

# Net-CSI: An RNN-Based Network Intrusion Detection System

Michael Lisano

July 14, 2020

## Abstract

### Overview

Net-CSI is a utility that uses Deep Learning to identify potentially dangerous traffic across a network. [GitHub Repository](#)

Traditionally, network IDS and IPS systems use a series of rulesets to look for potentially dangerous network activity. As useful as these rulesets are, they're almost always a game of cat and mouse, as industry and the community try to keep pace with bad actors. This project aims to leverage machine learning to learn the patterns of these rulesets and flags things in a way that wouldn't be possible with a ruleset.

As of right now, there are other products and projects such as Poseidon and Darktrace Enterprise Immune System in development that also employ deep learning to detect malicious network activity. These current machine learning methods work to profile typical machine activity and identify abnormal behaviors. While this works very well in enterprise settings, places with a wider range of devices coming and going (such as public wifi or a guest network) don't allow for this level of in-depth profiling. Net-CSI is made to address cases like these where the individual nodes on the network are moving targets".

### Dataset

Net-CSI's training dataset is generated from PCAP files, which are fed into Suricata. Suricata's output file (eve.json) is parsed, and packets whose indices appear in the output file are marked as suspicious. The dataset consists of two arrays, one containing each packet's hex dump, and the other containing the labels that are generated from Suricata's output.

### Training

Net-CSI will use a combination of RNN and Feed-Forward network. Since Net-CSI's objective is to identify serial patterns in packet hex dumps, it will process inputs in a similar way to NLP.

## Usage

Net-CSI will be able to analyze network traffic either retrospectively or in real-time, however the latter will obviously require much more computational power (and a much higher power bill).