[B_NATURAL_LANGUAGE] **Executive Report: SOC Detection Validation Simulation**

---

1. Overview

- **What was tested:**

- **Logs processed:** 10,000 synthetic logs simulating real-world network and endpoint activity.

- **Detection rules:** 1 set of Sigma rules (YARA rules were not used in this simulation).

- **Goal:** Validate the effectiveness of current SOC detection capabilities, assess rule robustness, and identify gaps in coverage.

---

2. Key Metrics

- **Total logs processed:** 10,000

- **Total alerts generated:** 0

- **Alerts by severity:** No alerts were triggered.

- **Alerts by rule:** No alerts were triggered.

- **Alerts by host:** No alerts were triggered.

- **Logs by host:** Activity was evenly distributed across 20 hosts, with no significant concentration on a single host.

---

3. Detection Quality

- **Strengths:**

- No false positives were observed (since no alerts were generated).

- The simulation suggests that current rules may be overly restrictive or not aligned with the synthetic attack patterns.

- **Weaknesses:**

- **Complete lack of alerts** indicates a critical gap in detection coverage.

- Potential blind spots for stealthy attacks, lateral movement, or privilege escalation.

- Possible misconfiguration in rule logic or thresholds.

---

4. Risk & Impact

- **Risk exposure:**

- The absence of alerts suggests that the SOC may be missing real attacks in production.

- Attackers could exploit undetected lateral movement, data exfiltration, or privilege escalation.

- **Potential attacker behaviors slipping past current rules:**

- Living-off-the-land (LOL) techniques.

- Stealthy persistence mechanisms.

- Low-and-slow data exfiltration.

---

5. Recommendations

- **Immediate actions:**
- **Review and refine Sigma rules** to ensure they align with realistic attack patterns.
- **Test with additional synthetic datasets** to validate rule effectiveness.
- **Long-term improvements:**
- **Expand detection coverage** for lateral movement, privilege escalation, and data exfiltration.
- **Integrate this simulator into CI/CD pipelines** for continuous validation of detection rules.
- **Conduct regular red team exercises** to test SOC detection capabilities.

Conclusion:

The simulation revealed a critical gap in detection coverage. Immediate action is required to refine rules and expand detection capabilities to ensure the SOC can effectively identify and respond to real-world threats.