Endpoint Detection and Response

4/2/2025

OVERVIEW

I am showcasing the importance of endpoint security management and how to respond to possible active threats on a production client machine. Included in this project is an agent installer, a configuration document explaining server requirements and install guidance, and a Web Interface to interact with the server and fit into your daily routine, no cloud services or third-party data collection; you host the service and maintain everything in-house.

GOALS

1. Design the Agent with encryption in mind
2. Design the Server with many connections in mind
3. Design the Web interface hosted on the Server
4. Track Progress

SPECIFICATIONS

The programming languages used to build this project aim to lean on Python and c++ the most, as these are highly popular and well-known for debugging issues, and adding open source customization.

MILESTONES

Day 0 - Gathering the Ground

Begin the project by documenting and tracking progress as well as development goals to maintain within a weekly schedule in mind.