

Subject: User Added to Office 365 Administrator Role | Medium | Non-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 Medium severity, which may not pose an immediate risk.
- The event was triggered from IP address 55.231.39.179 targeting 219.162.167.8, possibly indicating routine maintenance or a benign action.
- Further investigation is recommended to determine if this is a false positive or requires attention.

Verifications Required:

Review logs for anomalies and potential misconfigurations.

Recommended Next Steps:

Monitor the situation and ensure task disabling was intentional.

Sincerely,

SOC Team