BlogSpot

BruCON Student CTF

Saturday 6 October 9h00-17h00

Voldersstraat 9 Aula - 9000 Gent

Target public: Students interested in hacking and general IT Security in a fun challenging way.

We started in the morning by setting up in groups all around the room. It was very hard to get started with the CTF because of internet problems. I was also not very prepared, missing a lot of programs and VM's that could have been useful in solving some of the challenges. Finding, downloading and installing tools made me lose a lot of time that could have been spent on finding early challenges.

By the time it was noon, we had only found a few flags, so we took a break. We decided to go for a walk and some food and took our lunch from McDonald's back to the hall.

In the afternoon, we found some more flags, including most of the lockpicking ones and a Lego building challenge. We didn't participate in other physical hacking challenges and decided to focus on the online ones. I, myself, didn't participate in the lockpicking challenges because my team had it handled and I prefered the online challenges.

We didn't end with a great score, but learned a lot of new techniques. At the end, we watched the winners receive their prizes and all left for home.

Belgian Cyber Security Convention

Wednesday 16 October 8h30-17h30

Lamot Congress and heritage center - 2800 Mechelen

Target public: IT people, mostly professionals who work in IT, who want to learn about the newest and most recent technologies and gain more information about these topics.

Today I went to my first cyber security convention.

Personally, the first speaker was the most interesting of the whole day for me. The first speaker was someone from HackerOne, and he mostly talked about bug bounty programs and what it takes to make it a profession. An interesting example of a bug he found was from a Facebook bug bounty program putting 2 little bugs togethers. With some testing and logical thinking he was able to find a major fault in their group system and make himself leader. This tought me that it isn't always very technical to find these, just thinking logically and keep trying to think outside the box is required to be good at this.

Another talk was about Hybrid Cloud environments, where they talked about the growing market for Hybrid cloud. This combines both on-premise and cloud systems and makes them work together.

The third talk was about economics, the cost of pentesting for customers. This seemed a lot more expensive than I expected, still increasing every year. This talk was mostly about the growing cost of pentesting and increasing amount of attacks.

The next two speakers were from our own school, Howest. First was a talk about blockchain, mainly about the research team in school. We learned about what they've already achieved and what the future plans are. We've also learned about partnerships with other organizations and schools to further blockchain research. The last talk was about Industry 4.0, but since I already had seen this in school, I decided to skip this talk.

Integration - The Netflix Way

Thursday 14 November 18h00-21h00

Gaston Crommenlaan 8 Zuiderpoort - 9000 Gent

Target public: People interested in how Netflix changed streaming and what new technologies and concepts they used to achieve global recognition.

~ Organized by Integr8

This seminar was an explanation about a (relatively new) streaming platform Netflix and how they differ from previous TV shows/movie platforms to achieve a competitive edge, and proceeded to become the most-known streaming platform in the world.

We learned that different departments work closely together, so every team has their own area of expertise to work on. This is basically containers that stand on their own and always have a version ready for deployment. There is almost no downtime because every type of serie/movie has its own container, making the downtime always short and for a small part of the entire platform.

We also had a recap of waterfall vs agile, previously seen in classes. Here we saw how they also use it in Netflix to prevent downtime. They basically used agile but refined and compartmentalized it so the downtime is much less than other streaming platforms.

After the talk we went outside to have some nice fancy hotdogs and a conversation and ended our evening with full stomaches :)

Vacature

Pen tester - Ethical Hacker

Hack'em | Gent | Voltijds

Je zal verantwoordelijk zijn voor volgende taken:

- Seminaries, conventies en workshops bijwonen om de nieuwste technieken en exploits te leren.
- Mogelijke exploits in verschillende systemen en software vinden.
- Research naar bestaande kwetsbaarheden in zowel software als hardware.
- Analyseren van gekende cyberaanvallen.
- Kwetsbaarheden categoriseren volgens impact en waarschijnlijkbaarheid.
- Automatisering en samenwerking van verschillende kwetsbaarheidsscanners programmeren.

