Project Artifact

* Table of Contents
* Project Details (project details in paragraphs)
  + Explanation of the topic

Elasticsearch is an open source, full-text search and analysis engine, based on the Apache Lucene search engine. the ELK Stack is the world’s most popular log management platform

We would use ELK Stack to make our own SIEM which has log management and analyze capabilities

We would be using ELK stack as well as write our own SIGMA rules

Logstash is a log aggregator that collects data from various input sources, executes different transformations and enhancements and then ships the data to various supported output destinations.

Kibana is a visualization layer that works on top of Elasticsearch, providing users with the ability to analyze and visualize the data.

Beats are lightweight agents that are installed on edge hosts to collect different types of data for forwarding into the stack.

SIGMA rules actual signatures written in YAML that make it possible to detect anomalies in your environment by monitoring log events that can be signs of suspicious activity and cyber threats.

* + Why the topic was chosen

Elastic search has become popular since some years and because its open source and the use of it are incomparable to any other open-source available, we wanted to work on it and learn

We thought the SIEM will utilize it’s full capabilities and can actually use by small scale company or start ups

* + How it relates to your industry
* In cybersecurity there are SOC analyst whose job is to analyze logs and report the alerts generated on the servers, company has SOC’s setup just to analyze and keep and eye on their servers, even a small amount of alert can be dangerous
  + What problem does the project address, and how does it do address it

Sure, Splunk has long been a market leader in the space. But its numerous functionalities are increasingly not worth the expensive price especially for smaller companies such as SaaS products and tech startups. ELK being open source and popular, IT professional will learn it easily

* Resources
  + List ALL resources required to complete the deliverables.
* 2 VM’s with kali linux
* Deliverables
  + List and explain all deliverables.

A SIEM on elastic stack

cloud\_id - Capstone\_custom\_SIEM:dXMtZWFzdC0yLmF3cy5lbGFzdGljLWNsb3VkLmNvbTo0NDMkZGExZjQ1YmM4ZDRmNDdlYjhiNzAxMzliMTc0OTZmMWQkZmVkZWJkZWRkZDQ1NDhmNjg3YmNhY2Q3NzVjNTUzMDU=

deployment ID - e5e3e6

* + Explain at a high-level, the method(s) the team used to complete the deliverables.
* We first installed filebeat on test machines, configured it to send data to a logstash, configure logstash to send the aggregated data to elastic search
* elastic search will index it and with help of SIGMA rules elastic alerts will be generated
* These alerts are seen on dashboards
  + Note: The documentation goes into Appendix B, not here.
* Challenges
  + List the major technical and non-technical challenges the team had in producing the deliverables. Explain how they impacted the team, and any work-arounds or resolutions.
* Major technical challenge was writing SIGMA rules, because for writing SIGMA rules we have to understand the whole vulnerability, then reproduce it if we can, then identify signature and then we can write on SIGMA rule for one vulnerability, and there are many many vulnerabilities that are continuously found
* Major non-technical challenge - Coordination, team members have different time schedules and couldn’t work on few of their part
* Lessons Learned
  + In this section, you explain what would the team repeat, what would be done differently, with an explanation for both. If you had to provide guidance to a different team doing the same (or a very similar project), what would you advise them to do/not do? It builds off the Challenges, and provides you the opportunity to explain how to avoid them.
* Get some logs to test your SIEM, maybe setup a honeypot or run your own server so that your SIEM is tested heavily,
* Have your API key stored in safe place, if its lost you have to generate again and update all your work
* Change the default password of elasticsearch “changeme” to a secure one

* Future Potential
  + What else can be done to enhance or improve this project? What resources would be required to accomplish that?
* More integration would definitely enhance this project
* For example for more visualizalization we can have something like GraphFrames, GraphFrames is a package for Apache Spark which provides DataFrame-based Graphs
* For more people to understand our SIEM we can have Juypter books, they are open source project for building beautiful, publication-quality books, websites, and documents from source material that contains computational content
* Appendices
  + Appendix A – Work Allocation
    - A list of the individual sections/work assigned to each team member.

|  | Phase - 1 | Phase - 2 | Final |
| --- | --- | --- | --- |
| Pratik | Install and configure following   * Filebeat * Elastic Search | * Install logstash * Install kibana * Visualise | * Analyse logs |
| Apoorv | Install and configure following   * Filebeat * Elastic Search | * Sigma rules * Make elastic alert based on sigma rules | * Analyse logs |
| Vahid | Install and configure following   * Filebeat * Elastic Search | * Sigma rules * Make elastic alert based on sigma rules | * Analyse logs |

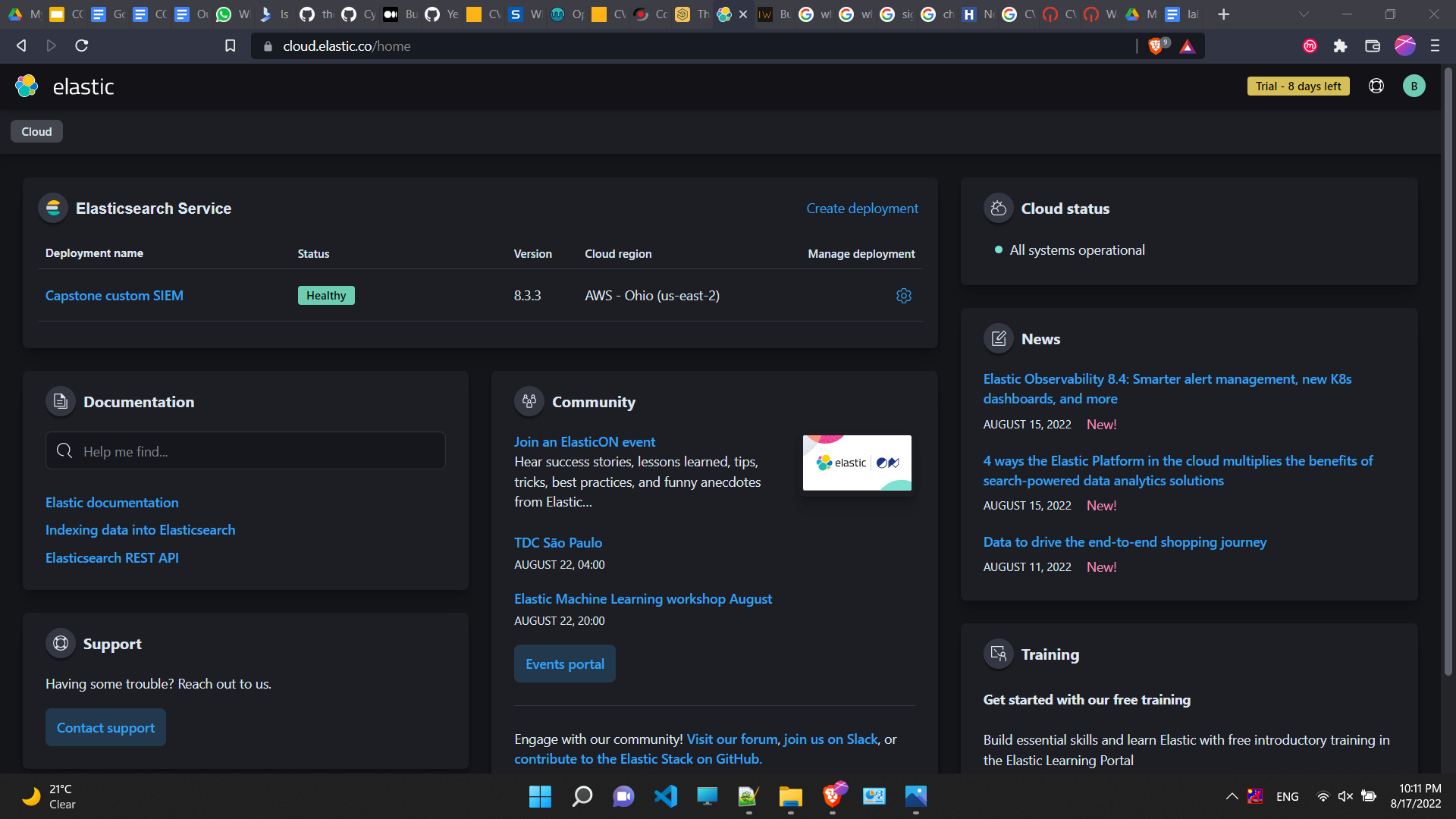
* + Appendix B – Deliverable Creation Documentation
    - This is where you place the deliverable documentation (the how-to)

