**Security Information Event Manager (SIEM)**

The purpose of a SIEM is to source all security events into one location. It is a platform that centralizes all the gathered logs which can be further analyzed within that platform. The logs gathered can be from Suricata, Syslogs, network logs, and firewall logs. Based on the events in these logs, the SIEM can highlight to the administrator of potential attacks or highlight suspicious access and see where it is coming from. While this project is focused on the Home Office network type of the SOHO network, it is worth mentioning as there are higher expectations of a SIEM being present in a small office. This project has various SIEMs that can be utilized in conjunction such as security onion and splunky enterprise. Splunky enterprise requires login information to gain access to the sixty day trial. Security Onion is a free SIEM setup with various types of installation versions to it.

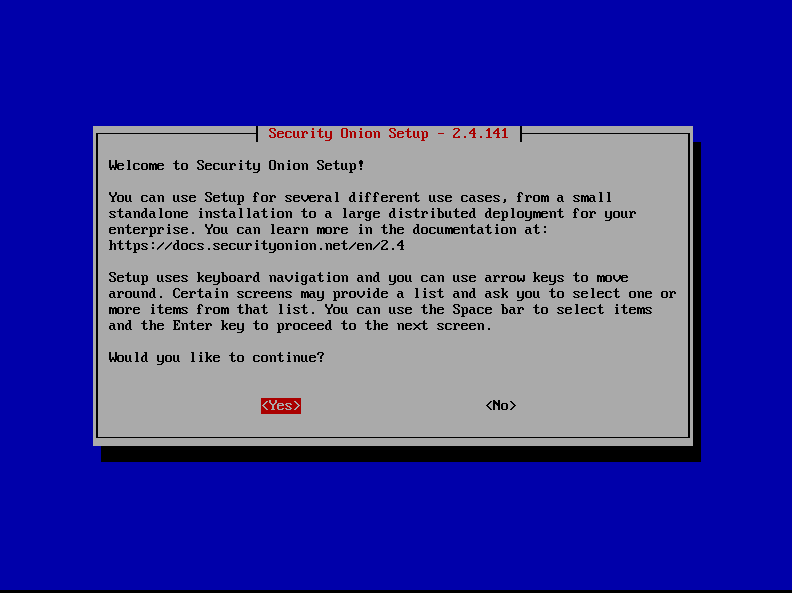


Figure 7: A screen capture of Security Onion setup on a virtual machine.