Windows 10 Azure SOC Lab Project

By Bear Schneider

Goal

The goal of this lab is to create a virtual Windows machine that is open to the internet and vulnerable to attackers that may attempt to gain access. Creating this environment will allow me to gain practical experience in observing traffic to open ports, reading logs, using Security Information and Event Management (SIEM) tools, writing custom queries, and gaining some hands-on experience with Microsoft Azure and its various tools.

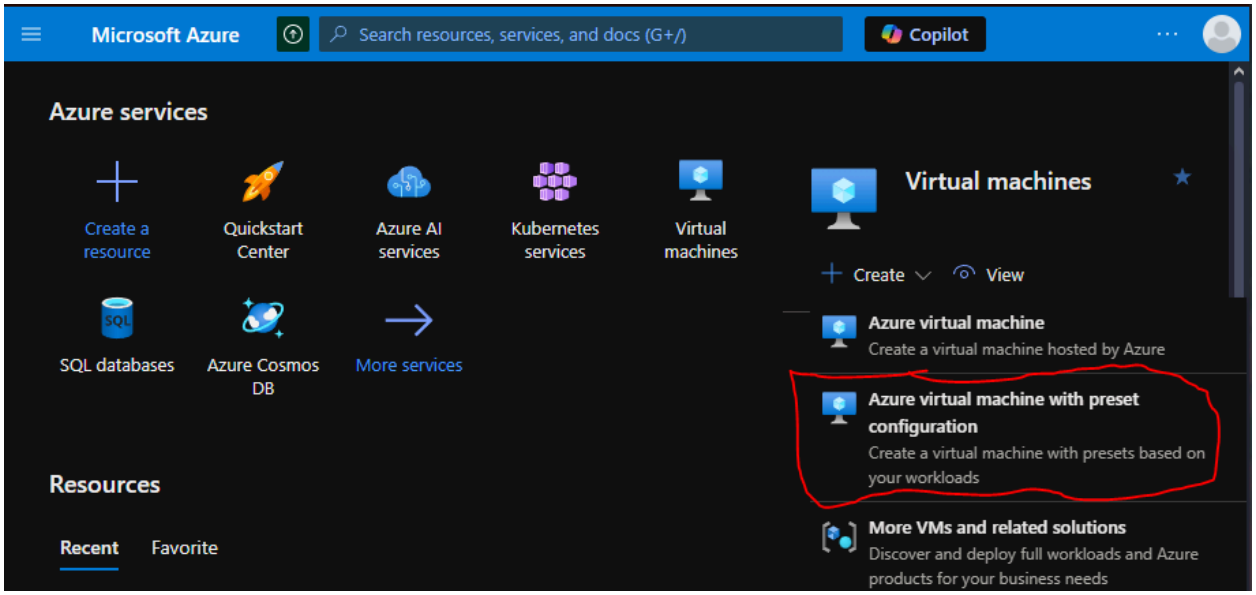
Summary

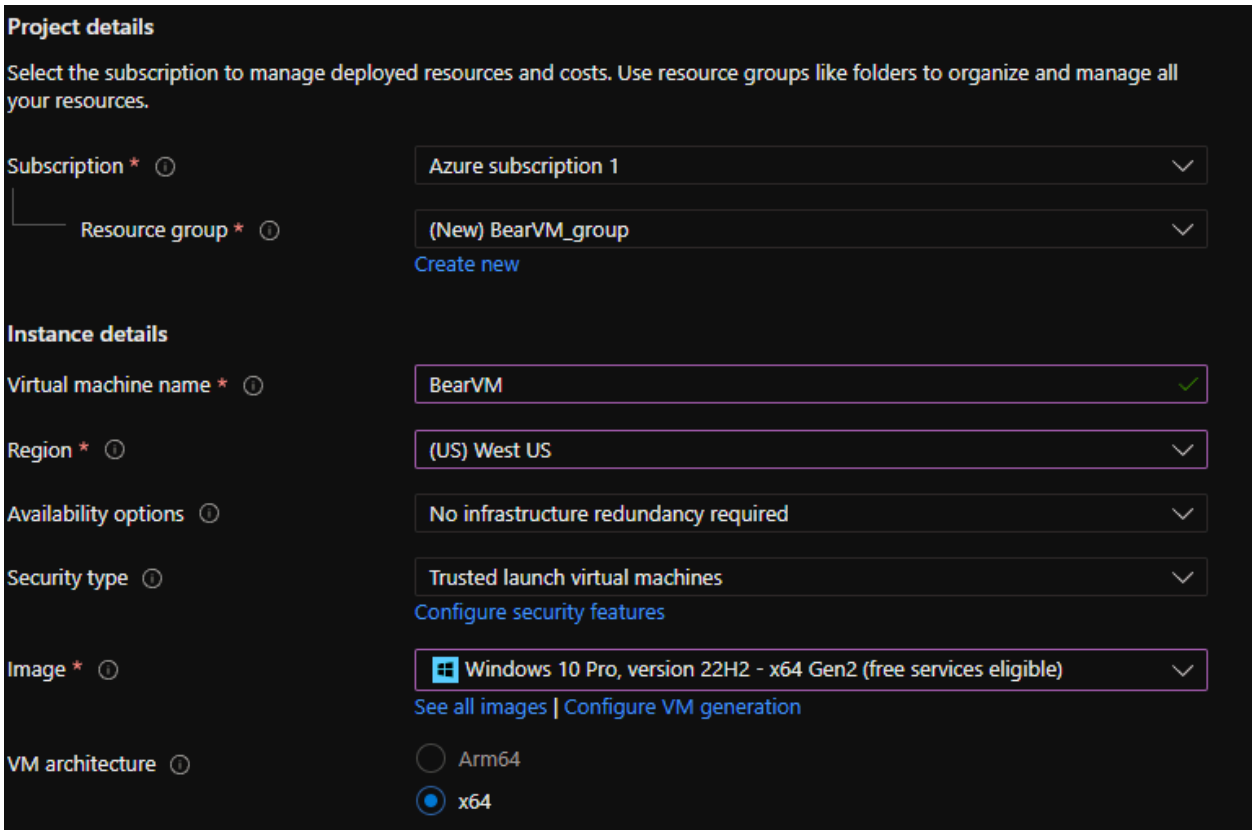
Creating a Virtual Machine (VM): We began by setting up a Windows 10 VM in Azure, The VM is set up with Remote Desktop Protocol (RDP) open, making it susceptible to security events such as brute force attacks.
Deploying Microsoft Sentinel: Once the VM was spun up, we next deployed Microsoft Sentinel, which acted as the SIEM solution. Sentinel was then added to a Log Analytics workspace, and configurations were made to ensure it could collect security events from the VM.
Setting Up Data Collection: We set up a data connector that pulled event logs from the VM, which were then sent to Sentinel for analysis.
Creating Custom Sentinel Rules: We then configured a custom Sentinel rule to monitor RDP login attempts, specifically successful sign-ins. The rule triggered alerts when unusual activity occurred, such as non-system accounts logging in via RDP.
Testing and Incident Generation: After configuring the rule, the system was tested by logging in to the VM via RDP. This generated an alert, which could be seen in the Sentinel interface as an incident, demonstrating the system's ability to detect and respond to security events.
Logging and Investigation: The VM was left running for a week to collect logs and alerts.