This report won’t have each and every step related to elastic search but the main feature our SIEM does

This report will also have some of the main steps we followed to create our SIEM

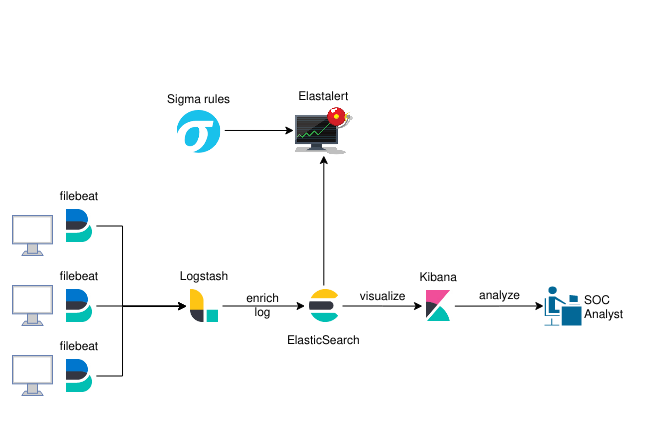
First off make an elastic search account, you can use google or facebook account for it, they give you 15 day free trial so make sure you use it well

Create your first deployment - ours is capstone custom SIEM

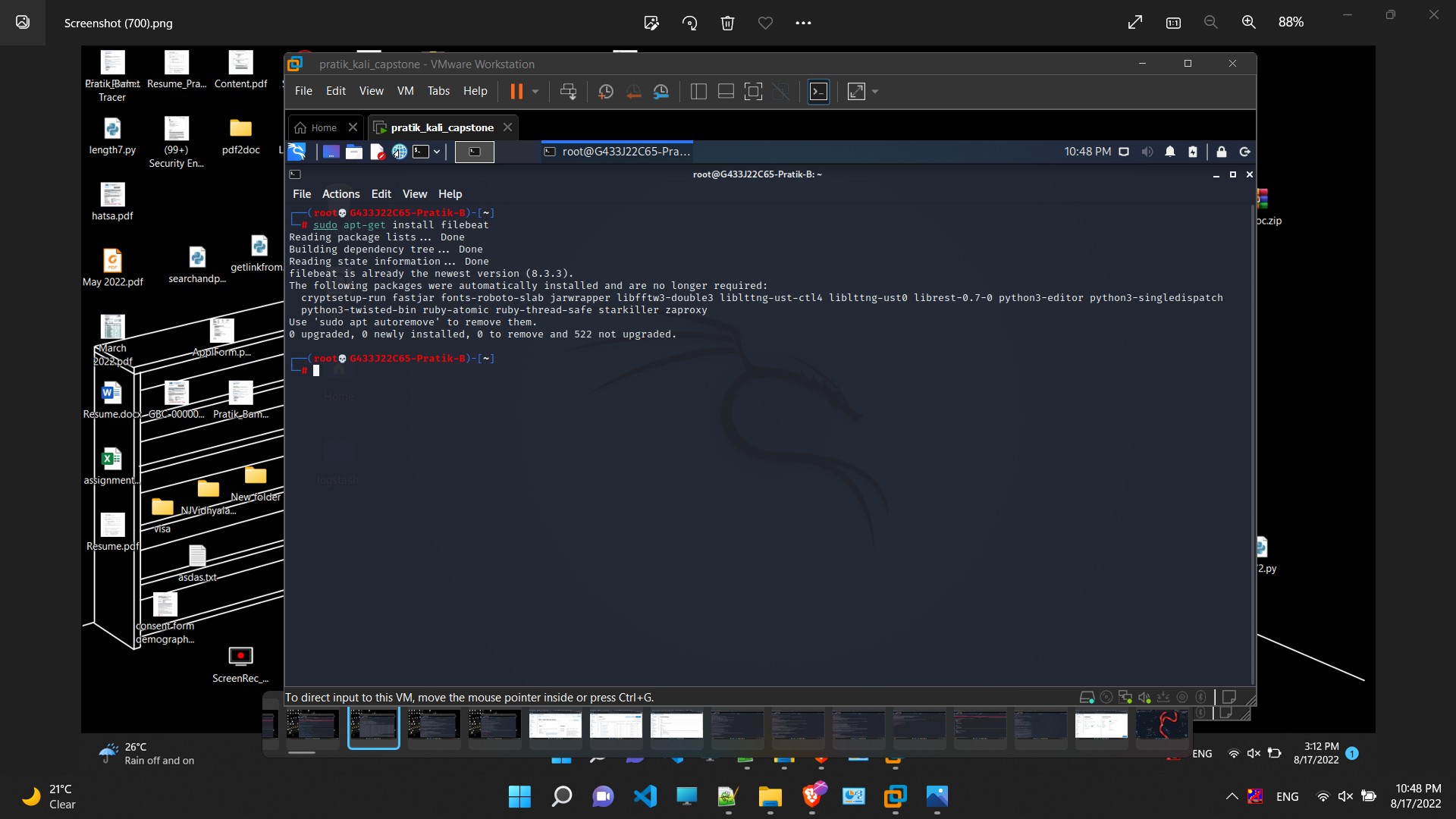


After that we need to get our cloud\_id to configure logstash so press on the setting button and it will displayed

