

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 indicates a potentially serious security issue.
- The activity was detected between source IP 116.50.42.87 and destination IP 204.159.41.37.
- Immediate investigation is required to determine the cause and mitigate any potential damage.

Verifications Required:

Review related logs for anomalies and potential misconfigurations.

Recommended Next Steps:

Initiate incident response protocols and isolate affected systems if necessary.

Sincerely,

SOC Team