Contents

[2.3] Deadline-Driven Risk Acceptance 1

[2.3] Deadline-Driven Risk Acceptance

1. Operational Definition: A cognitive state where the perceived pressure of an imminent deadline causes security personnel to consciously bypass or shortcut security protocols to meet the timeline, thereby accepting a higher level of risk.

2. Main Metric & Algorithm:

- **Metric:** Deadline Risk Acceptance Rate (DRAR). Formula: `DRAR = N_protocol_bypass / N_deadline_tasks`.
- **Pseudocode:**

  python

  ```
  def calculate_drar(tasks, start_date, end_date):
      """
      tasks: List of task objects with fields: ['deadline', 'completed_at', 'security_checks
      """
      bypass_count = 0
      total_deadline_tasks = 0

      for task in tasks:
          if task.deadline is not None and task.completed_at between start_date and end_date
              total_deadline_tasks += 1
              if task.security_checks_bypassed > 0: # Assuming this is a count or a boolean
                  bypass_count += 1

      if total_deadline_tasks > 0:
          DRAR = bypass_count / total_deadline_tasks
      else:
          DRAR = 0

      return DRAR
  ```

- **Alert Threshold:** `DRAR > 0.1` (i.e., more than 10% of tasks near a deadline involve security bypasses).

3. Digital Data Sources (Algorithm Input):

- **Project Management API (Jira, Asana):** `issues` or `tasks` endpoint. Fields: `due_date`, `updated_at`, `status`, `labels` (e.g., `#security_waiver`).
- **CI/CD Pipeline Logs (Jenkins, GitLab):** `pipeline_runs` index. Fields: `duration`, `end_time`, `success`, `variables` (e.g., `SKIP_TESTS=true`).
- **Version Control System (Git):** Commit messages containing keywords like "hotfix", "bypass", "skip".

4. Human-to-Human Audit Protocol: Conduct retrospective interviews after a major release or project deadline: "Were you aware of the security requirements for task X? What trade-offs did

you feel you had to make to meet the deadline? Did you formally document the risk acceptance?" Cross-reference answers with change logs.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement automated guardrails in CI/CD pipelines that prevent bypassing critical security steps (e.g., SAST, secrets detection) without mandatory, logged approval from a separate security lead.
- **Human/Organizational Mitigation:** Incorporate "schedule pressure" as a formal risk factor in project planning and threat modeling sessions. Train managers to recognize and mitigate this pressure.
- **Process Mitigation:** Institute a formal, lightweight risk acceptance procedure that must be completed and logged before any security control can be bypassed, creating accountability and a paper trail.