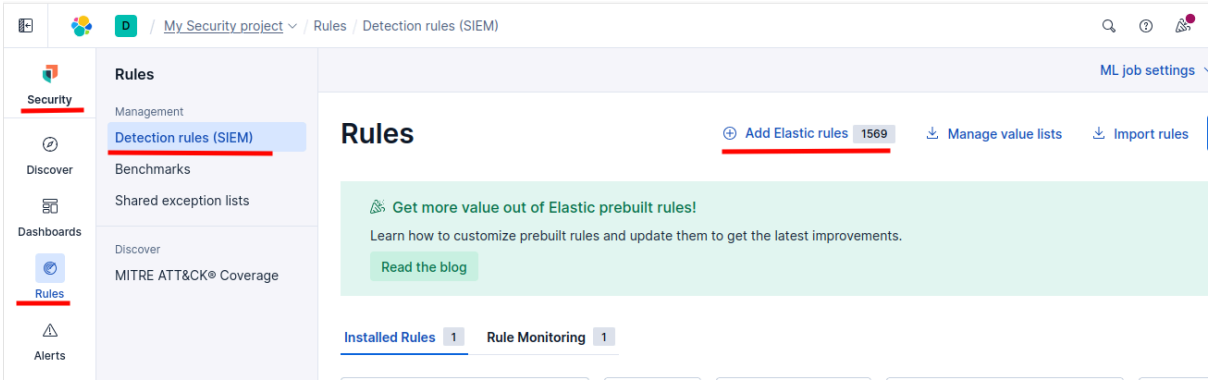
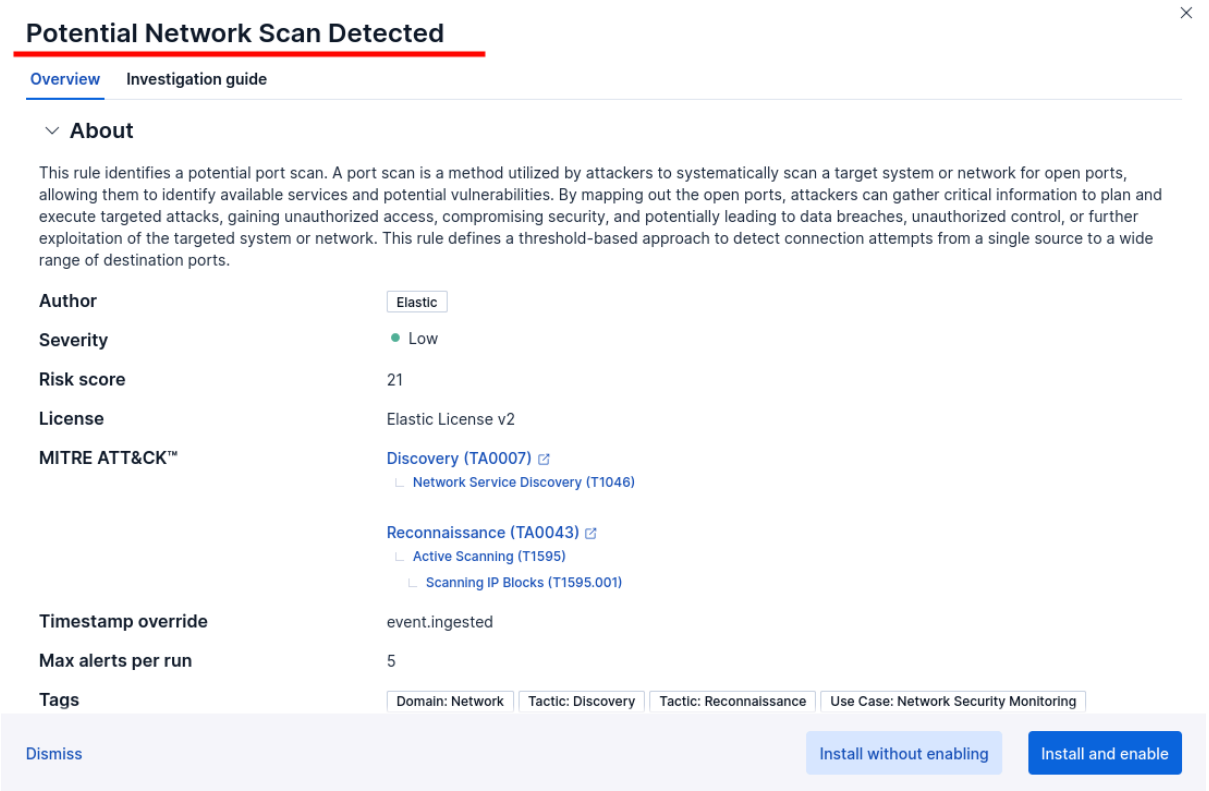
Brandon Gracy *16/12/2025*

