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
001	vbox	192.168.56.109	Wazuh v4.9.2	wazuh.manager	Debian GNU/Linux 12	Nov 26, 2024 @ 06:19:41.000	Dec 8, 2024 @ 21:02:15.000

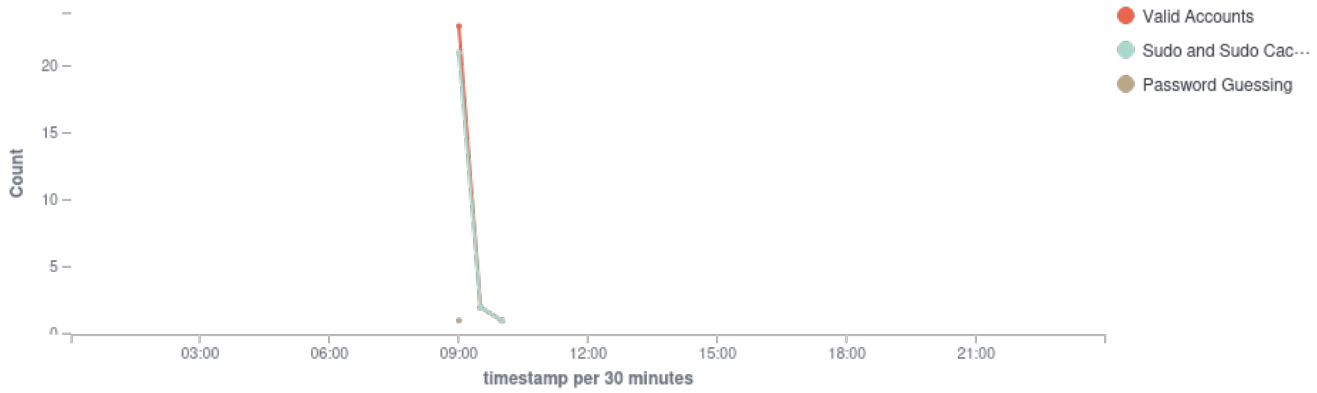
Group: default

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

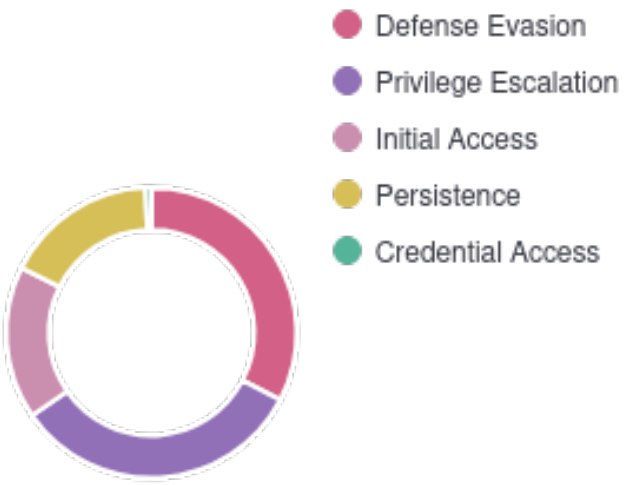
2024-12-07T00:00:00 to 2024-12-07T23:59:59

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

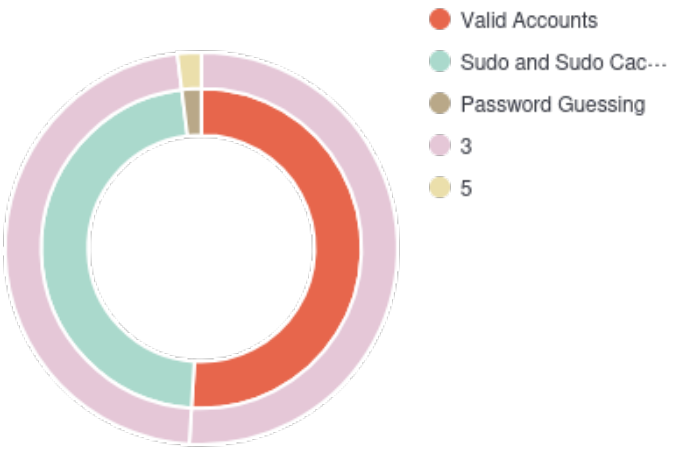
Alerts evolution over time



Top tactics

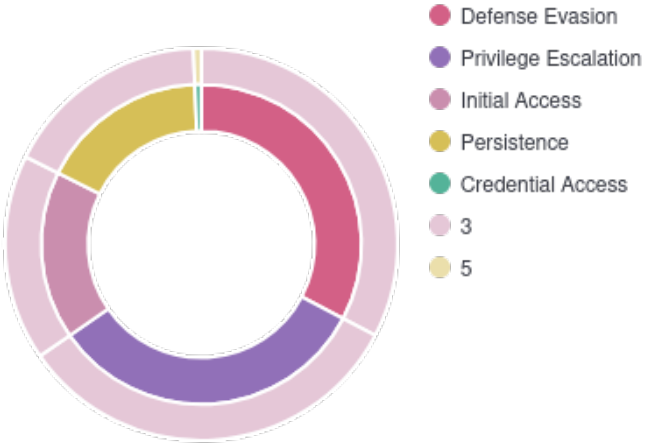


Rule level by attack



MITRE attacks by tactic

Rule level by tactic



Alerts summary

Rule ID	Description	Level	Count
5501	PAM: Login session opened.	3	26
5402	Successful sudo to ROOT executed.	3	24
5503	PAM: User login failed.	5	1