

# **Brute Force Attack Simulation: Investigating with Microsoft Sentinel**

## **Project Description**

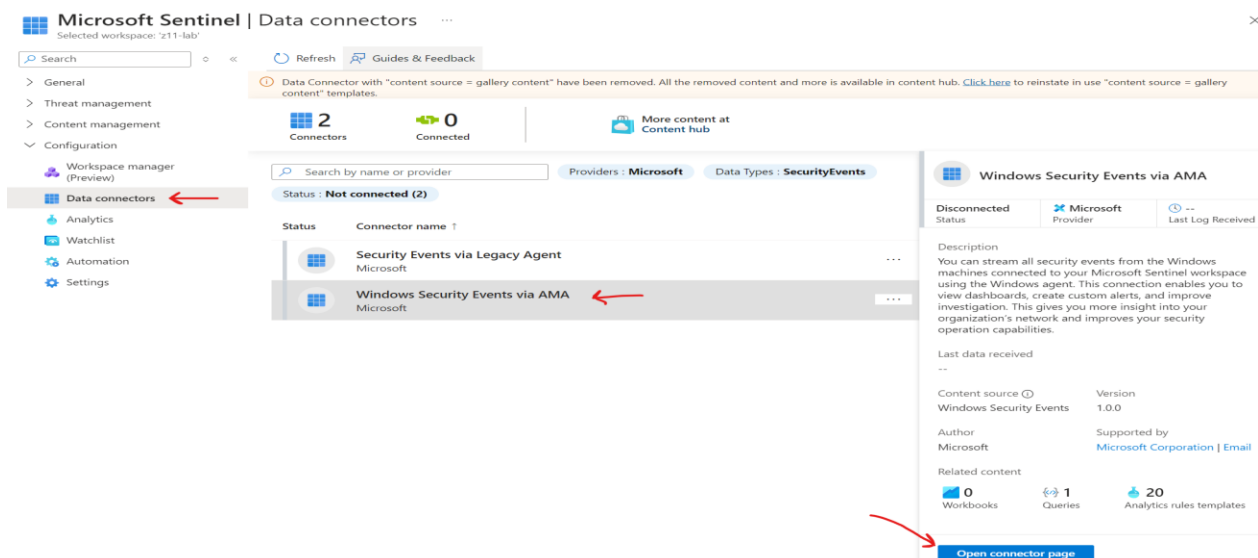
In this project, I will be simulating a brute force attack on Azure VM and then use Microsoft Sentinel logs to see details on the attack. I will create a Sentinel Analytics rule, and lastly close the investigation as benign positive.

## **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 > Configuration > 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.

**Create Data Collection Rule**  
Data collection rule management

Basic **Resources** Collect Review + create

Choose a set of machines to collect data from. This set of machines will replace any previous selection, make sure to re-select any you'd like to keep. The Azure Monitor Agent will automatically be installed.

This will also enable System Assigned Managed Identity on these machines, in addition to existing User Assigned Identities (if any). Note: Unless specified in the request, the machine will default to using System Assigned Identity for all other applications. [Learn more](#)

Subscriptions: Selected: All  
Resource Groups: Selected: All  
Resource Types: Selected: All  
Locations: Selected: All

Search to filter items... Show Selected

Scope	Resource Type	Location
Azure subscription 1		
z11group		
<input checked="" type="checkbox"/> Z11-VM	microsoft.compute/virtualmachines	East US

Prerequisites  
To integrate with Windows Security Events via AMA...

Configuration  
Enable data collection rule  
Security Events logs are collected only from Windows...

Rule name  
Created by

No results

+Create data collection rule

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

**Microsoft Sentinel | Data connectors**  
Selected workspace: 'z11-lab'

Search Refresh Guides & Feedback

> General  
> Threat management  
> Content management  
v Configuration

Workspace manager (Preview)  
**Data connectors**  
Analytics  
Watchlist  
Automation  
Settings

2 Connectors

1 Connected

Search by name or provider Provide

Status	Connector name ↑
	Security Events via Legacy Agent Microsoft
	Windows Security Events via AMA Microsoft

Next, I will create an Analytics rule. From **Configuration > 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.