Je profiel

- Minimum een Professionele Bachelor of Master in ICT.
- Vlot in Nederlands en Engels, zowel schriftelijk als verbaal.
- Kennis in pentesting en hacking tools.
- Goede kennis van Operating Systems (Windows, Linux)
- Goed kunnen samenwerken met anderen en ideeën wisselen.
- Je hebt een goede kennis rond netwerken en de meest voorkomende problemen.
- Je blijft up-to-date met IT Security kennis.

Locatie

Je zal hoofdzakelijk werken in onze hoofdzetel te Gent, en regelmatig reizen naar conventies en workshops over heel de wereld (vooral US).

Wat hebben wij te bieden?

- Persoonlijke samenwerking met sommige van de beste pen testers in België.
- Een trainingsplan afgestemd op jouw persoonlijke sterktes.
- Een flexibele open werkomgeving.
- Werken met de nieuwste technologieën in IT Security.
- Een aantrekkelijk startsalaris.
- Extralegale voordelen in de vorm van een auto, vervoerskosten en verblijf in buitenland tijdens onderzoeksreizen.

Tutorial

Azure Sentinel start guide

This tutorial is made for people who have installed Azure Sentinel and now want to start analyzing their data.

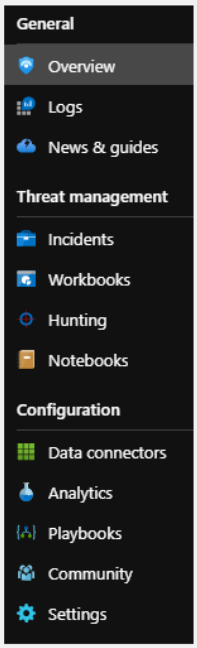

Fig.1 Azure Sentinel navigation bar

To first start collecting data from your environment, start on Configuration - Data connectors

Here you find a list with all the possible data sources you can connect to Azure Sentinel. This includes Windows Events, Linux or server syslogs, Firewall Applications, and many more.

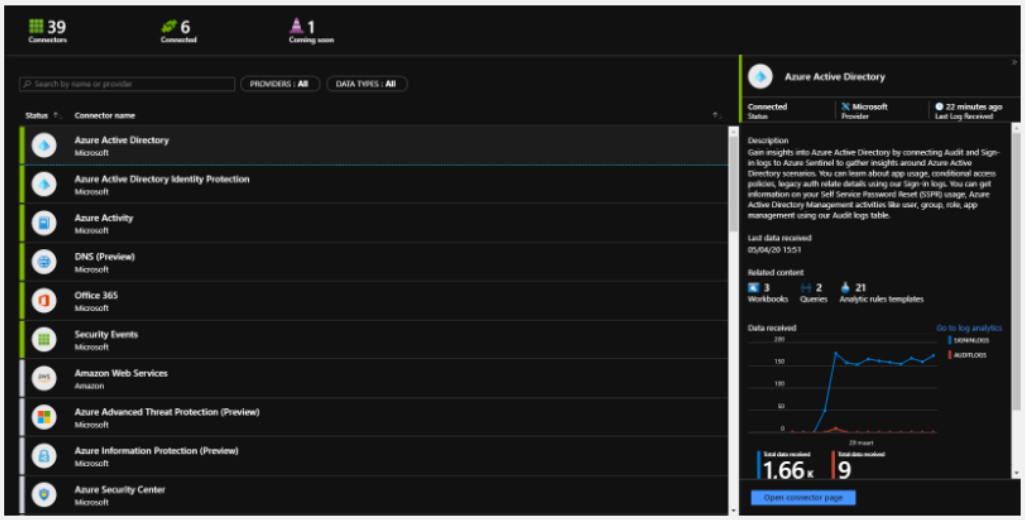

Fig.2 Data connectors

Select the data source you want to collect data from and press the Open connector page at the bottom.

Every connector has an instruction page for the requirements and how to gather data in Azure Sentinel. For example, to gather Windows logs you have to install a Microsoft Monitoring Agent on the system, which can then be found in **Control Panel - System and Security - Microsoft Monitoring Agent**

For Virtual Machines in Azure, you can just select an available VM from the list and no extra steps have to be taken.

