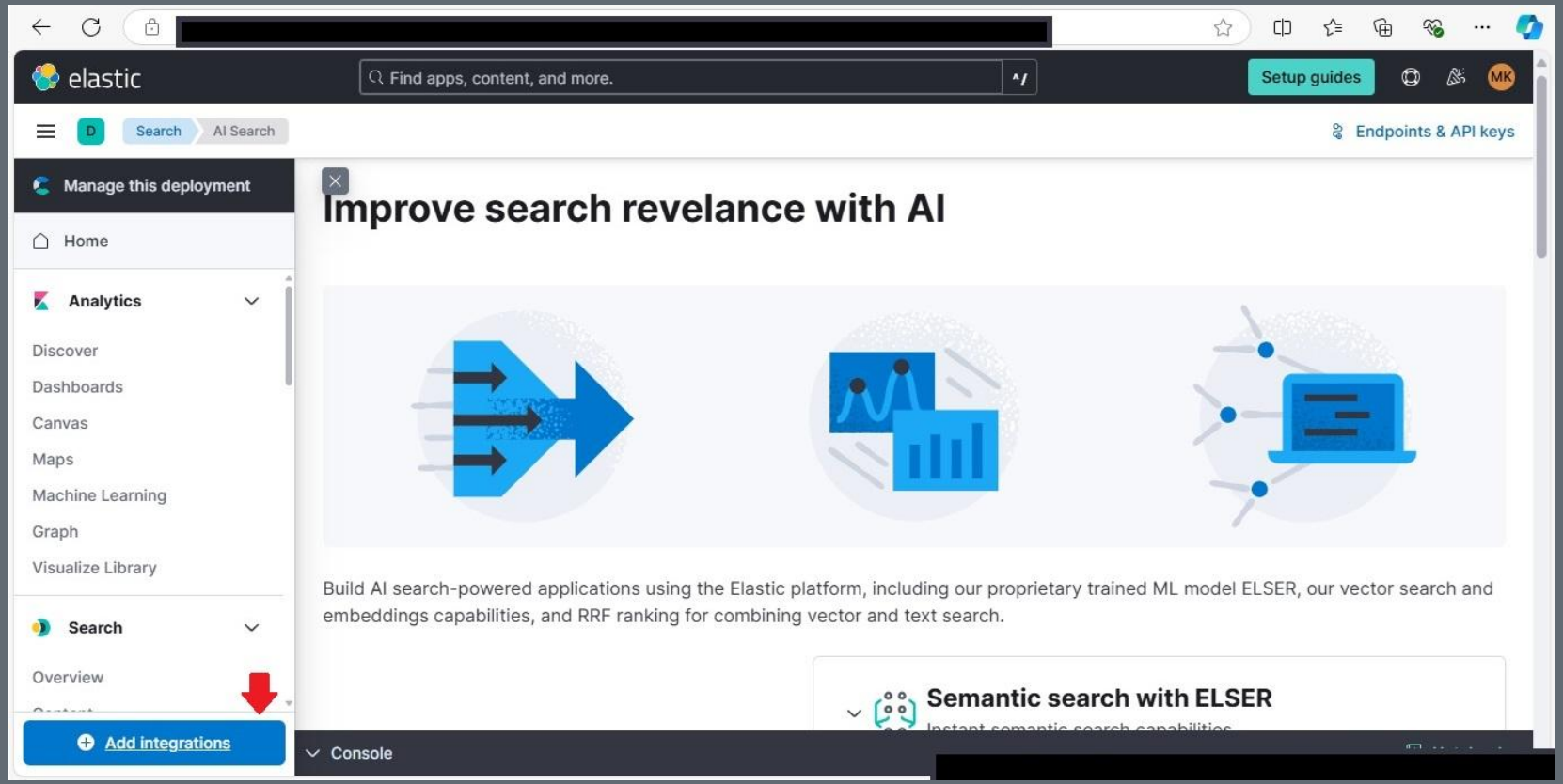
Building a SIEM in My Home Lab with Elastic

A Personal Project in Configuring a SIEM for Network Monitoring and Security by Miguel K.

