Subject: Mass file download by single user - O365 remotely access 4 new assets | Medium | Non-Actionable | host_31

Hi Team,

Mass file download by single user - O365 remotely access 4 new assets detected from 131.47.25.70 to 130.176.66.246.

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 131.47.25.70 targeting 130.176.66.246, 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