Title: Threat Hunting Report ("Unauthorized privilege escalation in domain accounts").

Date: 24 Nov 2025
Prepared by: Mayuri Sawle

1. Hunting Hypothesis

Hypothesis: "An attacker may have gained unauthorized privileged access using compromised domain credentials, leading to suspicious privilege escalation events."

Elastic Security Query (Event ID 4672 – Special Privilege Assigned)

Timestamp	User	Event ID	Notes
2025-08-18 15:00:00	testuser	4672	Unexpected admin role
2025-08-18 15:05:12	tempadmin	4672	Privilege assigned outside normal hours
2025-08-18 15:09:44	service01	4672	Service account privilege anomaly

2. Threat Intelligence Hunt

AlienVault OTX Search:

- Query for T1078 indicators (compromised credentials, suspicious IPs, brute-force sources).
- Example IOCs retrieved:
    - 185.244.25.91 (known credential-stuffing source)

Findings:

- Suspicious PowerShell executing encoded commands
- LSASS access attempts by non-admin user testuser
- Process tree indicates possible credential theft attempt

3. Summart 100-Word Hunting Report (MITRE ATT&CK T1078)

Report:
Unauthorized privilege escalation activity was detected through Event ID 4672 logs in Elastic Security, revealing anomalous admin role assignments for multiple accounts. AlienVault OTX identified related T1078 IOCs, including malicious IPs associated with credential compromise campaigns. These findings align with MITRE ATT&CK technique **T1078 (Valid Accounts)**, suggesting that threat actors may have used compromised credentials to escalate privileges and move laterally within the environment. Further account lockdown, IOC blocking, and password resets are recommended.