

New Search

```
1 source="WinEventLog:*" host="MSI"
```

Time range: Last 24 hours

✓ **4,860 events** (9/15/25 4:30:00.000 AM to 9/16/25 4:46:01.000 AM) No Event Sampling

Events (4,860)

Timeline format

1 hour per column



SELECTED FIELDS

```
# date_hour 8
# date_mday 2
# date_minute 51
a date_month 1
# date_second 60
a date_wday 2
# date_year 1
a date_zone 1
a host 1
a index 1
# linecount 23
a punct 100+
a source 3
a sourcetype 3
a splunk_server 1
a splunk_server_group 4
# timeendpos 1
# timestartpos 1
```

INTERESTING FIELDS

```

a Account_Domain 6
a Account_Name 15
a ComputerName 1
# EventCode 72
# EventType 4
a Keywords 7
a LogName 3
a Logon_ID 33
a Message 100+
a OpCode 4
a Read_Operation 2
# RecordNumber 100+
a Security_ID 15
a SourceName 30
a TaskCategory 22
a Type 3

```

91 more fields

+ Extract New Fields (/en-US/app/search/field_extractor?sid=1757978161.32)

Time

9/16/25
4:45:12.000 AM

Event

```
09/16/2025 04:45:12 AM
LogName=System
EventCode=33
EventType=4
ComputerName=MSI
Show all 12 lines

date_hour = 4      date_mday = 16
date_minute = 45   date_month = september
date_second = 12   date_wday = tuesday
date_year = 2025   date_zone = local   host = MSI
index = main       linecount = 12
punct =
//_::=====_:_.
source = WinEventLog:System
sourcetype = WinEventLog:System
splunk_server = MSI
splunk_server_group = dmc_group_indexer splunk_server_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head
timeendpos = 23    timestartpos = 0
```

Time	Event
9/16/25 4:43:11.000 AM	<p>09/16/2025 04:43:11 AM LogName=Security EventCode=4672 EventType=0 ComputerName=MSI Show all 31 lines</p> <pre> date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 11 date_wday = tuesday date_year = 2025 date_zone = local host = MSI index = main linecount = 31 punct = //_::=====_.===_==_.\r\r:\rt_:tt---\rt_:tt\rt source = WinEventLog:Security sourcetype = WinEventLog:Security splunk_server = MSI splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head timeendpos = 23 timestartpos = 0 </pre>
9/16/25 4:43:11.000 AM	<p>09/16/2025 04:43:11 AM LogName=Security EventCode=4624 EventType=0 ComputerName=MSI Show all 71 lines</p> <pre> date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 11 date_wday = tuesday date_year = 2025 date_zone = local host = MSI index = main linecount = 71 punct = //_::=====_.===_==_.\r\r:\rt_:tt---\rt_:tt\$r source = WinEventLog:Security sourcetype = WinEventLog:Security splunk_server = MSI splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head timeendpos = 23 timestartpos = 0 </pre>

Time	Event
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>

Time	Event
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>

Time	Event
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>

Time	Event
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>

Time	Event
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>

Time	Event
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>

Time	Event
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:\rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:\rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>

Time	Event
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>

Time	Event
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>

Time	Event
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>

Time	Event
9/16/25 4:43:05.000 AM	09/16/2025 04:43:05 AM LogName=Security EventCode=5379 EventType=0 ComputerName=MSI Show all 21 lines date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI index = main linecount = 21 punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t source = WinEventLog:Security sourcetype = WinEventLog:Security splunk_server = MSI splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head timeendpos = 23 timestartpos = 0
9/16/25 4:43:05.000 AM	09/16/2025 04:43:05 AM LogName=Security EventCode=5379 EventType=0 ComputerName=MSI Show all 21 lines date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI index = main linecount = 21 punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t source = WinEventLog:Security sourcetype = WinEventLog:Security splunk_server = MSI splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head timeendpos = 23 timestartpos = 0

Time	Event
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>

Time	Event
9/16/25 4:43:05.000 AM	09/16/2025 04:43:05 AM LogName=Security EventCode=5379 EventType=0 ComputerName=MSI Show all 21 lines date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI index = main linecount = 21 punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t source = WinEventLog:Security sourcetype = WinEventLog:Security splunk_server = MSI splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head timeendpos = 23 timestartpos = 0
9/16/25 4:43:05.000 AM	09/16/2025 04:43:05 AM LogName=Security EventCode=5379 EventType=0 ComputerName=MSI Show all 21 lines date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI index = main linecount = 21 punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t source = WinEventLog:Security sourcetype = WinEventLog:Security splunk_server = MSI splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head timeendpos = 23 timestartpos = 0

Time	Event
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>

Time	Event
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>

Time	Event
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>

Time	Event
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>

Time	Event
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>

Time	Event
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>

Time	Event
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>

Time	Event
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>

Time	Event
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct = //_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>

Time	Event
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct =</p> <p>//_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>
9/16/25 4:43:05.000 AM	<p>09/16/2025 04:43:05 AM</p> <p>LogName=Security</p> <p>EventCode=5379</p> <p>EventType=0</p> <p>ComputerName=MSI</p> <p>Show all 21 lines</p> <p>date_hour = 4 date_mday = 16 date_minute = 43 date_month = september date_second = 5 date_wday = tuesday date_year = 2025 date_zone = local host = MSI </p> <p>index = main linecount = 21 </p> <p>punct =</p> <p>//_::=====_.===_==_.\r\r:rt:tt-----\rt:t </p> <p>source = WinEventLog:Security </p> <p>sourcetype = WinEventLog:Security </p> <p>splunk_server = MSI </p> <p>splunk_server_group = dmc_group_indexer splunk_serv er_group = dmc_group_kv_store splunk_server_group = dmc_group_license_master splunk_server_group = dmc_group_search_head </p> <p>timeendpos = 23 timestartpos = 0</p>

Time	Event
9/16/25	09/16/2025 04:43:05 AM
4:43:05.000 AM	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=MSI
	Show all 21 lines
	date_hour = 4 date_mday = 16
	date_minute = 43 date_month = september
	date_second = 5 date_wday = tuesday
	date_year = 2025 date_zone = local host = MSI
	index = main linecount = 21
	punct =
	//_::====_.==_==_.\r\r:rt:tt-----\rt:t
	source = WinEventLog:Security
	sourcetype = WinEventLog:Security
	splunk_server = MSI
	splunk_server_group = dmc_group_indexer splunk_serv
	er_group = dmc_group_kv_store splunk_server_group =
	dmc_group_license_master splunk_server_group =
	dmc_group_search_head
	timeendpos = 23 timestartpos = 0