Brute Force Attack Simulation: Investigating with Microsoft Sentinel

Project Description

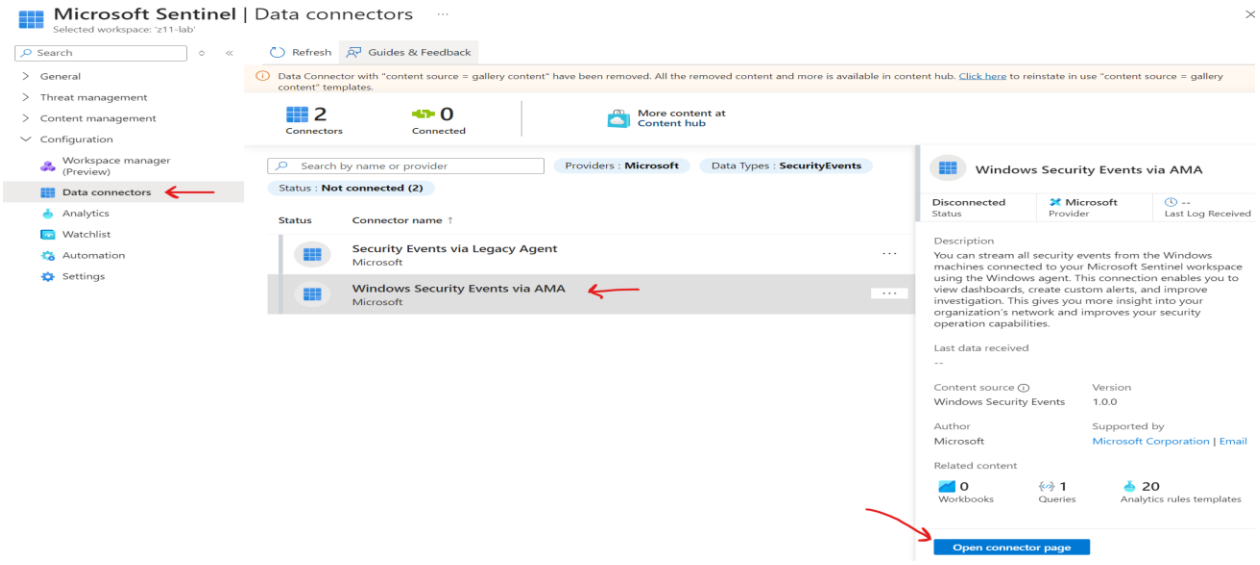
In this project, I will be simulating a brute force attack on Azure VM and then use Microsoft Sentinel logs to see details on the attack. I will create a Sentinel Analytics rule, and lastly close the investigation as benign positive.

