# Contents



## [8.2] Unconscious Identification with Threats

**1. Operational Definition:** A psychological state where security personnel develop an unconscious fascination or alignment with the tactics, techniques, and procedures (TTPs) of threat actors, potentially leading to reduced vigilance, missed alerts, or even unintentional facilitation of attacks.

**2. Main Metric & Algorithm:**

- **Metric:** Threat Actor Focus Ratio (TAFR). Formula: `TAFR = (Search_Volume_Threat_Terms + Tool_Usage) / Total_Work_Activity`.
- **Pseudocode:**

  python

  ```
  def calculate_tafr(analyst_id, start_date, end_date):
      # 1. Query analyst's internal search history (e.g., in SIEM, threat intel platforms)
      search_terms = query_internal_searches(analyst_id, start_date, end_date)
      threat_searches = filter_searches_for_threat_terms(search_terms, THREAT_ACTOR_KEYWORDS

      # 2. Query tool usage for threat emulation/malware analysis tools (outside of assigned
      tool_usage = query_tool_logs(analyst_id, start_date, end_date)
      non_task_tool_usage = filter_usage_without_ticket(tool_usage, THREAT_EMULATION_TOOL_ID

      # 3. Get a proxy for total activity (e.g., number of alerts processed, tickets closed)
      total_activity = query_ticket_count(analyst_id, start_date, end_date)

      # 4. Calculate ratio (weighting can be adjusted)
      tafr = (len(threat_searches) + len(non_task_tool_usage)) / total_activity
      return tafr

  # Example Threshold
  if tafr > 0.15:  # More than 15% of activity is threat-focused without clear task
      trigger_alert("High TAFR for analyst: Potential unconscious identification")
  ```

- **Alert Threshold:** `TAFR > 0.15` (Calibrate based on baseline organizational activity).

**3. Digital Data Sources (Algorithm Input):**

- **SIEM/Search Platforms:** Splunk search history logs (index `_audit`, fields `user`, `search_query`, `time`). Cortex XSOAR/TIM/Threat Intel platform query logs.
- **Endpoint/Tool Logs:** Logs from administrative tools, VM platforms, or malware analysis sandboxes (e.g., `user`, `tool_name`, `command_executed`, `timestamp`).
- **Ticketing System:** Jira/ServiceNow API (project `SOC`, fields `assignee`, `created`, `resolved`) to get `total_activity`.

**4. Human-to-Human Audit Protocol:** Conduct a confidential, non-punitive interview facilitated by a security culture expert. Questions should be open-ended: "Can you describe a recent threat actor or technique you found particularly interesting or clever? How do you think about the

motivations of attackers we face? In your opinion, what is the line between understanding a threat and sympathizing with it?"

**5. Recommended Mitigation Actions:**

- **Technical/Digital Mitigation:** Implement role-based access control (RBAC) to ensure access to advanced threat emulation tools is granted only for specific, justified tasks and is logged.
- **Human/Organizational Mitigation:** Establish a robust security culture program that includes discussions on ethics, the psychology of threat actors, and clear boundaries. Encourage mentorship and regular check-ins.
- **Process Mitigation:** Mandate peer review for any activity involving direct interaction with threat emulation tools or access to sensitive threat actor communication channels.