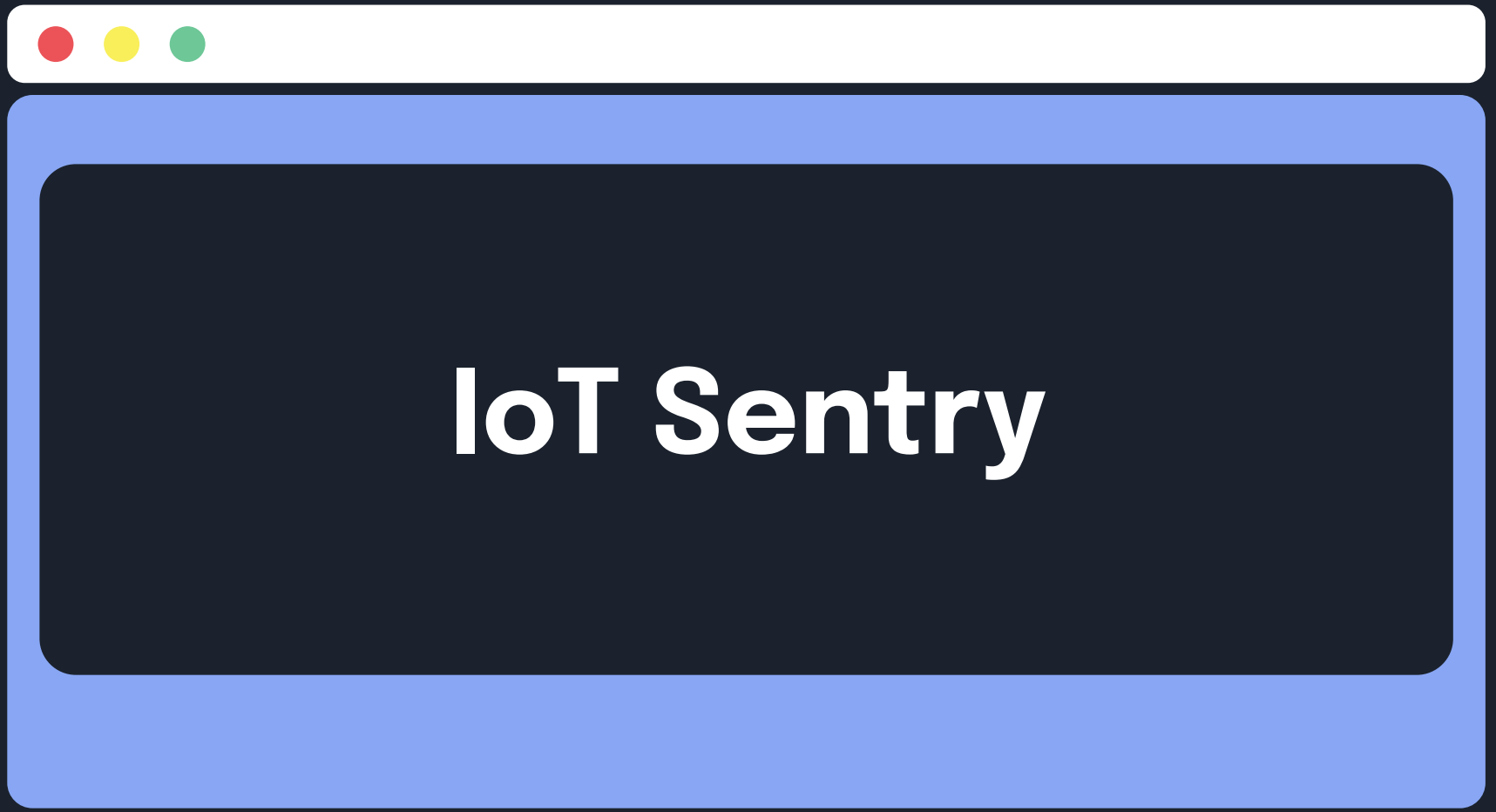

IoT Sentry

What is IoT Sentry?

IoT Sentry is a system that is able to passively monitor and analyze devices on a network.

To do so, the system is fed pre-recorded PCAPs in order to perform asset identification with an accuracy of at least the vendor of the device. It will also attempt to reason the likelihood of an unknown device being an IoT device as well as a credibility score based on if it is malicious or not.

IoT devices as well as other embedded devices are the main targets for identification on a network.

Motivation

Identifying devices on a network can be challenging because not all devices are directly correlated to their network card.

Asset identification is essential for security in an enterprise or critical environment.

Identification can help aid in discovering a threat actor's device or shed light on an unknown device on a large network.

