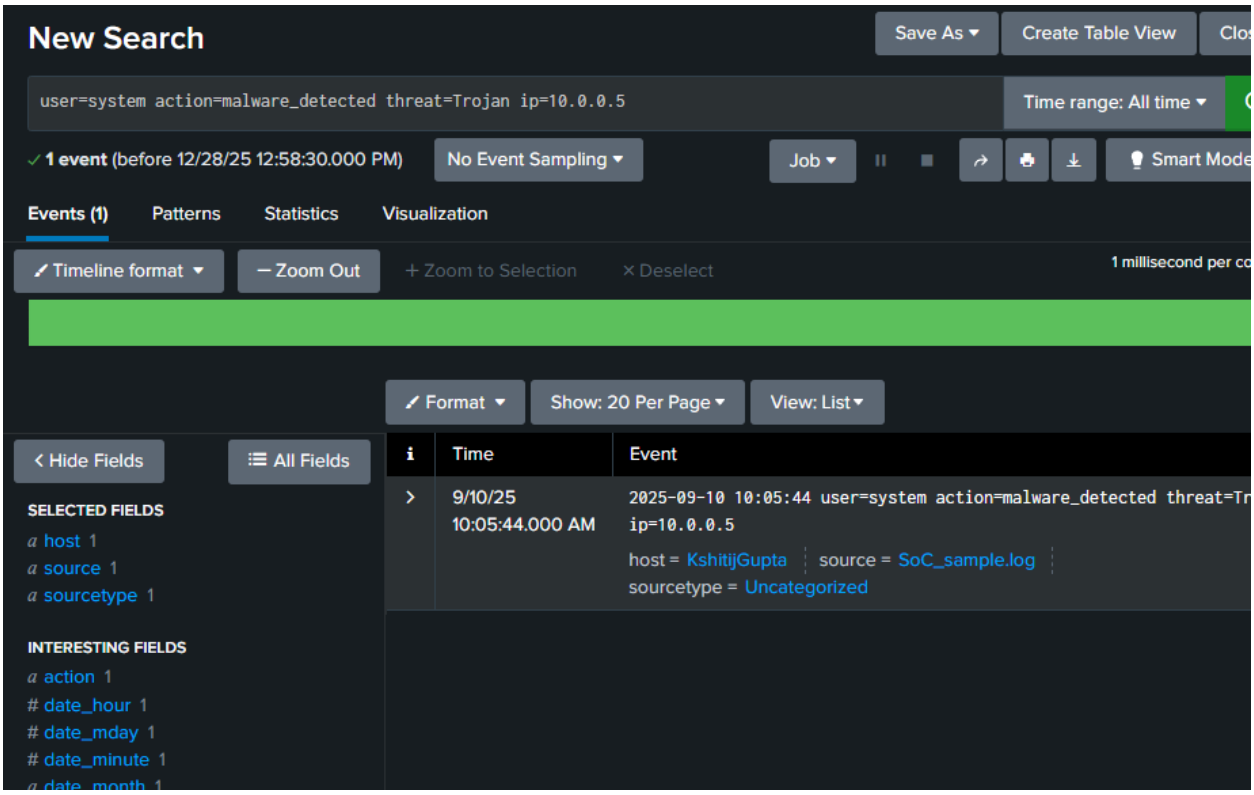
Review

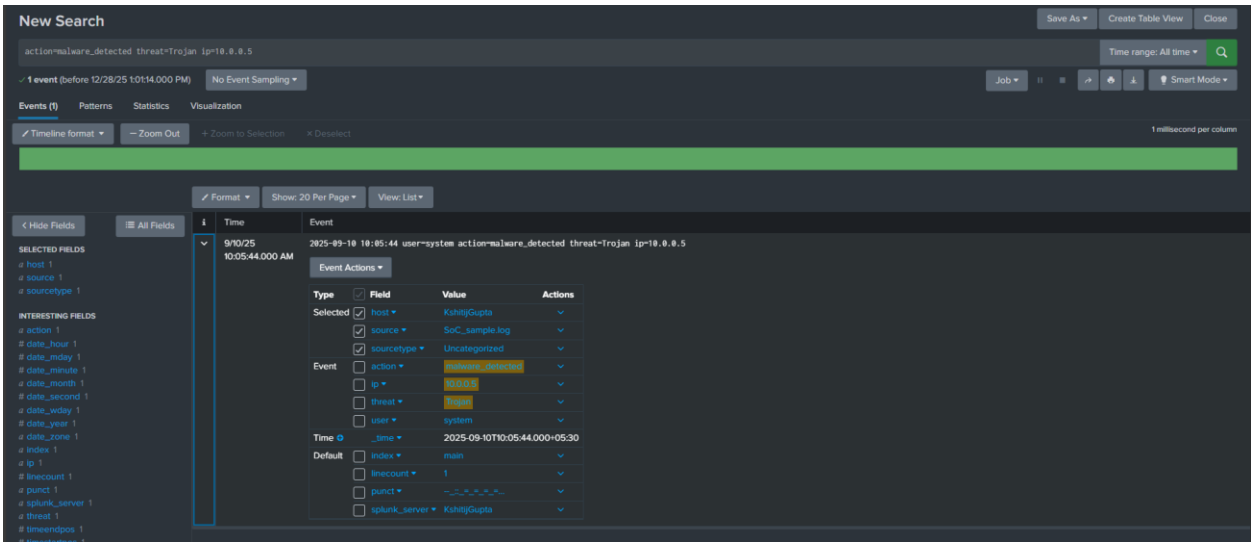
ıput Type	Uploaded File
ile Name	SoC_sample.log
ource Type	Uncategorized
lost	KshitijGupta
ıdex	Default

