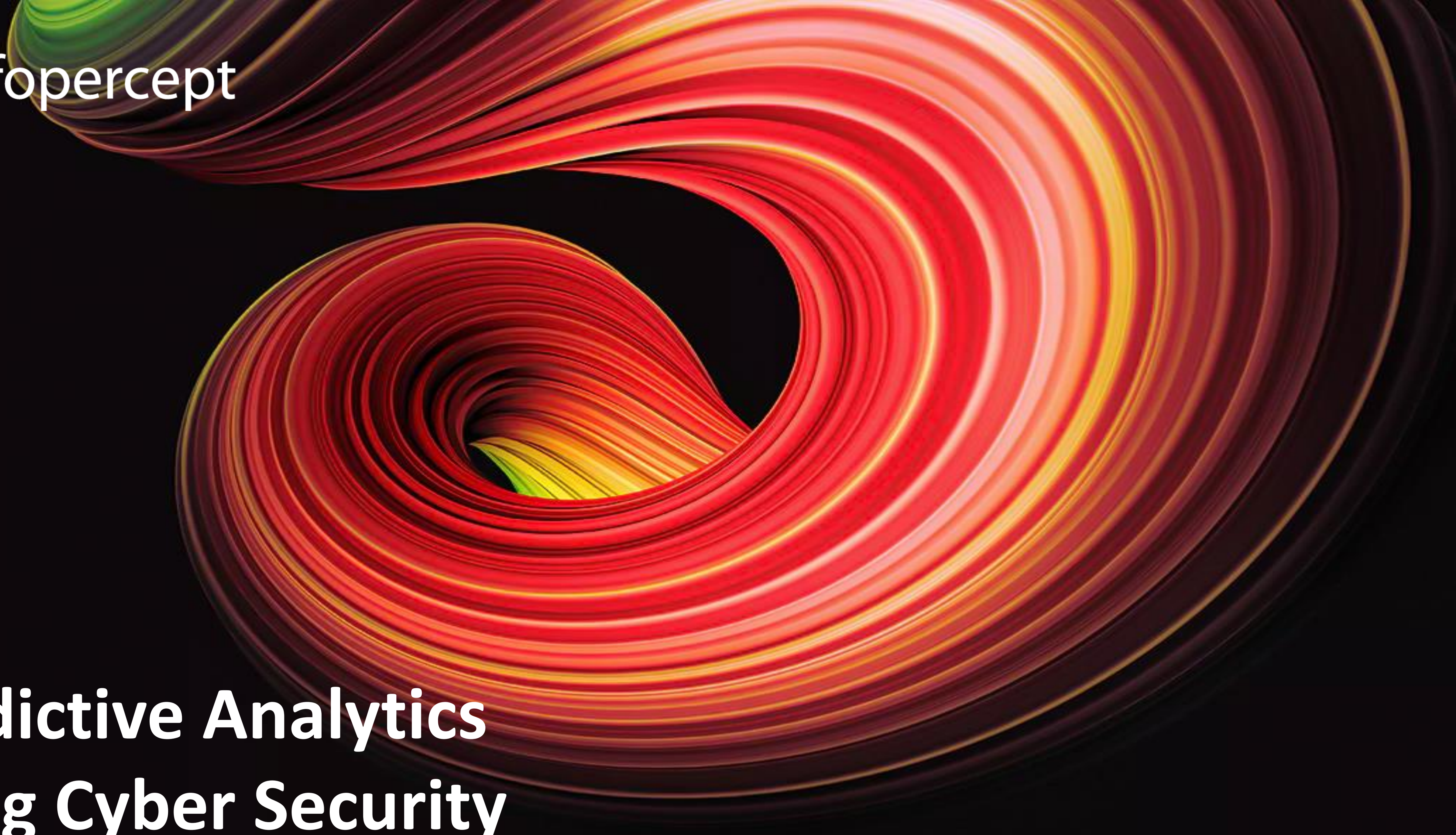
Infopercept



Predictive Analytics using Cyber Security

Definition

- Predictive analytics encompasses a variety of statistical techniques from data mining, predictive modelling, and machine learning, that analyze current and historical facts to make predictions about future or otherwise unknown events.

