Setting Up a Home Lab for Elastic SIEM: A Step-by-Step Guide

Christopher Elce · Follow
6 min read · Oct 15, 2023

In this comprehensive guide, I'll walk you through the process of creating your own Elastic Stack Security Information and Event Management (SIEM) home lab using the Elastic Web portal and a Kali Linux virtual machine (VM). By the end of this project, you'll be able to generate and analyze security events, set up agents for log forwarding, create dashboards, and establish security alerts. This hands-on experience is not only a great addition to your cyber security skillsets but also a valuable talking point for job interviews.

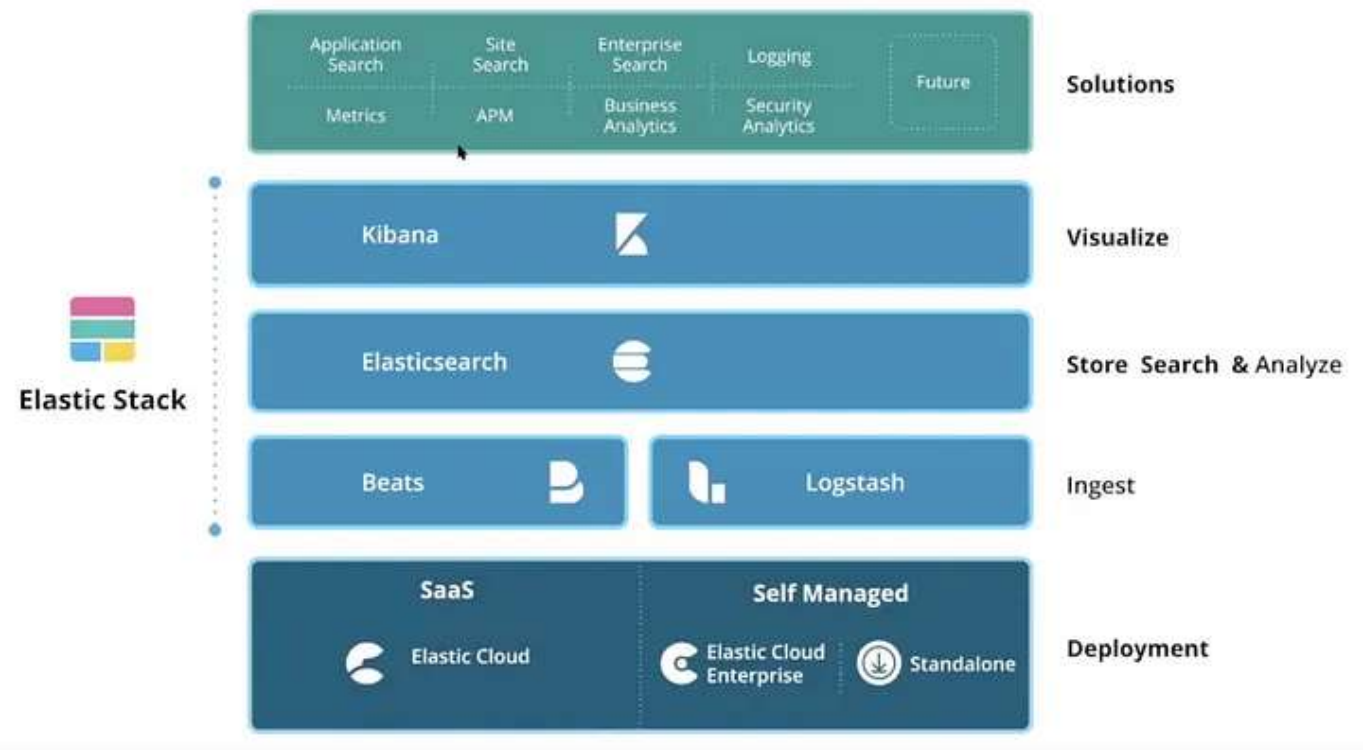
(Photo by Christin Hume on Unsplash)

Before getting started, it's important to understand structurally *what* Elastic Stack is and *why* it's important when compared to similar alternative tools, like Splunk. (At the end of the day, you and your employer will use whatever tool(s) are required based on business use cases).

The Elastic Stack, previously known as ELK, comprises four integral elements:

- Elasticsearch, the search engine and analytics platform
- Logstash, the data processing conduit
- Kibana, the data visualization tool

- Beats, a recent integration (this post won't go over beats, but worth checking out)



The Elastic Stack architecture

When implemented effectively, these elements create a formidable framework tailored for navigating and managing scalable datasets in real-time. The business world frequently adopts the Elastic/ELK stack to:

- Conduct thorough log analysis
- Perform live analytics
- Tackle challenges that demand exploration, analysis, and visualizations of boatloads of data.

Roll Up Your InfoSec Sleeves & Let's Get Started...

Prerequisites:

- VirtualBox or VMware (note that VMware is used in this guide)
- Basic knowledge of Linux and virtualization software

Step 1: Set up a free trial Elastic Account

- Create a free Elastic account.
- Log in to the Elastic Cloud console.
- Start a free trial, create an Elasticsearch deployment, and choose your region and deployment size.
- Install and enable Elastic prebuilt rules

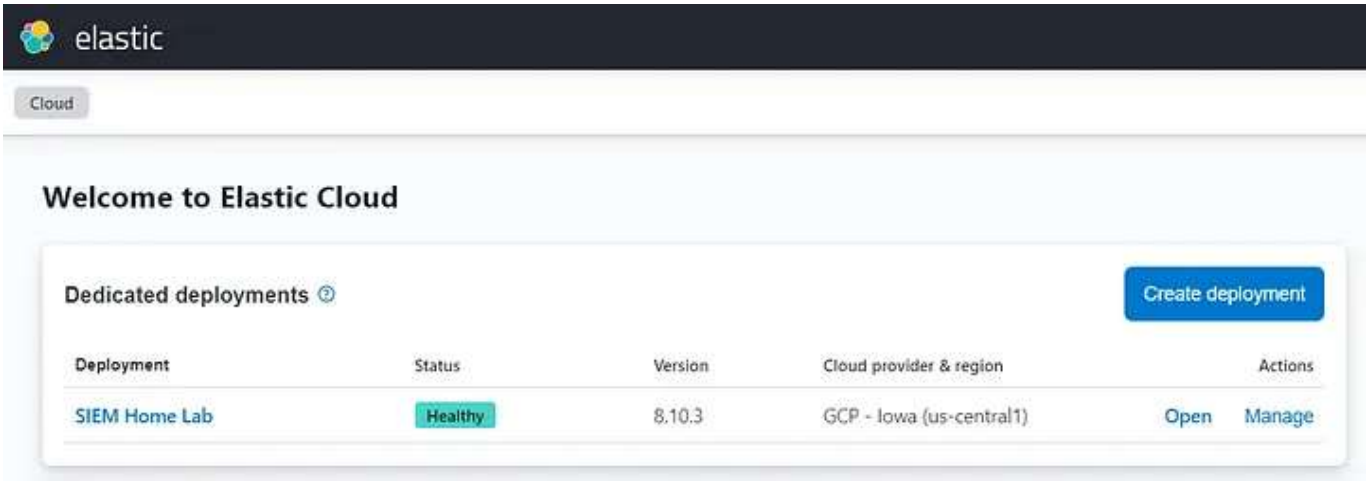
Step 2: Setting up the Linux VM

- Download the Kali Linux VM from the official website.
- Set up a new VM with the Kali VM file using your preferred virtualization platform (e.g., VirtualBox or VMware). If you're stuck on how to do this, read the Kali Linux documentation and look on Google or YouTube.
- Complete the Kali Linux installation and log in with both the default username and default password as *kali*

