

MICHIGAN STATE

U N I V E R S I T Y

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

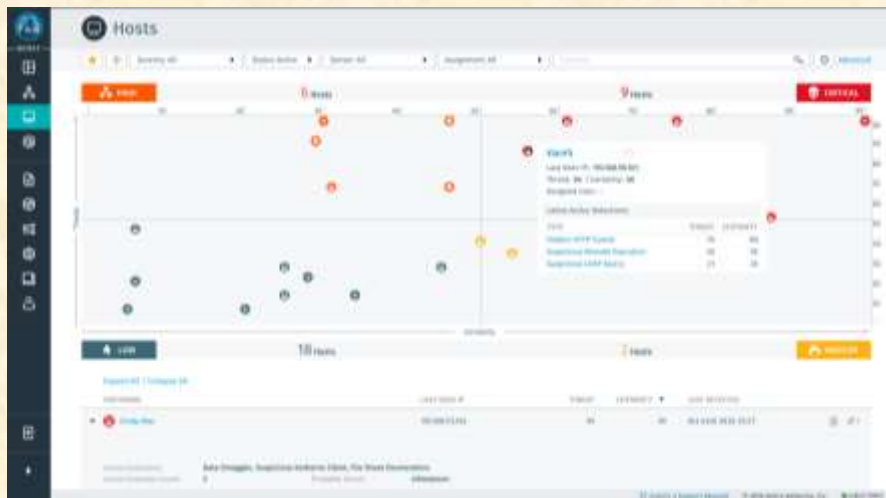
Spring 2023



*From Students...
...to Professionals*

Project Sponsor Overview

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



VECTRA®

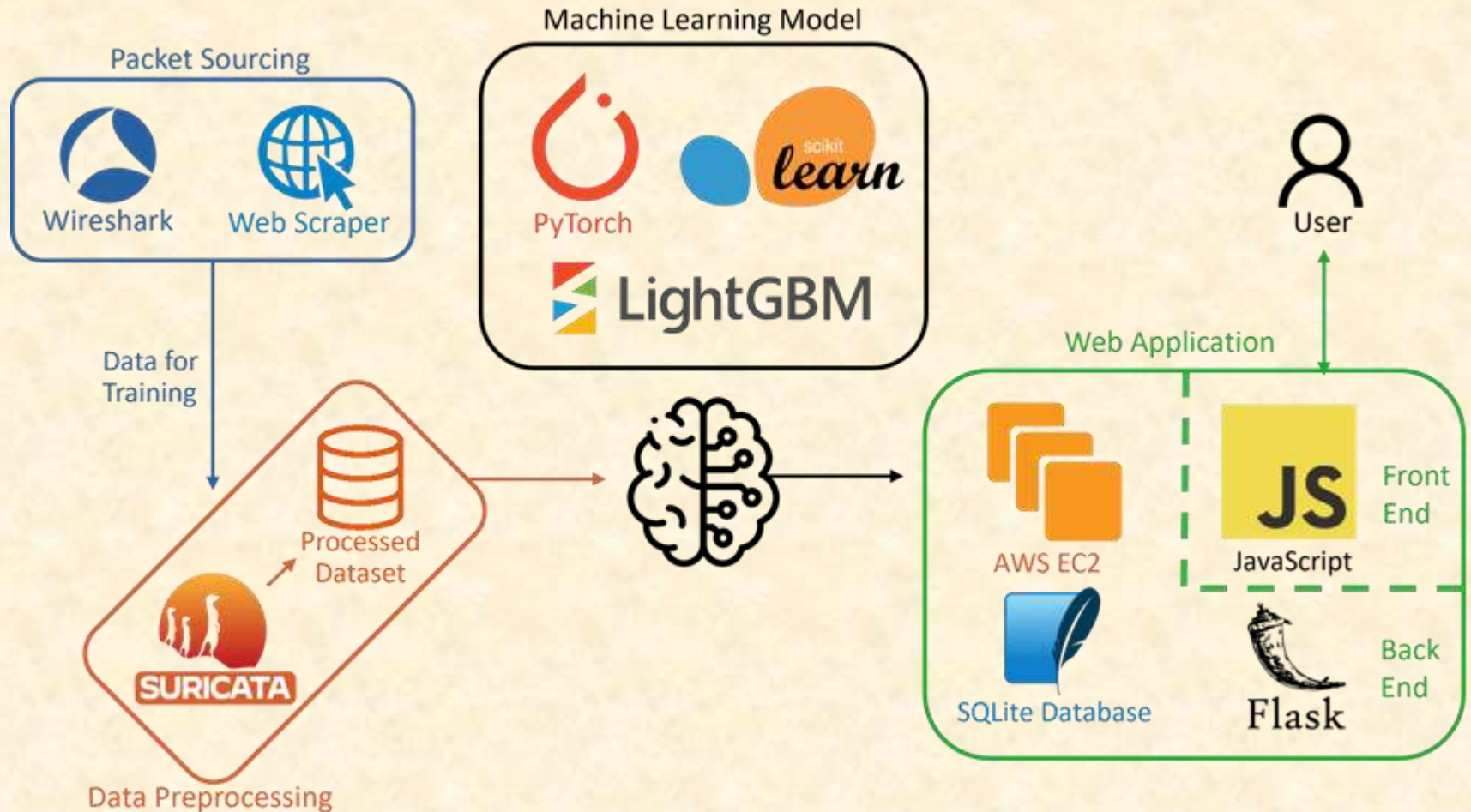


Project Overview

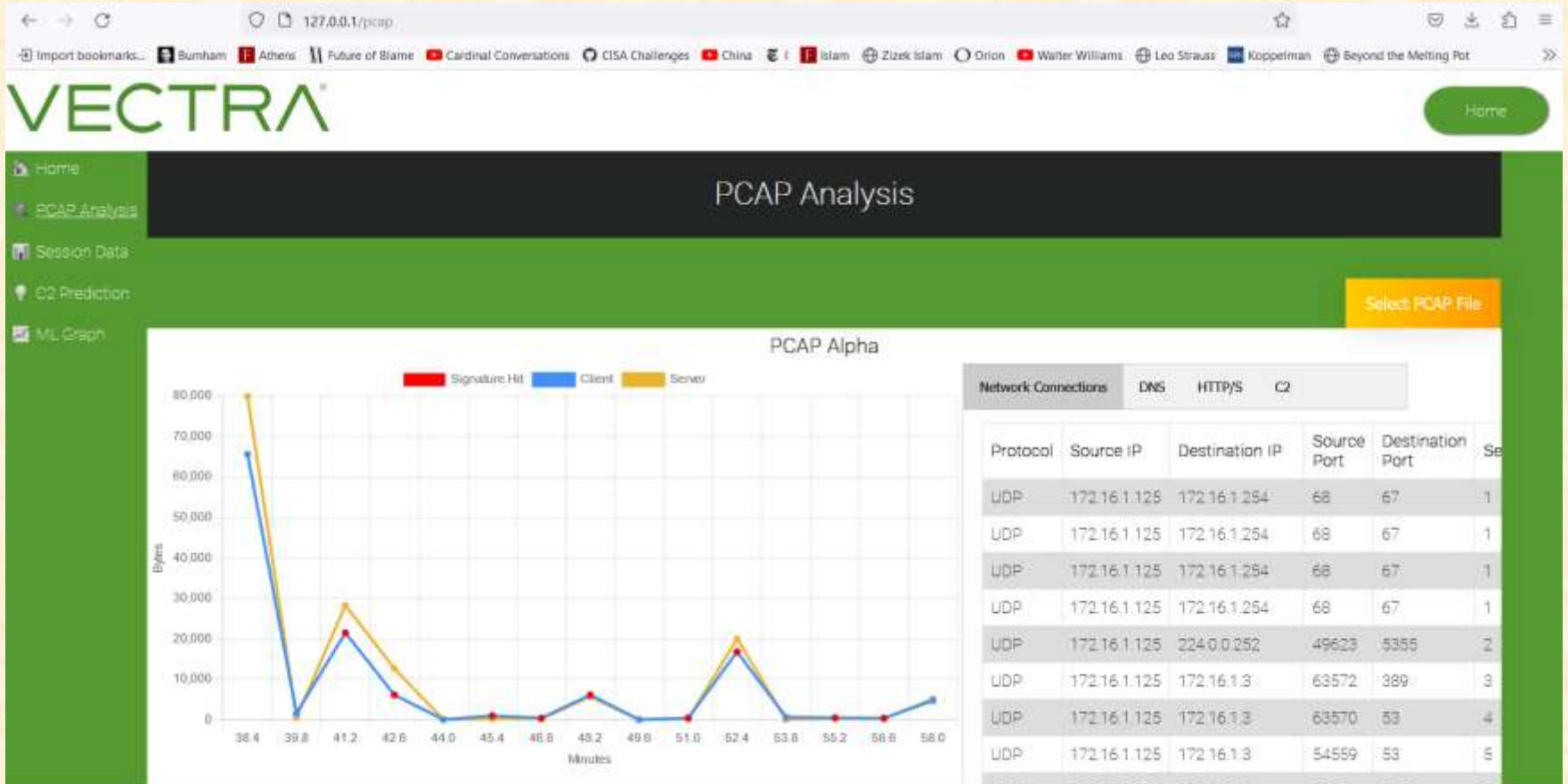
- C2 channels
- Signature-based intrusion detection
 - Utilizes previously recorded attack patterns
 - Not effective against novel techniques
- AI-based intrusion detection
 - Utilizes pattern recognition on network data
 - Needs data
- Goal: Combine Signature-based and AI-based intrusion detection to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



