Peersoc

MITRE ATT&CK report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	second_server	167.235.23.58	Wazuh v4.7.5	ubuntu-4gb-nbg1-2	Ubuntu 24.04.1 LTS	Nov 8, 2024 @ 11:02:54.000	Nov 8, 2024 @ 14:34:14.000

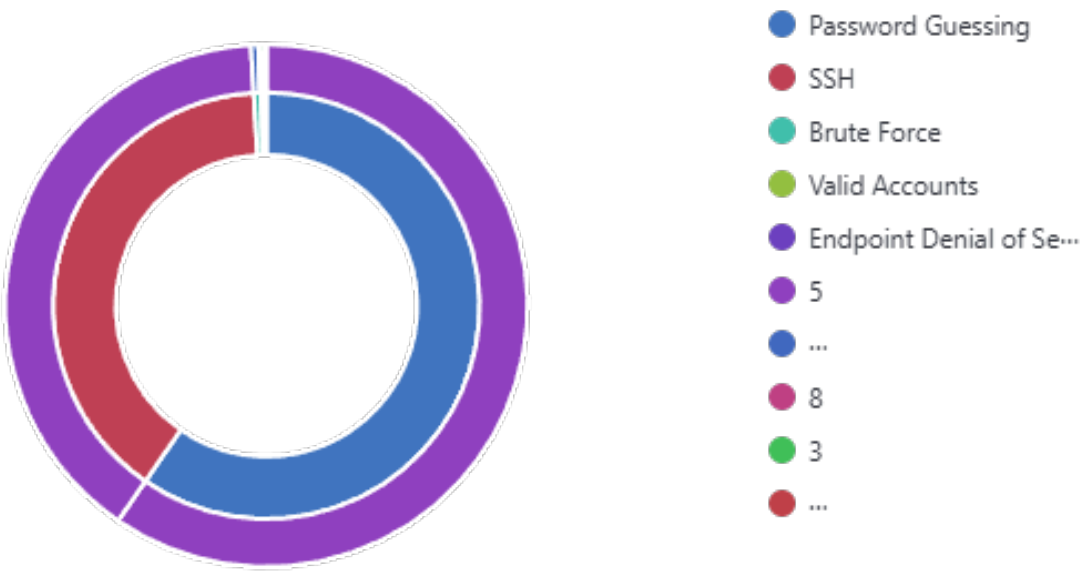
Group: default

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

2024-11-07T17:34:20 to 2024-11-08T17:34:20

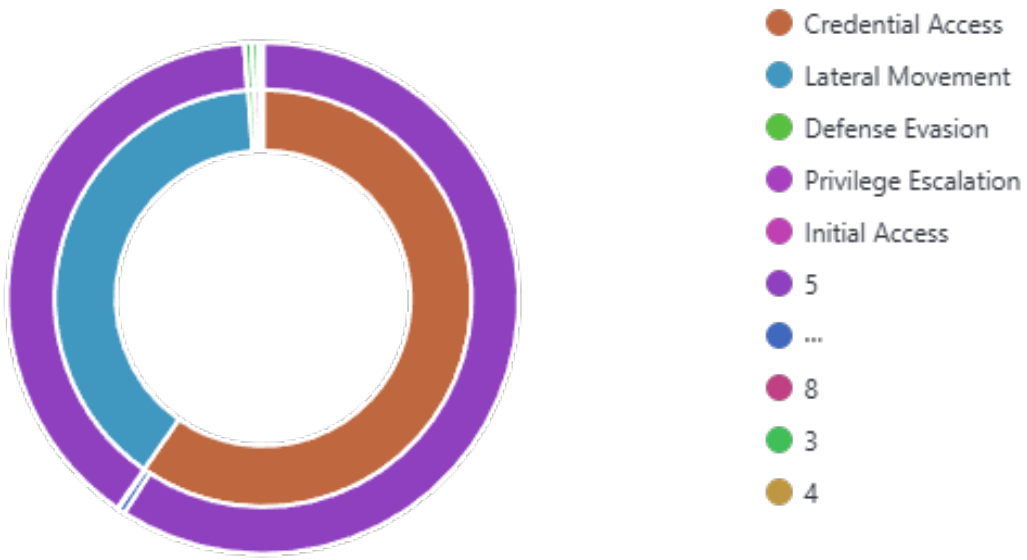
manager.name: ubuntu-4gb-nbg1-2 AND rule.mitre.id: * AND agent.id: 001