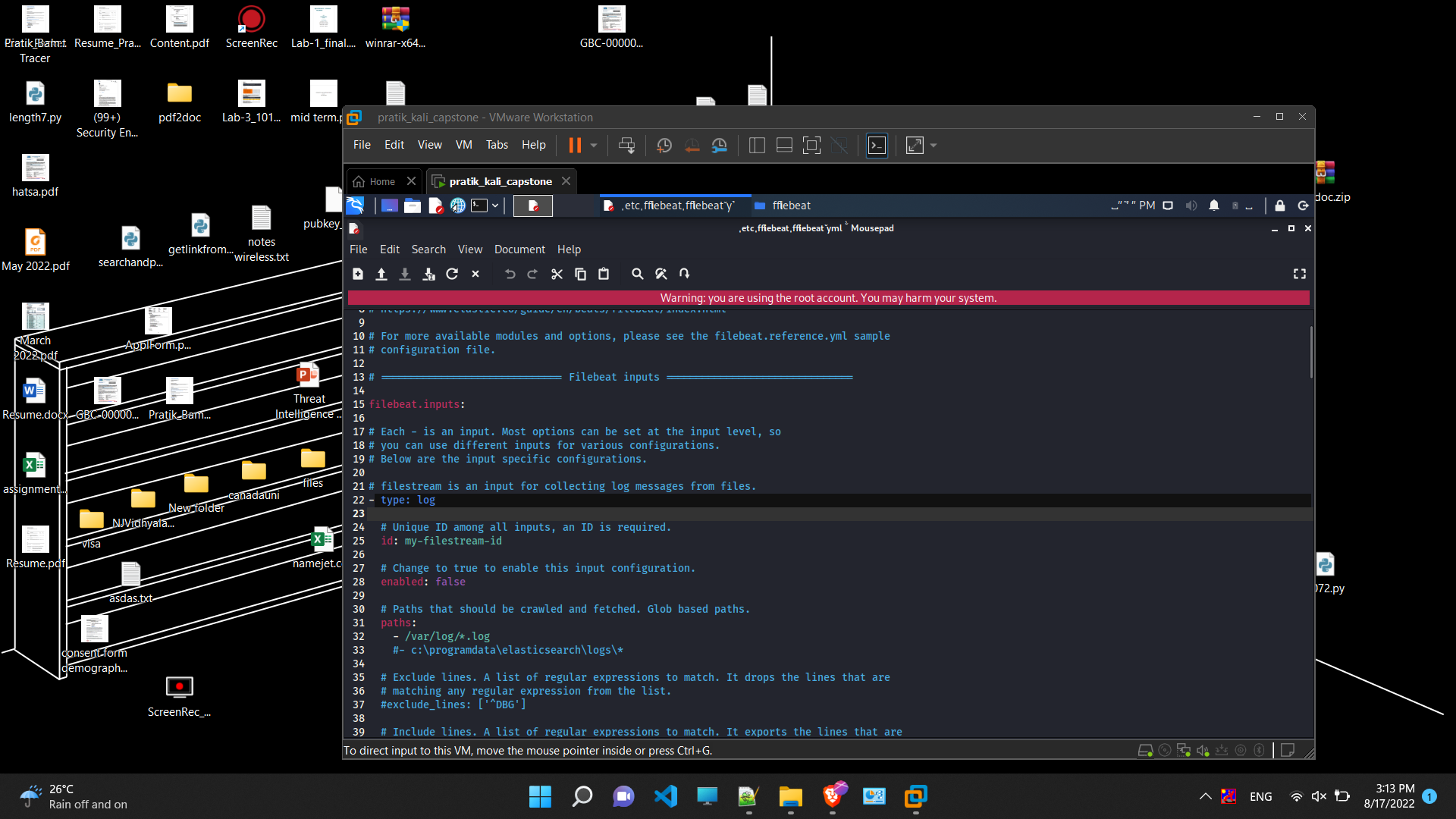
Based on the idea here is the architect we will follow for our SIEM



First we will setup filebeat on machine and configure it to send data to logstash

