Contents

[8.6] Defense Mechanism Interference

1. Operational Definition: The unconscious use of psychological defense mechanisms (e.g., denial, rationalization, projection) that actively interfere with performing security duties, such as dismissing clear evidence of a breach.

2. Main Metric & Algorithm:

- **Metric:** Evidence Dismissal Ratio (EDR). Formula: `EDR = Count_of_Dismissed_High_Confidence_IoCs / Total_High_Confidence_IoCs_Presented`.
- **Pseudocode:**

  python

```
def calculate_edr(analyst_id, start_date, end_date):
    # 1. Query high-confidence Indicators of Compromise (IoCs) from threat intel fed to th
    # (e.g., from Threat Intelligence Platform (TIP) or SIEM alert)
    high_confidence_iocs = query_iocs(confidence_min=85, analyst_id, start_date, end_date)

    # 2. Query the analyst's actions on these IoCs (e.g., dismissed, ignored, ruled out)
    dismissed_iocs = 0
    for ioc in high_confidence_iocs:
        if get_ioc_status(ioc, analyst_id) in ['dismissed', 'ignored', 'false_positive']:
            dismissed_iocs += 1

    # 3. Calculate ratio
    edr = dismissed_iocs / len(high_confidence_iocs) if high_confidence_iocs else 0
    return edr
```

- **Alert Threshold:** `EDR > 0.1` (Dismissing more than 10% of high-confidence threat intelligence).

3. Digital Data Sources (Algorithm Input):

- **Threat Intelligence Platform (TIP):** API to get IoCs (fields `ioc_value`, `ioc_type`, `confidence_score`, `timestamp`).
- **SIEM/SOAR:** Logs of analyst actions on alerts containing these IoCs (fields `user`, `action`, `alert_id`, `ioc_value`).

4. Human-to-Human Audit Protocol: Present the analyst with a recent case where they dismissed a high-confidence IoC in a simulated exercise. Use a cognitive interview technique: "Talk me through your thought process when you saw this indicator. What other possibilities did you consider? What would have needed to be different for you to escalate this?"

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement a "second look" rule in the SOAR: if an analyst dismisses a high-confidence IoC, it is automatically queued for a brief review by another analyst or a senior.

- **Human/Organizational Mitigation:** Integrate training on cognitive biases and defense mechanisms into security awareness programs for SOC analysts.
- **Process Mitigation:** Mandate a "pre-mortem" for major incident closures, where the team briefly assumes the breach *did* happen and must list what evidence they might have missed.