

**Log Analysis / SIEM Integration**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Authored By:

**Jon Murray**

6-15-23

Table of Contents

Overview \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ pg 1

Elastic Setup

Registering an account\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ pg 2,3

Create a Deployment \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ pg 4-8

Endpoint Integration \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ pg 8-10

Pseudo Threat Actor Activity \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ pg 11,12

Log Analysis \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ pg 13

Conclusion \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ pg 14

Sources:

Elastic SIEM

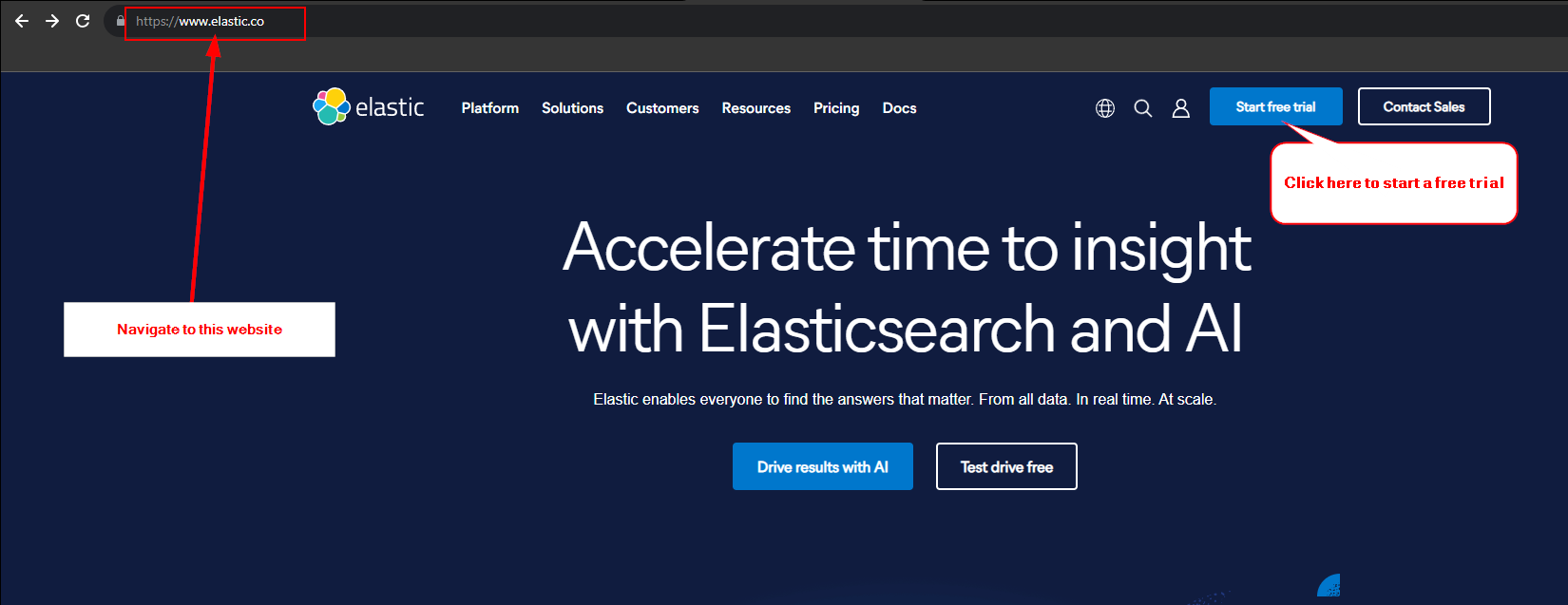
**Overview:**

This is a demonstration of setting up Elastic SIEM and then incorporating a local Kali Linux machine into the SEIM itself, in preparation for analyzing logs that recorded numerous security events. We will then conduct threat actor type activity against the Kali machine, including a pseudo-malicious scan of the Kali machine, the addition of a user to that machine and several attempted logins to that user that failed due to an incorrect password entry.

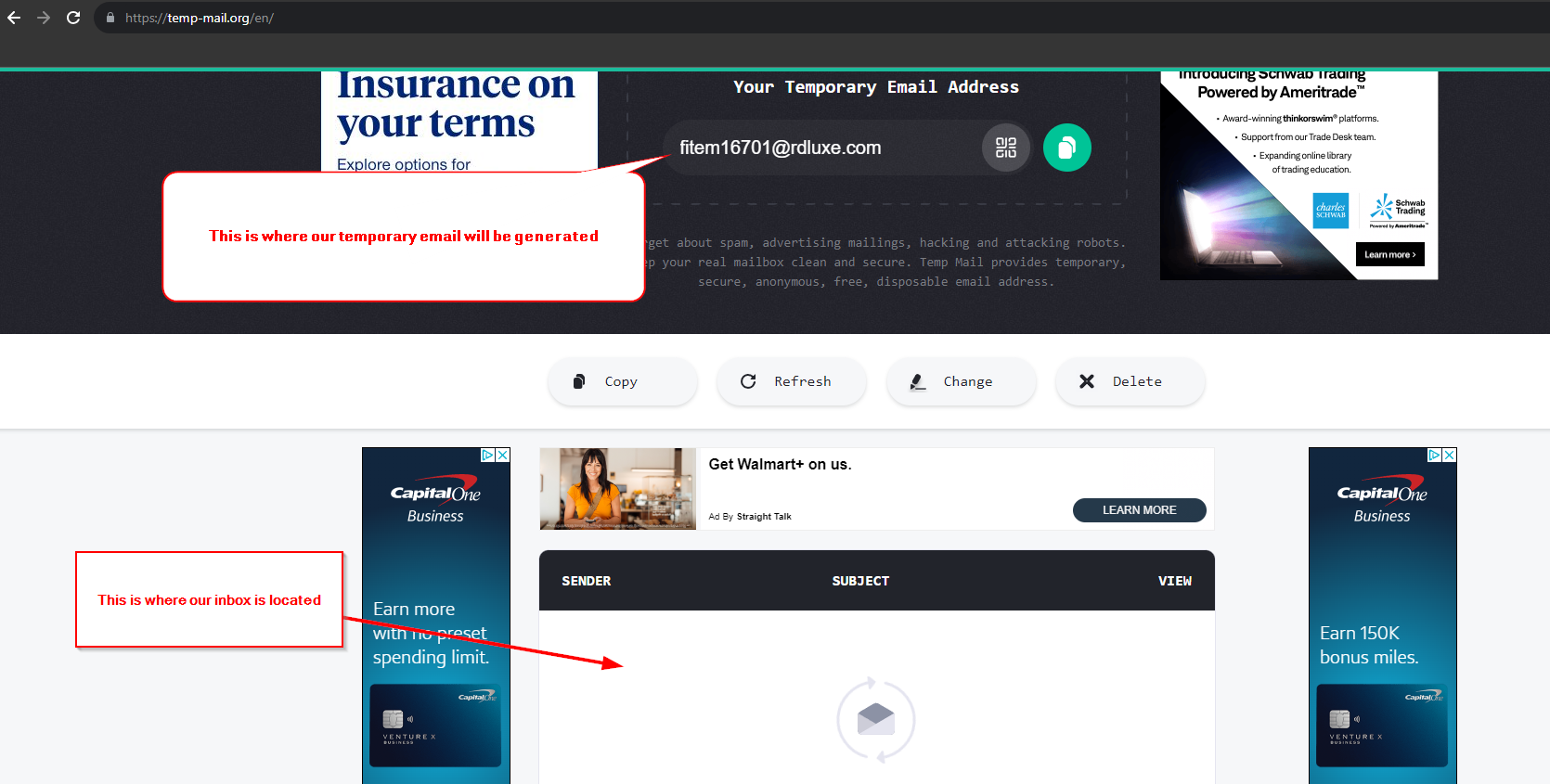
The security logs will be sent to Elastic after integration. Then we will run searches for the activity that we conducted, as a threat actor. We will review those logs, attempting to identify the malicious activity.

