**Glossary**

A place to write relevant words and definitions

Main Terminology

**OWR – Open world recognition**

Open World Recognition is the ability of a machine recognition system to classify items not in the original domain of learning, usually this is accomplished by defining a method of classifying things as unknowns.

**IOWR – Implementation of Open World Recognition**

This project is an implementation of an Open World Recognition system.

**NIDS – Network Intrusion Detection System**

NIDSs are systems that read packets that pass through a local internet network and determine if an intrusion has occurred on the network

**IOWR-NIDS – Implementation of an Open-World Recognition-capable Network Intrusion Detection System**

Self.project

Machine Learning Terminology

**ML – Machine Learning**

Machine learning is a method of classification that defines its classification values based on some input training data instead of developer set values. This is usually accomplished with Neural Networks.

**Machine learning model**

An instance of a Machine Learning algorithm.

**Neural Networks**

Neural networks are a type of machine learning that uses artificial neurons. The artificial neurons are standard linear equations with training values that are set by backpropagation. The specific methods of the backpropagation are beyond the scope of this glossary.

**Model Integrity**

A value that describes the expected accuracy of the current Machine Learning instance.

**LLM – Large Language Model**

Used to predict what packets are doing and put it into a readable string format.

**Model Degradation**

As more unknowns are experienced, the quality and accuracy of the model reduces.

**Model Retraining**

The process through which a model is refined and corrected for higher confidence against datasets.

Network Terminology

**Packet**

A small amount of data that is used in network traffic. Contains primary contents and metadata about source and destination.

**Packet Header**

A section of data within a packet identifying key information about its destination, source, type, and more.

**Packet Classification**

Determines whether a packet is benign, malicious, or unknown, and if it is malicious, what form of attack it is.

**Prediction Confidence**

The degree to which a neural network feels its assessment of certain inputs is accurate.

**Hex**

Hexadecimal is a format that makes it easier to read binary data. 0 through 15 are represented, with 0-9 for the first ten digits and A-F for the last five.

**Intrusion**

Intrusions are attempts from malicious actors to get into a local internet network or specific files on that network.

**Network**

A network is a series of computers that allow data to flow between them securely.

**Traffic**

The packets passed around on a network.

Project Specific Terminology

**Unknown Packet**

A packet which has not been identified within any existing categorization with a reasonable degree of confidence.

**Language Model Predictions**

A prediction by the LLM of the possible names to be given to an unknown packet after it is classified as such.

**Plotly**

A Python library used to create visualizations from datasets.

**Dash**

A Python library which can spin up a web server with both dynamic Plotly graphs and regular web technologies.