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

MITRE ATT&CK report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	kali	192.168.84.135	Wazuh v4.12.0	siem-VMware-Virtual-Platform	Kali GNU/Linux 2025.3	Sep 9, 2025 @ 15:07:31.000	Oct 6, 2025 @ 07:36:24.000

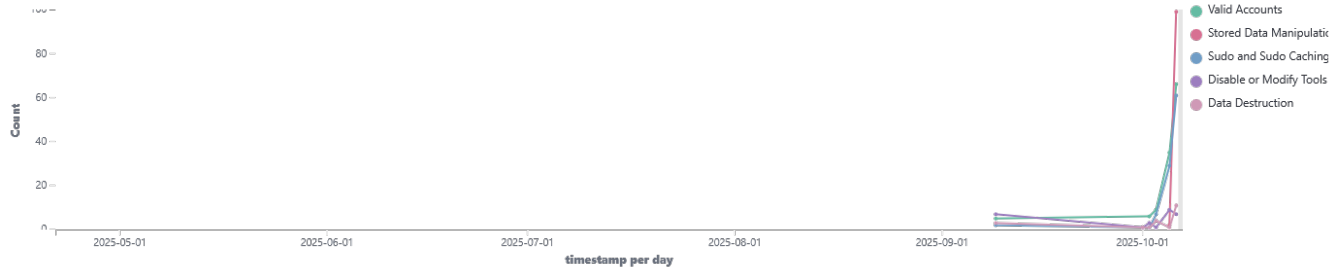
Group: default

Explore security alerts mapped to adversary tactics and techniques for better threat understanding.

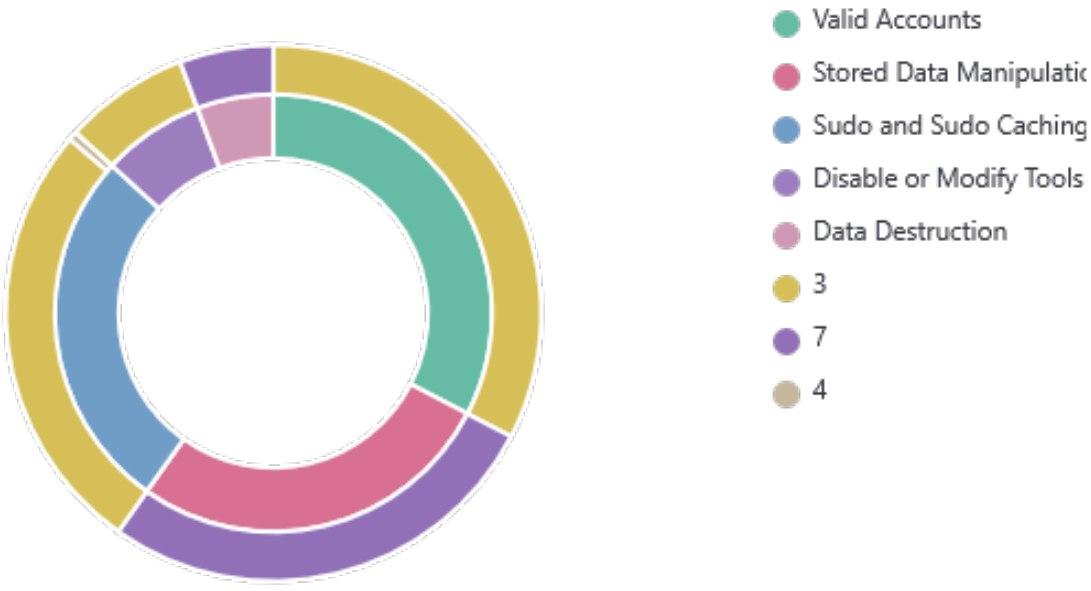
2025-04-21T07:36:28 to 2025-10-06T07:36:28

manager.name: siem-VMware-Virtual-Platform AND rule.mitre.id: * AND agent.id: 001