Alerts level by attack

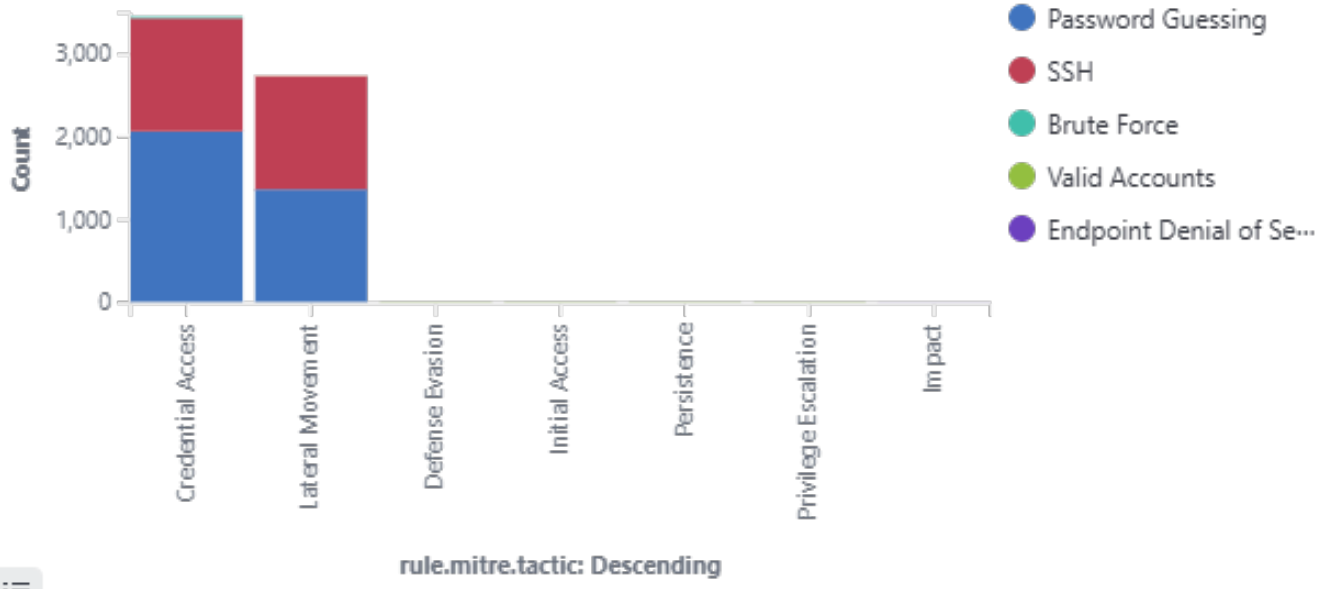


Peersoc

Alerts level by tactic

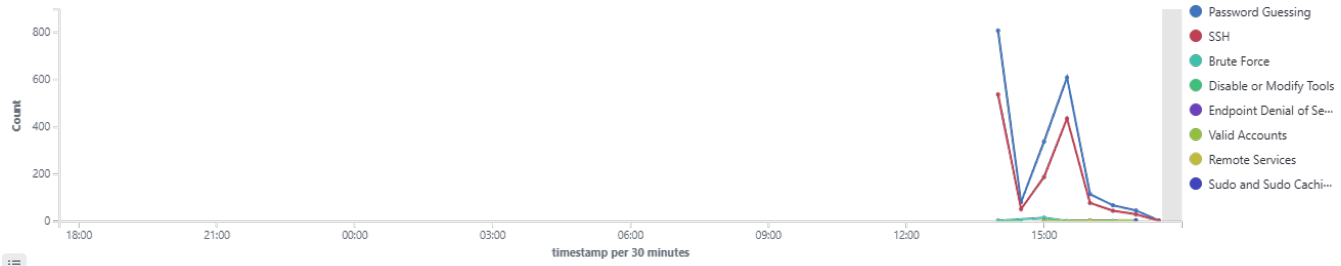


Top tactics

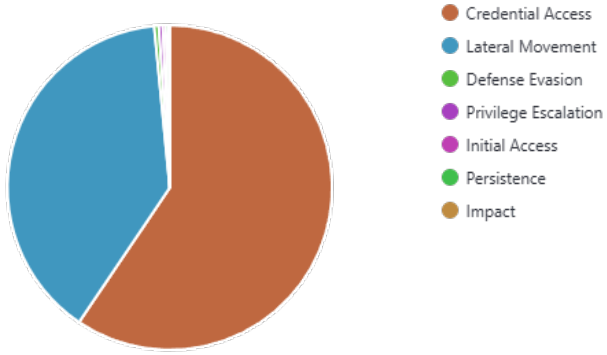


Peersoc

Mitre alerts evolution



Top tactics pie



Peersoc

Alerts summary

Rule ID	Description	Level	Count
5710	sshd: Attempt to login using a non-existent user	5	1023
5503	PAM: User login failed.	5	701
5760	sshd: authentication failed.	5	346
5501	PAM: Login session opened.	3	8
5712	sshd: brute force trying to get access to the system. Non existent user.	10	8
5108	System running out of memory. Availability of the system is in risk.	12	4
5551	PAM: Multiple failed logins in a small period of time.	10	4
2502	syslog: User missed the password more than one time	10	3
5402	Successful sudo to ROOT executed.	3	3
5758	Maximum authentication attempts exceeded.	8	3
506	Wazuh agent stopped.	3	2
5715	sshd: authentication success.	3	2
5403	First time user executed sudo.	4	1
5763	sshd: brute force trying to get access to the system. Authentication failed.	10	1