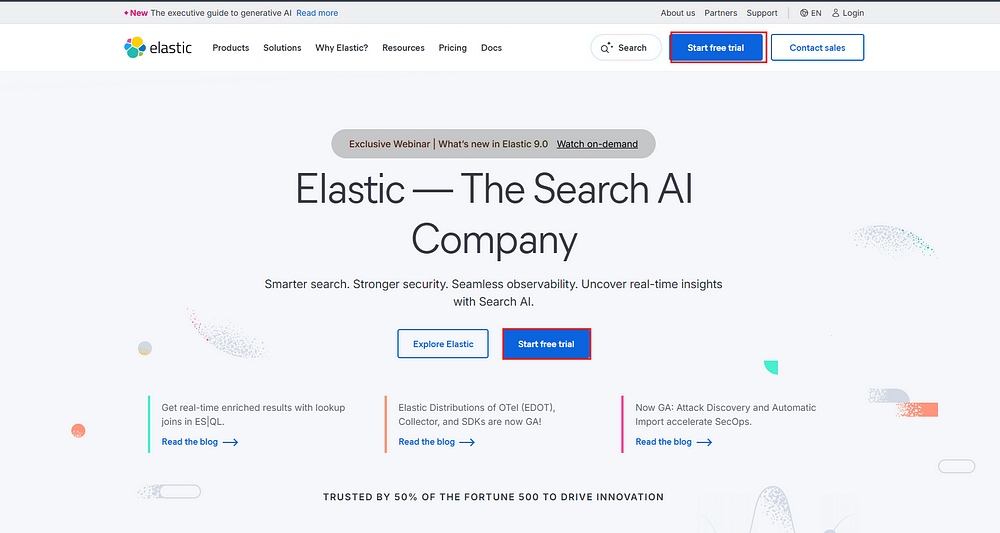
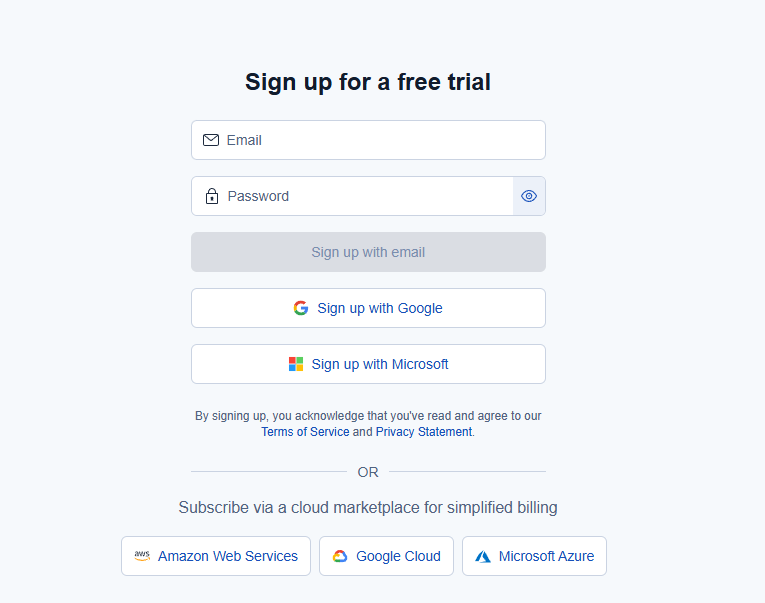
### **Elastic Setup**

This project entails the establishment of a complimentary trial on Elastic Cloud, followed by the deployment of an Elastic Agent on a Windows host for log generation purposes.

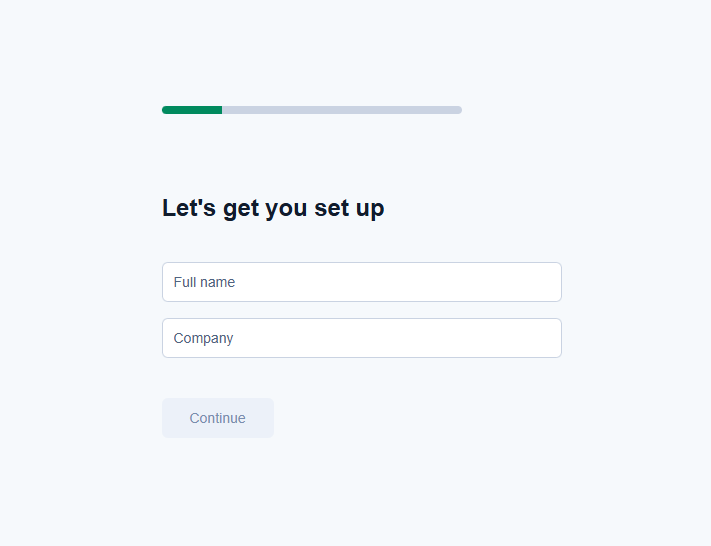
Initiate the process by navigating to<https://www.elastic.co/> and selecting the "Start Free Trial" option.



