**BLUF:**

Extremely brief bottom line up front. 1-2 sentences ideally, of the single take-away the reader needs to understand from the rest of the report.

**Background / Observations**

**Analysis / Predictions**

**Conclusion and Recommendations:**

# Example:

BLUF: [Organization] is experiencing a higher than industry average targeting of cloud administrator credentials which poses an increase risk to sensitive crown jewel assets in our cloud environments.

Observations:

* [Organization] is targeted by credential theft attempts more that healthcare and pharmaceutical industry average per Proofpoint TAP
* Credential theft attempts are trending upwards for the past two quarters per Proofpoint TAP
* Cloud-conscious threat actors are focused on obtaining credentials for administrators (Mandiant, Crowdstrike, HHS)
* "Cloud Services" is one of the top departments that receive malicious emails in their inboxes per Proofpoint TAP
* Credential phishing continued to inboxes through attachments is a low-priority Proofpoint alert for the SOC

Predictions:

* [Organization] is experiencing an increased threat pressure focused on credential theft, using campaigns which are using sophisticated enough campaigns to make it past or security controls and target cloud technology administrators. While a significant portion are blocked by Proofpoint TAP security controls, there are campaigns which are being delivered to user's inboxes observed in the past quarter.  [Organization] playbooks for SOC response currently have these delivered emails with malicious attachments for credential phishing at an extremely low priority for investigation, which increases the time possible for a user to be successfully attacked before malicious emails are removed. This represents an increased risk to [Organization] which is likely to *continue*to increase over time. Moderate confidence of an exposure of cloud administrative credentials within the next year if not mitigated.

Security Strategy Recommendation for Mitigations:

* Consider targeting the Cloud Services team for enhanced security training regarding phishing, MFA fatigue, MFA bombing, SIM swamping protection
* Evaluate the cloud administrators and digital workplace platform services team’s email security rules for potential improvements
* Add additional playbooks for investigating phishing email attachments which have been continued to user’s inboxes