Splunk SOC Lab – Log Generation, Detection & Dashboard

BY:- KAVINDRA PATEL

Project Objective

Content :

- Simulated real –world security logs
- Detected brute-force login attempts
- Analyzed Windows Event IDs
- Build security monitoring dashboard in Splunk

Lab Setup

Lab Architecture:

- Host Machine : Windows 11
- Target Server : Windows Server 2019
- Attacker Machine : kali Linux
- SIEM Tool: Splunk Enterprise
- Log Collector: Splunk Universal Forwarder

Installation & Setup

Install Splunk Enterprise :

- Go to official Splunk website
- Click Free Trial/Free Downloads
- Create Register Account
- Login to your Splunk Account & Download Splunk Enterprise
- After Installation configure admin username & password
- Splunk Web via **https://localhost:8000**

Universal Forwarder Setup

- Downloaded Splunk Universal Forwarder
- Install universal forwarder on windows
- Configured log forwarding to Splunk SIEM

Brute Force –Failed Login Attemps Generation

- Used Kali Linux to simulate brute-force attack
- Targeted Windows Server RDP service
- Executed Hydra tool with username and password wordlistndows Server RDP service
- **Command Used:**
- **hydra -V -f -l administrator -P rockyou.txt rdp://192.168.232.131 (tatget ip)**

Verifying Generated Logs in Windows Event Viewer

- Logged into Target Windows Server
- Opened **Event Viewer**
- Navigated to:
  Windows Logs → Security
- Filtered for **Event ID 4625 (Failed Login)**
- Verified multiple failed login events generated by brute-force attack
- Save all Events for file

How to add data in Splunk

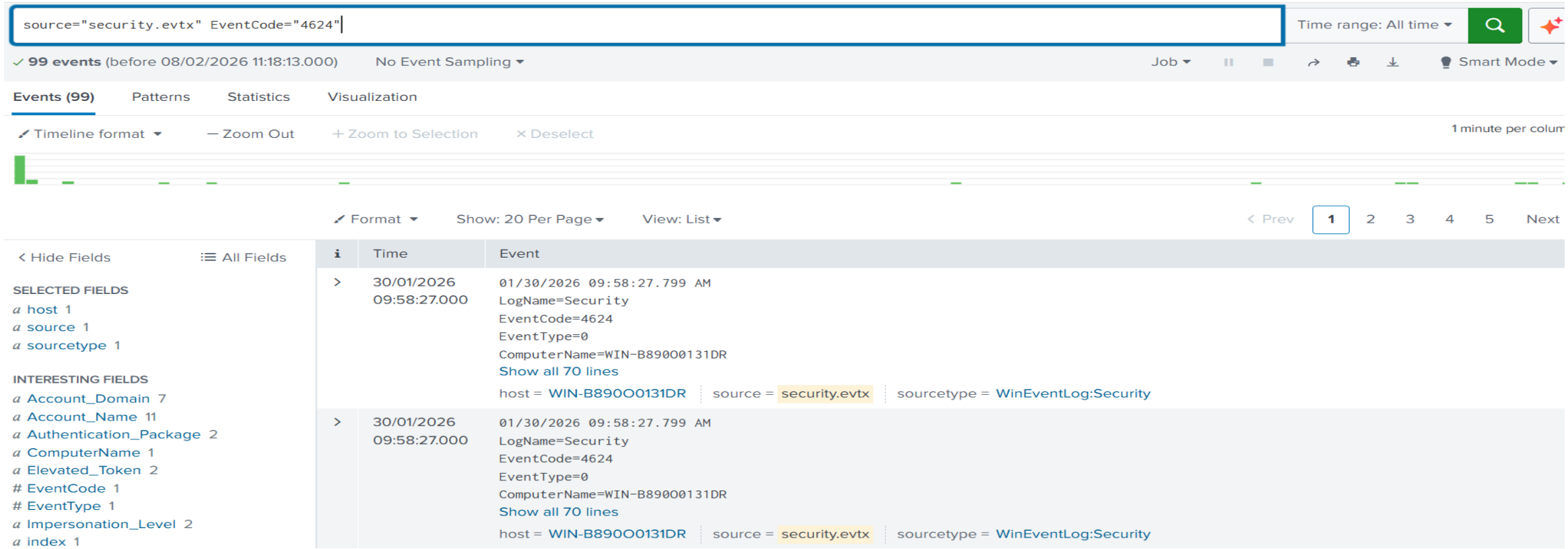
- Go to :Settings → Add Data , Click : Upload
- Click: Select File → Choose your .log or .txt file
- Click Next
- Source Typ:If it's a normal log → choose auto-detect
- Or manually select appropriate sourcetype
- Choose: Default
- Last : Review
- Start Searching

