Contents

[6.7] Posture di Sicurezza Fight-Flight (baF)

1. Definizione Operativa: Basato sull'Assunzione Fondamentale Bioniana Fight/Flight (baF), questa è la risposta inconscia del gruppo all'ansia combattendo un nemico esterno percepito ("Dobbiamo bloccare tutto!") o fuggendo/evitando la minaccia ("Questo è troppo complesso, non possiamo difenderci"). Questo porta a politiche di blocco eccessivamente aggressive e fragili o, conversely, a impotenza appresa e inazione.

2. Metrica Principale & Algoritmo:

- **Metrica:** Rapporto di Regola Binaria (BRR). Formula: `(Numero di regole di sicurezza con azione=BLOCK) / (Numero totale di regole di sicurezza)`.
- **Pseudocodice:**

```
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
```

- **Soglia di Allarme:** `BRR > 0.9` (Postura "Fight" estrema) O `BRR < 0.1` (Postura "Flight" estrema, cioè quasi tutto è in modalità solo di monitoraggio/avviso).

3. Fonti Dati Digitali (Input Algoritmo):

- **API di Gestione Firewall (ad es. Palo Alto Panorama):** Dati: `rulebase.security.rules -> action`.
- **API di Gestione WAF (ad es. F5 ASM):** Dati: `policy.violations -> blocking=true/false`.
- **API di Console EDR/XDR (ad es. CrowdStrike):** Dati: `ioa.exclusions -> action.taken`.

4. Protocollo di Audit Umano-a-Umano: Rivedi la metrica BRR con il team di architettura di sicurezza. Chiedi: "Questo rapporto riflette la nostra postura di sicurezza intesa? Siamo troppo aggressivi, portando a disruption aziendale? O siamo troppo passivi, lasciandoci esposti? Quale è la razionale dietro ogni regola"alert-only" per una minaccia critica?"

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementare una postura più sfumata con livelli di blocco (ad es. bloccare solo i malintesi noti, usare challenge/rate-limit per i sospetti, consentire ma avvisare per il greyware). Rivedi e affina i set di regole trimestralmente.
- **Mitigazione Umana/Organizzativa:** Fornire formazione sul concetto psicologico di baF agli architetti di sicurezza. Incoraggiare una mentalità di "difesa resiliente" piuttosto che

"fortezza impermeabile".

- **Mitigazione del Processo:** Introdurre una valutazione obbligatoria dell'impatto aziendale per qualsiasi nuova regola di blocco e una clausola di tramonto per tutte le regole per garantire che siano revisionate regolarmente.