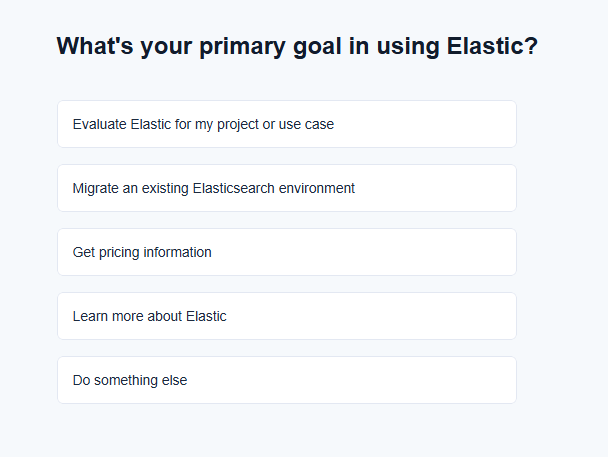
Subsequently, registration is to be completed using a valid email address and password.



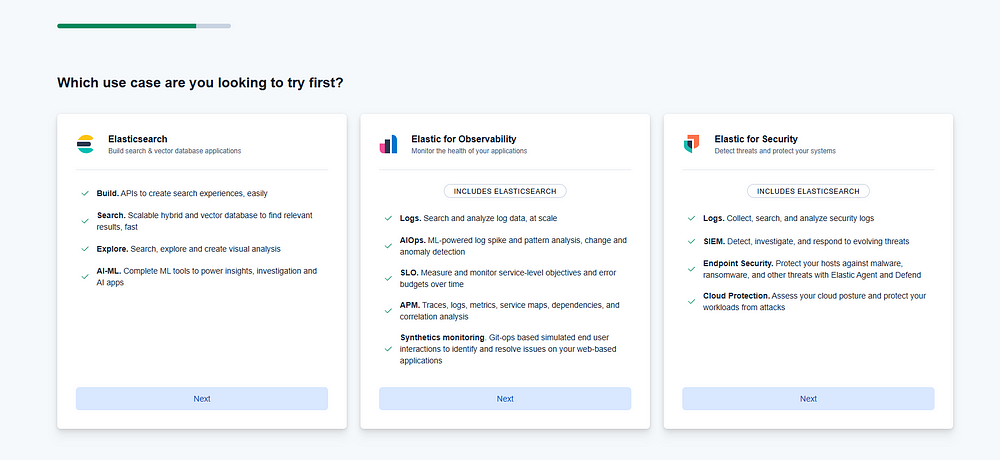
Upon completion of registration, please provide your full name and company details..



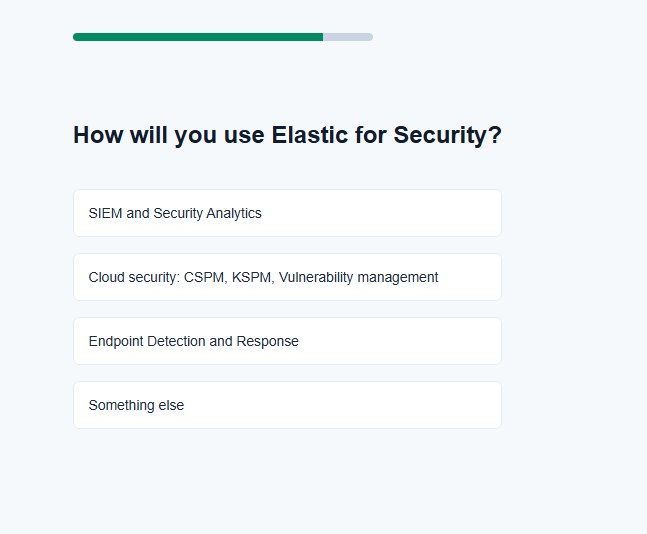
Subsequently, choose the option that most appropriately aligns with your specific requirements.



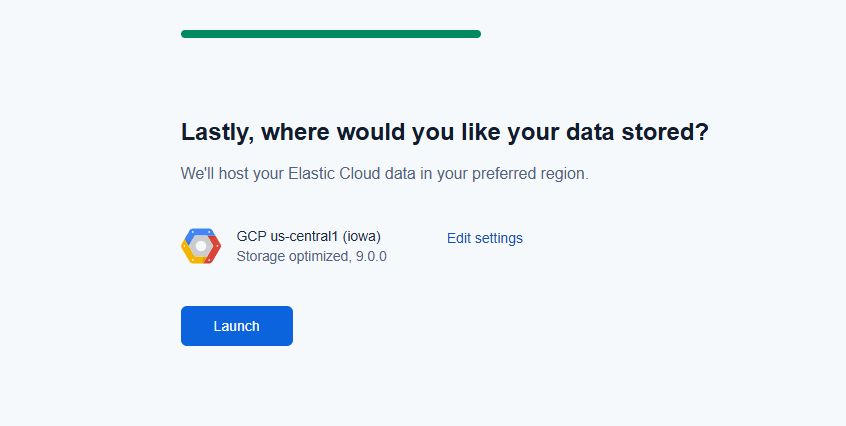
On the subsequent screen, select Elastic for Security.



