Subject: Multiple login failures for the same User - Windows | Unknown Severity | Non-Actionable | host_78

Hi Team,

Multiple login failures for the same User - Windows detected from 174.8.117.222 to 69.146.196.41.

Security Alert Details:

SOC Analyst Triage Comments:

- The alert is of medium severity, indicating a potential issue that requires attention.
- Activity between source IP 174.8.117.222 and destination IP 69.146.196.41 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