Challenge Title: AI FOR CYBER SECURITY WITH IBM QRADAR

Project ID : 705905-1704960173

Team Name: TRAILBLAZER

Team Size : 1

Team Lead: Ayush Dhiman

College Name: VIT BHOPAL UNIVERSITY

Business : Anomaly Detection in Network Traffic Using Machine Learnin g Challenge

INTRODUCTION

There is simply too much data to analyze and not enough time, resources, and talent to make it happen. Our solution's AI analytics can analyze 100% of the data you collect, detect anomalies and business incidents in real-time and identify their root cause, enabling you to remedy problems faster and capture opportunities sooner.Anomaly Detection is the technique of identifying rare events or observations which can raise suspicions by being statistically different from the rest of the observations. Such “anomalous” behavior typically translates to some kind of a problem like a credit card fraud, failing machine in a server, a cyber attack, etc.

LITERATURE SURVEY

Real-time eCommerce Analytics with our solution

Every day that passes with an incident or opportunity undetected has a negative impact. Lost revenue, degraded customer experiences, and failed promotions can add up a horror stories for

the business. These problems are often lurking in overlooked eCommerce analytics metrics, missed by overworked operators and data scientists relying on manual methods.

THEORITICAL ANALYSIS

Our solution's approach to business monitoring in eCommerce is autonomous. No manual dashboards. No operators sifting through false positives. Real-time analytics with our solution can help you detect incidents 80% faster and reduce incident costs by over 70%.An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for the harmful activity or policy breaching.

EXPERIMENTAL INVESTIGATIONS

Conversion rate monitoring

As conversion rate directly impacts revenue, monitoring for sudden drops can alert a company to errors in their checkout process and save a significant amount of otherwise lost revenue.

