Contents

[10.8] Emergence Unpredictability

1. Operational Definition: The inability to forecast novel attack patterns or system behaviors that arise (emerge) from the non-linear interaction of many simple components within the IT environment, which are not predictable from analyzing the components alone.

2. Main Metric & Algorithm:

- **Metric:** Novel Attack Pattern Rate (NAPR). Formula: `NAPR = Number_of_Incidents_With_Novel_TTPs / Total_Incidents`.
- **Pseudocode:**

  python

  ```
  def calculate_napr(start_date, end_date, mitre_attck_dict):
      all_incidents = get_incidents(start_date, end_date)
      novel_incidents = 0

      for incident in all_incidents:
          # Get the TTPs attributed to this incident
          incident_ttps = incident.attributed_ttps
          # Check if ANY TTP is not in the MITRE ATT&CK framework (i.e., is novel)
          if any(ttp not in mitre_attck_dict for ttp in incident_ttps):
              novel_incidents += 1

      total_incidents = len(all_incidents)
      return novel_incidents / total_incidents if total_incidents > 0 else 0
  ```

- **Alert Threshold:** A sustained `NAPR > 0` is an indicator. A sudden spike is a high-priority warning.

3. Digital Data Sources (Algorithm Input):

- **Threat Intelligence Platform / SIEM:** Incidents enriched with MITRE ATT&CK TTP codes (e.g., `T1059.001` for PowerShell).
- **Human Analysis:** Relies on threat hunters or SOC analysts to label TTPs as “novel” if they don’t map to existing frameworks.

4. Human-to-Human Audit Protocol: Hold regular threat hunting meetings focused on anomaly detection, not just IOC matching. Ask hunters: “What are the weirdest, most unusual behaviors you’ve seen in the logs lately, even if they didn’t trigger an alert?” This encourages looking for emergent patterns.

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Invest in behavioral analytics and User and Entity Behavior Analytics (UEBA) tools that are designed to detect anomalies and novel patterns, not just known-bad signatures.

- **Human/Organizational Mitigation:** Dedicate time for expert threat hunters to conduct hypothesis-free exploration of data to look for emerging patterns.
- **Process Mitigation:** Create a formal process to rapidly create and deploy new detection rules when a novel TTP is discovered, and share this intelligence with the community.