Lab Report Scenario 5: Detect Hidden User Account Creation and Privilege Escalation (T1136)

Objective

Detect when a new user account is created outside business hours or added directly to admin groups.

Attack Steps

- Create a user: net user support1 Password123! /add
- Add user to admins: net localgroup administrators support1 /add

Events to Monitor

- **4720**: User account created
- **4728** or **4732**: User added to privileged group

Detection Rule

Alert if:

- User created **outside business hours** (before 9 AM or after 6 PM) OR
- User added to privileged group anytime

Query

(event.code:"4720" or event.code:"4732" or event.code:"4728") and (NOT (event.time >= "09:00:00" and event.time <= "18:00:00"))

Email Alert Subject

Alert: Suspicious User Account Created Outside Business Hours

Results

- Created user at 8 PM → Alert triggered
- Added user to admins → Alert triggered
- Created user at 10 AM → No alert (inside business hours)

Conclusion

This detects suspicious user creation outside work hours and any direct admin group additions, helping catch hidden admin accounts.