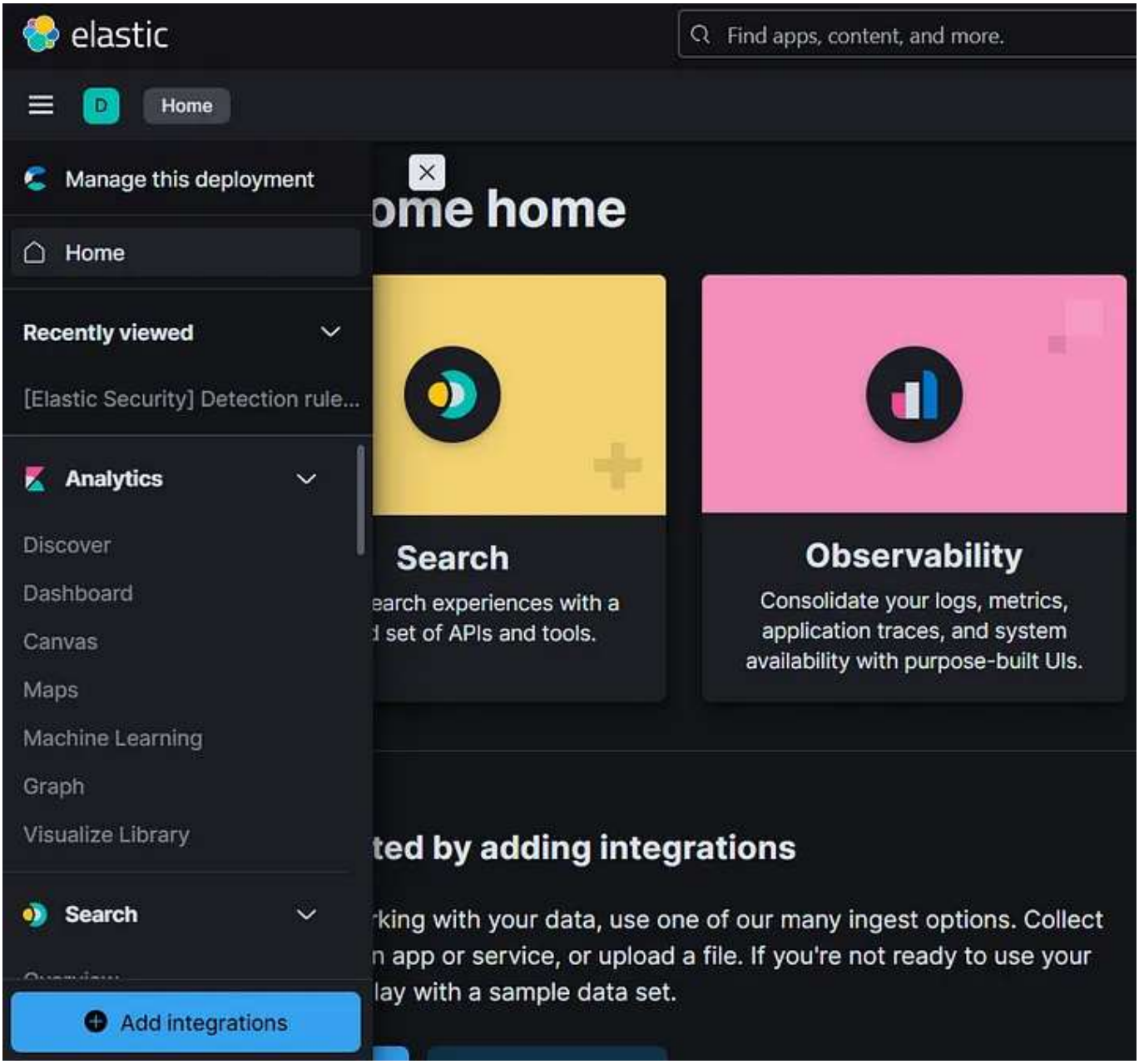
Step 3: Setting up the Agent to Collect Logs

- Learn about the role of agents in Elastic SIEM.

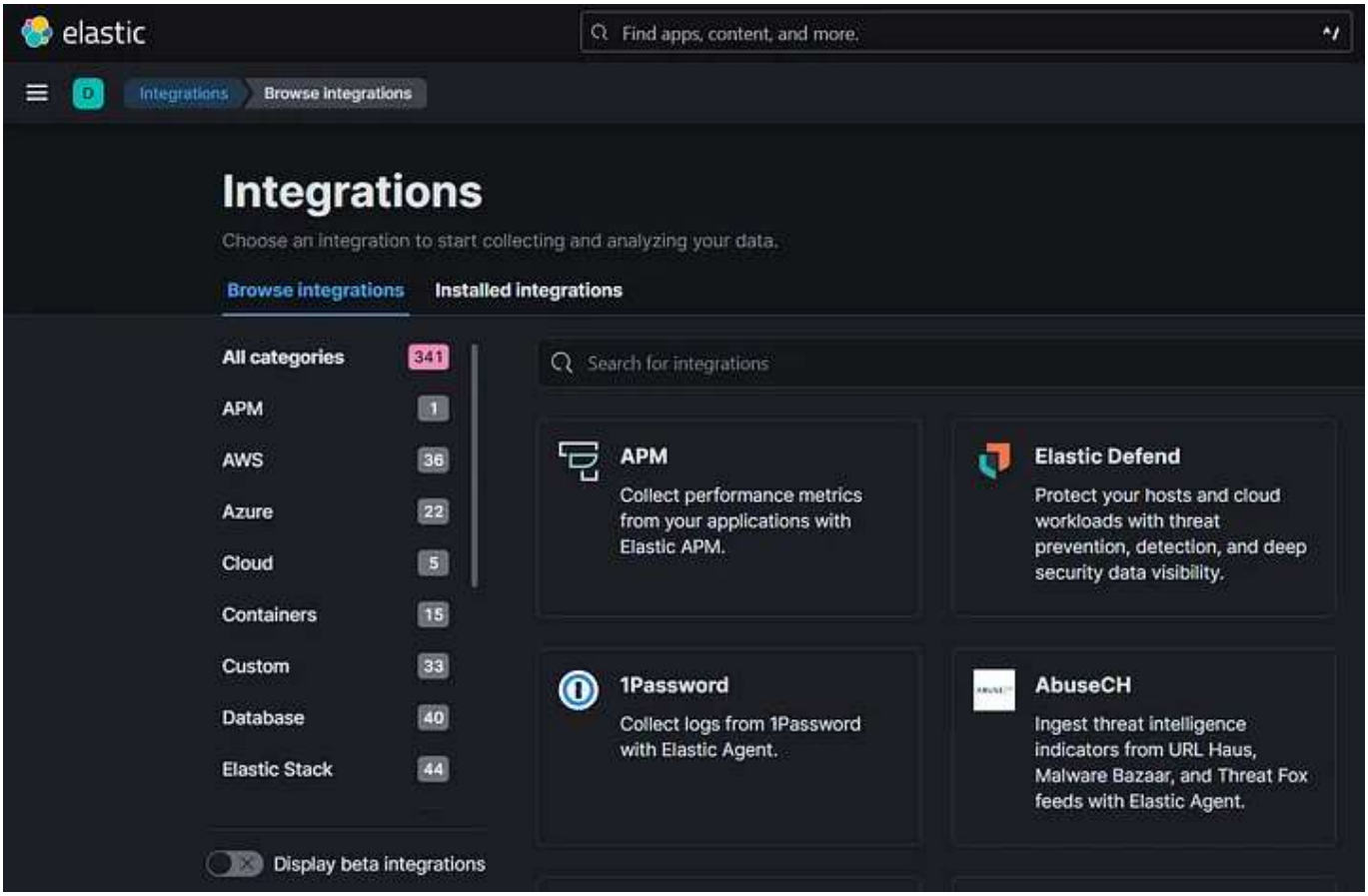
- Install the agent on your Kali VM by following steps provided on Elastic's blog post. Here's some helpful visuals…



Elastic Deployment successfully setup



Click on “Add integrations” on the bottom left.



Click on “Elastic Defend” and follow the instructions to install the Elastic agent on your Kali VM in your Kali terminal.

Verify that the agent successfully downloaded with the terminal command **sudo systemctl status elastic-agent.service**