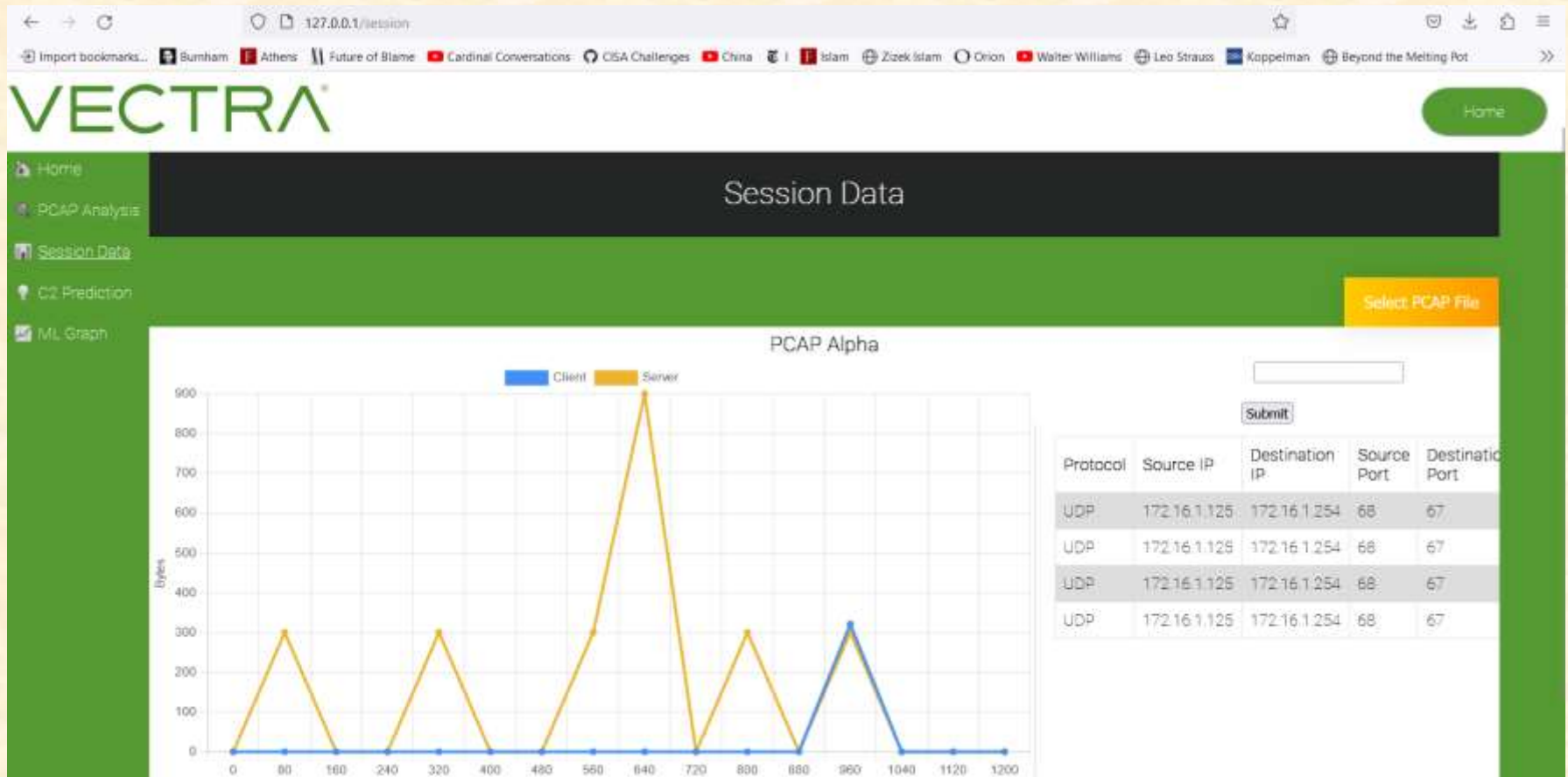
System Architecture



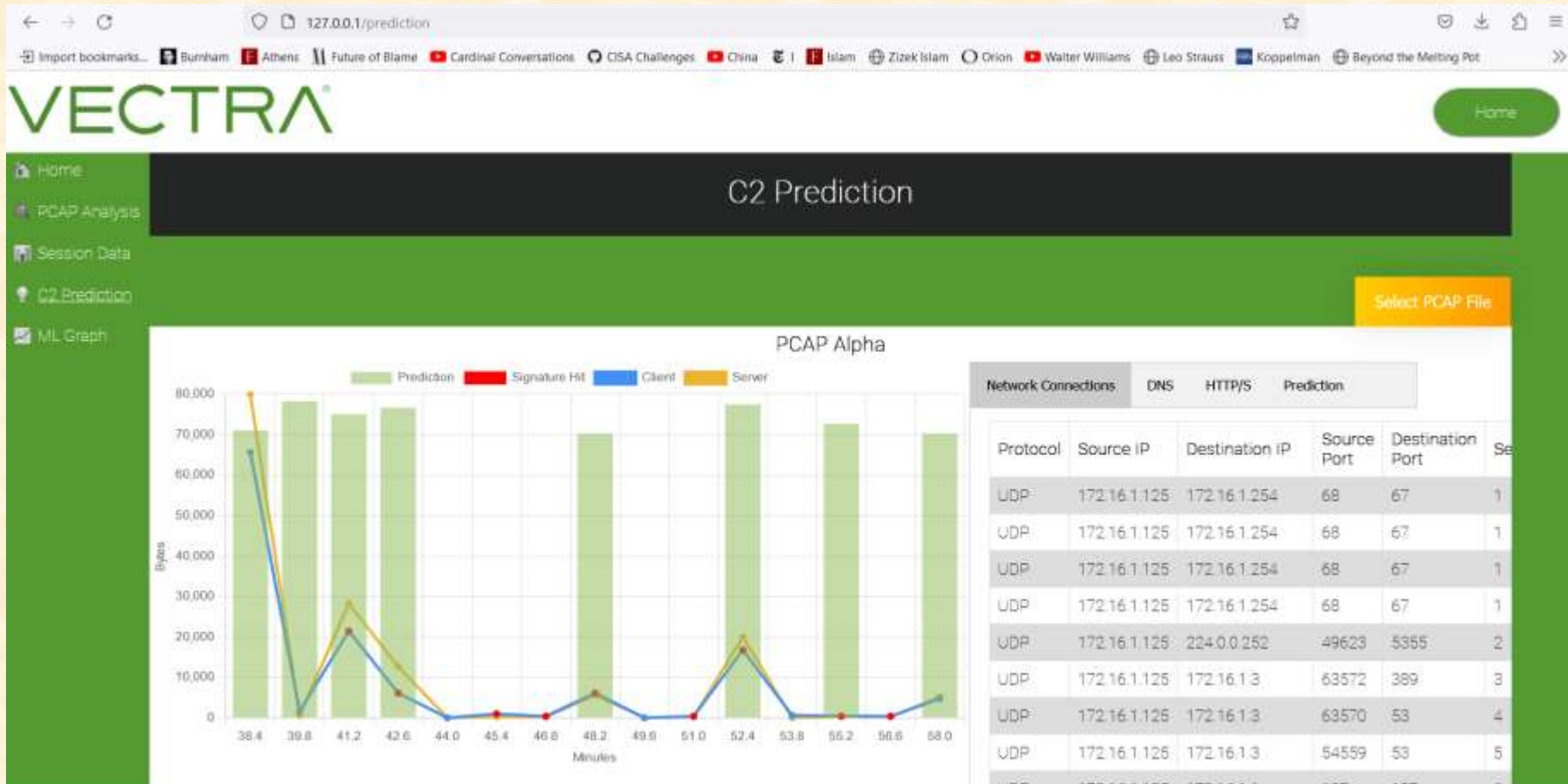
PCAP Analysis Page



Session Data Page



C2 Prediction Page



ML Graph Page

The screenshot displays the VECTRA web application interface. The top navigation bar includes a 'Home' button. A sidebar on the left contains menu items: Home, PCAP Analysis, Session Data, C2 Prediction, and ML Graph. The main content area is titled 'ML Graph' and features a 'Select Model' button. The central focus is a computational graph for an LSTM model. The graph starts with a 'Concat' node receiving input from a 'Static' node (1x14) and a 'Reshape' node (shape (2)). The 'Reshape' node takes input from 'States 1' (1x32) and 'States 2' (1x32). The 'LSTM' node receives inputs from 'States 1.1' (1x32), 'States 2.1' (1x32), and the 'Concat' node. The 'LSTM' node's parameters are listed as W (1x128x7), U (1x128x32), and B (1x256). The output of the LSTM is processed by a 'Transpose' node, which also receives input from a 'Time Series' node (1x128x7). The final output is connected to a 'Reshape' node (shape (2)).



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?

?

?

?

?

?

?

?

?

?