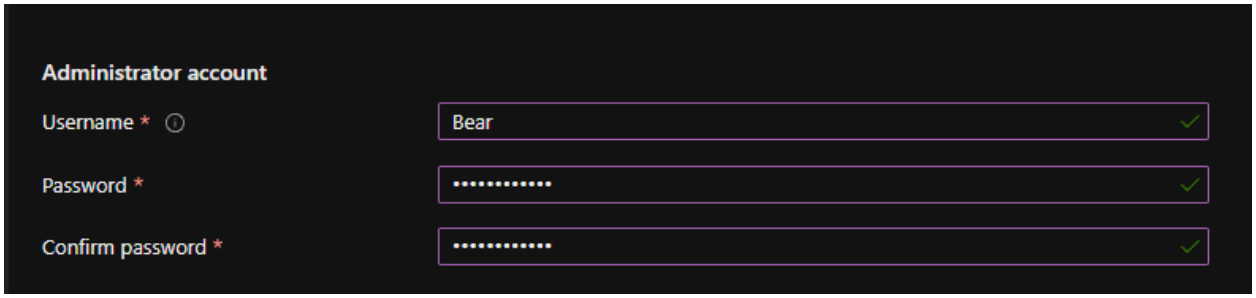
Incident Response:

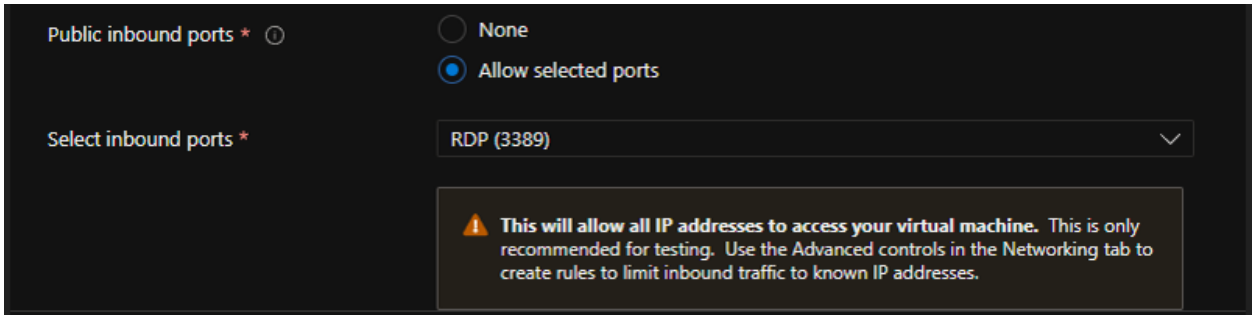
Process

The process starts by signing up for an Azure free trial, giving $200 in credit for a month. From here, we deployed a machine using Windows 10 Pro with default configurations.





