■■ SOC ANALYST AI
Security Analysis Report

Report Generated: 2025-10-22 13:20:15

Log Source: data/samples/sample_windows.log

Analysis Date: 2025-10-22 13:20:15

Log Type: windows_event

Analyst: SOC AI

■ Executive Summary

SEVERITY: MEDIUM | Threat Score: 3.91/10

This security analysis report covers 11 events analyzed by the SOC AI system. Of these, 7 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): Privilege Escalation. These patterns suggest potential malicious activity targeting the infrastructure.

Key Metrics:

Metric	Count
Total Events	11
Suspicious Events	7
Attack Patterns	1
Unique Threat Indicators	3
Affected Systems	0

■ Technical Analysis

Event Statistics:

Metric	Value
Total Events Analyzed	11
Suspicious Events	7
Unique Source IPs	0
Affected Hosts	0
Affected Users	0

Detected Attack Patterns:

1. Privilege Escalation
Severity: HIGH
Detected privilege escalation attempts
MITRE Technique: T1068 - Exploitation for Privilege Escalation

■ 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
T1110	Brute Force	Credential Access	5

■ Recommended Actions

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

1. ■ Audit and restrict administrative privileges
2. ■ Review and update access control policies
3. ■ 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.