Christian Somoya

Vulnerability Management Application

https://github.com/Csomoya/sql-project

JOB DESCRIPTION

1. The job I selected was Data Analyst at Crowdstrike. I selected this job due to the skillset I have developed at LMU as data analyst. However, I also am very interested in Cybersecurity. Due to this, I wanted to work in a job that I can further hone both skillsets. For my career, I would love to work in cybersecurity. I know that I may not be able to work as a security analyst right when I graduate, but utilizing my data analyst skills to get to this point feels more realistic. This particular job mentions Falcon Complete, which is Crowdstrike's XDR. I have experience working with Microsoft's XDR. I thought it would be cool to take a closer dive into the services offered by Crowdstrike and compare it to Microsoft's.

PROBLEM

2. One problem I plan to solve is vulnerability management for applications. Companies are generally made aware of new patches through advisory boards. However, this information is not curated specifically for that company. That patch or vulnerability that they are alerted for may be for a product that doesn't affect them. Some companies may only want to be made aware of these for specific products, too. I want to demonstrate the feasibility of building a service where companies could get a curated look at advisories. The dashboard would be very informative, showing the frequency of patches for one software used vs. others.

DATA SOURCES

3. VMWare is a very popular cloud computing and software provider. They also provide API's for Advisory. For the second, I would like to make a web scraper to grab information from the Known Exploited Vulnerabilities catalog on CISA. Both of these sources are very relevant and up to date. They are managed continuously.

SOLUTION

Using this data, I plan to only list vulnerabilities for specific vulnerabilities or services. For example, I may want to make a visualization about the number of known vulnerabilities for iOS vs Android. Another idea I had is to filter vulnerabilities based on specific constraints, such as whether or not a company might use that service.