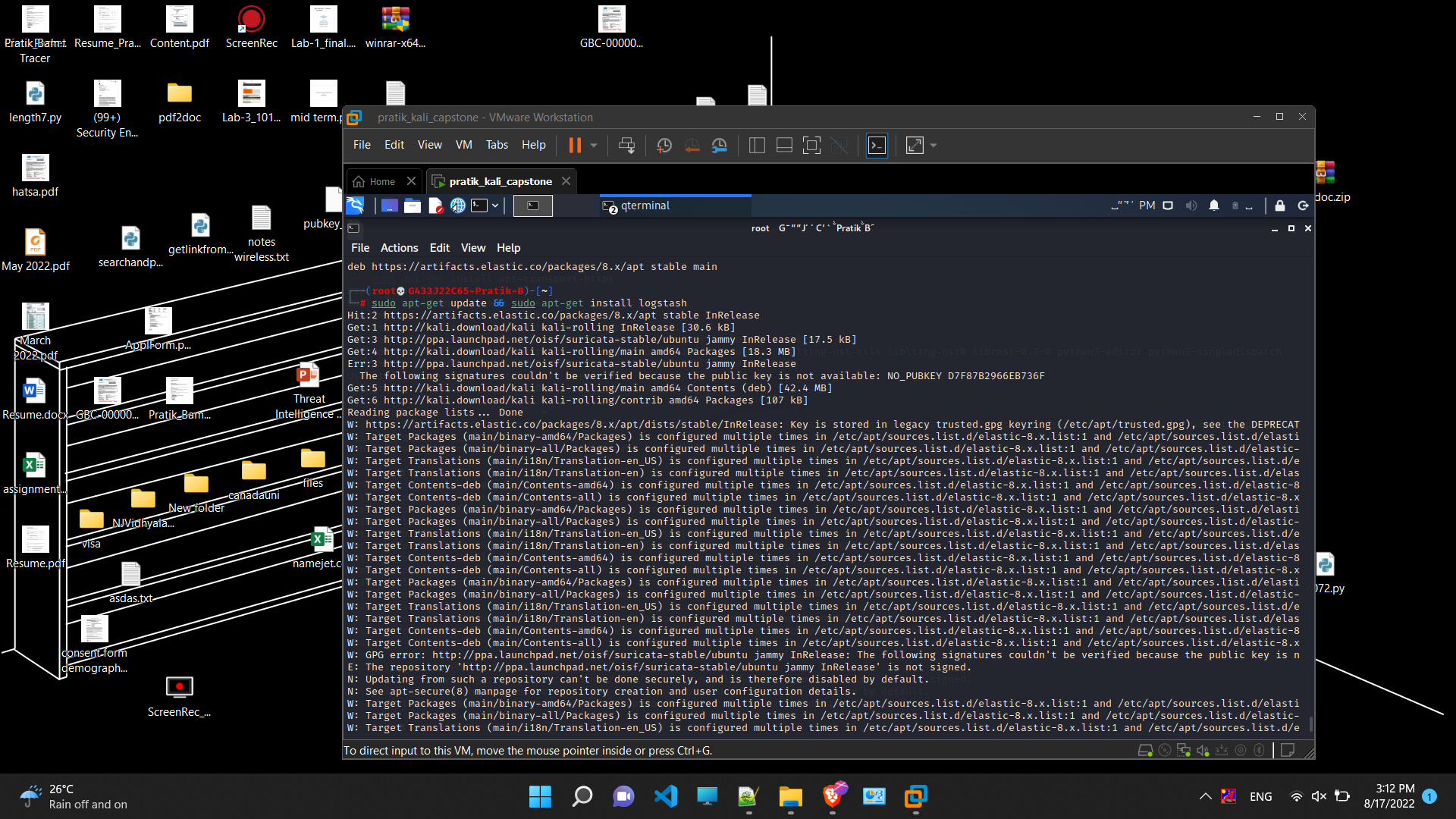


Configure and put the IP of logstash server, enable log, specify the path to /var/log/\*.log this will include all the log files



We will be view all the system logs

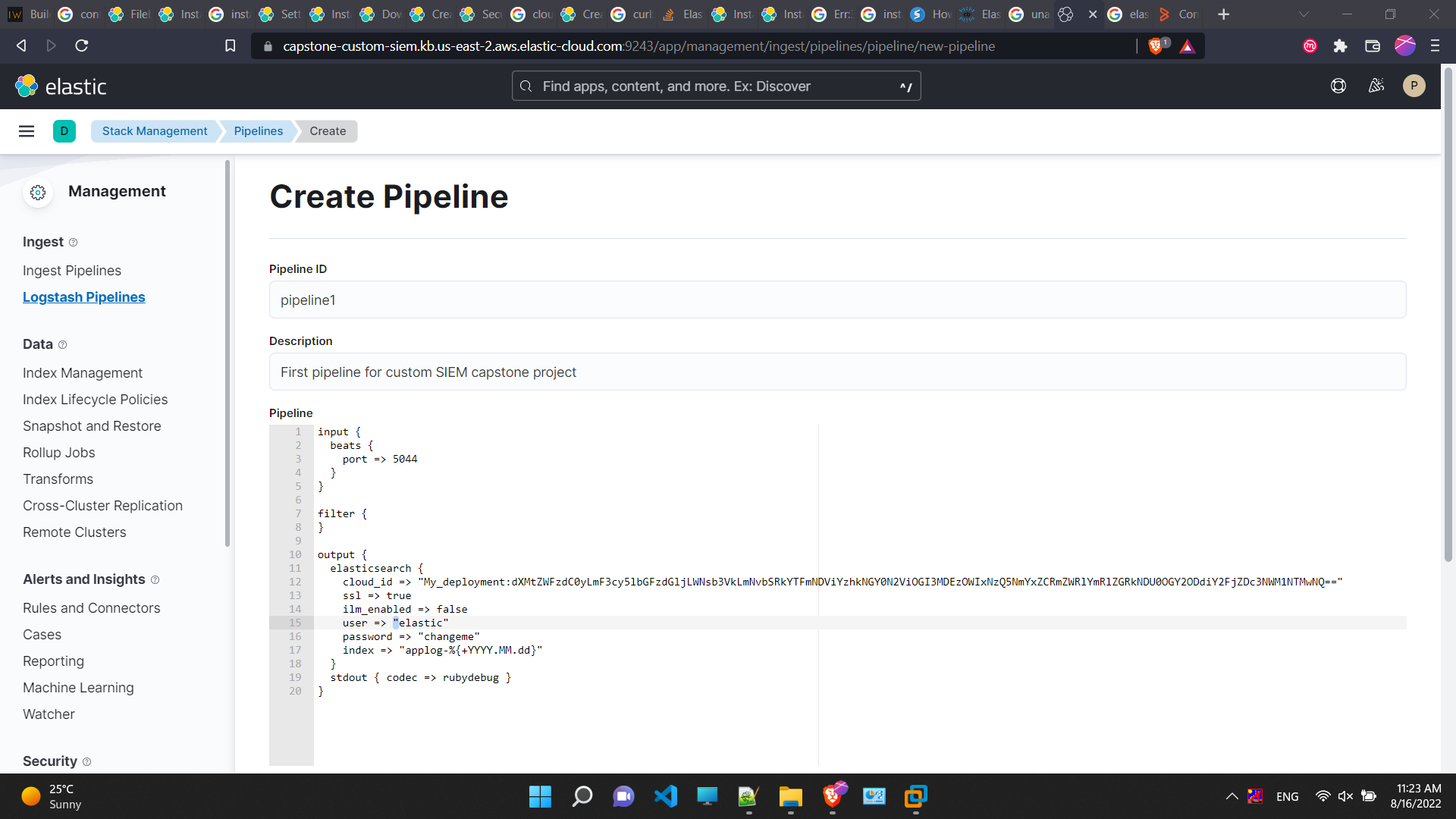
Install logstash



Put the cloud key in it so that it will push the aggregate logs to elastic search

