Security Analysis Report

Generated: February 01, 2026 08:27 PM

Executive Summary

[ANALYSIS] Security Status: CRITICAL (12.2/100)

Detected 5 security threat(s). Most common: Suspicious Network Traffic (1 occurrence(s)). [WARNING] Immediate attention recommended.

Security Overview

Metric	Value
Total Threats Detected	5
Security Score	12.2/100
Health Status	CRITICAL
Logs Analyzed	192
Compression Ratio	0.0%
Cost Savings	$0.00

Detected Threats

1. Suspicious Network Traffic

Severity	CRITICAL
Risk Score	56.2/100
Confidence	75%
Description	Unusual network traffic patterns detected
Affected Resources	203.0.113.50, 192.168.1.100, admin
Source IP	45.142.212.33
Location	Moldova

2. Malware Activity

Severity	CRITICAL
Risk Score	100.0/100
Confidence	80%
Description	Potential malware activity identified
Affected Resources	203.0.113.50, 192.168.1.100, admin
Source IP	45.142.212.33
Location	Moldova

3. Brute Force Attack

Severity	HIGH
Risk Score	92.6/100
Confidence	95%
Description	Multiple failed login attempts detected (5 occurrences)
Affected Resources	203.0.113.50, 192.168.1.100, admin
Source IP	45.142.212.33
Location	Moldova

4. Privilege Escalation

Severity	HIGH
Risk Score	100.0/100
Confidence	75%
Description	Suspicious privilege escalation attempt detected
Affected Resources	203.0.113.50, 192.168.1.100, admin
Source IP	45.142.212.33
Location	Moldova

5. Unauthorized Access Attempt

Severity	MEDIUM
Risk Score	90.0/100
Confidence	80%
Description	Unauthorized access attempts identified (2 occurrences)
Affected Resources	203.0.113.50, 192.168.1.100, admin
Source IP	45.142.212.33
Location	Moldova

IP Threat Intelligence

Analyzed 4 unique IP addresses. Found 1 malicious IPs.

IP Address	Country	Threat Level	Types
45.142.212.33	Moldova	LOW	Potential VPN/Proxy

Recommendations

- Review and address all CRITICAL and HIGH severity threats immediately
- Implement recommended security controls for each threat type
- Monitor suspicious IP addresses and consider blocking repeat offenders
- Enable additional logging for affected resources
- Schedule follow-up security assessment within 7 days
- Update incident response procedures based on findings

End of Report - Security Monitoring Agent