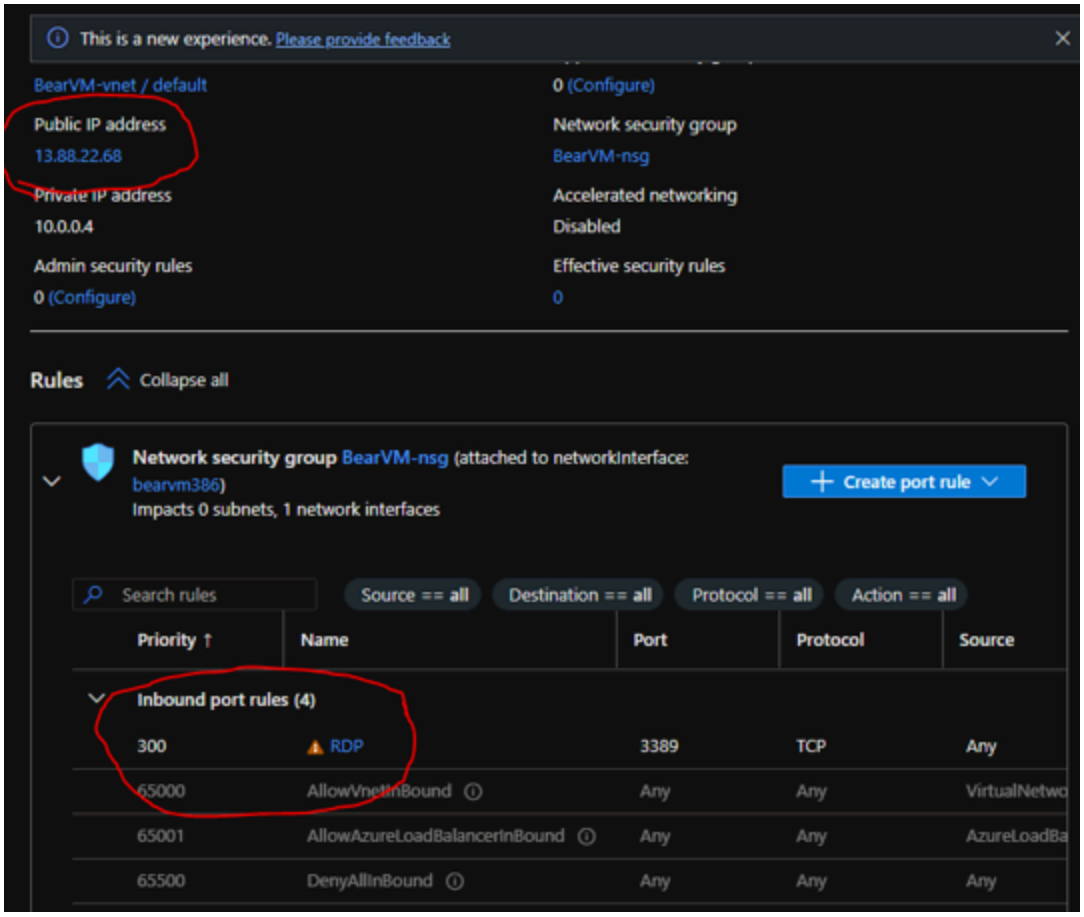




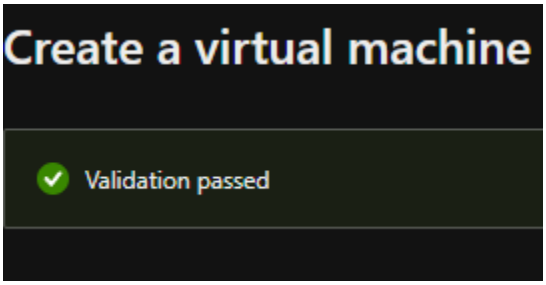
An important note for this project, as seen in the above screenshot, we are leaving Remote Desktop Protocol (RDP, port 3389) open and allowing that traffic so we can capture login attempts. We are also giving this admin account a short name and insecure password.

