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

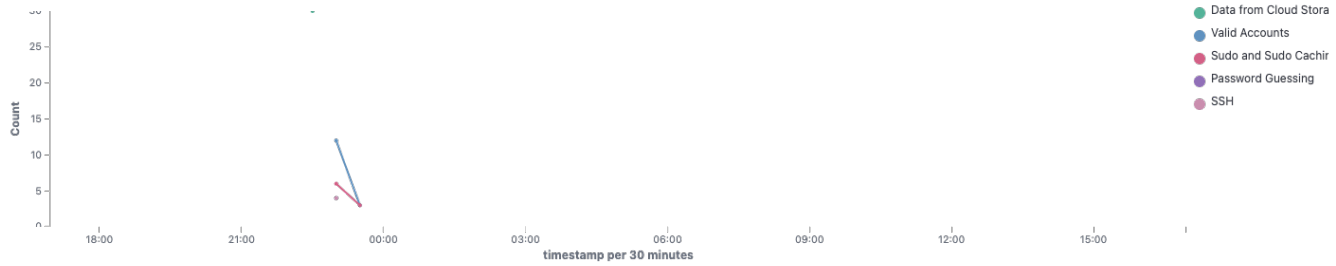
MITRE ATT&CK report

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

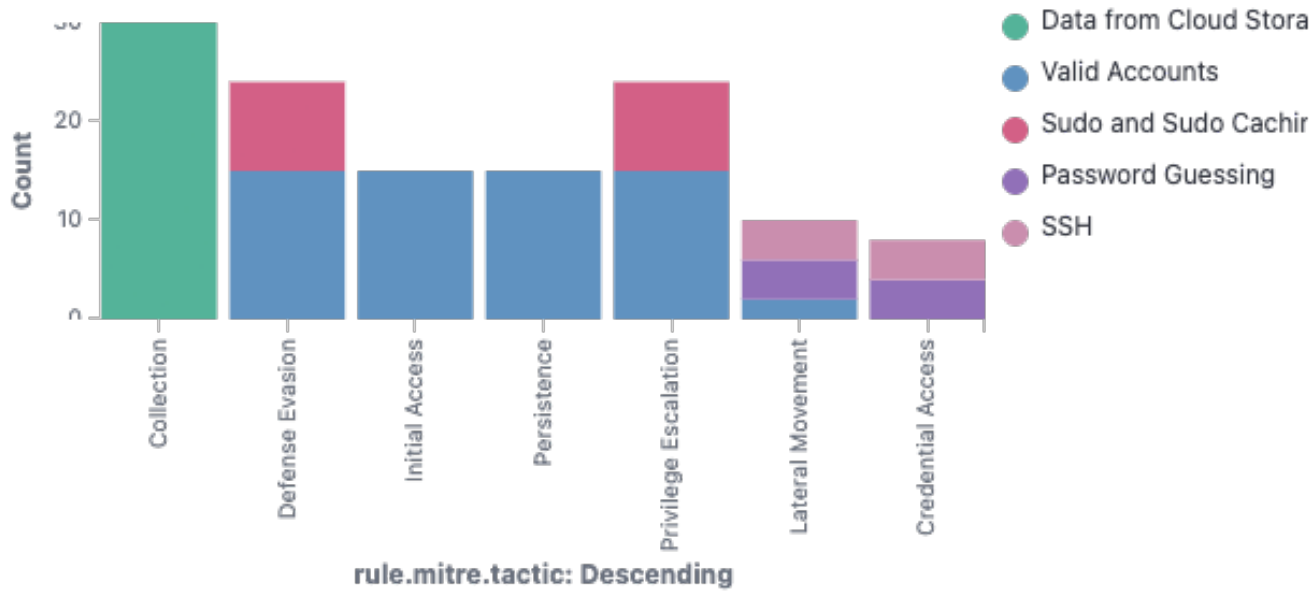
2025-10-07T16:57:37 to 2025-10-08T16:57:37

