Contents

[6.3] Diffusione della Responsabilità

1. Definizione Operativa: Un fenomeno socio-psicologico in cui gli individui sono meno propensi a intraprendere azioni o sentirsi responsabili di un compito quando credono che anche altri siano responsabili. In un SOC, questo si manifesta come avvisi critici o compiti che rimangono in uno stato non assegnato per periodi prolungati o vengono ripetutamente riassegnati senza azione.

2. Metrica Principale & Algoritmo:

- **Metrica:** Durata dell'Allarme Critico Non Assegnato (UCAD). Formula: `Tempo tra la creazione dell'avviso e l'assegnazione a un proprietario individuale`.
- **Pseudocodice:**

```
def calculate_ucad(alerts, severity='critical'):
    unassigned_critical_alerts = [a for a in alerts if a.severity == severity and a.owner
    total_duration = 0
    for alert in unassigned_critical_alerts:
        time_unassigned = alert.time_now - alert.created_time
        total_duration += time_unassigned
    # Restituire ore medie non assegnate
    return total_duration / len(unassigned_critical_alerts) if unassigned_critical_alerts
```

- **Soglia di Allarme:** `UCAD > 4 (ore)` per avvisi di severità critica.

3. Fonti Dati Digitali (Input Algoritmo):

- **SIEM (Splunk/Elasticsearch):** Indice di allarmi. Campi: `signature` (ad es. "Critical Vulnerability Detected"), `severity`, `created_time`, `owner`.
- **SOAR/Ticketing (ServiceNow, Jira):** Tabelle di Task/Incidenti. Campi: `state` (ad es. "New", "Assigned"), `assignment_group`, `assigned_to`, `sys_created_on`.

4. Protocollo di Audit Umano-a-Umano: Durante una riunione del team, presenta un elenco di tutti gli avvisi che erano non assegnati per più della soglia (4 ore) nell'ultima settimana. Chiedi al team: "Qual era il processo per assegnare questi? Era poco chiaro chi fosse responsabile? Tutti hanno presumo che qualcun altro l'avrebbe raccolto?"

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Configurare la piattaforma SOAR per assegnare automaticamente nuovi avvisi critici a uno specifico analista on-call o a una rotazione primaria/secondaria, eliminando lo stato non assegnato.
- **Mitigazione Umana/Organizzativa:** Definire e documentare chiaramente i grafici RACI (Responsible, Accountable, Consulted, Informed) per diversi tipi di avvisi e procedure di risposta agli incidenti.
- **Mitigazione del Processo:** Implementare un rituale di "audit non assegnato" giornaliero in cui il lead del turno rivede tutti gli elementi non assegnati più vecchi di 1 ora e li assegna esplicitamente, confermando verbalmente l'accettazione.