**Setting Up Elastic SIEM:**

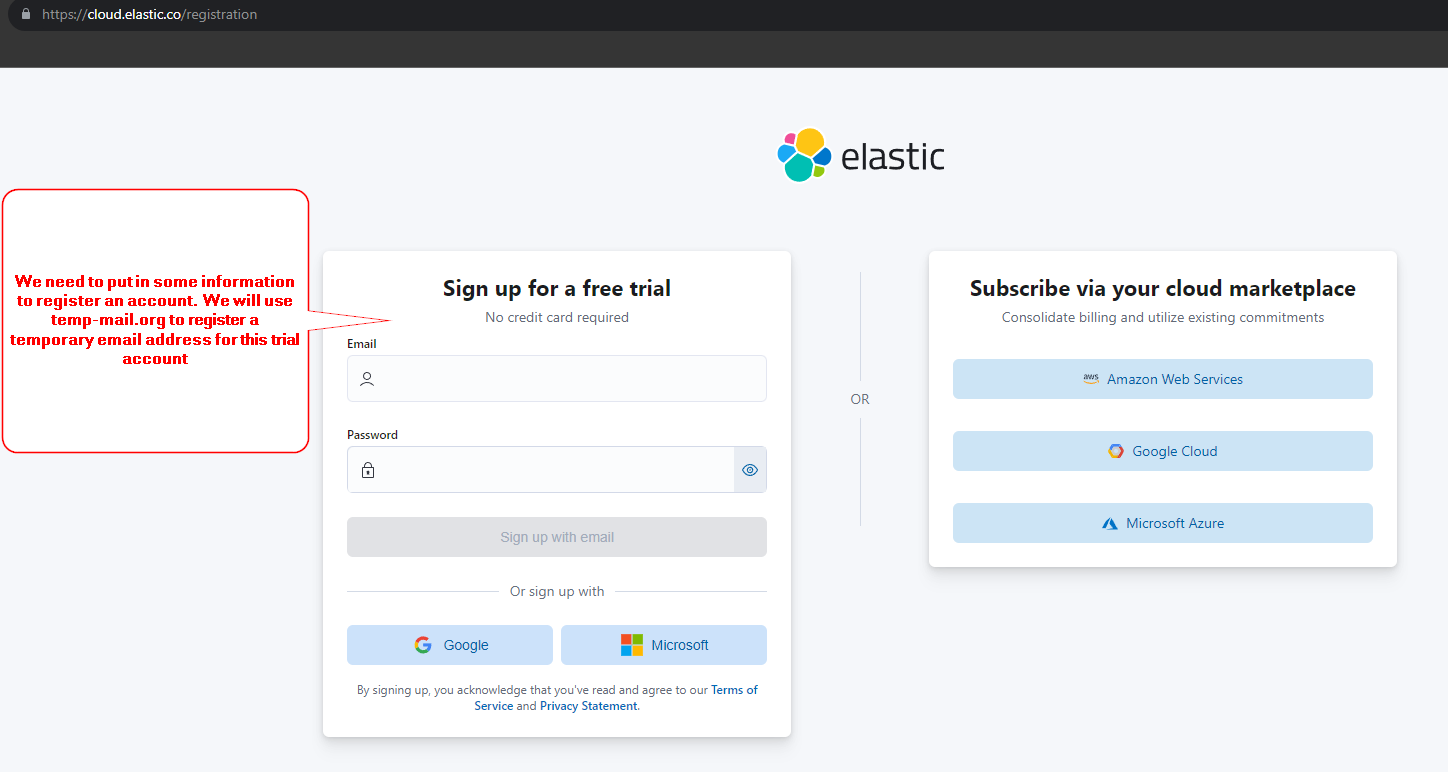
We need to begin this lab by setting up an Elastic account. First, let’s open the web browser and navigate over to <http://www.elastic.co>. This will bring us to the Elastic website as shown below. Now we need to set up an account that we can use to run our SIEM. Click on the blue “Start Free Trial” button in the upper right corner of the screen:

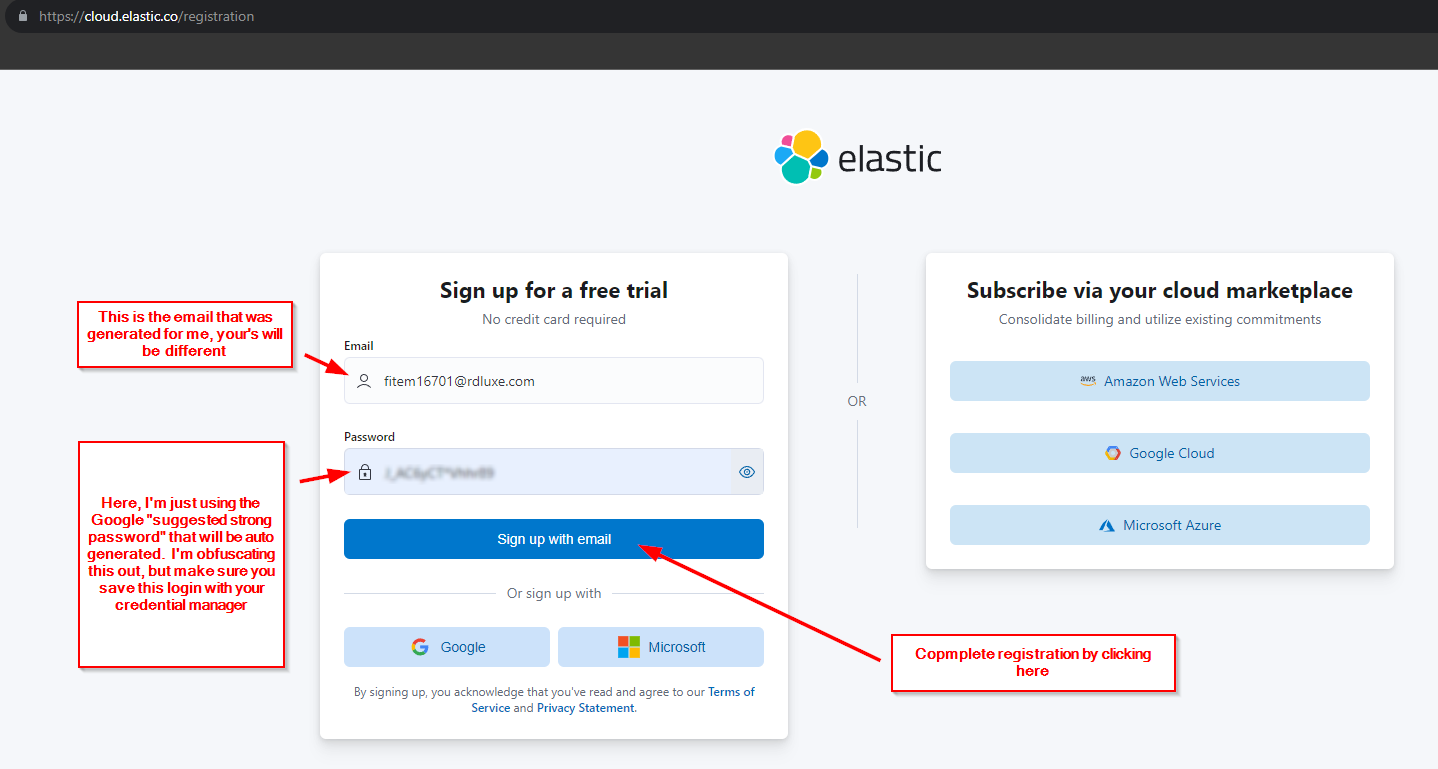


This brings us to the login page where we will create our account. As shown below, we need to enter an email address and password to use for the account. As this is just an exercise, I’m going to head on over to <https://temp-mail.org/en/> to generate a temporary email that we can use for this lab. Make sure you **DO NOT** close the browser tab on temp-mail or you will lose access to it:

