

Subject: User Added to Office 365 Administrator Role | High | Actionable | host\_18

Hi Team,

User Added to Office 365 Administrator Role detected from 55.231.39.179 to 219.162.167.8.

Security Alert Details:

SOC Analyst Triage Comments:

- This alert indicates High severity, suggesting a potential security risk.
- The event was triggered from IP address 55.231.39.179 targeting 219.162.167.8, 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