How to Use SPL Queries

STEP BY STEP

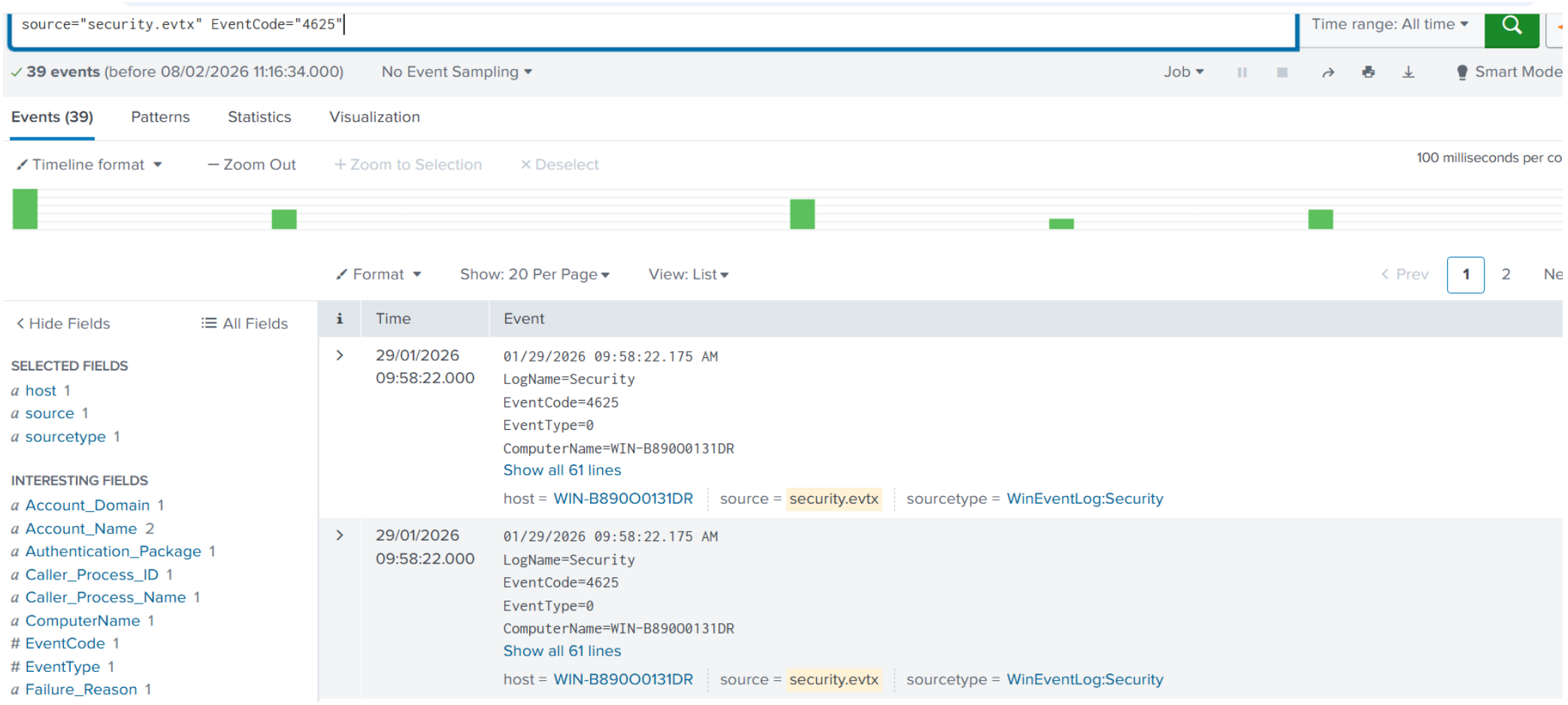
source=" security.evtx" host="WINB89000131DR"sourcetype="WinEventLog:Security" EventCode="4624“

(4624 Successful Logon)



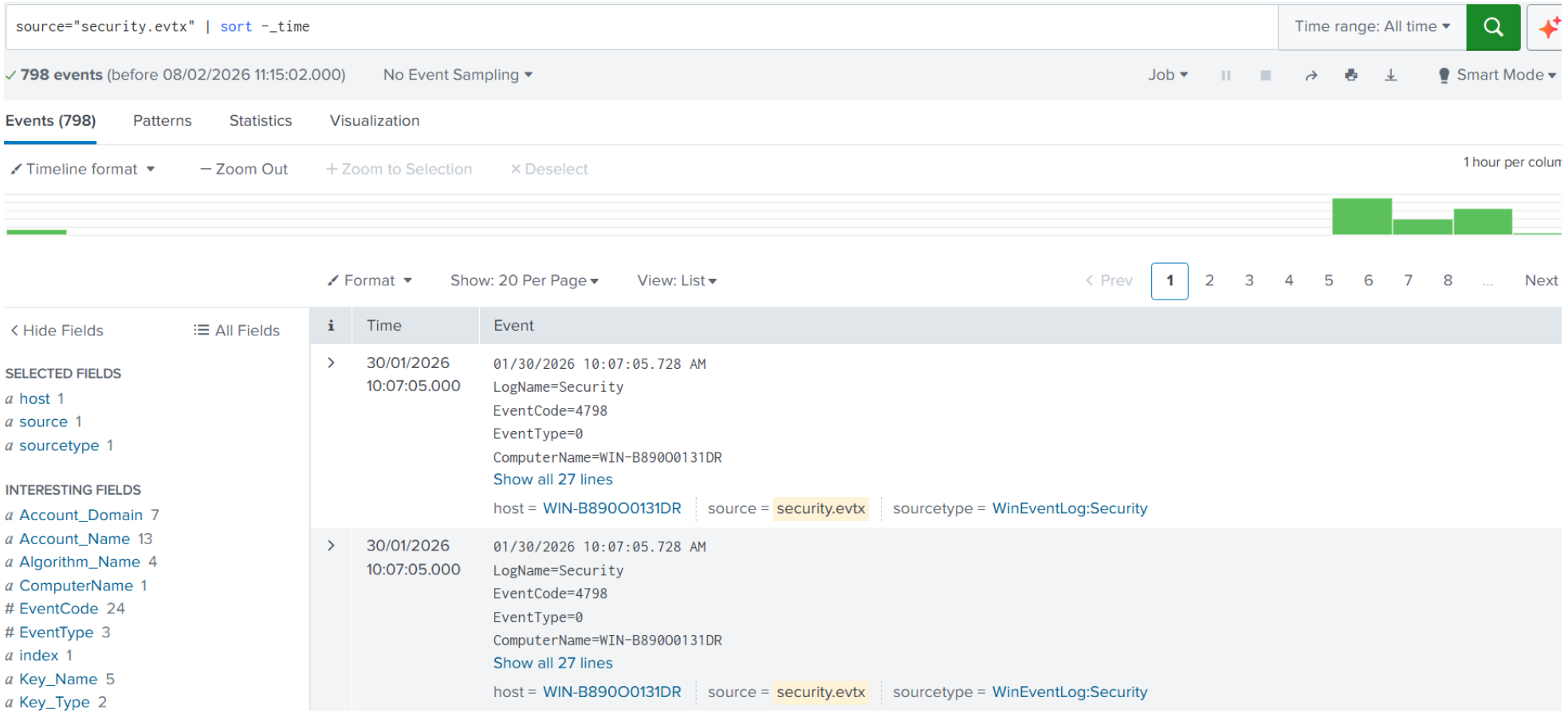
source=" security.evtx" host="WINB89000131DR"sourcetype="WinEventLog:Security" EventCode="4625"

(4625 = Failed Logon)



