

Threat Hunting Summary

Hunting for MITRE T1078 in Wazuh logs.
Detected unauthorized account usage.
Action: Escalated for further investigation.