RANK	PASSWORD	TIME TO CRACK IT
82	**Password@123**	2 Minutes

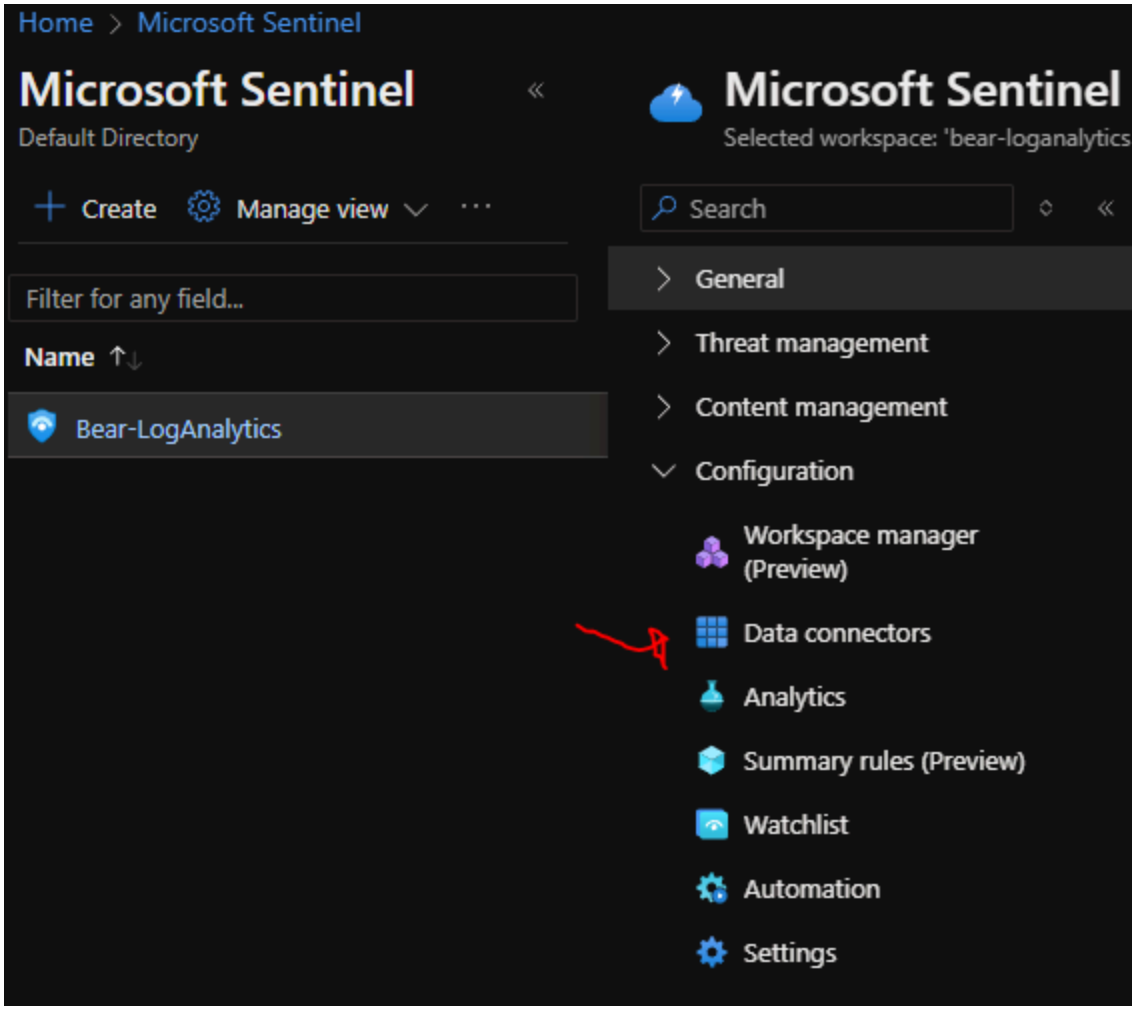
This is listed as the 82nd most common password, takes approximately 2 minutes to crack (couldn't