manager.name: ip-172-31-90-138.ec2.internal AND rule.mitre.id: *

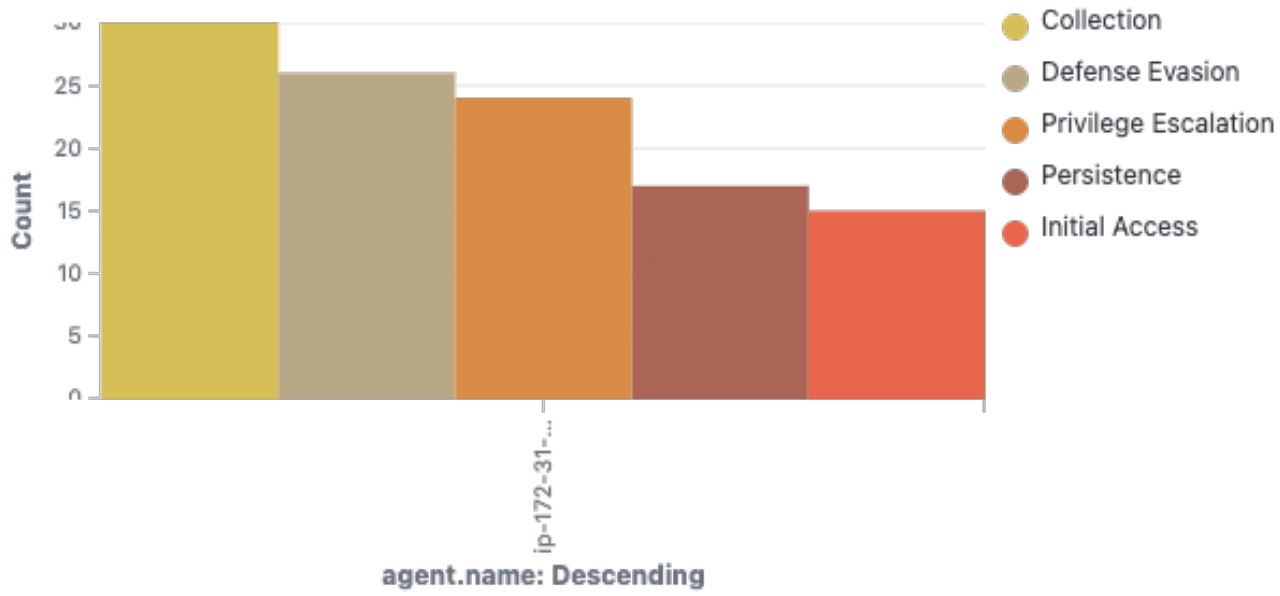
Alerts evolution over time



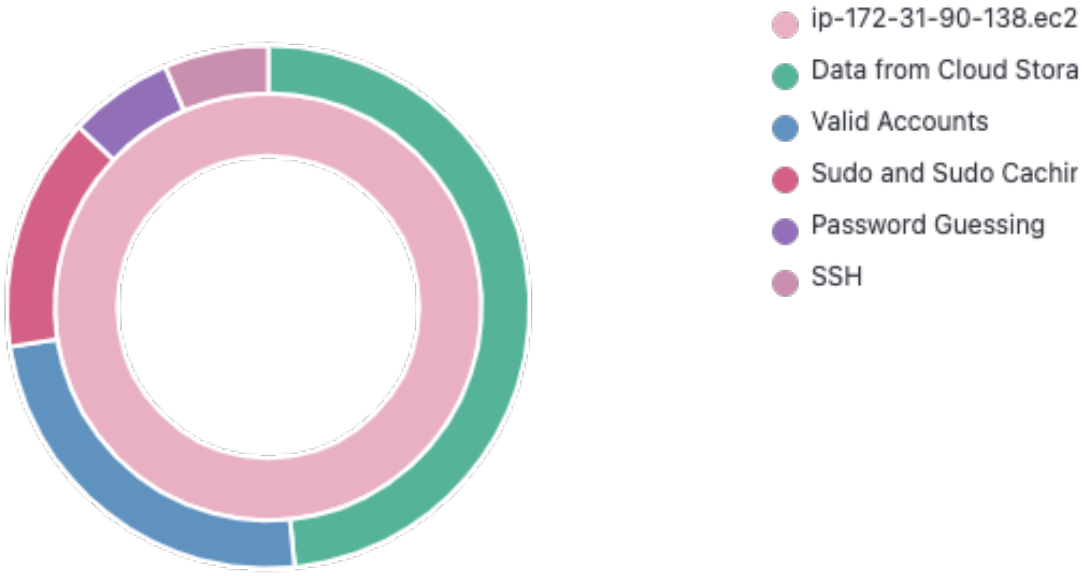
Attacks by technique



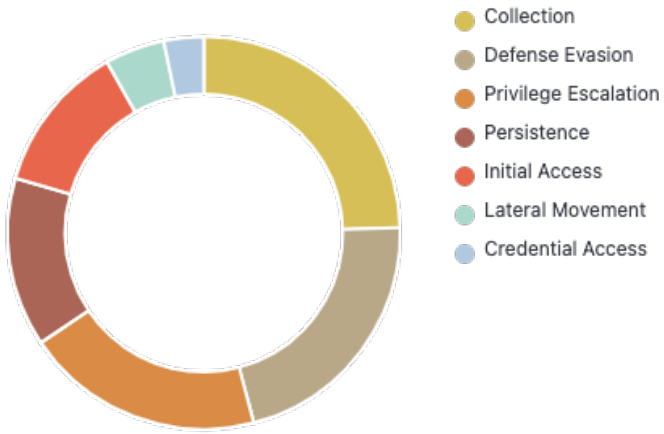
Top tactics by agent



Mitre techniques by agent



Top tactics



Alerts summary

Rule ID	Description	Level	Count
100100	Credentials access : Attempt to retrieve EC2 credentials	5	28
5501	PAM: Login session opened.	3	13
5402	Successful sudo to ROOT executed.	3	9
5710	sshd: Attempt to login using a non-existent user	5	4
100101	Credentials access : Multiple attempts to retrieve EC2 credentials	12	2
100103	Possible IAM Role backdooring: IAM role granted from an external account	12	2
100104	Possible disruption of CloudTrail Logging: Management events logging disabled with an event selector	12	2
5715	sshd: authentication success.	3	2