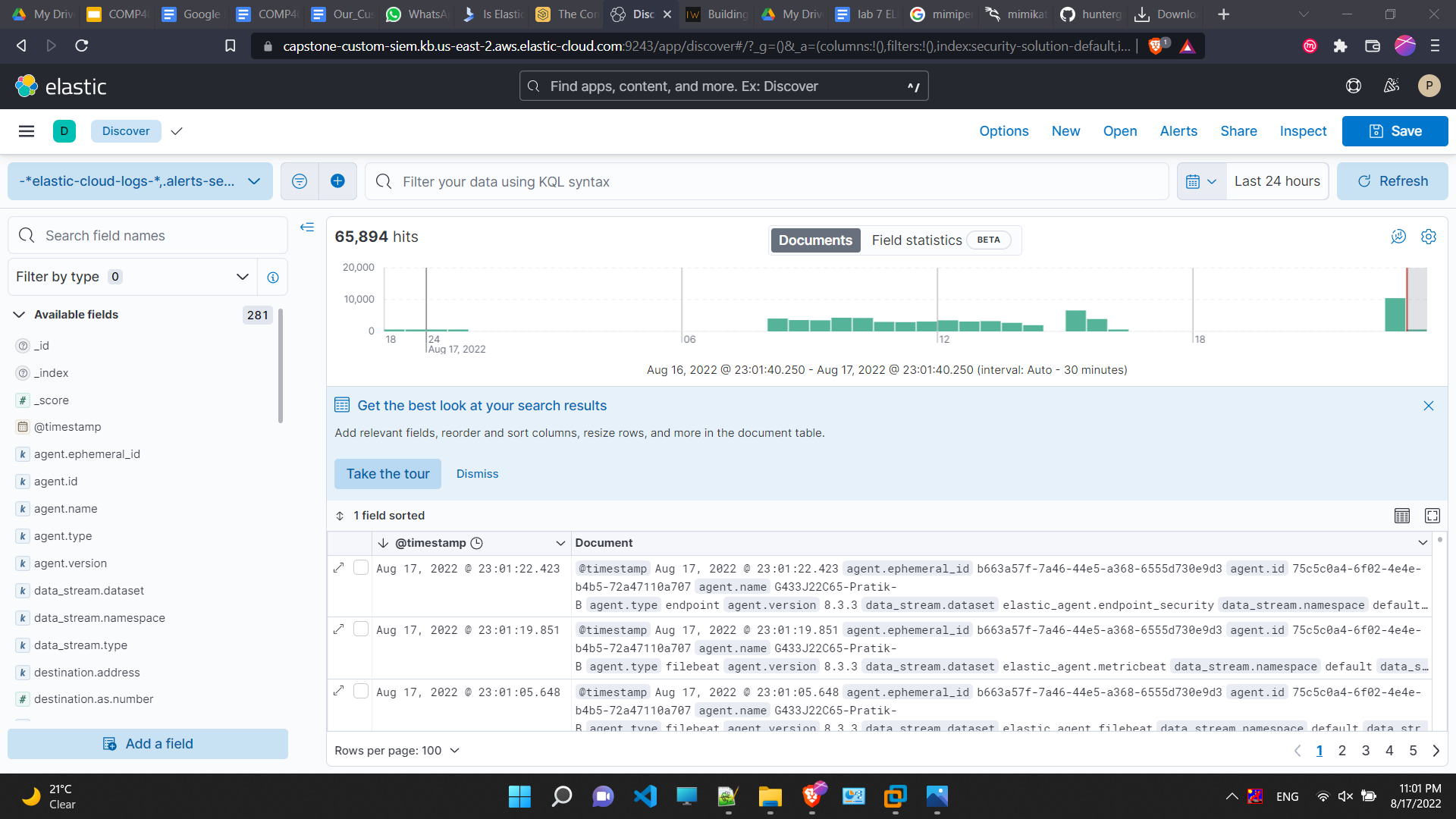
Now here we are using my VM as a logstash server

Configuration of pipeline, this will be added in logstash.yml file

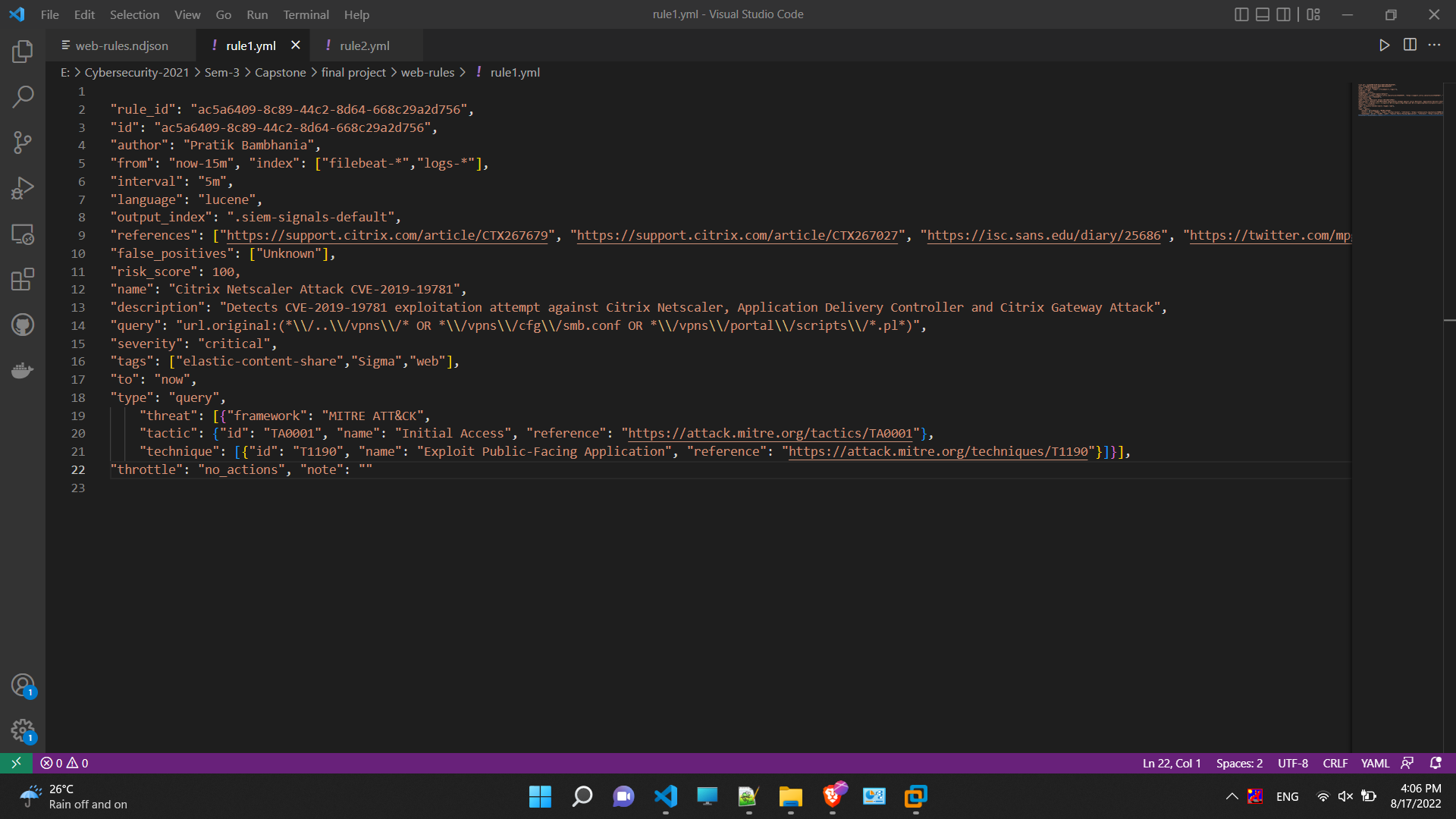


Once we have configured the logstash we are done with the configuration part and now the real part of our SIEM

Elastic search does gives us some way to see our logs



Write SIGMA rules and integrating it with our SIEM



Each of the rule has to be detailed and carefully written as it may lead to a false positive alert

