Contents

[8.10] Dream Logic in Digital Spaces

1. Operational Definition: The application of irrational, associative, and symbolically distorted thought processes—characteristic of dreaming—to digital environments and security incidents, leading to non-sequiturs, confabulation, and magical thinking in problem-solving.

2. Main Metric & Algorithm:

- **Metric:** Irrational Association Density (IAD). Formula: `IAD = Count_of_Illogical_Connections / Total_Connections_Made`.
- **Pseudocode:**

  python

```
# This is a highly complex metric requiring advanced NLP. This is a conceptual outline.
def calculate_iad(incident_id):
    # 1. Fetch all documentation and communication for a specific incident
    incident_data = fetch_incident_data(incident_id)  # tickets, chat logs, report

    # 2. Use NLP to extract causal relationships and logical connections asserted by analy
    extracted_connections = extract_causal_claims(incident_data)

    # 3. Validate these connections against a knowledge graph of known TTPs, infrastructur
    illogical_connections = 0
    for connection in extracted_connections:
        if not validate_connection(connection):  # e.g., against MITRE ATT&CK, CMDB
            illogical_connections += 1

    # 4. Calculate density
    iad = illogical_connections / len(extracted_connections) if extracted_connections else
    return iad
```

- **Alert Threshold:** `IAD > 0.25` (More than 25% of the causal links made during incident analysis are illogical or unsupported by facts).

3. Digital Data Sources (Algorithm Input):

- **Inciment Response Reports:** NLP analysis of the final report.
- **Communication Platforms:** Teams/Slack messages during the incident (anonymized).
- **Ticketing Systems:** Jira/ServiceNow incident tickets and investigation notes.

4. Human-to-Human Audit Protocol: A senior investigator reviews the evidence and timeline of a closed incident separately. They then interview the analysis team, asking them to walk through their reasoning process. The auditor looks for leaps in logic, assumptions treated as facts, or explanations that rely on coincidence rather than evidence.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Develop and use a structured incident documentation tool that forces analysts to link conclusions to specific pieces of evidence from logs and systems.
- **Human/Organizational Mitigation:** Implement a mandatory “peer review” or “devil’s advocate” step in the incident analysis process to challenge assumptions and logical gaps.
- **Process Mitigation:** Train investigators in structured analytical techniques (SATs) from intelligence analysis, such as Analysis of Competing Hypotheses (ACH), to counteract intuitive but flawed “dream logic.”