

Subject: User Added to Office 365 Administrator Role | Unknown Severity | Non-Actionable |
host_35

Hi Team,

User Added to Office 365 Administrator Role detected from 182.196.107.140 to 189.241.57.139.

Security Alert Details:

SOC Analyst Triage Comments:

- The alert is of medium severity, indicating a potential issue that requires attention.
- Activity between source IP 182.196.107.140 and destination IP 189.241.57.139 was flagged.
- Further analysis is necessary to determine if this is a false positive or a legitimate threat.

Verifications Required:

Review associated logs to verify the legitimacy of the activity.

Recommended Next Steps:

Monitor the situation and follow up with additional checks if necessary.

Sincerely,

SOC Team