Contents

[10.8] Imprevedibilità dell'Emergenza

1. Definizione Operativa: L'incapacità di prevedere pattern di attacco nuovi o comportamenti del sistema che emergono (nascono) dall'interazione non lineare di molti componenti semplici all'interno dell'ambiente IT, che non sono prevedibili analizzando i componenti da soli.

2. Metrica Principale e Algoritmo:

- **Metrica:** Tasso di Pattern di Attacco Nuovo (NAPR). Formula: `NAPR = Numero_Incidenti_Con_TTP_Nuov / Incidenti_Totali`.
- **Pseudocodice:**

  python

```
def calculate_napr(start_date, end_date, mitre_attck_dict):
    all_incidents = get_incidents(start_date, end_date)
    novel_incidents = 0

    for incident in all_incidents:
        # Ottieni i TTP attribuiti a questo incidente
        incident_ttps = incident.attributed_ttps
        # Verifica se QUALSIASI TTP non è nel framework MITRE ATT&CK (cioè è nuovo)
        if any(ttp not in mitre_attck_dict for ttp in incident_ttps):
            novel_incidents += 1

    total_incidents = len(all_incidents)
    return novel_incidents / total_incidents if total_incidents > 0 else 0
```

- **Soglia di Avviso:** Un `NAPR > 0` sostenuto è un indicatore. Un picco improvviso è un avviso ad alta priorità.

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

- **Piattaforma di Threat Intelligence / SIEM:** Incidenti arricchiti con codici TTP MITRE ATT&CK (ad es. `T1059.001` per PowerShell).
- **Analisi Umana:** Si affida a threat hunter o analisti del SOC per contrassegnare i TTP come "nuovi" se non corrispondono ai framework esistenti.

4. Protocollo di Audit Umano-Umano: Tieni regolarmente riunioni di threat hunting focalizzate sulla rilevazione di anomalie, non solo sulla corrispondenza di IOC. Chiedi ai hunter: "Quali sono i comportamenti più strani e insoliti che hai visto nei log ultimamente, anche se non hanno scatenato un avviso?" Questo incoraggia la ricerca di pattern emergenti.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Investii in analitiche comportamentali e strumenti User and Entity Behavior Analytics (UEBA) che sono progettati per rilevare anomalie e pattern nuovi, non solo firme note-bad.

- **Mitigazione Umana/Organizzativa:** Dedica tempo ai threat hunter esperti per condurre l'esplorazione dei dati senza ipotesi per cercare pattern emergenti.
- **Mitigazione dei Processi:** Crea un processo formale per creare e distribuire rapidamente nuove regole di rilevamento quando viene scoperto un nuovo TTP, e condividi questa intelligenza con la comunità.