Step 4: Generating Security Events on the Kali VM using Nmap

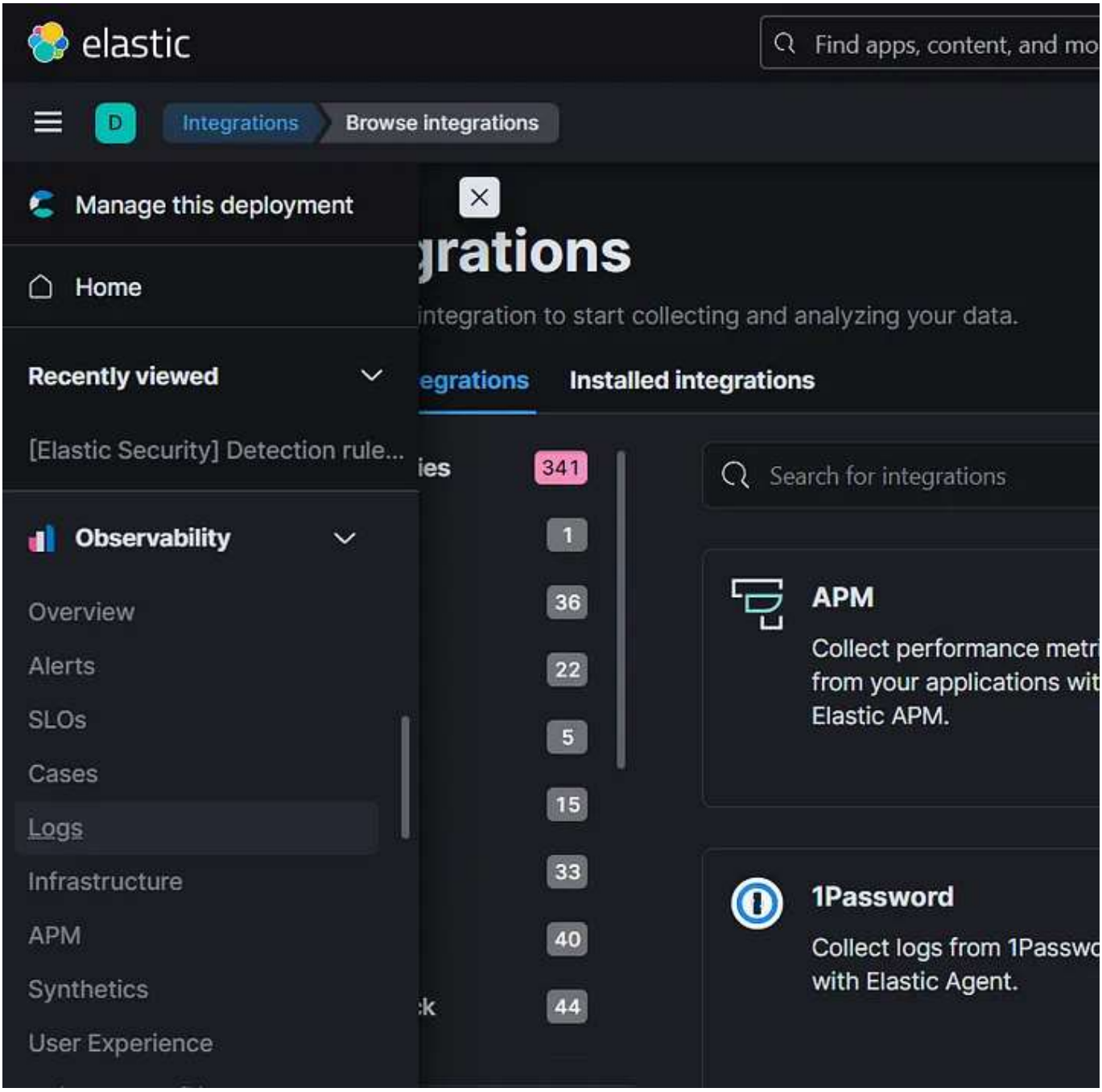
- Install Nmap on the Linux VM (if not using Kali).
- **Important Note: Use Nmap responsibly and know what that fully means before proceeding further**. If you are unfamiliar with Nmap and its legal implications, here is a good place start. Remember, with great cyber power comes great responsibility.
- Run some Nmap scans on your Kali VM's IP address to generate security events in Elastic.