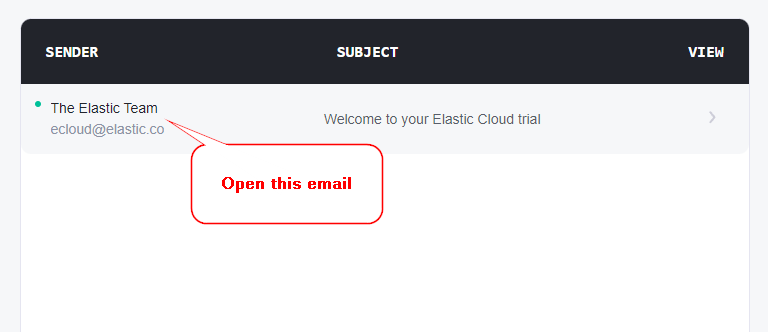


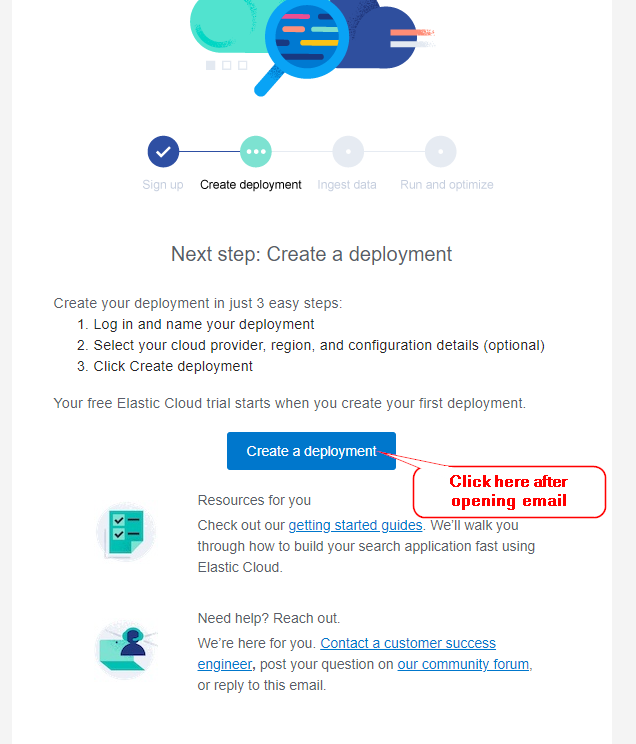
Once you have an email ready, copy that address into the email on the registration page of Elastic:



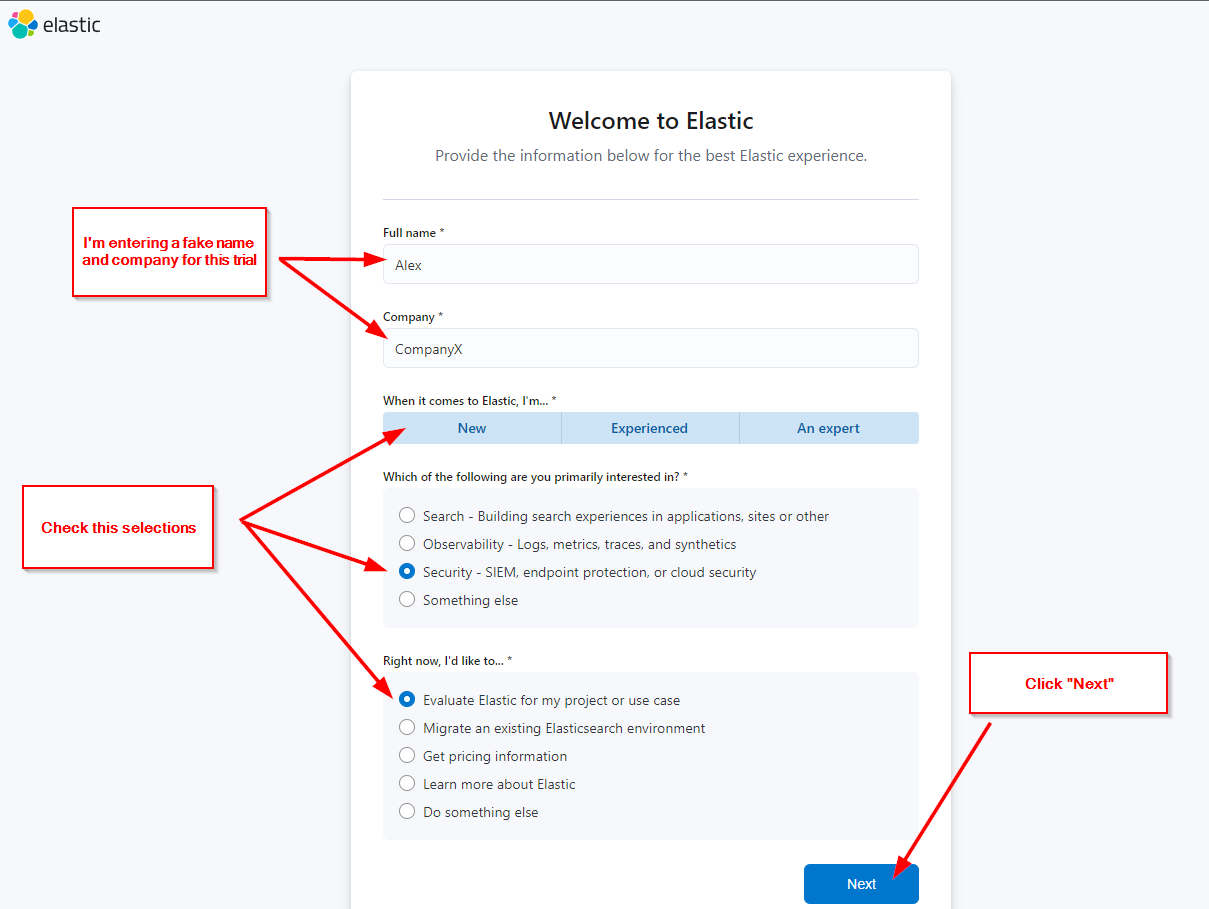


Click the blue “Sign up with email” button. This will take a few minutes to set up so just be patient. About 10 minutes later, we received an email from Elastic. After opening the email, we click on the link “Create a Deployment”:

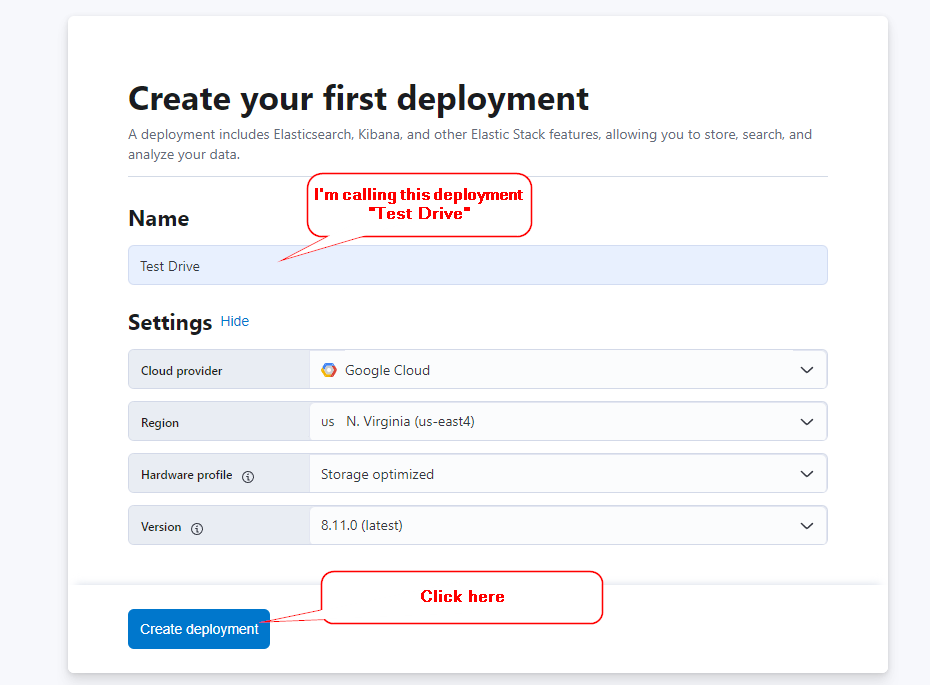




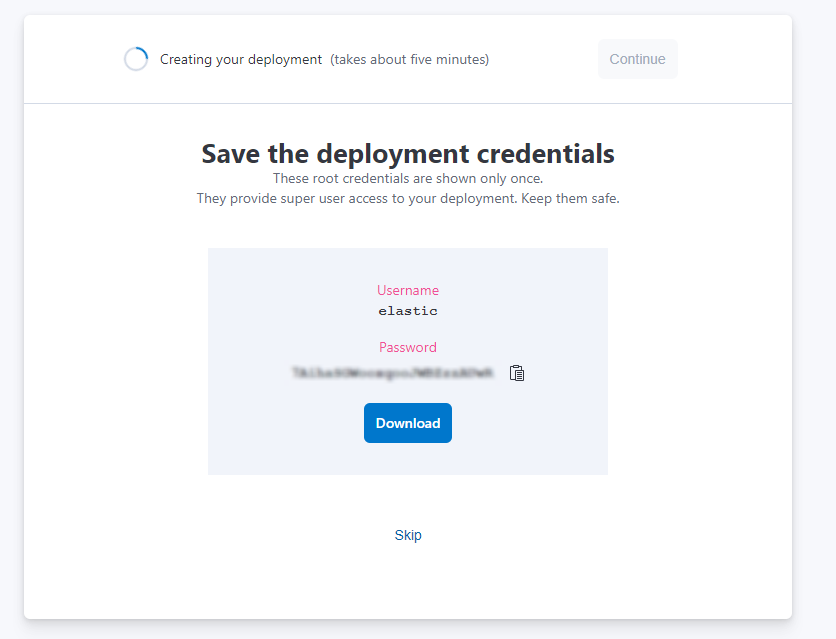
Now we need to complete some further registration information for our SIEM. I’m going to use the name Alex and the company name CompanyX. Once finished, click the blue “Next” button:



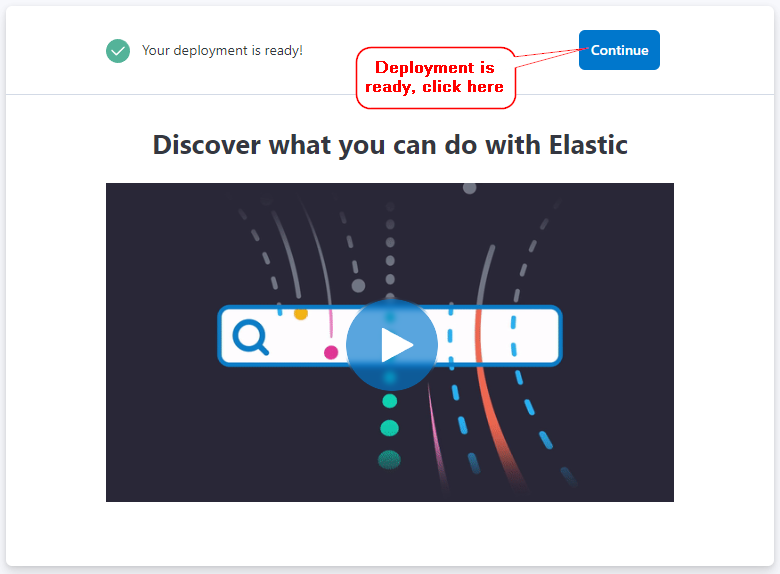
Now we need to enter a name for our deployment, which I’m just going to call “Test Drive”. The settings didn’t seem to matter too much to me but I did change the time zone. Click on the blue “Create Deployment” button at the bottom of the screen:



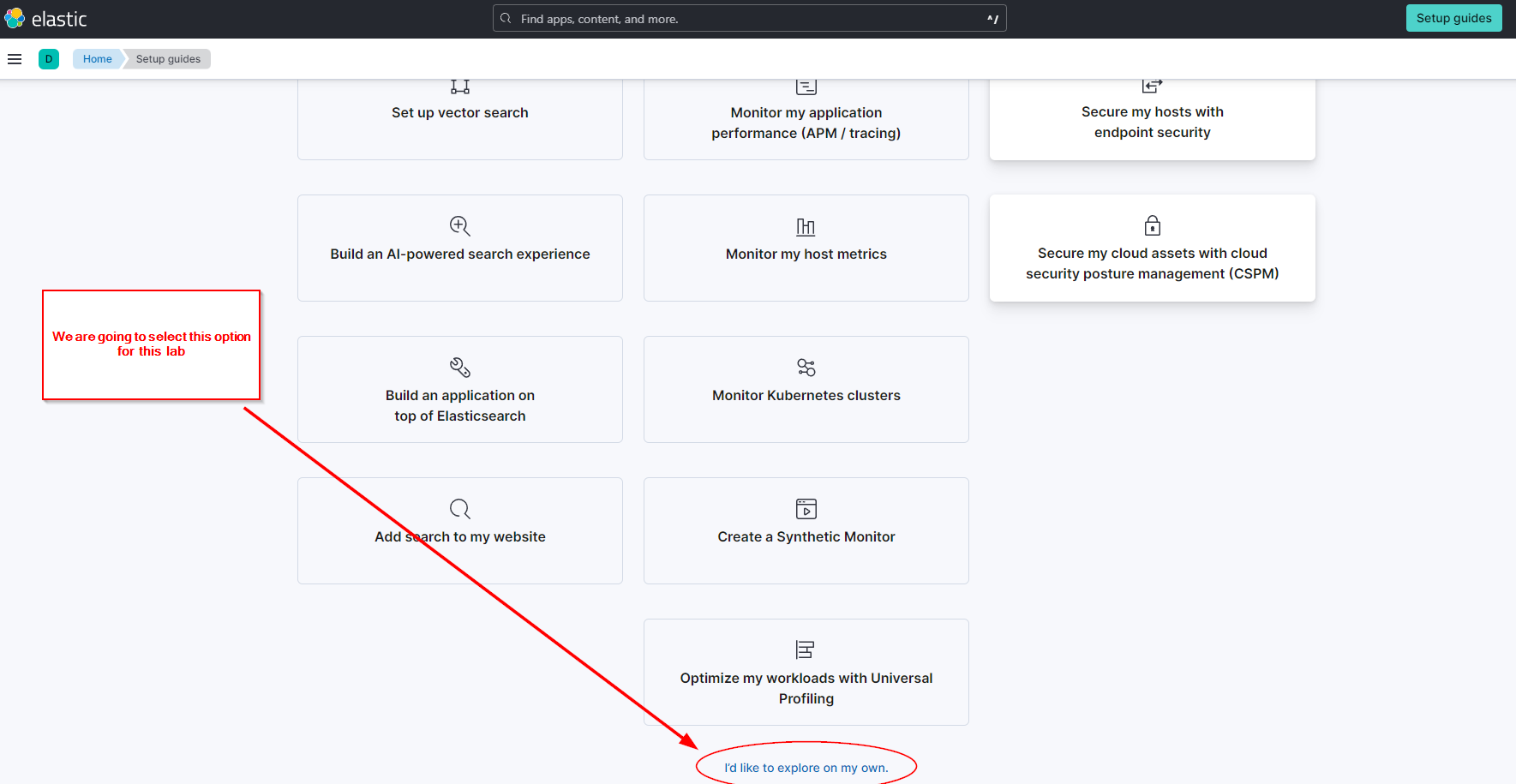
You will be presented with root credentials for your SIEM. I simply screenshotted these, you can download them if you wish:



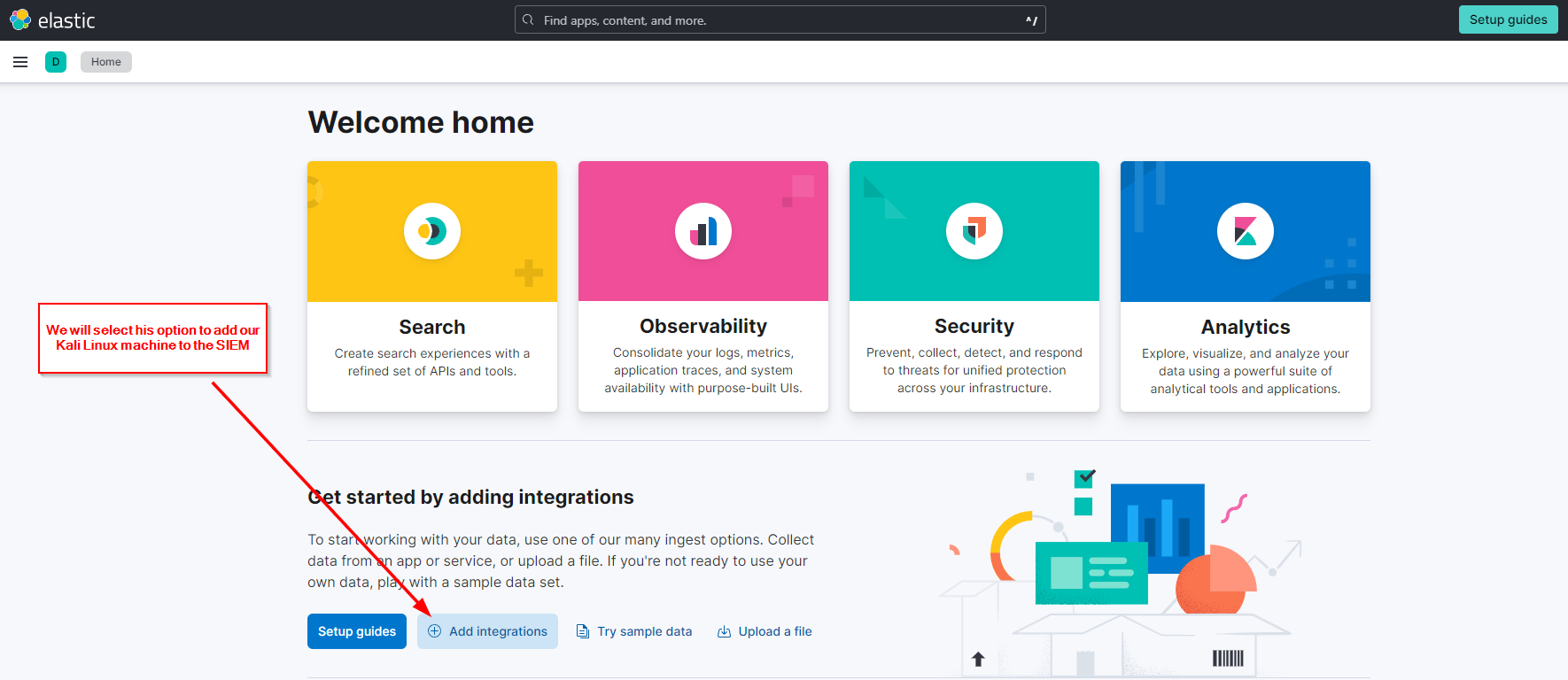
Once the deployment is ready, go ahead and click the blue “Continue” button:



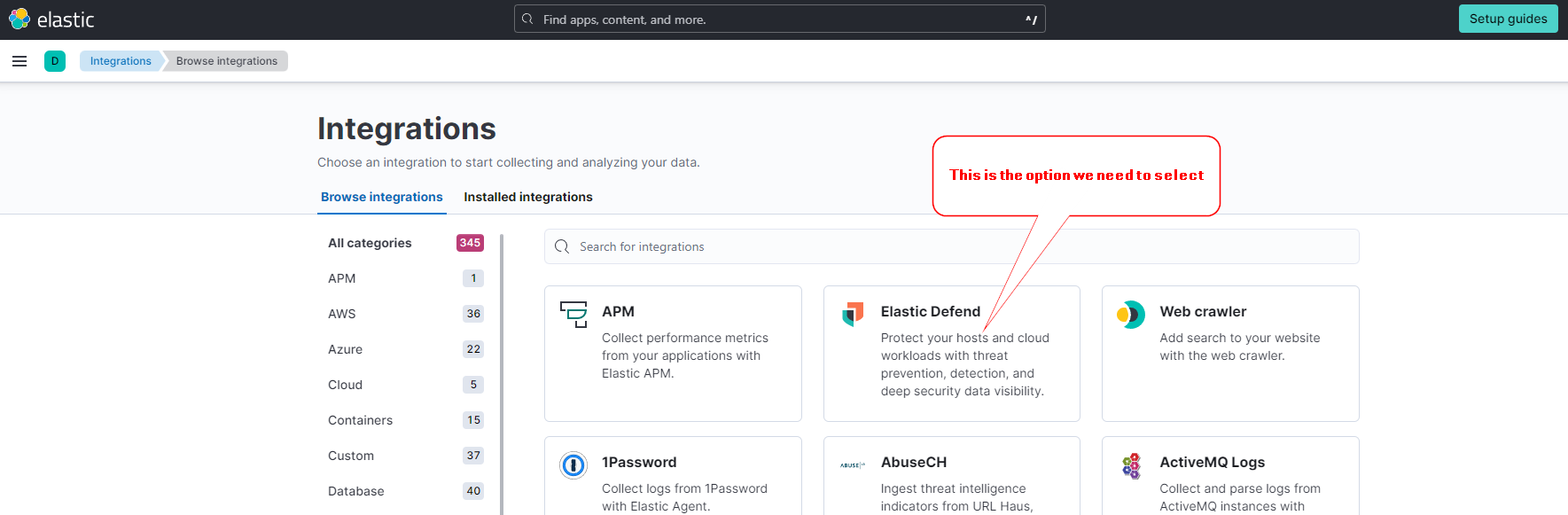
Finally, we will be brought to the setup page where we have options for numerous actions. At the very bottom of the page is a link “I’d like to explore on my own” which we will select, that will bring us to the home page:



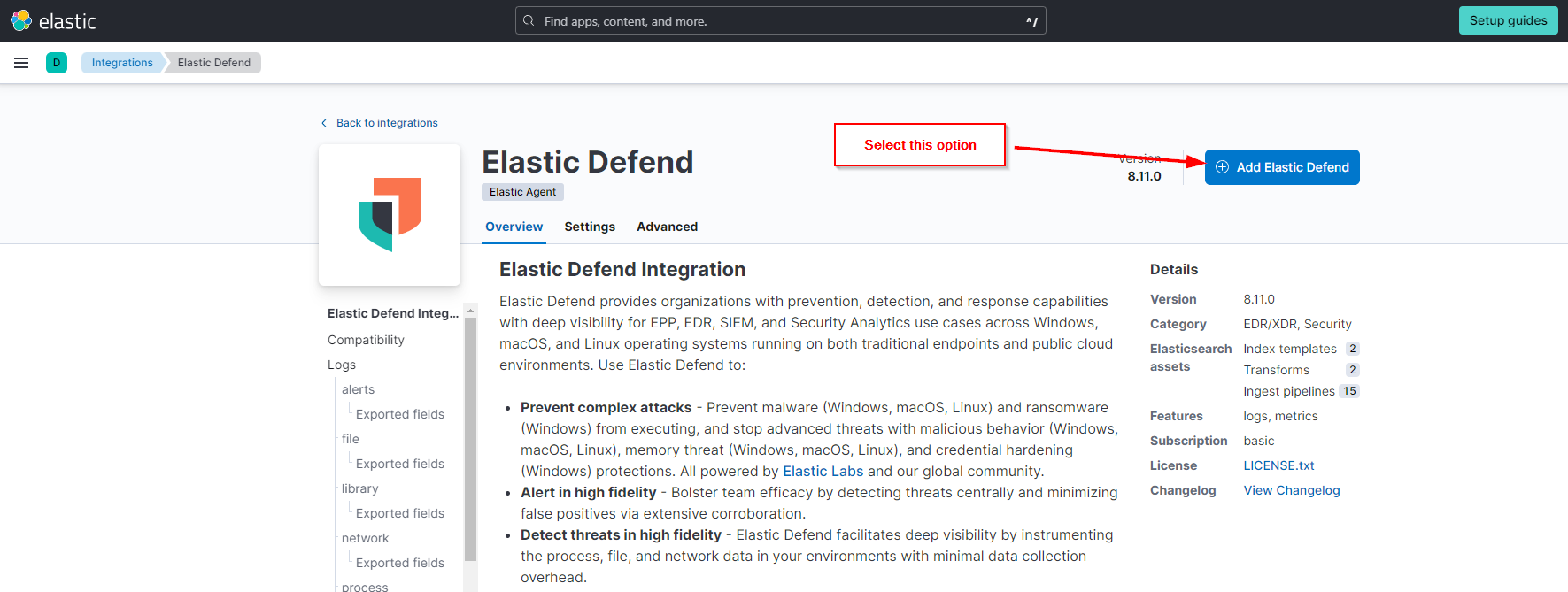
**Integrating an Endpoint:**

Now we are ready to add our Kali Linux machine to our seem. Our Kali Linux machine is what is called an Endpoint. The logs of this machine are what we are going to analyze, after we conduct some pseudo-threat actor activity. Before we do that, this machine needs to be connected to our SIEM so that the logs can be sourced.

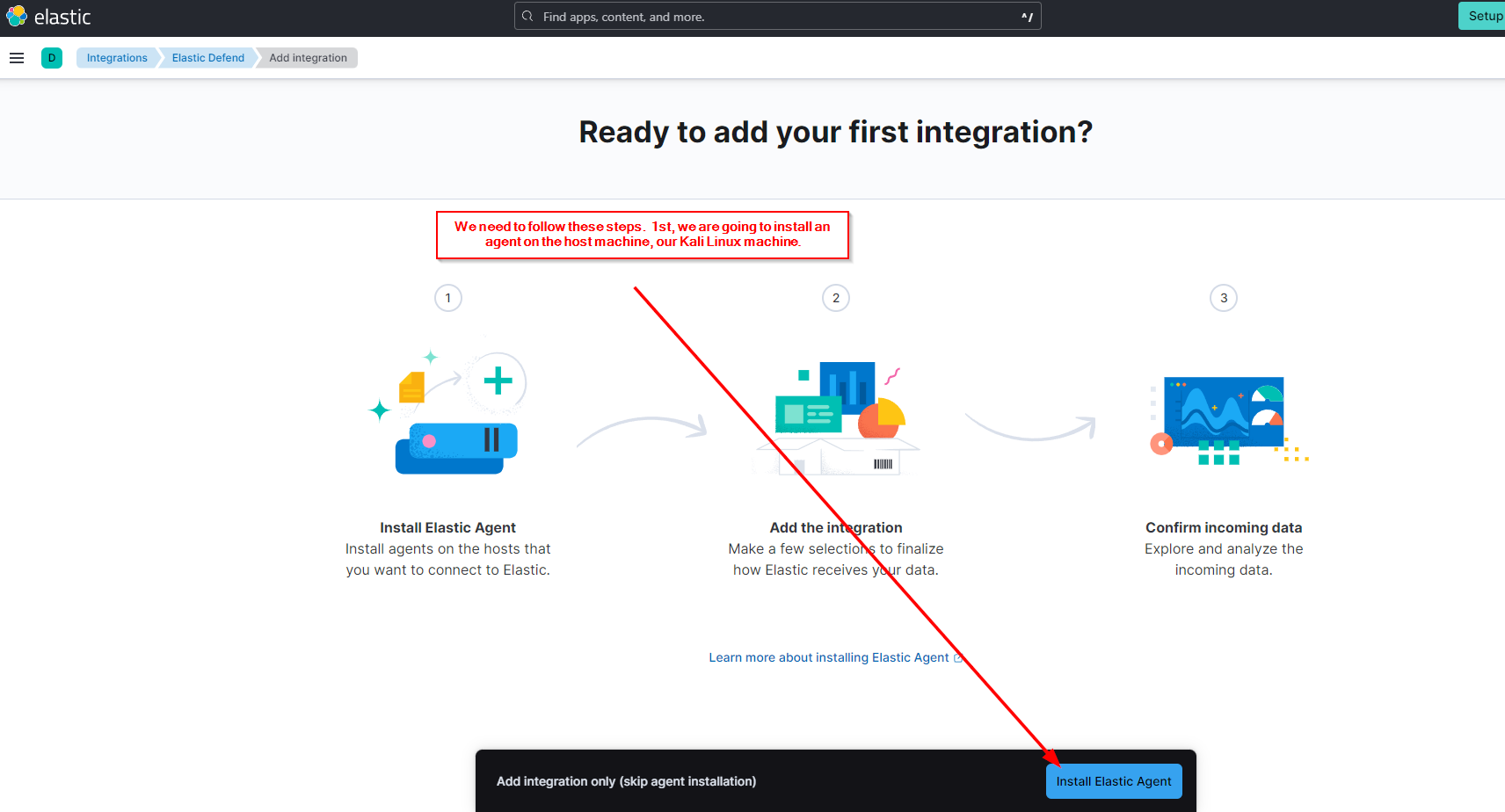
We are presented with a number of different applications that we can select. We need the top middle option called Elastic Defend (formerly Endpoint and Cloud Security Integration):