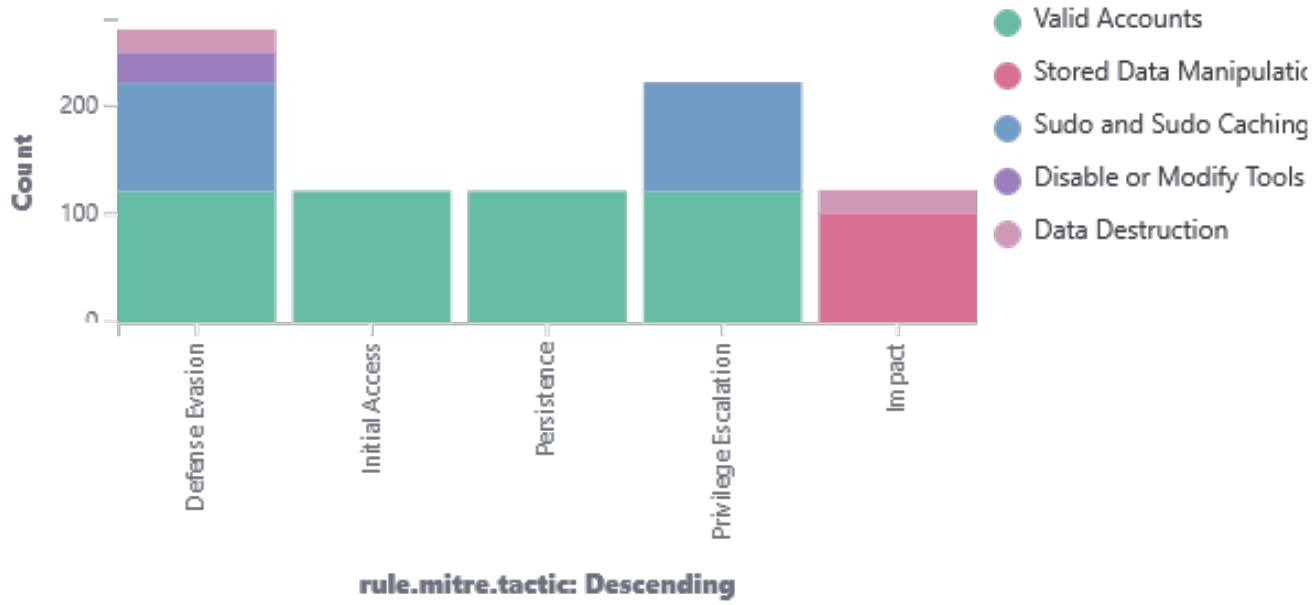
Alerts evolution over time



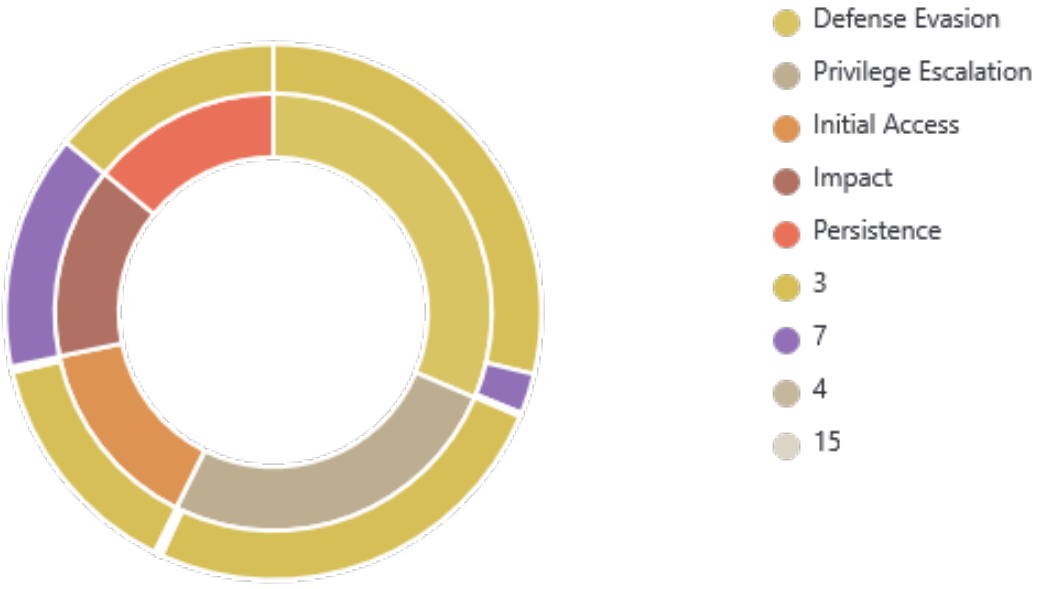
Rule level by attack



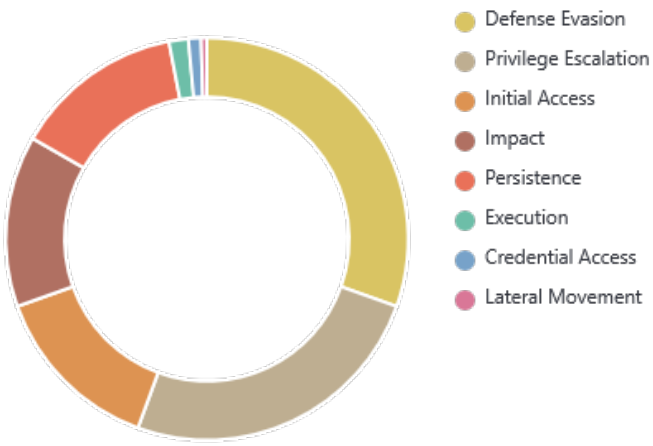
MITRE attacks by tactic



Rule level by tactic



Top tactics



Alerts summary

Rule ID	Description	Level	Count
5501	PAM: Login session opened.	3	121
550	Integrity checksum changed.	7	101
5402	Successful sudo to ROOT executed.	3	98
506	Wazuh agent stopped.	3	28
553	File deleted.	7	21
87105	VirusTotal: Alert - /home/kali/malware/ecir - 66 engines detected this file	12	6
5710	sshd: Attempt to login using a non-existent user	5	4
87105	VirusTotal: Alert - /home/kali/malware/ecir - 64 engines detected this file	12	3
87105	VirusTotal: Alert - /home/kali/malware/eicar - 65 engines detected this file	12	3
5503	PAM: User login failed.	5	3
87105	VirusTotal: Alert - /home/kali/malware/ecir - 65 engines detected this file	12	2
31168	Shellshock attack detected	15	2
5403	First time user executed sudo.	4	2
5557	unix_chkpwd: Password check failed.	5	2
31103	SQL injection attempt.	7	1