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

MITRE ATT&CK report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
002	wazuh_agent_ubuntu_2	172.20.0.7	Wazuh v4.9.0	wazuh-manager-4.9.0-7102	Ubuntu 22.04.3 LTS	May 14, 2024 @ 14:50:11.000	May 16, 2024 @ 15:34:39.000

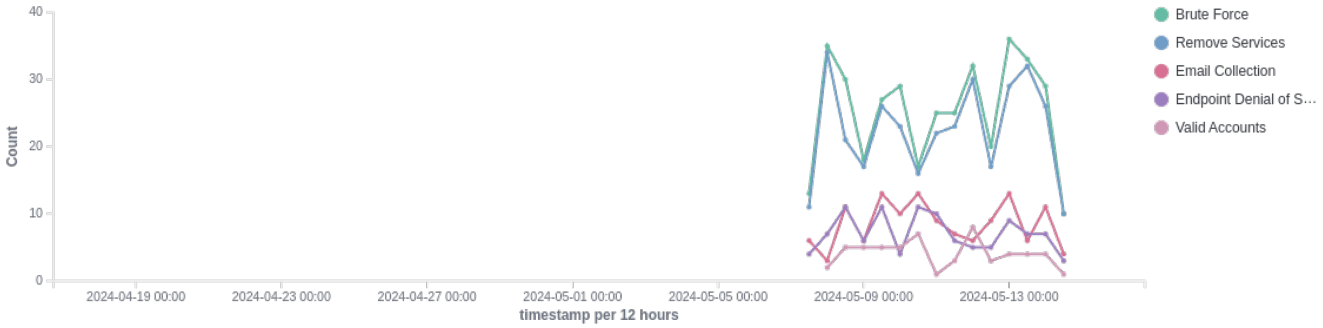
Group: default

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

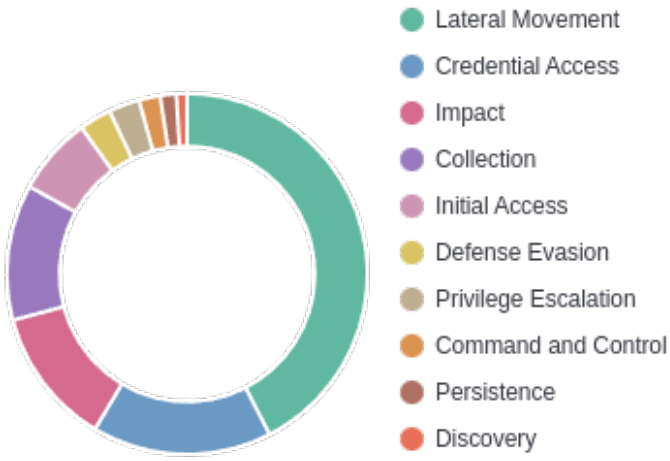
2024-04-16T17:34:48 to 2024-05-16T17:34:48

