Here's a professional executive report based on the provided data:

SOC Detection Validation Report

1. Overview

Purpose of Testing:

This report summarizes the results of a SOC detection validation exercise. The goal was to assess the effectiveness of our current Sigma rules against synthetic log data, simulating real-world attack patterns to identify strengths, gaps, and areas for improvement in our detection capabilities.

What Was Tested:

- **Logs Processed:** 10,000 synthetic logs simulating various user and system activities.
- **Rules Applied:** 100+ Sigma rules covering common attack vectors (e.g., suspicious processes, unauthorized access, lateral movement).
- **No YARA Rules:** File-based detection was not part of this simulation.

2. Key Metrics

- **Total Logs Processed:** 10,000
- **Total Alerts Generated:** 0
- **Alerts by Severity:** No alerts were triggered.
- **Alerts by Host:** No alerts were generated across any host.
- **Logs by Host:** Logs were evenly distributed across 20 hosts (no significant concentration).

Observations:

- **No alerts were generated**, indicating either:
- The synthetic logs did not contain trigger conditions for any rules, or
- The rules were not properly configured to detect the simulated activity.

3. Detection Quality

Strengths:

- The test environment was stable, with no false positives or noisy alerts.

Gaps & Weaknesses:

- **Zero detections** suggest potential issues with rule coverage or log quality.
- Possible causes:
- Rules may not be tuned to detect the simulated attack patterns.
- Logs may lack sufficient detail for rule triggers.
- Some attack vectors (e.g., stealthy lateral movement, privilege escalation) may not be covered.

False Positives & Noise:

- Since no alerts were generated, false positives were not a concern in this test.

4. Risk & Impact

Risk Exposure:

- If the synthetic logs contained realistic attack patterns, the lack of alerts indicates a **critical gap in detection capabilities**.
- Attackers could exploit undetected techniques (e.g., living-off-the-land binaries, fileless attacks, or insider threats).

Potential Attacker Behaviours Slipping Past Defenses:

- Lateral movement without suspicious process execution.
- Privilege escalation via legitimate tools (e.g., PowerShell, WMI).
- Data exfiltration via encrypted channels (e.g., HTTPS, DNS tunneling).

5. Recommendations

Immediate Actions:

- **Review Sigma Rule Coverage:** Ensure rules are tuned to detect common attack patterns (e.g., suspicious process execution, unauthorized access).
- **Test with More Realistic Logs:** Simulate advanced attack techniques (e.g., lateral movement, privilege escalation) to validate rule effectiveness.

Long-Term Improvements:

- **Expand Detection Rules:** Add rules for stealthy attack vectors (e.g., fileless malware, living-off-the-land techniques).
- **Integrate Detection Validation into CI/CD:** Automate rule testing in development pipelines to ensure robustness before deployment.
- **Enhance Log Collection:** Ensure logs contain sufficient context (e.g., command-line arguments, process parent-child relationships).

Next Steps:

- Conduct a follow-up test with refined rules and more realistic attack simulations.
- Review and update the SOC playbook to address identified gaps.

This report provides a clear, actionable summary for both management and SOC teams.