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

MITRE ATT&CK report

ID	Name	IP	Version	Manager	OS	Registration date	Last keep alive
001	WarBuntu	192.168.65.128	Wazuh v4.3.10	wazuh-server	Ubuntu 22.10	Mar 24, 2023 @ 14:20:46.000	Apr 27, 2023 @ 23:13:33.000

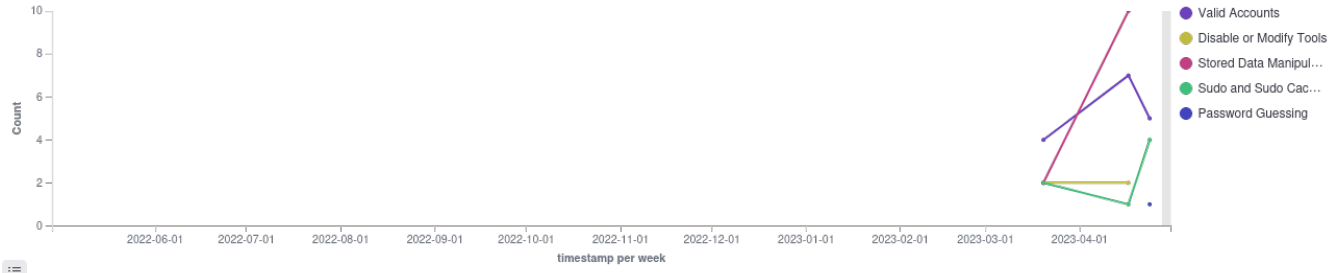
Group: default

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

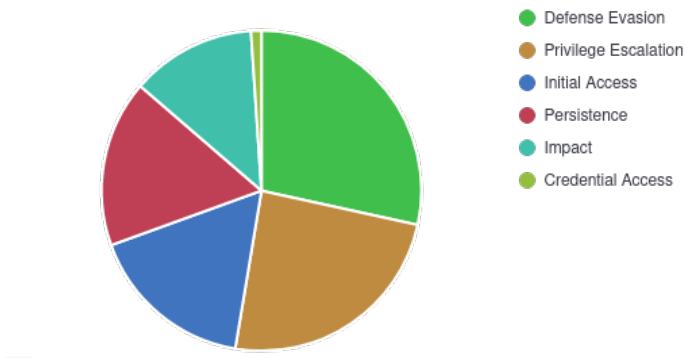
2022-04-28T00:13:32 to 2023-04-28T00:13:32

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

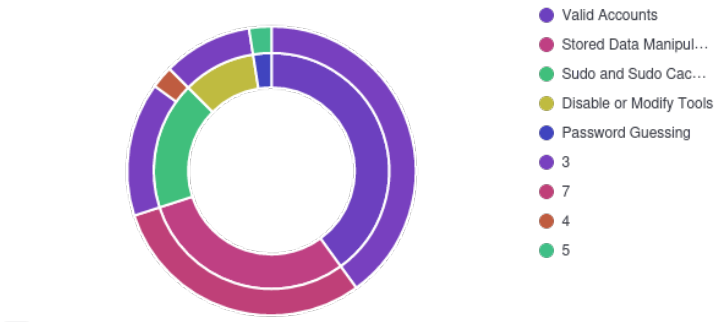
Mitre alerts evolution



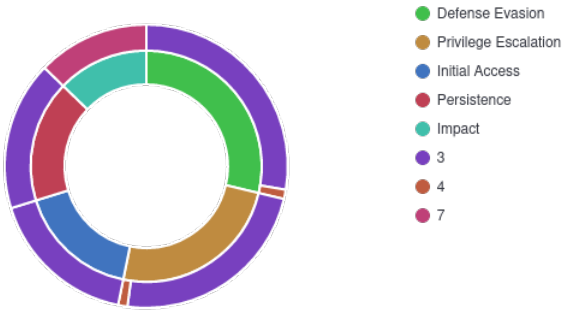
Top tactics pie



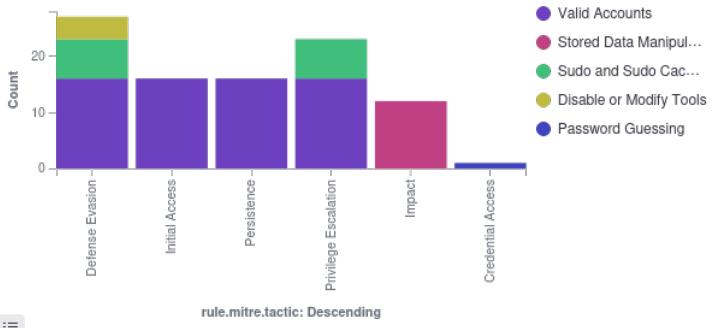
Alerts level by attack



Alerts level by tactic



Top tactics



Alerts summary

Rule ID	Description	Level	Count
5501	PAM: Login session opened.	3	16
550	Integrity checksum changed.	7	12
5402	Successful sudo to ROOT executed.	3	6
506	Ossec agent stopped.	3	4
5403	First time user executed sudo.	4	1
5503	PAM: User login failed.	5	1