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

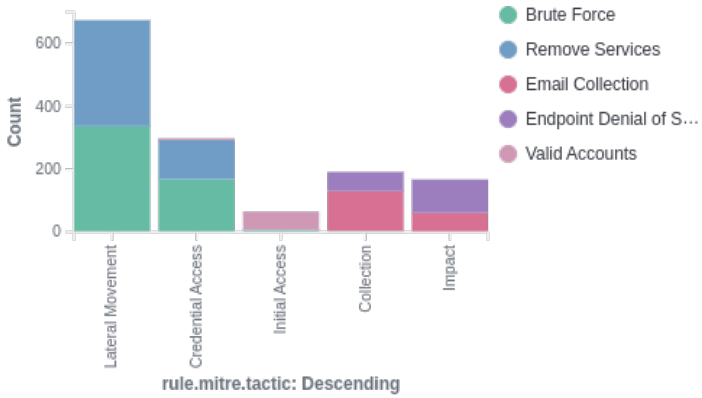
Mitre alerts evolution



Top tactics

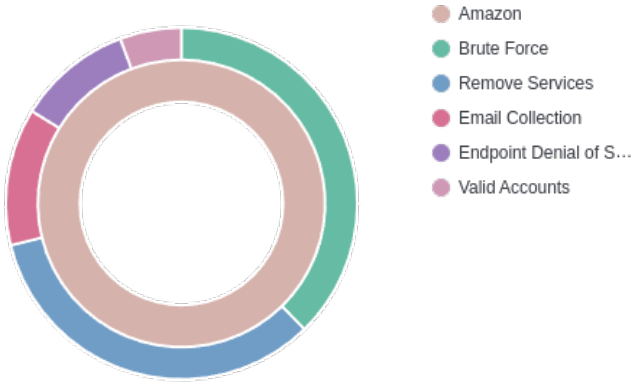


Attacks by technique



Top tactics by agent

Attack by agent



Alerts summary

Rule ID	Description	Level	Count
5703	sshd: Possible breakin attempt (high number of reverse lookup errors).	10	121
5702	sshd: Reverse lookup error (bad ISP or attack).	5	104
5701	sshd: Possible attack on the ssh server (or version gathering).	8	96
5758	Maximum authentication attempts exceeded.	8	88
5712	sshd: brute force trying to get access to the system.	10	38
3351	Postfix: Multiple relaying attempts of spam.	6	10
3335	Postfix: too many errors after RCPT from unknown	6	8
3602	Imapd user login.	3	8
4507	Netscreen firewall: Successfull admin login	8	8
5601	telnetd: Connection refused by TCP Wrappers.	5	8
3158	sendmail: Multiple pre-greetings rejects.	10	7
3910	Courier brute force (multiple failed logins).	10	7
4340	PIX: Firewall configuration changed.	8	7
4722	Cisco IOS: Successful login to the router.	3	7
5104	Interface entered in promiscuous(sniffing) mode.	8	7
5304	User successfully changed UID.	3	7
5403	First time user executed sudo.	4	7
2833	Root's crontab entry changed.	8	6
2960	User added to group.	2	6
3152	sendmail: Multiple attempts to send e-mail from a previously rejected sender (access).	6	6
3156	sendmail: Multiple rejected e-mails from same source ip.	10	6
3302	Postfix: Rejected by access list (Requested action not taken).	6	6
3330	Postfix process error.	10	6
3356	Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked).	10	6
4550	Netscreen firewall: Multiple critical messages from same source IP.	10	6
4551	Netscreen firewall: Multiple critical messages.	10	6
4810	SonicWall: Firewall administrator login.	3	6
4851	SonicWall: Multiple firewall error messages.	10	6
5303	User successfully changed UID to root.	3	6
5706	sshd: insecure connection attempt (scan).	6	6
2964	perdition: Multiple connection attempts from same source.	10	5
3102	sendmail: Sender domain does not have any valid MX record (Requested action aborted).	5	5
3104	sendmail: Attempt to use mail server as relay (550: Requested action not taken).	6	5
3108	sendmail: Sendmail rejected due to pre-greeting.	6	5
3151	sendmail: Sender domain has bogus MX record. It should not be sending e-mail.	10	5
3306	Postfix: IP Address black-listed by anti-spam (blocked).	6	5
3352	Postfix: Multiple attempts to send e-mail from a rejected sender IP (access).	6	5
3852	ms-exchange: Multiple e-mail 500 error code (spam).	9	5
3911	Courier: Multiple connection attempts from same source.	10	5

Rule ID	Description	Level	Count
4335	PIX: AAA (VPN) authentication successful.	3	5
4339	PIX: Firewall configuration deleted.	8	5
4505	Netscreen Erase sequence started.	11	5
505	Ossec agent removed.	3	5
5132	Unsigned kernel module was loaded	11	5
592	Log file size reduced.	8	5
593	Microsoft Event log cleared.	9	5
2301	xinetd: Excessive number connections to a service.	10	4
2502	syslog: User missed the password more than one time	10	4
3105	sendmail: Sender domain is not found (553: Requested action not taken).	5	4
3153	sendmail: Multiple relaying attempts of spam.	6	4