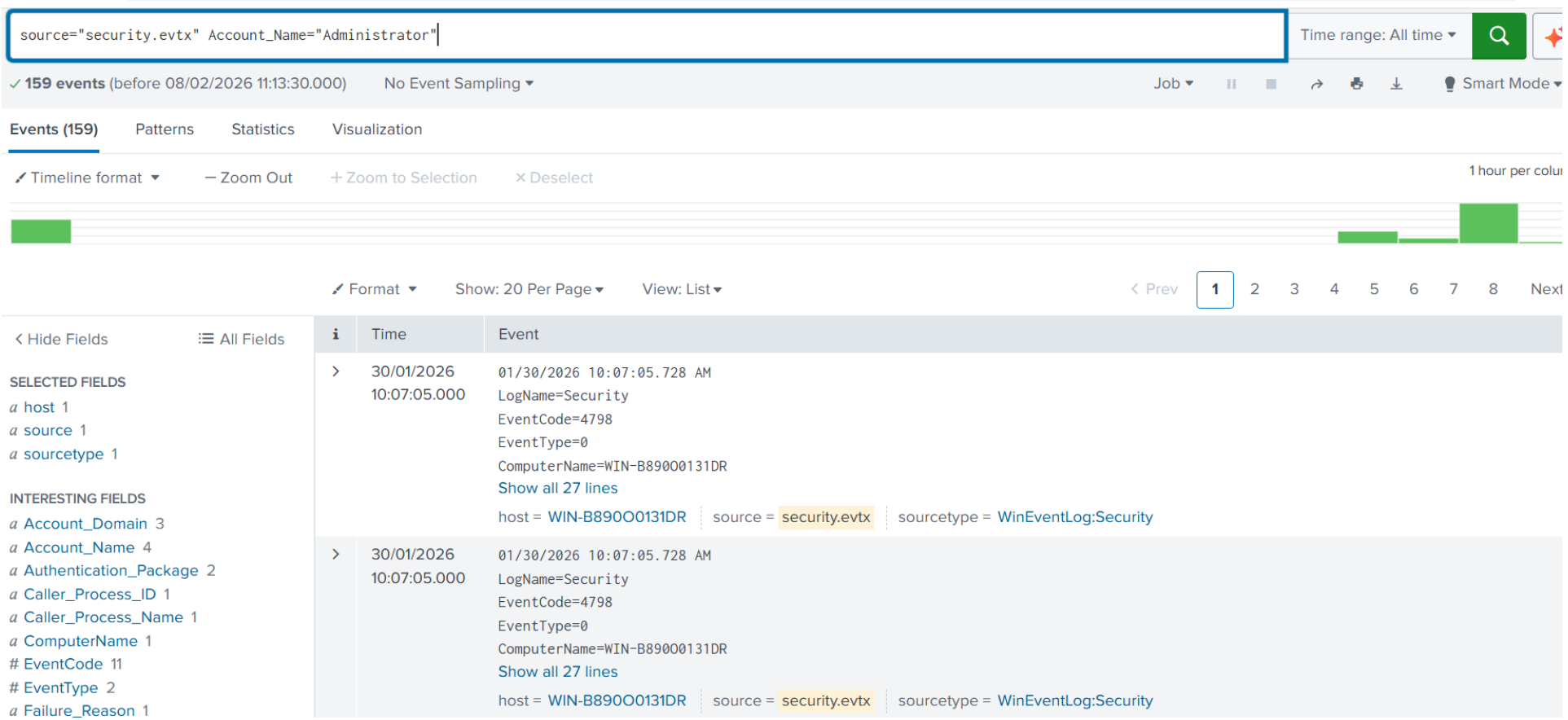
source=" security.evtx" host="WINB89000131DR“
sourcetype="WinEventLog:Security" | sort -_time
|

sort Events by Time(Most Recent First)



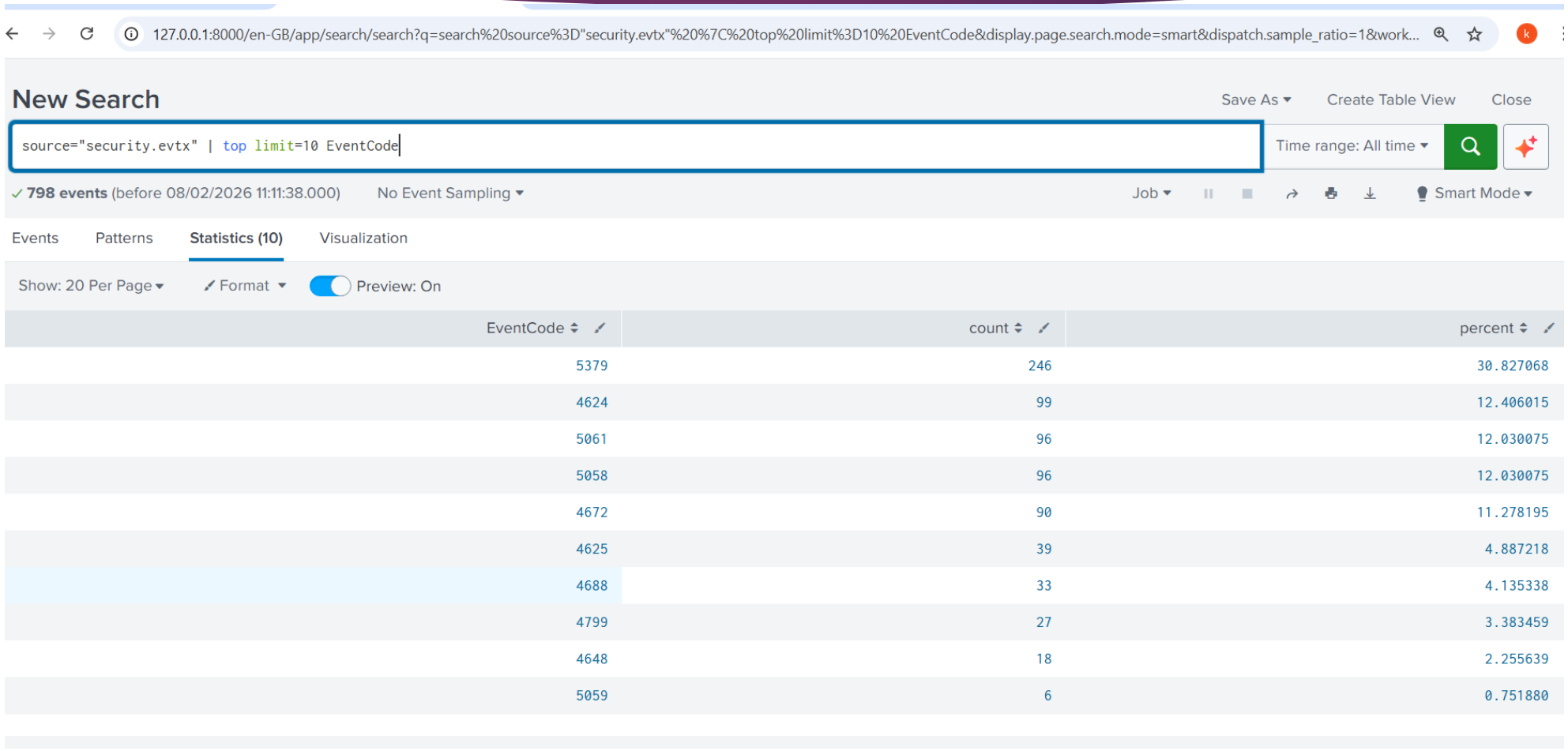
source=" security.evtx" host="WINB89000131DR“
sourcetype="WinEventLog:Security“ Account_Name=“Administrator”