In this lab we have to continues to enhance its Security Information and Event Management (SIEM) capabilities, your team has been tasked with enabling, testing, and analyzing security alerts within Elastic SIEM using the MITRE ATT&CK framework.

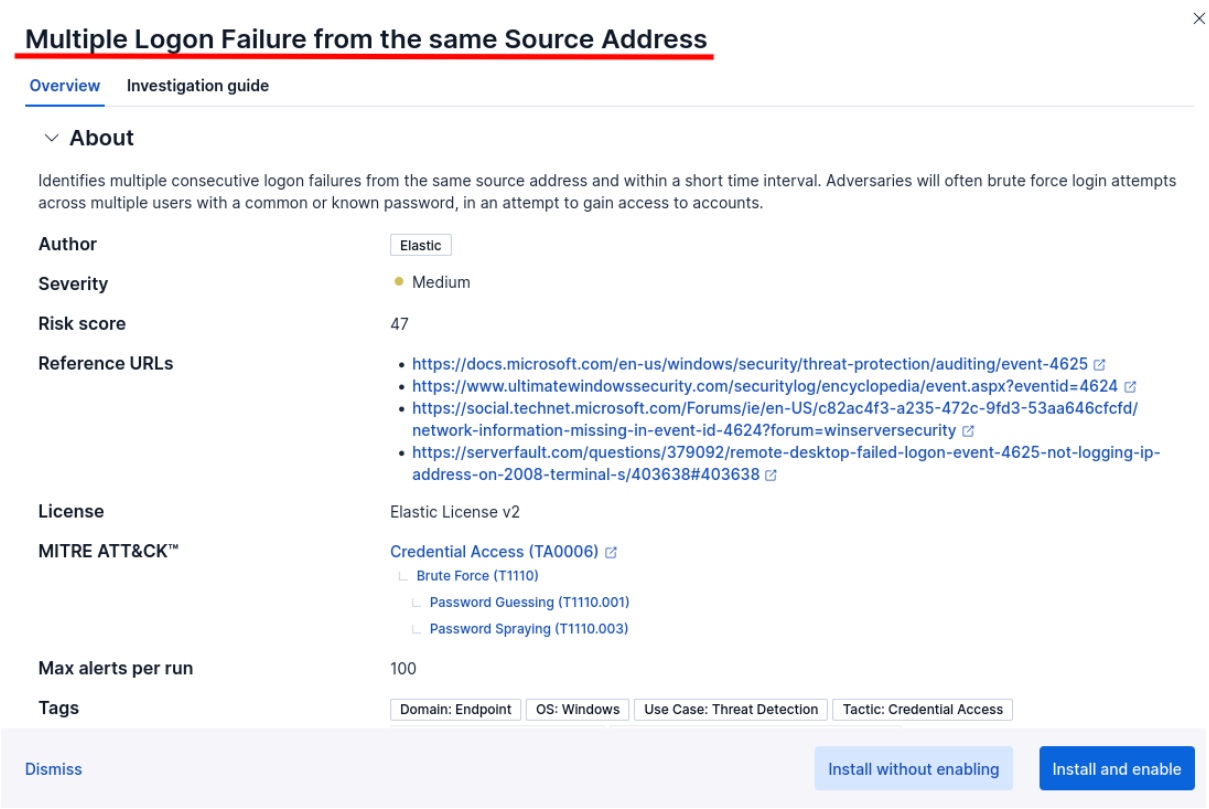
In this part we have to enable security rules in elastic SIEM.



Here, we are seeing the elastic cloud, so, we have to go into security, rules, detection rules(SIEM) and add elastic rules, because we need to add two new rules.

