

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 breach.
- The event was triggered from IP address 55.231.39.179 targeting 219.162.167.8, indicating unusual network activity.
- Immediate response is needed to isolate the affected systems and perform a detailed analysis.

Verifications Required:

Investigate network traffic logs and check for unauthorized access.

Recommended Next Steps:

Isolate affected systems and conduct a thorough investigation.

Sincerely,

SOC Team