### Analytics rule wizard - Create a new Scheduled rule ...

General Set rule logic Incident settings Automated response Review + create

Define the logic for your new analytics rule.

#### Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

```
SecurityEvent
| where EventID == 4625
| project TimeGenerated, EventID, Workstation, Computer, Account, LogonTypeName, IPAddress
| extend AccountEntity = Account
| extend IPEntity = IPAddress
```

[View query results >](#)

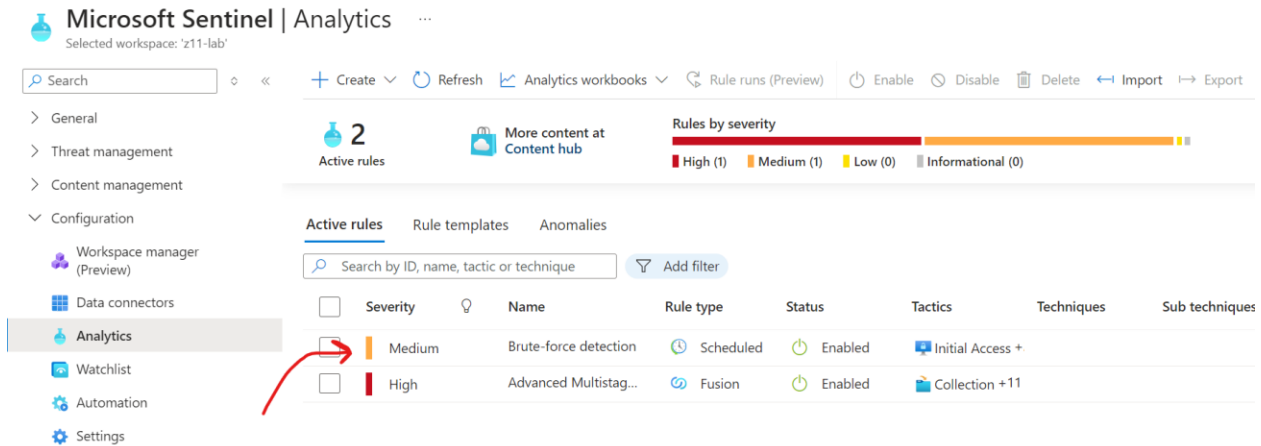
#### Alert enhancement

##### Entity mapping

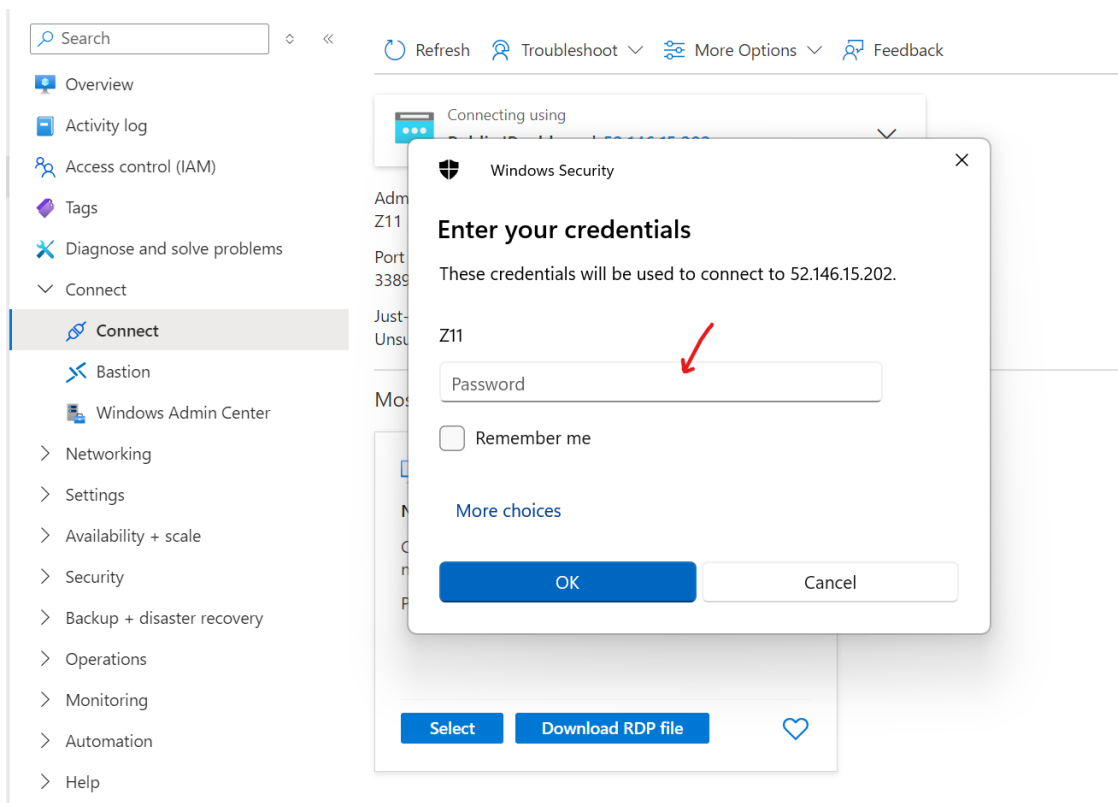
Map up to 10 entities recognized by Microsoft Sentinel from the appropriate fields available in your query results. This enables Microsoft Sentinel to recognize and classify the data in these fields for further analysis. For each entity, you can define up to 3 identifiers, which are attributes of the entity that help identify the entity as unique. [Learn more >](#)

