Contents

[10.4] Swiss Cheese Alignment

1. Operational Definition: A state where the holes (gaps) in multiple layers of defense (technical, human, process) temporarily align, allowing a threat to pass through unimpeded. This is measured by correlating failures across different control domains.

2. Main Metric & Algorithm:

- **Metric:** Defense Failure Correlation (DFC). Formula: For a given incident, `DFC = (Number_of_Failed_Controls / Total_Relevant_Controls) * (1 / Mean_Time_Between_Failures).` A high score indicates many controls failed in quick succession.
- **Pseudocode:**

  python

```
def calculate_dfc(incident_id, controls_list):
    # Get all control failure events related to this incident from logs
    control_failures = get_control_failures_for_incident(incident_id)

    num_failures = len(control_failures)
    total_relevant = len(controls_list) # e.g., all controls that should have stopped this

    # Calculate the time between the first and last control failure
    failure_times = sorted([f.time for f in control_failures])
    if num_failures > 1:
        time_window = (failure_times[-1] - failure_times[0]).total_seconds() / 60  # in mi
        mean_time_between = time_window / (num_failures - 1)
    else:
        mean_time_between = 0

    # Avoid division by zero
    if mean_time_between == 0:
        mean_time_between = 0.1

    dfc = (num_failures / total_relevant) * (1 / mean_time_between)
    return dfc
```

- **Alert Threshold:** `DFC > 1.0` (High ratio of controls failed in a very short time window).

3. Digital Data Sources (Algorithm Input):

- **SIEM:** Logs from various security controls (FW, EDR, Email Gateway, IAM) showing `deny` or `alert` messages that were bypassed.
- **GRC/Compliance Platform:** (e.g., RSA Archer) to define the `Total_Relevant_Controls` for a given attack pattern.

4. Human-to-Human Audit Protocol: During a post-incident review, use a whiteboard to map the attack path. For each step, ask: "What control was designed to stop this? Why did it fail?" The visual map will clearly show the "alignment of holes" through the layers of defense.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement controls that are technically diverse (e.g., signature-based + behavioral) to reduce the chance of a single flaw affecting all layers.
- **Human/Organizational Mitigation:** Cross-train control operators (e.g., network, endpoint, cloud teams) to understand the entire defense chain, not just their silo.
- **Process Mitigation:** Mandate "defense-in-depth" reviews for major incidents to identify and fix correlated control failures.