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 risk.
- The event was triggered from IP address 131.47.25.70 targeting 130.176.66.246, 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.

Recommended Next Steps:

Investigate further and apply necessary mitigations.

Sincerely,

SOC Team