TASK 5: SIMULATE COMMUNICATION WITH STAKEHOLDERS

Simulated SOC Analyst Message

[SOC Analyst - Moses]
:warning: Heads-up: We've detected multiple login failed events for **user david** from external IP 203.0.113.77.

This IP has also triggered **file access** and **malware alerts** earlier today, which raises the risk level.

Recommending we:

- Lock or reset bob's account
- Block 203.0.113.77 at firewall or add to watchlist
- Review surrounding logs for potential compromise

Event timestamp: 2025-07-03 07:44:14
Severity: **Medium**