# MITRE ATT&CK report

Warning. Agent is disconnected

| 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 3, 2025 @ 17:50:49.000 |

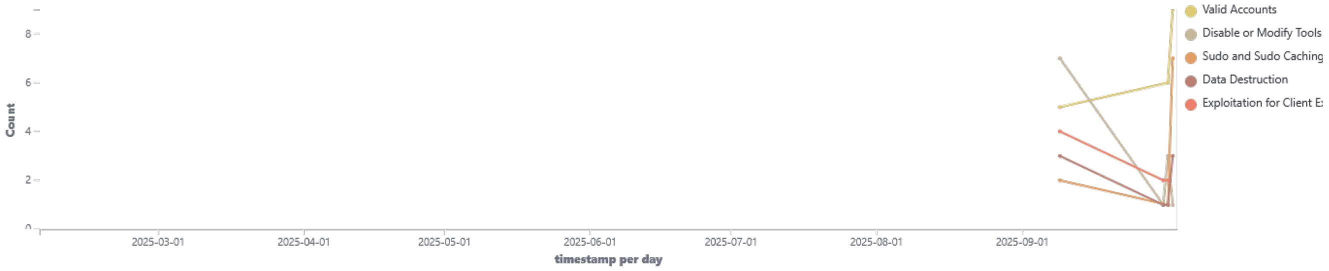
Group: default

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

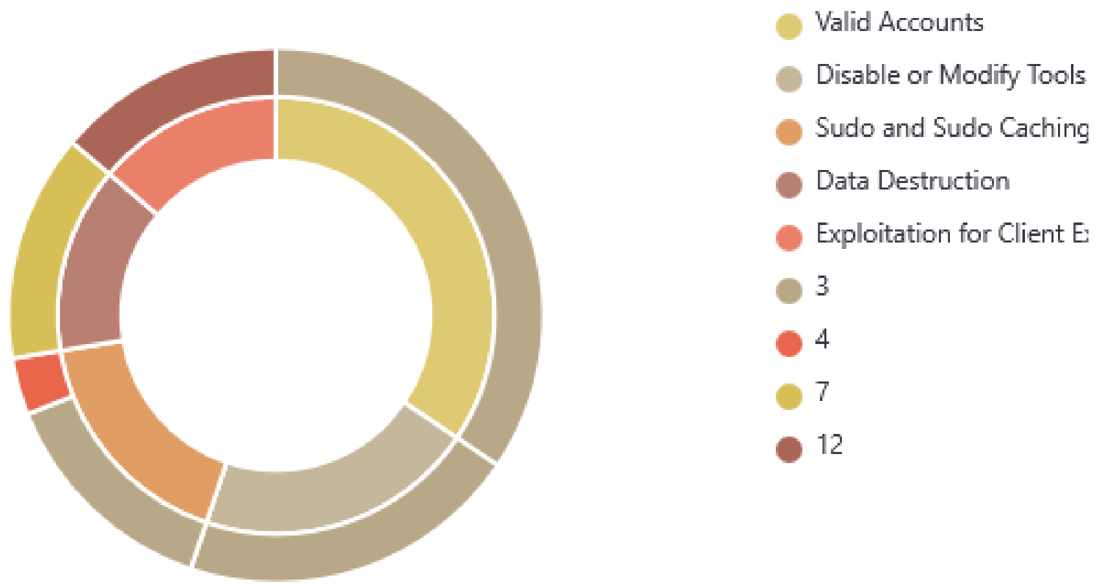
2025-02-03T17:56:32 to 2025-10-03T17:47:03