make it too easy), and it just meets Azure's password policy requirements.



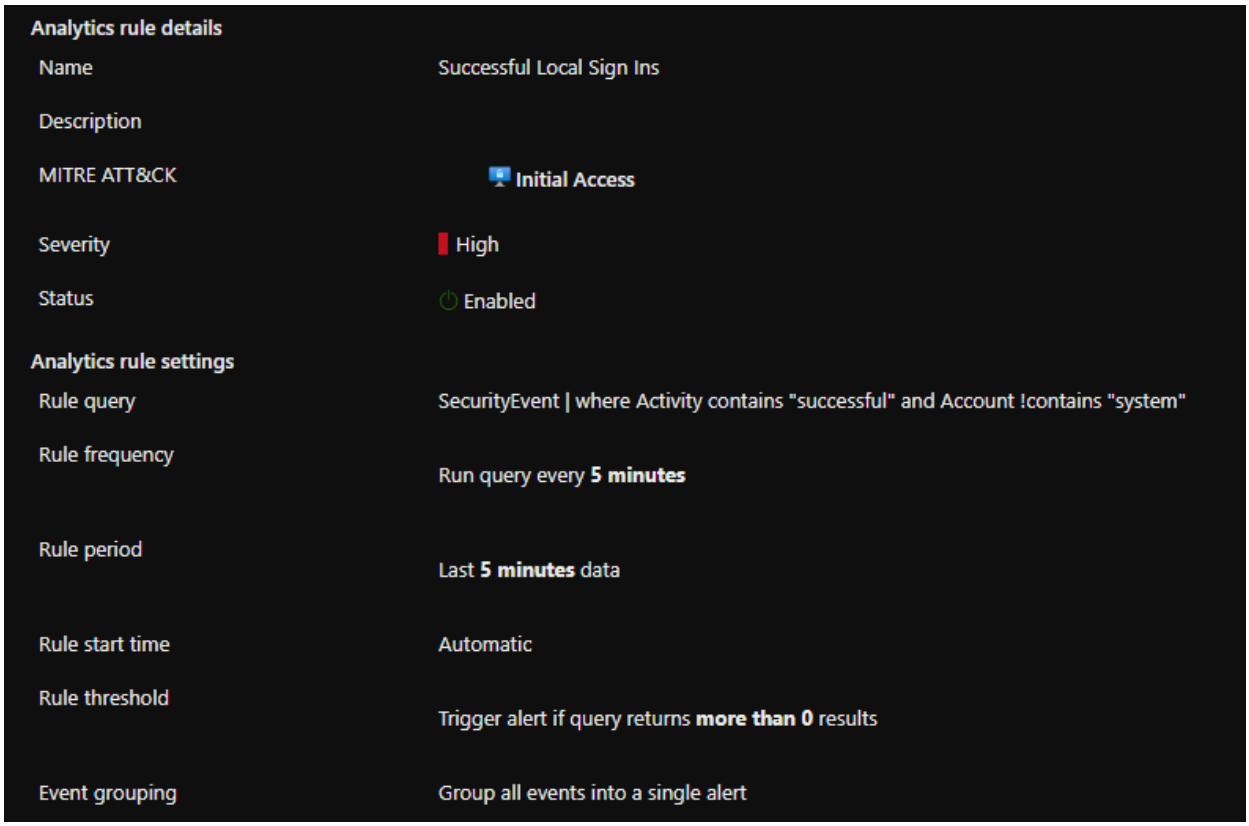
Here you can see the public IP address and confirmation that RDP is open.



