MITRE ATT&CK report

Warning. Agent is disconnected

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	lib-virtual-machine	192.168.57.133	Wazuh v4.7.2	random-virtual-machine	Ubuntu 22.04.4 LTS	Feb 29, 2024 @ 03:04:54.000	Mar 13, 2024 @ 18:43:26.000

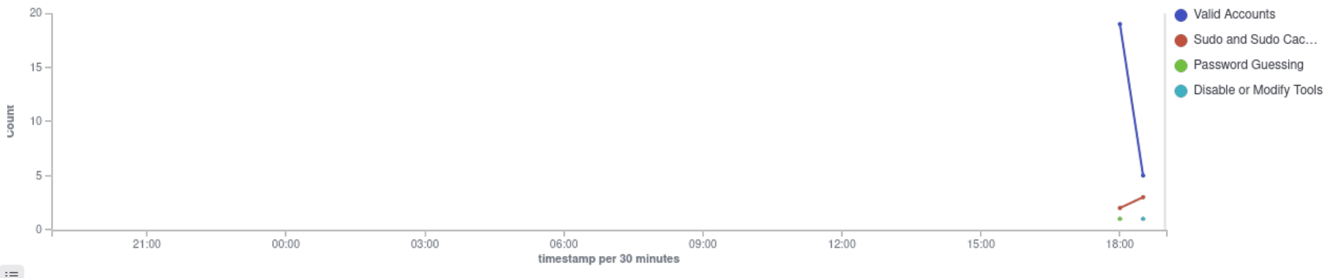
Group: default

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

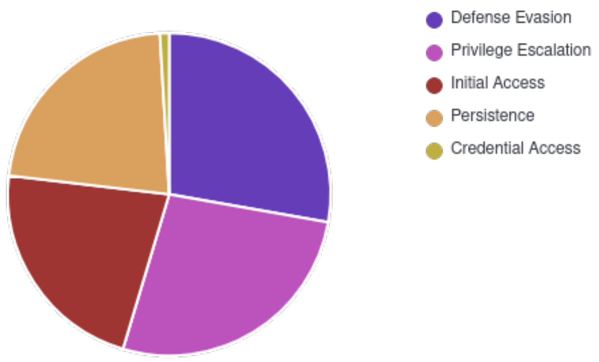
2024-03-12T18:56:41 to 2024-03-13T18:56:41

manager.name: random-virtual-machine AND rule.mitre.id: * AND agent.id: 001

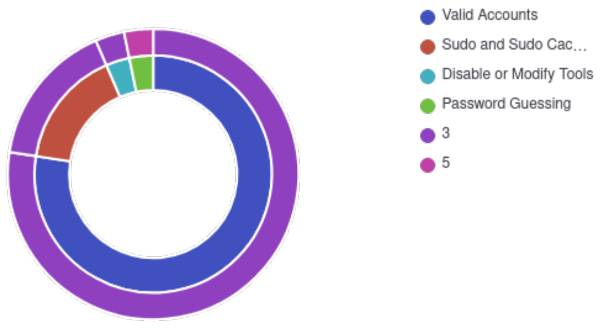
Mitre alerts evolution



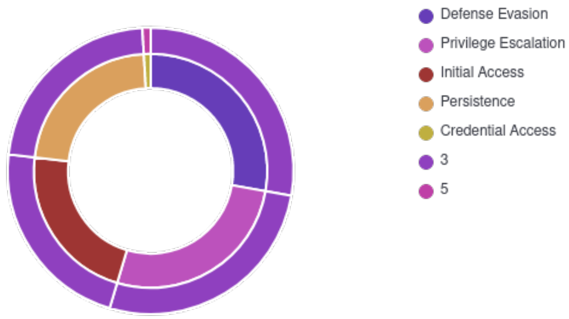
Top tactics pie



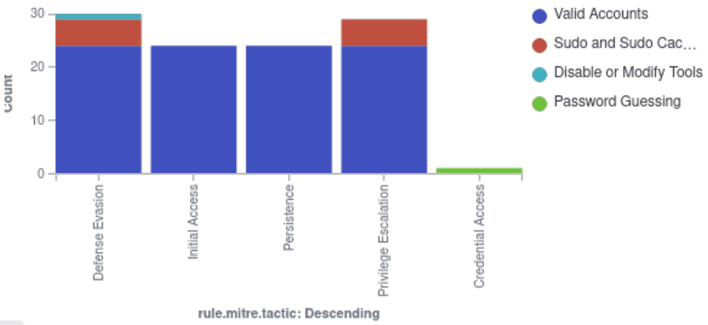
Alerts level by attack



Alerts level by tactic



Top tactics



Alerts summary

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