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 suggests a high severity issue that could indicate a security breach.
- The event was detected from source IP 220.156.84.144 to destination IP 160.166.248.64.
- Immediate action is recommended to mitigate any potential threat.

Verifications Required:

Check the network traffic logs for any unusual activity.

Recommended Next Steps:

Isolate affected systems and conduct a thorough investigation.

Sincerely,

SOC Team