Contents

[5.1] Alert fatigue desensitization

1. Operational Definition: A psychological state of mental exhaustion and reduced reactivity caused by being exposed to a high volume of security alerts, particularly false positives, leading to missed critical threats.

2. Main Metric & Algorithm:

- **Metric:** Missed Critical Alert Rate (MCAR). Formula: `MCAR = (Number of unactioned critical severity alerts) / (Total number of critical severity alerts)`.
- **Pseudocode:**

  python

```
def calculate_mcar(alerts, start_date, end_date, severity='critical'):
    """
    alerts: List of alert objects from SIEM
    """
    # 1. Filter for critical alerts in the time period
    critical_alerts = [a for a in alerts if a.severity == severity and start_date <= a.cre

    # 2. Check the status of each critical alert
    missed_count = 0
    for alert in critical_alerts:
        # An alert is "missed" if it was closed as false positive, ignored, or expired wit
        if (alert.status == 'closed' and alert.resolution == 'false_positive') or \
           (alert.status == 'expired') or \
           (alert.status == 'closed' and alert.time_to_acknowledge > alert.sla):
            missed_count += 1

    # 3. Calculate MCAR
    total_critical = len(critical_alerts)
    MCAR = missed_count / total_critical if total_critical > 0 else 0
    return MCAR
```

- **Alert Threshold:** `MCAR > 0.05` (More than 5% of critical alerts are missed)

3. Digital Data Sources (Algorithm Input):

- **SIEM API (Splunk, Elasticsearch):** Index: `alerts`, Fields: `severity`, `created_time`, `status`, `resolution`, `time_to_acknowledge`, `sla`.
- **SOAR/Ticketing System:** To enrich alert data with resolution notes and final status.

4. Human-to-Human Audit Protocol: Directly observe analysts during their shift. Note their body language and comments when alerts appear. Follow up with a short interview: "How do you decide which alerts to prioritize? Have you noticed yourself paying less attention to the alert queue over time?" Correlate these observations with the MCAR metric.

5. **Recommended Mitigation Actions:**
    - **Technical/Digital Mitigation:** Implement a machine learning-based alert triage system to automatically suppress, aggregate, or de-prioritize likely false positives, reducing the overall volume of noise the analyst sees.
    - **Human/Organizational Mitigation:** Establish a formal alert fatigue monitoring program using this MCAR metric. Rotate analysts regularly between high-volume alert monitoring and other, less repetitive tasks.
    - **Process Mitigation:** Continuously tune and refine SIEM correlation rules based on feedback from analysts on false positives. Make this tuning a documented and weekly recurring task for a dedicated rulesmith.