SOC LAB

I built this Splunk SOC home lab to get hands-on experience with how a SIEM actually operates in a real SOC-style environment. The goal was to investigate **Windows Authentication & Identity log dataset**

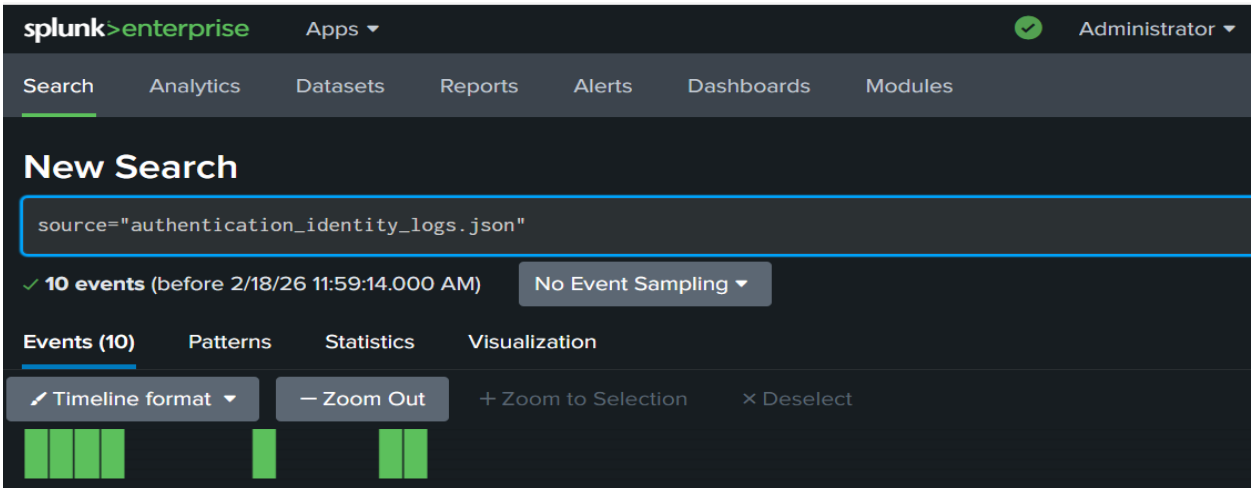
This lab focuses on defensive security, SIEM operations, and incident investigations

The task performed includes

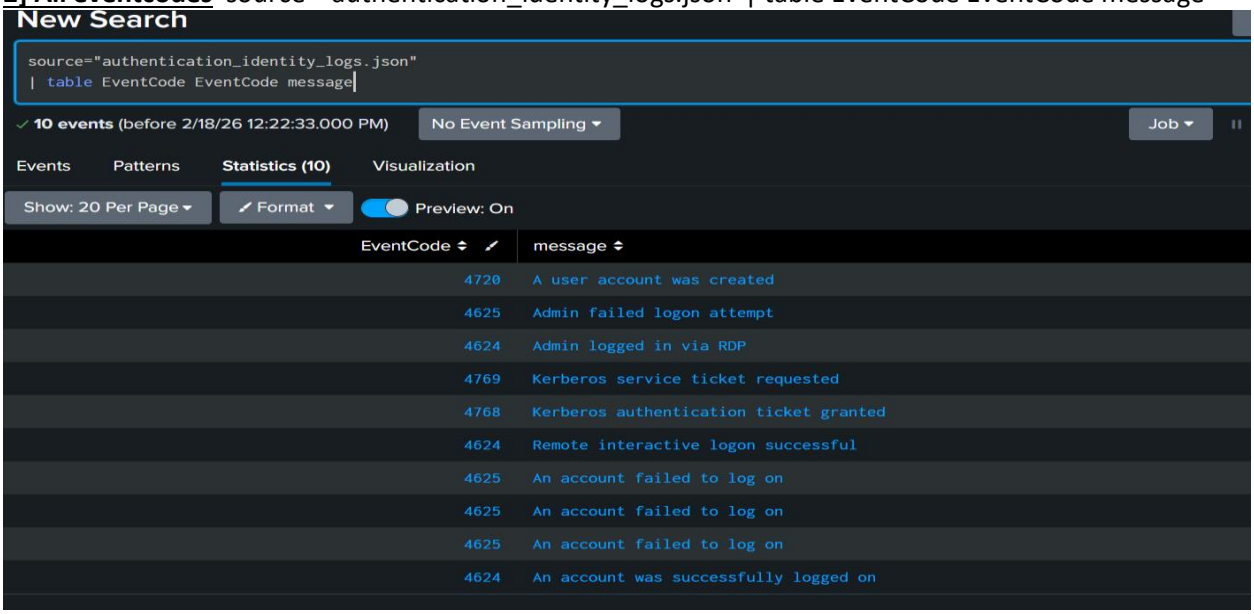
Identify Failed Login Attempts
Detect Brute-Force Behavior
Detect Logins from External / Unusual IPs