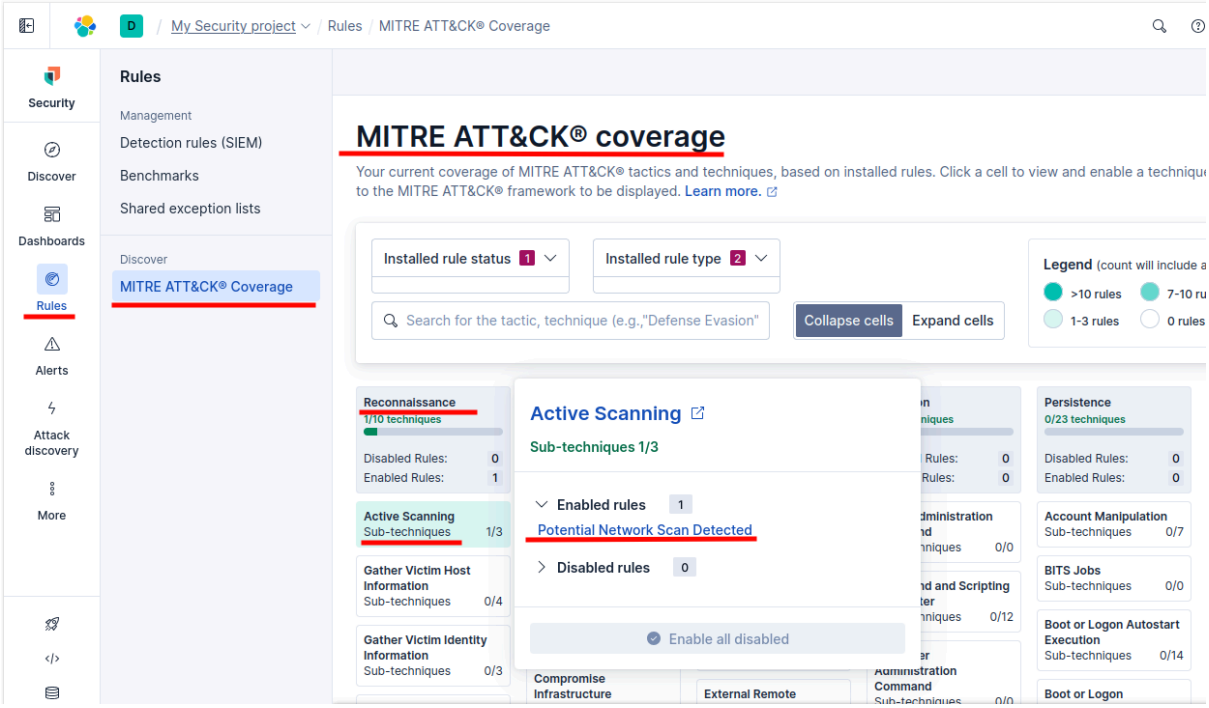


That's the first rule that we need to install.

