# 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 **9 agents** reveals a security score of **0** (Critical). The analysis identified **0 critical vulnerabilities** and **15 high-severity alerts** that require attention. Security monitoring covers **3 MITRE ATT&CK tactics**.

| Security Score | Active Agents | Total Alerts |
|---|---|---|
| 0 | 5 | 79 |
| Critical | of 9 Total | Security Events |

### Security Events Distribution

| | |
|---|---|
| Critical Vulnerabilities | 0 |
| High Severity Alerts | 15 |
| Medium Severity Alerts | 64 |

### Security Coverage

| | |
|---|---|
| MITRE Tactics Covered | 3 |
| Active Monitoring | 5 Agents |
| Total Vulnerabilities | 0 |

## Key Recommendations

### High Severity Alerts

Review and respond to 15 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 **3 unique techniques**, with a total of **18 technique detections**. This analysis provides insights into potential adversary behaviors and helps identify areas for security improvements.

| 3 | 3 | 18 |
|---|---|---|
| Tactics Monitored | Unique Techniques | Total Detections |

## Tactics Coverage

### Lateral Movement 3

Techniques related to this tactic

### Execution 3

Techniques related to this tactic

### Credential Access 12

Techniques related to this tactic

## Top Techniques

### Brute Force 12

ID: Brute Force | Occurrences: 12

Credential Access

## SMB/Windows Admin Shares

3

ID: SMB/Windows Admin Shares | Occurrences: 3

Lateral Movement | Execution

## Service Execution

3

ID: Service Execution | Occurrences: 3

Lateral Movement | Execution

Agent **falconenv_002_LM_victim** 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 | 0 |
| Security Events | Critical Events | Framework Controls |

## System Information

| Agent ID | Agent Name |
|---|---|
| 109 | falconenv_002_LM_victim |

| MITRE Coverage | Vulnerabilities |
|---|---|
| 2 Tactics | 0 |

## Top Rules

### Rule 92650

Level 12

New Windows Service Created to start from windows root path. Suspicious event as the binary may have been dropped using Windows Admin Shares.

win_evt_channel windows

Lateral Movement Execution

## Recent Alerts

2024/11/11 H6:27:04

Level 12

New Windows Service Created to start from windows root path. Suspicious event as the binary may have been dropped using Windows Admin Shares.

Lateral Movement Execution

Agent **falconenv_004** has reported **39 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 |
|---|---|---|
| **39** | **0** | **0** |
| Security Events | Critical Events | Framework Controls |

## System Information

| Agent ID | Agent Name |
|---|---|
| **111** | **falconenv_004** |

| 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

2024/11/27 H12:18:23 — Level 10

Multiple Windows error application events.

2024/11/21 H11:52:05 — Level 10

Multiple Windows error application events.

2024/11/21 H11:52:05 — Level 10

Multiple Windows error application events.

2024/11/19 H3:41:03 — Level 10

Multiple Windows error application events.

2024/11/19 H3:41:03 — Level 10

Multiple Windows error application events.

2024/11/19 H3:41:03 — Level 10

Multiple Windows error application events.

2024/11/19 H3:41:03 — Level 10

Multiple Windows error application events.

2024/11/19 H3:13:03 — Level 10

Multiple Windows error application events.

2024/11/19 H3:13:03 — Level 10

Multiple Windows error application events.

2024/11/19 H3:13:02

Level 10

Multiple Windows error application events.

Agent **falconenv_005** has reported **36 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 |
|---|---|---|
| **36** | **0** | **5** |
| Security Events | Critical Events | Framework Controls |

## System Information

| Agent ID | Agent Name |
|---|---|
| **112** | **falconenv_005** |

| 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

2024/11/14 H11:52:53

Level 10

Multiple Windows error application events.

2024/11/14 H11:52:53

Level 10

Multiple Windows error application events.

2024/11/14 H11:52:53

Level 10

Multiple Windows error application events.

2024/11/14 H11:52:47

Level 10

Multiple Windows error application events.

2024/11/14 H7:06:55

Level 10

Multiple Windows error application events.

2024/11/14 H7:06:55

Level 10

Multiple Windows error application events.

2024/11/14 H7:06:55

Level 10

Multiple Windows error application events.

2024/11/14 H7:06:55

Level 10

Multiple Windows error application events.

2024/11/14 H7:04:45

Level 10

Multiple Windows error application events.

2024/11/14 H7:01:20

Level 10

Multiple Windows error application events.

Agent **falconenv_006_0_LM_victim** has reported **2 security events**, including **2 high-severity alerts**. The agent monitors **2 MITRE ATT&CK tactics** and has detected **0 vulnerabilities**.

| Total Alerts | High Severity | Compliance |
|---|---|---|
| 2 | 2 | 0 |
| Security Events | Critical Events | Framework Controls |

## System Information

| Agent ID | Agent Name |
|---|---|
| 113 | falconenv_006_0_LM_victim |

| MITRE Coverage | Vulnerabilities |
|---|---|
| 2 Tactics | 0 |

## Top Rules

### Rule 92650

Level 12

New Windows Service Created to start from windows root path. Suspicious event as the binary may have been dropped using Windows Admin Shares.

win_evt_channel windows

Lateral Movement Execution

## Recent Alerts

2024/11/15 H3:01:50

Level 12

New Windows Service Created to start from windows root path. Suspicious event as the binary may have been dropped using Windows Admin Shares.

Lateral Movement Execution

2024/11/15 H2:50:20

Level 12

New Windows Service Created to start from windows root path. Suspicious event as the binary may have been dropped using Windows Admin Shares.

Lateral Movement Execution

Agent **falconenv_007_0_SMB_victim** has reported **1 security events**, including **1 high-severity alerts**. The agent monitors **1 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 |
|---|---|
| 115 | falconenv_007_0_SMB_victim |

| 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

2024/11/15 H2:22:07

Level 12

Multiple Windows Logon Failures

Credential Access

Go to Table of Contents