<div>Account</div>	<div>+</div>	<div>Add identifier</div>
<div>FullName</div>	<div>Account</div>	
<div>+ Add new entity</div>		

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**.

The screenshot shows a query in the Microsoft Sentinel interface. The query is: `SecurityEvent | where EventID == 4625`. The results table shows three entries, all for the account `MicrosoftAccount\Z11` on the computer `Z11-VM`. The times are 6/17/2024, 12:02:45.316 AM, 6/17/2024, 12:02:41.661 AM, and 6/17/2024, 12:02:39.713 AM. A red box highlights the results table.

TimeGenerated [UTC]	Account	AccountType	Computer
> 6/17/2024, 12:02:45.316 AM	MicrosoftAccount\Z11	User	Z11-VM
> 6/17/2024, 12:02:41.661 AM	MicrosoftAccount\Z11	User	Z11-VM
> 6/17/2024, 12:02:39.713 AM	MicrosoftAccount\Z11	User	Z11-VM

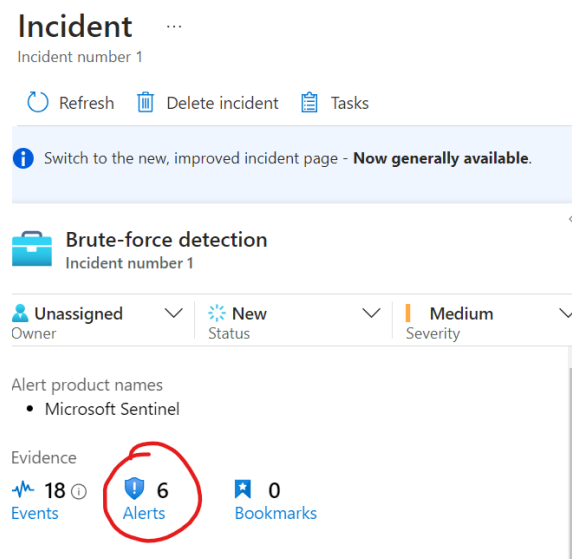
To further confirm the alert, I went to **Configuration > Incidents** to check if there are any new incidents. Once I got there, Sentinel showed one new incident titled "*Brute-force detection*", the same name as the alert I created.

The screenshot shows the Microsoft Sentinel Incidents page. The left sidebar has a red arrow pointing to the 'Incidents' link. The main area shows a summary of incidents: 1 Open incidents, 1 New incidents, and 0 Active incidents. Below this, there is a table of incidents. The first incident is titled 'Brute-force detection' with a severity of 'Medium' and 5 alerts. A red box highlights the '1 New incidents' count and the 'Brute-force detection' incident row.

Severity	Incident number	Title	Alerts	Incident provider na...	Alert product name
Medium	1	Brute-force detection	5	Azure Sentinel	Microsoft Sentinel

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*.

