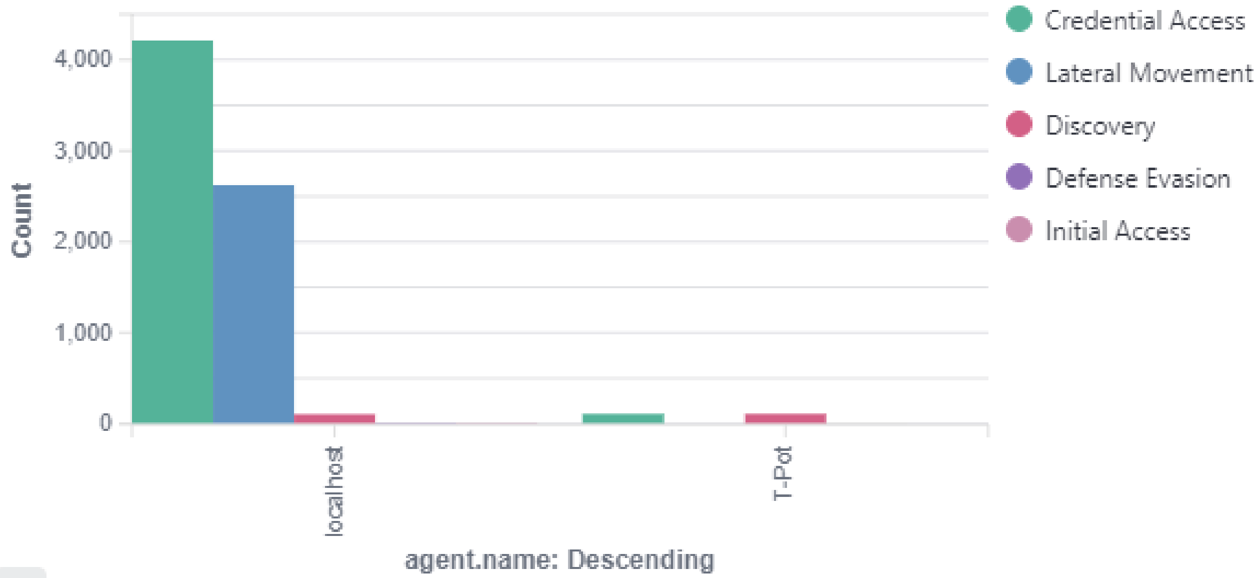
MITRE ATT&CK report

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

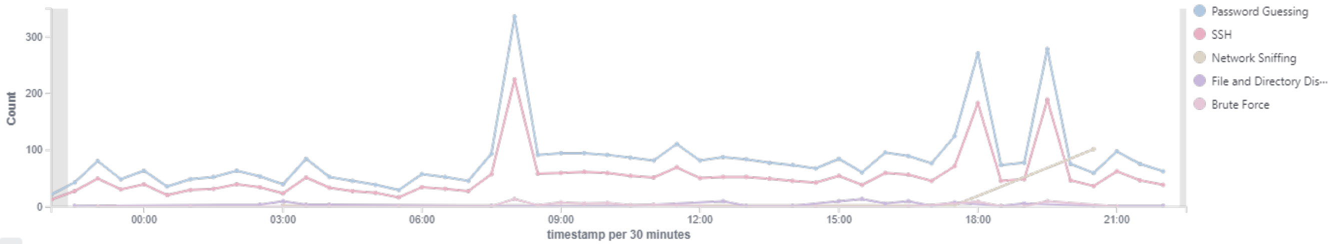
2024-07-20T22:21:35 to 2024-07-21T22:21:35

manager.name: localhost AND rule.mitre.id: *

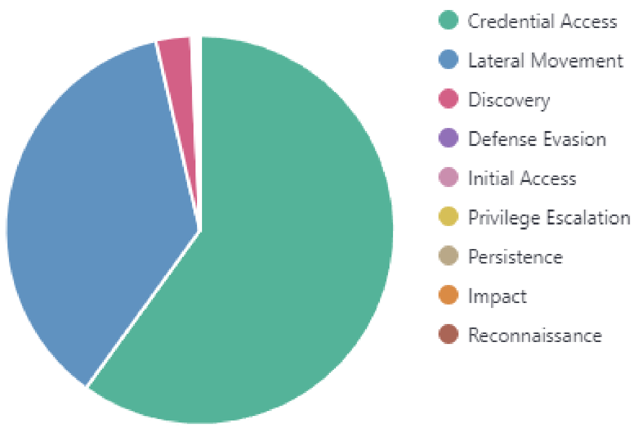
Top tactics by agent



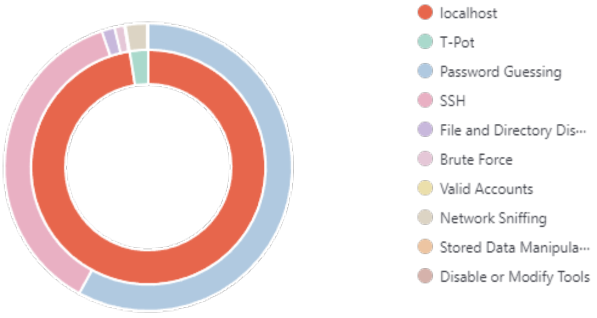
Mitre alerts evolution



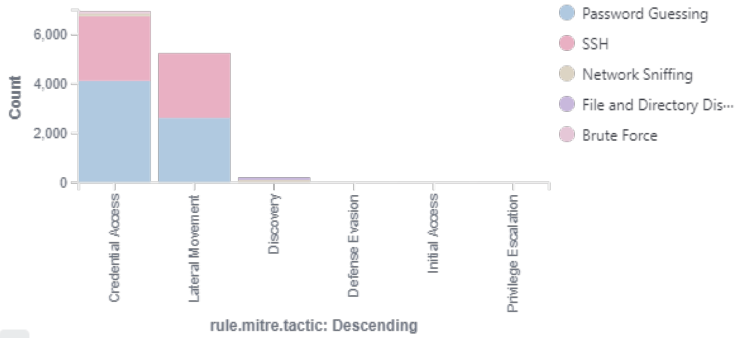
Top tactics



Mitre techniques by agent



Attacks by technique



Alerts summary

Rule ID	Description	Level	Count
5710	sshd: Attempt to login using a non-existent user	5	1974
5503	PAM: User login failed.	5	1511
5760	sshd: authentication failed.	5	647
5104	Interface entered in promiscuous(sniffing) mode.	8	108
31515	PHPMyAdmin scans (looking for setup.php).	6	102
2502	syslog: User missed the password more than one time	10	49
5551	PAM: Multiple failed logins in a small period of time.	10	27
11402	vsftpd: FTP Authentication success.	3	9
550	Integrity checksum changed.	7	3
5712	sshd: brute force trying to get access to the system. Non existent user.	10	3
592	Log file size reduced.	8	3
31104	Common web attack.	6	2
31151	Multiple web server 400 error codes from same source ip.	10	2
506	Wazuh agent stopped.	3	1

Copyright © 2024 Wazuh, Inc.