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.189.128
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-15 00:21 EDT
Nmap scan report for 192.168.189.128
Host is up (0.000011s latency).
All 1000 scanned ports on 192.168.189.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.189.128
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-15 00:22 EDT
Nmap scan report for 192.168.189.128
Host is up (0.000011s latency).
All 1000 scanned ports on 192.168.189.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.189.128
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-15 00:23 EDT
Nmap scan report for 192.168.189.128
Host is up (0.00032s latency).
All 1000 scanned ports on 192.168.189.128 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- 192.168.189.128
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-15 00:23 EDT
Nmap scan report for 192.168.189.128
Host is up (0.0000070s latency).
All 65535 scanned ports on 192.168.189.128 are in ignored states.
Not shown: 65535 closed tcp ports (reset)
```

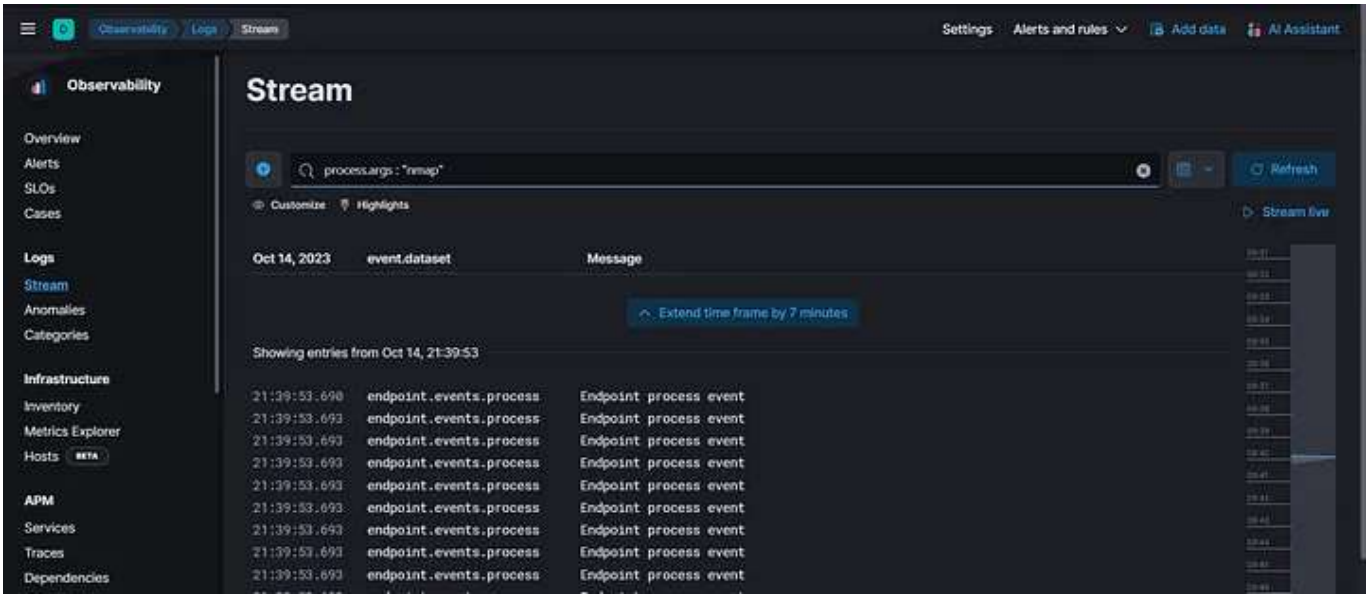
Remember, make sure to run Nmap scans on **your Kali VM's IP address**.

Step 5: Querying for Security Events in the Elastic SIEM

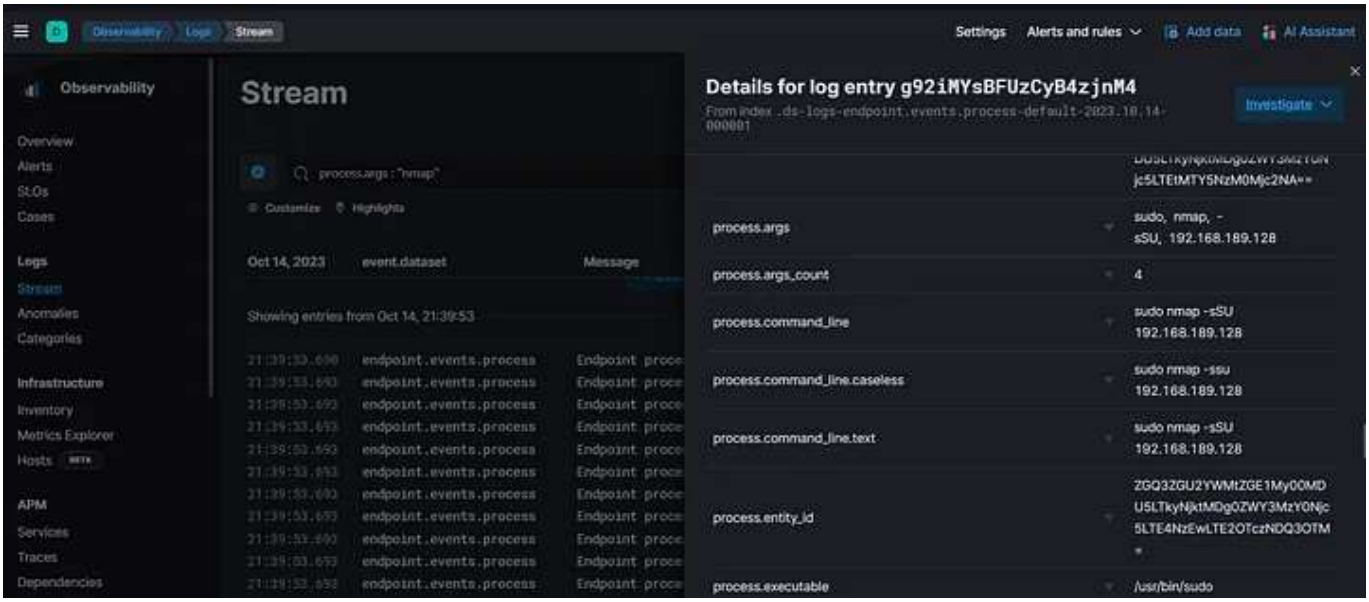
- Learn how to query and analyze logs in Elastic SIEM.
- Search for specific security events using Elastic's web interface.



Within your Elastic Deployment, click the menu icon (three horizontal lines at the top left) and then click on "Logs" tab under "Observability".



You should now see log events from you Kali VM. In the search bar under “Stream” type in **process.args: “nmap”** to display the Nmap events created on your Kali VM. Congratulations, you are now learning how to use KQL to filter data in your SIEM!



