Techniques to reduce false positives 10-09-2024

* Data-centric techniques
  + Data quality improvement
  + Improve performance by using techniques like Oversampling and Undersampling for the data imbalances
* Model-centric techniques
  + Support Vector Machine Algorithms
  + Hyperparameter tuning algorithms
* Human in the loop technique

Logic Notes 10-29-2024:

* Anomaly Detection Algorithms for Unusual Patterns
  + Isolation Forests - Decision-tree based approach, this algorithm is meant to identify outliers in a high-dimensional dataset. This is best used for Anomaly detection and good for detecting suspicious Patterns such as SQL Injection. This algorithm takes a learning based approach, identifying outliers in the data. You can Utilize Isolation Forests through
    - Loading/Preparing the Data
    - Training the Isolation Forests- Show the Isolation Forest a normal dataset so that it can differentiate between the norm and anything else.
    - Detect Anomalies- Any input considered an anomaly would be flagged
  + One-Class SVM- This is useful for enhancing the security pattern detection using ML. It works similarly to Isolation Forest, in the fact that it goes through the training process using normal, non-malicious data to differentiate between normal and malicious.
* Security Enhancement for Pattern Detection
  + SQL Injection - The most effective way to deal with SQL injection is by avoiding user inputs in SQL statements. Using prepared statements better prevent injection
  + Cross-site Scripting Detection- a web security sysyem that focuses on preventing the injection of dangerous code into a website. This would allow the content that users see to be manipulated and sensitive information to be stolen. Cross site scripting detection tools or scripts search for suspicious keywords, HTML tags, and JavaScript functions that are commonly used in attacks. The main Cross site Scripting attacks are:
    - Stored XSS: Malicious script is injected into the website directly
    - Reflected XSS: The Malicious Script is reflected off the website and onto the targets browser
    - Documented Object Model (DOM) based