Contents

[1.8] Executive Exception Normalization

1. Operational Definition: The established pattern where security policies are routinely bypassed or exceptions are granted for senior executives (C-level, VPs), creating a perceived "two-tier" system and undermining the overall security culture.

2. Main Metric & Algorithm:

- **Metric:** Executive Exception Ratio (EER). Formula: `EER = N_exceptions_for_executives / N_exceptions_for_all_others`.
- **Pseudocode:**

  python

  ```
  def calculate_eer(ticketing_data, hr_data, start_date, end_date):
      # Get all approved security policy exception tickets
      all_exceptions = query_tickets(type='security_exception', status='approved', date_rang

      exec_exceptions = 0
      non_exec_exceptions = 0

      for ticket in all_exceptions:
          requester_role = get_employee_role(ticket.requester_id, hr_data)
          if requester_role in ['c_level', 'vp', 'svp', 'executive']:
              exec_exceptions += 1
          else:
              non_exec_exceptions += 1

      EER = exec_exceptions / non_exec_exceptions if non_exec_exceptions > 0 else float('inf
      return EER
  ```

- **Alert Threshold:** `EER > 1.5` (i.e., executives are granted exceptions at a rate 50% higher than non-executives, adjusted for population size).

3. Digital Data Sources (Algorithm Input):

- **Ticketing System API** (ServiceNow, Jira): `security_exception` tickets with `requester`, `approval_status`.
- **HRIS API:** To map `requester` to job role and department.

4. Human-To-Human Audit Protocol: Review the minutes of Security Governance or Exception committees. Analyze the language used to justify exceptions for executives vs. other employees. Interview mid-level managers about their perception of policy fairness.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement technical controls that are role-agnostic. If an exception is technically necessary for an executive, it should be documented and applied in a way that minimizes risk, just like any other exception.

- **Human/Organizational Mitigation:** The CISO and CEO must publicly commit to the same security standards as all employees. Security training should be mandatory from the top down.
- **Process Mitigation:** Establish a transparent Security Exception Governance committee with cross-functional representation (e.g., IT, Security, Legal, HR) to review all exception requests against consistent, risk-based criteria.