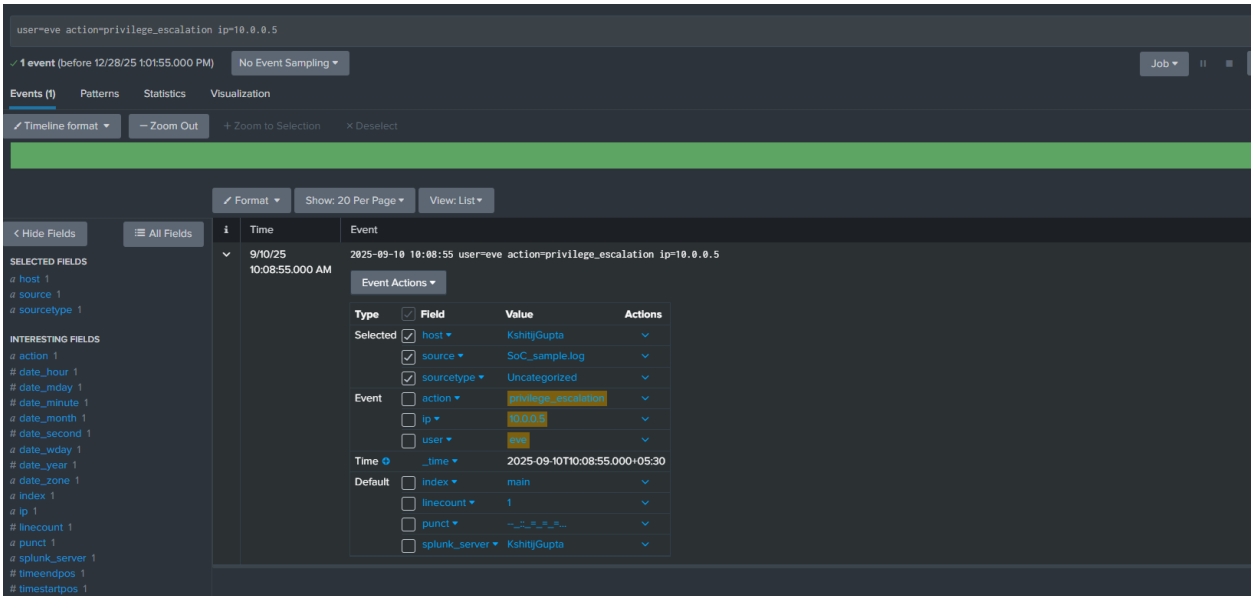

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="SoC_sample.log" host="KshitijGupta" sourcetype="Uncategorized"
Time range: All time
7 events (before 12/28/25 12:43:05.000 PM)
No Event Sampling
Job
Smart Mode
Events (7)
Patterns
Statistics
Visualization
Timeline format
– Zoom Out
+ Zoom to Selection
× Deselect
1 minute per column
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a action 5
date_hour 1
date_mday 1
date_minute 5
a date_month 1
date_second 7
a date_wday 1
date_year 1
a date_zone 1
a index 1
a ip 3
linecount 1
a punct 3
a splunk_server 1
timeendpos 1
timestartpos 1
a user 5
Time
Event
9/10/25 10:08:55.000 AM
2025-09-10 10:08:55 user=eve action=privilege_escalation ip=10.0.0.5
host = KshitijGupta source = SoC_sample.log sourcetype = Uncategorized
9/10/25 10:07:30.000 AM
2025-09-10 10:07:30 user=david action=file_accessed file="/etc/passwd ip=10.0.0.5
host = KshitijGupta source = SoC_sample.log sourcetype = Uncategorized
9/10/25 10:05:44.000 AM
2025-09-10 10:05:44 user=system action=malware_detected threat=Trojan ip=10.0.0.5
host = KshitijGupta source = SoC_sample.log sourcetype = Uncategorized
9/10/25 10:02:10.000 AM
2025-09-10 10:02:10 user=bob action=login_success ip=192.168.1.10
host = KshitijGupta source = SoC_sample.log sourcetype = Uncategorized
9/10/25 10:01:20.000 AM
2025-09-10 10:01:20 user=alice action=login_failed ip=203.0.113.45
host = KshitijGupta source = SoC_sample.log sourcetype = Uncategorized
9/10/25 10:01:15.000 AM
2025-09-10 10:01:15 user=alice action=login_failed ip=203.0.113.45
host = KshitijGupta source = SoC_sample.log sourcetype = Uncategorized
9/10/25 10:01:12.000 AM
2025-09-10 10:01:12 user=alice action=login_failed ip=203.0.113.45
