Lateral movement
refers to the techniques that a cyberattacker uses, after gaining initial access, to move deeper into a network in search of sensitive data and other high-value assets. After accessing the network, the attacker maintains ongoing access by moving through the compromised environment and obtaining increased privileges using various tools.

The detection algorithm for lateral movement is based on two signals :
(1) the relative Shannon entropy of the accesses to a destination machine by a user.
It is well understood that brute-force attacks or credential swiping hacks involves a repeated attempt by an attacker to gain access to many assets. In order to
Avoid being blocked off, an attacker has to keep the number of attempts limited to a certain low number usually by way of an automated process. The Shannon entropy
Is used to infer this behavior.
(2) the number of attempted destination machine accesses will likely be higher than usual for a certain user. We measure the abnormality of attempts by a user by calculating the probability of seeing such a high number of attempts compared to peers or historical behavior which should be abnormally high\

Data sources:
Any authentication logs such as:
Active Directory
Okta
Any other identity management logs