Windows Login Monitoring with Real-Time Alerting in Splunk

📌 Project Overview

Build a mini SOC (Security Operations Center) project using Splunk to monitor Windows login activity, detect suspicious behavior, and trigger real-time alerts based on key Event Codes.

🎯 Objective

Provide visibility into login attempts (successful, failed, RDP, off-hours, etc.), privileged access, account modifications, and generate alerts for potential threats.

🏁 Setup Steps

🔽 Install Splunk Enterprise

- Download: https://www.splunk.com
- Install on local Windows 10 machine
- Access at: http://localhost:8000

🔄 Install Splunk Universal Forwarder

- Forward Windows Event Logs from the same or another machine
- Configure `inputs.conf` and `outputs.conf`

✅ Verify Data Ingestion

```
index=wineventlog
```

Ensure events like 4624, 4625, 4672 are visible.

📊 Dashboard: “Windows Login Monitoring”

Short Description:

Real-time visibility into login attempts and account activities across Windows systems.

Detailed Description:

This dashboard provides a centralized view of Windows login patterns, failed attempts, RDP brute-force detection, privileged access, off-hours logins, and user account changes. Integrated real-time alerts allow quick SOC-level response.

Dashboard Panels

1. **Failed Login Attempts (4625)**

```
index=wineventlog EventCode=4625
| stats count by host, Account_Name, Workstation_Name
```

Column Chart — Brute force detection.

2. **Successful Login Attempts (4624)**

```
index=wineventlog EventCode=4624
| stats count by Account_Name, host
```

Column Chart — Authorized logins overview.

3. **Failed RDP Login Attempts by Host**

```
index=wineventlog EventCode=4625 Logon_Type=10
| stats count by host, Account_Name
```

Column Chart — Failed remote logins.

4. **Brute Force Attempts by IP**

```
index=wineventlog EventCode=4625
| stats count by Account_Name, host
| where count > 5
```

Column Chart — Suspicious repeated failures.

5. **Privileged Logins (4672)**

```
index=wineventlog EventCode=4672
| stats count by Account_Name, host
```

Column Chart — Admin/sensitive access.

6. **Logon Type Breakdown (4624)**

```
index=wineventlog EventCode=4624
| stats count by Logon_Type
```

Pie Chart — Console, RDP, network logins.

7. Top Failed Login Accounts

```
index=wineventlog EventCode=4625
| stats count by Account_Name
| sort - count
```

Bar Chart — Top failed users.

8. Unusual Login Times

```
index=wineventlog EventCode=4624
| eval hour=strftime(_time, "%H")
| search hour < "06" OR hour > "20"
| stats count by Account_Name, hour
```

Bar Chart — Off-hour logins.

9. Password Reset Attempts (4724)

```
index=wineventlog EventCode=4724
| table _time, host, Target_Username, Subject_Username
```

Table — Password reset monitoring.

10. User Account Disabled (4725)

```
index=wineventlog EventCode=4725
| table _time, Target_Username, Subject_Username, host
```

Table — Account deactivation.

11. User Account Enabled (4722)

```
index=wineventlog EventCode=4722
| table _time, Target_Username, Subject_Username, host
```

Table — Account re-enabling.

12. Real-Time Alert Status Panel

```
index=_internal sourcetype="scheduler" status=failure
| timechart count by savedsearch_name
```

Line Chart — Track failing/successful alerts.

13. Summary Panel

```
index=wineventlog (EventCode=4624 OR EventCode=4625)
| timechart count by EventCode
```

Line Chart — Login trends over time.

🚨 Real-Time Alerts

Privileged Login Alert

- SPL:

```
index=wineventlog EventCode=4672
```

- Trigger: Count > 0 in 60 min
- Trigger For: Each result
- Throttle: By Account_Name for 60 minutes

Brute Force Detection Alert

- SPL:

```
index=wineventlog EventCode=4625
| stats count by Account_Name, host
| where count > 5
```

- Trigger: Count > 0 in 15 min
- Trigger For: Each result
- Throttle: By Account_Name for 30 minutes
