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

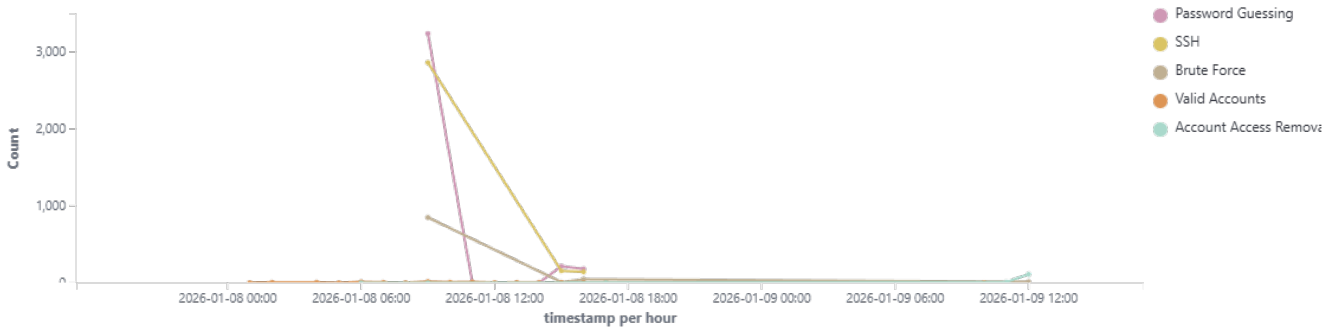
MITRE ATT&CK report

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

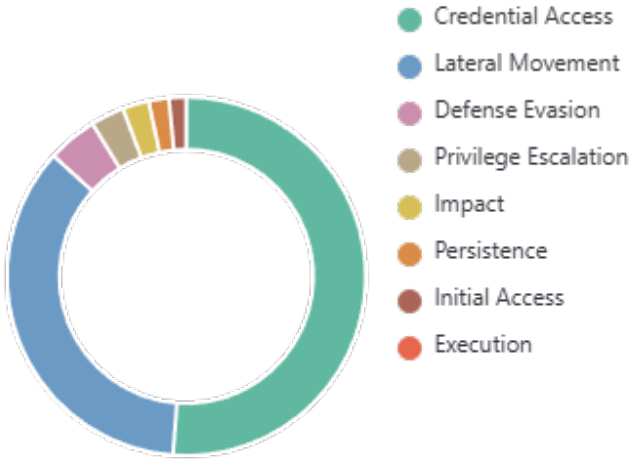
2026-01-07T17:12:01 to 2026-01-09T17:12:01

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

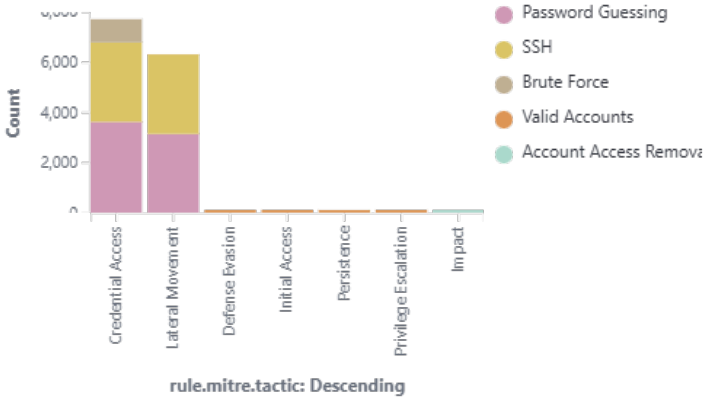
Alerts evolution over time



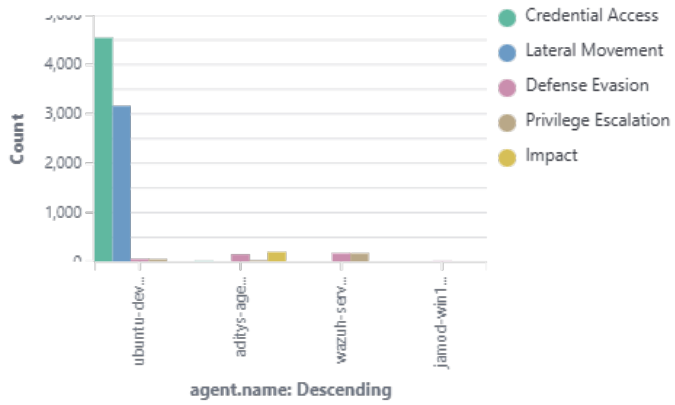
Top tactics



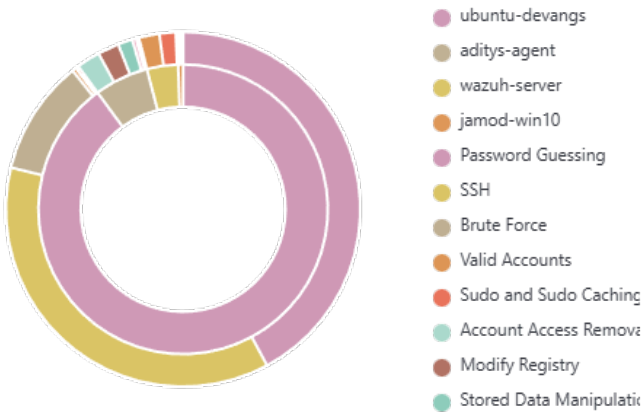
Attacks by technique



Top tactics by agent



Mitre techniques by agent



Alerts summary

Rule ID	Description	Level	Count
5710	sshd: Attempt to login using a non-existent user	5	1936
5760	sshd: authentication failed.	5	1224
5503	PAM: User login failed.	5	477
2502	syslog: User missed the password more than one time	10	410
5758	Maximum authentication attempts exceeded.	8	374
60122	Logon Failure - Unknown user or bad password	5	131
5501	PAM: Login session opened.	3	125
5402	Successful sudo to ROOT executed.	3	91
5551	PAM: Multiple failed logins in a small period of time.	10	64
40111	Multiple authentication failures.	10	48
594	Registry Key Integrity Checksum Changed	5	38
750	Registry Value Integrity Checksum Changed	5	37
598	Registry Key Entry Added to the System	5	24
67028	Special privileges assigned to new logon.	3	22
504	Wazuh agent disconnected.	3	15
60110	User account changed	8	15
60204	Multiple Windows Logon Failures	10	15
752	Registry Value Entry Added to the System	5	12
506	Wazuh agent stopped.	3	9
5763	sshd: brute force trying to get access to the system. Authentication failed.	10	9
5403	First time user executed sudo.	4	8
60118	Windows Workstation Logon Success	3	6
61138	New Windows Service Created	5	4
5715	sshd: authentication success.	3	3
5902	New user added to the system.	8	3
67018	System shutdown initiated.	3	3
5404	Three failed attempts to run sudo	10	2
5557	unix_chkpwd: Password check failed.	5	2
60111	User account disabled or deleted	8	2
60160	Domain Users Group Changed	5	2
60170	Users Group Changed	5	2
92652	Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack.	6	2
92657	Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that WINDOWS is allowed to perform RDP connections	6	2
5712	sshd: brute force trying to get access to the system. Non existent user.	10	1
60730	Inconsistent system shutdown detected.	5	1

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