Success login
compromised admin access
Remote desktop login

1] all logs source="authentication_identity_logs.json"

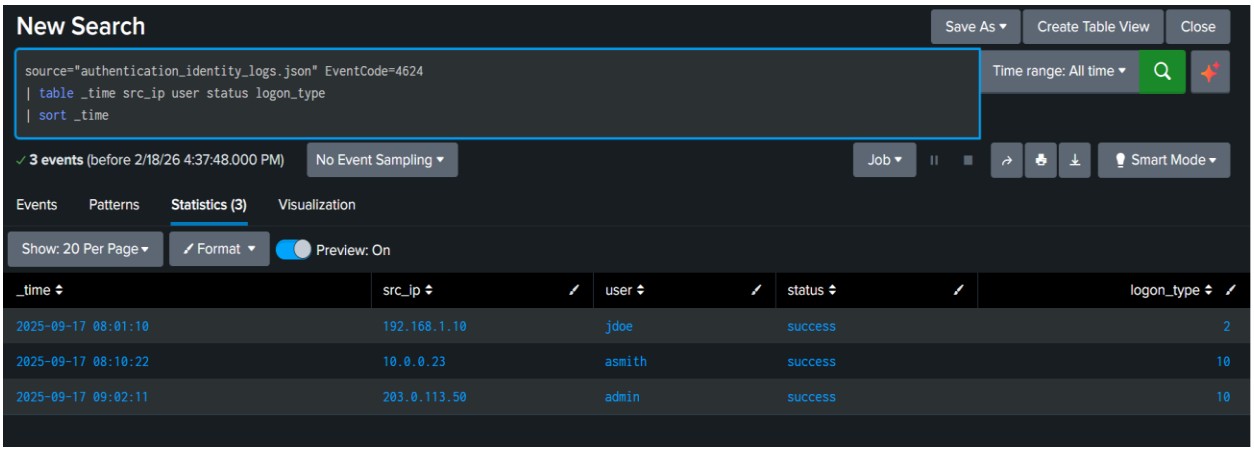


2] All eventcodes source="authentication_identity_logs.json"| table EventCode EventCode message



