Creating & Running a SIEM

Created an agent using Elastic Cloud to monitor NMAP scans happening on my Kali Linux Virtual Box. Installed the agent on my Kali Box network to monitor for all scans. Set up rules, alerts, and case generation based in my SIEM based on the Elastic Agent detecting a NMAP scan.