

Project: Windows Log Analysis

Tools: Splunk Free, Windows Event Viewer

Objective: Detect unauthorized login attempts

Findings: 3 critical and 5 warnings

App logs

index=* "fail" OR "warn" OR "critical"

9 events (before 11/7/25 6:37:32.000 AM) Sampling 1:10 ▾

Events (9) Patterns Statistics Visualization

Timeline format ▾ - Zoom Out + Zoom to Selection X Deselect

Time range: All time ▾

1 month 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

- # date_hour 5
- # date_mday 5
- # date_minute 6
- # date_month 5
- # date_second 8
- a date_wday 4
- # date_year 1
- a date_zone 1
- a index 1
- # linecount 2

i	Time	Event
>	9/10/25 8:04:42.000 PM	Information 10-09-2025 20:04:42 Microsoft-Windows-Winlogon 6003 None The winlogon notification subscriber <SessionEnv> was unavailable to handle a critical notification event. host = U-3PJCC64 source = ApplicationLgs.txt sourcetype = WinEvtLog
>	6/13/25 5:16:05.000 AM	Warning 13-06-2025 05:16:05 Microsoft-Windows-Winlogon 6004 None The winlogon notification subscriber <TrustedInstaller> failed a critical notification event. host = U-3PJCC64 source = ApplicationLgs.txt sourcetype = WinEvtLog
>	4/15/25 5:10:31.000 AM	Information 15-04-2025 05:10:31 Microsoft-Windows-Winlogon 6003 None The winlogon notification subscriber <SessionEnv> was unavailable to handle a critical notification event. host = U-3PJCC64 source = ApplicationLgs.txt sourcetype = WinEvtLog
>	3/3/25 6:31:23.000 PM	Warning 03-03-2025 18:31:23 cscan 259 (1) "The description for Event ID 259 from source cscan cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer. If the event originated on another computer, the display information had to be saved with the event. ... 4 lines omitted ...

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾

New Search

index=* ("authentication" OR "failed")
| eval category=if(match(_raw, "authentication"), "authentication",
if(match(_raw, "failed"), "failed", "other"))
| stats count by category

6 events (before 11/7/25 7:09:15.000 AM) Sampling 1:1,000 ▾

Save As ▾ Create Table View ▾ Close

Time range: All time ▾

Events Patterns Statistics (1) Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

category	count
other	6.00