Configuring Elastic SIEM for Network Security Monitoring

In this project, I configured Elastic Defender through the Windows terminal on my local device, creating a secure conduit within my home lab to send logs to the cloud. These logs are then accessible in my SIEM instance, where I can analyze thousands of events.

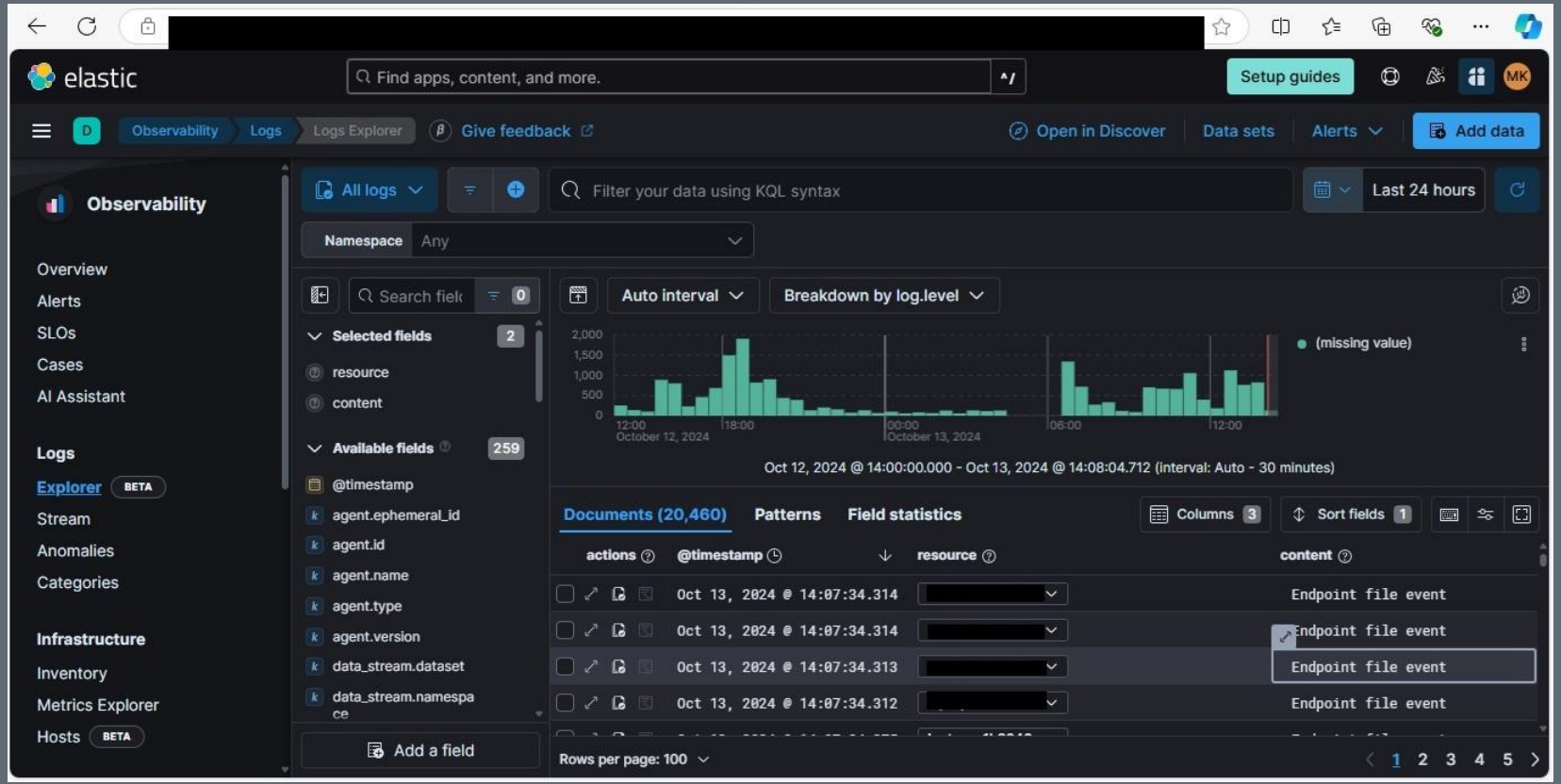
To demonstrate a practical use case, I created a rule that sends me an email alert whenever an Nmap scan is performe on my IP address. I successfully tested this by running an Nmap scan, and the SIEM sent the expected email alert, confirming that the rule was functioning as intended. This exemplifies how a SIEM can be effectively leveraged to enhance network protection.



