Build an Elastic SIEM Home Lab

Introduction

In today's ever-evolving threat landscape, organizations require robust security information and event management (SIEM) solutions to effectively detect, analyze, and respond to cyberattacks. This project delves into integrating the powerful capabilities of a SIEM platform with the penetration testing expertise of Kali Linux, utilizing the scalability and accessibility of the Elastic Cloud.

Our project specifically focuses on integrating Elastic Stack, a popular open-source SIEM platform, into a Kali Linux environment. This integrated approach leverages the strengths of both tools:

- **Kali Linux:** Provides a comprehensive arsenal of pentesting tools, allowing us to simulate security events like successful Nmap scans.
- **Elastic Stack in Elastic Cloud:** Offers a central hub for collecting, analyzing, and visualizing security data, enabling us to detect and investigate potential threats triggered by these events.

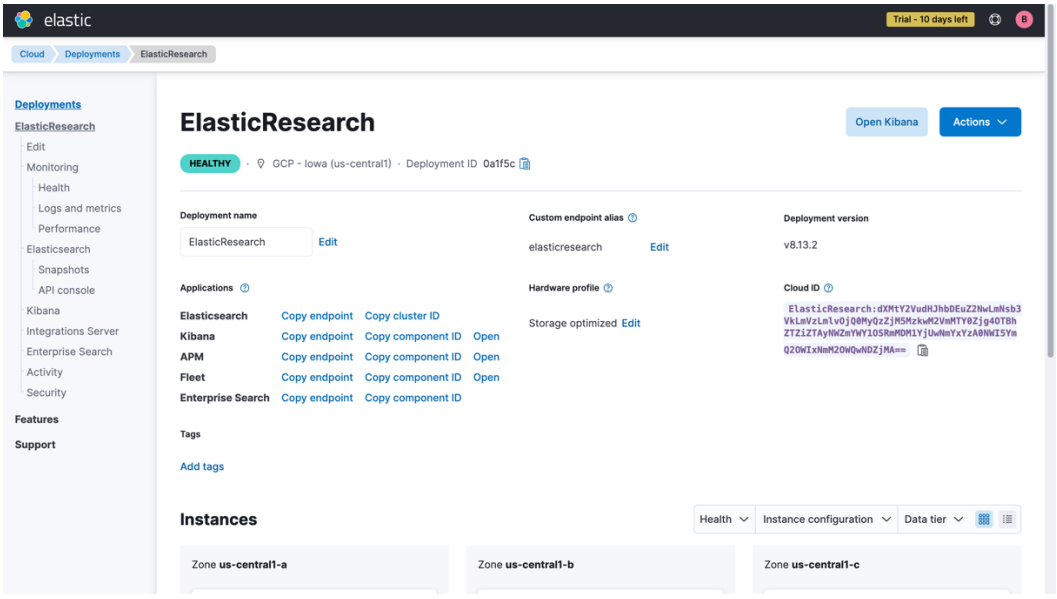
Through this integration, we'll establish security rules within the SIEM platform to identify anomalous activities, such as successful Nmap scans on our network. These rules will trigger alerts, notifying security personnel of potential intrusions. Additionally, we'll construct informative dashboards within the SIEM for real-time visualization of security incidents, aiding in efficient analysis and response.

By successfully integrating and configuring these elements, this project aims to demonstrate the effectiveness of SIEM solutions in detecting and responding to security threats. This practical exploration will equip us with valuable skills and insights into building and utilizing a robust security monitoring system.

