document 4: Threat Hunting Summary (Task 2.4)

A. Document Name
Task 2: Threat Hunting Summary

B. Purpose
This document highlights the findings of threat hunting performed for MITRE ATT&CK technique **T1078 – Valid Accounts**, which focuses on detecting misuse or brute-force attempts against valid user credentials.

C. Summary
Threat hunting for **T1078 (Valid Accounts)** in Windows logs confirmed around **50 failed login attempts** against a privileged user account within a short time frame. This pattern indicates a possible **credential brute-force attack**, requiring **account lockout** and a **review of access controls** to prevent unauthorized system access.