

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 suggests a high severity issue that could indicate a security breach.
- The event was detected from source IP 116.50.42.87 to destination IP 204.159.41.37.
- 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