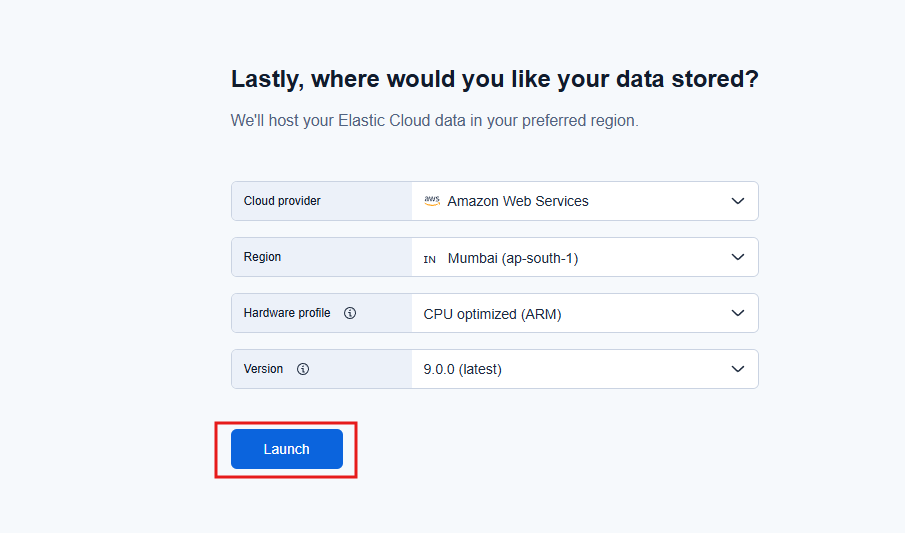
Subsequently, select the option that corresponds to your specific use case.



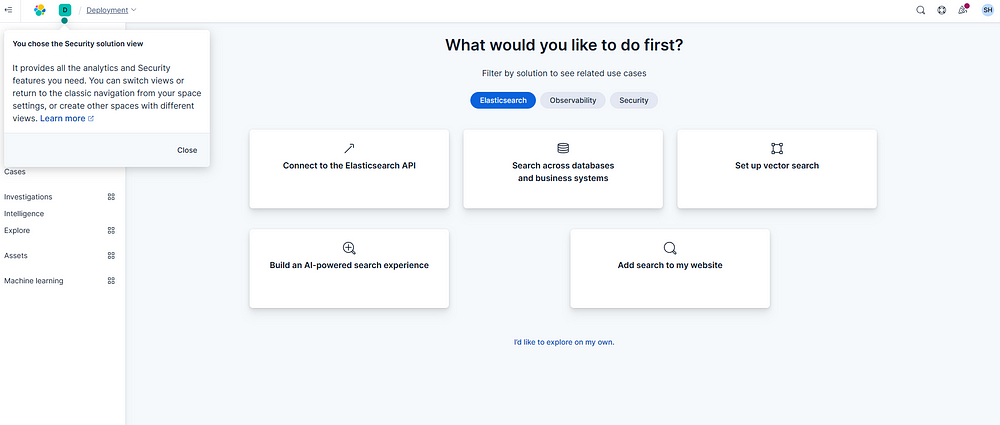
Subsequently, access the configuration modification options.



A cloud provider and location should be selected based on optimal criteria. The following outlines recommended preferences.



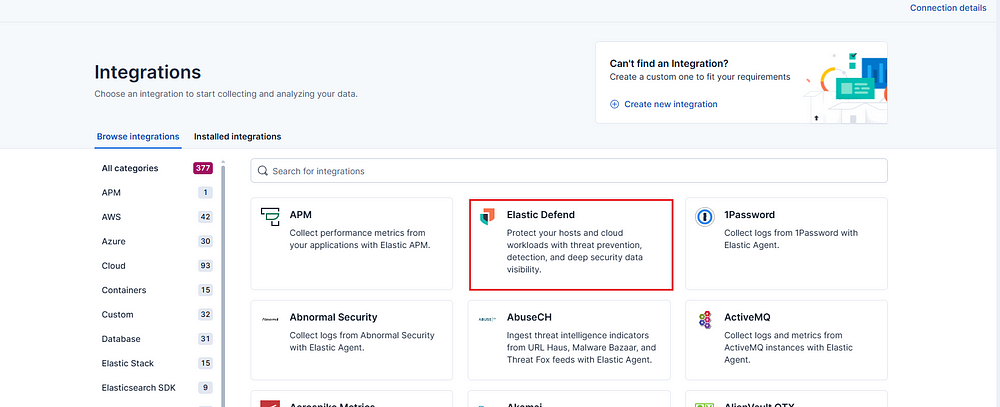
Initiate the launch procedure and allow several minutes for completion. Subsequently, the Elastic Cloud environment will be configured, culminating in the display of the succeeding interface.