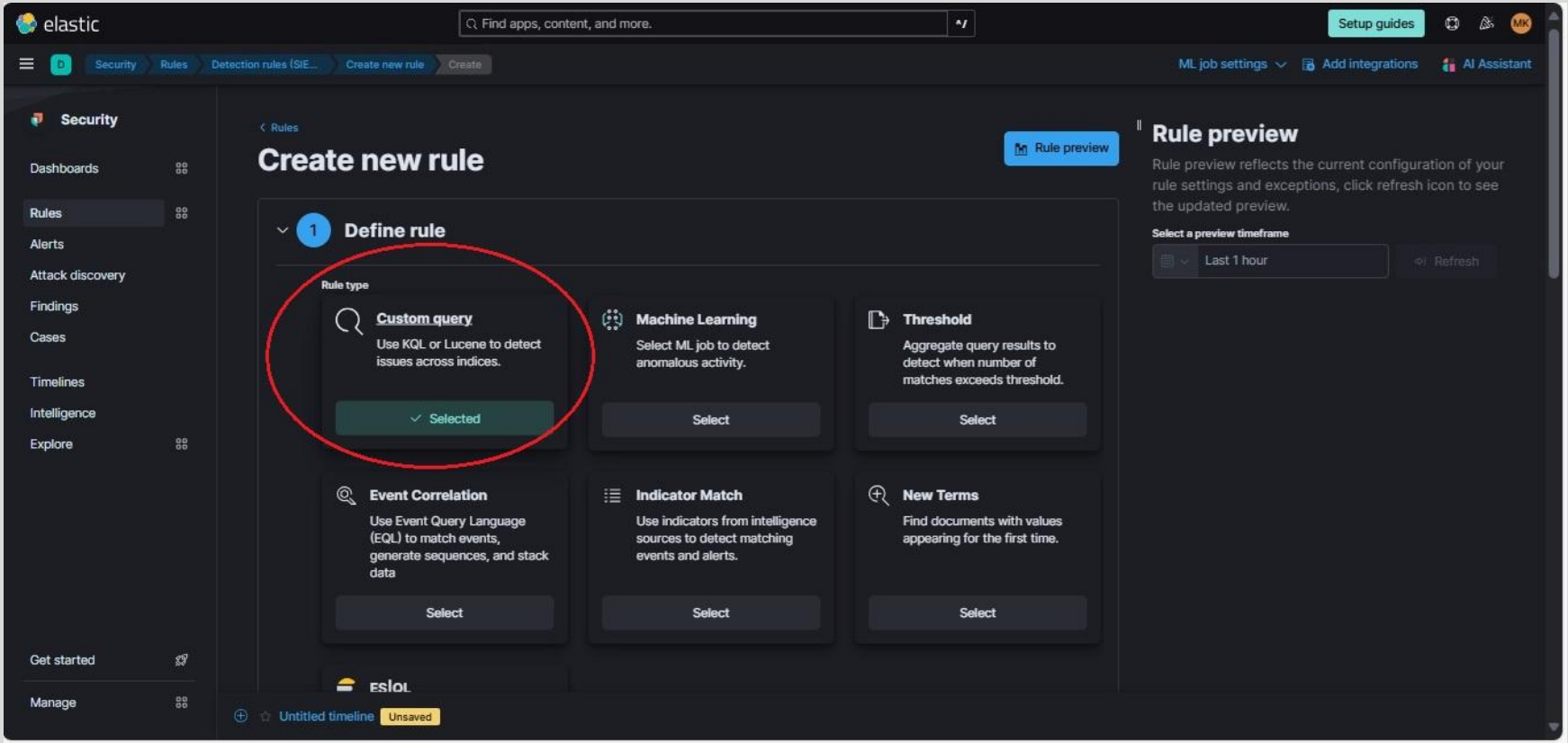
I accessed Elastic Cloud here to obtain the software necessary to build out the SIEM.

```
Administrator: Windows Powe

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> $ProgressPreference = 'SilentlyContinue'
PS C:\Users\Administrator> Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.15.2-windows-x86_64.zip
 -OutFile elastic-agent-8.15.2-windows-x86_64.zip
```

