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	Metasploitable3	192.168.56.105	Wazuh v4.9.2	wazuh.manager	Ubuntu 14.04.6 LTS, Trusty Tahr	Nov 26, 2024 @ 06:52:09.000	Dec 8, 2024 @ 21:11:45.000

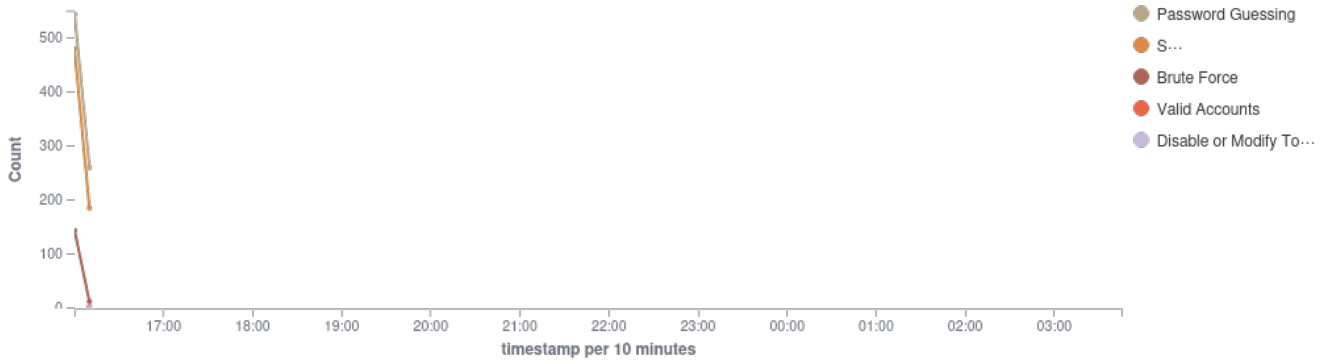
Group: default

Security events from the knowledge base of adversary tactics and techniques based on real-world observations

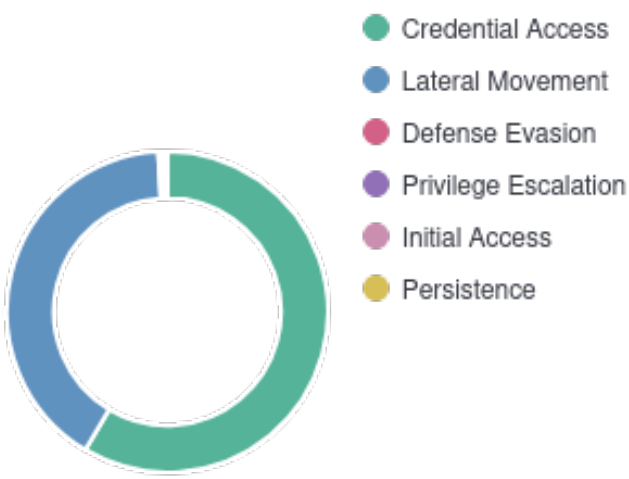
2024-12-08T16:00:00 to 2024-12-09T03:46:09

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

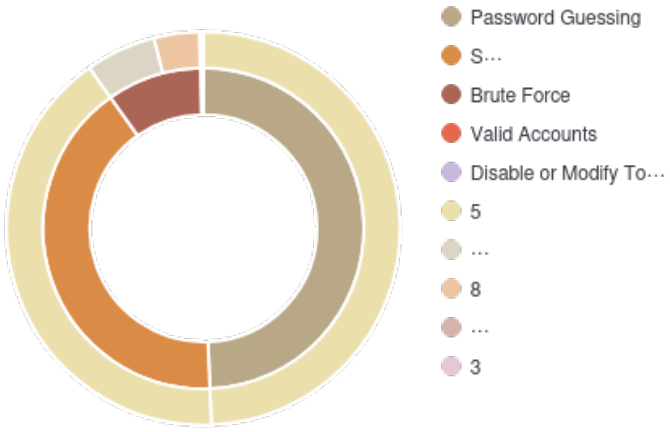
Alerts evolution over time



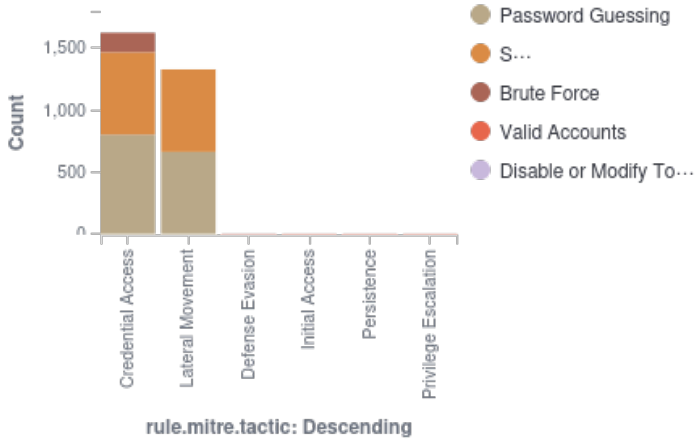
Top tactics



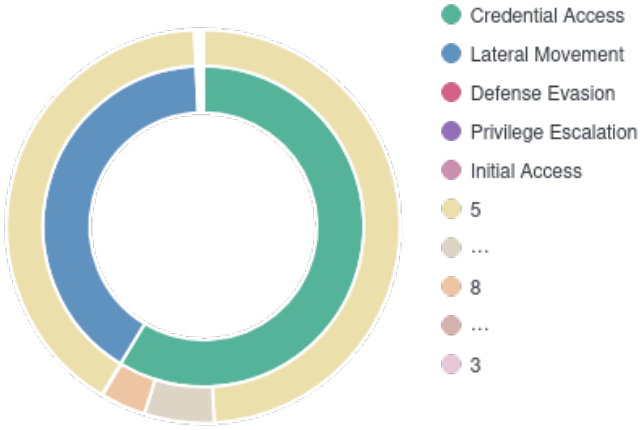
Rule level by attack



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	659
5503	PAM: User login failed.	5	139
2502	syslog: User missed the password more than one time	10	70
5758	Maximum authentication attempts exceeded.	8	61
5551	PAM: Multiple failed logins in a small period of time.	10	19
5760	sshd: authentication failed.	5	6
5712	sshd: brute force trying to get access to the system. Non existent user.	10	5
5501	PAM: Login session opened.	3	2
40112	Multiple authentication failures followed by a success.	12	1
506	Wazuh agent stopped.	3	1
5402	Successful sudo to ROOT executed.	3	1