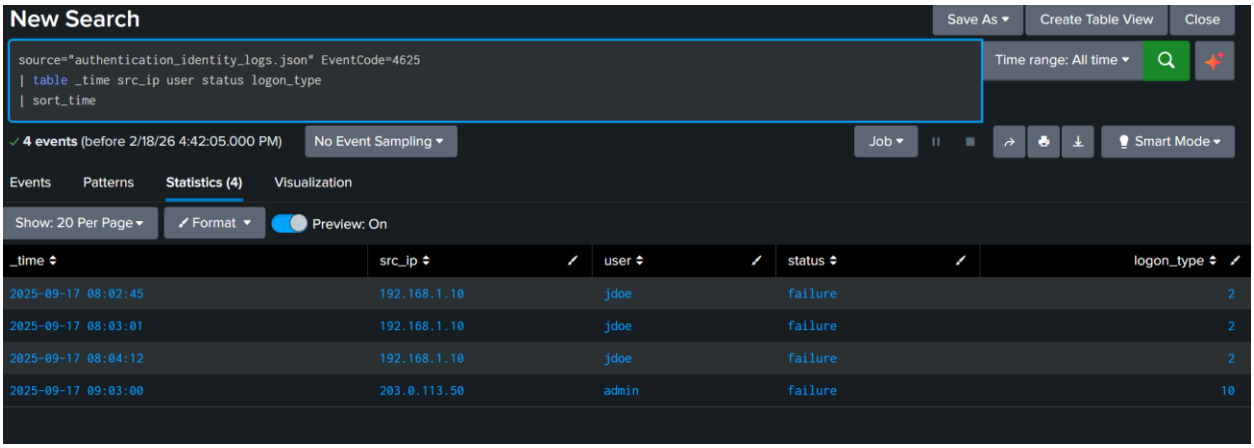
- `4624` – Successful logins
- `4625` – Failed logins
- `4768 / 4769` – Kerberos activity
- `4720` – Account creation

3] Success login source="authentication_identity_logs.json" EventCode=4624
| table _time src_ip user status logon_type
| sort _time



Look for suspicious login

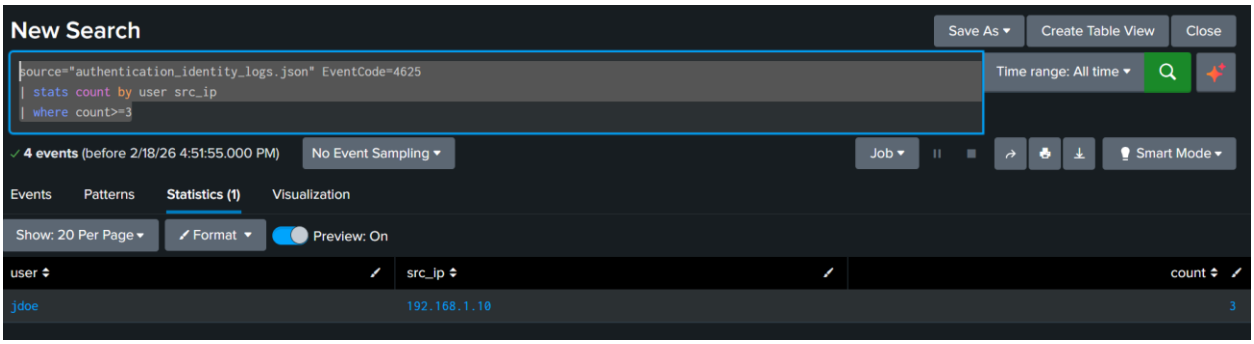
4] Failed login source="authentication_identity_logs.json" EventCode=4625
| table _time src_ip user status logon_type
| sort_time



