wazuh.

MITRE ATT&CK report

Warning. Agent is disconnected

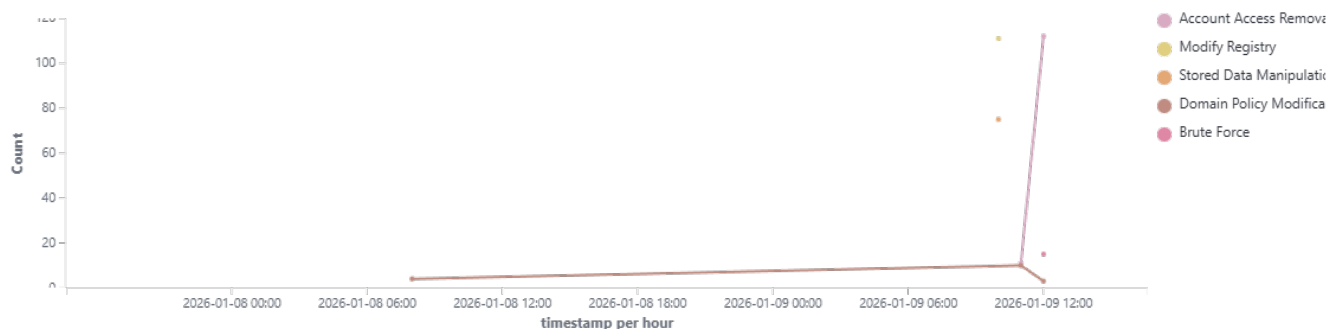| ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
004	aditys-agent	192.168.1.46	Wazuh v4.14.1	wazuh-server	Microsoft Windows 10 Pro 10.0.19045.6466	Jan 8, 2026 @ 02:45:52.000	Jan 9, 2026 @ 10:16:34.000

Group: default

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

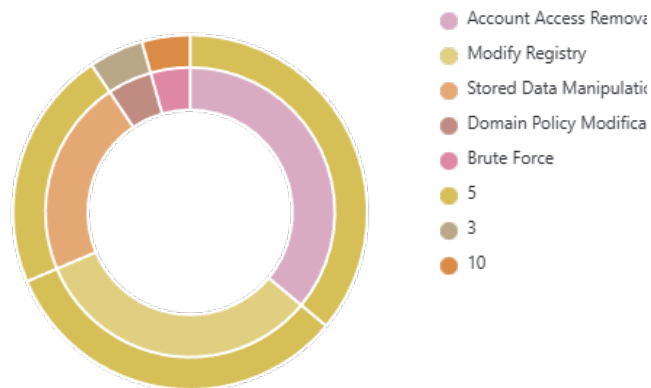🕐 2026-01-07T16:38:57 to 2026-01-09T16:38:57

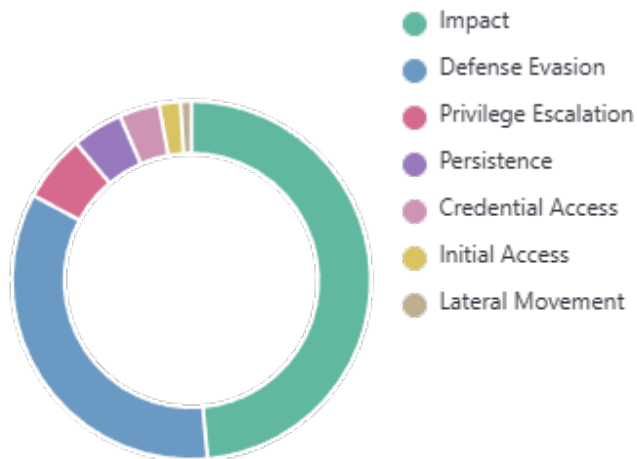🔍 manager.name: wazuh-server AND rule.mitre.id: * AND agent.id: 004

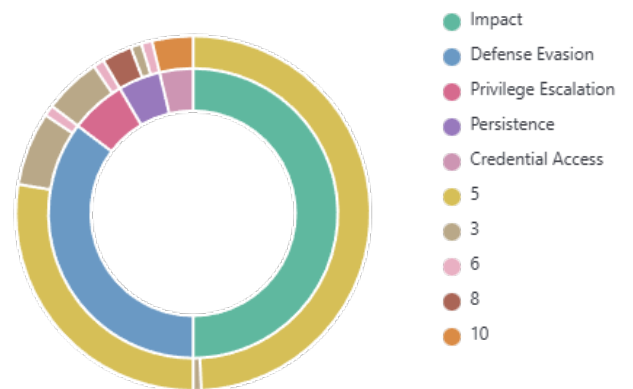## Alerts evolution over time

Top tactics

Rule level by attack

Legend:
- Impact
- Defense Evasion
- Privilege Escalation
- Persistence
- Credential Access
- Initial Access
- Lateral Movement

MITRE attacks by tactic

Legend:
- Account Access Remova
- Modify Registry
- Stored Data Manipulatio
- Domain Policy Modifica
- Brute Force

X-axis: rule.mitre.tactic: Descending
Y-axis: Count

Rule level by tactic

Legend:
- Impact
- Defense Evasion
- Privilege Escalation
- Persistence
- Credential Access
- 5
- 3
- 6
- 8
- 10

Alerts summary

Rule ID	Description	Level	Count
60122	Logon Failure - Unknown user or bad password	5	123
594	Registry Key Integrity Checksum Changed	5	38
750	Registry Value Integrity Checksum Changed	5	37
598	Registry Key Entry Added to the System	5	24
67028	Special privileges assigned to new logon.	3	17
60204	Multiple Windows Logon Failures	10	15
752	Registry Value Entry Added to the System	5	12
60110	User account changed	8	11
504	Wazuh agent disconnected.	3	5
60118	Windows Workstation Logon Success	3	4
67018	System shutdown initiated.	3	3
92652	Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack.	6	2
92657	Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that WINDOWS is allowed to perform RDP connections	6	2
506	Wazuh agent stopped.	3	1