Software and Tools

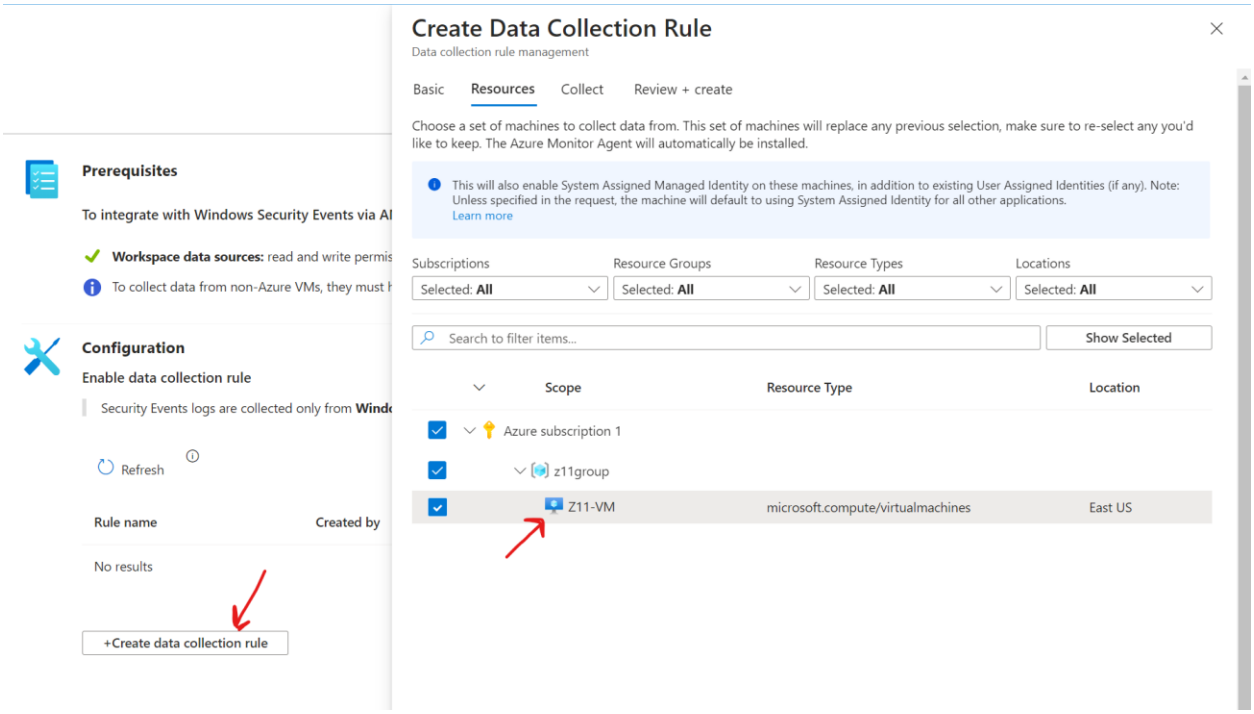
- Azure VM
- Microsoft Sentinel

Walkthrough

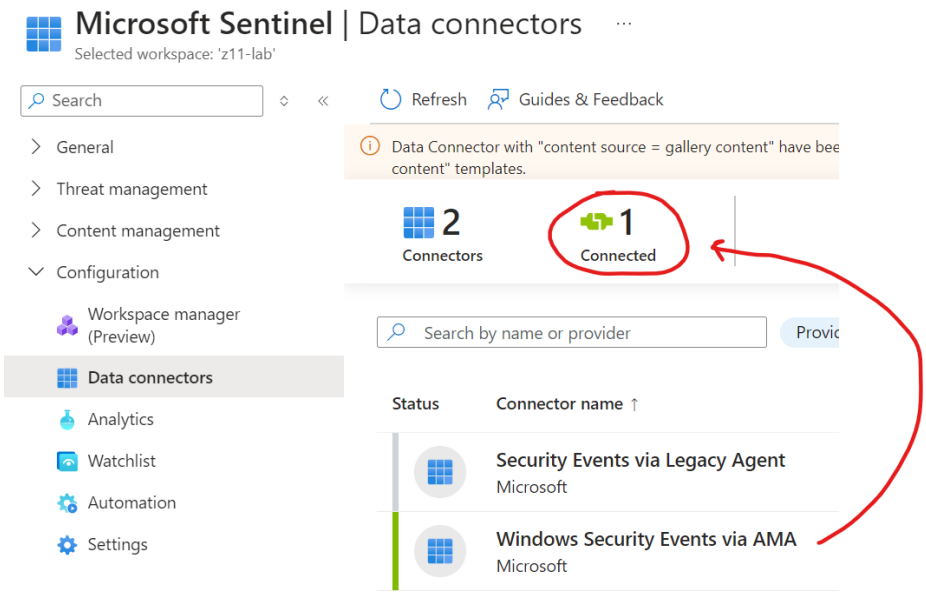
Before attempting the brute force attack, I will create a data collection rule. First, I will go to ***Microsoft Sentinel > Configutation > Data Connectors > Go to content hub***, to download the ***Windows Security Events*** connector. Once downloaded, I will open the connector page.