(Filter by Username)



source=" security.evtx" host="WINB89000131DR“
sourcetype="WinEventLog:Security" | top limit = 10 EventCode

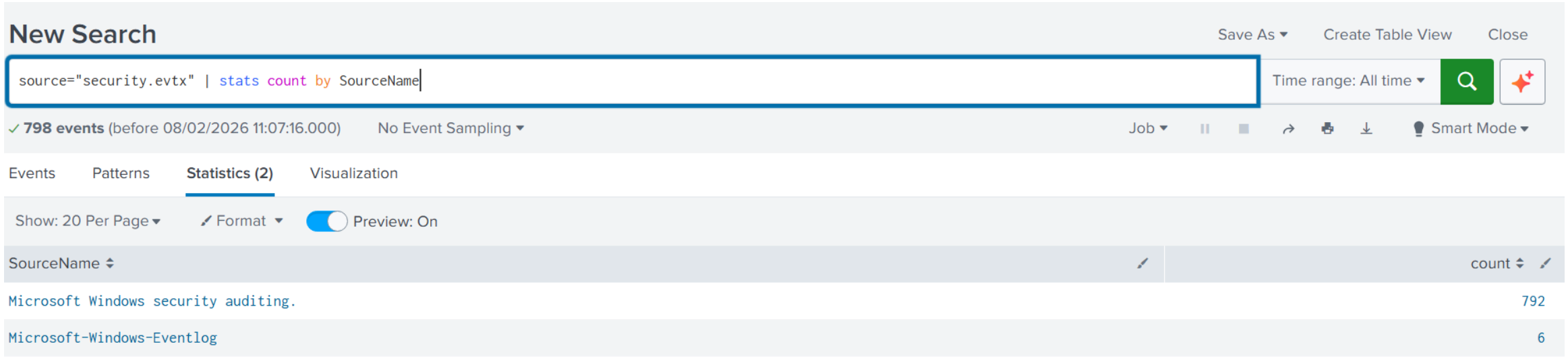
(Top 10 EventCodes)



EventCode	count	percent
5379	246	30.827068
4624	99	12.406015
5061	96	12.030075
5058	96	12.030075
4672	90	11.278195
4625	39	4.887218
4688	33	4.135338
4799	27	3.383459
4648	18	2.255639
5059	6	0.751880

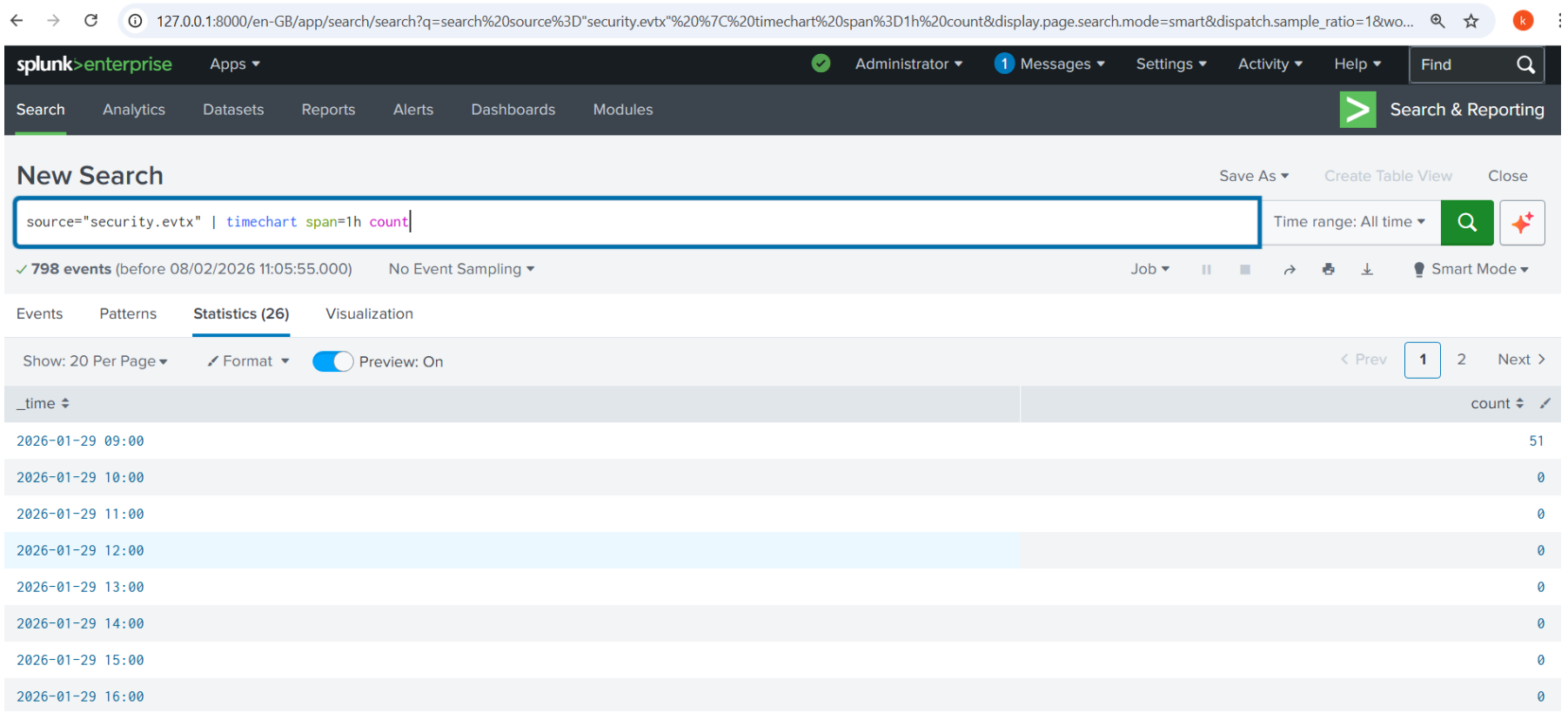
source=" security.evtx" host="WINB89000131DR“
sourcetype="WinEventLog:Security“ | stats count by SourceName

