MICHIGAN STATE UNIVERSITY

Beta Presentation

Predicting Malware Command and Control Channels

The Capstone Experience

Team Vectra

Ettore Campriani
Aidan Erickson
Nathaniel Ferry
Sam Kwiatkowski-Martin
Muhan Luo
Aidan McCoy

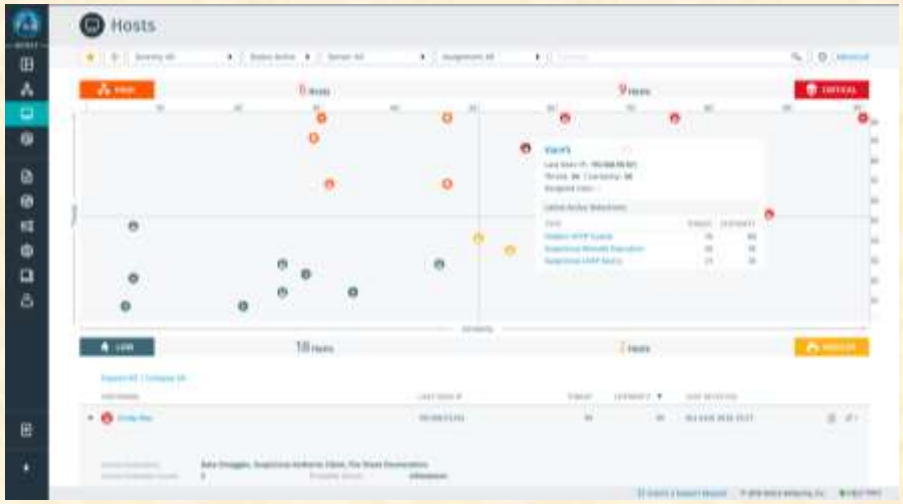
Department of Computer Science and Engineering
Michigan State University

Spring 2023

From Students…
…to Professionals

Project Sponsor Overview

- Sponsor Overview
  - Cybersecurity threat detection and prevention
  - Products built on machine learning and artificial intelligence

