Contents

[6.7] Fight-Flight Security Postures (baF) 1

[6.7] Fight-Flight Security Postures (baF)

1. Operational Definition: Based on Bion's Basic Assumption Fight/Flight (baF), this is the group's unconscious response to anxiety by either aggressively fighting a perceived external enemy ("We must block everything!") or fleeing/avoiding the threat ("This is too complex, we can't defend against it"). This leads to overly aggressive, brittle blocking policies or, conversely, learned helplessness and inaction.

2. Main Metric & Algorithm:

- **Metric:** Binary Rule Ratio (BRR). Formula: `(Number of security rules with action=BLOCK) / (Total number of security rules)`.
- **Pseudocode:**

  python

  ```
  def calculate_brr(firewall_rules, waf_rules, edr_rules):
      total_block = 0
      total_rules = 0
      for rule_set in [firewall_rules, waf_rules, edr_rules]:
          for rule in rule_set:
              total_rules += 1
              if rule.action == "BLOCK" or rule.action == "DENY":
                  total_block += 1
      return total_block / total_rules
  ```

- **Alert Threshold:** `BRR > 0.9` (Extreme "Fight" posture) OR `BRR < 0.1` (Extreme "Flight" posture, i.e., almost everything is in monitor/alert mode only).

3. Digital Data Sources (Algorithm Input):

- **Firewall Management API (e.g., Palo Alto Panorama):** Data: `rulebase.security.rules -> action`.
- **WAF Management API (e.g., F5 ASM):** Data: `policy.violations -> blocking=true/false`.
- **EDR/XDR Console API (e.g., CrowdStrike):** Data: `ioa.exclusions -> action.taken`.

4. Human-To-Human Audit Protocol: Review the BRR metric with the security architecture team. Ask: "Does this ratio reflect our intended security posture? Are we being too aggressive, leading to business disruption? Or are we being too passive, leaving ourselves exposed? What is the rationale behind each 'alert-only' rule for a critical threat?"

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement a more nuanced posture with tiers of blocking (e.g., block only known-bad, use challenge/rate-limit for suspicious, allow but alert for greyware). Review and refine rulesets quarterly.

- **Human/Organizational Mitigation:** Provide training on the psychological concept of baF to security architects. Encourage a mindset of "resilient defense" rather than "impermeable fortress."
- **Process Mitigation:** Introduce a mandatory business impact assessment for any new blocking rule and a sunset clause for all rules to ensure they are reviewed regularly.