(Group Events by Source and Count)



source=" security.evtx" host="WINB89000131DR“
sourcetype="WinEventLog:Security“ | timechart span=1h count

EventsOverTime(Hourly)

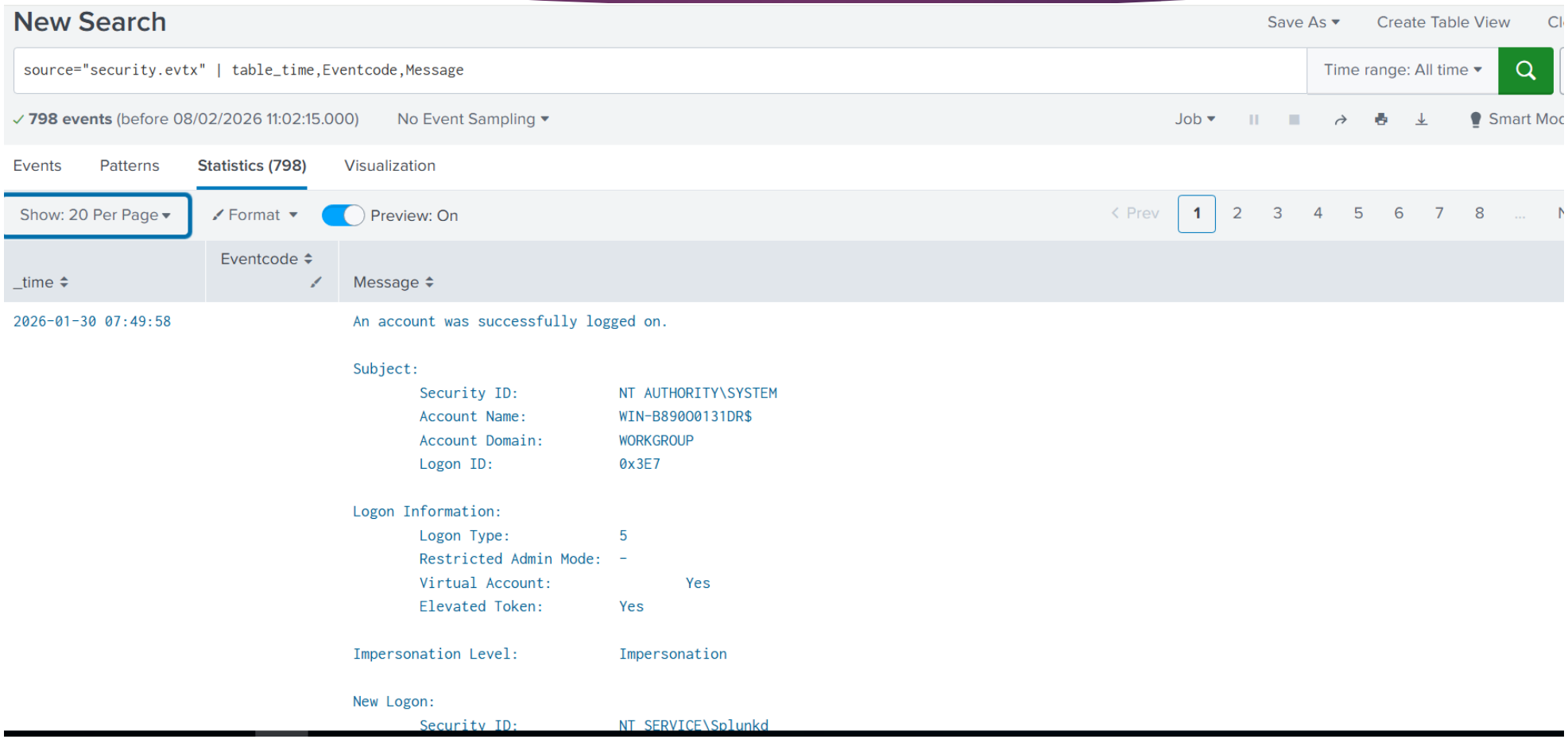


source=" security.evtx" host="WINB89000131DR“
sourcetype="WinEventLog:Security“ | stats count by ComputerName | sort-count

(Sort by ComputeName)

source=" security.evtx" host="WINB89000131DR“
sourcetype="WinEventLog:Security“ | table_time,EventCode,Message