Customer Discovery Process

- Ask for an initial list of requirements, with informed questions based on an understanding of the project goals.
- If requirements cause problems, discuss those issues with the sponsors and revise the requirement set if necessary.
- Periodically receive updated requirements from sponsors and revise requirements accordingly.

How Requirements Changed

Initially, IoT sentry was going to capture, filter and update real time as packets came over the wire.

Instead, we have transitioned to a pcap file approach where the capture happens separately and once completed is stored in a packet capture file (pcap).

Technologies Used

Wireshark: A open-source packet analyzer

Zeek: A passive, open-source network network traffic analyzer tool.

Kibana: An open-source data-visualization dashboard for Elasticsearch.

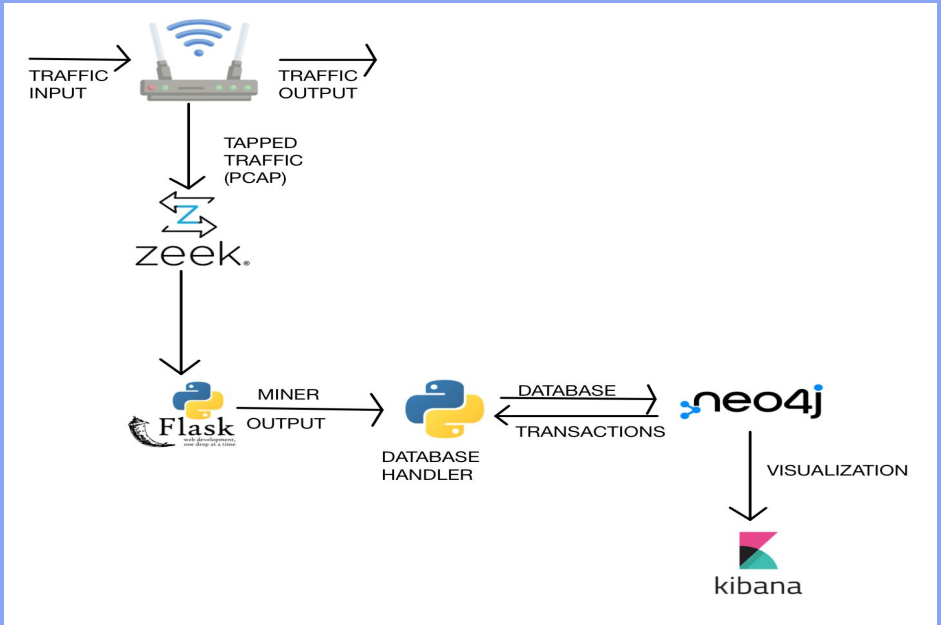
Docker: A platform for developing, shipping and running applications.

Neo4j: A graph database management system to build and visualize graph databases.

Flask: A micro web-framework written in Python.

