How to develop/code Machine Learning cyber security project

Scikit-learn

Coding Process

- Install python library
- Choose coding model
- Code ML program
- Find program logic error
- Fix the logic error

Coding model example

[model 1] detect DDoS attacks

[model 2] detect DoS attacks

[model 3] SYN flooding detection

[model 4] detect IP Spoofing

[model 1]

- Writing and testing Python code to detect DDoS attacks using Scikit-learn
- The algorithm used is Isolation ForestHow to detect DDoS attacks from network traffic data.
- python
- import numpy as np
- import pandas as pd
- from sklearn.ensemble import IsolationForest

[model 2]

Coding and testing DoS attack anormaly detection case using scikit-learn

 One-Class SVM effectively detects abnormal traffic such as DoS attacks. This algorithm learns the characteristics of normal traffic and separates abnormal traffic with different characteristics. It only uses three characteristics: number of packets, number of bytes, and connection duration. Actual network traffic data contains various characteristics.

[model 3]

Writing and testing DoS SYN Flooding detection code using Scikit-learn

- SYN Flooding is a type of DoS attack where the attacker continuously sends SYN packets to the server to exhaust the server's resources.
- The algorithm used is One-Class SVM and shows how to detect SYN Flooding attacks.

[model 4]

Writing and testing Python code for DoS detect IP Spoofing using scikit-learn

 IP Spoofing is a type of DoS attack where the attacker uses a different IP address to send traffic to the server.

The algorithm is Isolation Forest.

Reference site

https://www.geeksforgeeks.org/learning-model-building-scikit-learn-python-machine-learning-library/

https://github.com/scikit-learn/scikit-learn

https://www.google.co.kr/search?sca_esv=be16b17cae58a747&sxsrf=ADL YWIKi3ldGWmZF1hIVGovzfZvETdq1aw:1722126020874&q=Scikitlearn+Python&sa=X&ved=2ahUKEwjn5e2tu8iHAxWz6TQHHbqIF7IQ1QJ6 BAhKEAE&biw=1540&bih=742&dpr=1.25

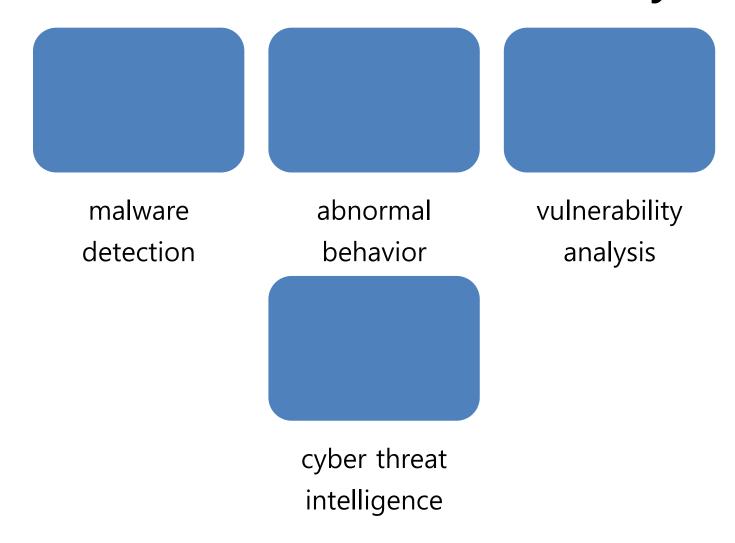
TensorFlow Deep learning basics

TensorFlow

• Widely used open source library for building and training machine learning and deep learning models.

• In the security field, TensorFlow can be used to develop programs with the functions:

TensorFlow for security



TensorFlow

- 1. Build a malware detection model Develop a model that can detect new malware by learning the characteristics of malware Use various data such as files, network traffic, and system logs as input
- 2. Build an abnormal behavior detection model• Detect abnormal behavior by learning normal user behavior patterns• Monitor user logins, file access, network activities, etc.

TensorFlow

- 3. Build a vulnerability analysis model• Automatically identify and classify vulnerabilities in software code• Use techniques such as static code analysis and dynamic execution analysis
- 4. Build a cyber threat intelligence model•
 Detect new cyber threats by
 collecting/analyzing online data•
 Automatically collect malicious URLs,
 malicious files, vulnerability information, etc.

Easy Steps to Pip Install TensorFlow for Beginners: Complete Guide

<u>Simple Steps to Install TensorFlow with Pip</u> (myscale.com)