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 indicates a potentially serious security issue.
- The activity was detected between source IP 220.156.84.144 and destination IP 160.166.248.64.
- Immediate investigation is required to determine the cause and mitigate any potential damage.

Verifications Required:

Review related logs for anomalies and potential misconfigurations.

Recommended Next Steps:

Initiate incident response protocols and isolate affected systems if necessary.

Sincerely,

SOC Team