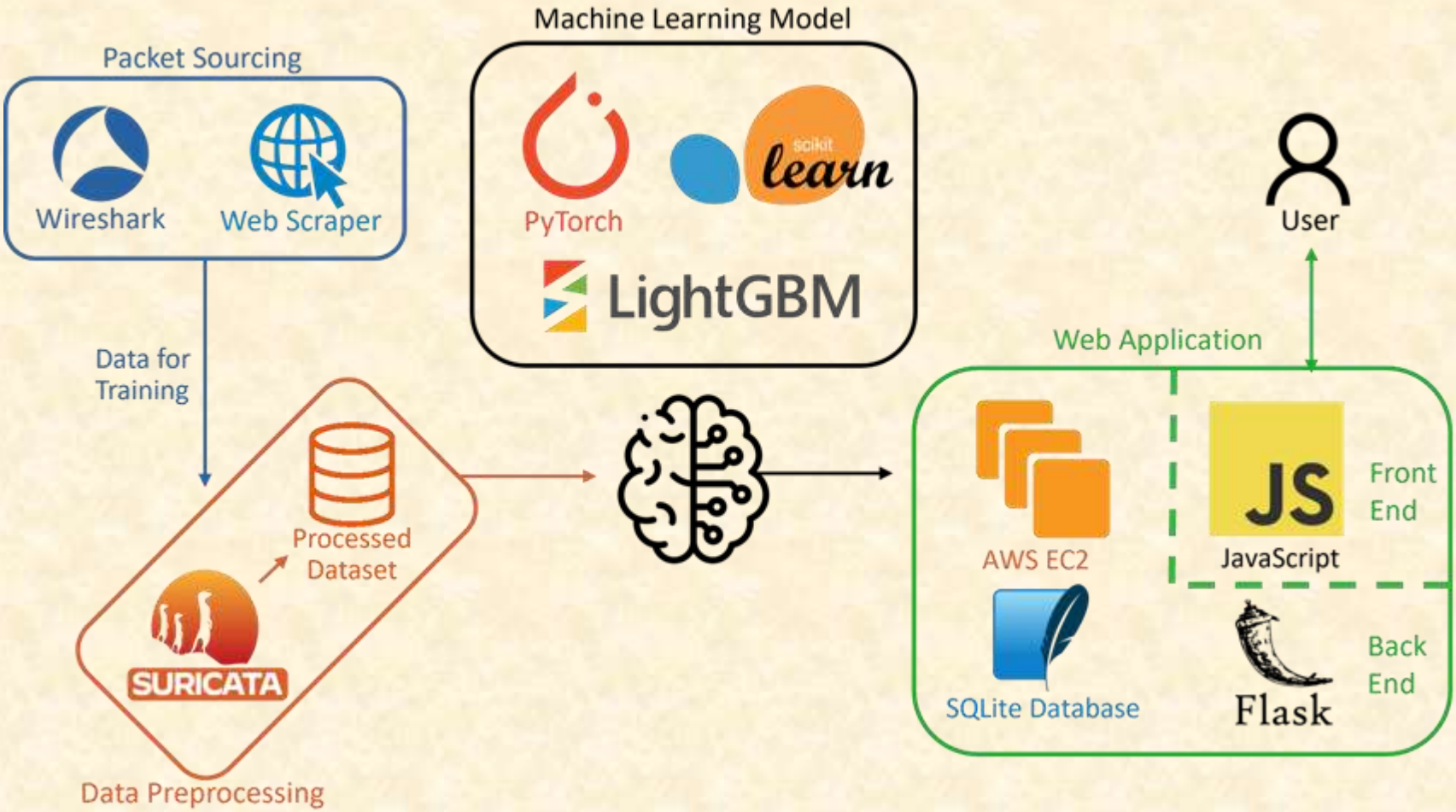


VECTRA®

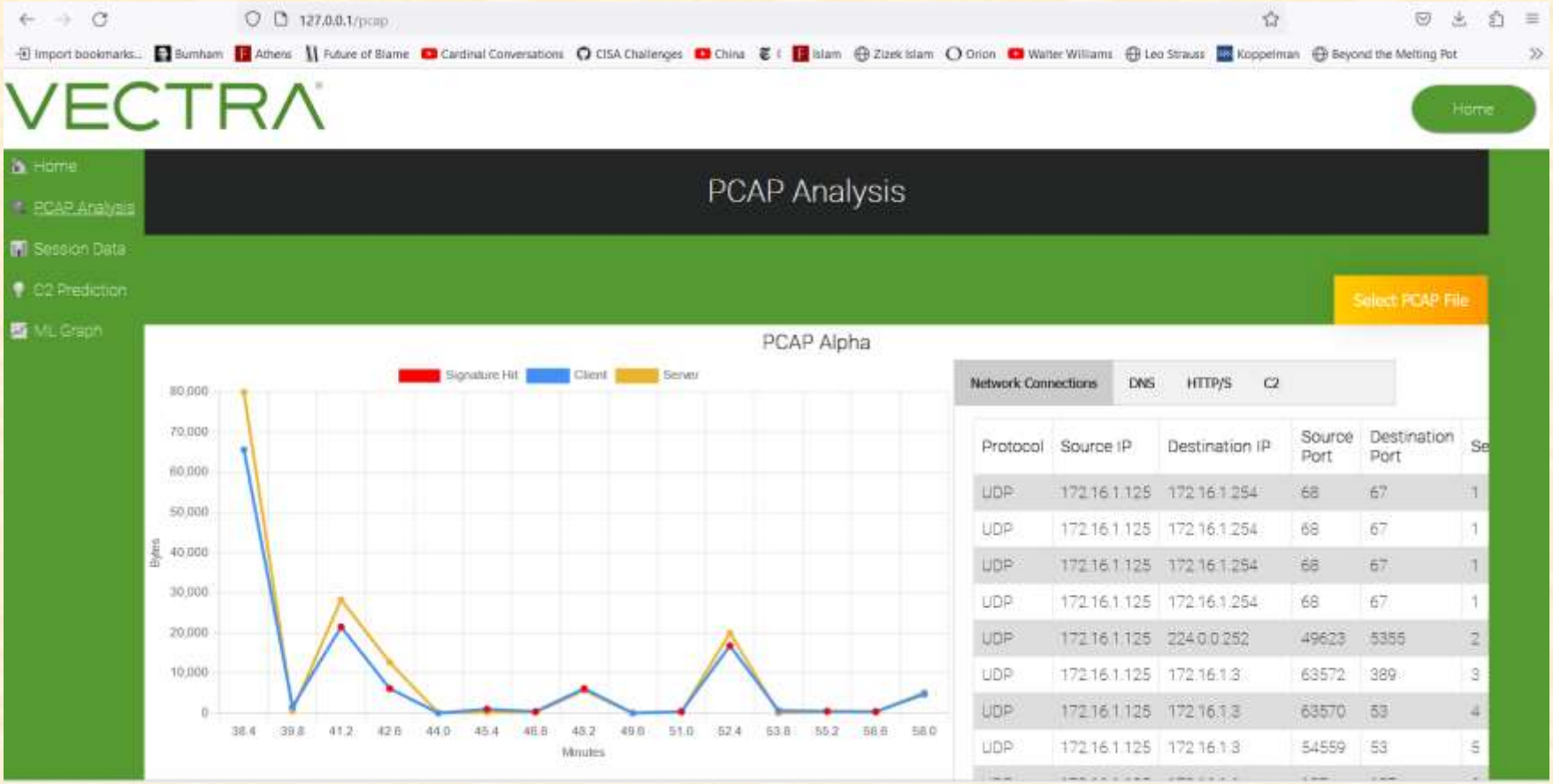
Project Overview

- C2 channels
- Signature-based intrusion detection
  - Utilizes previously recorded attack patterns
  - Not effective against novel techniques
- AI-based intrusion detection
  - Utilizes pattern recognition on network data
  - Needs data
- Goal: Combine Signature-based and AI-based intrusion detection to detect C2 channels

