SOC Training Report - Week 3

Advanced Log Analysis

Date: November 27, 2025 Analyst: Security Operations Team

1. Lab Setup

Wazuh infrastructure from Week 2 still operational. Manager on Ubuntu (192.168.56.103), agent on Kali (192.168.56.101) connected and reporting logs normally.

2. Log Correlation - Failed Logins & Network Activity

Failed authentication attempts detected from agent followed by suspicious outbound traffic:

Timestamp	Event	Source IP	Destination IP	Details
12:05:00	Failed SSH Login	192.168.56.101	192.168.56.103	User: invalid_user
12:05:03	Failed SSH Login	192.168.56.101	192.168.56.103	User: root
12:05:06	Failed SSH Login	192.168.56.101	192.168.56.103	User: admin
12:05:15	DNS Query	192.168.56.101	8.8.8.8	External DNS lookup
12:05:20	HTTP Request	192.168.56.101	8.8.8.8	Outbound HTTP
12:05:25	ICMP Ping	192.168.56.101	8.8.8.8	Network probe

Analysis: Three failed login attempts followed within 15 seconds by outbound DNS query and HTTP request to external IP 8.8.8.8. This pattern suggests reconnaissance activity after failed authentication.

3. Anomaly Detection - High-Volume Data Transfer

Created detection rules to identify suspicious data transfers:

Rule 100100: High-volume data transfer (bytes_out > 1MB in 60 seconds)
Rule 100101: Multiple transfers from same IP in 5-minute window

Test Results:

- Created 10MB test file on Kali
- Performed multiple file transfers
- Rule 100100 triggered with alert level 7
- Rule 100101 triggered with alert level 9 (multiple transfers detected)

Status: Both rules operational and validated.

4. Log Enrichment - GeoIP Analysis

External IP 8.8.8.8 enrichment results:

Field	Value
IP	8.8.8.8
Country	United States
City	Mountain View
ISP	Google LLC
Service	Google DNS

GeoIP Summary (50 words): DNS query to 8.8.8.8 resolved to Mountain View, California (Google DNS service). While Google DNS is legitimate public infrastructure, the timing correlation with failed authentication attempts indicates potential reconnaissance. The enrichment confirms this is not a malicious IP, but continued monitoring of this source IP recommended for pattern analysis.

5. Detection Rules Status

Verified the following rules are operational:

- Rule 5402: Sudo to ROOT executed - Operational
- Rule 5403: First time sudo - Operational
- Rule 5501: PAM Login session opened - Operational
- Rule 5502: PAM Login session closed - Operational
- Custom Rules 100100, 100101: Tested and validated

Total alerts generated during testing: 80+ authentication, 15+ network events.

6. Key Findings

1. Log Correlation: Successfully correlated failed logins with outbound network activity, identifying potential attack pattern.
2. Anomaly Detection: High-volume data transfer detection working correctly, triggering alerts at appropriate severity levels.
3. GeoIP Enrichment: External IPs automatically enriched with location data, providing analyst context for quick assessment.

4. Agent Connectivity: Kali agent maintaining consistent heartbeat with manager, all logs flowing correctly.

7. Recommendations

- Continue monitoring agent for suspicious patterns
- Expand detection rules to include port scanning and privilege escalation attempts
- Document all custom rules for audit purposes
- Monitor baseline network traffic to improve anomaly accuracy

Conclusion

Week 3 exercises successfully demonstrated log analysis, anomaly detection, and enrichment capabilities. All required tasks completed:

- Log correlation documented with sample data
- Anomaly detection rules created and tested
- GeoIP enrichment implemented and analyzed
- Detection infrastructure validated and operational

Lab environment ready for next training modules.