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 **41 agents** reveals a security score of **0** (Critical). The analysis identified **0 critical vulnerabilities** and **140 high-severity alerts** that require attention. Security monitoring covers **3 MITRE ATT&CK tactics**.

Security Score	Active Agents	Total Alerts
0	5	147
Critical	of 41 Total	Security Events

Security Events Distribution

Critical Vulnerabilities	0
High Severity Alerts	140
Medium Severity Alerts	7

Security Coverage

MITRE Tactics Covered	3
Active Monitoring	5 Agents
Total Vulnerabilities	0

Key Recommendations

High Severity Alerts

Review and respond to 140 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 **3 MITRE ATT&CK tactics** and **2 unique techniques**, with a total of **140 technique detections**. This analysis provides insights into potential adversary behaviors and helps identify areas for security improvements.

3	2	140
Tactics Monitored	Unique Techniques	Total Detections

Tactics Coverage

Credential Access 139

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 139

ID: Brute Force | Occurrences: 139

Credential Access

Domain Policy Modification 1

ID: Domain Policy Modification | Occurrences: 1

Defense Evasion | Privilege Escalation

Agent **poc2_010** has reported **56 security events**, including **10 high-severity alerts**. The agent monitors **1 MITRE ATT&CK tactics** and has detected **0 vulnerabilities**.

Total Alerts	High Severity	Compliance
56	**10**	**5**
Security Events	Critical Events	Framework Controls

System Information

Agent ID	Agent Name
173	**poc2_010**

MITRE Coverage	Vulnerabilities
1 Tactics	**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_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	High Severity	Compliance
1	1	5
Security Events	Critical Events	Framework Controls

System Information

Agent ID	Agent Name
179	poc2_016

MITRE Coverage	Vulnerabilities
2 Tactics	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_029** has reported **86 security events**, including **10 high-severity alerts**. The agent monitors **1 MITRE ATT&CK tactics** and has detected **0 vulnerabilities**.

Total Alerts	High Severity	Compliance
86	10	5
Security Events	Critical Events	Framework Controls

System Information

Agent ID	Agent Name
192	poc2_029

MITRE Coverage	Vulnerabilities
1 Tactics	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 **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
193	**poc2_030**

MITRE Coverage	Vulnerabilities
0 Tactics	**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

Agent **poc2_031** has reported **3 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
3	0	0
Security Events	Critical Events	Framework Controls

System Information

Agent ID	Agent Name
194	poc2_031

MITRE Coverage	Vulnerabilities
0 Tactics	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