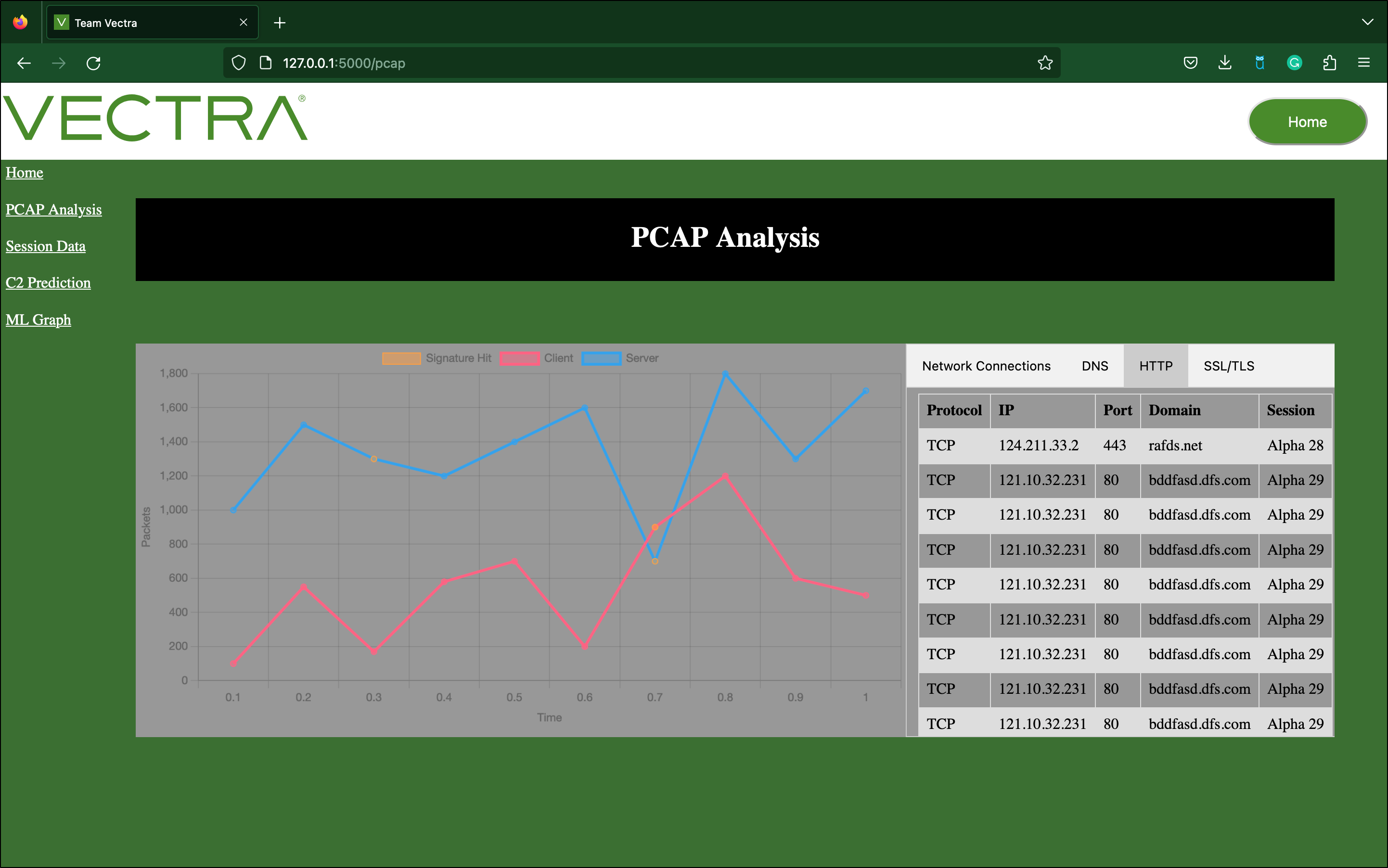