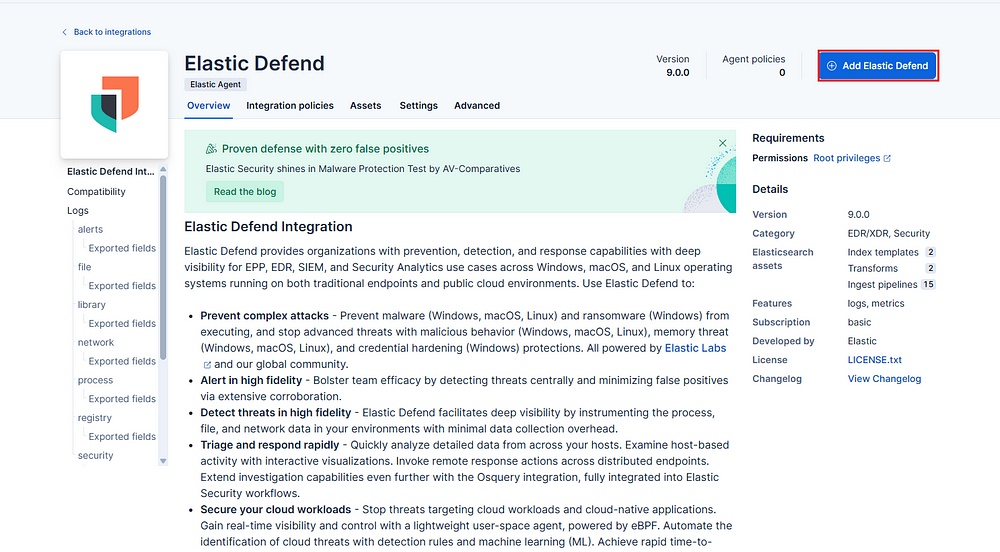
Navigate to the Management dropdown located at the bottom of the screen and select Integrations.



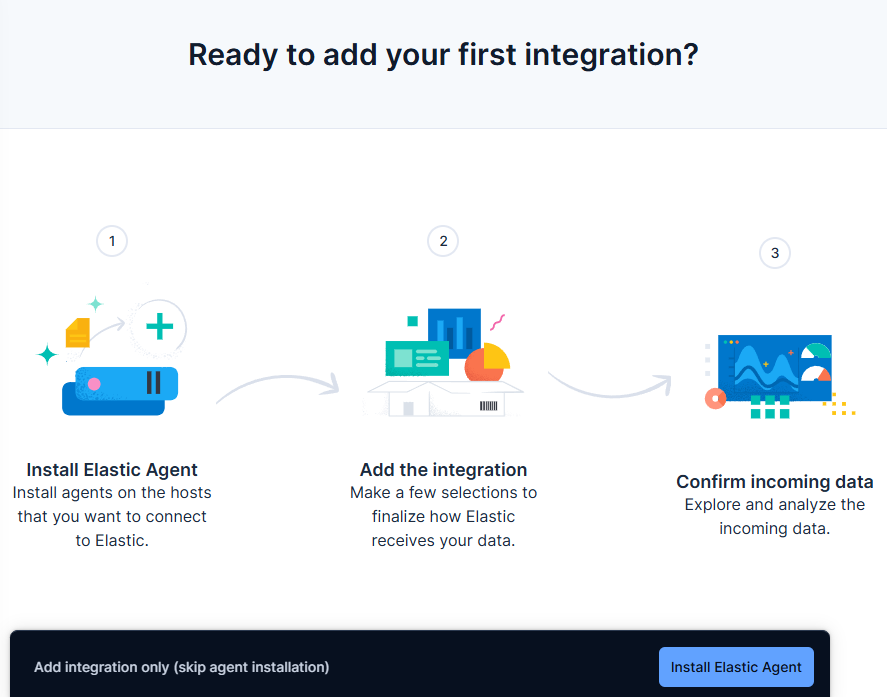
Subsequently, access Elastic Defend from the presented toolset.