host = KshitijGupta source = SoC_sample.log sourcetype = Uncategorized


New Search
Save As
index=*
7 events (before 12/28/25 12:49:41.000 PM)
No Event Sampling
Job
Events (7)
Patterns
Statistics
Visualization
Timeline format
– Zoom Out
+ Zoom to Selection
× Deselect
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a action 5
date_hour 1
date_mday 1
date_minute 5
a date_month 1
date_second 7
a date_wday 1
date_year 1
a date_zone 1
a index 1
a ip 3
linecount 1
a punct 3
a splunk_server 1
timeendpos 1
timestartpos 1
a user 5
Time
Event
9/10/25 10:08:55.000 AM
2025-09-10 10:08:55 user=eve action=privilege_escalation ip=10.0.0.5
host = KshitijGupta source = SoC_sample.log sourcetype = Uncategorized
9/10/25 10:07:30.000 AM
2025-09-10 10:07:30 user=david action=file_accessed file="/etc/passwd ip=10.0.0.5
host = KshitijGupta source = SoC_sample.log sourcetype = Uncategorized
9/10/25 10:05:44.000 AM
2025-09-10 10:05:44 user=system action=malware_detected threat=Trojan ip=10.0.0.5
host = KshitijGupta source = SoC_sample.log sourcetype = Uncategorized
9/10/25 10:02:10.000 AM
2025-09-10 10:02:10 user=bob action=login_success ip=192.168.1.10
host = KshitijGupta source = SoC_sample.log sourcetype = Uncategorized
9/10/25 10:01:20.000 AM
2025-09-10 10:01:20 user=alice action=login_failed ip=203.0.113.45
host = KshitijGupta source = SoC_sample.log sourcetype = Uncategorized
9/10/25 10:01:15.000 AM
2025-09-10 10:01:15 user=alice action=login_failed ip=203.0.113.45
host = KshitijGupta source = SoC_sample.log sourcetype = Uncategorized
9/10/25 10:01:12.000 AM
2025-09-10 10:01:12 user=alice action=login_failed ip=203.0.113.45
host = KshitijGupta source = SoC_sample.log sourcetype = Uncategorized