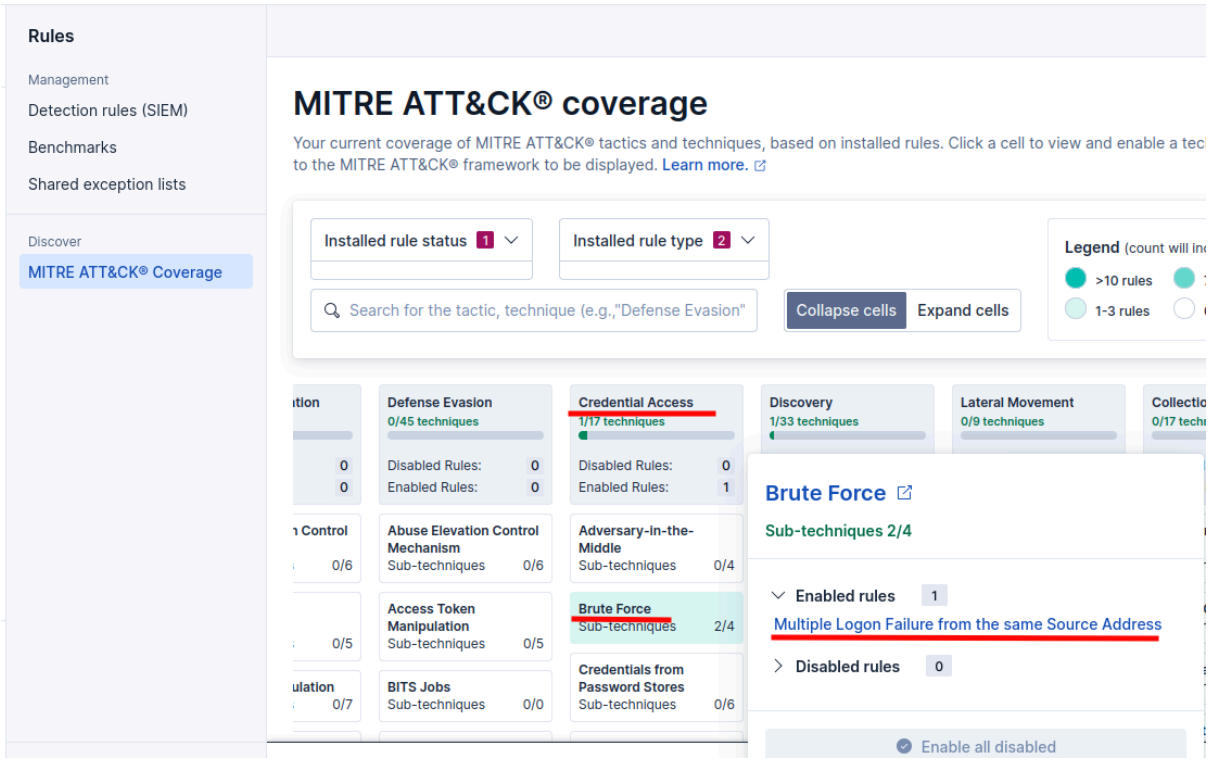


And this rule.

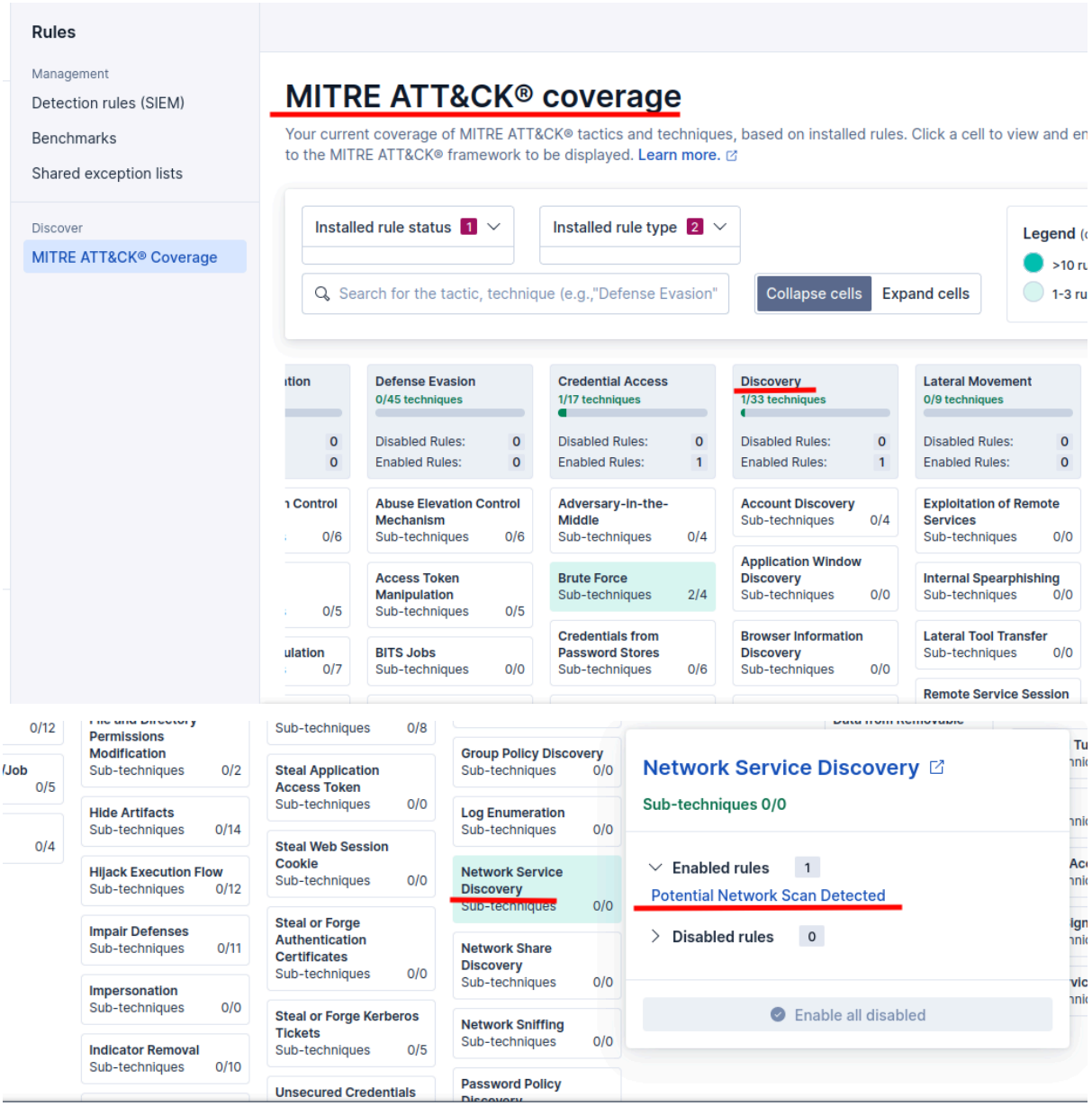
Now, let's open the MITRE ATT&CK techniques to confirm if the rules are enabled.