- Check same user + same IP
- Look for multiple failures in short time

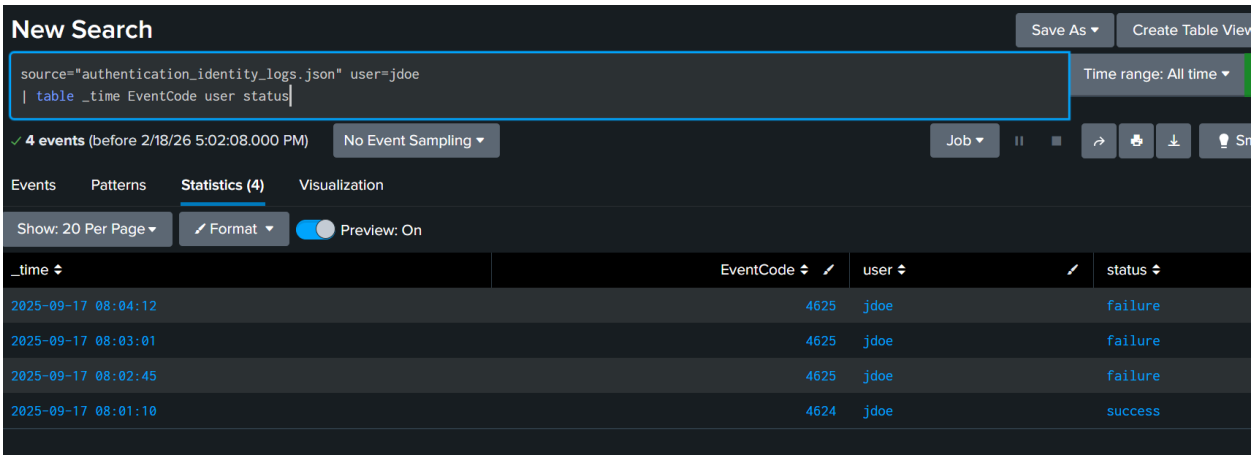
5] Identify multiple failed logins from same source. source="authentication_identity_logs.json" EventCode=4625| stats count by user src_ip

6] Possible brute force attack. source="authentication_identity_logs.json" EventCode=4625
| stats count by user src_ip
| where count>=3



- User `jdoe`
- IP `192.168.1.10`
- Multiple failures → **suspicious**

7]See if attacker eventually logged in. source="authentication_identity_logs.json" user=jdoe
| table _time EventCode user status

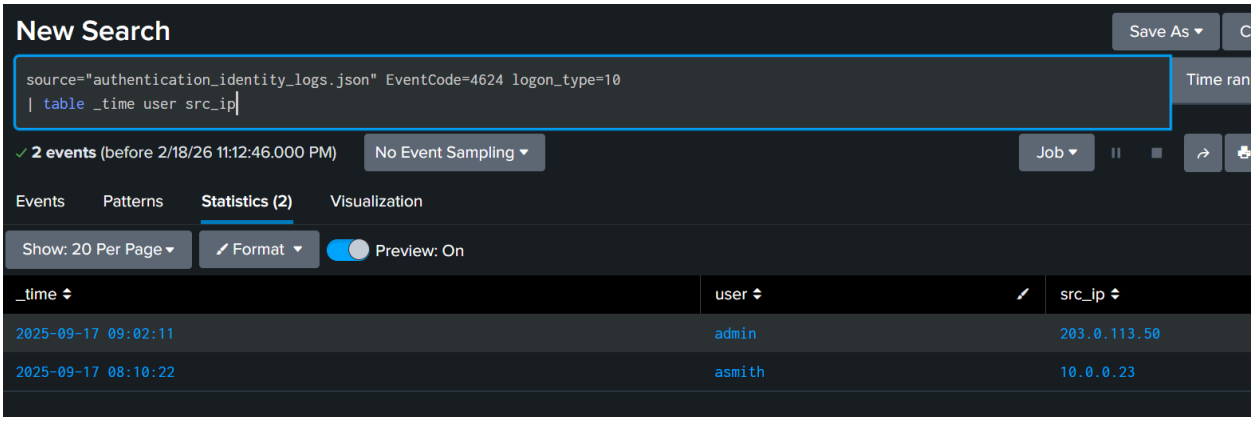


- Failures followed by `4624` success?
- Same IP?
- Escalate if yes

8] Spot possible compromised admin access. source="authentication_identity_logs.json" EventCode=4624
| where like(src_ip,"203.%") OR like(src_ip,"198.%")
| table _time user src_ip logon_type

- `admin` logged in from `203.0.113.50`
- External IP + Admin + RDP = **HIGH RISK**

