Subject: Multiple login failures for the same User - Windows | Medium | Non-Actionable | host_57

Hi Team,

Multiple login failures for the same User - Windows detected from 136.67.219.152 to 153.108.153.144.

Security Alert Details:

SOC Analyst Triage Comments:

- This alert indicates Medium severity, which may not pose an immediate risk.
- The event was triggered from IP address 136.67.219.152 targeting 153.108.153.144, possibly indicating routine maintenance or a benign action.
- Further investigation is recommended to determine if this is a false positive or requires attention.

Verifications Required:

Review logs for anomalies and potential misconfigurations.

Recommended Next Steps:

Monitor the situation and ensure task disabling was intentional.

Sincerely,

SOC Team