Observations:

* Observations at the org
* Observations of the threat landscape
* Observations on trends in TTPS
* Observations that are sector or vertical specific

Observations should tell a story about

* Threat pressure
* Threat actor TTPs including targeting, goals and sophistication
* Security control performance
* Impact (if known)

Predictions:

* Each prediction should be tied to one or observations

Recommendations:

* Should speak to steps that could be taken to change the prediction confidence levels or outcomes

*Example of a made up Strategic Intel Report using this format:*

**Observations:**

* [Organization] is targeted by credential theft attempts more that healthcare industry average, indicating an increased threat pressure focused on credential theft
* Unauthorized access accounts for the most incident types at [Organization]
* The threat landscape shows cloud-conscious threat actors are focused on obtaining credentials for administrators
* [Cloud Administrator team] is one of the top departments that receive malicious emails in their inboxes
* Exposed credentials and data exposure investigations account for 2% of incident investigations conducted by Security Operations Teams

**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 technology administrators. We expect to see a continuation (high confidence) of this behavior at a higher threat pressure than industry average.
* [Organization] playbooks for SOC response currently do not include emails with malicious attachments, and exposure credentials and data exposure investigations at an extremely low priority. We expect that this gap in our security processes will result within a Sev 3-4 incident within 12-18 months.
* There is no enhanced security training required for cloud engineers with critical administrative access. This represents an increased risk to [Organization] experiencing a Sev1 incident impacting our cloud environment.

**Security Strategy Recommendation:**

* Consider targeting the [Cloud Administrator team] team for enhanced security training regarding MFA fatigue, MFA bombing, SIM swamping protection
* Evaluate the cloud administrators team’s messaging security rules in our email security appliance for risk reduction improvements
* Add additional playbooks for investigating malicious email attachments which have been continued to user’s inboxes for the SOC, which include removing the malicious emails from user’s inboxes quickly to reduce risk of a high severity incident