Network Anomaly Detection and Visualization
Sponsor: ExtraHop
Mentor(s): Eric Ball, Andrew Bates
Caleb Corson, Collier Mayo, Ethan Cabbage, Roby Daquilante, Ryun Boyles, TJ Hohl

The Problem
In a web-enabled world, detecting anomalies can seem like trying to find a needle in a haystack when there might not even be one. Every day, man hours are spent digging through connections “just in case” there’s an anomaly.

Requirements
Our customer highlighted a single most important requirement for our project, that being simplicity and ease of use. We wanted to make choices clear to the user, and supply an easy work flow for users to find the information they want.

Background
Other approaches to network security focus on using signature detection but anomaly detection methods prove better able to detect zero-day attacks. Following this, we use ExtraHop’s metrics in an SVM anomaly detection approach.

Machine Learning Approach
The software uses an SVM (Support Vector Machine) to compare incoming flows to normal data found in a learning base.

Design

Social Impact
Currently, many anomalies are likely missed or left unchecked due to the inherent difficulty of detecting them manually. By developing a simple and robust system to detect anomalies, the Internet will be safer, connections more reliable, and System Admins can get a good night’s sleep.

Data Flow

Web Views
- Home Page - General overview of the network. Shows top anomalous connections.
- History Page - Displays top anomalous connections for selected IP.
- Map Page - Anomalous connections in the selected time field are plotted on a Bing Map.

Future Work
- Add use of malicious IP lists to learning base
- Add a simple UI to design a learning base for a new network
- Use configurable emails to alert admins when anomalous flows are detected

Glossary
- Flows - Whole “conversations”
- Feature Vector - Weighted knowledges
- Anomalousness - Deviation from "normal"
- Bucket - A group of flows

Acknowledgements
John Yates
Adam Hahn
Assefaw Gebremedhin
Hassan Ghasemzadeh
Sakire Arslan Ay

Team Bolton