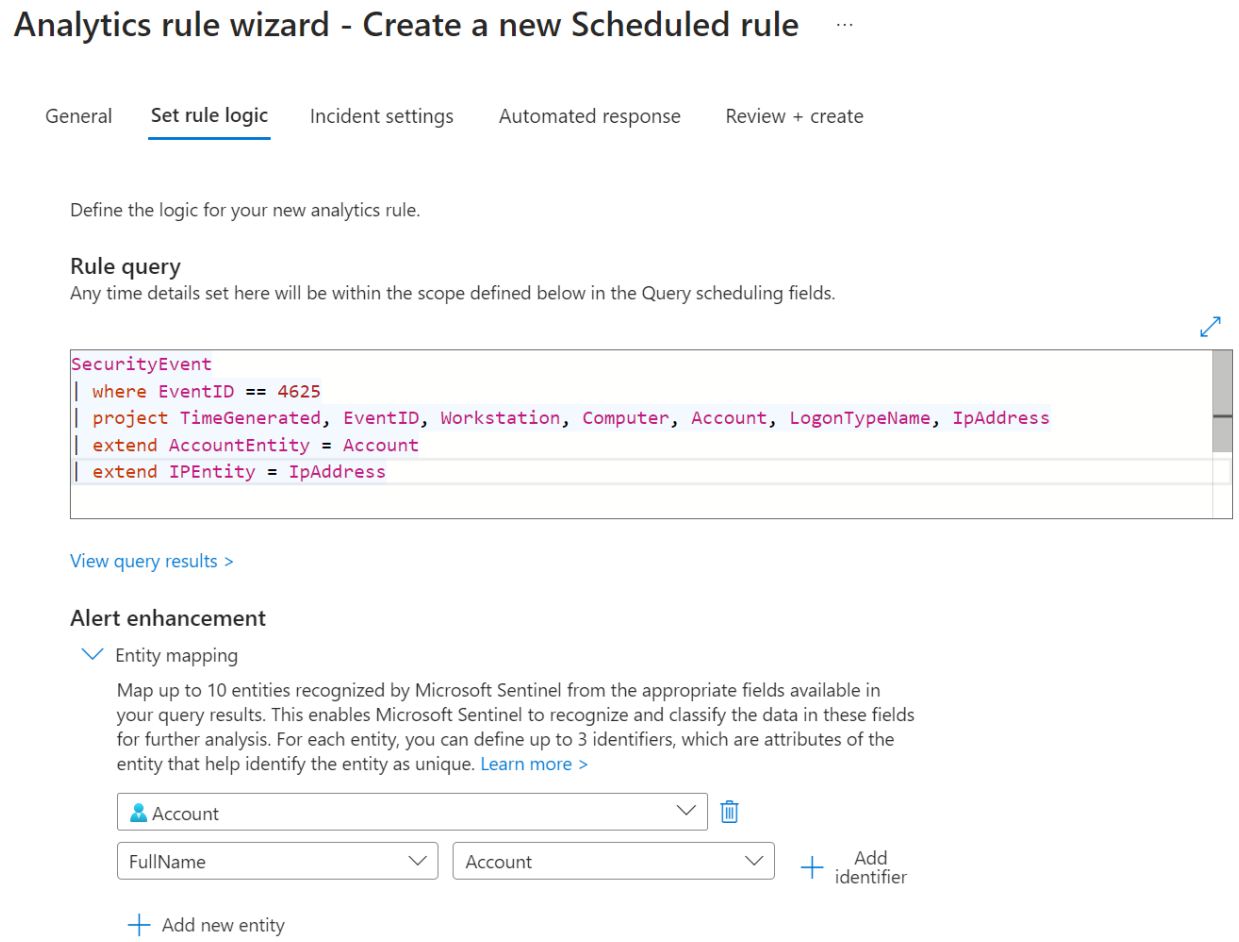
Once there, I will click on ***+Create data collection rule*** and select the machine which I want to collect data from. In this case, the machine is my VM called ***Z11-VM***. After that, I hit the Create button.



