Network Intrusion Detection with AI

Length	Module
Collection	Cyber Heroes
Updated	October 10, 2024
Contributors	Sergio Salinas
Academic Levels	Undergraduate, Graduate
Topics	
Link	https://clark.center/details/checoponcho/8a08232b-da0b-45ea-8df0-c9043afdca3e

Description

This learning object covers the data science workkflow for network intrusion detection using AI. The workflow steps covered include data cleaning, data exploration, ML/AI model design and trianing, and performance evaluation.

The learning objet walks students through how the process of designing and evaluating ML/AI models using a Python Jupyter Notebook and a sample PCAP with both legitimate and malicoius traffic.

Outcomes

- Describe the data science workflow for network intrusion detection using AI
- Build a network dataset from a packet capture file (PCAP)
- Perform dataset exploration
- Develop ML and AI models to detect anomalies in network datasets
- Evaluate the performance of ML/AI models detecting network attacks

Alignment

The standards and guidelines this learning object is mapped to

- NICE Framework (2017) (2020) - K0046: Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.
- CAE Cyber Defense Knowledge Units 2020 (2020) - Intrusion Detection/Prevention Systems (IDS): The intent of the Intrusion Detection/Prevention Systems (IDS) Knowledge Unit is to provide students with knowledge and skills related to detecting and analyzing vulnerabilities and threats and taking steps to mitigate associated risks.

- NICE Framework (2017) (2020) - S0199: Skill in creating and extracting important information from packet captures.
- NICE Framework (2017) (2020) - S0221: Skill in extracting information from packet captures.
- CAE CDE 2019 (2019) - Advanced Network Technology and Protocols: Develop the intellectual tools to explore and understand advance network concepts and protocols.
- CAE CDE 2019 (2019) - Intrusion Detection/Prevention Systems: Use tools and algorithms to detect various types of malware (keyloggers, rootkits) and unauthorized devices (rogue wireless access points) on a live network.
- CAE CDE 2019 (2019) - Network Forensics: Analyze and decipher network traffic, identify anomalous or malicious activity, and provide a summary of the effects on the system.
- CAE Cyber Defense (2019) - Network Forensics (KU2): Analyze and decipher network traffic, identify anomalous or malicious activity, and provide a summary of the effects on the system.
- CAE Cyber Defense Knowledge Units 2020 (2020) - Network Technology and Protocols (NTP): The intent of the Network Technology and Protocols Knowledge Unit is to expand students' knowledge of networking to include an understanding common network protocols, how network components interact, and how networks evolve over time. The Knowledge Unit will also extend student experiences in using tools to monitor and analyze a network. Students expand their familiarity with network vulnerabilities.

Links

External links that are associated with this learning object

- Github repo
- Jupyter Server