Security Analysis Report

Comprehensive Security Assessment and Threat Analysis

Vulnerability Analysis

In-depth security assessment with CVSS scoring and detailed remediation guidance

MITRE Coverage

Comprehensive evaluation of security events and MITRE ATT&CK framework alignment

Generated on
November 28, 2024

Powered by
SenseL Copilot Analytics

CONTENTS

OVERVIEW

AGENT ANALYSIS

Security assessment across **10 agents** reveals a security score of **0** (Critical). The analysis identified **0 critical vulnerabilities** and **1 high-severity alerts** that require attention. Security monitoring covers **0 MITRE ATT&CK tactics**.

Security Score	Active Agents	Total Alerts
0	5	1749
Critical	of 10 Total	Security Events

Security Events Distribution

Critical Vulnerabilities	0
High Severity Alerts	1
Medium Severity Alerts	1748

Security Coverage

MITRE Tactics Covered	0
Active Monitoring	5 Agents
Total Vulnerabilities	0

Key Recommendations

High Severity Alerts

Review and respond to 1 high severity security events that may indicate significant security threats.

MITRE Coverage

Expand security monitoring to cover more MITRE ATT&CK tactics for comprehensive threat detection.

Detected **0 vulnerabilities** across all agents. This analysis includes CVSS scores, affected packages, and detailed vulnerability information to help prioritize remediation efforts.

0	0	0
Critical Vulnerabilities	High Severity	Medium Severity

Other Vulnerabilities

No additional vulnerabilities detected

Security monitoring covers **0 MITRE ATT&CK tactics** and **0 unique techniques**, with a total of **0 technique detections**. This analysis provides insights into potential adversary behaviors and helps identify areas for security improvements.

0	0	0
Tactics Monitored	Unique Techniques	Total Detections

Tactics Coverage

No MITRE tactics detected

Top Techniques

No MITRE techniques detected

Agent **HOOST_001_poc5** has reported **1 security events**, including **0 high-severity alerts**. The agent monitors **0 MITRE ATT&CK tactics** and has detected **0 vulnerabilities**.

Total Alerts	High Severity	Compliance
1	0	0
Security Events	Critical Events	Framework Controls

System Information

Agent ID	Agent Name
143	HOOST_001_poc5

MITRE Coverage	Vulnerabilities
0 Tactics	0

Top Rules

Rule 61110

Level 10

Multiple System error events

windows windows_system

Recent Alerts

2024/11/26 H7:57:42

Level 10

Multiple System error events

Agent **HOOST_002_poc5** has reported **30 security events**, including **0 high-severity alerts**. The agent monitors **0 MITRE ATT&CK tactics** and has detected **0 vulnerabilities**.

Total Alerts	High Severity	Compliance
30	0	0
Security Events	Critical Events	Framework Controls

System Information

Agent ID	Agent Name
079	HOOST_002_poc5

MITRE Coverage	Vulnerabilities
0 Tactics	0

Top Rules

Rule 61110 Level 10

Multiple System error events

windows windows_system

Recent Alerts

2024/11/7 H5:56:21 Level 10

Multiple System error events

2024/11/7 H5:56:21

Level 10

Multiple System error events

2024/11/7 H5:56:21

Level 10

Multiple System error events

2024/11/7 H5:56:20

Level 10

Multiple System error events

2024/11/7 H8:04:20

Level 10

Multiple System error events

2024/11/7 H8:04:20

Level 10

Multiple System error events

2024/11/7 H8:04:19

Level 10

Multiple System error events

2024/11/7 H8:04:18

Level 10

Multiple System error events

2024/11/7 H8:04:18

Level 10

Multiple System error events

2024/11/7 H8:04:18

Level 10

Multiple System error events

Agent **HOOST_003_poc5** has reported **87 security events**, including **0 high-severity alerts**. The agent monitors **0 MITRE ATT&CK tactics** and has detected **0 vulnerabilities**.

Total Alerts	High Severity	Compliance
87	0	0
Security Events	Critical Events	Framework Controls

System Information

Agent ID	Agent Name
145	HOOST_003_poc5

MITRE Coverage	Vulnerabilities
0 Tactics	0

Top Rules

Rule 61061

Level 10

Multiple Windows error application events.

windows windows_application

Recent Alerts

2024/11/28 H4:19:57

Level 10

Multiple Windows error application events.

2024/11/27 H10:12:41

Level 10

Multiple Windows error application events.

2024/11/27 H9:58:07

Level 10

Multiple Windows error application events.

2024/11/27 H3:50:50

Level 10

Multiple Windows error application events.

2024/11/26 H9:43:34

Level 10

Multiple Windows error application events.

2024/11/26 H9:29:00

Level 10

Multiple Windows error application events.

2024/11/26 H3:21:44

Level 10

Multiple Windows error application events.

2024/11/25 H9:14:27

Level 10

Multiple Windows error application events.

2024/11/25 H3:07:10

Level 10

Multiple Windows error application events.

2024/11/25 H8:59:53

Level 10

Multiple Windows error application events.

Agent **HOOST_007_poc5** has reported **1 security events**, including **0 high-severity alerts**. The agent monitors **0 MITRE ATT&CK tactics** and has detected **0 vulnerabilities**.

Total Alerts	High Severity	Compliance
1	0	0
Security Events	Critical Events	Framework Controls

System Information

Agent ID	Agent Name
208	**HOOST_007_poc5**

MITRE Coverage	Vulnerabilities
0 Tactics	**0**

Top Rules

Rule 61110

Level 10

Multiple System error events

windows windows_system

Recent Alerts

2024/11/27 H7:58:24

Level 10

Multiple System error events

Agent **HOOST_006_poc5** has reported **1630 security events**, including **0 high-severity alerts**. The agent monitors **0 MITRE ATT&CK tactics** and has detected **0 vulnerabilities**.

Total Alerts	High Severity	Compliance
1630	0	2
Security Events	Critical Events	Framework Controls

System Information

Agent ID	Agent Name
083	HOOST_006_poc5

MITRE Coverage	Vulnerabilities
0 Tactics	0

Top Rules

Rule 61110

Level 10

Multiple System error events

windows windows_system

Rule 204

Level 12

Agent event queue is flooded. Check the agent configuration.

wazuh agent_flooding PCI DSS GDPR

Recent Alerts

2024/11/22 H9:11:56 Level 10

Multiple System error events

2024/11/22 H9:11:56 Level 10

Multiple System error events

2024/11/22 H9:11:56 Level 10

Multiple System error events

2024/11/22 H9:11:56 Level 10

Multiple System error events

2024/11/22 H9:11:56 Level 10

Multiple System error events

2024/11/22 H9:11:56 Level 10

Multiple System error events

2024/11/22 H9:11:56 Level 10

Multiple System error events

2024/11/22 H9:11:56 Level 10

Multiple System error events

2024/11/22 H9:11:55 Level 10

Multiple System error events

2024/11/22 H9:11:55

Level 10

Multiple System error events