International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 13th Sept 2019. Link :http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-09

Title AN APPROACH FOR CYBER SECURITY FRAME WORK WITH OPTIMIZATION IN OPERATIONAL COST

Volume 08, Issue 09, Pages: 629–633.

Paper Authors

REGALLA SIVAPARVATHI, N.MARY VIJAYA NIRMALA

G.V.R. & S. COLLEGE OF ENGINEERING & TECHNOLOGY NEAR BUDAMPADU, GUNTUR-522007, A.P, INDIA

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

AN APPROACH FOR CYBER SECURITY FRAME WORK WITH OPTIMIZATION IN OPERATIONAL COST

[1]REGALLA SIVAPARVATHI, [2]N.MARY VIJAYA NIRMALA

[1]STUDENT, DEPARTMENT OF CSE, G.V.R. & S. COLLEGE OF ENGINEERING & TECHNOLOGY, NEAR BUDAMPADU, GUNTUR-522007, A.P, INDIA.
[2]ASSOCIATE PROFESSOR DEPARTMENT OF CSE, G.V.R. & S. COLLEGE OF ENGINEERING & TECHNOLOGY NEAR BUDAMPADU, GUNTUR-522007, A.P, INDIA.
[1]sivaparvathiregalla@gmail.com, [2]nirmala.neelam@gmail.com

ABSTRACT: In order to ensure a company's Internet security, SIEM (Security Information and Event Management) system is in place to simplify the various preventive technologies and flag alerts for security events. Inspectors (SOC) investigate warnings to determine if this is true or not. However, the number of warnings in general is wrong with the majority and is more than the ability of SCO to handle all awareness. Because of this, malicious possibility. Attacks and compromised hosts may be wrong. Machine learning is a possible approach to improving the wrong positive rate and improving the productivity of SOC analysts. In this article, we create a user-centric engineer learning framework for the Internet Safety Functional Center in the real organizational context. We discuss regular data sources in SOC, their work flow, and how to process this data and create an effective machine learning system. This article is aimed at two groups of readers. The first group is intelligent researchers who have no knowledge of data scientists or computer safety fields but who engineer should develop machine learning systems for machine safety. The second groups of visitors are Internet security practitioners that have deep knowledge and expertise in Cyber Security, but do Machine learning experiences do not exist and I'd like to create one by themselves. At the end of the paper, we use the account as an example to demonstrate full steps from data collection, label creation, feature engineering, machine learning algorithm and sample performance evaluations using the computer built in the SOC production of Seyondike.

1. INTRODUCTION

Presently system connected by internet, such as the hardware, software & data can be protected from cyberattacks by means of cyber security. Cybersecurity is a set of technologies and processes designed to protect computers, networks, programs and data from attacks and unauthorized access, alteration, or destruction. As threats become more sophisticated the most recent technologies such as Machine learning (ML) and deep learning (DL) are used in the cybersecurity community to leverage security abilities. Nowadays, cyber security is a stimulating issue in the cyber space and it has been depending on computerization of different application domains such as finances, industry, medical, and many other important areas [11]. To identify various

network attacks, particularly not previously seen attacks, is a key issue to be solved urgently [1].

This paper deals with previous work in machine learning (ML) and deep learning (DL) methods for cybersecurity applications and some applications of each method in cyber security operations are described. The ML and DL methods covered in this paper are applicable to detect cyber security threats such as hackers and predators, spyware, phishing and network intrusion detection in ML/DL. Thus, great prominence is placed on a thorough description of the ML/DL methods, and references to seminal works for each ML and DL method are provided [1]. And discuss the challenges and opportunities of using ML / DL for cybersecurity.

