

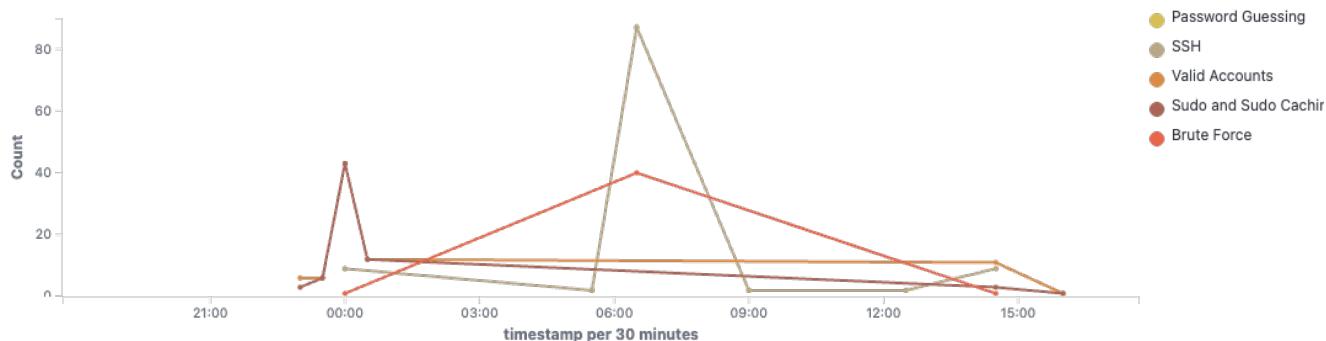
MITRE ATT&CK report

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

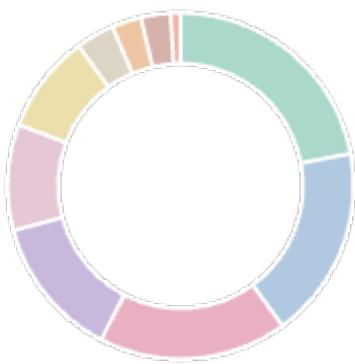
⌚ 2025-11-27T17:42:42 to 2025-11-28T17:42:42

🔍 manager.name: ip-172-31-16-30 AND rule.mitre.id: *

Alerts evolution over time



Top tactics

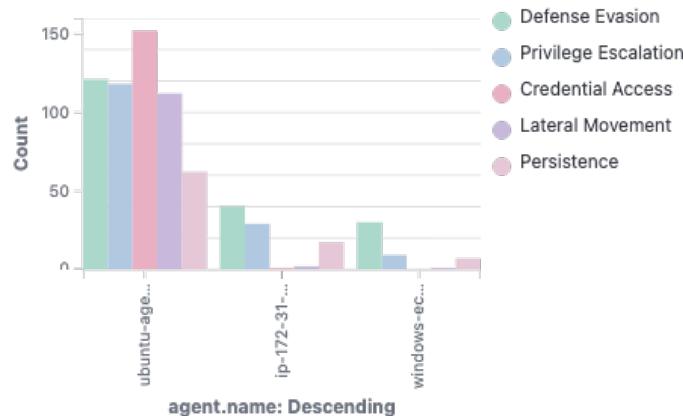


- Defense Evasion
- Privilege Escalation
- Credential Access
- Lateral Movement
- Persistence
- Initial Access
- Command and Control
- Execution
- Impact
- Discovery

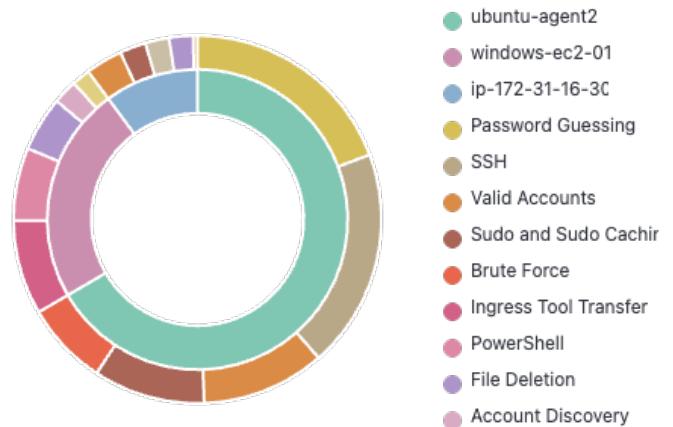
Attacks by technique



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	111
5501	PAM: Login session opened.	3	76
5402	Successful sudo to ROOT executed.	3	65
5758	Maximum authentication attempts exceeded.	8	36
92205	Powershell process created an executable file in Windows root folder	9	24
92066	C:\\Windows\\SysWOW64\\SecEdit.exe binary in a suspicious location launched by C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe	4	20
92021	Powershell was used to delete files or directories	3	18
550	Integrity checksum changed.	7	12
553	File deleted.	7	11
92031	Discovery activity executed	3	8
92213	Executable file dropped in folder commonly used by malware	15	7
506	Wazuh agent stopped.	3	6
5712	sshd: brute force trying to get access to the system. Non existent user.	10	5
5403	First time user executed sudo.	4	3
5715	sshd: authentication success.	3	3
92027	Powershell process spawned powershell instance	4	3
60109	User account enabled or created	8	2
60160	Domain Users Group Changed	5	2
60170	Users Group Changed	5	2
61138	New Windows Service Created	5	2
67028	Special privileges assigned to new logon.	3	2
40111	Multiple authentication failures.	10	1
60110	User account changed	8	1
60111	User account disabled or deleted	8	1
92018	CertUtil.exe used to decode binary file	13	1
92029	Powershell executed script from suspicious location	6	1
92073	Powershell executing certutil to decode a file	6	1
92652	Successful Remote Logon Detected - User:\\Administrator - NTLM authentication, possible pass-the-hash attack.	6	1