Contents

[10.7] Catastrofe della Complessità

1. Definizione Operativa: Uno stato in cui la complessità dell'ambiente di sicurezza (strumenti, regole, processi) supera la capacità cognitiva umana, portando a interazioni imprevedibili, errori di configurazione e un'incapacità di gestire il sistema in modo efficace.

2. Metrica Principale e Algoritmo:

- **Metrica:** Tasso di Incidenti Causato da Complessità (CIIR). Formula: `CIIR = (Numero_Incidenti_Causati_Da_Errore_Configurazione / Incidenti_Totali) in un periodo di tempo`.
- **Pseudocodice:**

  python

  ```
  def calculate_ciir(start_date, end_date):
      all_incidents = get_incidents(start_date, end_date)
      misconfig_incidents = 0

      for incident in all_incidents:
          # Questo richiede che la causa principale dell'incidente sia contrassegnata
          if incident.root_cause == "Misconfiguration":
              misconfig_incidents += 1

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

- **Soglia di Avviso:** `CIIR > 0,3` (Oltre il 30% degli incidenti è causato da errori di configurazione).

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

- **Piattaforma SOAR / Gestione degli Incidenti:** (ad es. Jira, ServiceNow) con un campo `root_cause` obbligatorio per gli incidenti chiusi. I valori dovrebbero includere "Misconfiguration".

4. Protocollo di Audit Umano-Umano: Intervista gli amministratori di sistema e gli ingegneri cloud: "Quanto sei sicuro che comprendi pienamente l'interazione tra tutte le policy di sicurezza applicate a un sistema? Puoi facilmente tracciare perché una specifica richiesta è stata consentita o bloccata?" Un alto livello di incertezza indica catastrofe della complessità.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementa la scansione di sicurezza Infrastructure as Code (IaC) (ad es. Checkov, Terrascan) e policy-as-code per applicare coerenza e semplicità nelle configurazioni.
- **Mitigazione Umana/Organizzativa:** Crea una "Task Force della Semplicità" con il mandato di dismettere gli strumenti ridondanti e standardizzare le configurazioni in tutto l'ambiente.

- **Mitigazione dei Processi:** Introduci una valutazione dell'impatto della complessità obbligatoria per l'acquisto di qualsiasi nuovo strumento di sicurezza o la creazione di qualsiasi nuova policy di sicurezza.