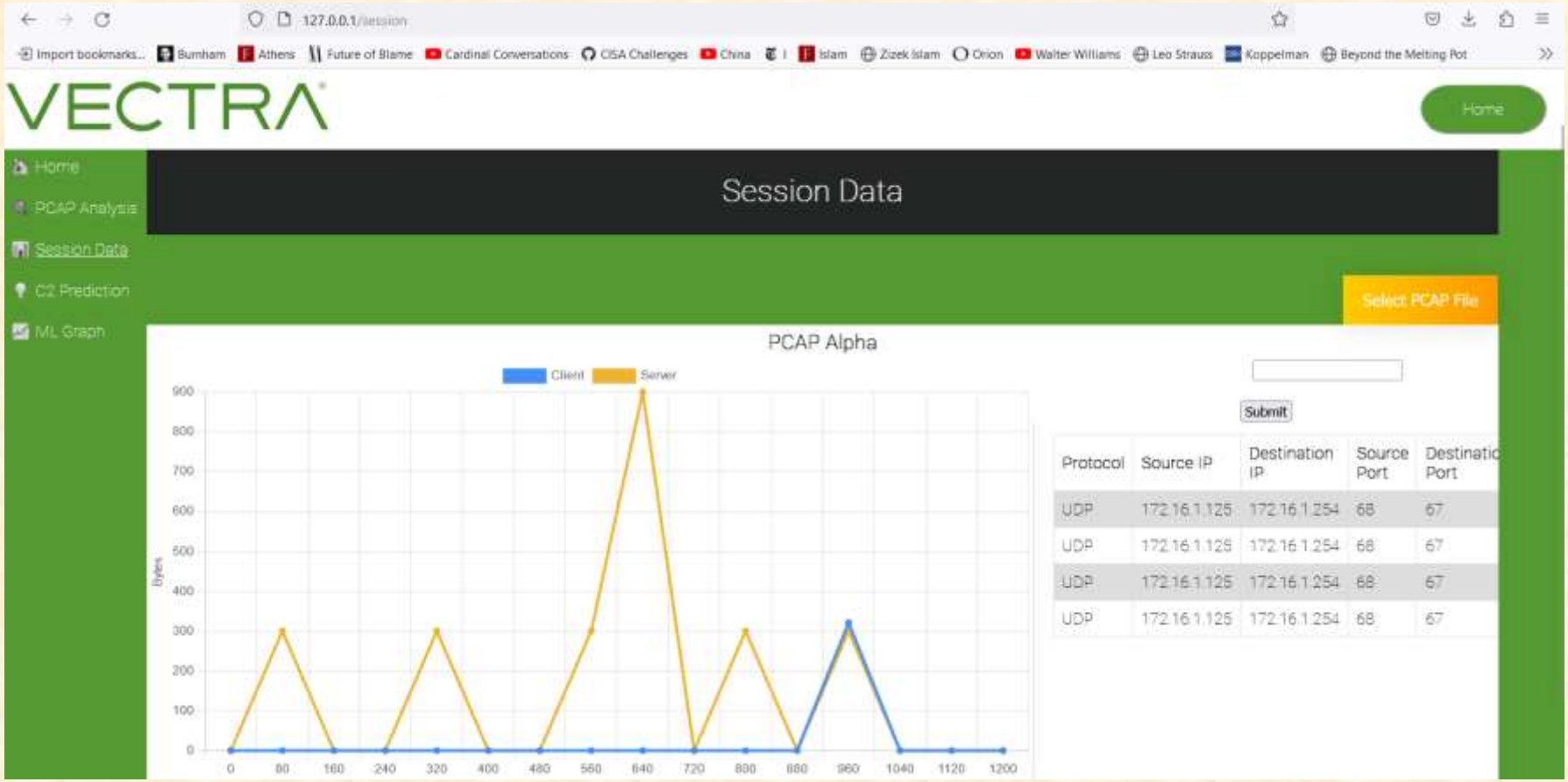
System Architecture



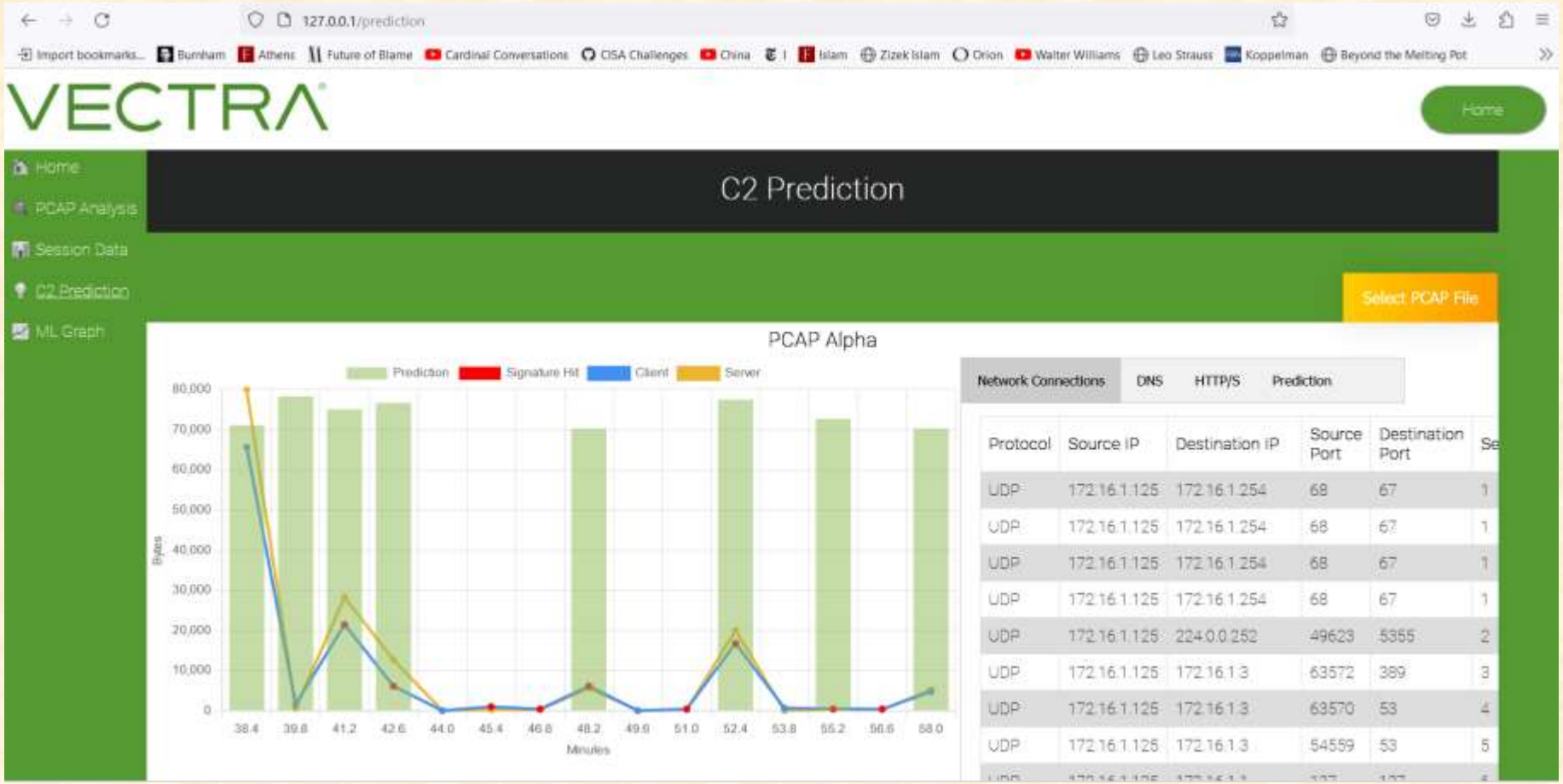
PCAP Analysis Page



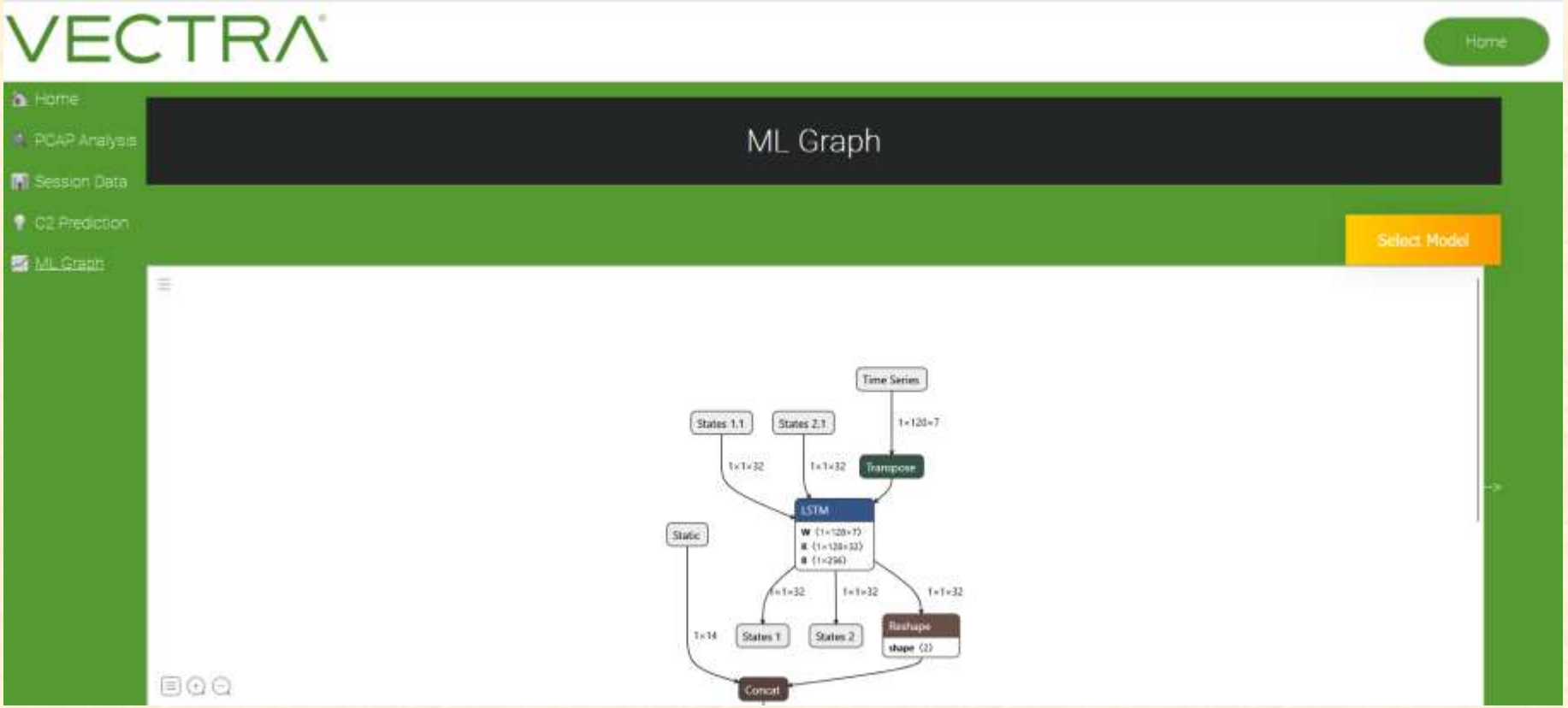
Session Data Page



C2 Prediction Page



ML Graph Page



What's left to do?

- Features
  - N/A - Feature complete
- Stretch Goals
  - Threat map
  - Website table pagination
- Other Tasks
  - Improving website CSS
  - Optimize website queries

Questions?