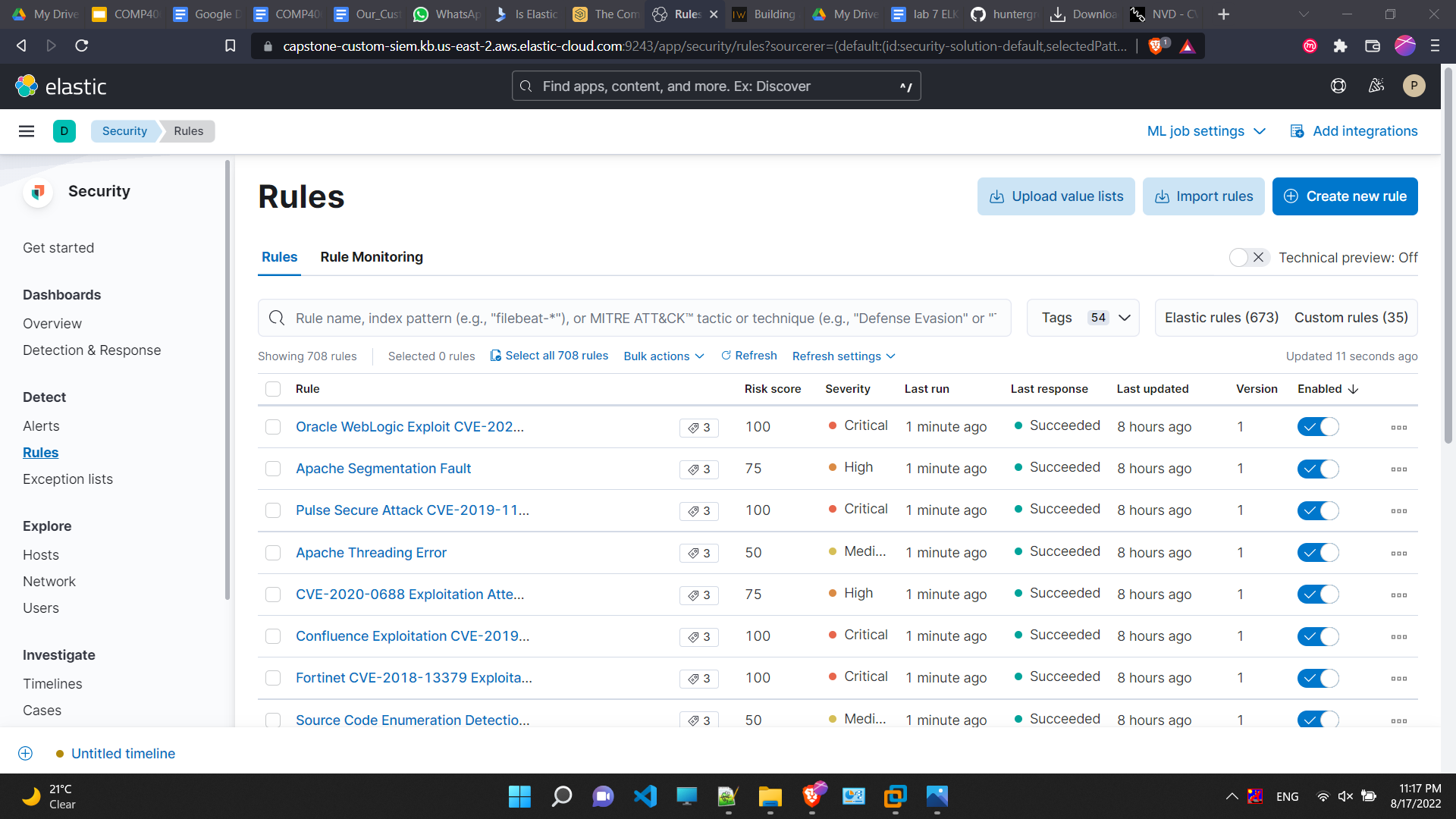
So how do you write SIGMA rules, for this we need to decide what vulnerability we need to write for

<https://nvd.nist.gov/vuln> is an excellent source to see vulnerability details

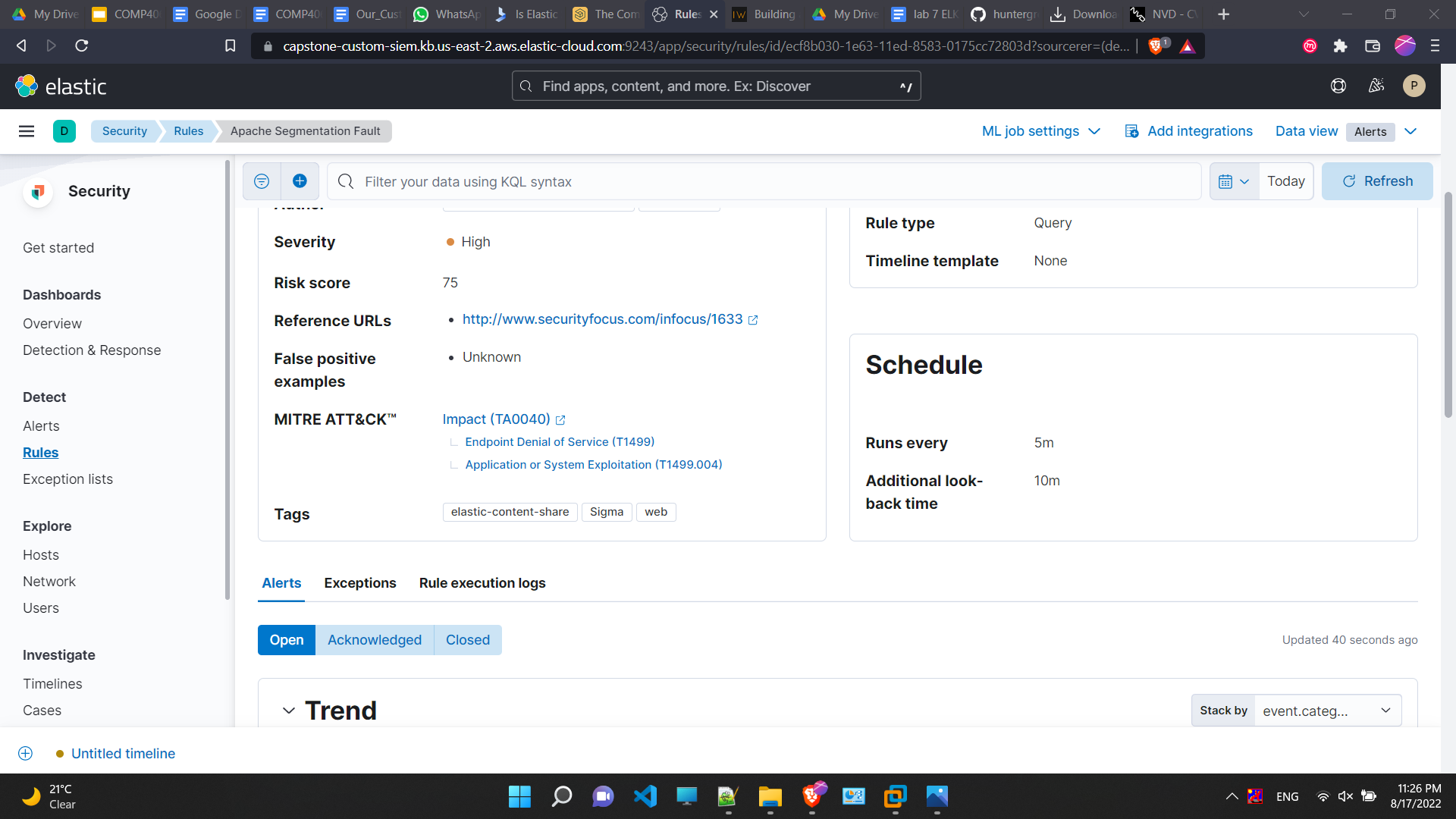
Here I have written rule for CVE- 2019-9670 which is a vulnerability when exploited gives attacker an initial access

