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

MITRE ATT&CK report

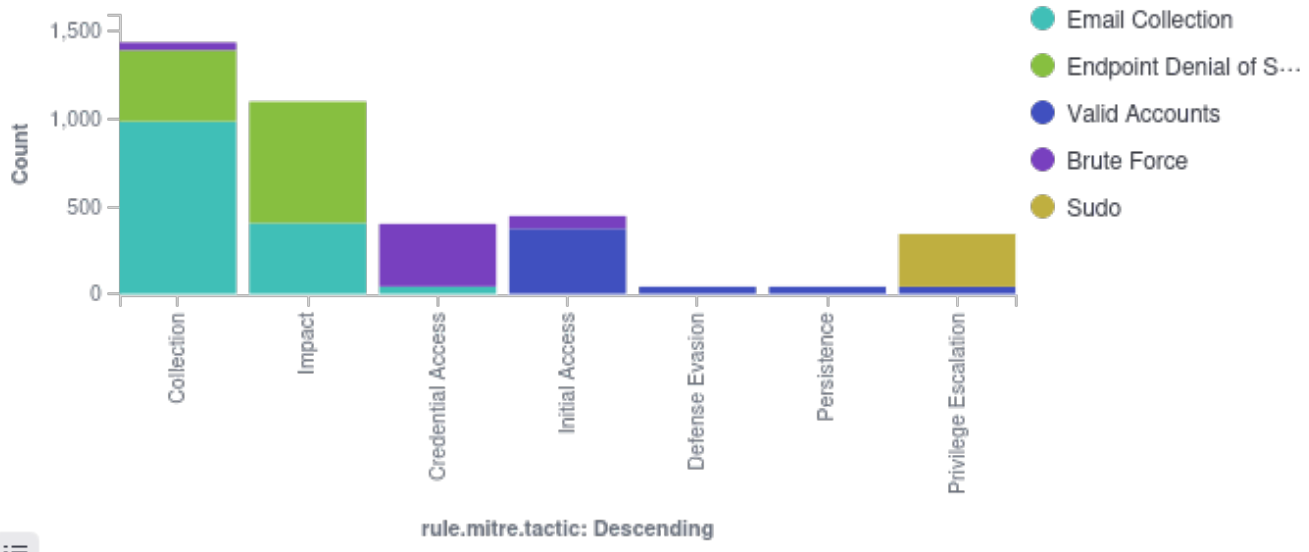
Security events from the knowledge base of adversary tactics and techniques based on real-world observations

2021-09-24T02:58:53 to 2023-09-24T02:58:53

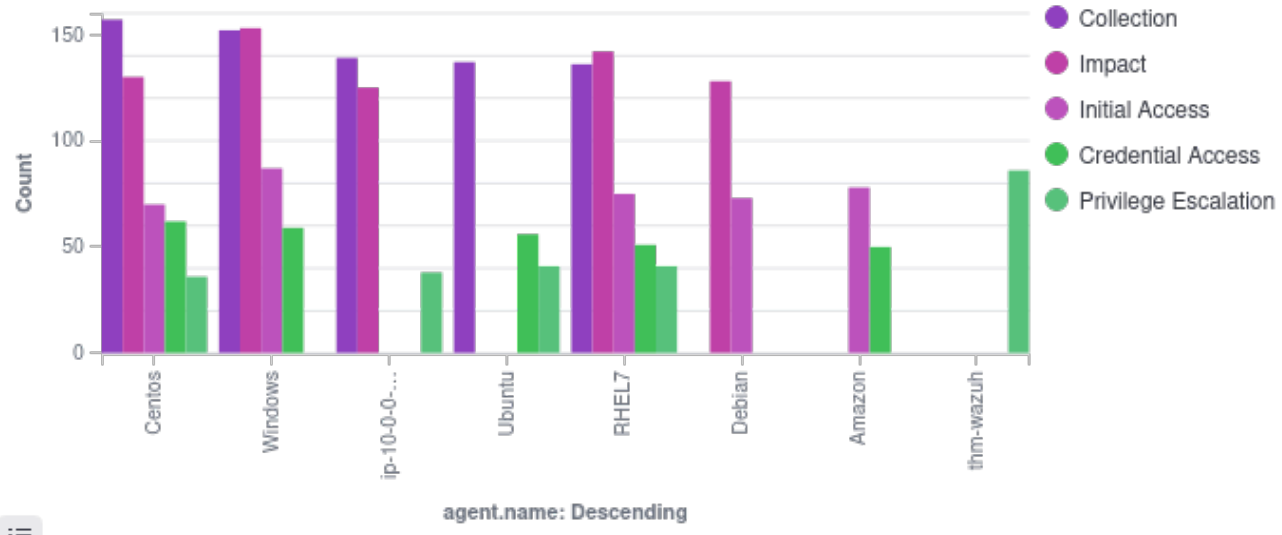
manager.name: thm-wazuh AND rule.mitre.id: *