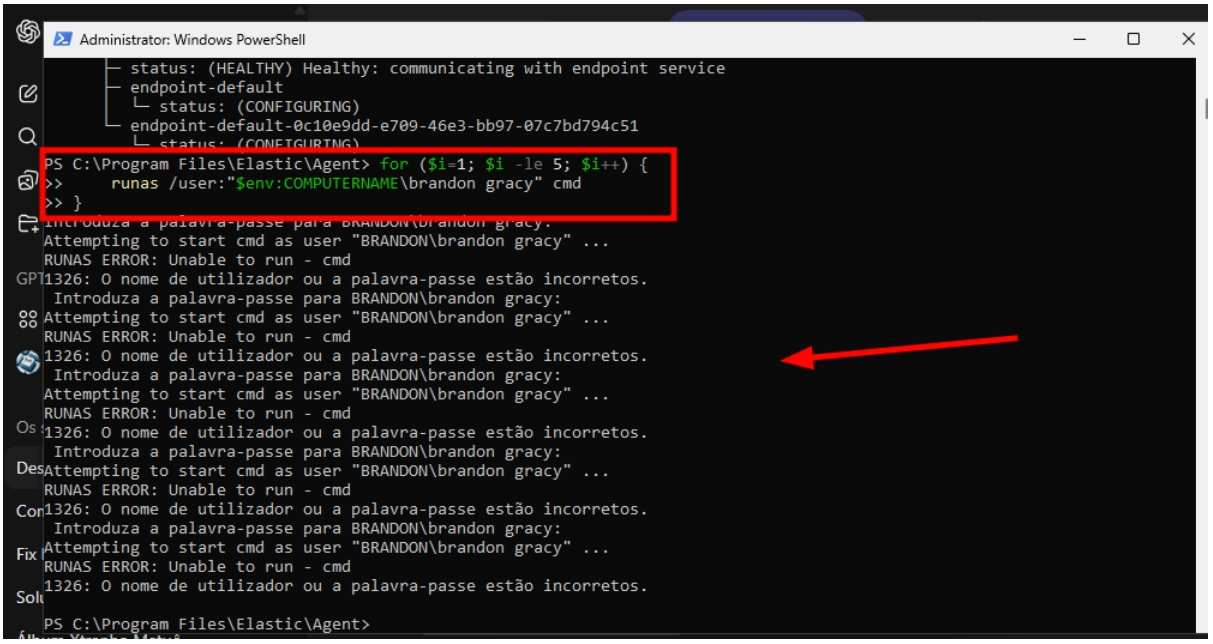
Here we can check that our rule Potential Network Scan Detected is in reconnaissance tatic, and is inside of Active Scanning techniques, let’s check the clothes to see more.