New Search
Save As
Create Table View
user=alice action=login_failed ip=203.0.113.45
Time range: All time
3 events (before 12/28/25 12:57:59.000 PM)
No Event Sampling
Job
Smart Mode
Events (3)
Patterns
Statistics
Visualization
Timeline format
– Zoom Out
+ Zoom to Selection
× Deselect
100 milliseconds per co
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a action 1
date_hour 1
date_mday 1
date_minute 1
a date_month 1
date_second 3
a date_wday 1
date_year 1
a date_zone 1
a index 1
a ip 1
linecount 1
a punct 1
Time
Event
9/10/25
10:01:20.000 AM
2025-09-10 10:01:20 user=alice action=login_failed ip=203.0.113.4
host = KshitijGupta
source = SoC_sample.log
sourcetype = Uncategorized
9/10/25
10:01:15.000 AM
2025-09-10 10:01:15 user=alice action=login_failed ip=203.0.113.4
host = KshitijGupta
source = SoC_sample.log
sourcetype = Uncategorized
9/10/25
10:01:12.000 AM
2025-09-10 10:01:12 user=alice action=login_failed ip=203.0.113.4
host = KshitijGupta
source = SoC_sample.log
sourcetype = Uncategorized


New Search
Save As
Create Table View
user=system action=malware_detected threat=Trojan ip=10.0.0.5
Time range: All time
1 event (before 12/28/25 12:58:30.000 PM)
No Event Sampling
Job
Smart Mode
Events (1)
Patterns
Statistics
Visualization
Timeline format
– Zoom Out
+ Zoom to Selection
× Deselect
1 millisecond per co
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a action 1
date_hour 1
date_mday 1
date_minute 1
Time
Event
9/10/25
10:05:44.000 AM
2025-09-10 10:05:44 user=system action=malware_detected threat=Tr
ip=10.0.0.5
host = KshitijGupta
source = SoC_sample.log
sourcetype = Uncategorized


New Search
Save As
Create Table View
Close
action=malware_detected threat=Trojan ip=10.0.0.5
Time range: All time
1 event (before 12/28/25 1:01:14.000 PM)
No Event Sampling
Job
Smart Mode
Events (1)
Patterns
Statistics
Visualization
Timeline format
– Zoom Out
+ Zoom to Selection
× Deselect
1 millisecond per column
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a action 1
date_hour 1
date_mday 1
date_minute 1
a date_month 1
date_second 1
a date_wday 1
date_year 1
a date_zone 1
a index 1
a ip 1
linecount 1
a punct 1
a splunk_server 1
a threat 1
timeendpos 1
Time
Event
9/10/25
10:05:44.000 AM
2025-09-10 10:05:44 user=system action=malware_detected threat=Trojan ip=10.0.0.5
Event Actions
Type
Field
Value
Actions
Selected
host
KshitijGupta
source
SoC_sample.log
sourcetype
Uncategorized
Event
action
malware_detected
ip
10.0.0.5
threat
Trojan
user
system
Time
_time
2025-09-10T10:05:44.000+05:30
Default
index
main
linecount
1
punct
splunk_server
KshitijGupta


user=eve action=privilege_escalation ip=10.0.0.5
1 event (before 12/28/25 1:01:55.000 PM)
No Event Sampling
Job
Events (1)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a action 1
date_hour 1
date_mday 1
date_minute 1
a date_month 1
date_second 1
a date_wday 1
date_year 1
a date_zone 1
a index 1
a ip 1
linecount 1
a punct 1
a splunk_server 1
timeendpos 1
timestartpos 1
Time
Event
9/10/25
10:08:55.000 AM
2025-09-10 10:08:55 user=eve action=privilege_escalation ip=10.0.0.5
Event Actions
Type
Field
Value
Actions
Selected
host
KshitijGupta
source
SoC_sample.log
sourcetype
Uncategorized
Event
action
privilege_escalation
ip
10.0.0.5
user
eve
Time
_time
2025-09-10T10:08:55.000+05:30
Default
index
main
linecount
1
punct
splunk_server
KshitijGupta