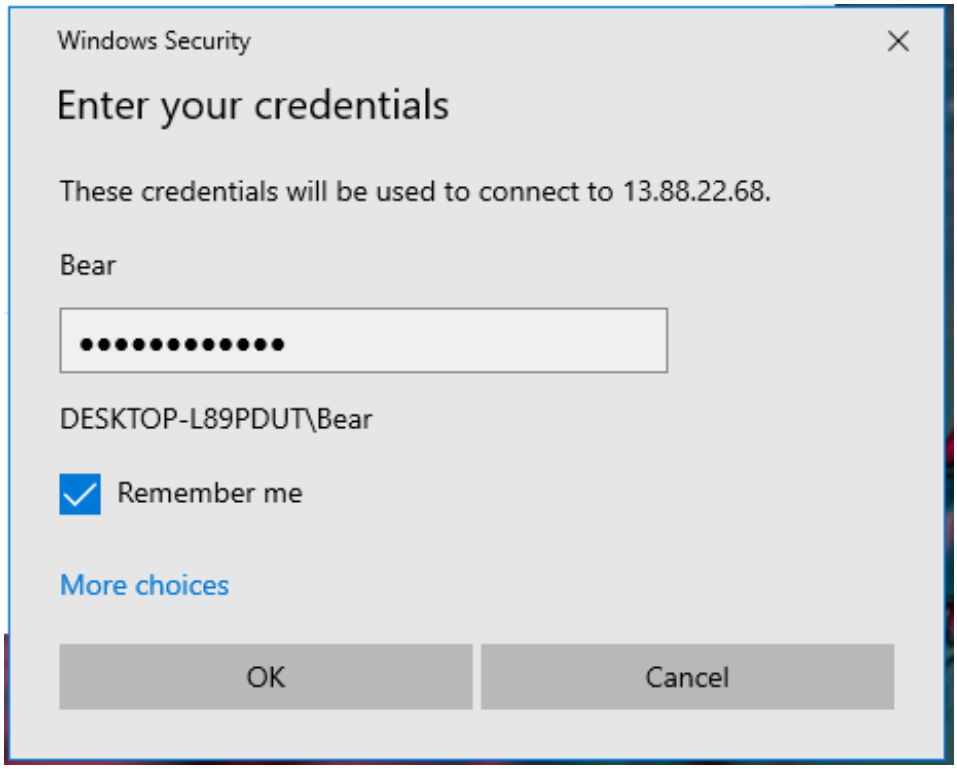
Upon successful deployment, our next steps were to create a data analytics workspace, and to configure both Microsoft Sentinel and a data connector to allow Sentinel to ingest logs for the VM.

