Contents

[2.9] Shift Change Exploitation Windows

1. Operational Definition: A specific type of temporal vulnerability caused by the inherent friction, distraction, and potential for miscommunication during the handover period between two security shifts, leading to alerts being missed or incidents being mishandled.

2. Main Metric & Algorithm:

- **Metric:** Shift Change Drop Rate (SCDR). Formula: `SCDR = N_alerts_during_change / N_alerts_total (for same severity)`.
- **Pseudocode:**

  python

  ```
  def calculate_scdr(alerts, shift_change_start, shift_change_duration_minutes):
      """
      alerts: List of alert objects with ['timestamp', 'severity', 'status']
      """
      total_alerts = len(alerts)
      dropped_during_change = 0

      change_end = shift_change_start + timedelta(minutes=shift_change_duration_minutes)

      for alert in alerts:
          # Check if alert arrived during the change window and was not acknowledged
          if shift_change_start <= alert.timestamp <= change_end:
              if alert.status == "new" or alert.status == "closed" and alert.resolution_note
                  dropped_during_change += 1

      if total_alerts > 0:
          SCDR = dropped_during_change / total_alerts
      else:
          SCDR = 0

      return SCDR
  ```

- **Alert Threshold:** `SCDR > 0.15` (Over 15% of alerts that arrive during shift change are not properly handled).

3. Digital Data Sources (Algorithm Input):

- **SIEM (Splunk ES):** `notable_events` index. Fields: `_time`, `status`, `owner`.
- **SOAR (Phantom, XSOAR):** `playbook_runs` to see if alerts triggered during shift change were processed later than others.

4. Human-to-Human Audit Protocol: Directly observe a shift change. Afterwards, interview both the incoming and outgoing analysts: “What alerts were open? Were they all discussed? Was

there any confusion about ownership or next steps?" Review the handover notes in the ticketing system.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement a technical "handover mode" in the SOC dashboard that automatically assigns all unacknowledged high-severity alerts to the incoming shift lead 30 minutes before the end of a shift.
- **Human/Organizational Mitigation:** Mandate a minimum 30-minute overlap between shifts dedicated solely to the handover process. Use a standardized handover template.
- **Process Mitigation:** Formalize the " two-man rule" for critical alerts during shift change: both incoming and outgoing analysts must verbally confirm the status and action plan for any severity "high" or "critical" alert before the shift change is considered complete.