Project Phases

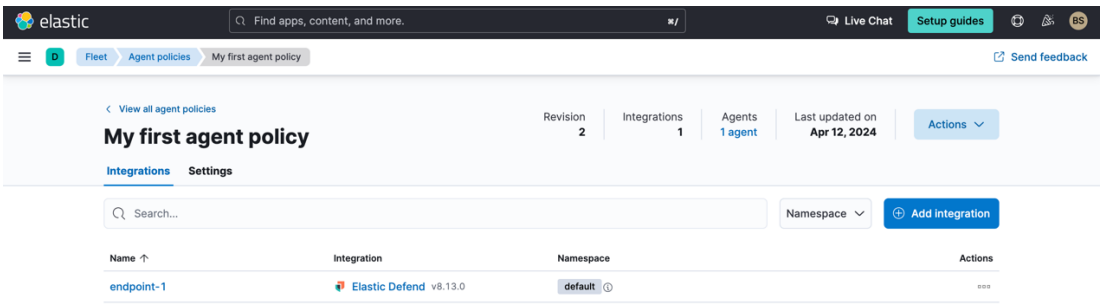
1) Elastic Cloud Deployment

I have created the Elastic cloud Deployment named Elastic Research.



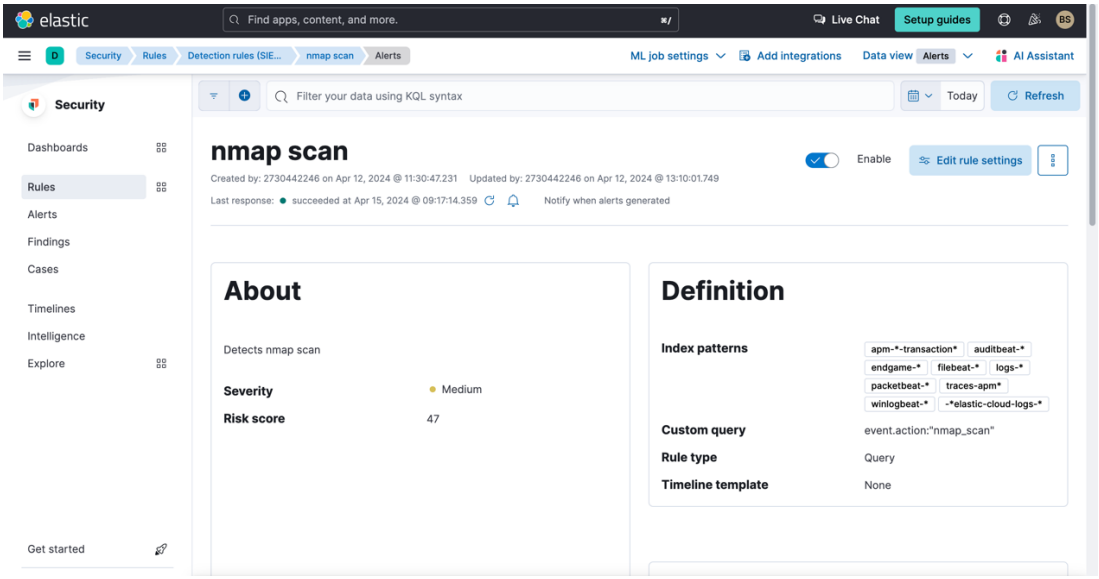
2) Elastic Cloud Integration

After deployment, I have added Integration of Elastic Defend. Elastic Defend stands out as a comprehensive Endpoint Detection and Response (EDR) solution. It offers a powerful combination of preventative measures, threat detection capabilities, and response options, all bolstered by security analytics. This integration goes beyond basic data collection, providing deep visibility into your system's activities. Successfully deploying Elastic Defend on Kali Linux empowers you to monitor processes, file changes, network activity, and more, granting you a clear picture of potential security risks. This integration seamlessly blends with Elastic Security workflows, including the Osquery integration, further enhancing your investigation capabilities.



3) Setup Detection Rule in Elastic

After successful integration of elastic Defend, it requires a Detection Rules for SIEM. Here I have created a nmap scan detection Rule in which, every nmap scan taken place into system will be detected. The query is *event.action:"nmap_scan"*. This rule will constantly monitor any event actions in Kali Linux.



4) SIEM Dashboard

I have Developed a custom dashboard in Elastic SIEM to visualize security events. This dashboard will display all the security events & Alerts integrated with Detection Rule. In this scenario, all the security events in Kali Linux with action of Nmap scan will be detected and visualized in SIEM dashboard.