Contents

[2.5] Hyperbolic Discounting of Future Threats

1. Operational Definition: The cognitive bias where the perceived cost of addressing a future potential threat is weighed as more significant than the actual, discounted future cost of a breach, leading to the perpetual deferral of mitigation actions.

2. Main Metric & Algorithm:

- **Metric:** Mitigation Deferral Index (MDI). Formula: `MDI = (N_vulns_deferred / N_vulns_identified) * Average_Deferral_Time`.
- **Pseudocode:**

  python

```
def calculate_mdi(vulnerabilities):
    """
    vulnerabilities: List of vuln objects with fields: ['vuln_id', 'discovery_date', 'risk
    """
    deferred_vulns = []
    total_vulns = len(vulnerabilities)

    for vuln in vulnerabilities:
        if vuln.planned_remediation_date and vuln.actual_remediation_date:
            # If remediated later than planned, it was deferred
            if vuln.actual_remediation_date > vuln.planned_remediation_date:
                deferral_time = (vuln.actual_remediation_date - vuln.planned_remediation_d
                deferred_vulns.append(deferral_time)

    if total_vulns > 0 and len(deferred_vulns) > 0:
        deferral_rate = len(deferred_vulns) / total_vulns
        avg_deferral_time = sum(deferred_vulns) / len(deferred_vulns)
        MDI = deferral_rate * avg_deferral_time
    else:
        MDI = 0

    return MDI
```

- **Alert Threshold:** `MDI > 7` (e.g., A pattern where 10% of vulns are deferred by an average of 70 days, or 20% by 35 days).

3. Digital Data Sources (Algorithm Input):

- **Vulnerability Management Platform (Qualys, Tenable):** `vulnerabilities` API. Fields: `discovered`, `severity`, `planned_remediation_date`, `remediated`.
- **Ticketing System (Jira, ServiceNow):** `issues` of type 'Risk Acceptance'. Fields: `created`, `risk_assessment.expiry_date`.

4. Human-to-Human Audit Protocol: Review risk acceptance forms and meeting minutes from the past quarter: "What was the rationale for accepting this risk? Was a cost-benefit analysis done that compared the mitigation cost now vs. potential future loss? Has this finding been deferred before?"

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Configure the VM platform to automatically escalate and re-assign vulnerabilities whose planned remediation date has passed without action.
- **Human/Organizational Mitigation:** Train risk owners on proper quantitative risk assessment techniques, forcing a numerical evaluation of future cost.
- **Process Mitigation:** Implement a policy where any deferral of a "high" or "critical" vulnerability requires formal, time-bound risk acceptance signed by a business unit head, with mandatory quarterly reviews.