Subject: Mass file download by single user - O365 remotely access 4 new assets | High | 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 High severity, suggesting a potential security breach.
- The event was triggered from IP address 131.47.25.70 targeting 130.176.66.246, 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