Contents

[2.4] Present Bias in Security Investments

1. Operational Definition: The tendency of decision-makers to prioritize security projects with immediate, visible results over those with long-term strategic value, leading to a neglect of foundational security hygiene.

2. Main Metric & Algorithm:

- **Metric:** Strategic Investment Ratio (SIR). Formula: `SIR = man_hours_long_term / total_security_man_hours`.
- **Pseudocode:**

  python

```
def calculate_sir(projects, fiscal_year):
    """
    projects: List of project objects with fields: ['project_id', 'type', 'man_hours_consu
    project.type: 'reactive' (e.g., incident response, pentest findings), 'strategic' (e.g
    """
    strategic_hours = 0
    total_hours = 0

    for project in projects:
        if project.fiscal_year == fiscal_year:
            total_hours += project.man_hours_consumed
            if project.type == 'strategic':
                strategic_hours += project.man_hours_consumed

    if total_hours > 0:
        SIR = strategic_hours / total_hours
    else:
        SIR = 0

    return SIR
```

- **Alert Threshold:** `SIR < 0.25` (Less than 25% of effort is spent on strategic, long-term security work).

3. Digital Data Sources (Algorithm Input):

- **Project Portfolio Tool (Jira Portfolio, Asana):** `projects` endpoint. Fields: `custom_field.strategic_flag`, `time_tracked`.
- **Financial Management System (SAP, QuickBooks):** `cost_centers` for security budget. Analyze spend on new tools (reactive) vs. training/platform engineering (strategic).
- **Time Tracking Software (Toggl, Harvest):** `time_entries` tagged with project IDs, analyzed by the project's classification.

4. Human-to-Human Audit Protocol: Review the last year's project portfolio with CISO and team leads: "Which of these projects was a direct response to an incident or audit finding? Which were proactive initiatives? What percentage of your team's time would you estimate is spent on firefighting vs. building?" Compare their perception with the data.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement dashboards that visualize the SIR metric for leadership, tying it to key risk indicators.
- **Human/Organizational Mitigation:** Link a portion of security leadership performance bonuses to improving the SIR metric over time.
- **Process Mitigation:** Mandate that a minimum percentage (e.g., 30%) of the security team's quarterly objectives and key results (OKRs) must be dedicated to strategic initiatives.