Subject: Multiple login failures for the same User | Unknown Severity | Non-Actionable | host_4

Hi Team,

Multiple login failures for the same User detected from 41.234.160.62 to 105.253.27.136.

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 41.234.160.62 to destination IP 105.253.27.136.

- 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