[BBOX]

SOC Detection Validation Report

1. Overview

- **What was tested**:
- **Logs processed**: 10,000 synthetic logs simulating real-world activity.
- **Detection rules**: 1 Sigma rule (strong.yml) and no YARA rules applied.
- **High-level goal**:
- Validate the effectiveness of current SOC detection capabilities.
- Assess the robustness of existing Sigma rules against simulated threats.
- Identify gaps in detection coverage for potential attacker behaviors.

2. Key Metrics

- **Total logs processed**: 10,000
- **Total alerts generated**: 0
- **Alerts per severity**: None generated.
- **Alerts per rule**: No alerts triggered.
- **Alerts per host**: No alerts generated across any hosts.
- **Logs per host**:
- **Highest activity**: Hosts 8, 4, and 18 (534-535 logs each).
- **Lowest activity**: Hosts 17 and 7 (456-457 logs each).
- **Patterns observed**:
- Log distribution was relatively even across hosts, with no single host overwhelming the dataset.

3. Detection Quality

- **Strengths**:
- No false positives were generated, indicating the rule was not overly sensitive.
- **Weaknesses**:
- **No alerts triggered**: The Sigma rule (strong.yml) did not detect any simulated malicious activity, suggesting potential gaps in coverage.
- **Potential blind spots**:
- Lateral movement, privilege escalation, or stealthy attacks may not be effectively detected.
- Data exfiltration or insider threats may also evade current detection mechanisms.

4. Risk & Impact

- **Risk exposure**:

- The lack of alerts indicates a potential failure to detect simulated threats, increasing the organization’s risk of undetected breaches.

- **Potential attacker behaviors that may slip past**:

- Lateral movement across hosts.

- Privilege escalation attempts.

- Data exfiltration via covert channels.

- Stealthy persistence mechanisms.

5. Recommendations

- **Immediate actions**:

- **Tune existing rules**: Adjust the Sigma rule (strong.yml) to improve detection of simulated threats.

- **Expand rule coverage**: Add new Sigma or YARA rules targeting lateral movement, privilege escalation, and data exfiltration.

- **Process improvements**:

- **Integrate simulation into CI/CD**: Use this simulator to validate new rules before deployment.

- **Regular validation testing**: Schedule periodic simulations to ensure detection capabilities remain effective.

- **Enhance threat intelligence**: Incorporate real-world attack patterns into future simulations.

[/BBOX]