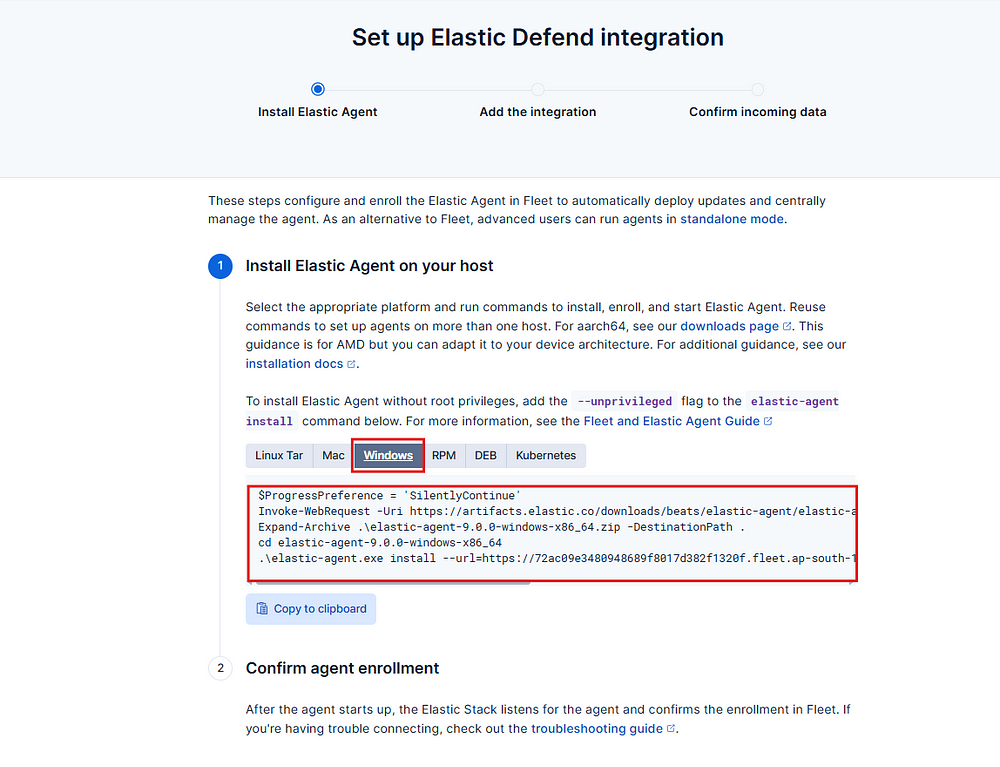
Subsequently, review the overview and select "+Elastic Defend".



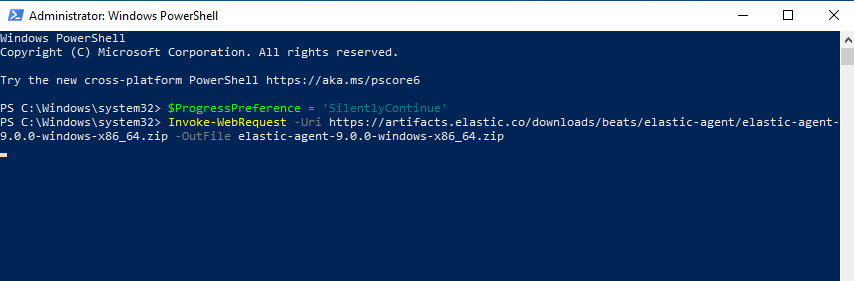
Following this, Elastic will provide instructions for setting up our integration. Select "Install Elastic Agent" at the bottom of the screen..



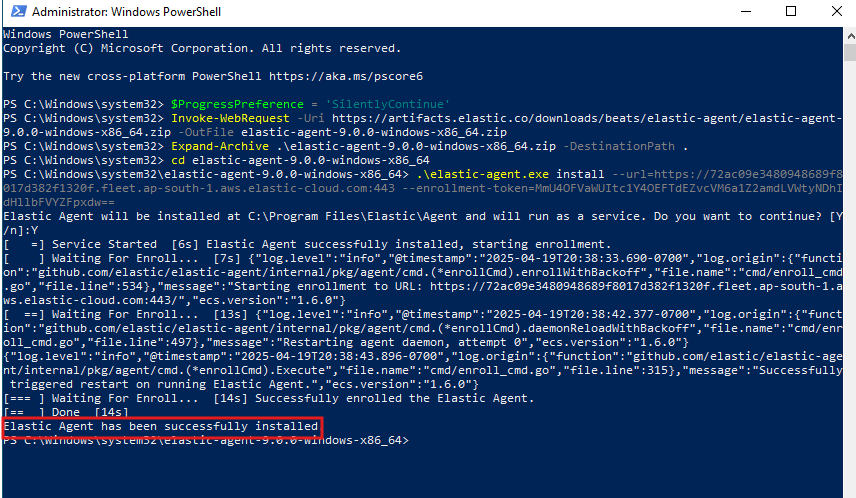
Subsequent to this, Elastic will provide instructions for installing the software across various platforms. As the installation is to be performed on a Windows operating system, the Windows option was selected, and the corresponding commands were copied.