SIGMA rules have sigmac tool which are use to transform rule for elastic search

Then we add to rule and add all the rules we have made

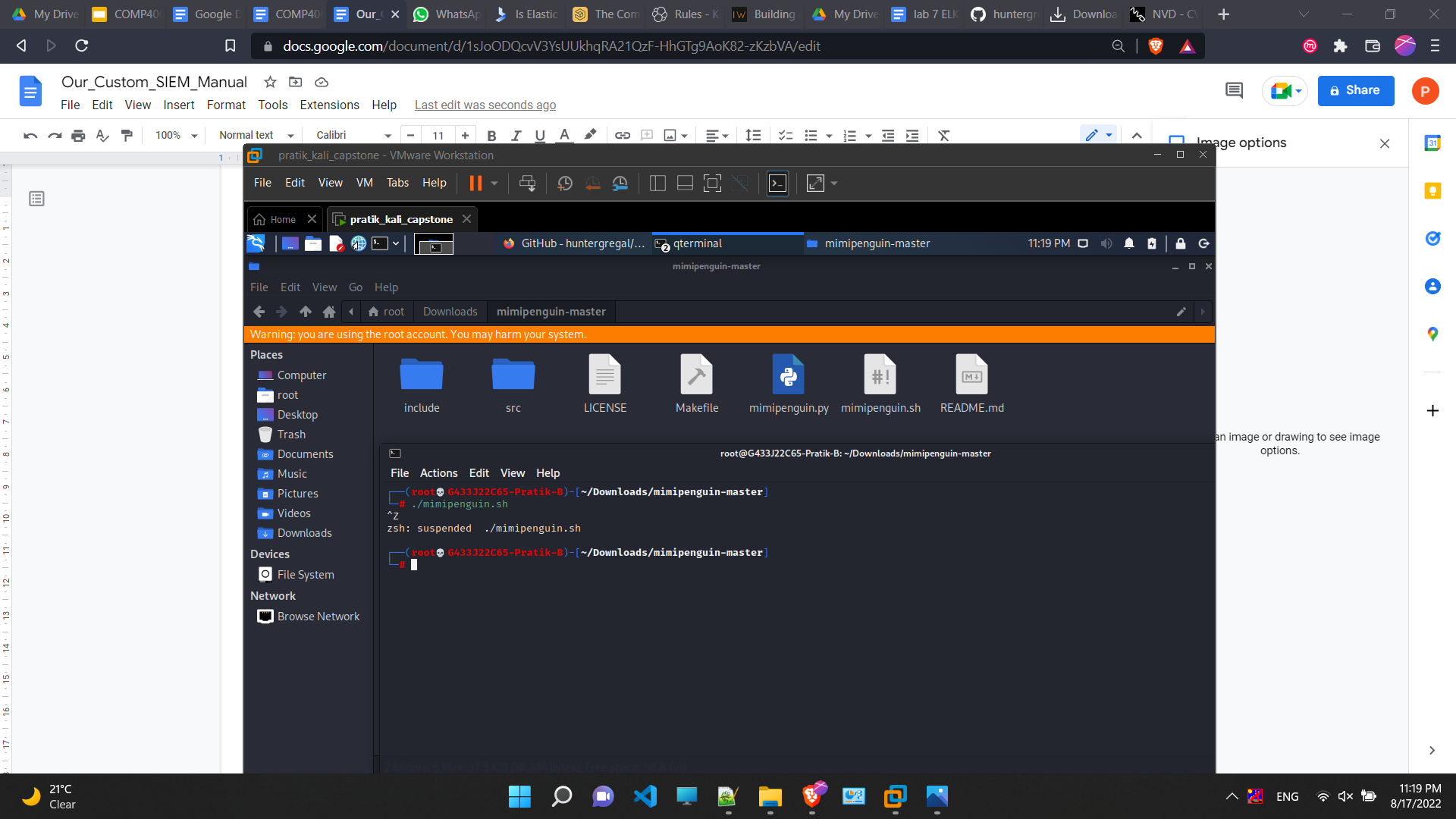


Some details on the rule



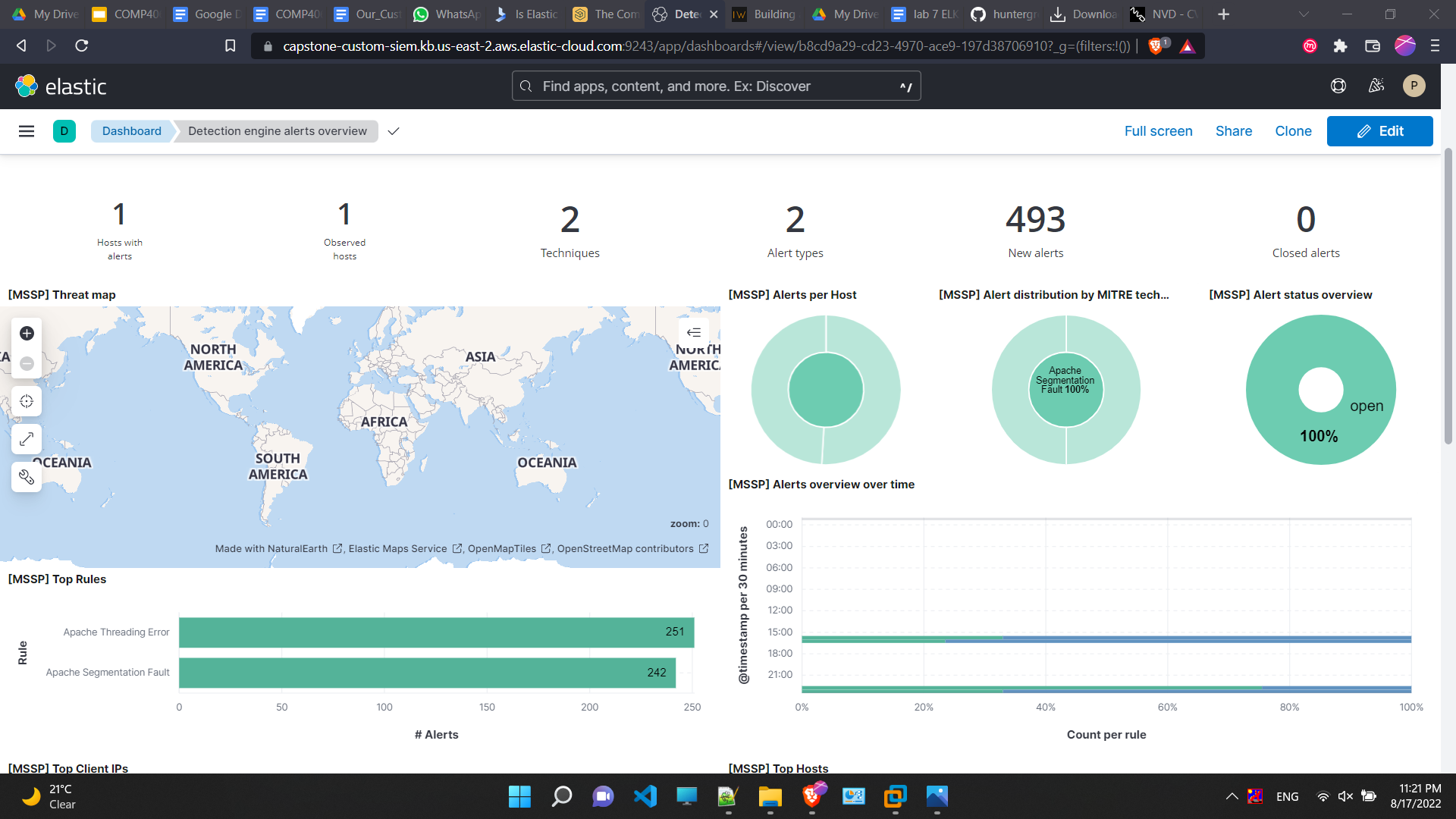
Now for testing we will use a mimipengin malware which if run on linux will extract password of plaintext

Download and run it

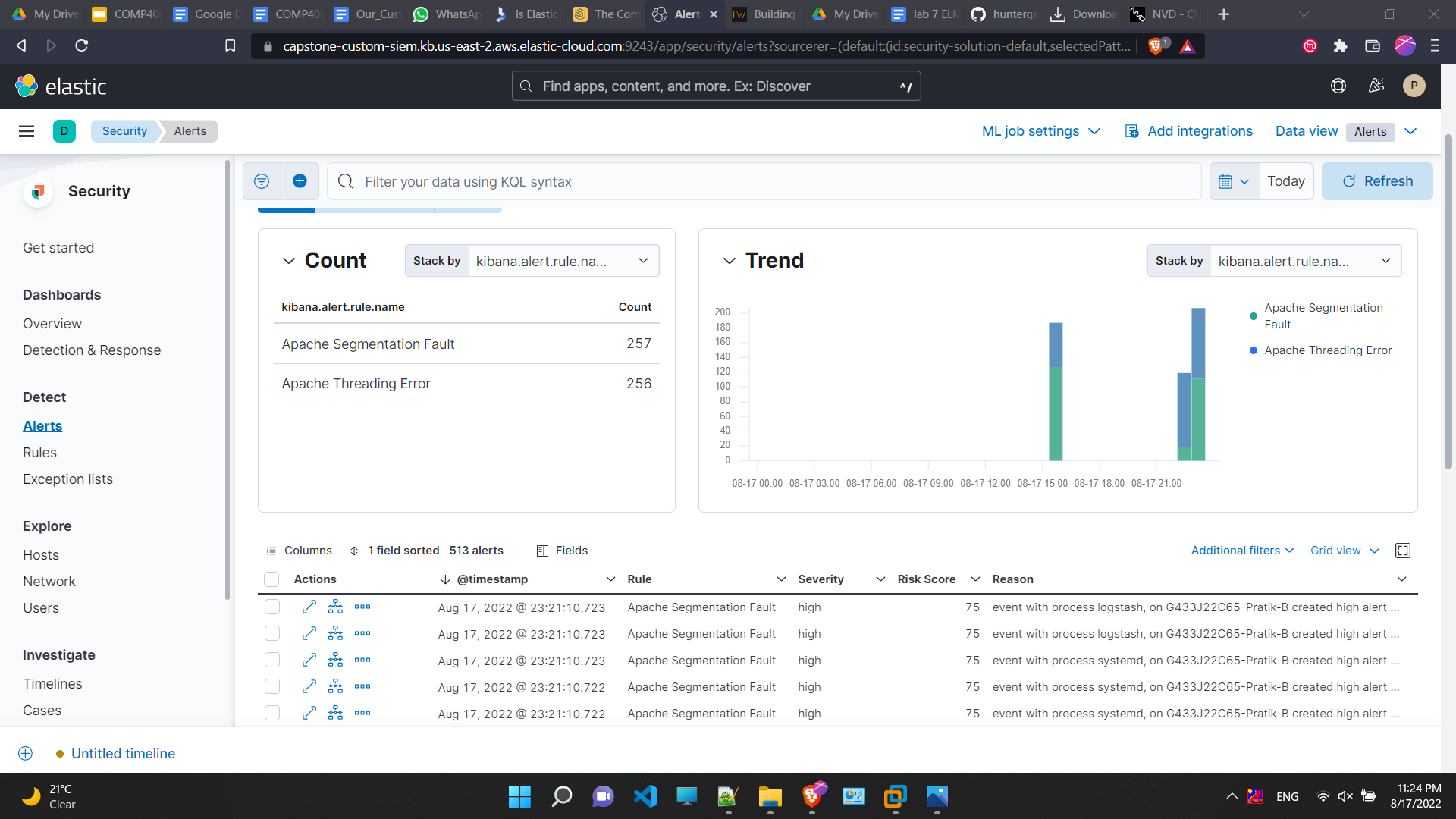


This dashboard are created by us and it will be part of SIEM

As you can see there are already 493 alerts generated , there was one apache segmentation sigma rule triggered which was shown earlier



Some more info on our alert generated



* + Appendix C – References
    - A full list of all sources used, with citations.
* <https://github.com/SigmaHQ/sigma>
* <https://www.elastic.co/>
* https://nvd.nist.gov/vuln/detail/CVE-2019-9670#VulnChangeHistorySection