Contents

[8.2] Identificazione Inconscia con Minacce

1. Definizione Operativa: Uno stato psicologico in cui il personale della sicurezza sviluppa una fascinazione o un allineamento inconscio con le tattiche, le tecniche e le procedure (TTP) degli attori di minaccia, potenzialmente portando a una ridotta vigilanza, a mancati avvisi o addirittura a una facilitazione involontaria degli attacchi.

2. Metrica Principale & Algoritmo:

- **Metrica:** Rapporto di Focus su Attori di Minaccia (TAFR). Formula: `TAFR = (Volume_Ricerca_Termini_Minaccia + Utilizzo_Strumenti) / Attività_Lavoro_Totale`.
- **Pseudocodice:**

```
def calculate_tafr(analyst_id, start_date, end_date):
    # 1. Interroga la cronologia di ricerca interna dell'analista (es. in SIEM, piattaform
    search_terms = query_internal_searches(analyst_id, start_date, end_date)
    threat_searches = filter_searches_for_threat_terms(search_terms, THREAT_ACTOR_KEYWORDS

    # 2. Interroga l'utilizzo di strumenti per gli strumenti di emulazione delle minacce/a
    tool_usage = query_tool_logs(analyst_id, start_date, end_date)
    non_task_tool_usage = filter_usage_without_ticket(tool_usage, THREAT_EMULATION_TOOL_ID

    # 3. Ottieni un proxy per l'attività totale (es. numero di avvisi elaborati, ticket ch
    total_activity = query_ticket_count(analyst_id, start_date, end_date)

    # 4. Calcola il rapporto (il peso può essere regolato)
    tafr = (len(threat_searches) + len(non_task_tool_usage)) / total_activity
    return tafr

# Esempio Soglia
if tafr > 0.15:  # Più del 15% dell'attività è focalizzata su minacce senza compito chiaro
    trigger_alert("High TAFR for analyst: Potential unconscious identification")
```

- **Soglia di Allerta:** `TAFR > 0.15` (Calibra in base all'attività organizzativa della baseline).

3. Fonti Dati Digitali (Input dell'Algoritmo):

- **Piattaforme SIEM/Ricerca:** Log di cronologia di ricerca di Splunk (index `_audit`, campi `user`, `search_query`, `time`). Log di interrogazione di Cortex XSOAR/TIM/Piattaforma Threat Intel.
- **Log di Endpoint/Strumenti:** Log da strumenti amministrativi, piattaforme di VM o sandbox di analisi di malware (es. `user`, `tool_name`, `command_executed`, `timestamp`).
- **Sistema di Ticketing:** API Jira/ServiceNow (progetto `SOC`, campi `assignee`, `created`, `resolved`) per ottenere `total_activity`.

4. Protocollo di Audit Umano-Umano: Condurre un'intervista riservata e non punitiva facilitata da un esperto di cultura della sicurezza. Le domande dovrebbero essere aperte: "Puoi

descrivere un attore di minaccia recente o una tecnica che hai trovato particolarmente interessante o intelligente? Come pensi alle motivazioni degli attaccanti che affrontiamo? Nel tuo parere, qual è il confine tra comprendere una minaccia e simpatizzare con essa?"

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementare il controllo degli accessi basato sui ruoli (RBAC) per garantire che l'accesso a strumenti avanzati di emulazione delle minacce sia concesso solo per compiti specifici e giustificati e sia registrato.
- **Mitigazione Umana/Organizzativa:** Stabilire un programma robusto di cultura della sicurezza che includa discussioni su etica, psicologia degli attori di minaccia e confini chiari. Incoraggiare il mentoring e i check-in regolari.
- **Mitigazione del Processo:** Mantenere la revisione dei pari per qualsiasi attività che coinvolga l'interazione diretta con gli strumenti di emulazione delle minacce o l'accesso ai canali di comunicazione sensibili degli attori di minaccia.