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

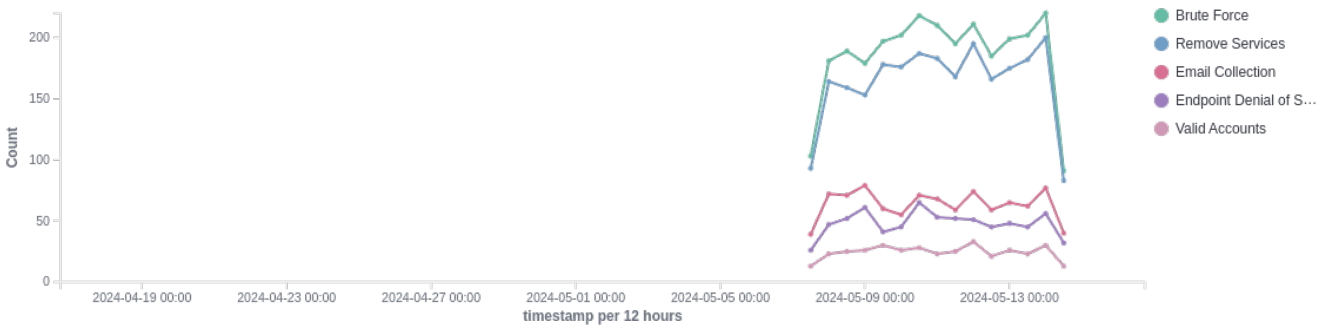
MITRE ATT&CK report

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

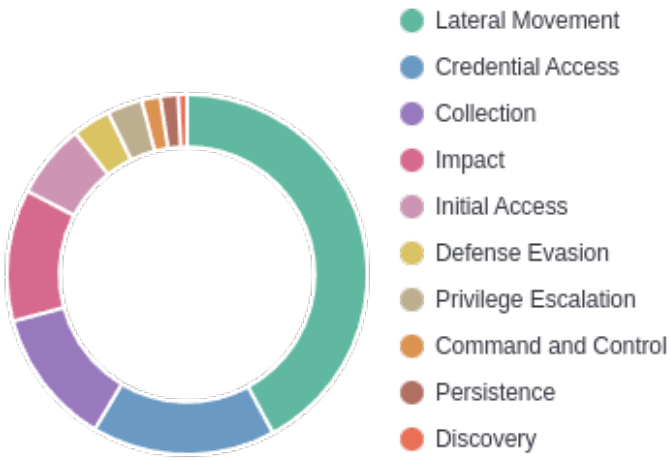
2024-04-16T17:54:21 to 2024-05-16T17:54:21

