

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

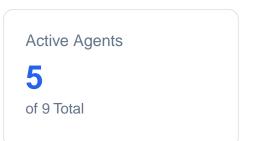
| Executive Summary | 3 |
|-------------------------------|----------|
| <u>Vulnerability Analysis</u> | 4 |
| MITRE ATT&CK Analysis | <u>5</u> |

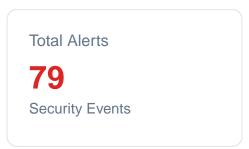
AGENT ANALYSIS

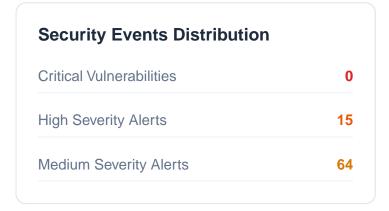
| Agent 1 Analysis | <u>6</u> |
|------------------|----------|
| Agent 2 Analysis | 7 |
| Agent 3 Analysis | 8 |
| Agent 4 Analysis | <u>9</u> |
| Agent 5 Analysis | 10 |

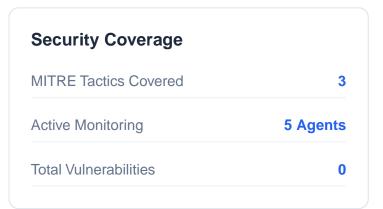
Security assessment across **9 agents** reveals a security score of **0** (Critical). The analysis identified **0 critical vulnerabilities** and **15 high-severity alerts** that require attention. Security monitoring covers **3 MITRE ATT&CK tactics**.











Key Recommendations

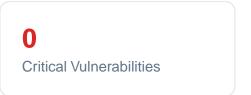
High Severity Alerts

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.







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.

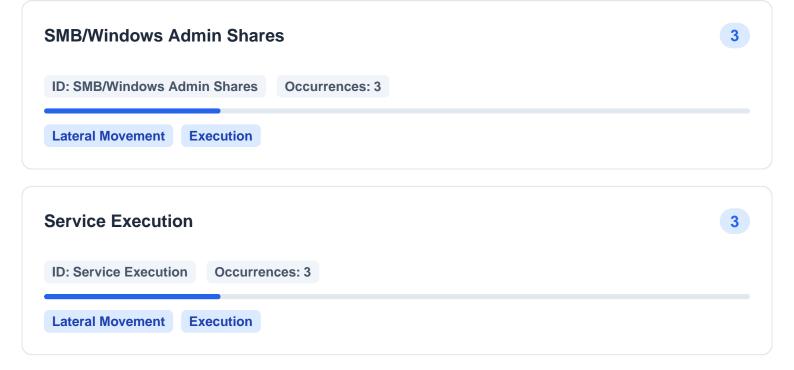


Tactics Coverage



Top Techniques





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

1
Security Events

High Severity

1
Critical Events

Compliance

O

Framework Controls

System Information

Agent ID
109

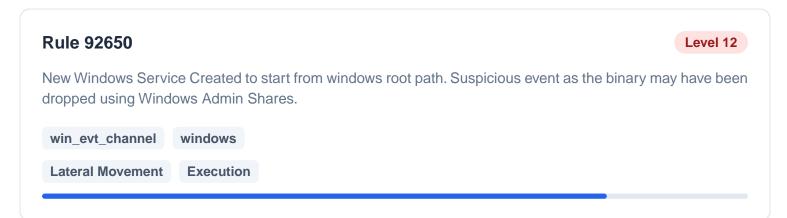
MITRE Coverage
2 Tactics

Agent Name
falconenv_002_LM_victim

Vulnerabilities

0

Top Rules



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.

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

39
Security Events

High Severity

O

Critical Events

Compliance

O

Framework Controls

System Information

Agent ID
111

MITRE Coverage
0 Tactics

Agent Name
falconenv_004

Vulnerabilities
0

Top Rules





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

36

Security Events

High Severity

N

Critical Events

Compliance

5

Framework Controls

System Information

Agent ID

112

Agent Name

falconenv_005

MITRE Coverage

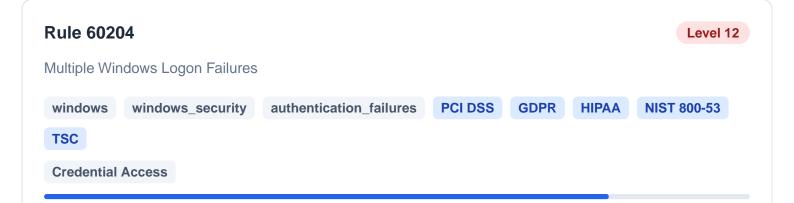
1 Tactics

Vulnerabilities

0

Top Rules





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

2

Security Events

High Severity

2

Critical Events

Compliance

0

Framework Controls

System Information

Agent ID

113

Agent Name

falconenv_006_0_LM_victim

MITRE Coverage

2 Tactics

Vulnerabilities

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

1
Security Events

High Severity

1
Critical Events

Compliance

5
Framework Controls

System Information

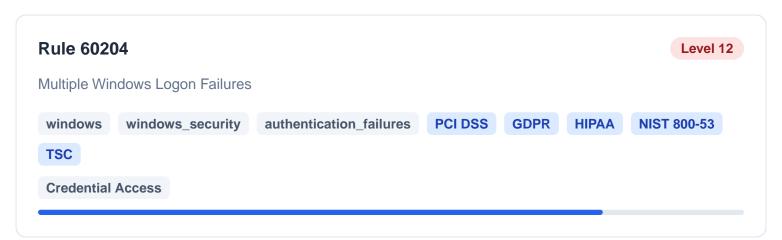
Agent ID
115

MITRE Coverage
1 Tactics

Agent Name
falconenv_007_0_SMB_victim

Vulnerabilities
0

Top Rules



Recent Alerts

Credential Access

2024/11/15 H2:22:07

Multiple Windows Logon Failures