- Predictive analytics help businesses identify security threats before they can do any damage. Instead of only focusing on the “infection stage” of an attack, enterprises can detect future incidents and maximize prevention.

Abstract

Cyber-attacks are often detected too late. According to reports on reported cyber-attack incidents, most victim organizations do not know that their systems have been breached until they are informed by organizations or individuals external to the victim organization’s physical or logical network. This is a significant problem for cyber security professionals and organizations.

PREDICTING CYBER-ATTACKS USING PUBLICLY AVAILABLE DATA

Cybersecurity failures happen in phases. These failures are only detected at their later phases or after they have been completed. Being able to detect early stages of an attack will provide organizations significant advantage in their effort to secure the organization’s information. Automated detection of cyber-attacks using Probabilistic warning systems, that fuse both Internal and External Sensors, is an ongoing research subject. Various governments are funding for it. Such systems will gather information from multiple sources including open sources to analyze the data and predict attacks. It will help organizations to protect themselves from attacks.

Infopercept

Keywords

Network security, cyberattack prediction, social network, probabilistic warning, open source intelligence, cyber threat intelligence, Attack Graph, Non-homogeneous Markov Model, CVSS.

STATEMENT OF THE PROBLEM

- The big problem that occurs in this is that the cyber attacks are often detected too late, most victim organizations do not know that they have been hacked until they are informed by organizations external to the victim organization’s corporate network.

- .This is a significant problem for cyber security professionals.

PURPOSE OF THE STUDY

The purpose of this study is to investigate current approaches to cyberattack detection, as well as prediction, based on publicly available data. Analyzing openly available data can provide useful information that can be used to predict cyber-attacks.

Scope

Not every cyber-attack is reported to the public and therefore this study could not have examined data on all cyber-attacks. Also, the available data was filtered based on key phrases such as “bruteforce attack”, “password guessing”.

LITERATURE REVIEW

- Cybersecurity failures happen in phases. Typically, these failures are only detected at their later phases or after they have been completed. Being able to detect early stages of an attack will provide organizations significant advantage in their effort to secure the organization’s information.

- In pursuance of such a solution, on July 17, 2015 Intelligence Advanced Research Projects Activity (IARPA), a United States government agency published a Broad Agency Announcement (BAA) calling for teams to participate in its research program titled Cyber-Attack Unconventional Sensor Environment (CAUSE). In the BAA, the program indicated that it was seeking to research on multidisciplinary methods for accurate and timely forecast of cyber-attacks. The program started in February 2016 and is expected to continue until August 2019 (IARPA, 2015).

Meet the Future Star of Cybersecurity: HackerBots

First hacking contest in history organised by DARPA to fight bot against bot instead of humans. The contest was enlightening and surprising - even those who designed the bots were impressed with the outcomes. The bots were able to detect bugs faster than any human, protecting their own systems while systematically fleshing out other bots weak points and attacking.The technology behind hacker bots has the potential to keep up with the ever-increasing load of potential security threats. Now, enterprises can use hacker bots to catch potential threats and holes faster than human efforts - which leads us to

Infopercept

Explore the Landscape of Predictive Analytics

Predictive analytics have the power to proactively help businesses identify security threats before they can do any damage. Instead of only focusing on the “infection stage” of an attack, enterprises can detect future incidents and maximize prevention. Just as IBM’s mobile analyzer detects weaknesses within the applications, the hacker bots use complex analytics to sniff out vulnerabilities before an attack.

Model Representation

We define the base exploitability score $e(v)$ as the measure of complexity in exploiting the vulnerability v. The CVSS standard provides a framework for computing these scores using the access vector (AV), access complexity (AC) and authentication (Au) as follows-

$$e(v) = 20 \times AV \times AC \times Au$$

Given the base exploitability score and the temporal weight, the effective temporal exploitability score is as follows

$$e(v\text{t}) = \text{temporal weight} \times e(v)$$

the state of exploitability for this vulnerability is documented as high, medium or low according to the results.

