



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
Agent 5 Analysis	10
Agent 6 Analysis	11
Agent 7 Analysis	12
Agent 8 Analysis	13

Security assessment across **41 agents** reveals a security score of **0** (Critical). The analysis identified **0 critical vulnerabilities** and **879 high-severity alerts** that require attention. Security monitoring covers **3 MITRE ATT&CK tactics**.

Security Score

0

Critical

Active Agents

8

of 41 Total

Total Alerts

902

Security Events

Security Events Distribution

Critical Vulnerabilities 0

High Severity Alerts 879

Medium Severity Alerts 23

Security Coverage

MITRE Tactics Covered 3

Active Monitoring 8 Agents

Total Vulnerabilities 0

Key Recommendations

High Severity Alerts

Review and respond to 879 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
Critical Vulnerabilities

0
High Severity

0
Medium Severity

Other Vulnerabilities

No additional vulnerabilities detected

Security monitoring covers **3 MITRE ATT&CK tactics** and **2 unique techniques**, with a total of **879 technique detections**. This analysis provides insights into potential adversary behaviors and helps identify areas for security improvements.

3

Tactics Monitored

2

Unique Techniques

879

Total Detections

Tactics Coverage

Credential Access

878

Techniques related to this tactic



Defense Evasion

1

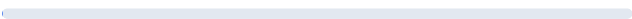
Techniques related to this tactic



Privilege Escalation

1

Techniques related to this tactic



Top Techniques

Brute Force

878

ID: Brute Force

Occurrences: 878

Credential Access

Domain Policy Modification

1

ID: Domain Policy Modification

Occurrences: 1

Defense Evasion

Privilege Escalation

Agent **poc2_004** has reported **5 security events**, including **0 high-severity alerts**. The agent monitors **0 MITRE ATT&CK tactics** and has detected **0 vulnerabilities**.

Total Alerts

5

Security Events

High Severity

0

Critical Events

Compliance

0

Framework Controls

System Information

Agent ID

168

Agent Name

poc2_004

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 H8:30:32

Level 10

Multiple Windows error application events.

2024/11/26 H4:31:58

Level 10

Multiple Windows error application events.

2024/11/26 H4:27:07

Level 10

Multiple Windows error application events.

2024/11/26 H3:55:45

Level 10

Multiple Windows error application events.

2024/11/26 H2:40:25

Level 10

Multiple Windows error application events.

Agent **poc2_010** has reported **84 security events**, including **10 high-severity alerts**. The agent monitors **1 MITRE ATT&CK tactics** and has detected **0 vulnerabilities**.

Total Alerts

84

Security Events

High Severity

10

Critical Events

Compliance

5

Framework Controls

System Information

Agent ID

173

Agent Name

poc2_010

MITRE Coverage

1 Tactics

Vulnerabilities

0

Top Rules

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

2024/11/27 H4:17:50

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/27 H4:17:50

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/27 H4:17:49

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/27 H4:17:49

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/27 H4:17:49

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/27 H4:17:49

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/27 H4:17:49

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/27 H3:31:01

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/27 H3:31:01

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/27 H3:31:01

Level 12

Multiple Windows Logon Failures

Credential Access

Agent **poc2_012** has reported **285 security events**, including **10 high-severity alerts**. The agent monitors **1 MITRE ATT&CK tactics** and has detected **0 vulnerabilities**.

Total Alerts

285

Security Events

High Severity

10

Critical Events

Compliance

5

Framework Controls

System Information

Agent ID

175

Agent Name

poc2_012

MITRE Coverage

1 Tactics

Vulnerabilities

0

Top Rules

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

2024/11/26 H4:29:57

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/26 H4:29:37

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/26 H4:29:27

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/26 H4:29:07

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/26 H4:28:57

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/26 H4:28:37

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/26 H4:28:17

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/26 H4:28:07

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/26 H4:27:47

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/26 H4:27:37

Level 12

Multiple Windows Logon Failures

Credential Access

Agent **poc2_016** has reported **1 security events**, including **1 high-severity alerts**. The agent monitors **2 MITRE ATT&CK tactics** and has detected **0 vulnerabilities**.