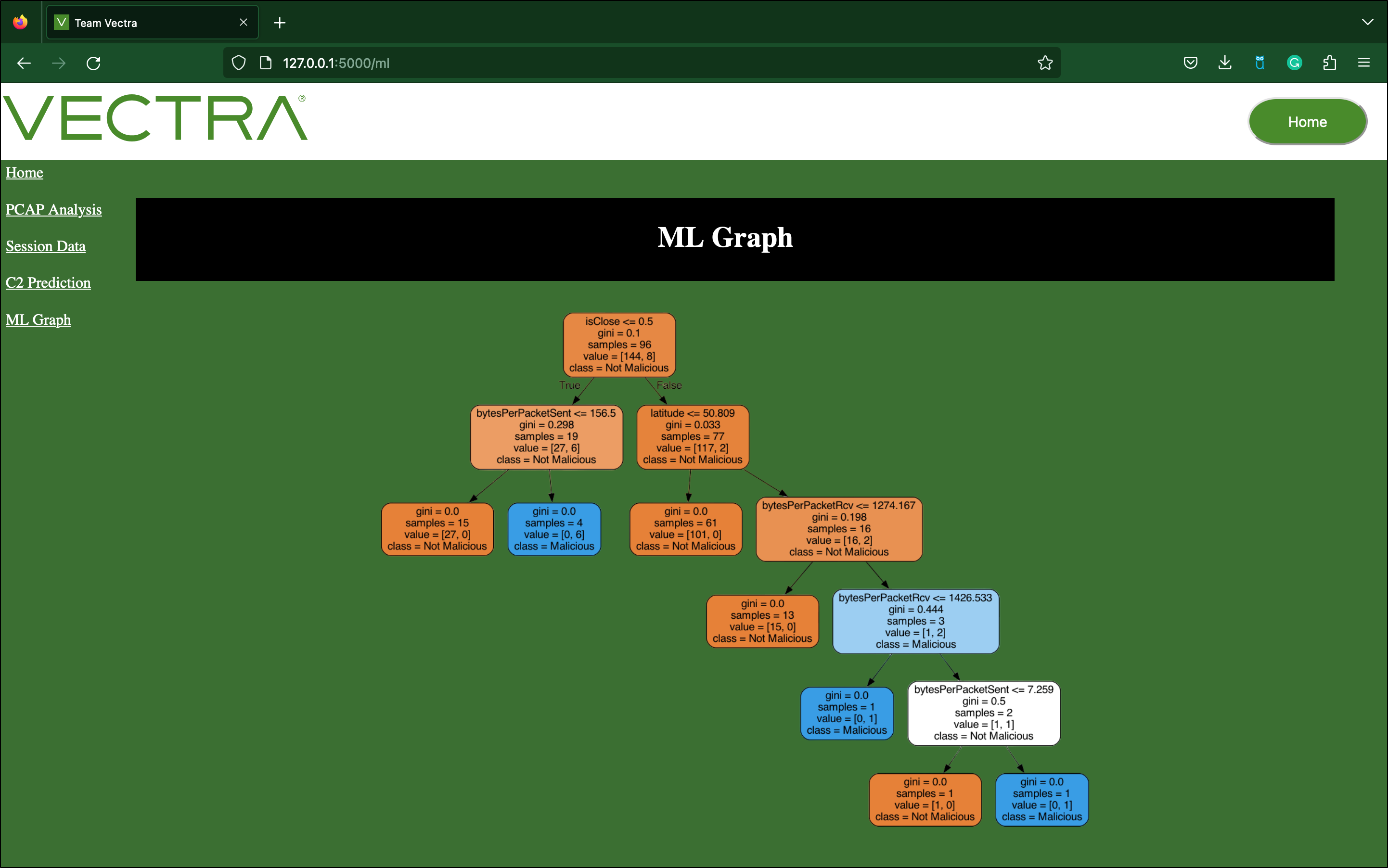
Design Day Booklet Team Page





