TASK 5: SIMULATE COMMUNICATION WITH STAKEHOLDERS

Subject: Multiple Failed Login Attempts for User "david"

Hi Manager,

We've observed repeated failed login attempts for user david, originating from a public IP 203.0.113.77. The event was detected at 2025-07-03 09:02:14 and is classified as **Medium severity**.

Notably, this IP has also been associated with file access and malware alerts, raising concern of a coordinated attack or compromised device.

Recommended actions:

- Lock or reset credentials for david
- Block or monitor traffic from 203.0.113.77
- Investigate other events from this IP for lateral movement

Please advise on escalation or further containment steps.

Best regards,
MOSES ADJEWODA
SOC Intern, Future SOC Team