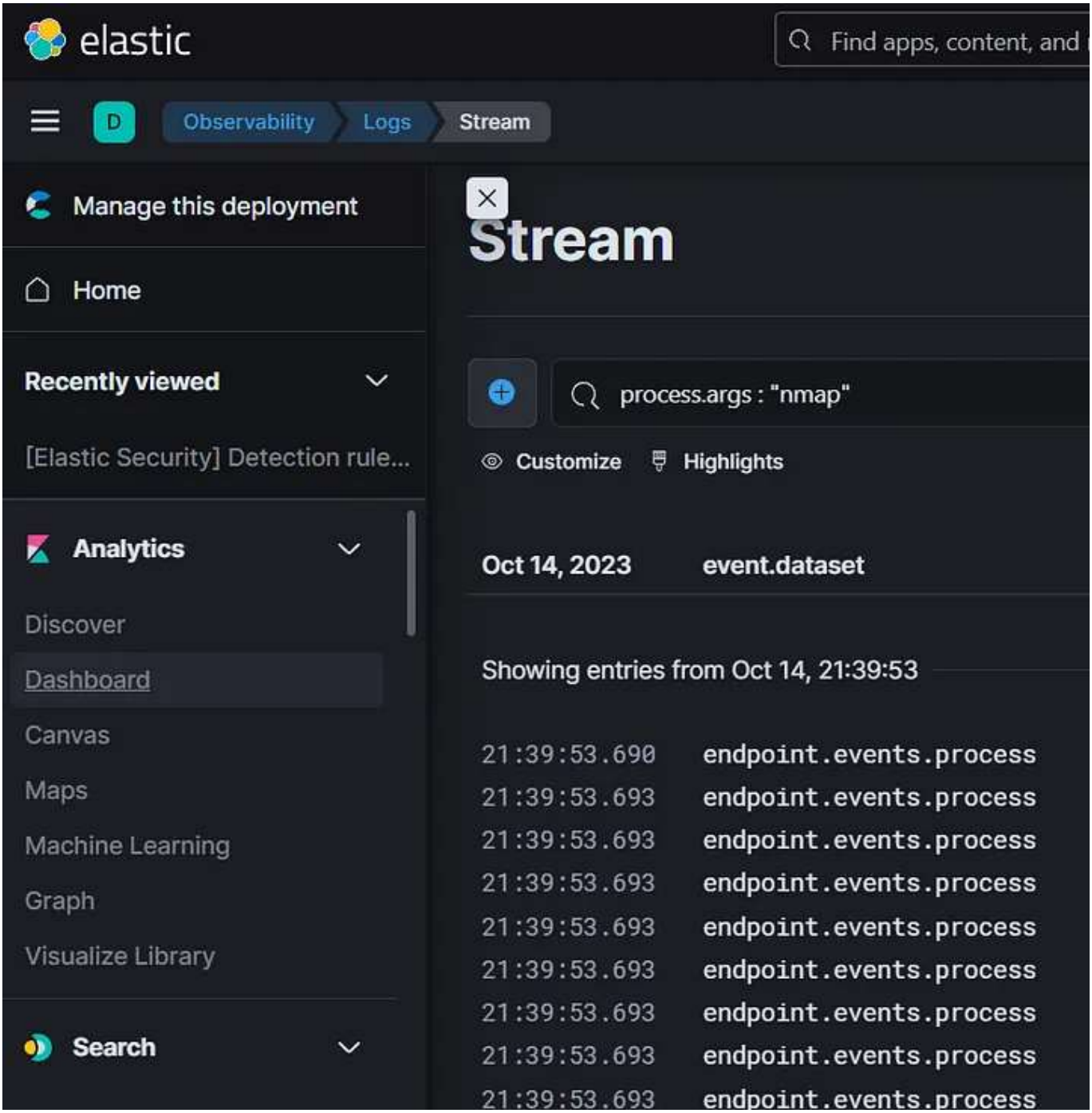
Hover over any of your listed Nmap events. Click on the three dots to the right of the event to view the event’s details. In this particular example, an Nmap UDP scan was detected. Your Nmap event details will most likely differ and that’s OK!

Analyzing diverse security events in Elastic SIEM provides valuable insights into real-world security incident detection, investigation, and response procedures. Try opening different applications or create other events on your Kali VM and see if you can spot them in Elastic. Doing this will

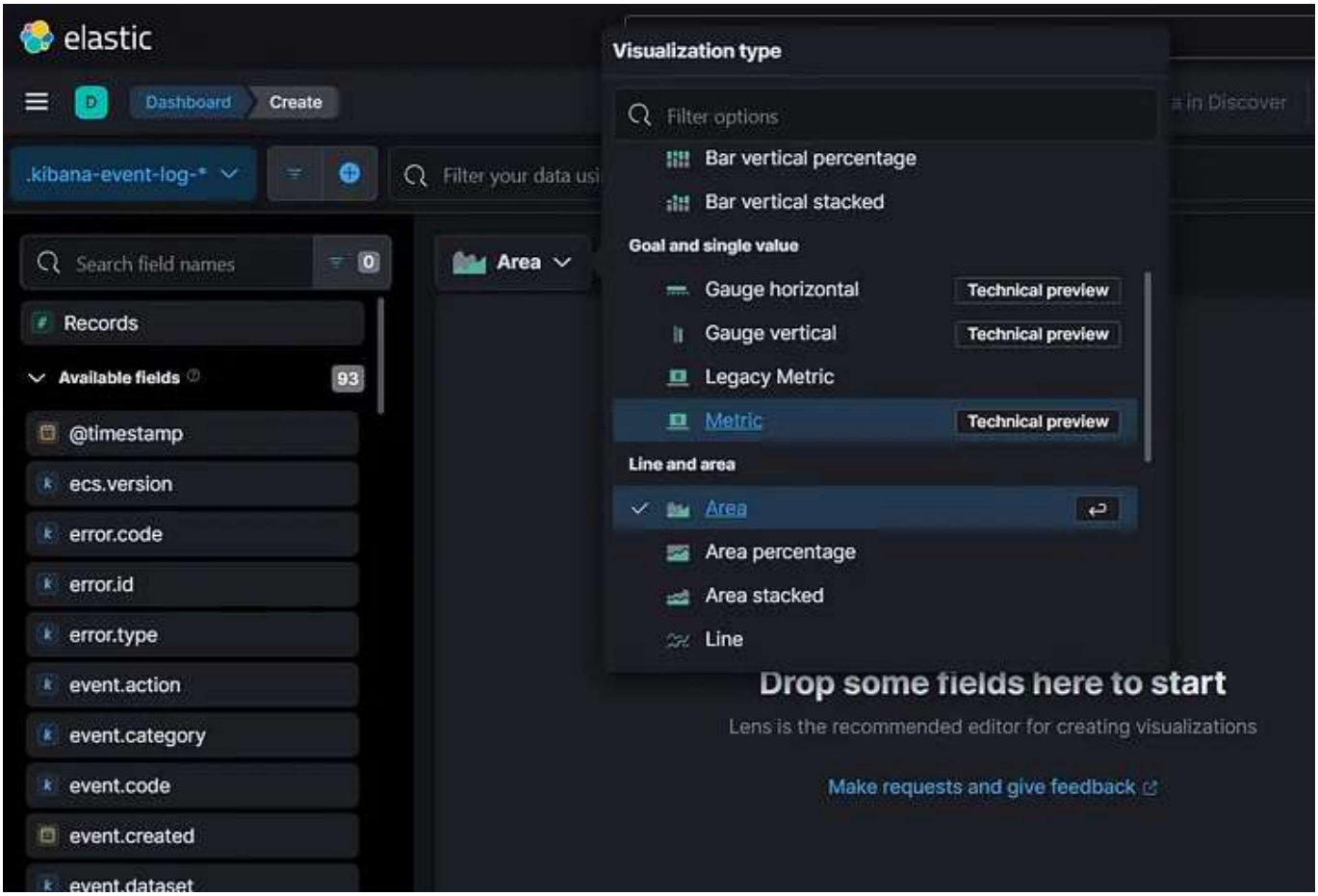
reinforce your understanding of Kali, Linux terminal commands, and how to better spot true positive and false positive security events in your SIEM.

Step 6: Create a Dashboard to Visualize the Events

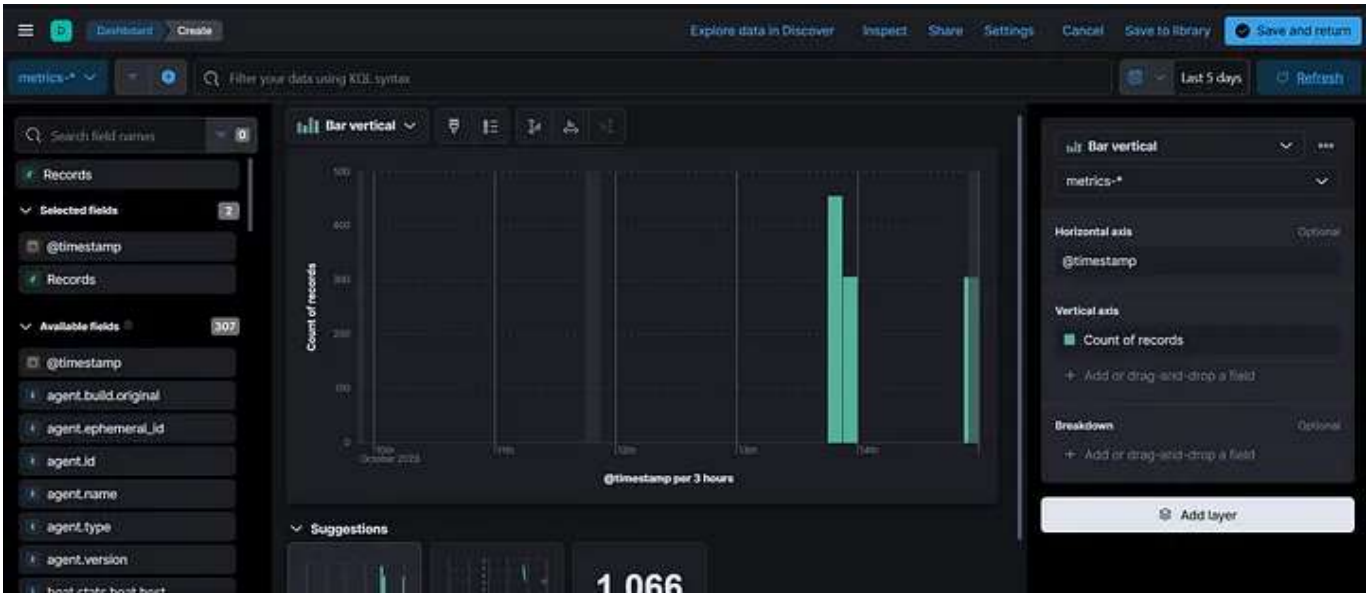
- Explore how to use visualizations and dashboards to analyze event logs.
- Create a simple dashboard to visualize the count of security events over time. Knowing how to do this is a very important skill to have for communicating cyber security to decision makers and stakeholders in your company! A lot of your daily tasks will involve composing reports along with using communication and collaboration soft skills.



Click on “Dashboard” under “Analytics” in the menu. Next, click on “Create dashboard” at the top right to create a new dashboard. Then, click on “Create Visualization” to add a new visualization to the dashboard.



Pick a visualization display type by choosing “Area”, “Line”, or “Bar vertical” (the author picked this one). Doing so will create a chart that shows the count of events over time.