PAGE N + 30



Vectra

Project Sponsors

Colin Jermain

Boston, Massachusetts

Christopher Thissen

Boston, Massachusetts

Brad Woodberg

Plymouth, Michigan

Michigan State University

Team Members (left to right)

Muhan Luo

Portage, Michigan

Aidan McCoy

Ann Arbor, Michigan

Nathaniel Ferry

Grosse Pointe, Michigan

Ettore Campriani

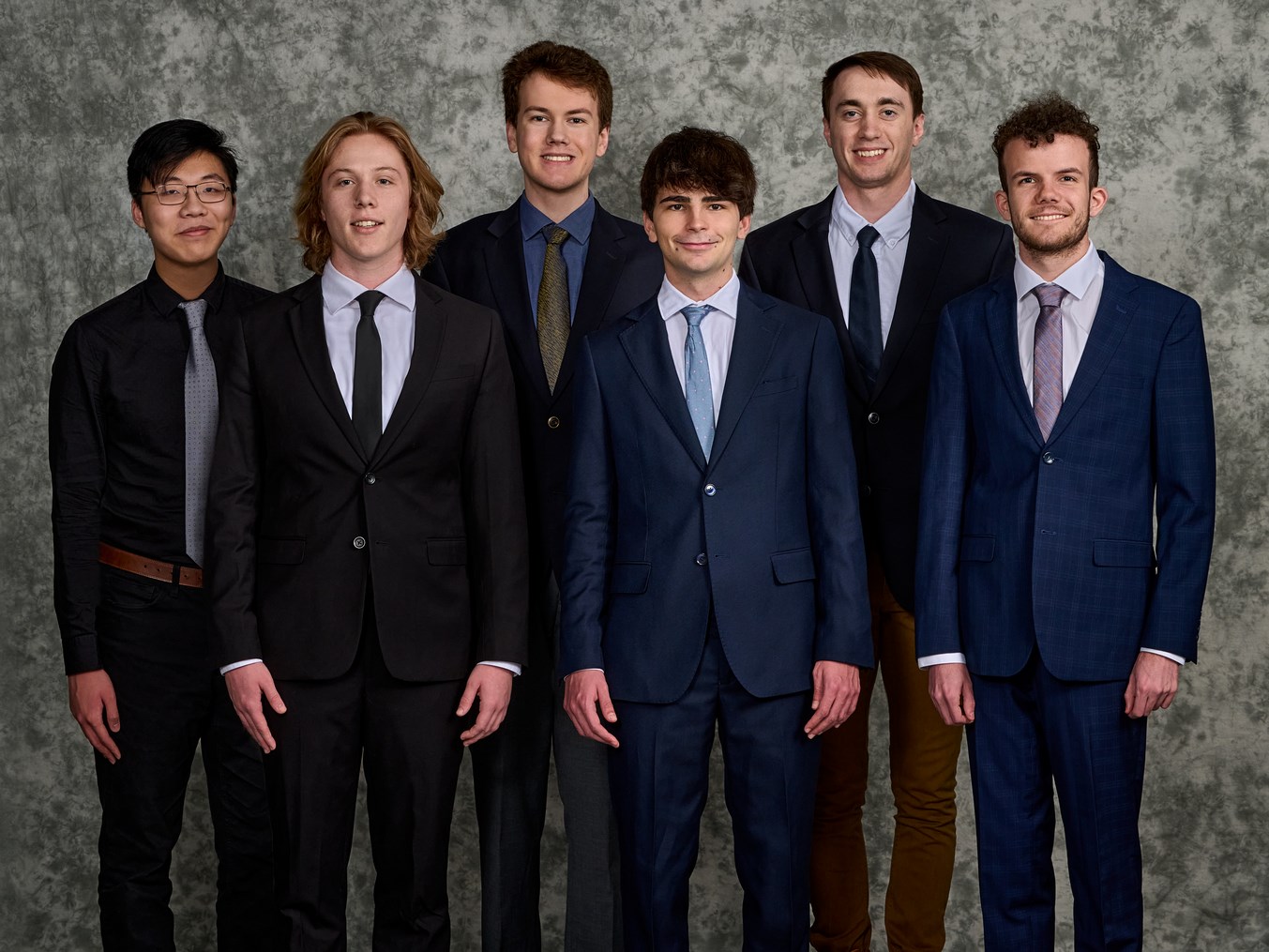
Modena, Emilia Romagna, Italy

Sam Kwiatkowski-Martin

Midland, Michigan

Aidan Erickson

Clarkston, Michigan



Vectra is a cybersecurity company that provides artificial intelligence-driven threat detection and response that is capable of defending against threats that bypass traditional security tools. Serving customers across the globe, Vectra redefines the standard of what it means for a network to be secure.

Traditional intrusion detection systems use an extensive list of previously recorded attacks known as signatures. These signature-based detection systems work well when met with known attack techniques, but when met with novel attack techniques, they fail to recognize them as threats.

Our Predicting Malware Command and Control Channels system is centered around combining signature-based intrusion detection and artificial intelligence-based intrusion detection, creating a singular robust system that draws from the strengths of both.

Our machine learning models detect command and control channels. Command and control is a technique that malicious actors use to communicate with an infected machine and send instructions for it to perform. A common factor behind many types of attacks, the presence of a command and control channel is a reliable way of detecting system compromise.

Using our web application, users gain a better understanding of the performance of our models by comparing where the signature-based system alone detects threats versus where our system detects threats. Visual representations of how our models are structured are also included to show the flow of a prediction. These tools make it easier to detect command and control channels, improving security.

Our machine learning models are built in Python using PyTorch, scikit-learn and LightGBM. Suricata is our signature-based intrusion detection system. Flask, JavaScript, and an SQLite database power the web application.

The Capstone Experience

Vectra

Predicting Malware Command and Control Channels