Mitre techniques by agent

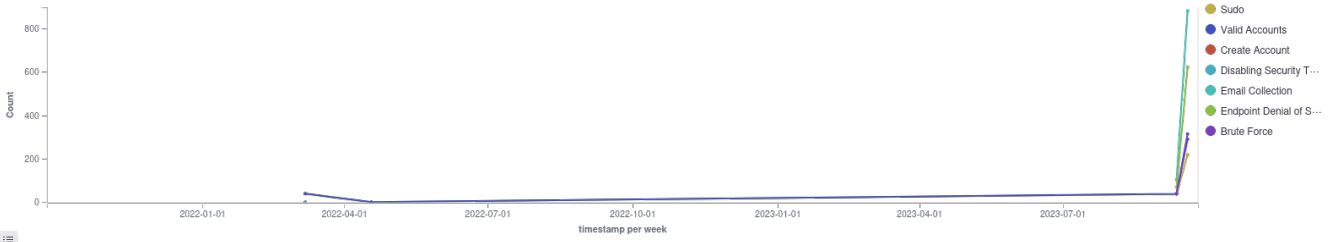
Attacks by technique



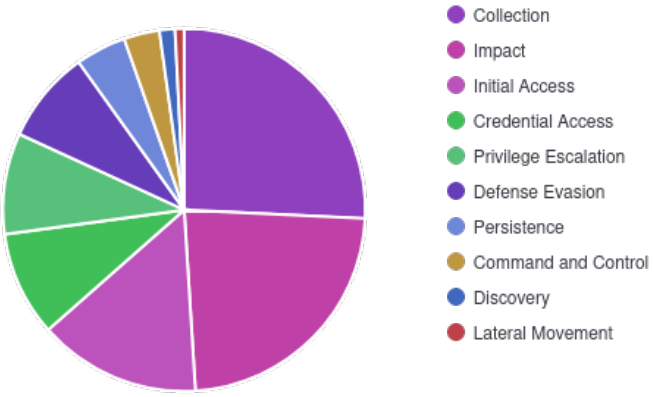
Top tactics by agent



Mitre alerts evolution



Top tactics



Alerts summary

Rule ID	Description	Level	Count
3330	Postfix process error.	10	47
3751	mailscanner: Multiple attempts of spam.	6	44
3602	Imapd user login.	3	43
4507	Netscreen firewall: Successfull admin login	8	43
5501	PAM: Login session opened.	3	43
3156	sendmail: Multiple rejected e-mails from same source ip.	10	40
4386	PIX: Multiple AAA (VPN) authentication failures.	10	40
5132	Unsigned kernel module was loaded	11	40
5402	Successful sudo to ROOT executed.	3	40
2502	syslog: User missed the password more than one time	10	39
3151	sendmail: Sender domain has bogus MX record. It should not be sending e-mail.	10	38
4335	PIX: AAA (VPN) authentication successful.	3	38
553	File deleted.	7	38
3851	ms-exchange: Multiple e-mail attempts to an invalid account.	9	37
3104	sendmail: Attempt to use mail server as relay (550: Requested action not taken).	6	36
3352	Postfix: Multiple attempts to send e-mail from a rejected sender IP (access).	6	35
4506	Netscreen firewall: Successfull admin login	8	35
5302	User missed the password to change UID to root.	9	35
2961	User added to group sudo.	5	34
3158	sendmail: Multiple pre-greetings rejects.	10	34
3306	Postfix: IP Address black-listed by anti-spam (blocked).	6	34
3397	Postfix: RBL lookup error: Host or domain name not found	6	34
3852	ms-exchange: Multiple e-mail 500 error code (spam).	9	34
3910	Courier brute force (multiple failed logins).	10	34
4851	SonicWall: Multiple firewall error messages.	10	34
505	Ossec agent removed.	3	34
2301	xinetd: Excessive number connections to a service.	10	33
3103	sendmail: Rejected by access list (55x: Requested action not taken).	6	33
3105	sendmail: Sender domain is not found (553: Requested action not taken).	5	33
3335	Postfix: too many errors after RCPT from unknown	6	33
4337	PIX: The PIX is disallowing new connections.	8	33
5703	sshd: Possible breakin attempt (high number of reverse lookup errors).	10	33
592	Log file size reduced.	8	33
3191	sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED).	6	32
3303	Postfix: Sender domain is not found (450: Requested mail action not taken).	5	32
3353	Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain.	10	32
4325	PIX: ARP collision detected.	8	32
4339	PIX: Firewall configuration deleted.	8	32
5404	Three failed attempts to run sudo	10	32

Rule ID	Description	Level	Count
5405	Unauthorized user attempted to use sudo.	5	32
5601	telnetd: Connection refused by TCP Wrappers.	5	32
5705	sshd: Possible scan or breakin attempt (high number of login timeouts).	10	32
5706	sshd: insecure connection attempt (scan).	6	32
3304	Postfix: Improper use of SMTP command pipelining (503: Bad sequence of commands).	5	31
3351	Postfix: Multiple relaying attempts of spam.	6	31
4323	PIX: Successful login.	3	31
4509	Netscreen firewall: configuration changed.	8	31
518	Windows Adware/Spyware application found.	9	31
5631	telnetd: Multiple connection attempts from same source (possible scan).	10	31
593	Microsoft Event log cleared.	9	31