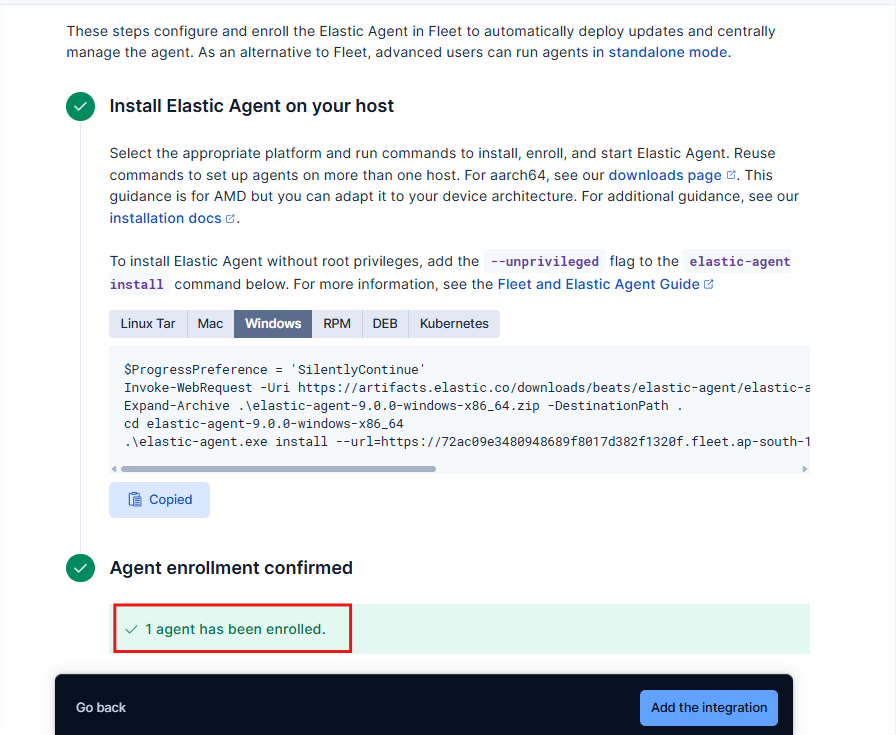
Subsequently, on Windows, launch a PowerShell window with elevated administrative privileges. Copy and paste the provided commands into the window, then execute them by pressing Enter. When the prompt for the Elastic agent path appears, confirm by entering 'Y' and pressing Enter.



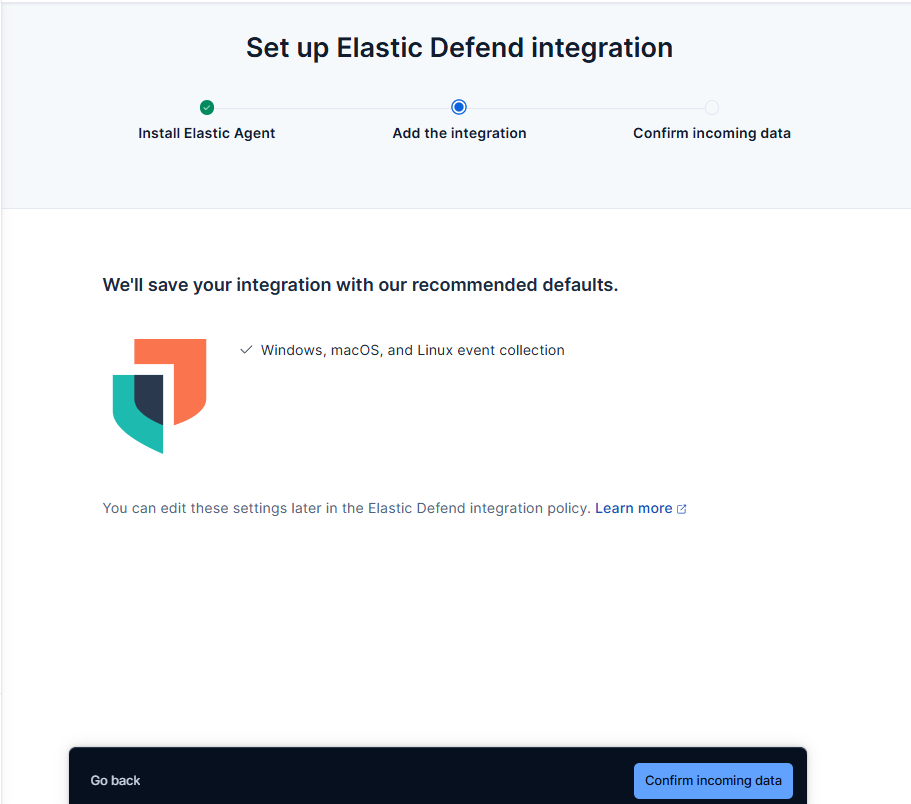
Following a brief installation period of approximately one to two minutes, the elastic agent deployment will be finalized.



