

Contents

[2.7] Finestre di Vulnerabilità Legate all’Ora del Giorno 1

[2.7] Finestre di Vulnerabilità Legate all’Ora del Giorno

1. Definizione Operativa: Periodi prevedibili di ridotto monitoraggio della sicurezza o responsività che si verificano alla stessa ora ogni giorno (es. durante i cambi di turno, le pause pranzo), creando ricorrenti opportunità di attacco.

2. Metrica Principale e Algoritmo:

- **Metrica:** Punteggio dei Gap Ricorrenti (RGS). Formula: $RGS = (\text{N_incidents_during_window} / \text{N_hours_in_window}) / (\text{N_incidents_outside} / \text{N_hours_outside})$.
- **Pseudocodice:**

python

```
def calculate_rgs(incidents, start_time, end_time, analysis_period_days):
    """
    incidents: Lista di incidenti con timestamp.
    window: es. ('11:00', '13:00') per finestra pranzo, o ('08:50', '09:10') per cambio turno
    """
    window_incidents = 0
    outside_incidents = 0
    total_hours_in_window = (end_time - start_time).hours * analysis_period_days
    total_hours_outside = (24 * analysis_period_days) - total_hours_in_window

    for incident in incidents:
        if start_time <= incident.time.time() <= end_time:
            window_incidents += 1
        else:
            outside_incidents += 1

    # Calcolare i tassi di incidenti per ora
    rate_in_window = window_incidents / total_hours_in_window
    rate_outside = outside_incidents / total_hours_outside

    if rate_outside > 0:
        RGS = rate_in_window / rate_outside
    else:
        RGS = float('inf') # Gestire la divisione per zero

    return RGS
```

- **Soglia di Allarme:** $RGS > 1.5$ (Il tasso di incidenti durante la finestra è del 50% più alto del tasso di base).

3. Fonti di Dati Digitali (Input dell’Algoritmo):

- **SIEM (Splunk, Elastic):** Indice notable_events o incidents. Query per `| bucket _time span=1h | stats count by _time`.
 - **SOAR / Ticketing (ServiceNow):** Tabella incident. Campi: opened_at.
 - **Log Active Directory:** Eventi 4768 (Kerberos TGS richiesto) o 4624 (logon), cercando picchi durante le ore fuori orario.
4. **Protocollo di Audit da Persona a Persona:** Esaminare la procedura di passaggio di turno: “Esiste un periodo di sovrapposizione documentato di 15 minuti? Esiste un processo per il monitoraggio durante le pause pranzo? Chi è formalmente responsabile della copertura durante questi momenti?” Osservare un passaggio.

5. **Azioni di Mitigazione Consigliate:**

- **Mitigazione Tecnica/Digitale:** Configurare playbook automatizzati per attivare notifiche di gravità superiore o aggiuntive per gli allarmi rilevati durante le finestre di vulnerabilità note.
- **Mitigazione Umana/Organizzativa:** Implementare turni sovrapposti obbligatori per garantire una copertura continua. Creare una rotazione formale di “copertura pranzo” all’interno del team.
- **Mitigazione dei Processi:** Documentare e far rispettare un protocollo di passaggio di turno rigoroso che includa un briefing verbale e una revisione degli allarmi di alta gravità aperti. Pianificare i patch critici del sistema al di fuori di queste finestre.