info@wazuh.com
https://wazuh.com

MITRE ATT&CK report

Warning. Agent is disconnected

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
002	ubuntu-devangs	192.168.1.51	Wazuh v4.14.1	wazuh-server	Ubuntu 20.04.6 LTS	Jan 8, 2026 @ 01:14:39.000	Jan 8, 2026 @ 11:45:15.000

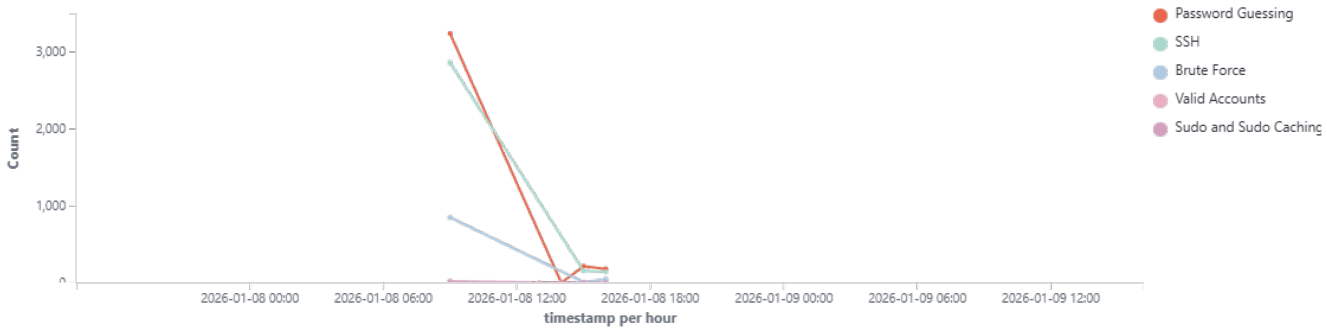
Group: default

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

2026-01-07T16:12:14 to 2026-01-09T16:12:14

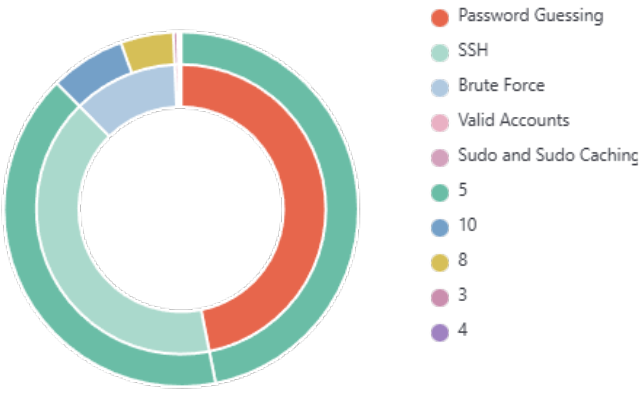
manager.name: wazuh-server AND rule.mitre.id: * AND agent.id: 002

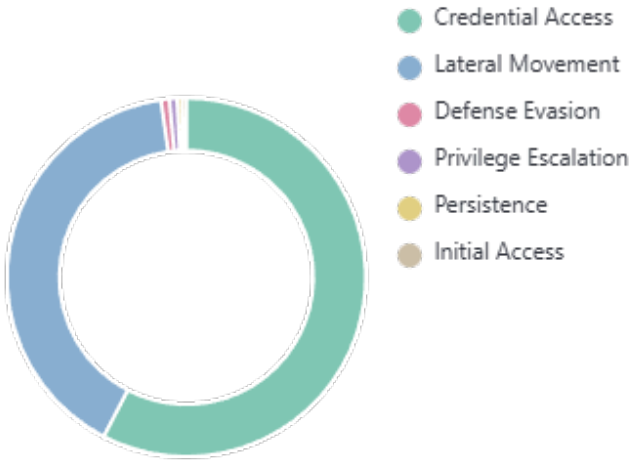
Alerts evolution over time



Top tactics

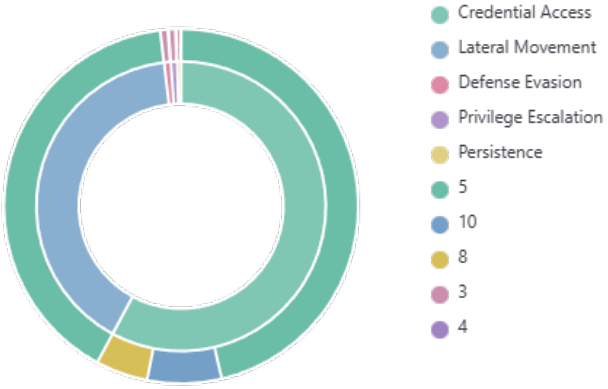
Rule level by attack





MITRE attacks by tactic

Rule level by tactic



Alerts summary

Rule ID	Description	Level	Count
5710	sshd: Attempt to login using a non-existent user	5	1936
5760	sshd: authentication failed.	5	1224
5503	PAM: User login failed.	5	475
2502	syslog: User missed the password more than one time	10	410
5758	Maximum authentication attempts exceeded.	8	374
5551	PAM: Multiple failed logins in a small period of time.	10	64
40111	Multiple authentication failures.	10	48
5501	PAM: Login session opened.	3	30
5402	Successful sudo to ROOT executed.	3	18
5763	sshd: brute force trying to get access to the system. Authentication failed.	10	9
504	Wazuh agent disconnected.	3	4
5403	First time user executed sudo.	4	4
5902	New user added to the system.	8	3
5404	Three failed attempts to run sudo	10	2
5712	sshd: brute force trying to get access to the system. Non existent user.	10	1
5715	sshd: authentication success.	3	1