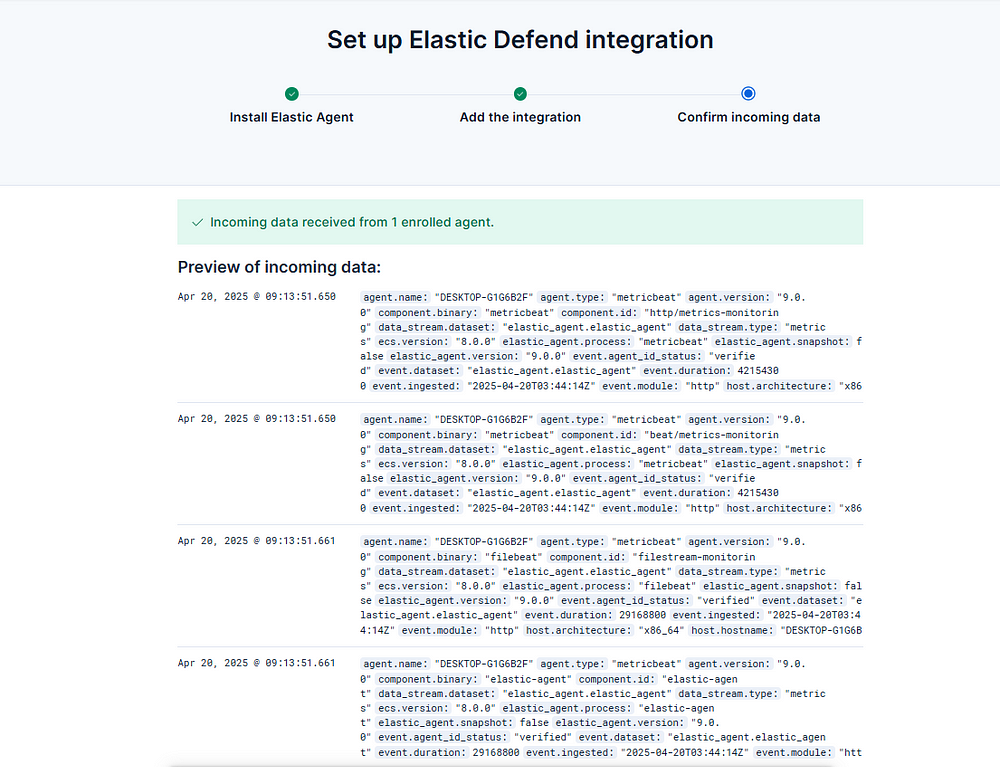
Within the Elastic Cloud interface, confirmation of agent installation is now visible.



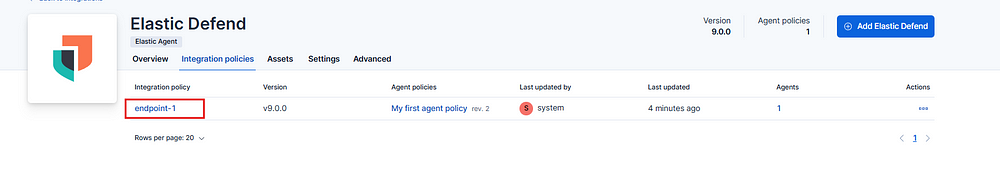
Kindly proceed by clicking the "Add Integration" button located at the bottom.



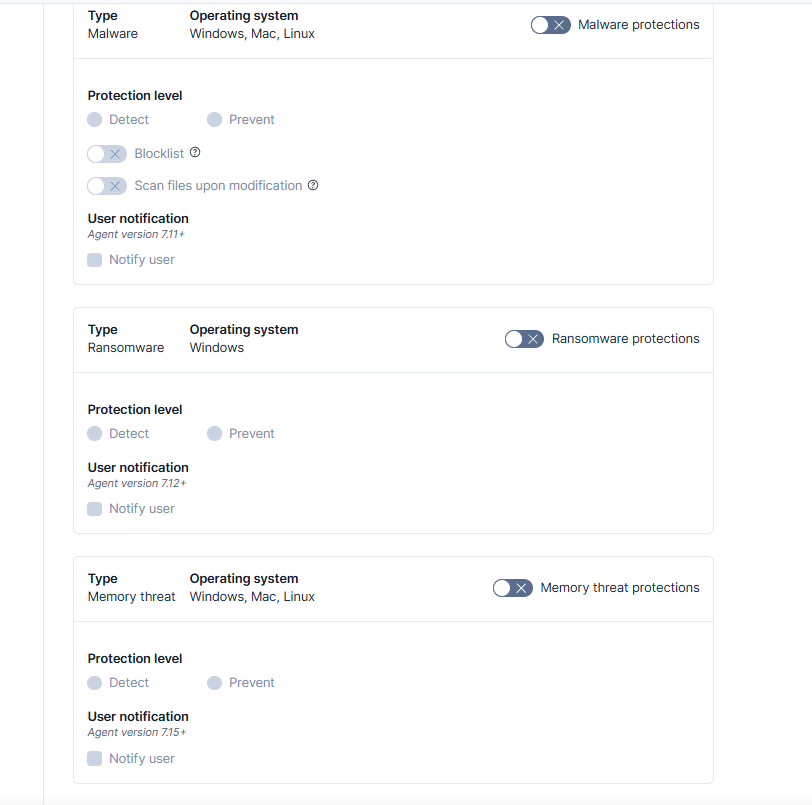
Subsequently, select "Confirm incoming data."



