Contents

[8.9] Collective Unconscious Patterns

1. Operational Definition: The manifestation of deeply ingrained, species-wide predispositions within an organization's security culture, leading to universal but often suboptimal reactions to threats (e.g., innate fear of snakes/spiders translating to an overemphasis on certain malware types).

2. Main Metric & Algorithm:

- **Metric:** Threat Focus Disparity (TFD). Formula: `TFD = (Resources_Allocated_to_Archetypal_Threats / (Resources_Allocated_to_Actual_Prevalent_Threats)`.
- **Pseudocode:**

  python

  ```
  def calculate_tfd(org_id, start_date, end_date):
      # 1. Define archetypal vs. prevalent threats (requires expert input)
      archetypal_threats = ['ransomware', 'apt', 'zero-day', 'insider']
      prevalent_threats = get_top_threats_from_intel(org_id, 10)  # e.g., ['phishing', 'conf

      # 2. Measure resources allocated to each (e.g., spending, tooling, analyst time)
      # This is a complex proxy metric. Example: count of alerts worked per category.
      arch_alerts = query_alert_count(archetypal_threats, start_date, end_date)
      prev_alerts = query_alert_count(prevalent_threats, start_date, end_date)

      # 3. Calculate a simple ratio
      total_arch = sum(arch_alerts.values())
      total_prev = sum(prev_alerts.values())
      tfd = total_arch / total_prev if total_prev > 0 else float('inf')
      return tfd
  ```

- **Alert Threshold:** `TFD > 2.0` (Spending more than twice the resources on archetypal vs. prevalent threats).

3. Digital Data Sources (Algorithm Input):

- **SIEM:** Alert logs categorized by threat type.
- **Ticketing System:** Time tracking on incidents per category.
- **Finance/Procurement:** Data on security tool and service spending per threat category.

4. Human-to-Human Audit Protocol: Conduct a workshop with security leadership. Present data on the actual threat landscape faced by the organization versus the allocation of resources. Ask: "Why do we think there is a disparity? What fears or ingrained beliefs might be influencing our investment strategy?"

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Use a data-driven threat intelligence platform to regularly report on the *actual* top threats to the organization and automatically compare them to control allocations.

- **Human/Organizational Mitigation:** Hire or consult with threat intelligence analysts who can provide an objective, data-driven view of the threat landscape.
- **Process Mitigation:** Integrate a mandatory "threat landscape review" into the annual security budgeting process, requiring justification for investments that deviate significantly from the actual prevalent threats.