Executive Report: SOC Detection Validation

1. Overview

- **What was tested**:
- **Logs**: 10,000 synthetic logs simulating real-world network and system activity.
- **Detection Rules**: Sigma and YARA rules designed to identify malicious behavior.
- **High-level goal**:
- Validate the effectiveness of current SOC detection capabilities.
- Assess the robustness of rules in identifying threats.
- Identify gaps in coverage for potential attacker techniques.

2. Key Metrics

- **Total logs processed**: 10,000
- **Total alerts generated**: 165
- **Alert severity breakdown**:
- Medium: 165
- **Alerts per rule**:
- MALWARE_SIG_A: 165
- **Alerts per host (top 5)**:
- Host11: 14
- Host9: 13
- Host14: 13
- Host2: 11
- Host3: 10
- **Logs per host (top 5)**:
- Host4: 535
- Host8: 534
- Host20: 504
- Host2: 503
- Host11: 488
- **Patterns observed**:
- High concentration of alerts on a few hosts (e.g., Host11, Host9, Host14).
- All alerts triggered by a single rule (MALWARE_SIG_A), suggesting potential over-reliance on one detection method.

3. Detection Quality

- **Strengths**:
- Strong coverage for malware detection (MALWARE_SIG_A rule).

- Consistent alerting across multiple hosts, indicating reliable detection for certain attack vectors.

- **Weaknesses**:

- No alerts for lateral movement, privilege escalation, or data exfiltration, suggesting gaps in detection.

- Over-reliance on a single rule may indicate missed opportunities for broader threat detection.

- **Potential false positives/noise**:

- High volume of alerts from a single rule (MALWARE_SIG_A) may indicate noise or over-triggering.

4. Risk & Impact

- **Risk exposure**:

- Current rules may not adequately detect stealthy or advanced attack techniques.

- Potential for attacker techniques to evade detection, increasing risk of undetected breaches.

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

- Lateral movement within the network.

- Privilege escalation attempts.

- Data exfiltration via non-standard methods.

5. Recommendations

- **Rule tuning**:

- Reduce noise on the MALWARE_SIG_A rule to improve alert quality.

- Implement additional rules for lateral movement, privilege escalation, and data exfiltration.

- **New detection ideas**:

- Develop rules for detecting unusual lateral movement patterns.

- Enhance detection for privilege escalation attempts.

- Monitor for data exfiltration via non-standard channels.

- **Process improvements**:

- Integrate this simulator into CI/CD pipelines for continuous validation of detection rules.

- Establish a regular review process for rule effectiveness and coverage.