

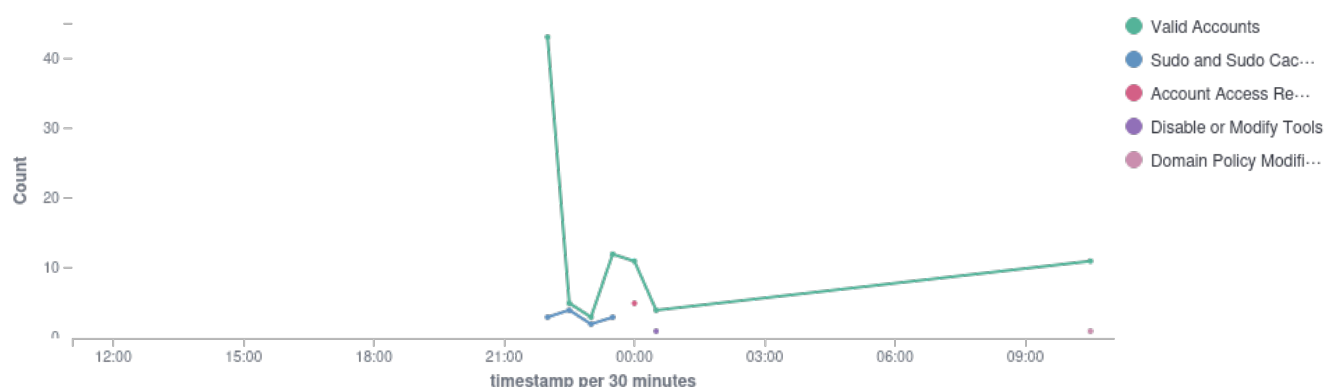
MITRE ATT&CK report

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

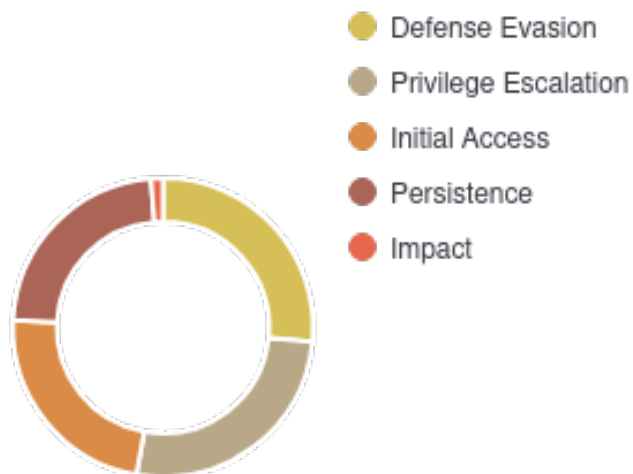
🕒 2024-10-19T11:03:08 to 2024-10-20T11:03:08

🔍 manager.name: reem-VMware AND rule.mitre.id: *

Alerts evolution over time



Top tactics

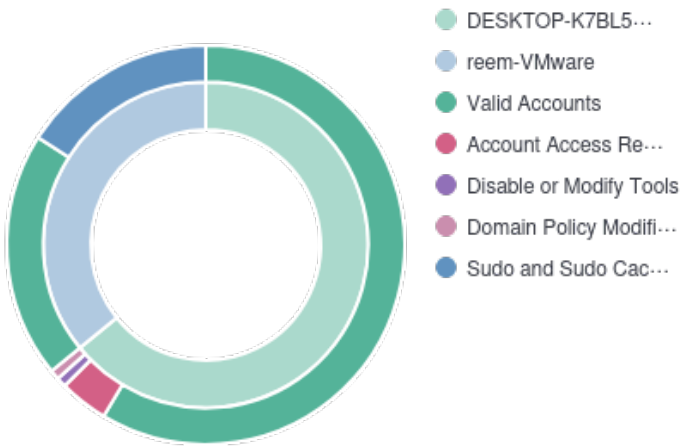


Attacks by technique



Top tactics by agent

Mitre techniques by agent



Alerts summary

Rule ID	Description	Level	Count
60106	Windows Logon Success	3	72
5501	PAM: Login session opened.	3	15
5402	Successful sudo to ROOT executed.	3	12
60122	Logon Failure - Unknown user or bad password	5	5
60118	Windows Workstation Logon Success	3	2
504	Wazuh agent disconnected.	3	1
67028	Special privileges assigned to new logon.	3	1