Contents

[6.8] Pairing Hope Fantasies (baP)

1. Operational Definition: Based on Bion's Basic Assumption Pairing (baP), this is the unconscious group belief that a future event, technology, or hire ("the silver bullet") will solve all current security problems. This manifests as continuous research and acquisition of new tools without fully implementing or mastering existing ones, and a delay in addressing current issues.

2. Main Metric & Algorithm:

- **Metric:** Tool Utilization Score (TUS). Formula: `(Number of actively used features of a tool) / (Total number of available features)`.
- **Pseudocode:**

  python

  ```
  def calculate_tus(tool_audit_list):
      """
      tool_audit_list: A list for each tool, with a count of features configured/used.
      """
      total_available_features = 0
      total_used_features = 0
      for tool in tool_audit_list:
          total_available_features += tool.total_features
          total_used_features += tool.used_features
      return total_used_features / total_available_features
  ```

- **Alert Threshold:** `TUS < 0.4` (Less than 40% of purchased tool capabilities are being used).

3. Digital Data Sources (Algorithm Input):

- **SIEM/SOAR/EDR API:** Audit logs and configuration endpoints to check for enabled features vs. available features.
- **CMDB:** List of owned security tools and their licensing tiers (which often map to features).
- **Project Management Tools:** Tickets related to evaluating new tools vs. tickets for enhancing use of existing tools.

4. Human-To-Human Audit Protocol: In a strategy meeting, ask: "In the last year, what has given us the biggest security improvement: a new tool we purchased, or a new process or use case we implemented with an existing tool?" Catalogue all major tools and have the team honestly score their utilization level.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Before any new tool evaluation, require a formal review of the existing toolstack to identify if the need can be met by improving the use of current capabilities.
- **Human/Organizational Mitigation:** Shift the measure of success for security engineers from "evaluated X new tools" to "unlocked Y new features in our existing platform."

- **Process Mitigation:** Implement a "capability maturity model" for each major tool. Define what "full utilization" looks like and create a roadmap to get there before greenlighting new purchases.