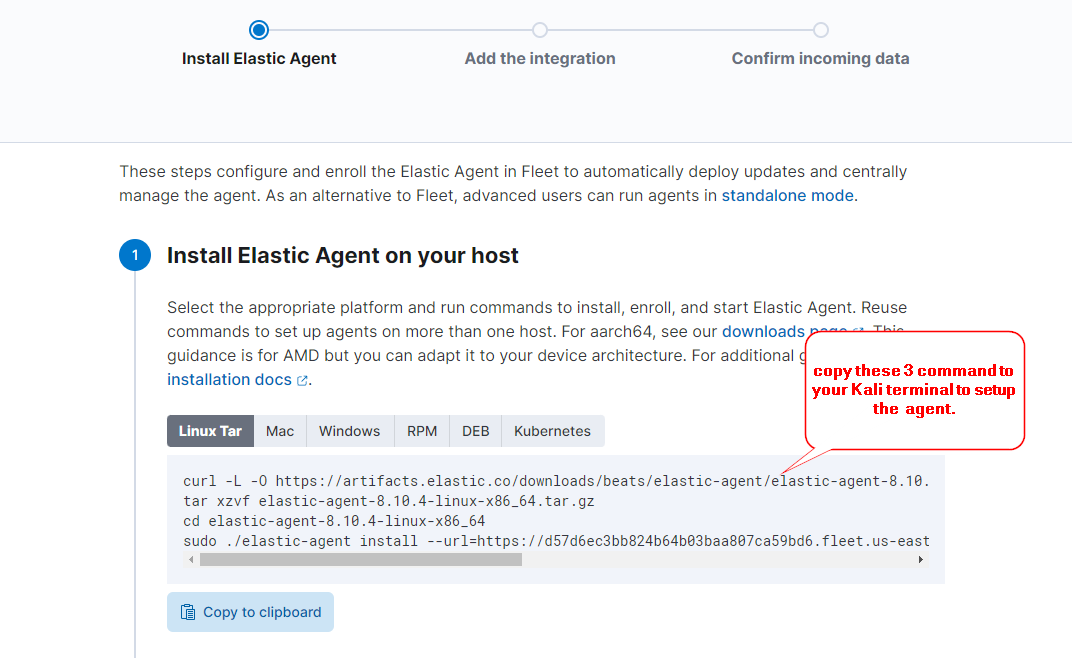
Select the option to “Add Elastic Defend”

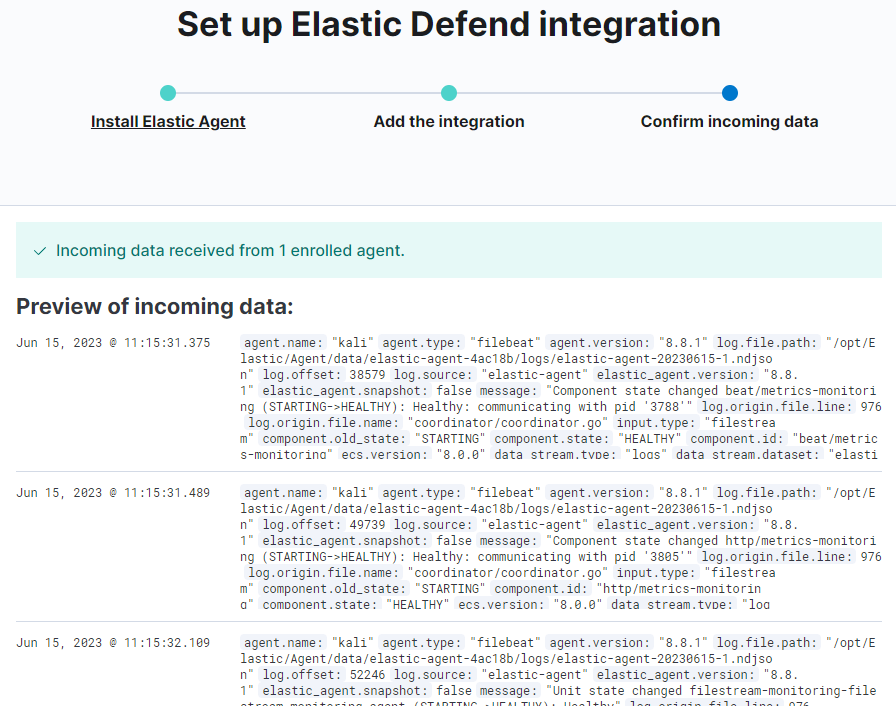


Now we are presented with a few steps we need to follow. The 1st will be to install the Elastic Agent on our Kali Linux machine, so that it can communicate with our SIEM. Click on the blue “Install Elastic Agent”:



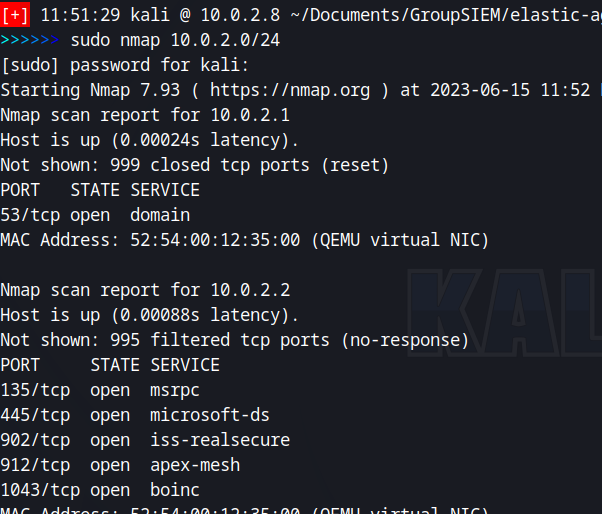
Next, we need to copy the 3 commands listed in the clipboard and run them 1 by 1 on the terminal in our Kali Linux machine. My machine already has an agent on it, so I will skipping this portion. Follow the prompts and confirm that data is being sent to the SIEM:



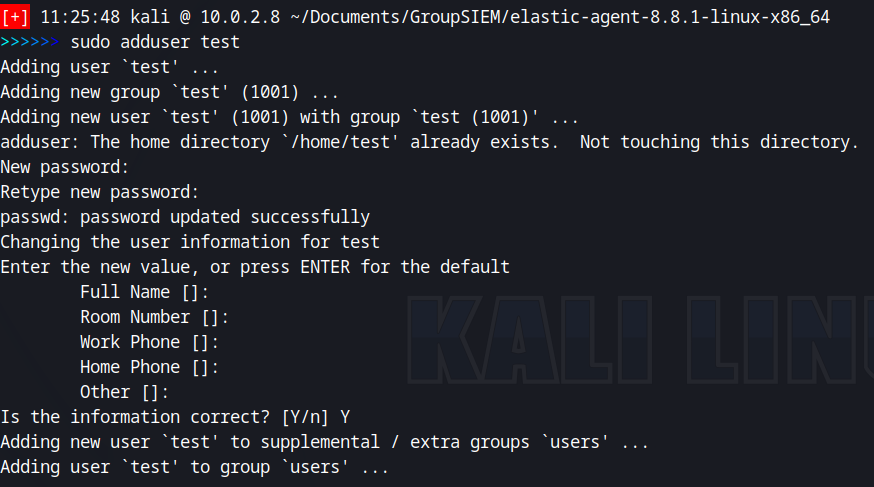


**Pseudo Threat Actor Activity:**

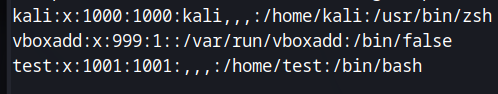
Perfect. Now we have an agent installed on the Kali Linux host machine that is communicating with the SIEM. Now it’s time to conduct some threat actor activity on our Kali Linux machine. This activity will create logs that are sent to the SIEM, that we can analyze later. First up, let’s run an nmap scan against our Kali machine, to simulate a threat actor conducted a scan of our network, or an endpoint within our network:



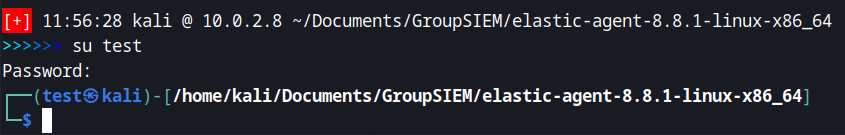
Now let’s simulate a threat actor adding persistence to our endpoint, in the form of creating a new user on the machine:



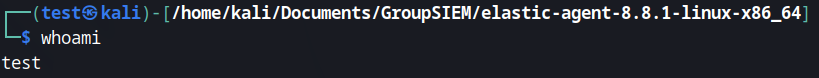
And now we can verify that the user was created by using the command <**cat /etc/passwd**> on our terminal. This will display the list of users on the machine:



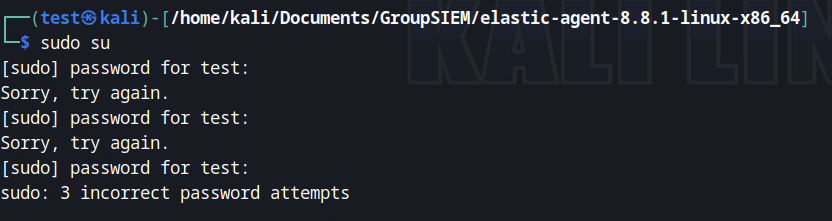
The user “test” has been successfully created. Let’s switch to that user using command <**su test**> on the terminal:



Next, we use command <**whoami**> to check our current user:

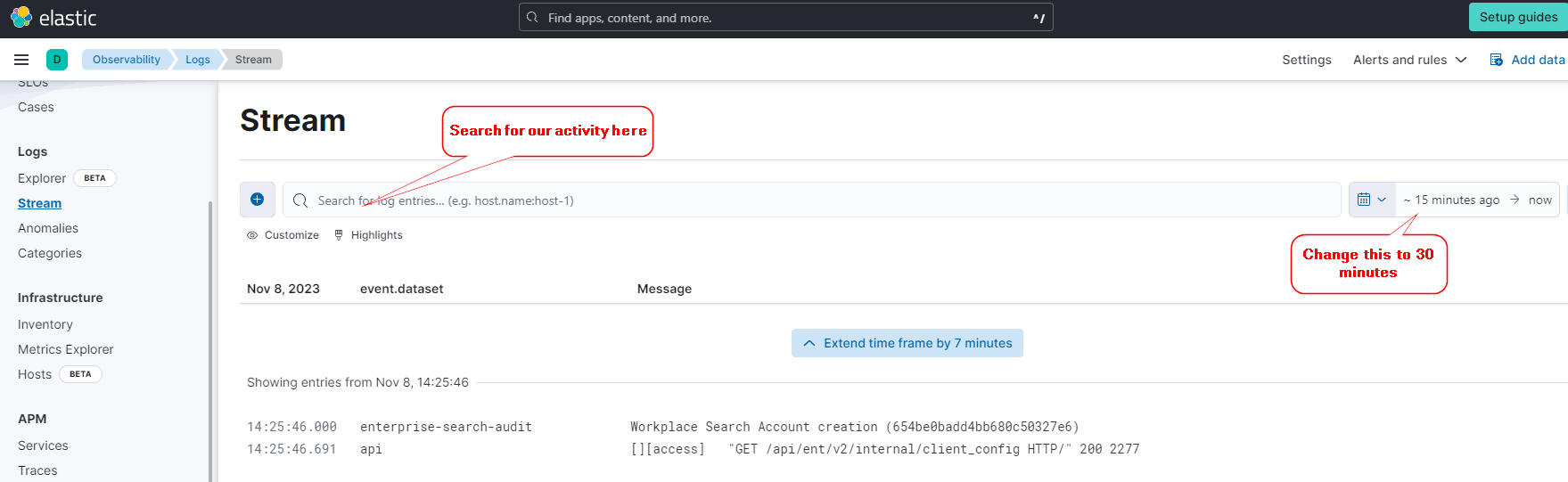


If the setuid binary is set for both the “sudo” command and the “su” commands (we never changed this when we setup our Kali Linux machine in VirtualBox, originally), we can use the command <**sudo su**> to instantly switch to the root user on the machine. Note: This is a security violation and setuid binaries should always be checked to make sure that a non-root user cannot leverage setuid binary exploits to gain root user privileges. These types of attacks are detailed in my write-up named “How Many Shells”, however, this is an advanced topic and is beyond the scope of this lab, so I will not go over that here. Understand that this command is exploiting the setuid binary. Following this command, we will be asked for the sudo password of the current user, which in this case is “test” and since we are still acting as the threat actor, we would know the password we assigned to “test” when we created the account. Therefore, after entering test’s password, we would instantly be switched from the “test” user, to the “root” user. For this lab, we **WILL NOT** enter test’s password. We will simply hit “enter” to simulate a password being entered. Kali Linux affords you 3 opportunities to enter a correct password before exiting the command. We are hitting enter each time and **NOT** entering a password. The purpose of this is to simulate a threat actor entering passwords, which we will analyze in the logs sent to the SIEM:

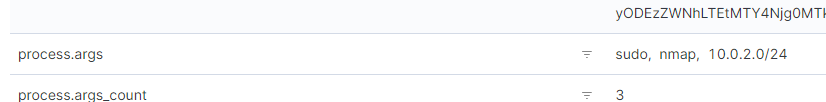


**Log Analysis:**

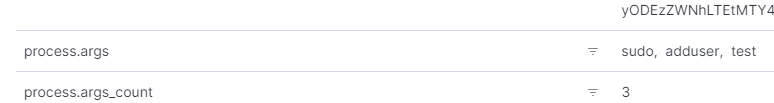
Now it’s time to switch roles to the Security Analyst and analyze our logs to find our malicious activity. In the real world, alerts would be setup to hit on this kind of activity, in which case the Analyst would take further action. Many other SIEMs, including Splunk and Crowdstrike, have these capabilities. Elastic is not the only SIEM, it’s just one we are using for this lab. Under the Obervability/Logs/Stream section, we can search for the activity we conducted as a threat actor. We will begin by running a search for the nmap scan of the Kali Linux machine:



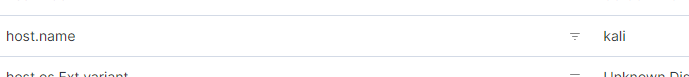
Here is a sample of the log data from one of the logs. In the process.args line, we can see that the nmap scan was conducted:



Here is a sample of the log data from the search for the “adduser” command that the threat actor used to establish persistence on our Kali Linux machine. Again, the process.args line contains the command used, as well as the name of the user who was added:



Further down, on the host.name line, we can see that the threat actor was initially logged in as the “kali” user, when the “test” user was created:



**Conclusion:**

In this lab, we set up an Elastic SIEM. We then installed an agent on our Kali Linux machine that sent log files to our SIEM. Acting as a threat actor, we conducted pseudo-malicious activity against our Kali Linux machine including scanning the machine (which is referred to as an endpoint in our SIEM) with an nmap scan, adding persistence in the form of adding an unauthorized user, and then attempting to switch to that user to gain root privileges.

After this activity, we then switched roles to the Security Analyst and searched for the activity in our SIEM. Logs showed that the activity was detected.

In a real-world situation, we could then take action to mitigate the threat, which would include identifying the IP address of the threat actor and blocking it from accessing our endpoint/network, removing the persistence by deleting the “test” user, and identifying the methods by which the threat actor was able to install it in the first place. We then could make sure that setuid binaries were reviewed and removed, and that no regular user on the endpoint, could run sudo commands.