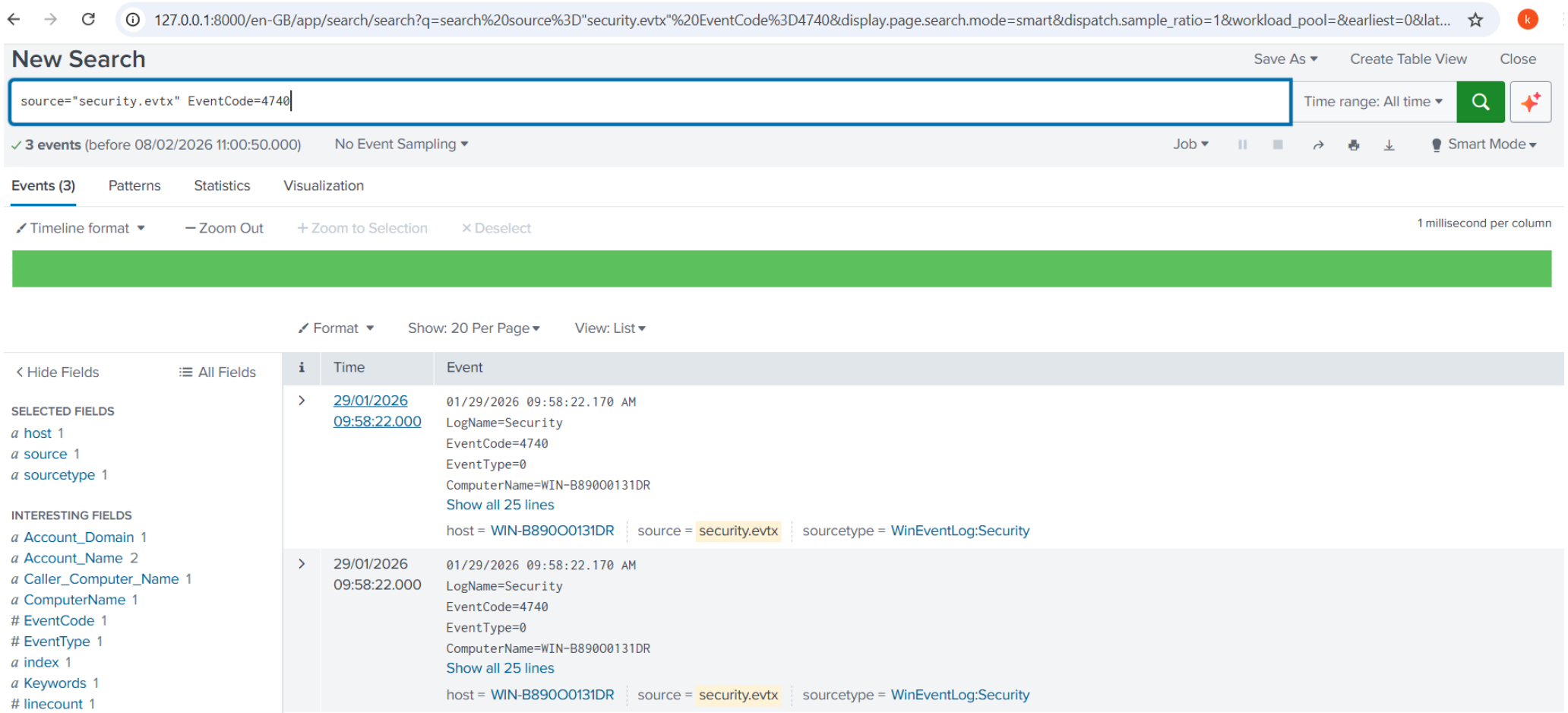
(See Message Details for Each Event)



source=" security.evtx" host="WINB89000131DR“
sourcetype="WinEventLog:Security“ EventCode=4740

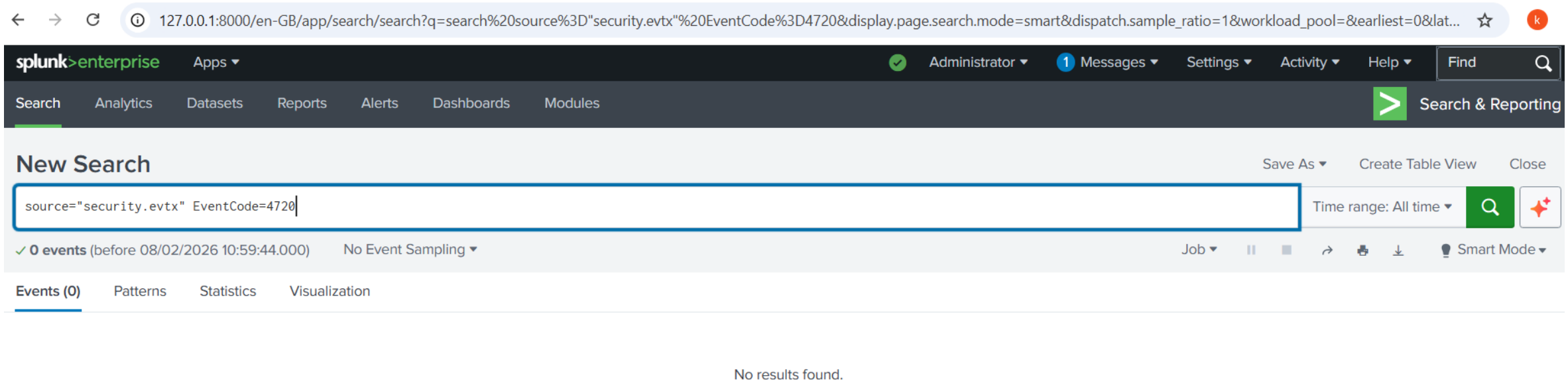
(AccountLockouts)

monitor users who were locked out due to repeated login failures



source=" security.evtx" host="WINB89000131DR“
sourcetype="WinEventLog:Security“ EventCode=4720

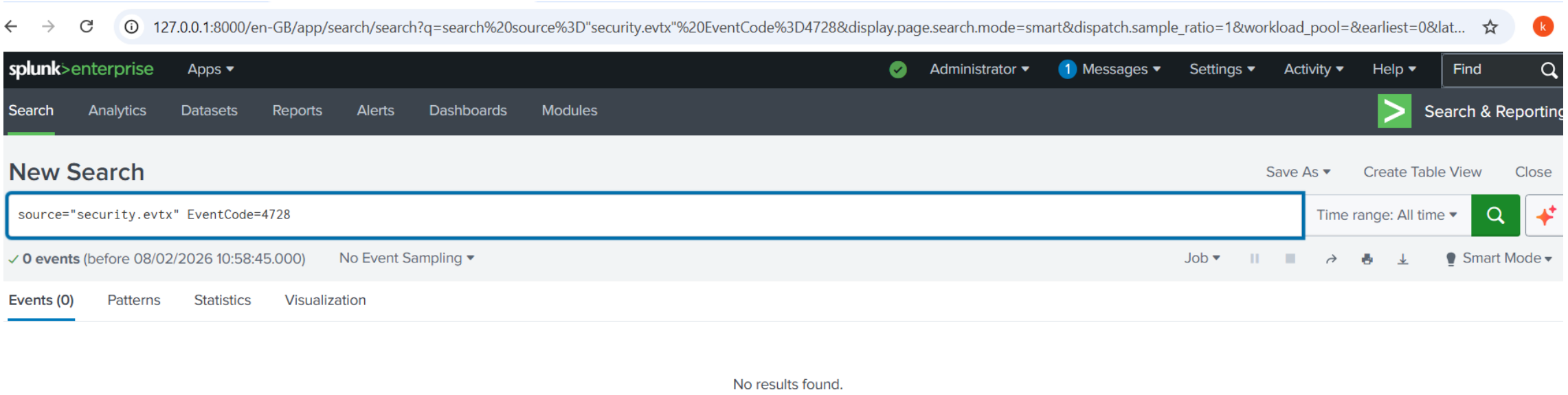
(New Users Creation)



source=" security.evtx" host="WINB89000131DR“
sourcetype="WinEventLog:Security“ EventCode=4728