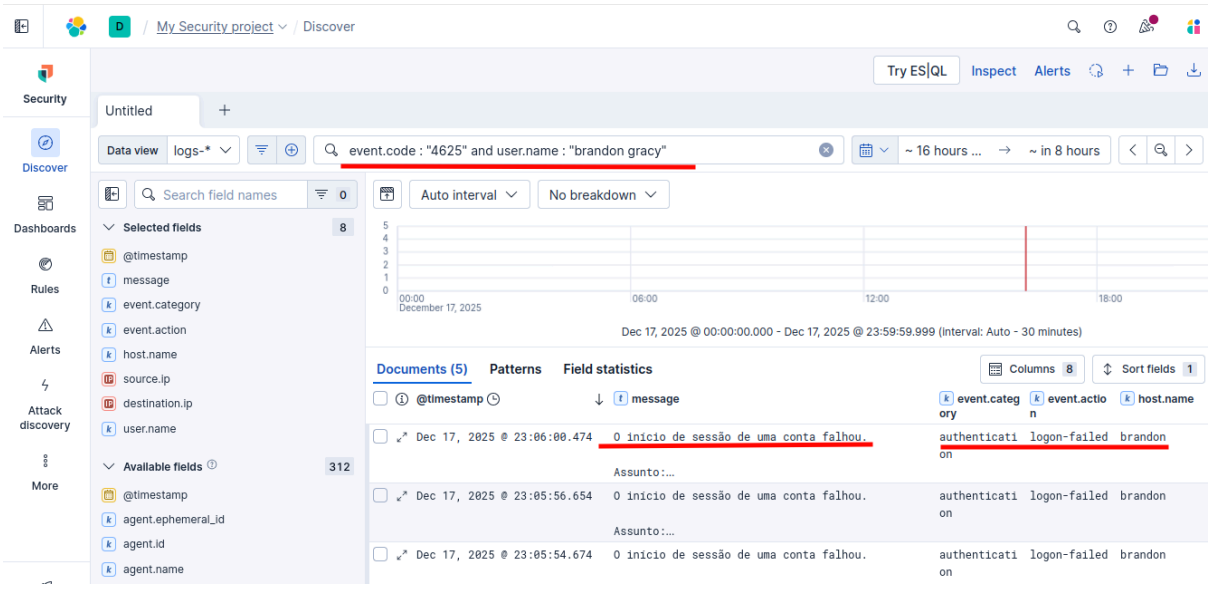
Here we can check that our Multiple Logon Failure from the same Source Address is in Credentials access tactic, and inside of brute force techniques.



