Subject: Users or Group Add Operation Detected by User | Medium | Non-Actionable | host_95

Hi Team,

Users or Group Add Operation Detected by User detected from 226.8.247.216 to 39.39.4.252.

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 226.8.247.216 targeting 39.39.4.252, 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