# Guardians of the Port: AI/ML in Cyber Wargaming

1/c Faith Arnold, 1/c Elkhan Bagirov, 1/c Sean Dreher, 1/c Jake Kim, 1/c Alex Mathes, LT Ryan Quarry

## Problem

Increasing cyber threats to maritime ports are straining the resources of Coast Guard Cyber Protection Teams (CPTs).

## Objective

Use machine learning to train artificially intelligent agents as a tool CPTs can efficiently and automatically diagnose maritime ports.

## Context

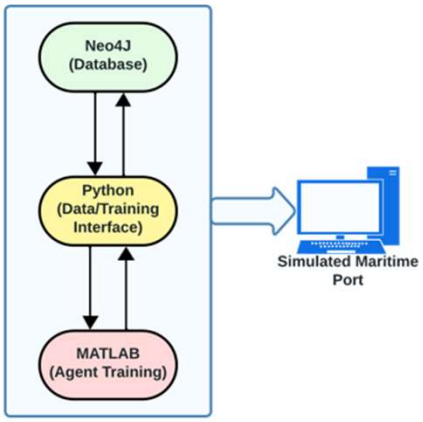
- **Vulnerability**: specific exploitable liability within a software or system
- **Weakness**: group of vulnerabilities that can affect any system
- **Attack**: a pattern in which a vulnerability can be exploited
- **Machine Learning**: subfield of Artificial Intelligence (AI) that focuses on learning through algorithms
- **Reinforcement Learning**: trains an algorithm to take actions on a rewards-based system

## Impact

- Increased cyber threats, such as **ransomware**, have disrupting maritime port critical infrastructure.
- **Foreign adversaries** consistently disrupt the maritime transportation system (MTS), hindering the U.S. economy and supplies.
- The MTS supports 95% of cargo into the U.S.
- Coast Guard's current solution involves **Cyber Protection Teams** that deploy to maritime ports to assess networks and respond to cyber attacks.

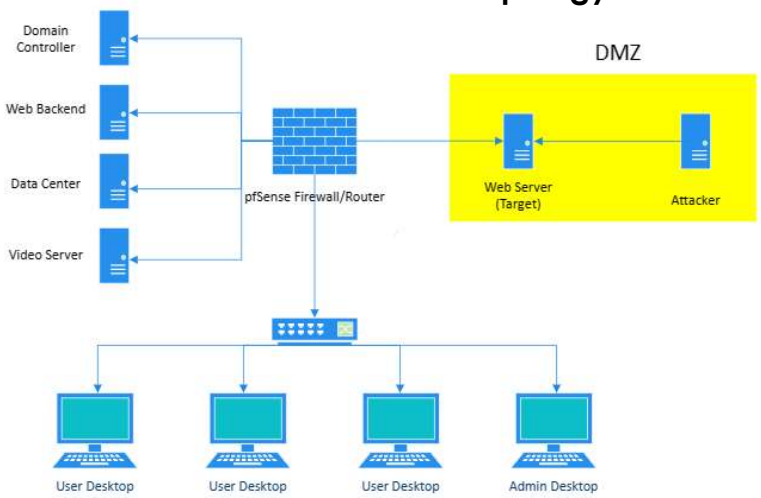
## System Design

### Technology Stack



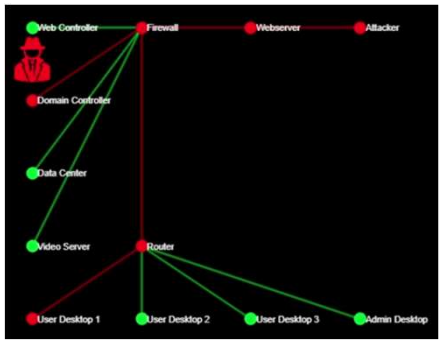

- The Neo4J graphical database is populated with Lockheed Martin's Vortex. It serves as a **knowledge repository** for the agent.
- Vortex uses the MITRE Ontology to outline **paths between offensive and defensive cyber techniques**.
- Python serves as the **machine learning environment** to configure the agent.
- MATLAB uses the reinforcement learning **toolbox and associated algorithms to train** the agent.

### Maritime Port Network Topology




- This diagram represents the cyber infrastructure of the **simulated port network**, modeled off the port of Los Angeles, that will be used to deploy the agents.
- The network hosts various **external and internal services** that support operations within a maritime port.
- A number of these services contain **vulnerabilities** that an attacker could exploit.

### Agent Training




- Agents are **trained for specific steps** within a cyber attack kill chain.
- Agent distributes ransomware across the network, **disrupting the operations** within the maritime port.
- CPTs **defend maritime port based off agent success** in infiltrating the network.

UNITED STATES COAST GUARD ACADEMY

Approved for Public Release