Threat Hunting Report

1. Executive Summary

A threat hunt was performed to investigate potential unauthorized privilege escalation in the environment. Elastic Security flagged Windows Event ID 4672 for the user vboxuser, which typically indicates elevated privileges being assigned. Initial concern suggested possible misuse of valid credentials. For in-depth analysis Elastic Security, Velociraptor, and AlienVault OTX was used.

2. Alert & Timeline

Timestamp	User	Event ID	Notes
2025-12-25 15:00:00	vboxuser	4672	Unexpected admin role

Table 1: Alert

Time (UTC)	Event / Action
2025-12-25 15:00:00	Event ID 4672 detected
2025-12-25 15:02:00	PowerShell launched by vboxuser
2025-12-25 15:03:00	PowerShell executed harmless system query
2025-12-25 15:05:00	OTX search returned 0 threat matches
2025-12-25 15:10:00	Activity confirmed as benign

Table 2: Timeline

3. Endpoint Validation

- PowerShell.exe spawned from a normal parent process.
- Executed benign commands like Get-Process and Get-Item.
- No lateral movement indicators.

4. Threat Intelligence Review (AlienVault OTX)

- No IPs, domains, hashes, or campaigns matched any artifacts from the environment.
- No overlap between event metadata and known threat indicators.

5. MITRE ATT&CK Mapping

Technique	Name	Relevance
T1078	Valid Accounts	Initial hypothesis; disproven
T1059.001	PowerShell	PowerShell used, but benign

Table 3: MITRE

6. Summary

A threat hunt was conducted to investigate potential misuse of valid accounts following detection of Windows Event ID 4672, which indicates special privileges assigned at logon. Initial findings showed an unexpected privilege assignment, raising concern for possible credential abuse aligned with MITRE ATT&CK T1078 (Valid Accounts). Further analysis of correlated logon and process creation events revealed that the user vboxuser legitimately escalated privileges to launch PowerShell for benign system queries. Threat intelligence checks returned no relevant Indicators of Compromise, and endpoint validation confirmed normal process behavior. The activity was determined to be legitimate, with no evidence of malicious use of valid credentials.