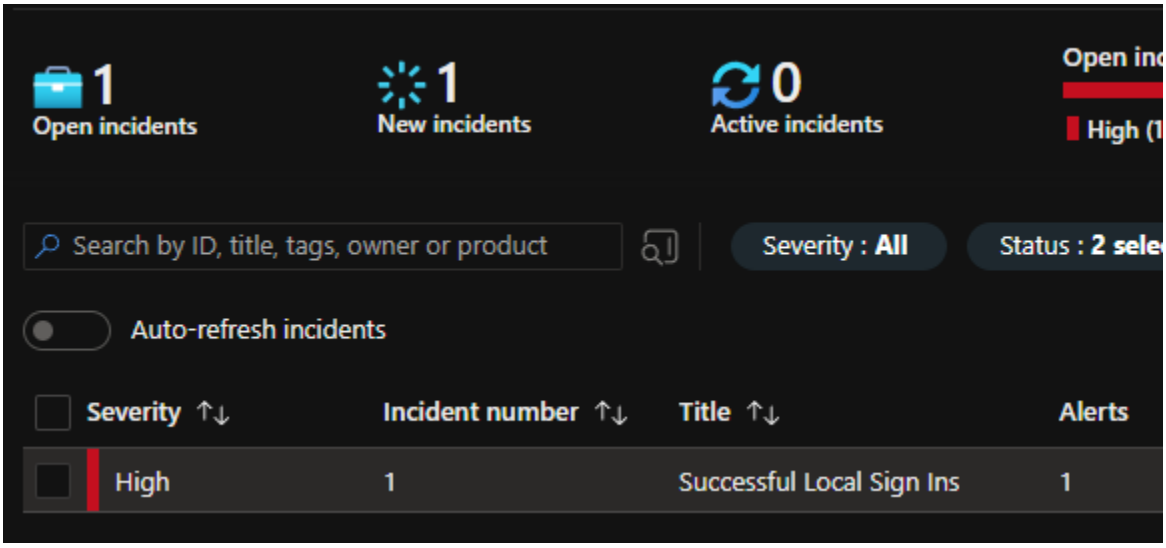

Home > Microsoft Sentinel
Microsoft Sentinel
Default Directory
Create
Manage view
Filter for any field...
Name
Bear-LogAnalytics
Microsoft Sentinel
Selected workspace: 'bear-loganalytics
Search
General
Threat management
Content management
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules (Preview)
Watchlist
Automation
Settings

We used Windows Security Events via AMA as our data connector.



Next, we created a rule to send an alert upon successful logins. We exclude any events that come from the system accessing the VM, and later we refined the Account section of the query to only return logs that had accounts that contained “Bear”, as management tools sent false positives, and any non-automated account fields start with “BearVM/”. This query runs every 5 minutes and returns any relevant logs as a single alert.





We logged in to the machine to test the alert system, and the alert did show up on the dashboard.

The next step was to wait and analyze the logs as they came in.

Account	IpAddress
\BHALL	31.43.185.39
\BPSC	31.43.185.39
\STELZER	31.43.185.39
\JAYCN	31.43.185.39
\MIMO	31.43.185.39
\KONICA	31.43.185.39
\DIRECCION	31.43.185.39
\SHAFAEY	31.43.185.39
\NAIARA	31.43.185.39
\LOGISTIC	31.43.185.39
\ROZNICA	31.43.185.39
\LPF	31.43.185.39
\GEOVANE	31.43.185.39
\OMNICOM	31.43.185.39
\GIANCARLOF	31.43.185.39
\PORTARIA	31.43.185.39
\ADISYON	31.43.185.39

