Internship Report: Scenario 2

Suspicious Logon Times – After-Hours Admin Activity (T1078.004)

Objective

To detect privileged account logins occurring outside defined business hours (9 AM to 7 PM UTC), indicating potential unauthorized access.

Attack Chain

- A privileged user (e.g., Administrator, domain admin, or Machine1) logs into the system at an unusual hour (e.g., 2:30 AM).
- The user accesses sensitive folders or services during this session.
- The goal is to alert on such off-hours activity for security monitoring.

Detection Methodology

- Monitoring Windows Security Event ID **4624** representing successful logons.
- Filtered by LogonType:
  - **2** = Interactive logon
  - **10** = Remote Desktop logon
- Focused on privileged user accounts by matching usernames and checking user privilege flags.
- Applied time-based filtering to only detect logons occurring outside the time window 09:00 to 19:00 UTC.
- Utilized **KQL (Kibana Query Language)** for query and alert creation in Elastic Cloud SIEM.

Query Used

```
event.code: "4624" AND (

winlog.event_data.LogonType: 2 OR winlog.event_data.LogonType: 10

) AND (

  user.name: "Administrator" OR user.name: "admin" OR user.name: "domain admin" OR user.name: "Machine1"

) AND NOT (

  @timestamp >= now/d+9h AND @timestamp < now/d+19h

)
```

Testing & Results

- Simulated a login by user **Machine1** at 8.55 AM , outside business hours.
- The Elastic Cloud alert system detected and triggered an alert for this suspicious login.
- Matched login events during testing, confirming the detection logic works as intended.

Conclusion

This scenario demonstrates effective detection of after-hours privileged logins using Elastic Cloud SIEM. The use of correlation logic and time-based filtering helps monitor suspicious activity, improving security posture.