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

Security Score	Active Agents	Total Alerts
0	2	373
Critical	of 6 Total	Security Events

Security Events Distribution

Critical Vulnerabilities	0
High Severity Alerts	0
Medium Severity Alerts	373

Security Coverage

MITRE Tactics Covered	0
Active Monitoring	2 Agents
Total Vulnerabilities	0

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.

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 **AO108027** 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
005	AO108027

MITRE Coverage	Vulnerabilities
0 Tactics	0

Top Rules

Rule 61110 Level 10

Multiple System error events

windows windows_system

Recent Alerts

2024/11/27 H11:53:24 Level 10

Multiple System error events

Agent **PDM-SERVER** has reported **372 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
372	0	0
Security Events	Critical Events	Framework Controls

System Information

Agent ID	Agent Name
125	PDM-SERVER

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 H5:21:05

Level 10

Multiple Windows error application events.

2024/11/28 H5:17:40

Level 10

Multiple Windows error application events.

2024/11/28 H5:14:15

Level 10

Multiple Windows error application events.

2024/11/28 H5:10:50

Level 10

Multiple Windows error application events.

2024/11/28 H5:07:25

Level 10

Multiple Windows error application events.

2024/11/28 H5:04:00

Level 10

Multiple Windows error application events.

2024/11/28 H5:00:35

Level 10

Multiple Windows error application events.

2024/11/28 H4:57:10

Level 10

Multiple Windows error application events.

2024/11/28 H4:53:45

Level 10

Multiple Windows error application events.

2024/11/28 H4:50:20

Level 10

Multiple Windows error application events.