■■ SOC ANALYST AI
Security Analysis Report

Report Generated: 2025-10-22 13:18:34

Log Source: data/samples/sample_firewall.log

Analysis Date: 2025-10-22 13:18:34

Log Type: firewall

Analyst: SOC AI

■ Executive Summary

SEVERITY: MEDIUM | Threat Score: 5.62/10

This security analysis report covers 24 events analyzed by the SOC AI system. Of these, 21 events were flagged as suspicious and warrant further investigation. The overall threat severity has been assessed as **MEDIUM**.

The analysis identified 1 distinct attack pattern(s): Lateral Movement. These patterns suggest potential malicious activity targeting the infrastructure.

The security events affected 1 host(s) and 0 user account(s). Immediate review of these assets is recommended to ensure no compromise has occurred.

Key Metrics:

Metric	Count
Total Events	24
Suspicious Events	21
Attack Patterns	1
Unique Threat Indicators	4
Affected Systems	1

■ Technical Analysis

Event Statistics:

Metric	Value
Total Events Analyzed	24
Suspicious Events	21
Unique Source IPs	7
Affected Hosts	1
Affected Users	0

Detected Attack Patterns:

1. Lateral Movement
Severity: CRITICAL
Detected potential lateral movement activity
MITRE Technique: T1021 - Remote Services

■ MITRE ATT&CK; Mapping

The following MITRE ATT&CK; techniques were identified based on observed behaviors and patterns in the analyzed security events. This mapping helps understand the tactics and techniques potentially used by adversaries.

Technique ID	Name	Tactic	Occurrences
T1021	Remote Services	Lateral Movement	4

■ Indicators of Compromise (IoC)

The following Indicators of Compromise (IoCs) were extracted from the security events. These should be used for threat hunting and blocking at security controls.

IP Indicators:

Value	Severity	Occurrences	First Seen
192.168.1.100	MEDIUM	7	
192.168.1.101	MEDIUM	1	2025-10-22T13:18:34
45.76.123.45	HIGH	1	
203.0.113.45	HIGH	5	2024-10-22T10:15:30
185.220.101.23	HIGH	1	2024-10-22T10:17:20

■■ Event Timeline

Chronological timeline of significant security events:

2024-10-22T10:15:30 - [MEDIUM]
Type: deny
SSH connection attempt blocked

2024-10-22T10:15:31 - [MEDIUM]
Type: deny
SSH connection attempt blocked

2024-10-22T10:15:32 - [MEDIUM]
Type: deny
SSH connection attempt blocked

2024-10-22T10:15:33 - [MEDIUM]
Type: deny
SSH connection attempt blocked

2024-10-22T10:15:34 - [MEDIUM]
Type: deny
SSH connection attempt blocked

2024-10-22T10:17:20 - [MEDIUM]
Type: deny
SMB access attempt blocked

2025-10-22T13:18:34 - [MEDIUM]
Type: deny
%ASA-3-106014: Deny inbound icmp src outside:192.168.1.101 dst inside:10.0.0.1

■ Recommended Actions

Based on the analysis, the following actions are recommended to mitigate identified threats and improve security posture:

1. ■■ CRITICAL: Isolate affected systems immediately
2. ■ Force password reset for affected accounts
3. ■ Conduct full forensic investigation
4. ■ Continue monitoring for 24-48 hours

■ Conclusion

■ *MEDIUM - Action Recommended*

Moderate security events detected. Review and address recommendations during normal business hours.

This report was generated automatically by SOC Analyst AI. For questions or additional analysis, contact the Security Operations Center.