

#### Alert: User Added to Office 365 Administrator Role

##### GPT-4 Analysis:

- Severity: High
- Actionability: Actionable
- Endpoint Name: host\_16
- Short Description: User Added to Office 365 Administrator Role detected from 181.42.146.47 to 4.21.49.101.
- Analyst Comments:
  - This alert indicates High severity, suggesting a potential security risk.
  - The event was triggered from IP address 181.42.146.47 targeting 4.21.49.101, 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.
- Next Steps: Investigate further and apply necessary mitigations.
- Team Name: SOC Team

##### GPT-3.5 Analysis:

- Severity: Medium
- Actionability: Non-Actionable
- Endpoint Name: host\_16
- Short Description: User Added to Office 365 Administrator Role detected from 181.42.146.47 to 4.21.49.101.
- Analyst Comments:
  - This alert indicates medium severity, which may not pose an immediate risk.
  - The event was triggered from IP address 181.42.146.47 targeting 4.21.49.101, 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.
- Next Steps: Monitor the situation and ensure task disabling was intentional.
- Team Name: SOC Team

##### LLaMA-3 Analysis:

- Severity: High
- Actionability: Actionable
- Endpoint Name: host\_16
- Short Description: User Added to Office 365 Administrator Role detected from 181.42.146.47 to 4.21.49.101.
- Analyst Comments:
  - This alert indicates High severity, suggesting a potential security breach.
  - The event was triggered from IP address 181.42.146.47 targeting 4.21.49.101, 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.
- Next Steps: Isolate affected systems and conduct a thorough investigation.
- Team Name: SOC Team