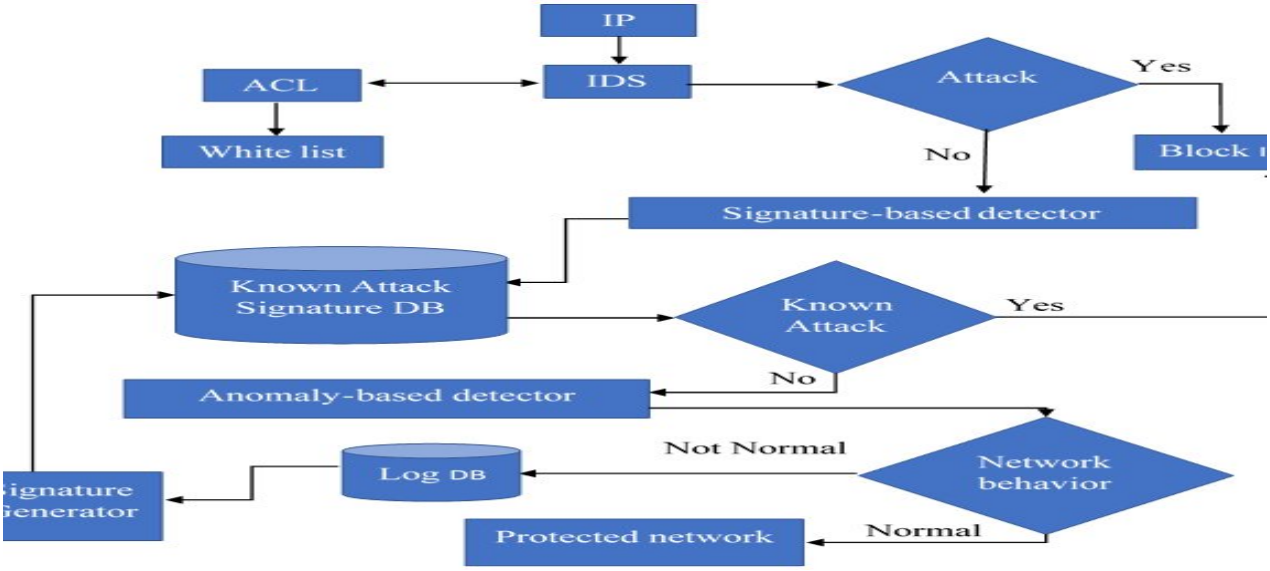
Revenue monitoring

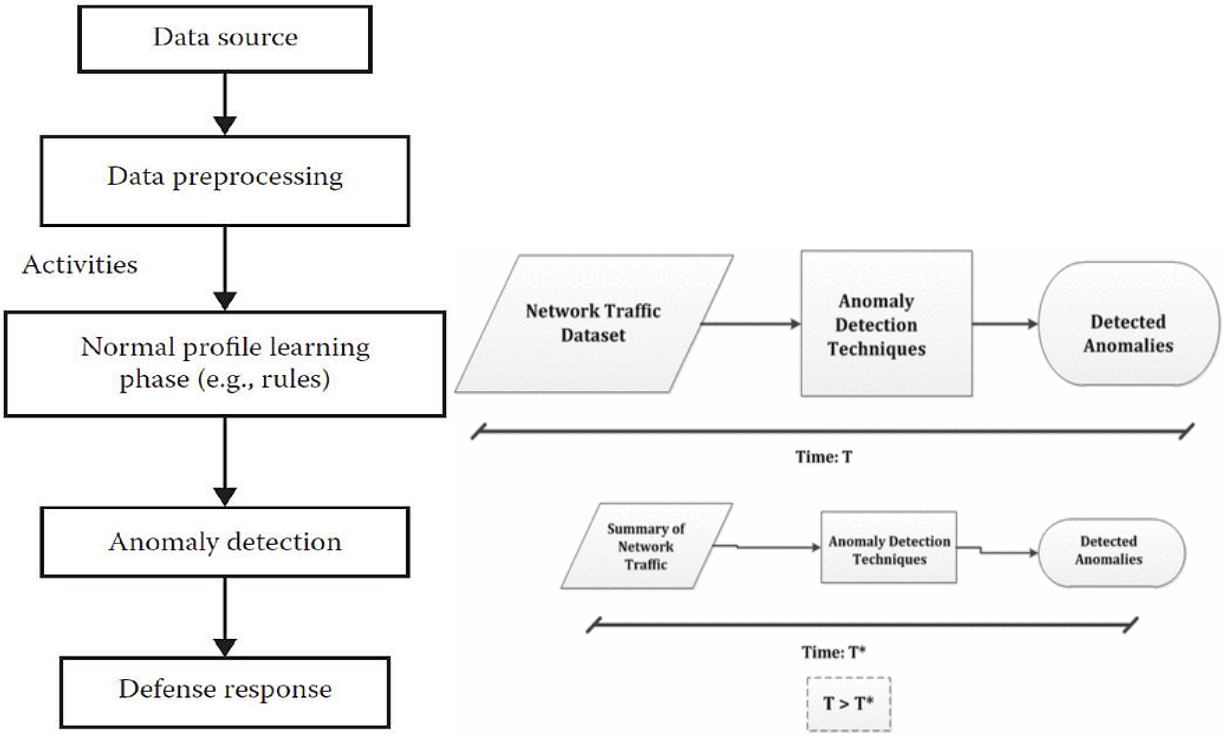
Companies can leverage autonomous monitoring on all revenue-related metrics, including revenue from each acquisition channel, completed purchases and sales velocity.

Customer fraud alerts

Operators can apply AI/ML analytics to fraud detection and protect merchants against unexpected patterns in user behavior.