Common Vulnerability Scoring System

$$\begin{aligned}\text{Predicted CVSS Score}\\ &= -0.2893 + 0.07174 * \text{Number of vulnerabilities}\\ &\quad \text{on the IT application reported by tools}\\ &\quad + 0.0025 * \text{Proposed average input network traffic}\\ &\quad \text{for the application for a week measured in KBPS.}\end{aligned}$$

Predictive analytics helps the banking sector

- Fraud Detection - Analytics can be used to recognize frauds that are not very obvious and then predictive analytics can be implemented on them to analyze them further. Data integration, utilizing unstructured data and machine learning techniques like supervised and unsupervised learning can help detect fraud.

- Application screening - Predictive analysis in banking can help process huge volumes of applications, without excluding important variables, without delays or errors, without growing tired- all of it with regularity and steadiness.

- Customer acquisition & retention -
- Identifies the customers most likely to defect before they end their relationship.
- Keeps the right customers longer
- Predicts which actions will earn their loyalty.

Knowing customer buying habits - With predictive analytics, banks can rapidly segregate various customer segments and replace it with highly relevant, individualized messages tailored to each customer’s profile, resulting in a higher response rate. This ultimately helps deliver the right product to the right person. As in if someone who has a history of buying gadgets then the sale of high-end gadgets can be targeted at him and in fact he would be happy to get such updates.

- Cross-selling - Predictive analytics helps examine customers usage, spending, and other behavior and leads to effective cross-selling of the right product at the right time. Today, securing one profitable customer is a big task for banks, hence cross-selling another product to an existing customer helps a lot.

- Collections - Banks have a mix of customers who always pay on time and those who lag. It is a tricky task to keep a track and maintain records of all individuals and differentiate who to focus more. Predictive analytics offers clear benefits in this area. Banks can attain a better understanding of their portfolio risk and thus improve the productiveness of the collections process.

- Better cash - Predictive analytics can help banks track the past usage patterns and the daily coordination between the in- and out-payments at their branches and ATM’s, hence predicting the future needs of their potential customers.

- Marketing optimization - Predictive analytics help marketers to plan marketing campaigns and programs and monitor the results closely. By providing an insight into customer behavior and attitudes, and a complete, current view of the customers, analytics help the marketing team deliver the right message at the right time to the right customer.

- Customer Lifetime Value (LTV) - Know which customers should be the focus of new customer engagement efforts. Identify the previous factors that enhanced returns on customer engagements in the past. Use that knowledge to understand why customers responded to certain messages and promotions.

- Feedback management - Predictive analytics allows banks and financial firms to keep up their relationship with the customers by giving them the right services and products for their need and matching individual preferences in the most sorted way.

Bank Customers Benefit

- Credit scoring - Credit scoring models use data to predict the creditworthiness.
- Help with budgeting - Computer models can help in managing the finances. They can identify a person's income and expenses typically hit his account, and they can see where his money goes.
- Fraud prevention - Predictive analytics helps on noticing when somebody else uses a person's credit card or if somebody logs in to the account in an unexpected way. They may also be able to reduce bad check scams, which can cause significant losses for victims.
- Financial management - Software can assist with bigger-picture decisions as well. For example, after reviewing the finances, predictive analytics helps to know how much a person might be able to put toward eliminating his debt. Banks might also be able to coach him on how to earn higher rates on his savings.
- Loan approval - Lenders are getting more sophisticated about how they evaluate loan applications. They realize that not everybody has a high FICO (Financial Accounting Controlling) score-but they should still qualify for loans.

Infopercept

Predictive Analytics Challenges with Solutions

- Expertise - Expertise is a challenge because predictive analytics solutions are typically designed for data scientists who have deep understanding of statistical modeling, R, and Python.

- Solution - Today, new predictive analytics solutions are emerging, and they're designed for almost anyone to use.

- Adoption - Users have to switch from their primary business application over to the predictive analytics solution in order to use it. Traditional predictive tools are hard to scale and deploy, which makes updating them a painful process.

- Solution - Predictive analytics is most effective when it's embedded inside the applications people already rely on.

- Empowering End Users - Predictive tools deliver information and insights, but they fail to let users take action. If users wants to act on the data, they have to jump to yet another application, ultimately wasting time and interrupting their workflow.

- Solution - By embedding intelligence workflows into regular business applications.

Infopercept

THANK YOU

For More Information Please Visit our Website

www.infopercept.com