Subject: Multiple login failures for the same User - 0365 | Unknown Severity | Non-Actionable | host_51

Hi Team,

Multiple login failures for the same User - 0365 detected from 220.156.84.144 to 160.166.248.64.

Security Alert Details:

SOC Analyst Triage Comments:

- The alert is of medium severity, indicating a potential issue that requires attention.
- Activity between source IP 220.156.84.144 and destination IP 160.166.248.64 was flagged.
- Further analysis is necessary to determine if this is a false positive or a legitimate threat.

Verifications Required:

Review associated logs to verify the legitimacy of the activity.

Recommended Next Steps:

Monitor the situation and follow up with additional checks if necessary.

Sincerely,

SOC Team