Contents

[5.1] Desensibilizzazione da affaticamento degli avvisi

1. Definizione operativa: Uno stato psicologico di esaurimento mentale e reattività ridotta causato dall'esposizione a un alto volume di avvisi di sicurezza, in particolare falsi positivi, che porta a minacce critiche mancate.

2. Metrica principale e algoritmo:

- **Metrica:** Tasso di avvisi critici mancati (MCAR). Formula: `MCAR = (Numero di avvisi di severità critica non azionati) / (Numero totale di avvisi di severità critica)`.
- **Pseudocodice:**

```
def calculate_mcar(alerts, start_date, end_date, severity='critical'):
    """
    alerts: Elenco degli oggetti avvisi da SIEM
    """
    # 1. Filtrare gli avvisi critici nel periodo di tempo
    critical_alerts = [a for a in alerts if a.severity == severity and start_date <= a.cre

    # 2. Verificare lo stato di ogni avviso critico
    missed_count = 0
    for alert in critical_alerts:
        # Un avviso è "mancato" se è chiuso come falso positivo, ignorato o scaduto senza
        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. Calcolare MCAR
    total_critical = len(critical_alerts)
    MCAR = missed_count / total_critical if total_critical > 0 else 0
    return MCAR
```

- **Soglia di avviso:** `MCAR > 0.05` (Più del 5% degli avvisi critici sono mancati)

3. Fonti di dati digitali (Input dell'algoritmo):

- **API SIEM (Splunk, Elasticsearch):** Indice: `alerts`, Campi: `severity`, `created_time`, `status`, `resolution`, `time_to_acknowledge`, `sla`.
- **Sistema SOAR/Ticketing:** Per arricchire i dati degli avvisi con note di risoluzione e stato finale.

4. Protocollo di audit uomo-uomo: Osservare direttamente gli analisti durante il turno. Annotare il linguaggio del corpo e i commenti quando appaiono gli avvisi. Seguire con una breve intervista: "Come decidi quali avvisi dare priorità? Hai notato che presti meno attenzione alla coda degli avvisi nel tempo?" Correlare queste osservazioni con la metrica MCAR.

5. Azioni di mitigazione consigliate:

- **Mitigazione tecnica/digitale:** Implementare un sistema di triage degli avvisi basato su machine learning per sopprimere automaticamente, aggregare o deprioritizzare i probabili falsi positivi, riducendo il volume complessivo di rumore che l'analista vede.
- **Mitigazione umana/organizzativa:** Stabilire un programma formale di monitoraggio dell'affaticamento degli avvisi utilizzando questa metrica MCAR. Ruotare regolarmente gli analisti tra il monitoraggio di avvisi ad alto volume e altri compiti meno ripetitivi.
- **Mitigazione dei processi:** Continuamente sintonizzare e affinare le regole di correlazione SIEM in base al feedback degli analisti sui falsi positivi. Rendere questa sintonizzazione un compito ricorrente documentato e settimanale per un rulesmith dedicato.