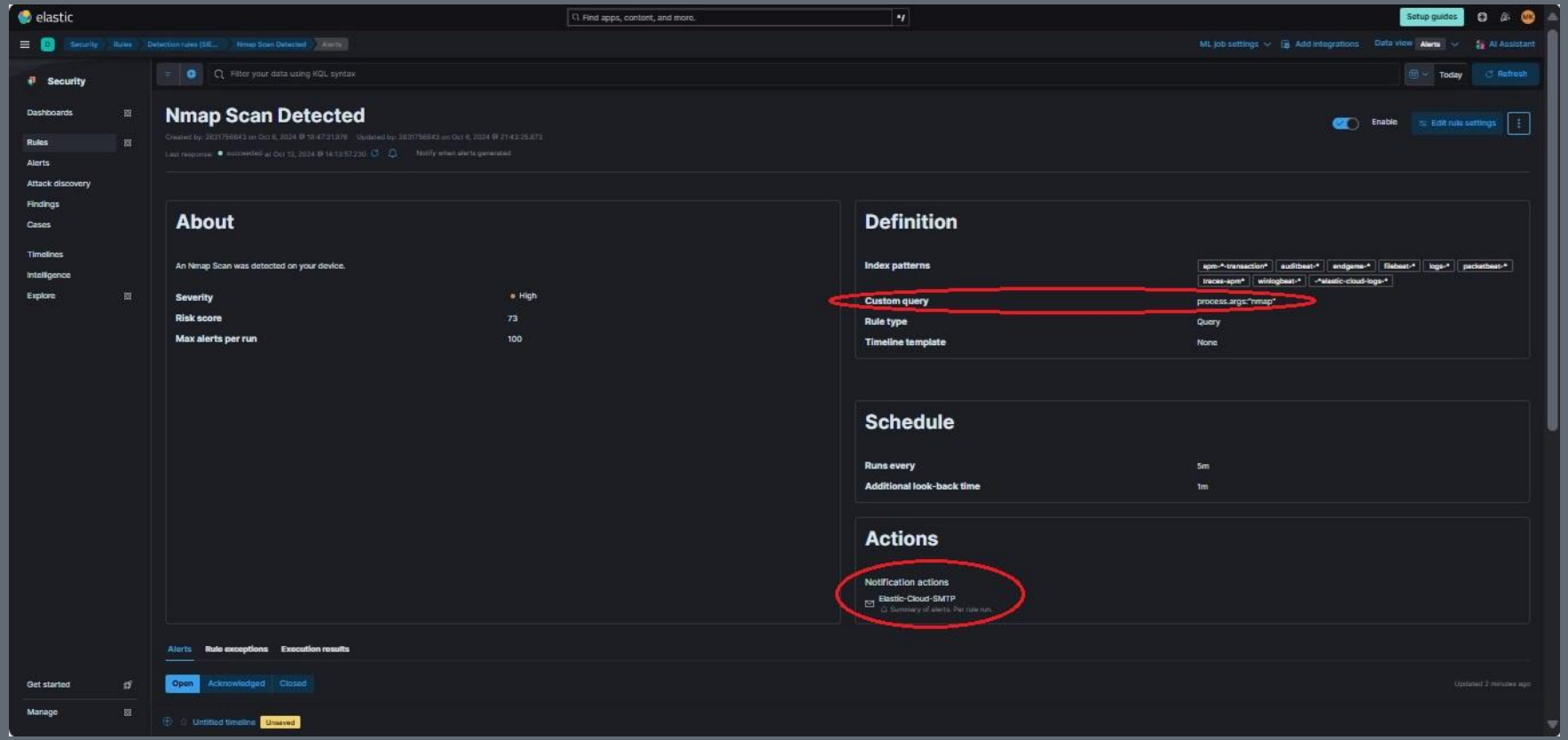
After adding the Elastic Defender integration, I configured Elastic to run on Windows by executing the command displayed in the image.