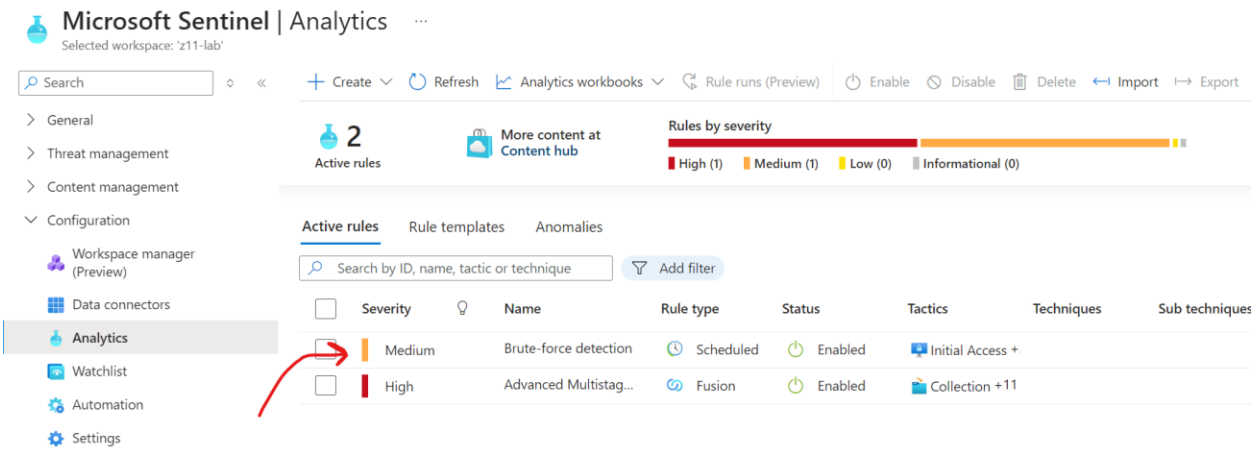
When I go back to ***Data Connectors***, I can see that Windows Security Events connector is connected.



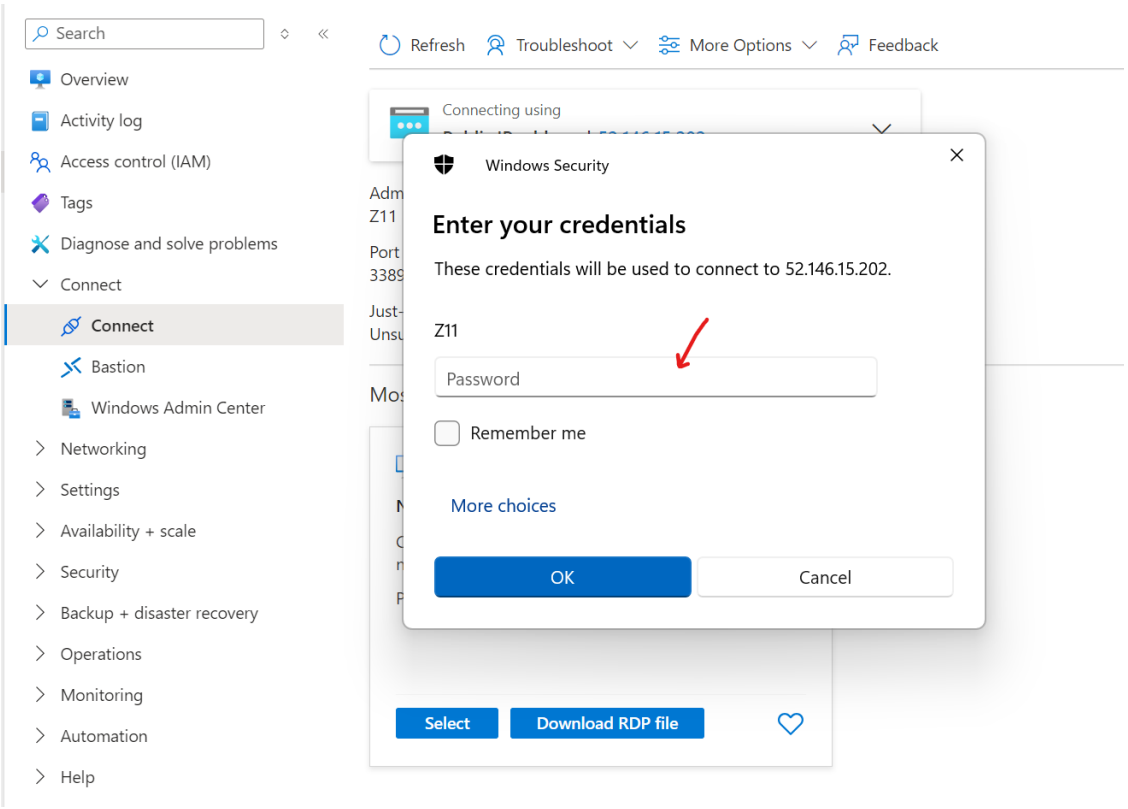
Next, I will create an Analytics rule. From ***Configutation > Analytics*** I drop down the arrow from the ***+Create*** button, then hit ***Scheduled query rule***. I will name the rule as "*Brute-force detection"* and set the Severity as *Medium.* As for MITRE ATT&CK, I will select *Initial Access, Privilege Escalation,* and *Credential Access*. Next, I will define the rule logic in the ***Analytics rule wizard*** section and select the entity that will be mapped to the alert. Both are seen in the image below.



