Threat Hunting Practice – Privilege Escalation (T1078)

Threat hunting is a proactive SOC activity focused on identifying suspicious behaviors that may not trigger traditional alerts. In this exercise, a hypothesis-driven hunting approach was used to detect potential misuse of valid accounts within the environment.

Hunting Hypothesis

Hypothesis: Unauthorized privilege escalation is occurring in domain user accounts, potentially indicating credential compromise or insider misuse.

This hypothesis focuses on detecting abnormal assignment of elevated privileges, which attackers often leverage to maintain persistence and perform lateral movement.

Log Query and Analysis

To validate the hypothesis, authentication and privilege assignment logs were analyzed in Elastic Security. Windows **Event ID 4672**, which indicates special privileges assigned to a user during logon, was queried to identify abnormal behavior.

Timestamp	User	Event ID	Notes
2025-08-18 15:00:00	testuser	4672	Unexpected admin role

Analysis of the logs revealed that the user *testuser*, who is not part of the standard administrative group, received elevated privileges unexpectedly. This behavior deviates from normal access patterns and supports the hunting hypothesis.

Threat Intelligence–Driven Hunt

Threat intelligence was used to further validate the findings. AlienVault OTX was consulted to review indicators and attack patterns related to **MITRE ATT&CK technique T1078 (Valid Accounts)**. This technique is commonly associated with attackers abusing legitimate credentials to evade detection.

To correlate endpoint behavior, Velociraptor was used to review running processes using the query:

```
SELECT * FROM processes
```

This helped identify unusual processes running under the affected user context, strengthening suspicion of credential misuse.

Hunting Report (Summary)

The threat hunting activity identified suspicious privilege escalation associated with a domain user account. Analysis of Event ID 4672 showed that a non-administrative user was granted elevated privileges unexpectedly. Threat intelligence mapping linked this behavior to MITRE ATT&CK technique T1078, indicating potential misuse of valid credentials. Endpoint process review supported the hypothesis of abnormal user activity. Although no confirmed breach was detected, the findings justify continued monitoring and deeper investigation.