Contents

[4.4] Attachment to Legacy Systems

1. Operational Definition: An emotional preference for familiar, legacy systems that leads to the avoidance of migration, the dismissal of their security risks, and the rationalization of maintaining end-of-life software and hardware.

2. Main Metric & Algorithm:

- **Metric:** Legacy Risk Acceptance Score (LRAS). Formula: `LRAS = (N_legacy_assets * Avg_CVSS) / N_total_assets`.
- **Pseudocode:**

  python

  ```
  def calculate_lras(cmdb_assets, vuln_scans):
      """
      cmdb_assets: List from CMDB with ['asset_id', 'name', 'os', 'is_legacy' (bool)]
      vuln_scans: List from vuln scanner with ['asset_id', 'cve_id', 'cvss_score', 'severity
      """
      # Get all assets marked as legacy (e.g., EOL OS like Win7, unsupported software)
      legacy_assets = [a for a in cmdb_assets if a['is_legacy']]
      total_assets = len(cmdb_assets)

      # For each legacy asset, find its open vulnerabilities and calculate an average CVSS
      total_legacy_risk = 0
      for asset in legacy_assets:
          asset_vulns = [v for v in vuln_scans if v['asset_id'] == asset['asset_id'] and v['
          avg_cvss = sum([v['cvss_score'] for v in asset_vulns]) / len(asset_vulns) if asset
          total_legacy_risk += avg_cvss

      # Calculate overall score
      lras = (len(legacy_assets) * (total_legacy_risk / len(legacy_assets))) / total_assets
      return lras
  ```

- **Alert Threshold:** `LRAS > 0.25` AND `len(legacy_assets) > 0` (A significant portion of the asset base is legacy and carries high risk).

3. Digital Data Sources (Algorithm Input):

- **CMDB (ServiceNow/AWS Tags):** REST API query to get asset list with a custom `is_legacy` tag or based on `os_version`.
- **Vulnerability Management (Qualys/Tenable):** API to pull all open High/Critical vulnerabilities, their CVSS scores, and the affected assets.

4. Human-to-Human Audit Protocol: Interview IT and security managers: "What is the plan for decommissioning [specific legacy system]? What are the perceived barriers?" Review project charters and budgets for evidence of legacy migration projects being deferred or deprioritized.

5. **Recommended Mitigation Actions:**

    - **Technical/Digital Mitigation:** Enforce strict network segmentation and microsegmentation for all identified legacy systems to contain potential breaches.
    - **Human/Organizational Mitigation:** Run workshops to map the emotional and practical dependencies on legacy systems, creating a shared, objective view of the risk.
    - **Process Mitigation:** Integrate a mandatory "Legacy System Impact Assessment" into the risk acceptance process, requiring CISO approval for any exception.