

## Contents

[10.10] Lacune di Sicurezza per Isteresi . . . . . 1

### [10.10] Lacune di Sicurezza per Isteresi

**1. Definizione Operativa:** L'effetto di ritardo o persistente di un incidente di sicurezza o di un periodo di stress elevato sul sistema o sul team, dove le prestazioni o la postura di sicurezza non tornano allo stato originale anche dopo che la causa iniziale è stata rimossa.

#### 2. Metrica Principale e Algoritmo:

- **Metrica:** Decadimento delle Prestazioni Post-Incidente (PIPD). Formula:  $PIPD = (MTTA_{Baseline} - MTTA_{Post\_Incidente}) / MTTA_{Baseline}$ . Un valore negativo indica che le prestazioni sono peggiori dopo l'incidente.

- **Pseudocodice:**

```
python

def calculate_pipd(team_id, major_incident_date):
    # Definisci finestre temporali: 30 giorni prima (baseline) e 30 giorni dopo (recupero)
    baseline_start = major_incident_date - timedelta(days=30)
    baseline_end = major_incident_date
    recovery_start = major_incident_date
    recovery_end = major_incident_date + timedelta(days=30)

    # Calcola MTTA per il periodo di baseline
    baseline_mtta = calculate_mtta_team(baseline_start, baseline_end, team_id)

    # Calcola MTTA per il periodo di recupero
    recovery_mtta = calculate_mtta_team(recovery_start, recovery_end, team_id)

    # Calcola la variazione percentuale
    if baseline_mtta > 0:
        pipd = (recovery_mtta - baseline_mtta) / baseline_mtta
    else:
        pipd = 0
    return pipd # ad es. -0,15 significa un rallentamento del 15% dopo l'incidente
```

- **Soglia di Avviso:**  $PIPD < -0,1$  (Degrado delle prestazioni superiore al 10% persiste per un mese dopo un incidente principale).

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

- **SIEM / SOAR:** Per il calcolo dell'MTTA per un team specifico su periodi di tempo definiti.

**4. Protocollo di Audit Umano-Umano:** Conduci una sessione di “lezioni apprese” 4-6 settimane dopo un incidente principale. Vai oltre “cosa è andato male” e chiedi: “Come sta il team ora? Stiamo ancora sentendo gli effetti? Stiamo prendendo decisioni diverse (forse eccessivamente caute) a causa di questo evento?” Questi dati qualitativi rivelano l'isteresi.

#### 5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Usa la metrica PIPD per attivare automaticamente risorse di supporto aggiuntive (ad es. analisti SOC contractor) per i team in recupero da un incidente principale.
- **Mitigazione Umana/Organizzativa:** Fornisci accesso al supporto psicologico professionale o consulenza per i team dopo incidenti critici per mitigare il burnout e il trauma.
- **Mitigazione dei Processi:** Formalizza un processo di recupero post-incidente che includa l'alleggerimento del carico di lavoro, il tutoraggio e un ritorno graduale alle responsabilità complete per il team colpito.