After you've followed the instructions page, you can get started with your data.

To start analyzing the collected data from your environment, go to Configuration - Analytics

There are over 100 Rule templates which can be enabled to protect against low to high severity threats.

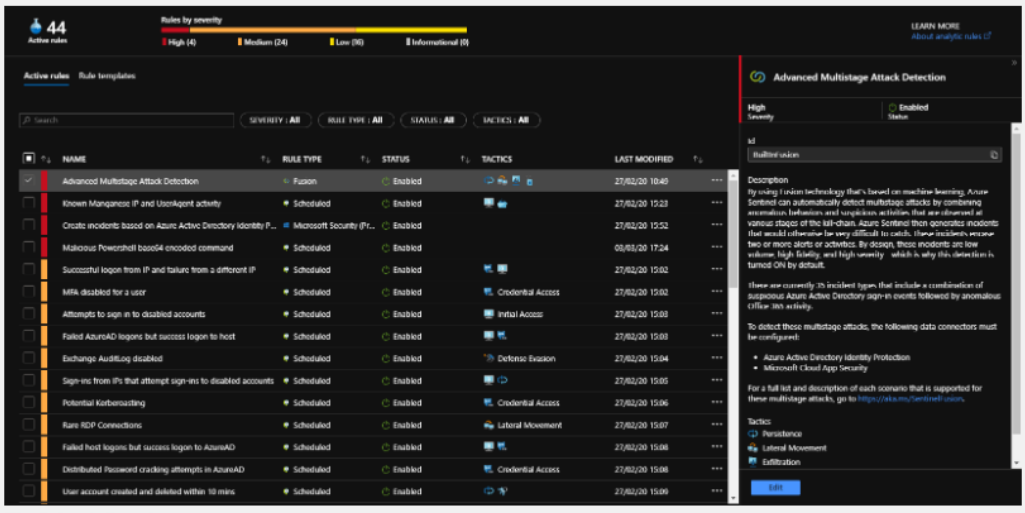

Fig.3 Analytic rules

You can also create your own custom rules using the Kusto Query Language, KQL, much like SQL.

For all these rules you can set an automated response to resolve common threats using playbooks you have to create yourself.

When one of the Analytics rules you just enabled is triggered, it will show up in Threat management - Incidents

In this tab you can focus on threat details, such as accounts and hosts involved, and all data from the run query.

Another important part is **Threat management - Workbooks**, these are visual representations of data collected, customizable dashboards for a clean look and the most important data for you. There are again templates available for people who are just getting started.

