Subject: Users or Group Add Operation Detected by User | Unknown Severity | Non-Actionable | host_79

Hi Team,

Users or Group Add Operation Detected by User detected from 116.50.42.87 to 204.159.41.37.

Security Alert Details:

SOC Analyst Triage Comments:

- The alert is of medium severity, indicating a potential issue that requires attention.

- Activity between source IP 116.50.42.87 and destination IP 204.159.41.37 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