

MITRE ATT&CK report

| ID | Name | IP address | Version | Manager | Operating system | Registration date | Last keep alive |
|-----|------|--------------|---------------|--------------|--|-----------------------------|-----------------------------|
| 001 | MSI | 10.22.137.43 | Wazuh v4.12.0 | wazuh-server | Microsoft Windows 11 Home 10.0.26100.4946 | Aug 26, 2025 @ 00:29:56.000 | Aug 26, 2025 @ 00:55:50.000 |

Group: default

Explore security alerts mapped to adversary tactics and techniques for better threat understanding.

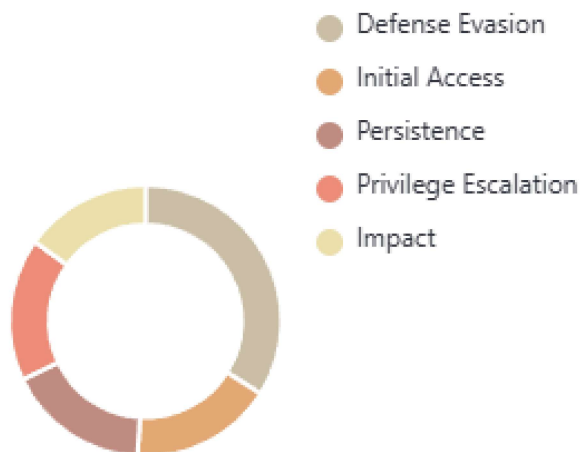
🕒 2025-08-25T06:25:59 to 2025-08-26T06:25:59

🔍 manager.name: wazuh-server AND rule.mitre.id: * AND agent.id: 001

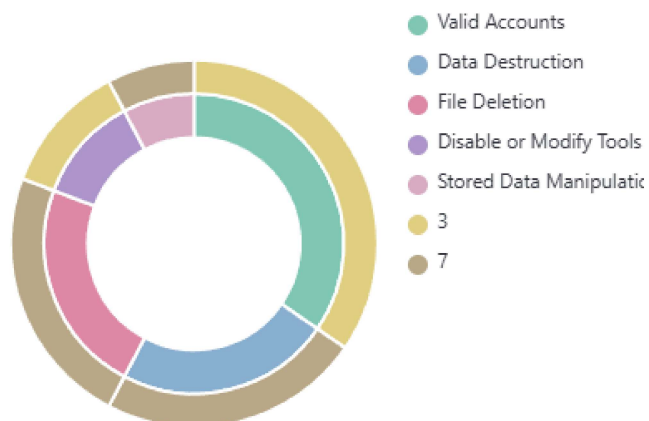
Alerts evolution over time



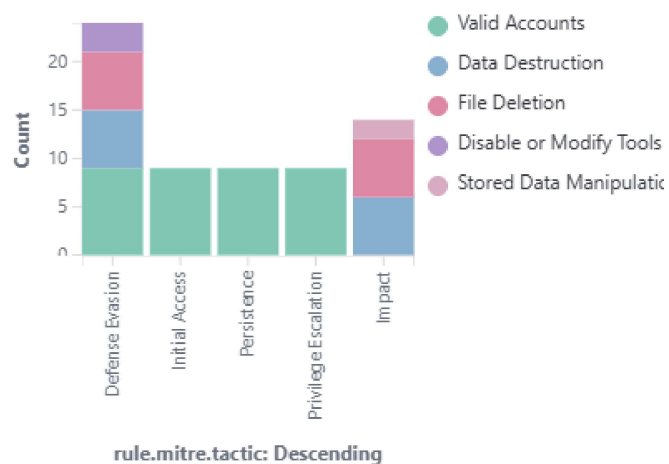
Top tactics



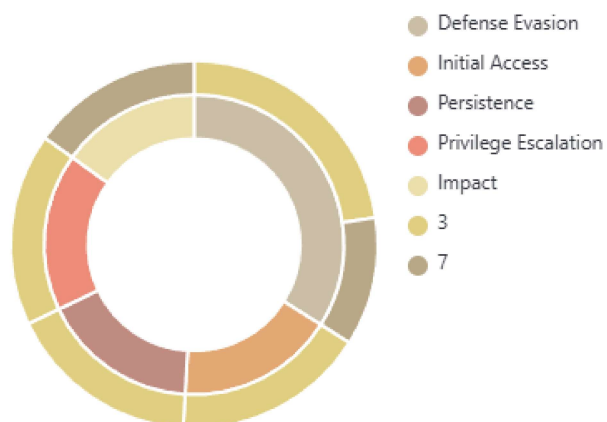
Rule level by attack



MITRE attacks by tactic



Rule level by tactic



Alerts summary

| Rule ID | Description | Level | Count |
|---------|-----------------------------|-------|-------|
| 60106 | Windows Logon Success | 3 | 9 |
| 553 | File deleted. | 7 | 6 |
| 506 | Wazuh agent stopped. | 3 | 3 |
| 550 | Integrity checksum changed. | 7 | 2 |