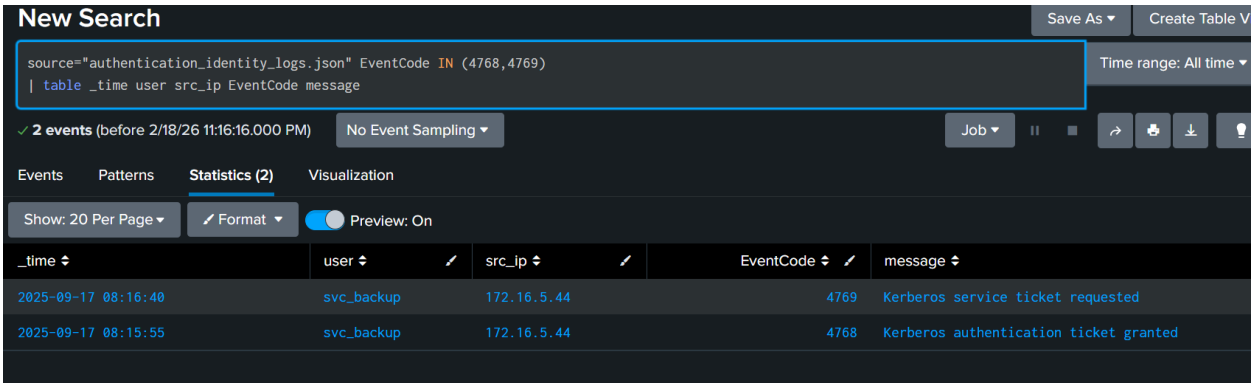
9] Investigate Remote Desktop Logins (RDP Abuse). source="authentication_identity_logs.json" EventCode=4624 logon_type=10
| table _time user src_ip



Logon Type 10 = **Remote Interactive (RDP)**

10]Monitor Kerberos Authentication Activity.
Goal: Detect service account abuse.
SOC Notes:
Service accounts (`svc_backup`) should:
Log in from **known IPs**
Have **predictable behavior**

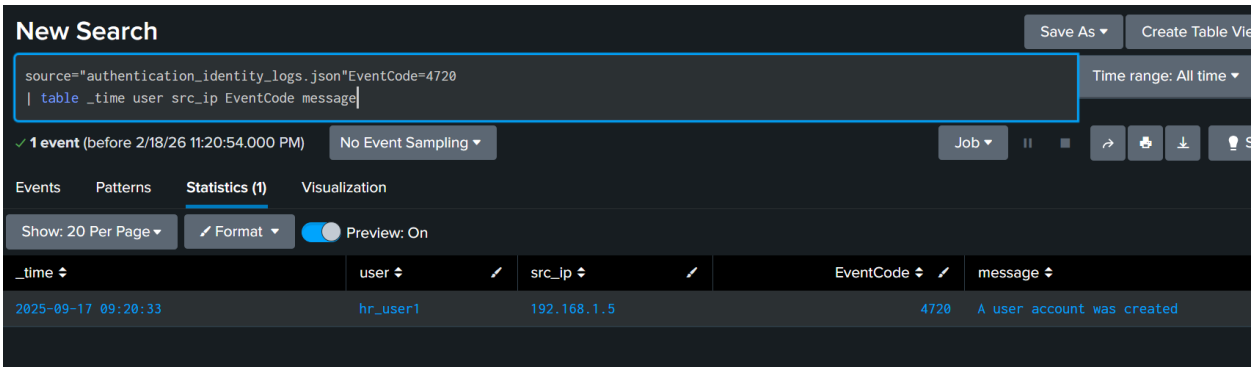
source="authentication_identity_logs.json" EventCode IN (4768,4769)
| table _time user src_ip EventCode message



11]Detect New User Account Creation.

Goal: Catch unauthorized identity creation.

source="authentication_identity_logs.json"EventCode=4720
| table _time user src_ip EventCode message



.....

- Confirm with IAM / HR
- If unauthorized → **Immediate escalation**