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

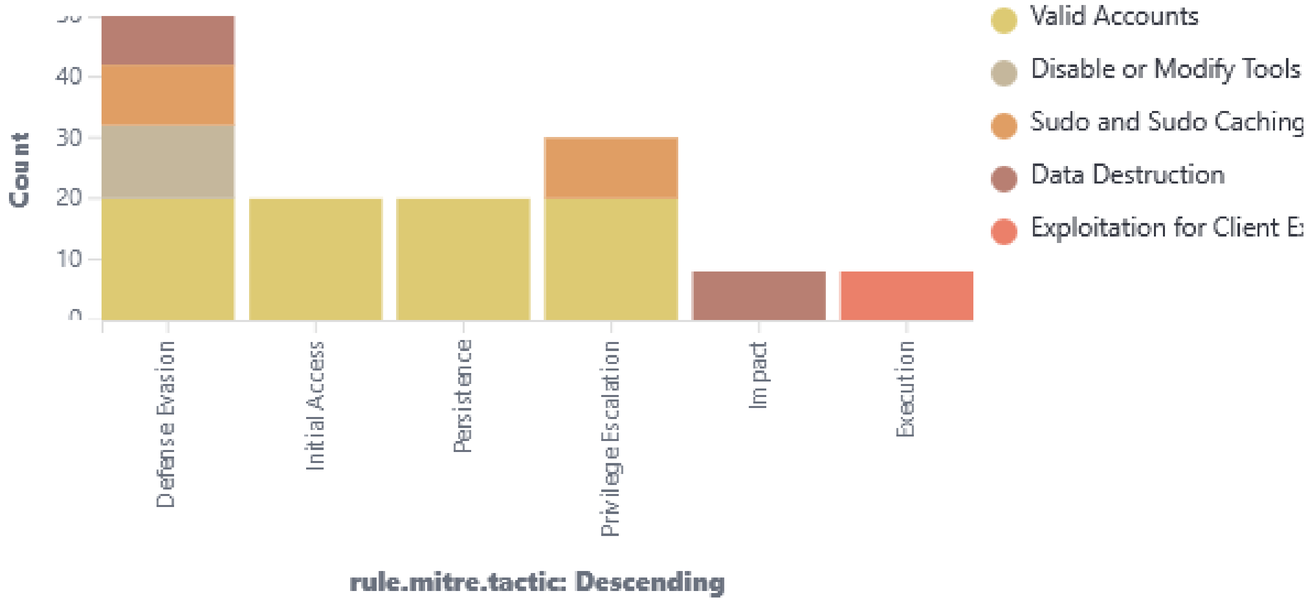
## Alerts evolution over time



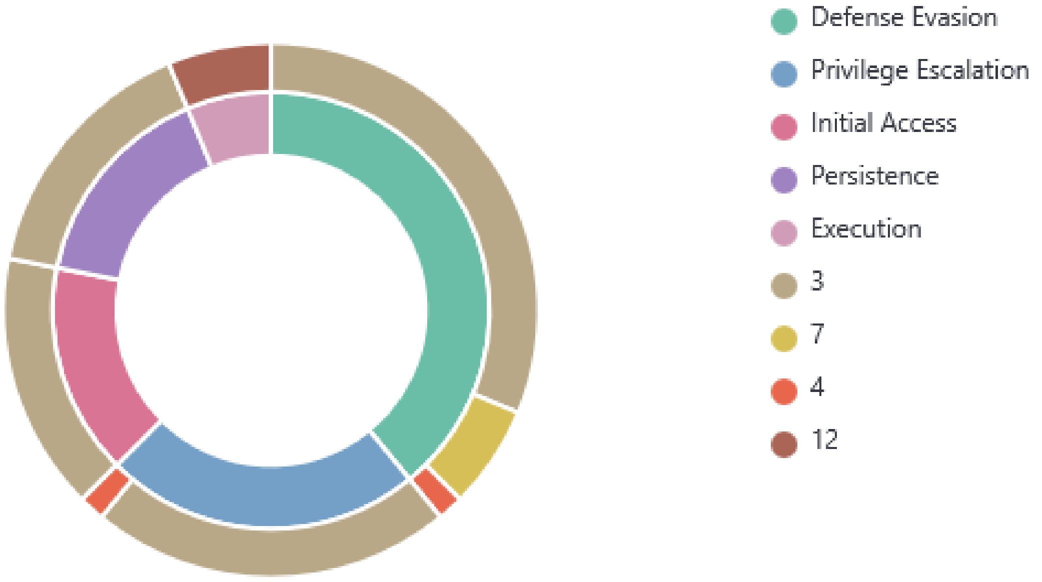
## Rule level by attack



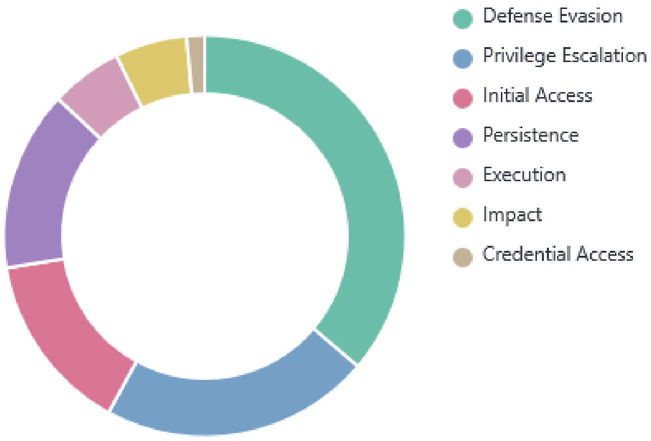
## MITRE attacks by tactic



## Rule level by tactic



## Top tactics



## Alerts summary

| Rule ID | Description | Level | Count |
|---|---|---|---|
| 5501 | PAM: Login session opened. | 3 | 20 |
| 506 | Wazuh agent stopped. | 3 | 12 |
| 5402 | Successful sudo to ROOT executed. | 3 | 8 |
| 553 | File deleted. | 7 | 8 |
| 87105 | VirusTotal: Alert - /home/kali/malware/ecir - 66 engines detected this file | 12 | 6 |
| 87105 | VirusTotal: Alert - /home/kali/malware/ecir - 65 engines detected this file | 12 | 2 |
| 5403 | First time user executed sudo. | 4 | 2 |
| 5503 | PAM: User login failed. | 5 | 1 |
| 5557 | unix_chkpwd: Password check failed. | 5 | 1 |