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

Executive Summary 3

Vulnerability Analysis 4

MITRE ATT&CK Analysis 5

AGENT ANALYSIS

Agent 1 Analysis 6

Agent 2 Analysis 7

Agent 3 Analysis 8

Agent 4 Analysis 9

Security assessment across **6 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 **1 MITRE ATT&CK tactics**.

Security Score	Active Agents	Total Alerts
0	4	5425
Critical	of 6 Total	Security Events

Security Events Distribution

Critical Vulnerabilities	0
High Severity Alerts	1
Medium Severity Alerts	5424

Security Coverage

MITRE Tactics Covered	1
Active Monitoring	4 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 **1 MITRE ATT&CK tactics** and **1 unique techniques**, with a total of **1 technique detections**. This analysis provides insights into potential adversary behaviors and helps identify areas for security improvements.

1	1	1
Tactics Monitored	Unique Techniques	Total Detections

Tactics Coverage

Credential Access 1

Techniques related to this tactic

Top Techniques

Brute Force 1

ID: Brute Force | Occurrences: 1

Agent **AO108027** has reported **18 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
18	**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

2024/11/26 H8:37:10

Level 10

Multiple System error events

2024/11/25 H5:07:17

Level 10

Multiple System error events

2024/11/25 H12:11:34

Level 10

Multiple System error events

2024/11/23 H10:28:16

Level 10

Multiple System error events

2024/11/21 H6:15:52

Level 10

Multiple System error events

2024/11/21 H11:13:19

Level 10

Multiple System error events

2024/11/20 H7:34:42

Level 10

Multiple System error events

2024/11/19 H8:39:37

Level 10

Multiple System error events

2024/11/18 H8:46:17

Level 10

Multiple System error events

Agent **AO110006** has reported **42 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
42	0	0
Security Events	Critical Events	Framework Controls

System Information

Agent ID	Agent Name
030	AO110006

MITRE Coverage	Vulnerabilities
0 Tactics	0

Top Rules

Rule 61061

Level 10

Multiple Windows error application events.

windows windows_application

Rule 61110

Level 10

Multiple System error events

windows windows_system

Recent Alerts

2024/11/26 H10:00:03 — Level 10

Multiple Windows error application events.

2024/11/25 H12:08:05 — Level 10

Multiple Windows error application events.

2024/11/24 H4:46:55 — Level 10

Multiple System error events

2024/11/24 H4:46:54 — Level 10

Multiple System error events

2024/11/24 H4:46:54 — Level 10

Multiple System error events

2024/11/22 H5:38:31 — Level 10

Multiple System error events

2024/11/22 H5:38:31 — Level 10

Multiple System error events

2024/11/21 H4:51:32 — Level 10

Multiple Windows error application events.

2024/11/21 H11:46:07 — Level 10

Multiple Windows error application events.

2024/11/21 H11:46:07

Level 10

Multiple Windows error application events.

Agent **PDM-SERVER** has reported **5363 security events**, including **0 high-severity alerts**. The agent monitors **1 MITRE ATT&CK tactics** and has detected **0 vulnerabilities**.

Total Alerts	High Severity	Compliance
5363	**0**	**5**
Security Events	Critical Events	Framework Controls

System Information

Agent ID	Agent Name
125	**PDM-SERVER**

MITRE Coverage	Vulnerabilities
1 Tactics	**0**

Top Rules

Rule 61061

Level 10

Multiple Windows error application events.

windows | windows_application

Rule 60204

Level 12

Multiple Windows Logon Failures

windows | windows_security | authentication_failures | PCI DSS | GDPR | HIPAA | NIST 800-53 | TSC

Credential Access

Recent Alerts

2024/11/28 H5:31:20 **Level 10**

Multiple Windows error application events.

2024/11/28 H5:27:55 **Level 10**

Multiple Windows error application events.

2024/11/28 H5:24:30 **Level 10**

Multiple Windows error application events.

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.

Agent **AO113005** has reported **2 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
2	0	0
Security Events	Critical Events	Framework Controls

System Information

Agent ID	Agent Name
140	AO113005

MITRE Coverage	Vulnerabilities
0 Tactics	0

Top Rules

Rule 61110

Level 10

Multiple System error events

windows windows_system

Recent Alerts

2024/11/26 H5:31:02

Level 10

Multiple System error events

2024/11/26 H5:31:02

Level 10

Multiple System error events