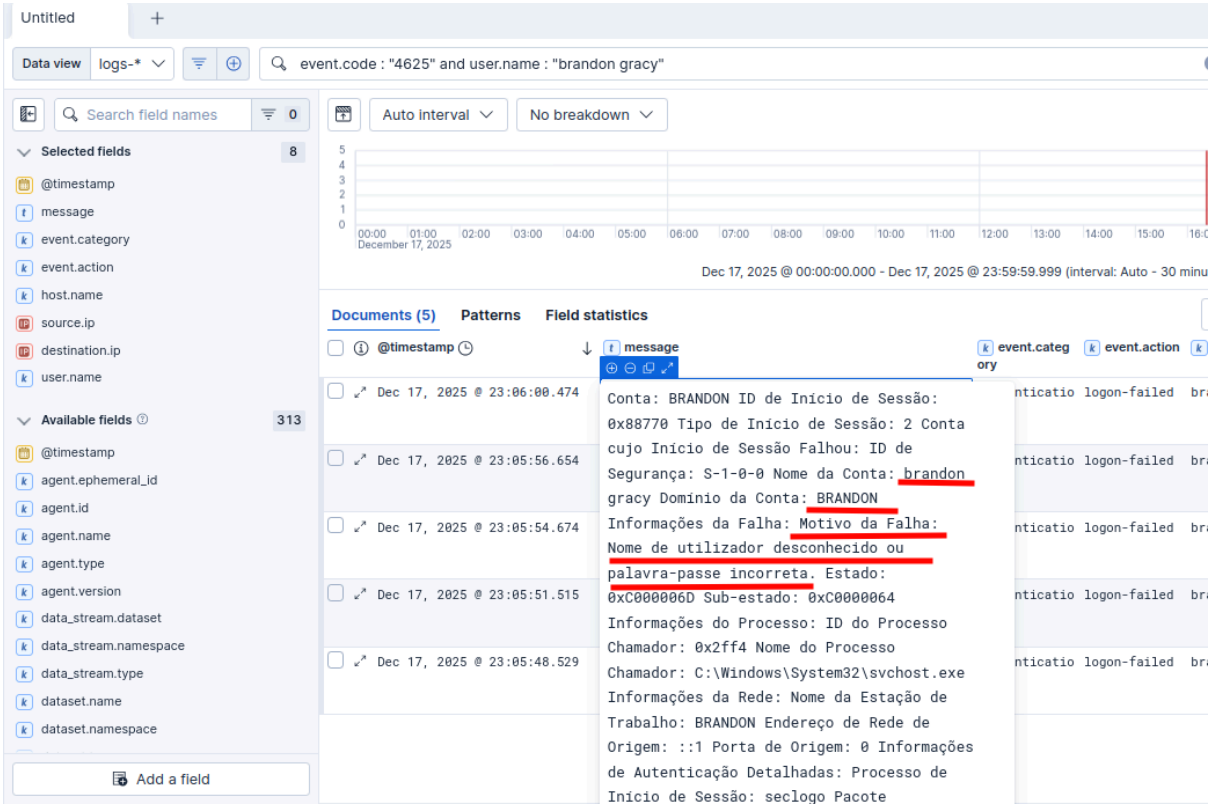
Here in Discovery tactic we can check that inside of Network Service Discovery, we can find the Potential Network Scan Detected rule enabled also.



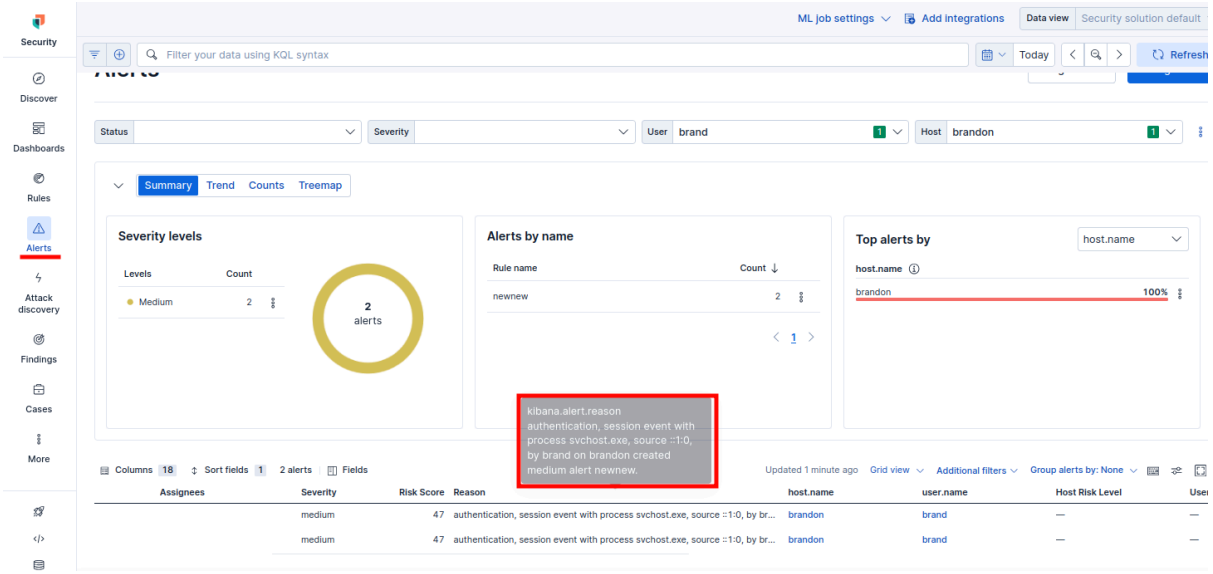
Now, in the windows vm, we run a command to fail the password authentication to see in the elastic the error.



Here we can check if the attempt failed to login.



Here, we can check what the issue is.



If we go to alerts, we can check the alert about the attempt of login.