Contents

[1.10] Escalation dell'autorità in crisi

1. Definizione operativa: Durante una crisi di sicurezza confermata o percepita, il trasferimento automatico e spesso non contestato dell'autorità decisionale all'individuo di livello più alto presente, potenzialmente aggirando i protocolli di risposta agli incidenti stabiliti e i consigli di esperti.

2. Metrica principale e algoritmo:

- **Metrica:** Frequenza di bypass del protocollo durante gli incidenti (PBFI). Formula: `PBFI = Conteggio(deviazioni_protocollo) / N_incidenti_importanti`.
- **Pseudocodice:**

  python

  ```
  def calculate_pbfi(incident_reports, comms_data, start_date, end_date):
      major_incidents = query_incidents(severity=['high', 'critical'], date_range=(start_dat
      deviation_count = 0

      for incident in major_incidents:
          # Analizzare i passaggi del playbook IR rispetto alle azioni effettive intraprese
          planned_steps = get_playbook_steps(incident.type)
          actual_actions = get_incident_actions(incident.id)

          # Verificare i comandi dai dirigenti che hanno ignorato i passaggi del playbook
          exec_comms = get_incident_comms(incident.id, from_users=get_executives())
          for comm in exec_comms:
              if comm.command not in planned_steps:
                  deviation_count += 1
                  break # Contare una deviazione per incidente

      PBFI = deviation_count / len(major_incidents) if major_incidents else 0
      return PBFI
  ```

- **Soglia di avviso:** `PBFI > 0.2` (ad es., i playbook vengono bypassati in più del 20% degli incidenti importanti).

3. Fonti di dati digitali (input dell'algoritmo):

- **API della piattaforma SOAR/Incident Management:** Log degli incidenti, playbook assegnati e timeline delle azioni.
- **API della piattaforma di comunicazione (Slack, Teams):** Canali dedicati ai principali incidenti, per analizzare il flusso di comandi e decisioni.
- **API HRIS:** Per identificare gli utenti con ruoli esecutivi.

4. Protocollo di audit da umano a umano: Durante le revisioni post-incidente (postmortem senza colpa), chiedere esplicitamente: "Tutte le azioni intraprese sono state conformi ai nostri runbook? In caso negativo, qual era il motivo? È stata presa una decisione di deviare da qualcuno in base alla loro anzianità piuttosto che al protocollo?"

5. Azioni di mitigazione consigliate:

- **Mitigazione tecnica/digitale:** Implementare "interruttori di circuito" tecnici nei playbook SOAR che richiedono un motivo documentato e un secondo parere per deviazioni critiche.
- **Mitigazione umana/organizzativa:** Condurre esercizi di simulazione di crisi in cui un dirigente è presente ma il ruolo di Incident Commander è chiaramente assegnato a un esperto addestrato. Debrief della catena di comando.
- **Mitigazione dei processi:** Formalizzare il ruolo di "Incident Commander" nella politica IR, dando loro chiara autorità per eseguire il playbook durante un incidente, con supporto pre-approvato dalla leadership.