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

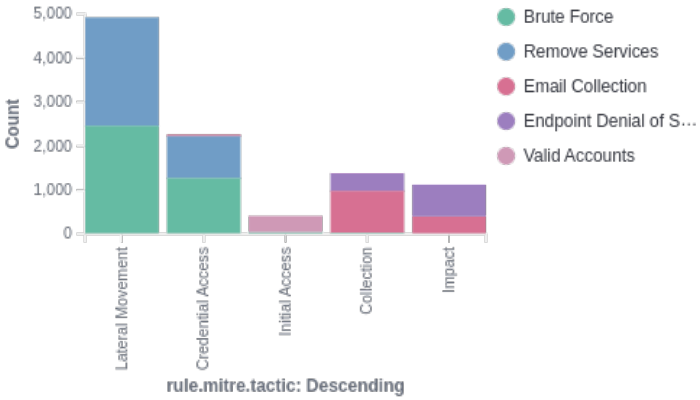
Mitre alerts evolution



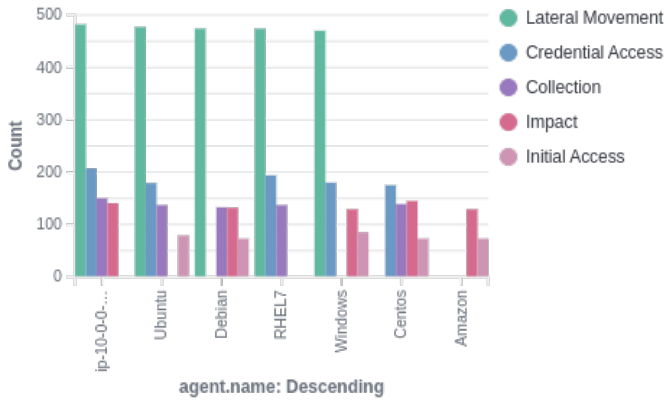
Top tactics



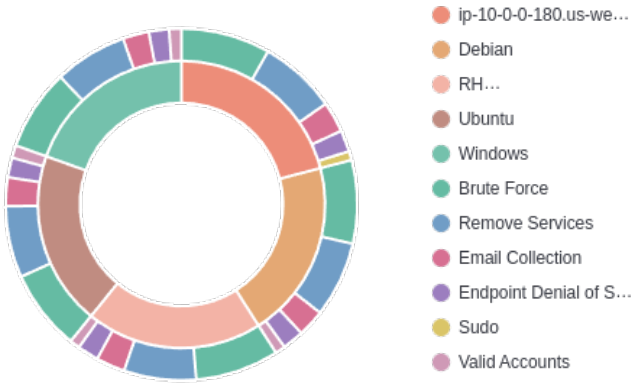
Attacks by technique



Top tactics by agent



Attack by agent



Alerts summary

Rule ID	Description	Level	Count
5702	sshd: Reverse lookup error (bad ISP or attack).	5	772
5703	sshd: Possible breakin attempt (high number of reverse lookup errors).	10	755
5701	sshd: Possible attack on the ssh server (or version gathering).	8	752
5758	Maximum authentication attempts exceeded.	8	646
5712	sshd: brute force trying to get access to the system.	10	309
4551	Netscreen firewall: Multiple critical messages.	10	46
4722	Cisco IOS: Successful login to the router.	3	46
4335	PIX: AAA (VPN) authentication successful.	3	41
3158	sendmail: Multiple pre-greetings rejects.	10	40
5132	Unsigned kernel module was loaded	11	40
593	Microsoft Event log cleared.	9	40
3104	sendmail: Attempt to use mail server as relay (550: Requested action not taken).	6	38
3351	Postfix: Multiple relaying attempts of spam.	6	37
3910	Courier brute force (multiple failed logins).	10	37
4323	PIX: Successful login.	3	37
4506	Netscreen firewall: Successfull admin login	8	37
5631	telnetd: Multiple connection attempts from same source (possible scan).	10	37
3151	sendmail: Sender domain has bogus MX record. It should not be sending e-mail.	10	36
4337	PIX: The PIX is disallowing new connections.	8	36
4851	SonicWall: Multiple firewall error messages.	10	36
3302	Postfix: Rejected by access list (Requested action not taken).	6	35
3356	Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked).	10	35
4505	Netscreen Erase sequence started.	11	35
5302	User missed the password to change UID to root.	9	35
3352	Postfix: Multiple attempts to send e-mail from a rejected sender IP (access).	6	34
3396	Postfix: hostname verification failed	6	34
5551	PAM: Multiple failed logins in a small period of time.	10	34
2503	syslog: Connection blocked by Tcp Wrappers.	5	33
3153	sendmail: Multiple relaying attempts of spam.	6	33
3303	Postfix: Sender domain is not found (450: Requested mail action not taken).	5	33
3330	Postfix process error.	10	33
4325	PIX: ARP collision detected.	8	33
5706	sshd: insecure connection attempt (scan).	6	33
2551	Connection to rshd from unprivileged port. Possible network scan.	10	32
3152	sendmail: Multiple attempts to send e-mail from a previously rejected sender (access).	6	32
3904	Courier (imap/pop3) authentication success.	3	32
3911	Courier: Multiple connection attempts from same source.	10	32
5303	User successfully changed UID to root.	3	32
5402	Successful sudo to ROOT executed.	3	32

Rule ID	Description	Level	Count
5601	telnetd: Connection refused by TCP Wrappers.	5	32
1003	Non standard syslog message (size too large).	13	31
3103	sendmail: Rejected by access list (55x: Requested action not taken).	6	31
3305	Postfix: Recipient address must contain FQDN (504: Command parameter not implemented).	5	31
3306	Postfix: IP Address black-listed by anti-spam (blocked).	6	31
3751	mailscanner: Multiple attempts of spam.	6	31
4810	SonicWall: Firewall administrator login.	3	31
5113	System is shutting down.	7	31
5405	Unauthorized user attempted to use sudo.	5	31
553	File deleted.	7	31
2960	User added to group.	2	30