The analytic rule is now listed on my *Active Rules* tab.

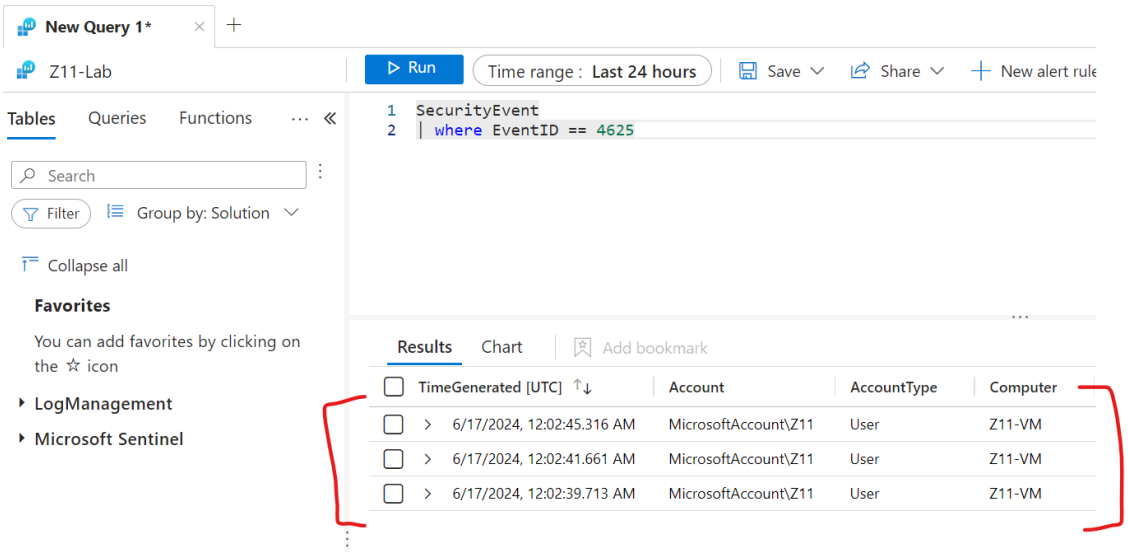


Now, I will go back to my virtual machine and hit *Connect*. I will click on *Download RDP file.* After downloading the file and double-clicking on it, it prompted me to enter the password of my VM account as seen below. This is where I will purposely enter incorrect passwords to simulate a brute force attack. In this case, I will attempt to access the account three times.

