



Security Analysis Report

Comprehensive Security Assessment
and Threat Analysis



Vulnerability Analysis

In-depth security assessment with
CVSS scoring and detailed reme-
diation guidance



MITRE Coverage

Comprehensive evaluation of se-
curity events and MITRE ATT&CK
framework alignment

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 **0 high-severity alerts** that require attention. Security monitoring covers **0 MITRE ATT&CK tactics**.

Security Score

0

Critical

Active Agents

4

of 6 Total

Total Alerts

1217

Security Events

Security Events Distribution

Critical Vulnerabilities 0

High Severity Alerts 0

Medium Severity Alerts 1217

Security Coverage

MITRE Tactics Covered 0

Active Monitoring 4 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
Critical Vulnerabilities

0
High Severity

0
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

Tactics Monitored

0

Unique Techniques

0

Total Detections

Tactics Coverage

No MITRE tactics detected

Top Techniques

No MITRE techniques detected

Agent **AO108027** has reported **4 security events**, including **0 high-severity alerts**. The agent monitors **0 MITRE ATT&CK tactics** and has detected **0 vulnerabilities**.

Total Alerts

4

Security Events

High Severity

0

Critical Events

Compliance

0

Framework Controls

System Information

Agent ID

005

Agent Name

AO108027

MITRE Coverage

0 Tactics

Vulnerabilities

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

Agent **AO110006** 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

2

Security Events

High Severity

0

Critical Events

Compliance

0

Framework Controls

System Information

Agent ID

030

Agent Name

AO110006

MITRE Coverage

0 Tactics

Vulnerabilities

0

Top Rules

Rule 61061

Level 10

Multiple Windows error application events.

windows

windows_application

Recent Alerts

2024/11/26 H10:00:03

Level 10

Multiple Windows error application events.

Multiple Windows error application events.

Agent **PDM-SERVER** has reported **1209 security events**, including **0 high-severity alerts**. The agent monitors **0 MITRE ATT&CK tactics** and has detected **0 vulnerabilities**.

Total Alerts

1209

Security Events

High Severity

0

Critical Events

Compliance

0

Framework Controls

System Information

Agent ID

125

Agent Name

PDM-SERVER

MITRE Coverage

0 Tactics

Vulnerabilities

0

Top Rules

Rule 61061

Level 10

Multiple Windows error application events.

windows

windows_application

Recent Alerts

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.

2024/11/28 H4:57:10

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

2

Security Events

High Severity

0

Critical Events

Compliance

0

Framework Controls

System Information

Agent ID

140

Agent Name

AO113005

MITRE Coverage

0 Tactics

Vulnerabilities

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

Multiple System error events