

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"

The screenshot shows the Splunk 'New Search' interface. The search bar contains the query `source="authentication_identity_logs.json"`. Below the search bar, it indicates '10 events (before 2/18/26 11:59:14.000 AM)' and 'No Event Sampling'. The 'Events (10)' tab is selected, showing a timeline visualization with green bars. The top navigation bar includes 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', 'Dashboards', and 'Modules'. The user is logged in as 'Administrator'.

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

The screenshot shows the Splunk 'New Search' interface with the query `source="authentication_identity_logs.json" | table EventCode EventCode message`. It indicates '10 events (before 2/18/26 12:22:33.000 PM)' and 'No Event Sampling'. The 'Statistics (10)' tab is selected, showing a table of results. The table has two columns: 'EventCode' and 'message'. The 'Preview: On' toggle is enabled.

EventCode	message
4720	A user account was created
4625	Admin failed logon attempt
4624	Admin logged in via RDP
4769	Kerberos service ticket requested
4768	Kerberos authentication ticket granted
4624	Remote interactive logon successful
4625	An account failed to log on
4625	An account failed to log on
4625	An account failed to log on
4624	An account was successfully logged on

- 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

New Search Save As Create Table View Close

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

Time range: All time Q +

✓ 3 events (before 2/18/26 4:37:48.000 PM) No Event Sampling Job II ■ ↶ ↷ ↓ Smart Mode

Events Patterns **Statistics (3)** Visualization

Show: 20 Per Page Format Preview: On

_time	src_ip	user	status	logon_type
2025-09-17 08:01:10	192.168.1.10	jdoe	success	2
2025-09-17 08:10:22	10.0.0.23	asmith	success	10
2025-09-17 09:02:11	203.0.113.50	admin	success	10

Look for suspicious login

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

New Search Save As Create Table View Close

source="authentication_identity_logs.json" EventCode=4625
 | table _time src_ip user status logon_type
 | sort _time

Time range: All time Q +

✓ 4 events (before 2/18/26 4:42:05.000 PM) No Event Sampling Job II ■ ↶ ↷ ↓ Smart Mode

Events Patterns **Statistics (4)** Visualization

Show: 20 Per Page Format Preview: On

_time	src_ip	user	status	logon_type
2025-09-17 08:02:45	192.168.1.10	jdoe	failure	2
2025-09-17 08:03:01	192.168.1.10	jdoe	failure	2
2025-09-17 08:04:12	192.168.1.10	jdoe	failure	2
2025-09-17 09:03:00	203.0.113.50	admin	failure	10

- 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

New Search

source="authentication_identity_logs.json" EventCode=4625
| stats count by user src_ip

Time range: All time

4 events (before 2/18/26 4:48:10.000 PM) No Event Sampling

Events Patterns Statistics (2) Visualization

Show: 20 Per Page Format Preview: On

user	src_ip	count
admin	203.0.113.50	1
jdoe	192.168.1.10	3

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

New Search

source="authentication_identity_logs.json" EventCode=4625
| stats count by user src_ip
| where count>=3

Time range: All time

4 events (before 2/18/26 4:51:55.000 PM) No Event Sampling

Events Patterns Statistics (1) Visualization

Show: 20 Per Page Format Preview: On

user	src_ip	count
jdoe	192.168.1.10	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

New Search

source="authentication_identity_logs.json" user=jdoe
| table _time EventCode user status

Time range: All time

4 events (before 2/18/26 5:02:08.000 PM) No Event Sampling

Events Patterns Statistics (4) Visualization

Show: 20 Per Page Format Preview: On

_time	EventCode	user	status
2025-09-17 08:04:12	4625	jdoe	failure
2025-09-17 08:03:01	4625	jdoe	failure
2025-09-17 08:02:45	4625	jdoe	failure
2025-09-17 08:01:10	4624	jdoe	success

- 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

New Search

```
source="authentication_identity_logs.json" EventCode=4624
| where like(src_ip,"203.%") OR like(src_ip,"198.%")
| table _time user src_ip logon_type
```

Time range: All time

1 event (before 2/18/26 11:04:45.000 PM)

Events Patterns **Statistics (1)** Visualization

Show: 20 Per Page Format Preview: On

_time	user	src_ip	logon_type
2025-09-17 09:02:11	admin	203.0.113.50	10

- 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

New Search

```
source="authentication_identity_logs.json" EventCode=4624 logon_type=10
| table _time user src_ip
```

Time range: All time

2 events (before 2/18/26 11:12:46.000 PM)

Events Patterns **Statistics (2)** Visualization

Show: 20 Per Page Format Preview: On

_time	user	src_ip
2025-09-17 09:02:11	admin	203.0.113.50
2025-09-17 08:10:22	asmith	10.0.0.23

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

New Search Save As ▾ Create Table View

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

Time range: All time ▾

✓ 2 events (before 2/18/26 11:16:16.000 PM) No Event Sampling ▾ Job ▾ ▮ → 📄 ⬇ 💡

Events Patterns **Statistics (2)** Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

_time ▾	user ▾	src_ip ▾	EventCode ▾	message ▾
2025-09-17 08:16:40	svc_backup	172.16.5.44	4769	Kerberos service ticket requested
2025-09-17 08:15:55	svc_backup	172.16.5.44	4768	Kerberos authentication ticket granted

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

New Search Save As ▾ Create Table View

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

Time range: All time ▾

✓ 1 event (before 2/18/26 11:20:54.000 PM) No Event Sampling ▾ Job ▾ ▮ → 📄 ⬇ 💡

Events Patterns **Statistics (1)** Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

_time ▾	user ▾	src_ip ▾	EventCode ▾	message ▾
2025-09-17 09:20:33	hr_user1	192.168.1.5	4720	A user account was created

.....

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