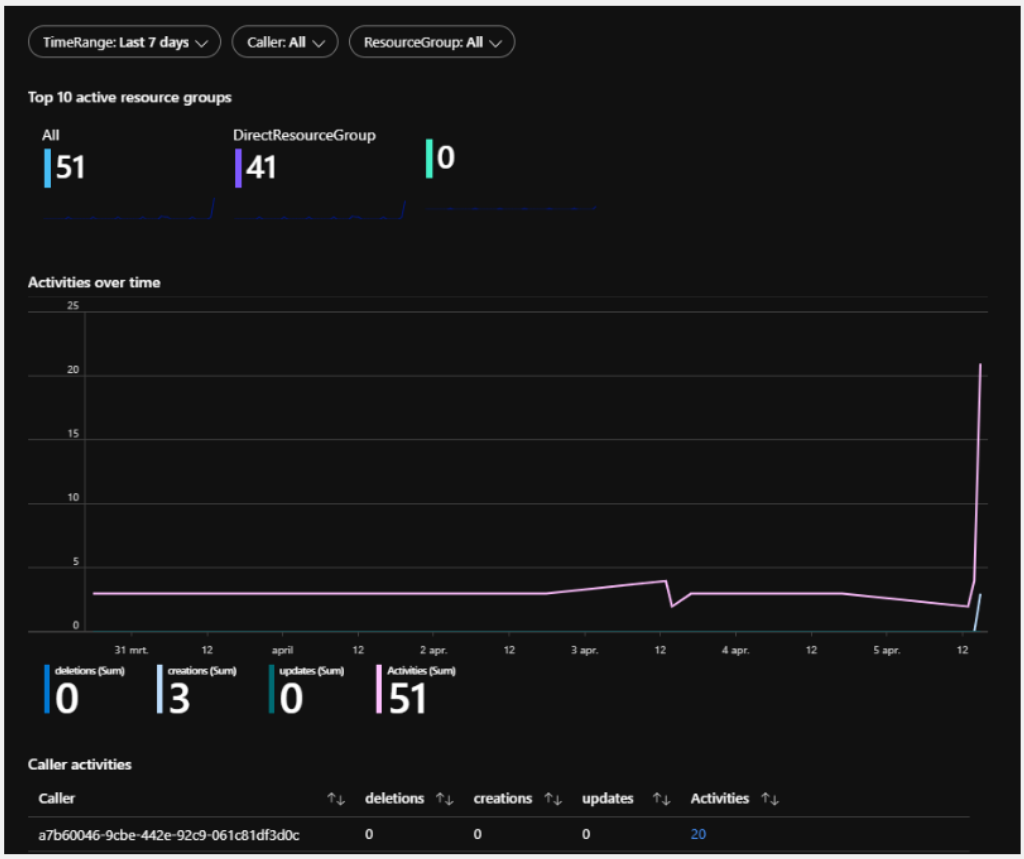

Fig.4 Azure Workbook example

To configure the automated responses of Azure Sentinel, we use **Configuration - Playbooks**. Here we can set the responses to a triggered alert.

To trigger an automatic response for Azure Sentinel alerts, use the search function to look for "Azure Sentinel" and select the "When a response to an Azure Sentinel alert is triggered (Preview)"

To configure the automated responses of Azure Sentinel, we use **Configuration - Playbooks**. Here we can set the responses to a triggered alert.

To trigger an automatic response for Azure Sentinel alerts, use the search function to look for "Azure Sentinel" and select the "When a response to an Azure Sentinel alert is triggered (Preview)"

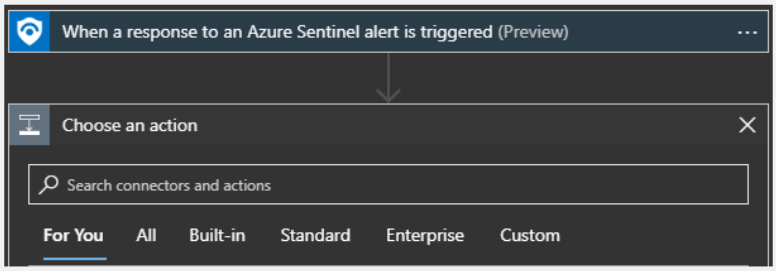

Fig.5 Logic App Designer

From here we can search for other actions to take on certain alerts such as mailing the alert, creating a ticket, integration with other products, etc.

These playbooks will now be available as a list when creating an analytics rule.

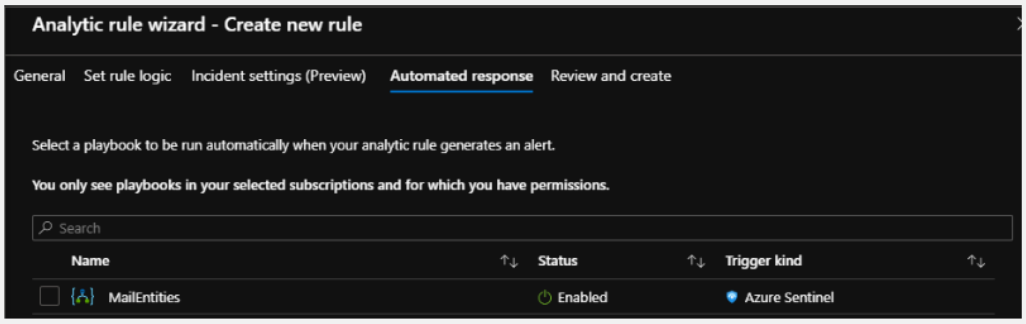

Fig.6 Playbook selection list