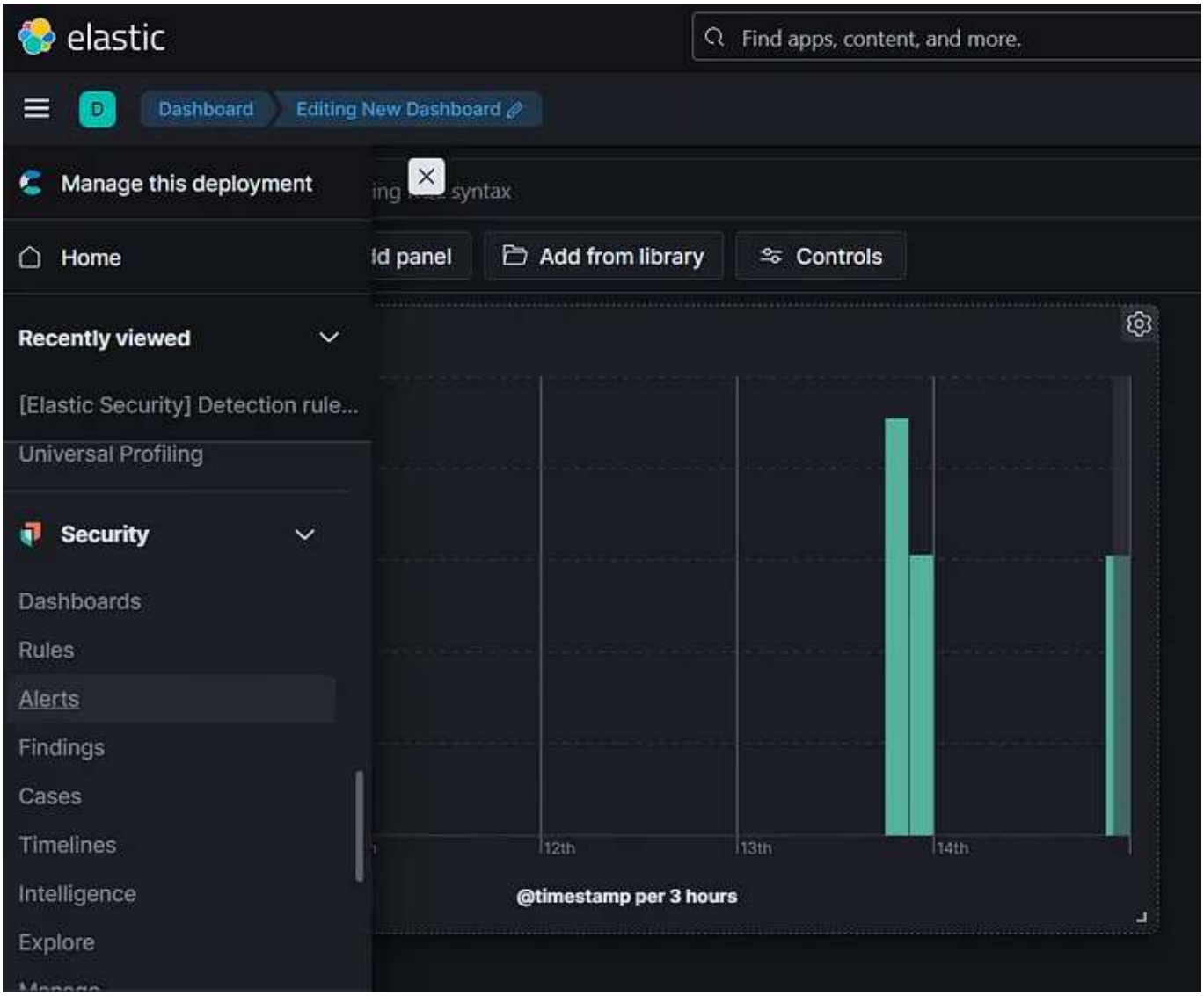


Setup the parameters for the visualization with those indicated on the right in this example. Click on the “Save” button at the top right.

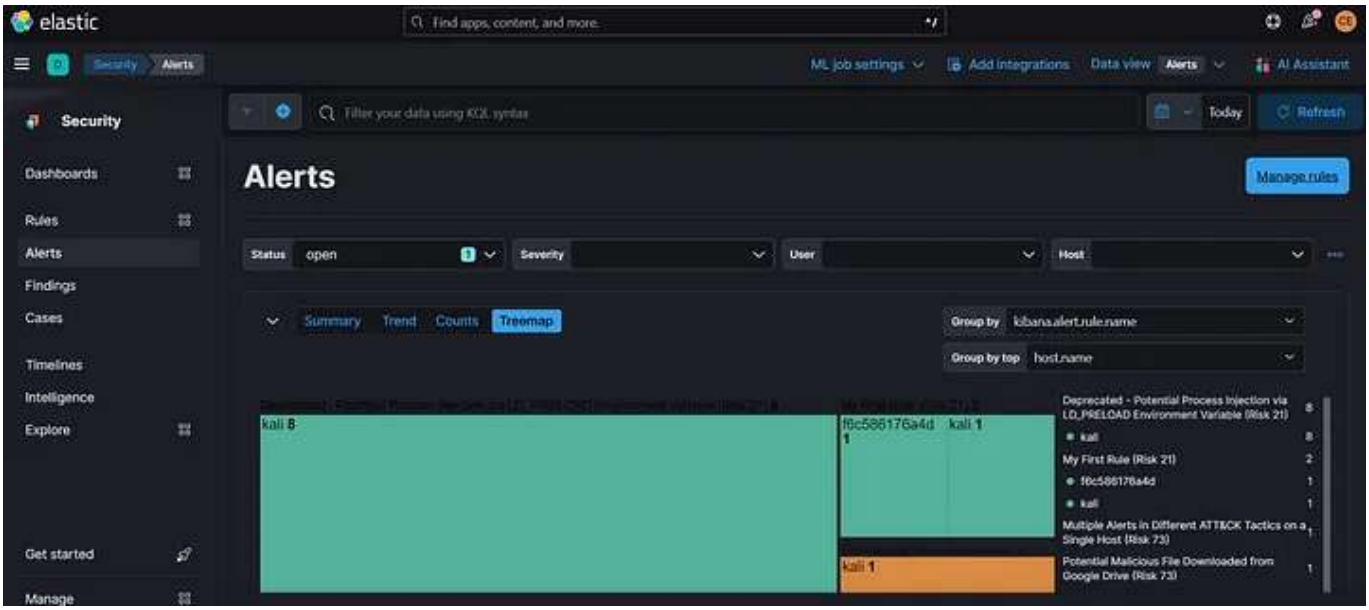
Step 7: Create an Alert

- Discover the importance of alerts in SIEM.
- Create an alert in Elastic SIEM to detect Nmap scans based on custom queries.

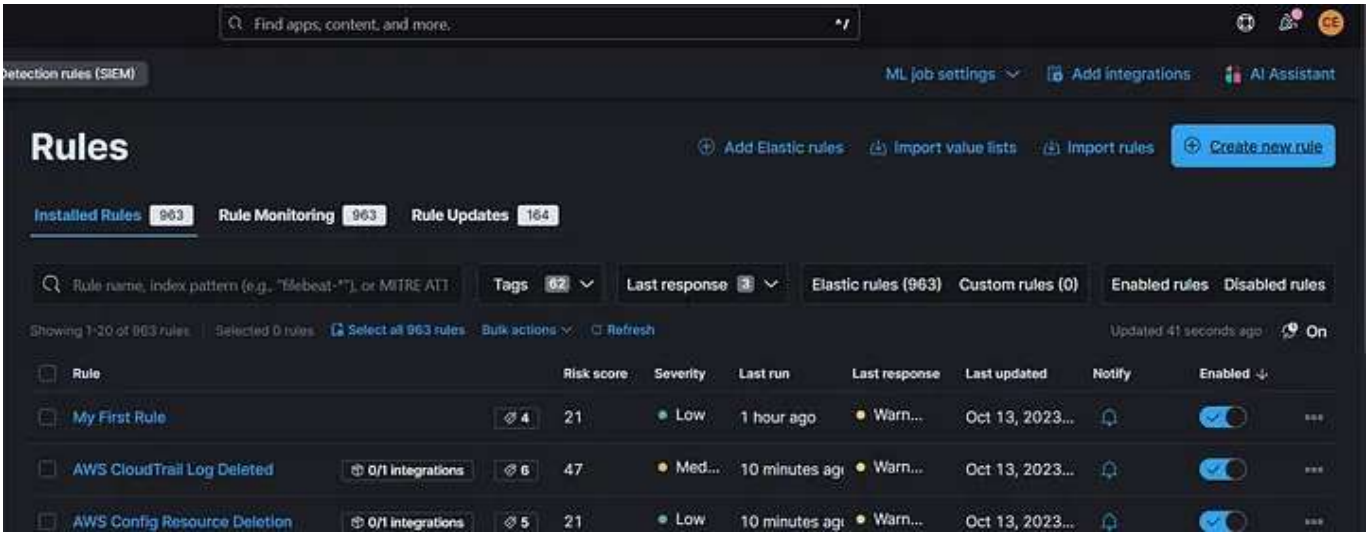
Alerts serve as a vital component in a SIEM system, ensuring the prompt detection and response to security incidents. These alerts are crafted based on predefined rules or customized queries, tailored to trigger precise actions when specific conditions are met. The focus here is to walk you through the process of setting up an alert within Elastic SIEM, designed to detect specified events (in this case, Nmap scans). By adhering to these steps, you'll establish an alert system that actively monitors your logs for predefined activities that promptly informs you upon their detection.



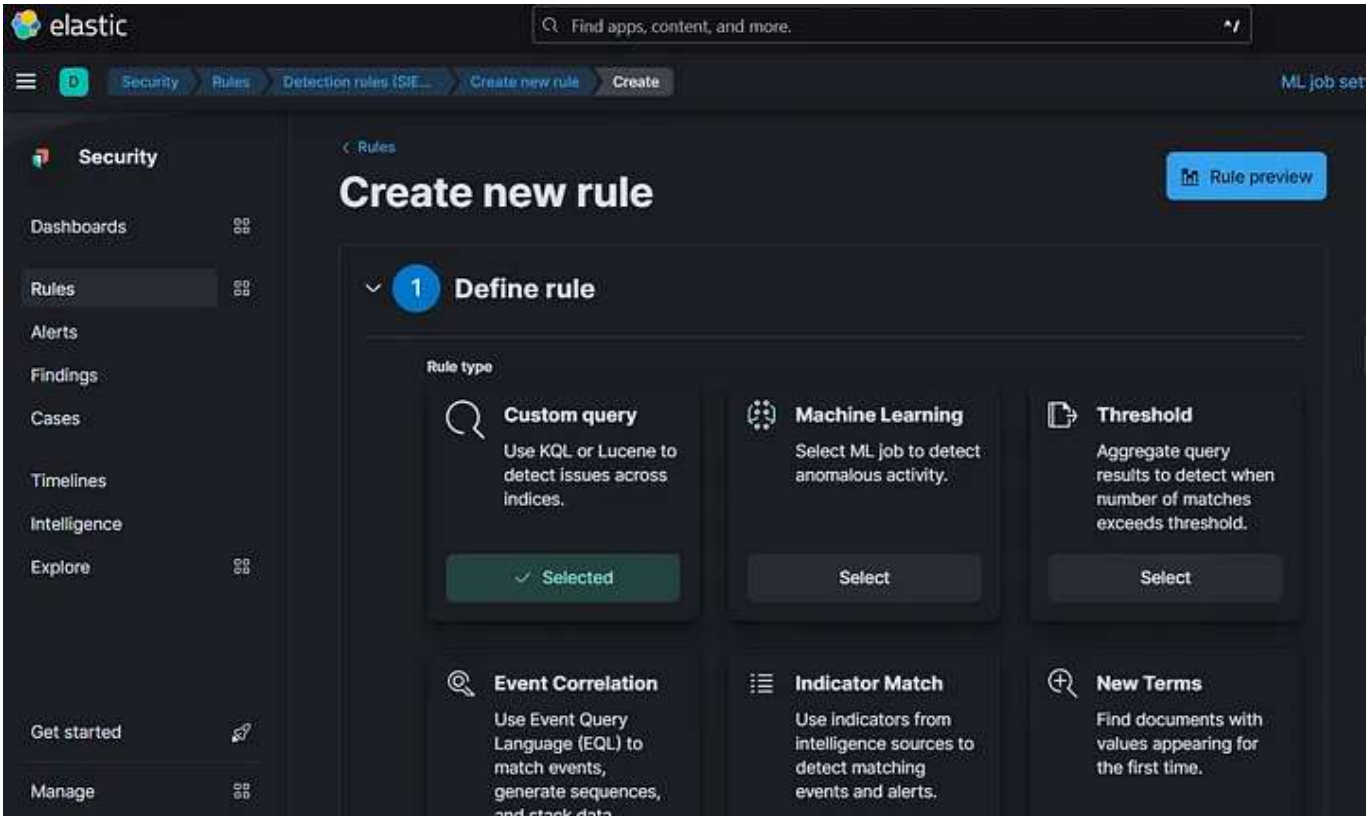
Click on “Alerts” in the menu at the top left.



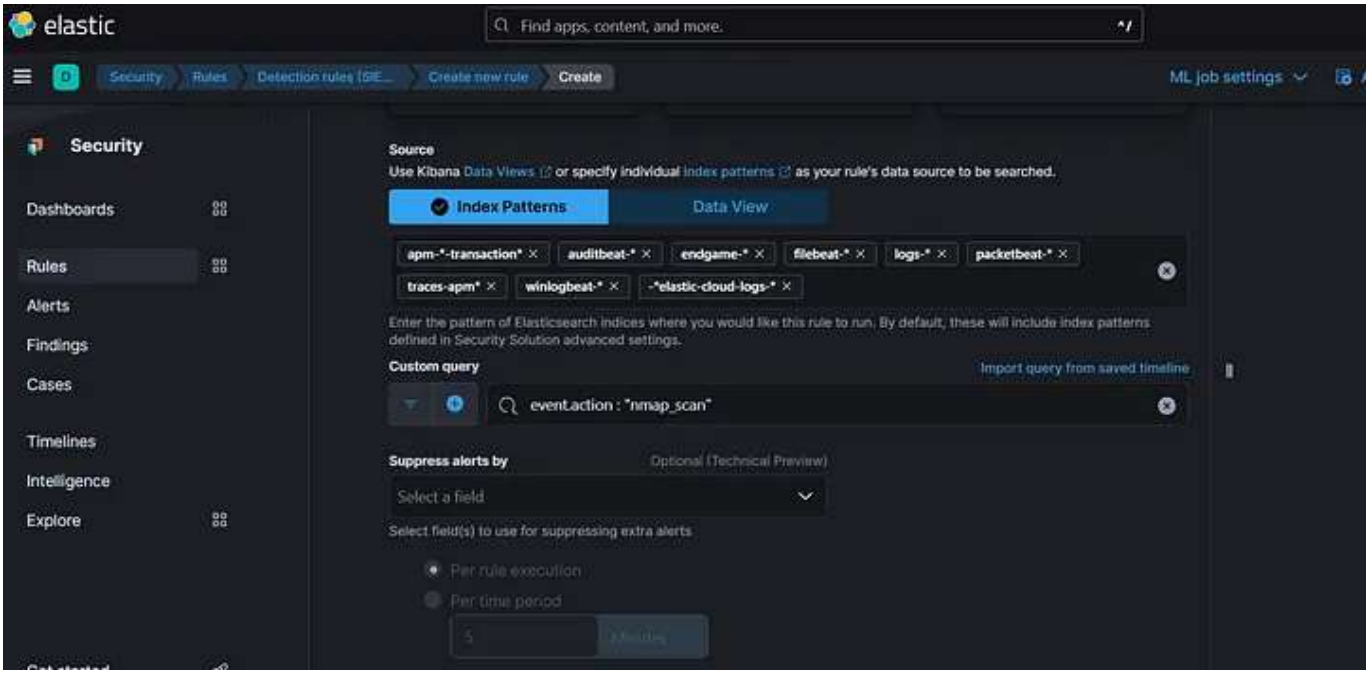
Select “Manage rules” in the box at the top right.



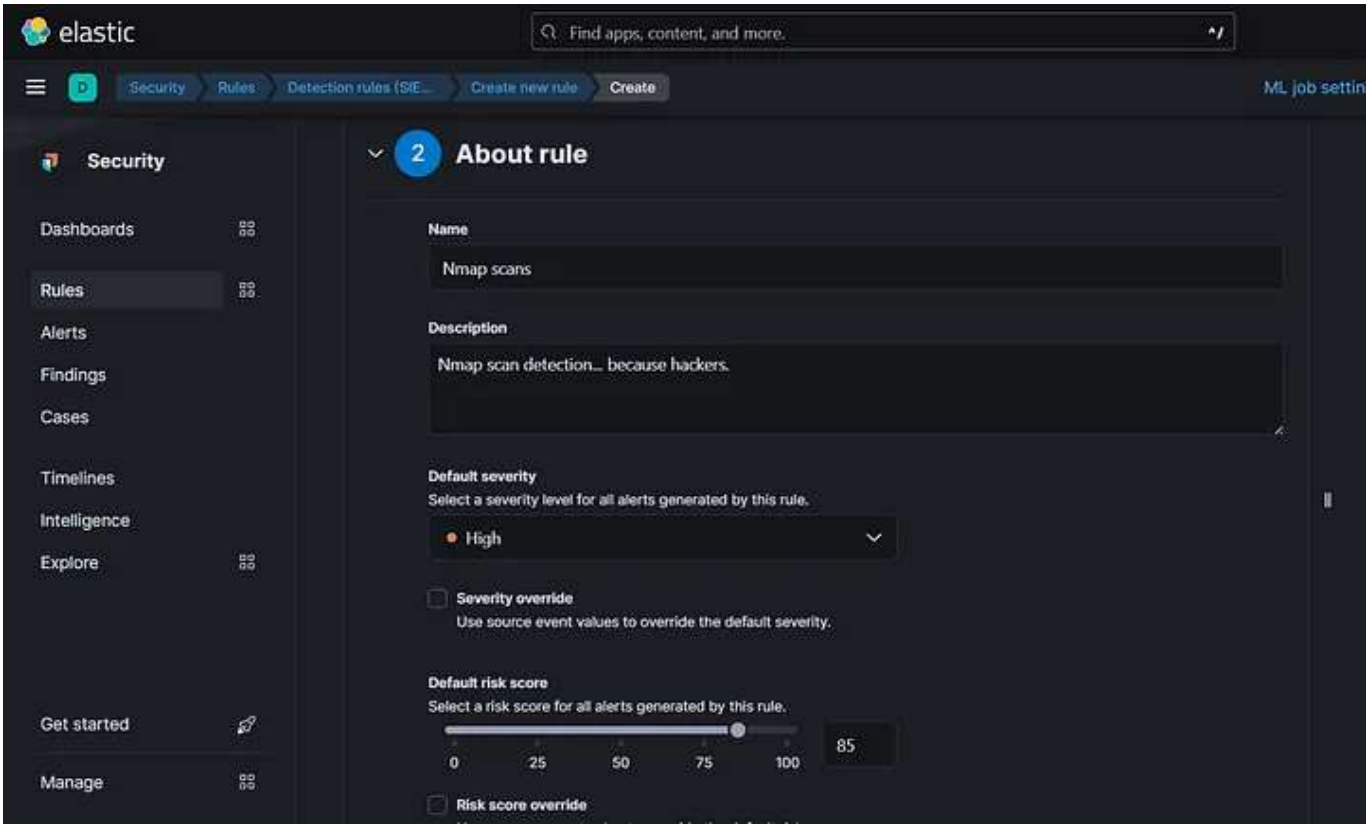
Select “Create new rule” in the box at the top right.



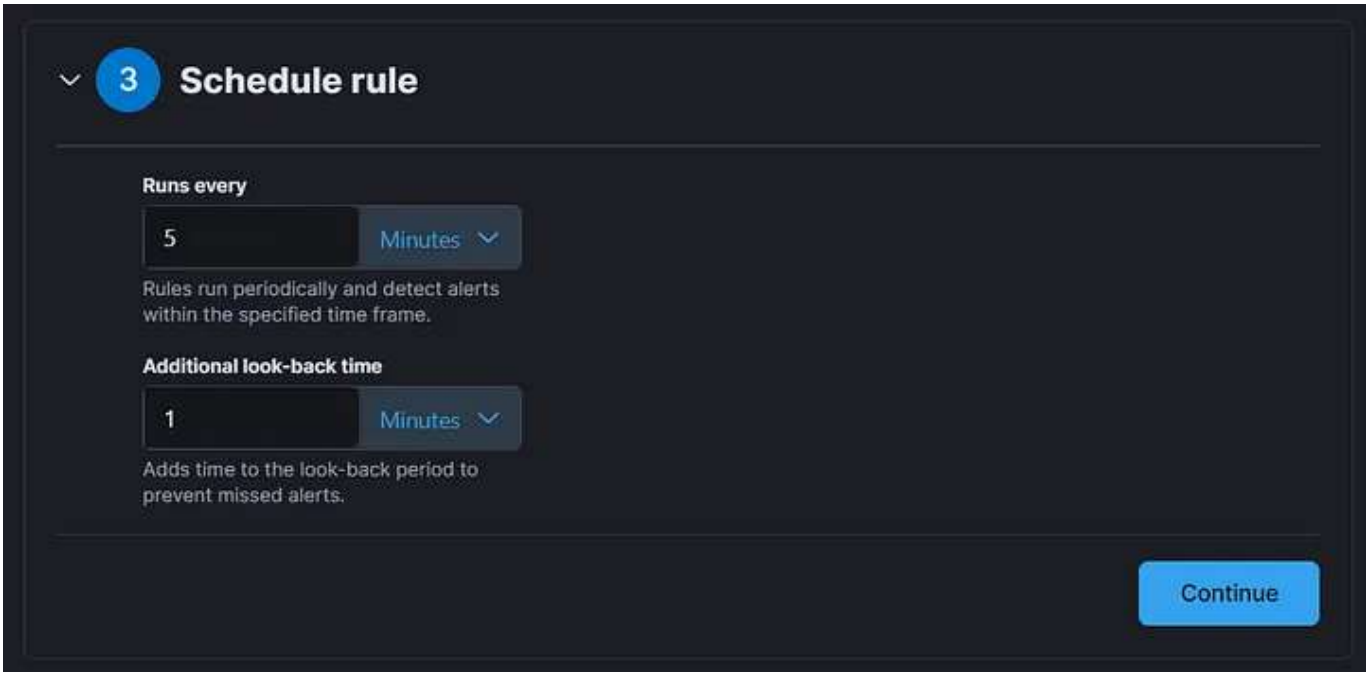
Select the “Custom query” Rule type.



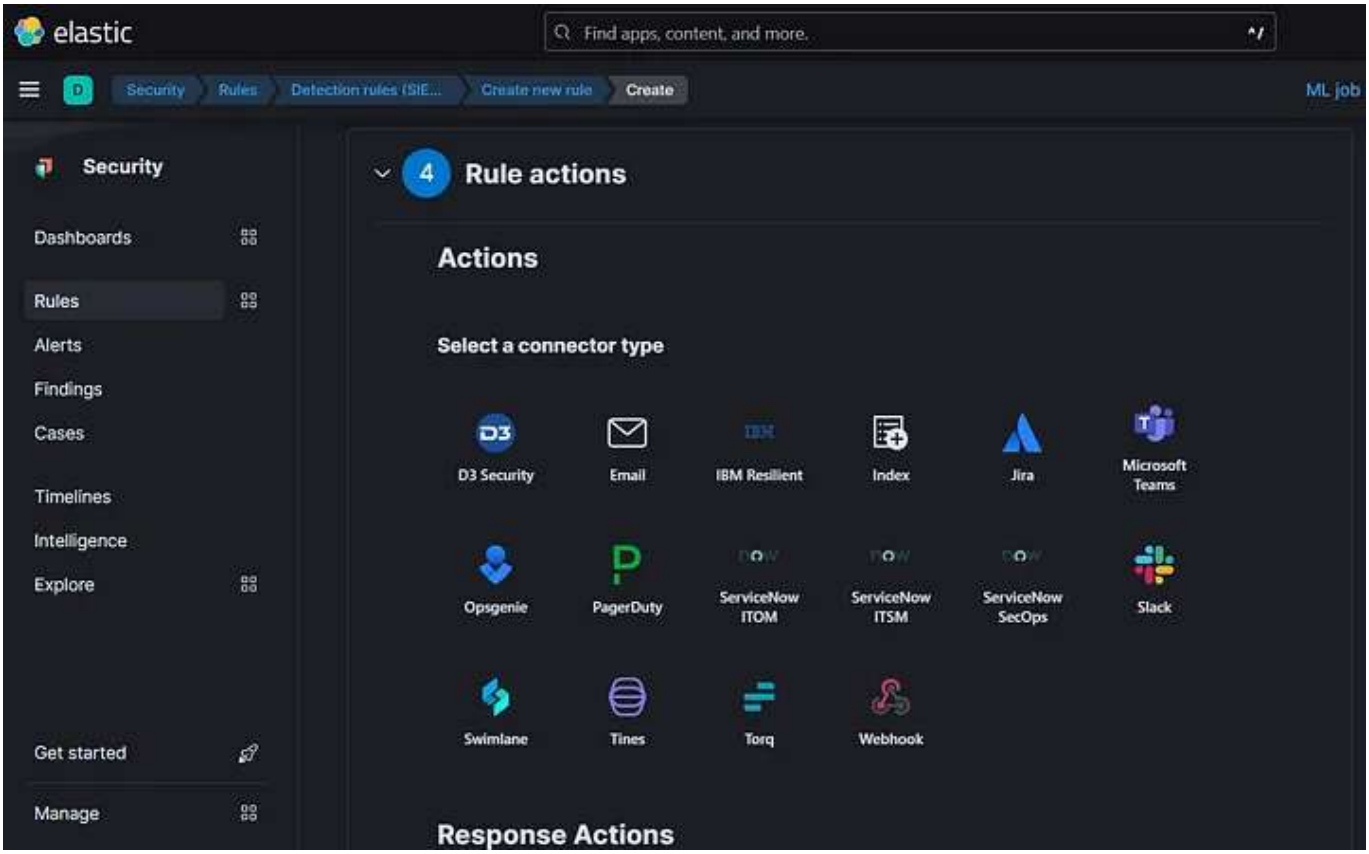
Under “Custom query,” type **event.action: “nmap_scan”** which is the condition for the rule and will match all events with the action “nmap_scan.” Next, click “Continue.”



Fill in the “About rule” section however you prefer. In this example, the Default severity level is set to High with a Default risk score of 85. Click “Continue”.



