Contents

[4.9] Euphoria-Induced Carelessness

1. Operational Definition: A state of overconfidence and excitement, often following a success, that leads to underestimating risks, skipping verification steps, and a general relaxation of security vigilance.

2. Main Metric & Algorithm:

- **Metric:** Post-Success Verification Bypass Rate (PSVBR). Formula: `PSVBR = N_unverified_actions_post` `/ N_total_actions_post_success`.
- **Pseudocode:**

  python

```
def calculate_psvbr(action_log, success_events, verification_window='1h'):
    """
    success_events: A list of major incident resolutions or other success markers.
    """
    # For each success event, look at the actions in the following time window
    total_actions_post_success = 0
    unverified_actions = 0

    for success in success_events:
        post_success_actions = get_actions_in_window(success.time, verification_window)
        total_actions_post_success += len(post_success_actions)

        # Check if actions lacked verification (e.g., no MFA, no peer review log)
        for action in post_success_actions:
            if not action['was_verified']: # This flag must be defined in logs
                unverified_actions += 1

    psvbr = unverified_actions / total_actions_post_success if total_actions_post_success
    return psvbr
```

- **Alert Threshold:** `PSVBR > 0.4` (A significant increase in unverified actions following a success event).

3. Digital Data Sources (Algorithm Input):

- **SOAR/SIEM Logs:** To define "success events" (e.g., incident closed with "resolved").
- **Authentication Logs (e.g., Okta):** To check for MFA on sensitive actions.
- **Version Control (Git):** To check for code reviews before commits post-success.

4. Human-to-Human Audit Protocol: In post-incident reviews for successful resolutions, explicitly ask: "After the threat was contained, what were the next steps? Did anyone feel a sense of relief or excitement that might have led to rushing?"

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Enforce “cool-down” rules in SOAR playbooks that maintain security controls even after a success state is declared.
- **Human/Organizational Mitigation:** Leadership and team leads should model and communicate the importance of maintaining procedure through all phases of an incident.
- **Process Mitigation:** Integrate a mandatory “Post-Success Checklist” into incident response playbooks, requiring verification of key steps before declaring full resolution.