Total Alerts

1
Security Events

High Severity

1
Critical Events

Compliance

5
Framework Controls

System Information

Agent ID
179

Agent Name
poc2_016

MITRE Coverage
2 Tactics

Vulnerabilities
0

Top Rules

Rule 60154

Level 12

Administrators Group Changed

windows

windows_security

group_changed

win_group_changed

PCI DSS

GDPR

HIPAA

NIST 800-53

TSC

Defense Evasion

Privilege Escalation

Recent Alerts

2024/11/27 H5:56:32

Level 12

Administrators Group Changed

Defense Evasion

Privilege Escalation

Agent **poc2_017** 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

180

Agent Name

poc2_017

MITRE Coverage

0 Tactics

Vulnerabilities

0

Top Rules

Rule 61110

Level 10

Multiple System error events

windows

windows_system

Recent Alerts

2024/11/26 H6:44:25

Level 10

Multiple System error events

Multiple System error events

Agent **poc2_029** has reported **514 security events**, including **10 high-severity alerts**. The agent monitors **1 MITRE ATT&CK tactics** and has detected **0 vulnerabilities**.

Total Alerts

514

Security Events

High Severity

10

Critical Events

Compliance

5

Framework Controls

System Information

Agent ID

192

Agent Name

poc2_029

MITRE Coverage

1 Tactics

Vulnerabilities

0

Top Rules

Rule 60204

Level 12

Multiple Windows Logon Failures

windows

windows_security

authentication_failures

PCI DSS

GDPR

HIPAA

NIST 800-53

TSC

Credential Access



Rule 61110

Level 10

Multiple System error events

windows

windows_system



Recent Alerts

2024/11/27 H1:49:33

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/27 H1:44:33

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/27 H1:39:33

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/27 H1:34:32

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/27 H1:34:32

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/27 H1:34:32

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/27 H1:34:26

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/27 H1:31:52

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/27 H1:31:13

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/27 H1:31:13

Level 12

Multiple Windows Logon Failures

Credential Access

Agent **poc2_030** has reported **5 security events**, including **0 high-severity alerts**. The agent monitors **0 MITRE ATT&CK tactics** and has detected **0 vulnerabilities**.

Total Alerts

5

Security Events

High Severity

0

Critical Events

Compliance

0

Framework Controls

System Information

Agent ID

193

Agent Name

poc2_030

MITRE Coverage

0 Tactics

Vulnerabilities

0

Top Rules

Rule 61110

Level 10

Multiple System error events

windows

windows_system

Recent Alerts

2024/11/27 H8:02:32

Level 10

Multiple System error events

2024/11/27 H7:50:07

Level 10

Multiple System error events

2024/11/27 H7:50:06

Level 10

Multiple System error events

2024/11/27 H7:49:30

Level 10

Multiple System error events

2024/11/27 H7:49:18

Level 10

Multiple System error events

Agent **poc2_031** has reported **6 security events**, including **0 high-severity alerts**. The agent monitors **0 MITRE ATT&CK tactics** and has detected **0 vulnerabilities**.

Total Alerts

6

Security Events

High Severity

0

Critical Events

Compliance

0

Framework Controls

System Information

Agent ID

194

Agent Name

poc2_031

MITRE Coverage

0 Tactics

Vulnerabilities

0

Top Rules

Rule 61110

Level 10

Multiple System error events

windows

windows_system

Recent Alerts

2024/11/27 H8:03:55

Level 10

Multiple System error events

2024/11/27 H8:03:09

Level 10

Multiple System error events

2024/11/27 H8:02:23

Level 10

Multiple System error events

2024/11/26 H7:19:34

Level 10

Multiple System error events

2024/11/26 H5:37:50

Level 10

Multiple System error events

2024/11/26 H5:37:50

Level 10

Multiple System error events