FLOWCHART

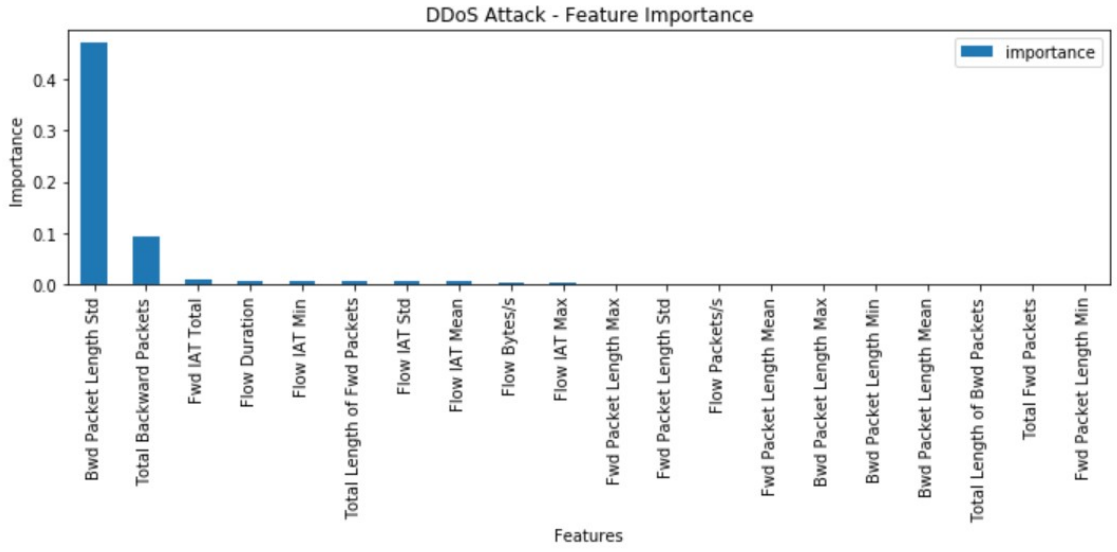


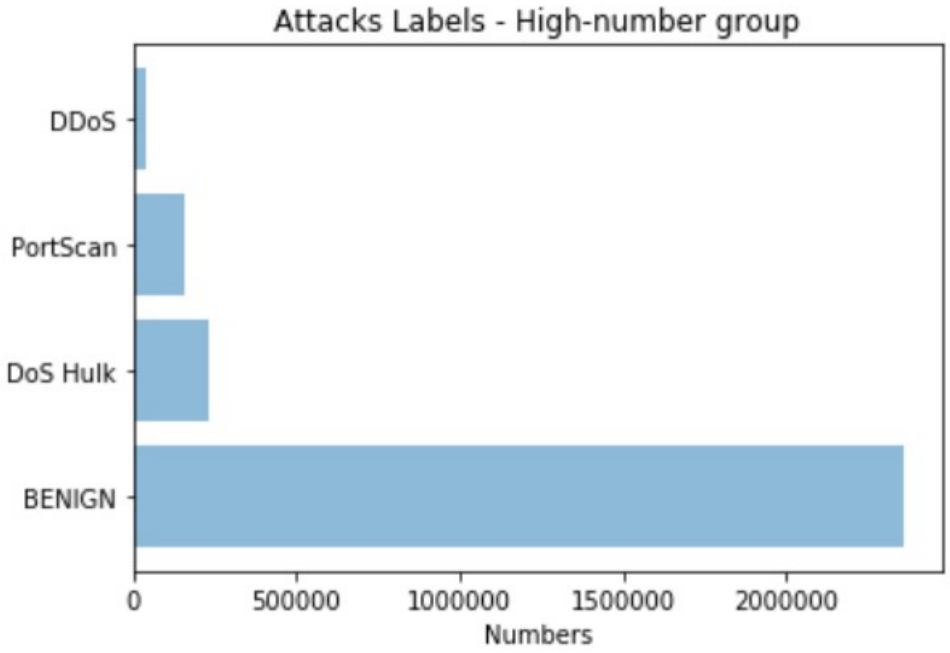


RESULT

At our solution, false positive reduction is our main KPI. Every alert counts. Alerts are scored according to deviation, duration, frequency, and related conditions.Our solution's patented anomaly scoring method runs probabilistic Bayesian models to evaluate the anomaly delta both relative to normal, and relative to each other. Anomaly Detection is the technique of identifying rare events or observations which can raise suspicions by being statistically different from the rest of the observations.

```
DDoS=["Bwd Packet Length Std","Total Backward Packets","Fwd IAT Total","Flow Duration","Flow IAT Min"]
```





ADVANTAGES & DISADVANTAGES

Modern computer threats and intrusion attacks are far more complicated than those seen in the past. In IOT devices, these threats and attacks become even more visible and predominant as the heterogeneous and distributed characters of the devices make conventional intrusion detection methodologies hard to deploy. discusses the principal cyber threats for IoT devices like Denial of Service, Malware based attacks, data breaches and weakening parameters, enlists the security issues identified in IoT as per the Open Web Application Security Project (OWASP) and also highlights few of the past example attacks identified towards IoT. Detecting these threats requires new tools, which are able to capture the essence of their behavior, rather than looking for fixed signatures in the attacks. Anomaly detection algorithms, which are able to learn the normal behavior of systems and alert for abnormalities, with or without any prior knowledge on the system model, nor any knowledge on the characteristics of the attack, can be a key to handle such complexities.

APPLICATIONS

Autonomous learning of metric behavior

Our solution leverages advanced AI and ML to learn the unique behavior of every metric and its weekly, monthly and annual seasonality- in real time and at scale.Every metric that comes in goes through a classification phase, and is matched with the optimal model from a library of model types for different signal types.

Comprehensive metric & events correlation
Correlation is crucial for understanding metrics in context.Our solution uses a patented combination of four derivatives of behavioral topology learning: abnormal correlation, naming correlation, graph correlation, and implicit analytics topology.

CONCLUSION

The implementation phase consists of 5 steps, which are: 1- Pre-processing 2- Statistics 3- Attack Filtering 4- Feature Selection 5- Machine Learning Implementation

Each of these steps contains one or more Python files. The same file was saved with both "py" and "ipynb" extensions. The code they contain is exactly the same. The file with the ipynb extension has the advantage of saving the state of the last run of that file and the screen output.

Thus, screen output can be seen without re-running the files. Files with the ipynb extension can be run using the jupyter notebook program. When running the codes, the sequence numbers in the filenames should be followed.

Because the output of almost every program is the prerequisite for the operation of the next program.

FUTURE SCOPE

Our solution's accuracy can be improved as it is one of the biggest challenges for both network administrators and researchers.If they had a tool that could accurately and expeditiously detect these anomalies, they would prevent many of the serious problems caused by them. Our findings will help researchers and network administrators to select effective internal-based features for each particular type of anomaly, and to choose a proper machine learning algorithms

https://github.com/smartinternz02/SI-GuidedProject-705905-1704960173