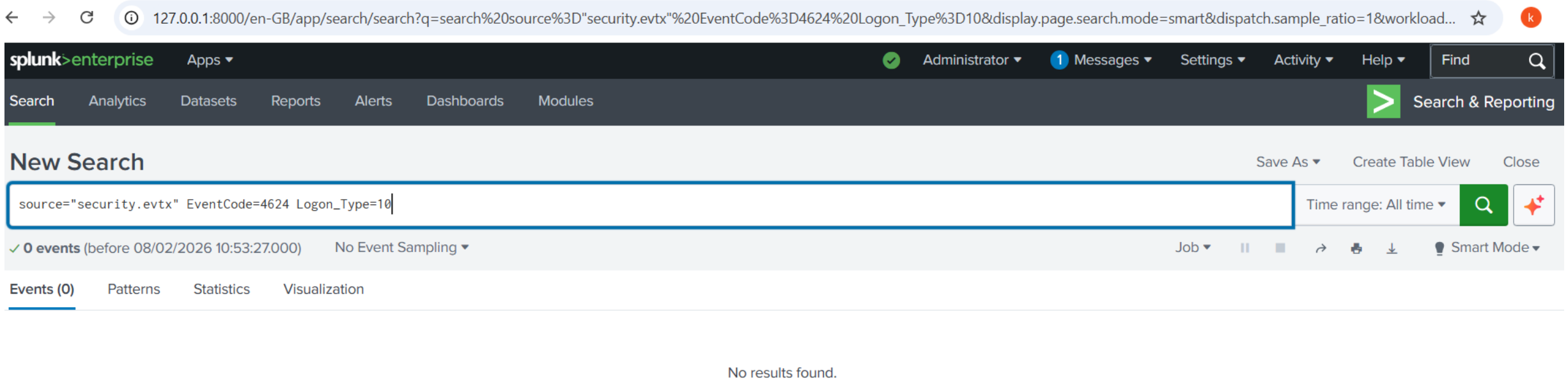
(User Added to Admin Group)

Alert on privilege escalation attempts.



source=" security.evtx" host="WINB89000131DR“
sourcetype="WinEventLog:Security“ EventCode=4624 Logon_Type=10

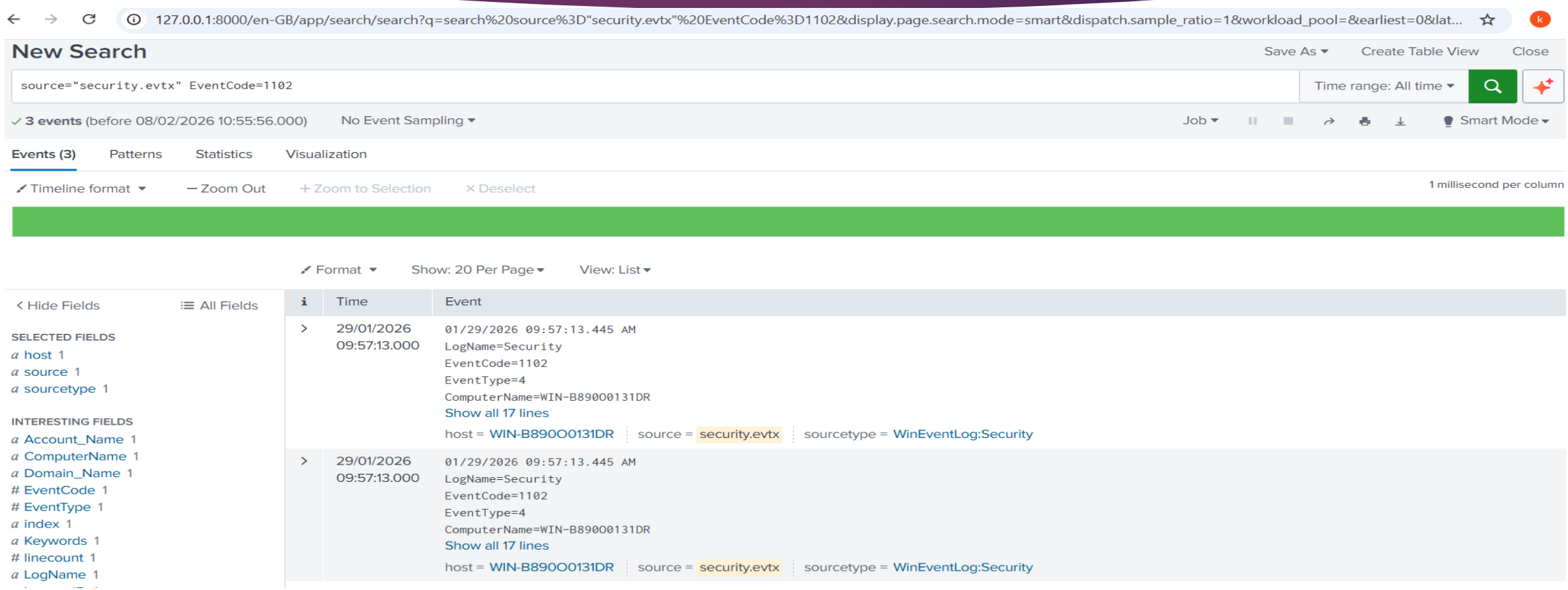
(Remote Logon Detection)



source=" security.evtx" host="WINB89000131DR“
sourcetype="WinEventLog:Security“ EventCode=1102

(Clearing of EventLogs)