Runtime for rules can be adjusted under “Schedule rule”. In this example, the default values were used. Click “Continue”.



In the “Rule actions” section, pick the action to take when the rule is triggered. Notice that these actions can range from email, Jira or Slack alerts depending on which tools your business units/teams prefer to use. Click the “Create and enable rule” button to create the alert.

Conclusion:

In this guide, you've set up a home lab to practice Elastic SIEM and gain hands-on experience in security monitoring and incident response. You've learned how to forward data, generate and analyze security events, create dashboards, and set up alerts. This practical experience will enhance your skills and prepare you for a career as a security analyst or engineer.

I would like to extend a sincere thank you to Abdullahi Ali for providing inspiration and encouragement for this blog post. You can find Abdullahi's blog post about using Elastic SIEM, here: https://medium.com/@aali23/a-simple-elastic-siem-lab-6765159ee2b2

Next Steps:

- Experiment with different security and non-security events on your Kali VM and test the alert. Doing this will help reinforce your Linux and threat hunting skills at the same time.
- Explore more features of Elastic!
- Setup your own Elastic project based on a specific simulated business use case.

Cybersecurity | Information Security | Technology | Data Science | Blue Team

Written by Christopher Elce

Follow

129 Followers

Currently on the job hunt for a career in cybersecurity and posting about what I'm learning.

More from Christopher Elce

Christopher Elce