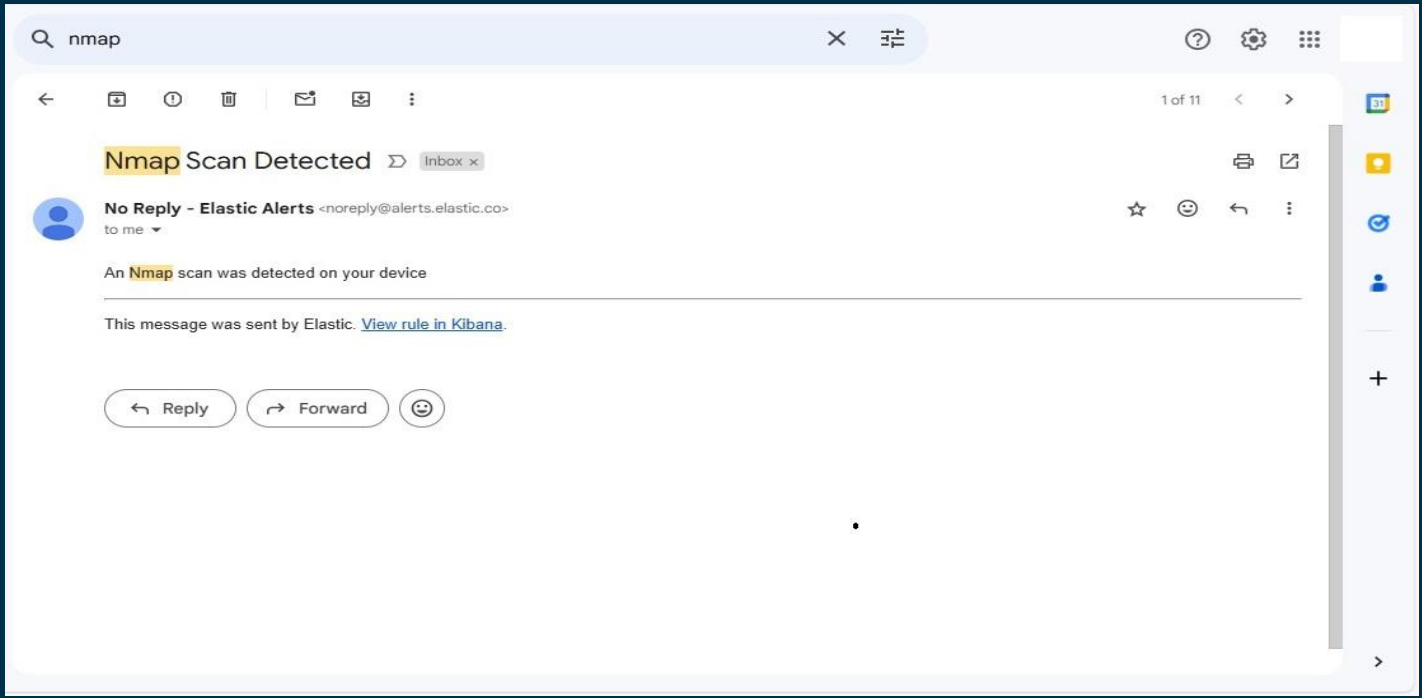
After configuration, the SIEM has begun collecting data. I can now utilize queries to search for specific information and sort and filter results according to my preferences.



I created a custom rule to illustrate how a SIEM can generate alerts in response to specified events.



I developed a custom query using `process.args: "nmap"`, designed to detect any logs associated with "nmap" on the system. Additionally, I configured the alert to be sent to my email whenever Nmap activity is detected.



After executing an Nmap scan on the system, I received an alert from the SIEM in accordance with the established rules. This successful alerting process highlights the effectiveness of the SIEM in monitoring and responding to network activities.

In conclusion, this project demonstrates how SIEMs serve as powerful tools for enhancing security monitoring by aggregating and analyzing log data to detect and respond to potential threats in real time.