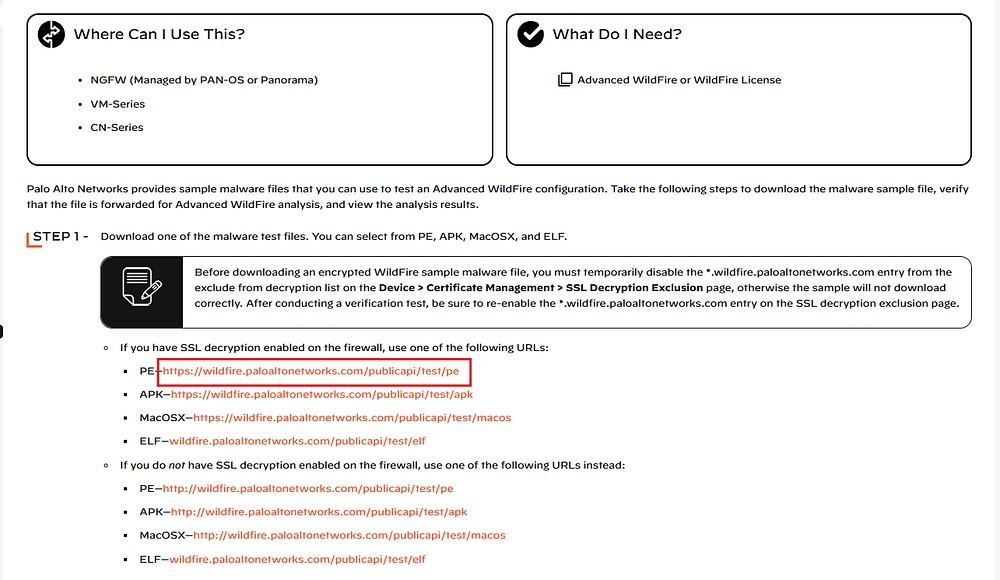
The preceding indicates the successful configuration of our agent and the receipt of data. Subsequently, one may proceed to the integration interface to modify the policy for the purpose of identifying and responding to various threats.



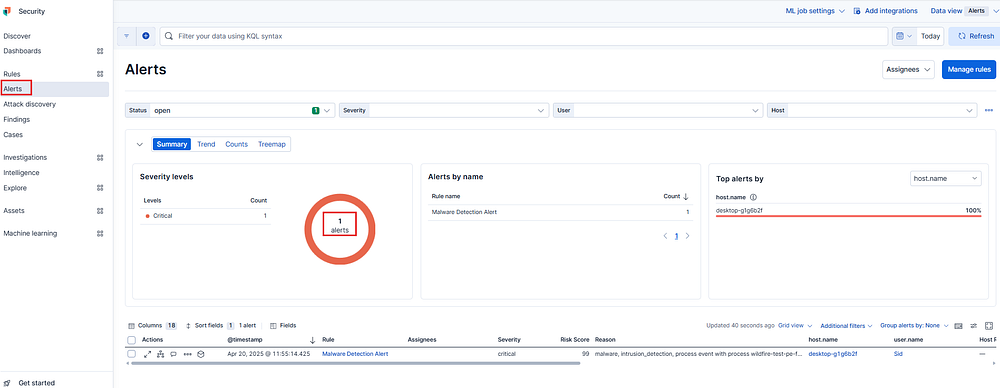
Navigate to the endpoint identified as "endpoint-1."



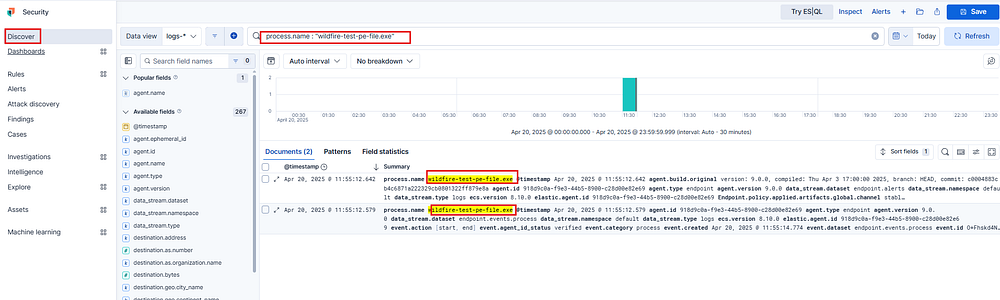
It is demonstrated that policies can be implemented to either identify or mitigate threats. To illustrate this functionality, a sample malware file, EICAR, can be downloaded for testing purposes from the following resource:<https://docs.paloaltonetworks.com/advanced-wildfire/administration/configure-advanced-wildfire-analysis/verify-wildfire-submissions/test-a-sample-malware-file>.



Execute the provided file within a secure, isolated environment. Subsequently, navigate to the alerts section of the Elastic Cloud platform.



The alert generation is evident above. Proceed to Discover and search for the respective program.



Observation of the generated logs confirms the successful operation of Elastic.