

# 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**

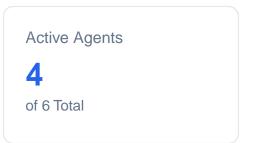
Executive Summary	3
<u>Vulnerability Analysis</u>	4
MITRE ATT&CK Analysis	<u>5</u>

### **AGENT ANALYSIS**

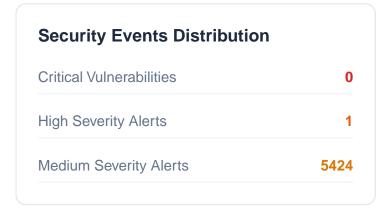
Agent 1 Analysis	<u>6</u>
Agent 2 Analysis	7
Agent 3 Analysis	8
Agent 4 Analysis	9

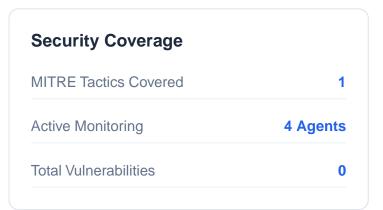
Security assessment across 6 agents reveals a security score of 0 (Critical). The analysis identified 0 critical vulnerabilities and 1 high-severity alerts that require attention. Security monitoring covers 1 MITRE ATT&CK tactics.











### **Key Recommendations**

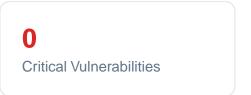
### **High Severity Alerts**

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.







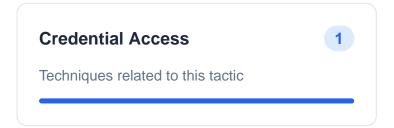
### Other Vulnerabilities

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.



# **Tactics Coverage**



# **Top Techniques**



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** 

18

Security Events

**High Severity** 

Critical Events

Compliance

0

Framework Controls

# **System Information**

Agent ID

005

**Agent Name** 

AO108027

MITRE Coverage

**0 Tactics** 

**Vulnerabilities** 

0

### **Top Rules**



Multiple System error events

windows windows\_system

### **Recent Alerts**

2024/11/27 H11:53:24

Level 10

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
42
Security Events

High Severity

O

Critical Events

Compliance

O

Framework Controls

# **System Information**

Agent ID
030

MITRE Coverage
0 Tactics

Agent Name
AO110006

Vulnerabilities

# **Top Rules**



0



### **Recent Alerts**

2024/11/21 H11:46:07

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.

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** 

5363

Security Events

**High Severity** 

0

Critical Events

Compliance

5

Framework Controls

# **System Information**

Agent ID

125

Agent Name

**PDM-SERVER** 

MITRE Coverage

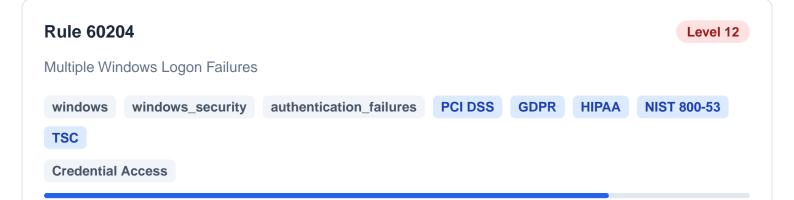
1 Tactics

**Vulnerabilities** 

0

### **Top Rules**





### **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** 

Security Events

**High Severity** 

Critical Events

Compliance

0

Framework Controls

# **System Information**

Agent ID

140

**Agent Name** 

AO113005

MITRE Coverage

**0 Tactics** 

**Vulnerabilities** 

0

### **Top Rules**



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