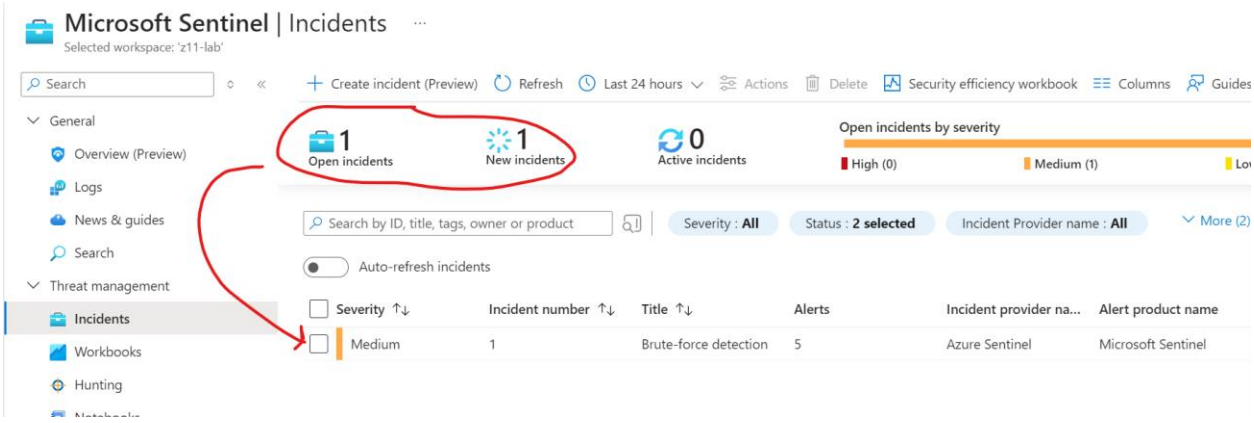


After failing to access my VM account, I went back to Microsoft Sentinel to start querying events. Specifically, I am interested in querying events with

the ID ***4625*** since it's the event related to failed login attempts. As seen in the image below, we can see that Microsoft Sentinel collected three logs after I queried this specific event, which matches the amount of attempts I made. It also matches the account that attempted the logins which is ***Z11***.

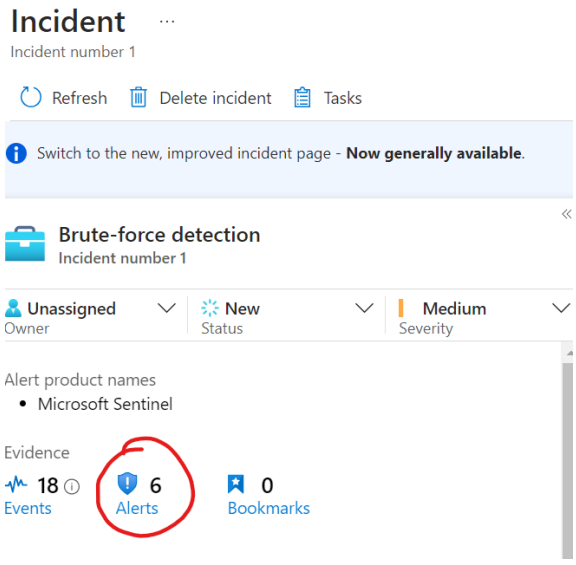


To further confirm the alert, I went to ***Configutation > Incidents*** to check if there are any new incidents. Once I got there, Sentinel showed one new incident titled "*Brute-force detection",* the same name as the alert I created.



From there, I clicked on *View Full Details.* It showed an overview of the events and alerts. Apparently, it displayed six alerts and not three. After doing some research, the reason why it shows double the number of alerts,

is due to another rule set for abnormal behaviors (like failed logins), which I have not disabled and triggered these additional alerts.



Lastly, I will conclude my investigation by clicking on the *Status* tab, choose *Close*, and classify it as *Benign Positive*.