

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

CONTENTS

OVERVIEW

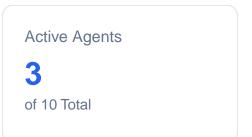
Executive Summary	3
<u>Vulnerability Analysis</u>	4
MITRE ATT&CK Analysis	<u>5</u>

AGENT ANALYSIS

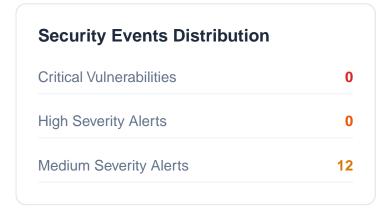
Agent 1 Analysis	<u>6</u>
Agent 2 Analysis	7
Agent 3 Analysis	<u>8</u>

Security assessment across 10 agents reveals a security score of 76 (Fair). The analysis identified 0 critical vulnerabilities and 0 high-severity alerts that require attention. Security monitoring covers 0 MITRE ATT&CK tactics.









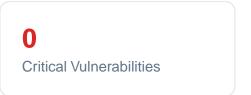


Key Recommendations

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.



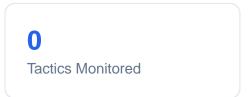




Other Vulnerabilities

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.







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

1
Security Events

High Severity

O

Critical Events

Compliance

O

Framework Controls

System Information

Agent ID
143

MITRE Coverage
0 Tactics

Agent Name
HOOST_001_poc5

Vulnerabilities

Top Rules



0

Recent Alerts

2024/11/26 H7:57:42

Multiple System error events



Agent HOOST_003_poc5 has reported 10 security events, including 0 high-severity alerts. The agent monitors 0 MITRE ATT&CK tactics and has detected 0 vulnerabilities.

Total Alerts

10

Security Events

High Severity

Critical Events

Compliance

0

Framework Controls

System Information

Agent ID

145

Agent Name

HOOST_003_poc5

MITRE Coverage

0 Tactics

Vulnerabilities

0

Top Rules



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

1
Security Events

High Severity

O

Critical Events

Compliance

O

Framework Controls

System Information

Agent ID
208

MITRE Coverage
0 Tactics

Agent Name
HOOST_007_poc5

Vulnerabilities
0

Top Rules



Recent Alerts

2024/11/27 H7:58:24

Multiple System error events