\TAMIRES	45.143.201.131
\USER	45.143.201.131
\PESSOAL	45.143.201.131
\PLANO	45.143.201.131
\USER	45.143.201.131
\RH01	45.143.201.131
\CARMEN	45.143.201.131
\MARIA	45.143.201.131
\JOAO	45.143.201.131
\PROSOFT	45.143.201.131
\ROBERTO	45.143.201.131
\MANUEL	45.143.201.131
\ESTAGIO	45.143.201.131
\HR	45.143.201.131
\IGOR	45.143.201.131
\ALBERTO	45.143.201.131
\JAVIER	45.143.201.131

Within a few hours, we had several thousand brute force attempts. These are the top 2 IP's, and a couple guesses from iplocation:

Geolocation data from IP2Location — Product: DB6, 2024-10-15

IP ADDRESS: 31.43.185.39	**ISP:** FOP Dmytro Nedilskyi
COUNTRY: Netherlands	**ORGANIZATION:** Not available
REGION: Noord-Holland	**LATITUDE:** 52.3785
CITY: Amsterdam	**LONGITUDE:** 4.9000

Incorrect location? Contact IP2Location — view map

Geolocation data from ipinfo.io — Product: API, real-time

IP ADDRESS: 31.43.185.39	**ISP:** Not available
COUNTRY: Ukraine	**ORGANIZATION:** AS211736 FOP Dmytro Nedilskyi
REGION: Kyiv City	**LATITUDE:** 50.4547
CITY: Kyiv	**LONGITUDE:** 30.5238

Incorrect location? Contact ipinfo.io — view map

Geolocation data from ipbase.com — Product: API, real-time

IP ADDRESS: 45.143.201.131	**ISP:** TOV E-RISHENNYA
COUNTRY: Belgium	**ORGANIZATION:** TOV E-RISHENNYA
REGION: Brussels	**LATITUDE:** 50.8504
CITY: Brussels	**LONGITUDE:** 4.3488

Incorrect location? Contact ipbase.com — view map

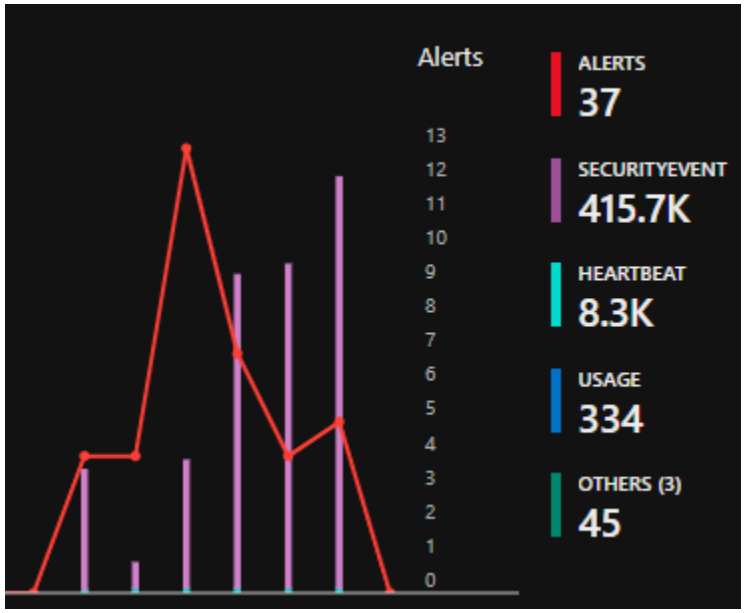
Geolocation data from criminalip.io — Product: API, real-time

IP ADDRESS: 45.143.201.131	**ISP:** Not available
COUNTRY: Russia	**ORGANIZATION:** Tov E-rishennya
REGION: Not available	**LATITUDE:** 55.7386
CITY: Not available	**LONGITUDE:** 37.6068

Personal note: This last site is called “criminalip.io” and was the only source with Russia as the address, I found that humorous

After two days, we did encounter some successful attempts and were properly alerted.

We left the VM running for a week, and here are the results:



In total, 37 separate events with 57 successful logins from different sources, and 415,000 events in total