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 suggests a high severity issue that could indicate a security breach.
- The event was detected from source IP 174.8.117.222 to destination IP 69.146.196.41.
- 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