Contents

[6.10] Collective Defense Mechanisms

1. Operational Definition: The unconscious, organization-wide use of psychological defenses (e.g., denial, rationalization, projection) to avoid anxiety associated with security threats. This manifests as a systematic downplaying of risk metrics, attributing breaches solely to "sophisticated nation-states" (projection), or believing "it won't happen to us" (denial).

2. Main Metric & Algorithm:

- **Metric:** Risk Rationalization Ratio (RRR). Formula: `(Number of confirmed true positive alerts) / (Number of alerts initially closed as 'false positive' or 'risk accepted')`.
- **Pseudocode:**

  python

  ```
  def calculate_rrr(alerts):
      true_positives = 0
      rationalized_alerts = 0
      for alert in alerts:
          if alert.final_verdict == "True Positive":
              true_positives += 1
          if alert.initial_closure_reason in ["False Positive", "Risk Accepted", "Not Applic
              rationalized_alerts += 1
      return true_positives / rationalized_alerts if rationalized_alerts > 0 else 0
  ```

- **Alert Threshold:** `RRR > 0.1` (More than 10% of alerts initially dismissed are actually true positives, indicating a pattern of rationalization/denial).

3. Digital Data Sources (Algorithm Input):

- **SIEM/SOAR:** Alert queue. Fields: `initial_closure_reason`, `final_verdict` (from later investigation or pentest findings), `severity`.

4. Human-To-Human Audit Protocol: In a blameless post-incident review meeting for a missed true positive, focus on the initial triage decision. Ask: "What was the thought process behind initially closing this as a non-issue? Was there any pressure, conscious or unconscious, to make the alert queue go down? Did we convince ourselves it was fine because dealing with it would have been difficult?"

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement a mandatory peer review step for closing any high-severity alert as a false positive. Require a second opinion.
- **Human/Organizational Mitigation:** Leadership must actively foster a culture of psychological safety where speaking up about risks and admitting mistakes is rewarded, not punished. Discuss cognitive biases openly.

- **Process Mitigation:** Institute a regular (e.g., quarterly) "alert audit" process where a sample of closed alerts, especially those dismissed as FP, is re-examined by a different team (e.g., Red Team) to validate the conclusions.