Operating a SOC Analyst Home Lab

... “Find Evil—Know Normal.” (SANS DFIR slogan)

10 min read · Jul 29, 2023

303 4

Christopher Elce

How I Supercharge Learning Cybersecurity with Cisco Packet...

“Whatever, I’m getting cheese fries.” (Regina George, Mean Girls)

5 min read · Aug 12, 2023

34

Christopher Elce

Learn Cybersecurity with Minecraft and Docker

"Imagination is the only weapon in the war with reality."

14 min read · Aug 8, 2023

See all from Christopher Elce

Recommended from Medium

Software Sinner

Offensive Security Proving Grounds (Amaterasu)

Offensive Security offers free lab machines under their “Proving Grounds” library that I...

5 min read · Jan 9

68 2

David Varghese in InfoSec Write-ups

Building a Virtual Security Home Lab: Part 1 - Network Topology

A step-by-step guide for building your very own Cybersecurity Home Lab using...

6 min read · Dec 31, 2023

133 1

Lists

Predictive Modeling w/ Python
20 stories · 821 saves

ChatGPT prompts
34 stories · 997 saves

AI Regulation
6 stories · 283 saves

Coding & Development
11 stories · 394 saves

Fazla rabbi

10 OSINT Tools We Use in Our SOC

In our modern digital era, virtually every individual and institution generates a...

15 min read · Dec 11, 2023

Juan Pablo De Armas

Cybersecurity Detection Lab using Security Onion

Objective

7 min read · Jan 8

186 3

13

Sulaiman Alhasawi

My Journey Through ICS Cybersecurity in 2023: Personal...

As 2023 draws to a close, it becomes crucial for me, to pause and ponder over the path...

3 min read · Dec 31, 2023

Hari Ganesh M

Windows Forensics (DFIR)

This write-up is a walkthrough for the challenge in LetsDefend.io

9 min read · Oct 7, 2023

76

See more recommendations