Executive Report: SOC Detection Simulation Results

1. Overview

This report summarizes the results of a SOC detection simulation exercise designed to validate the effectiveness of our current detection capabilities. The simulation processed:

- **10,000 synthetic logs** simulating various network and system activities

- **5 Sigma rules** (no YARA rules were applied in this test)

The primary goal was to assess:

- The robustness of our existing detection rules

- The coverage of our current alerting framework

- The potential for false positives and alert fatigue

2. Key Metrics

High-Level Results

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

- **Total alerts generated:** 6,698

- **Alerts per log:** 0.67 (67% of logs triggered at least one alert)

Alert Breakdown

- **Severity Distribution:**

- Low: 6,698 (100% of alerts)

- **Top Alerting Rules:**

1. **WEAK-NOISE-040:** 3,347 alerts (50% of total)

2. **WEAK-GET-017:** 1,685 alerts (25% of total)

3. **WEAK-POST-016:** 1,662 alerts (25% of total)

4. **WEAK-RAND-031 & WEAK-RAND-032:** 4 alerts combined (0.06% of total)

- **Top Alerting Hosts:**

- **host1:** 382 alerts (6% of total)

- **host8:** 369 alerts (5.5% of total)

- **host10:** 370 alerts (5.5% of total)

- **host18:** 366 alerts (5.5% of total)

Notable Patterns

- **Alert concentration:** 3 rules (WEAK-NOISE-040, WEAK-GET-017, WEAK-POST-016) generated 99.8% of all alerts

- **Host distribution:** Alerts were relatively evenly distributed across hosts, with no single host generating an excessive number of alerts

3. Detection Quality

Strengths

- **Comprehensive coverage of basic web traffic:** The rules effectively detected common HTTP GET and POST requests
- **Consistent detection across hosts:** Alerts were generated for all hosts, indicating broad coverage

Weaknesses

- **Limited severity distribution:** All alerts were classified as "low" severity, suggesting potential gaps in high-severity detection
- **Potential noise generation:** The top 3 rules generated nearly all alerts, which could indicate:
- Overly broad detection criteria
- High volume of benign activity matching these rules
- Need for severity tuning or rule refinement

False Positive Concerns

- The high volume of alerts from WEAK-NOISE-040 (50% of total) suggests this rule may be too sensitive or too broadly applied
- The nearly identical alert counts for WEAK-GET-017 and WEAK-POST-016 (25% each) may indicate these rules are detecting similar activities

4. Risk & Impact

Current Risk Exposure

- **High alert volume:** The current rule set generates a significant number of alerts, which could:
- Overwhelm SOC analysts
- Lead to alert fatigue
- Increase the risk of missing genuine threats
- **Potential blind spots:** The absence of medium/high severity alerts suggests:
- Current rules may not be effectively detecting more sophisticated attacks
- Attackers might successfully execute lateral movement, privilege escalation, or data exfiltration without detection

Potential Attacker Behaviors That Might Slip Past

- **Lateral movement:** No rules specifically targeting internal host-to-host communication
- **Privilege escalation:** No alerts related to privilege changes or suspicious process execution
- **Data exfiltration:** No detection of large data transfers or unusual outbound connections
- **Stealthy attacks:** No rules designed to detect slow, low-and-slow attacks or living-off-the-land techniques

5. Recommendations

Immediate Actions

- **Tune high-volume rules:**
- Investigate WEAK-NOISE-040 for potential noise reduction

- Review WEAK-GET-017 and WEAK-POST-016 for potential overlap
- **Add severity classification:**
- Implement a more nuanced severity scoring system
- Add medium/high severity rules to detect more sophisticated attacks

Detection Gaps to Address

- **Develop new rules for:**
- Lateral movement detection (e.g., unusual remote execution, SMB connections)
- Privilege escalation (e.g., unexpected process execution, service changes)
- Data exfiltration (e.g., large file transfers, unusual outbound connections)
- Stealthy attacks (e.g., slow data exfiltration, living-off-the-land techniques)

Process Improvements

- **Integrate simulation into CI/CD pipeline:**
- Run regular detection simulations as part of rule development
- Use simulation results to validate new rules before deployment
- **Establish alert threshold baselines:**
- Determine acceptable alert volumes per rule and host
- Implement automated alerts when thresholds are exceeded
- **Enhance rule documentation:**
- Document expected alert volumes and false positive rates
- Maintain a knowledge base of common benign triggers

This simulation provides valuable insights into our current detection capabilities and highlights areas for improvement. Addressing these recommendations will enhance our ability to detect and respond to genuine threats while reducing alert fatigue.