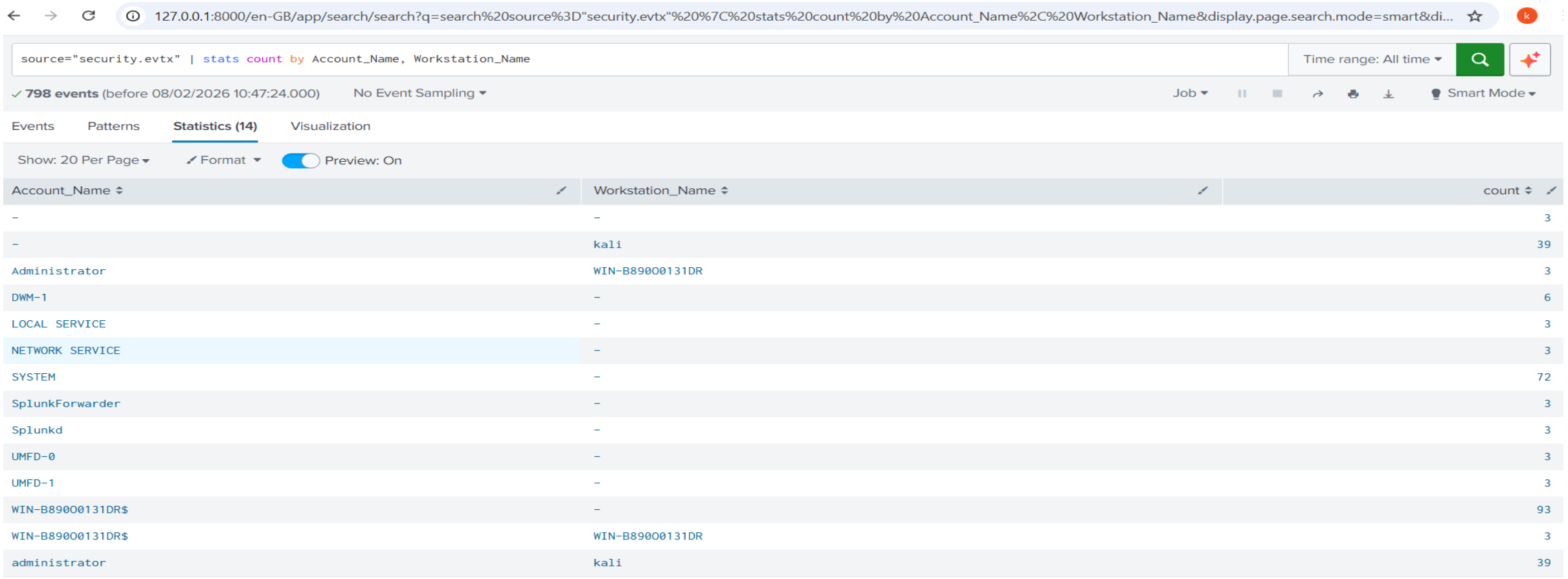
suspicious:someone tried to cover their tracks by clearing logs.



source=" security.evtx" host="WINB89000131DR“sourcetype="WinEventLog:Security“ EventCode=4625 | stats count by Account_Name,Workstation_Name

(Top Failed Logins)

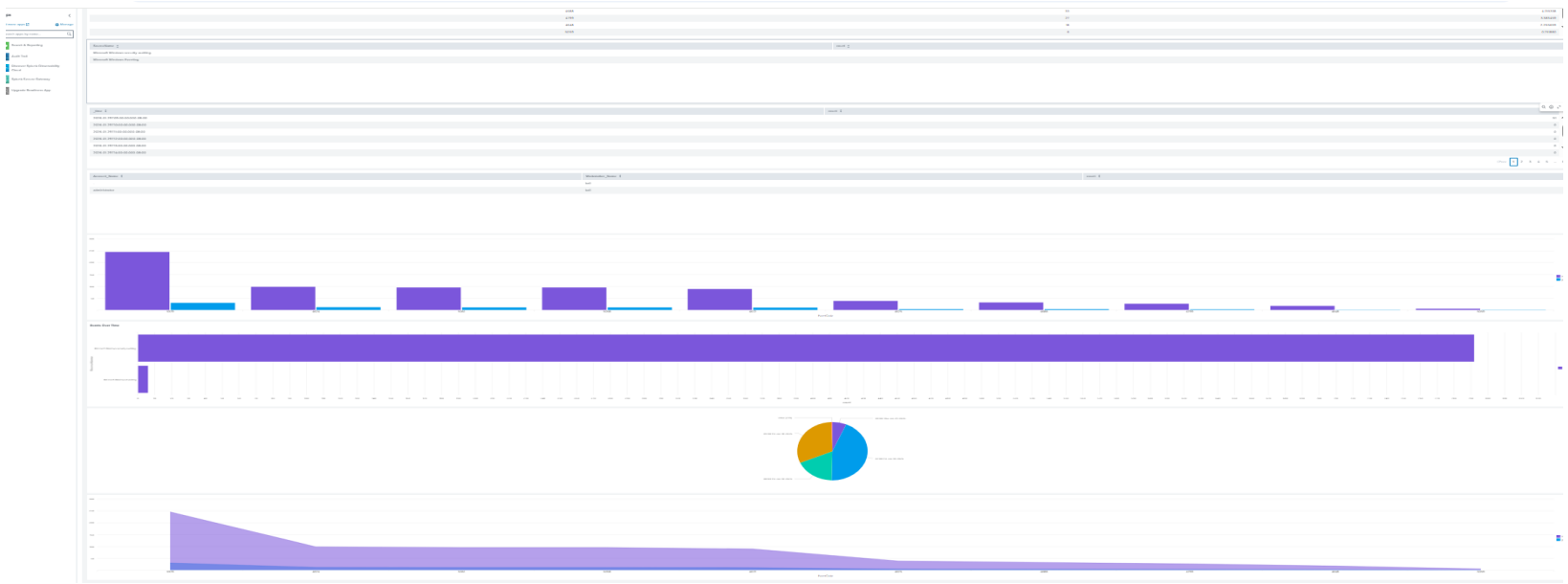
see which users or systems are generating the most failures



Account_Name	Workstation_Name	count
-	-	3
-	kali	39
Administrator	WIN-B890O0131DR	3
DWM-1	-	6
LOCAL SERVICE	-	3
NETWORK SERVICE	-	3
SYSTEM	-	72
SplunkForwarder	-	3
Splunkd	-	3
UMFD-0	-	3
UMFD-1	-	3
WIN-B890O0131DR$	-	93
WIN-B890O0131DR$	WIN-B890O0131DR	3
administrator	kali	39

Security Monitoring Dashboard

- This dashboard was created to monitor brute-force failed login attempts in real-time.
- It visualizes security logs collected from Windows Server using Splunk SIEM.



Conclusion

- Successfully simulated brute-force attack in controlled lab environment
- Generated and analyzed Windows Security logs (Event ID 4625)
- Detected suspicious login activity using SPL queries
- Designed a real-time security monitoring dashboard
- Demonstrated practical understanding of SIEM implementation