Subject: Users or Group Add Operation Detected by User | High | 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 High severity, suggesting a potential security risk.
- The event was triggered from IP address 226.8.247.216 targeting 39.39.4.252, possibly indicating suspicious activity.
- Immediate action is recommended. This may involve isolating affected systems, performing root cause analysis, and reviewing access controls.

Verifications Required:

Check server logs for unauthorized access or misconfiguration.

Recommended Next Steps:

Investigate further and apply necessary mitigations.

Sincerely,

SOC Team