Design

High Level Design

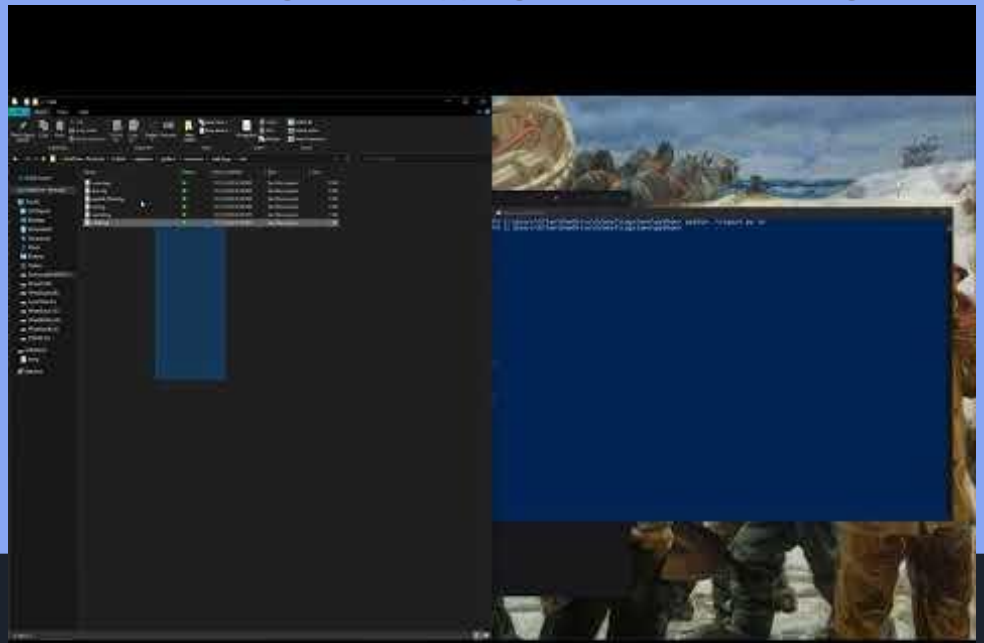


Justification

- Using Zeek and Wireshark for packet capture allows us to capture packets and nicely format them for export in one component.
- Python database handler allows us to keep the database protected, so that only one single piece of the application can modify it.
- Flask allows us to create a very API interface between the database handler and any other applications that might want to communicate with it.
- Neo4j was chosen for the database because it's non-relational, so can easily the data restructuring that will happen as the application grows.
- Kibana is great as a data visualization tool for this project because it is naturally designed to handle the types of data that we're working with.

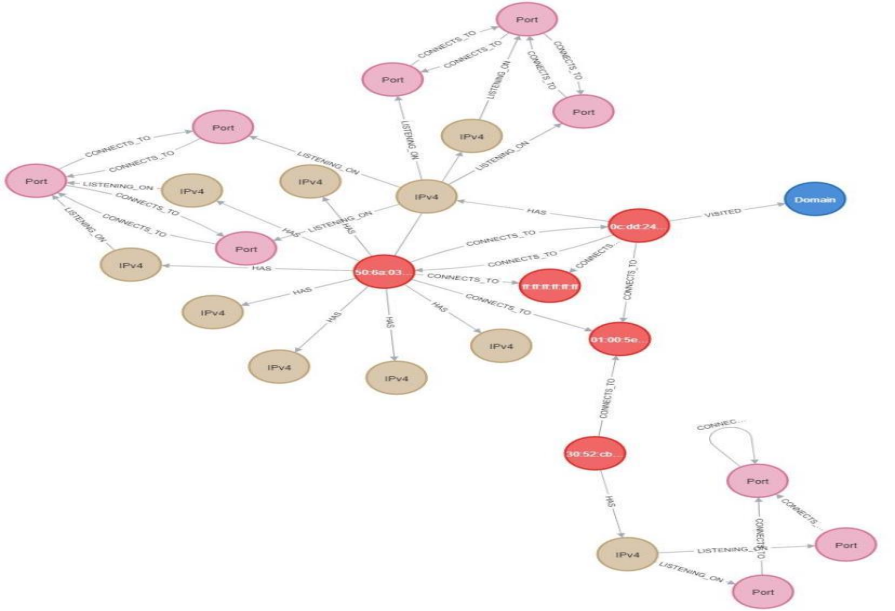
Results

In the link layer we can take a pcap, process it through Zeek and pull any reserved MAC address prefixes from the IEEE. This gives a stepping stone to establishing credibility of a device.



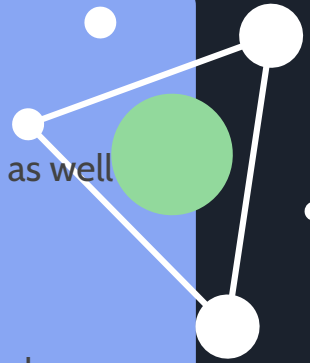
Results

A zoomed in version of the graph generated by Neo4j for a PCAP file.



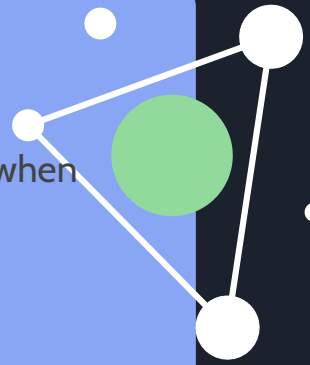
Value Created

- IoT Sentry will allow for easier, automated network analysis for network administrators as well as security contractors
- This automation will reduce the manpower needed to conduct regular auditing
- Financially, audits are expensive and for IT administrators avoiding them with more regular auditing aided by IoT sentry they can avoid those expenses. For contractors, it allows them to complete the same job, with less manpower and faster.
- Societally, providing this tool to people less experienced with network analysis gives them a tool to do their own network audits without requiring an intense manpower commitment and underlying understanding of networking and network packets.



Lessons Learned

It is critical to allow yourselves to downscale and focus on core competencies of the project when certain unnecessary features are causing issues.



Future Plans

- Flesh out credibility scores to give a usable likelihood factor to each device on a network based on the likelihood of it being an IoT or embedded device.
- Extend credibility scores to a malicious score to identity possible malicious devices based on packet analysis and alter the user to these devices
- Simplify operation for the user