2. EXISTING SYSTEM

Most approaches to security in the enterprise have focused on protecting the network infrastructure with no or little attention to end users. As a result, traditional security functions and associated devices, such as firewalls and intrusion detection and prevention devices, deal mainly with network level protection. Although still part of the overall security story, such an approach has limitations in light of the new security challenges described in the previous section.Data Analysis for Network Cyber-Security focuses on monitoring and analyzing network traffic data, with the intention of preventing, or quickly identifying, malicious activity. Risk values were introduced in an information security management system (ISMS) and quantitative evaluation was conducted for detailed risk assessment. The quantitative evaluation showed that the proposed countermeasures could reduce risk to some extent. Investigation into the cost-effectiveness of the proposed countermeasures is an important future work.It provides users with attack information such as the type of attack, frequency, and target host ID and source host ID. Ten et al. proposed a cyber-security framework of the SCADA system as a critical infrastructure using real-time monitoring, anomaly detection, and impact analysis with an attack tree-based methodology, and mitigation strategies

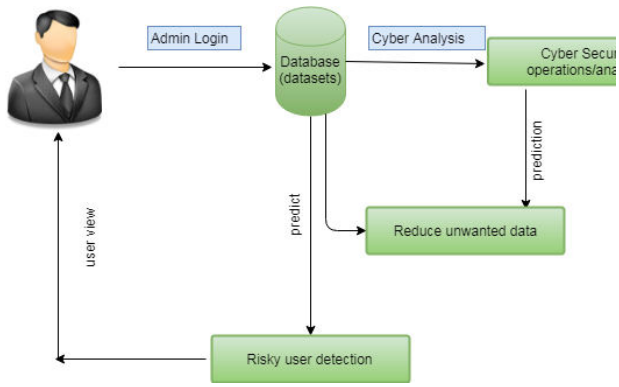
3. PROPOSED SYSTEM:

User-centriccyber security helps enterprises reduce the risk associated with fast-evolving end-user realities by reinforcing security closer to end users. User-centriccyber security is not the same as user security. User-centriccyber security is about answering peoples' needs in ways that preserve the integrity of the enterprise network and its assets. User security can almost seem like a matter of protecting the network from the user — securing it against vulnerabilities that user needs introduce. User-centric security has the greater value for enterprises.cyber-security systems are real-time and robust independent systems with high performances requirements. They are used in many application domains, including critical infrastructures, such as the national power grid, transportation, medical, and defense. These applications require the attainment of stability, performance, reliability, efficiency, and robustness, which require tight integration of computing, communication, and control technological systems. Critical infrastructures have always

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

been the target of criminals and are affected by security threats because of their complexity and cyber-security connectivity. These CPSs face security breaches when people, processes, technology, or other components are being attacked or risk management systems are missing, inadequate, or fail in any way. The attackers target confidentialdata. Main scope of this project in reduce the unwanted data for the dataset.

4. ARCHITECTURE



5. IMPLEMENTATION

CYBER ANALYSIS

Cyber threatanalysis is a process in which the knowledge of internal and external information vulnerabilities pertinent to a particular organization is matched against real-world cyber-attacks. With respect to cyber security, this threat-oriented approach to combating cyber-attacks represents a smooth transition from a state of reactive security to a state of proactive one. Moreover, the desired result of a threat assessment is to give best practices on how to maximize the protective instruments with respect to availability, confidentiality and integrity, without turning back to usability and functionality conditions. CYPER ANALYSIS.A threat could be anything that leads to interruption, meddling or destruction of any valuable service or item existing in the firm's repertoire. Whether of "human" or "nonhuman" origin, the analysis must scrutinize each element that may bring about conceivable security risk.

DATASET MODIFICATION

If a dataset in your dashboard contains many dataset objects, you can hide specific dataset objects from display in the Datasets panel. For example, if you decide to import a large amount of data from a file, but do not remove every unwanted data column before importing the data into Web, you can hide the unwanted attributes and metrics, To hide dataset objects in the Datasets panel, To show hidden objects in the Datasets panel, To rename a dataset object, To create a metric based on an attribute, To create an attribute based on a metric, To define the geo role for an attribute, To create an attribute with additional time information, To replace a dataset object in the dashboard

DATA REDUCTION

Improve storage efficiency through data reduction techniques and capacity optimization using datareduplication, compression, snapshots and thin provisioning. Data reduction via simply deleting unwanted or unneeded data is the most effective way to reduce a storing's data

RISKY USER DETECTION

False alarm immunity to prevent customer embarrassment, High detection rate to protect all kinds of goods from theft, Wide-exit coverage offers greater flexibility for entrance/exit layouts, Wide range of attractive designs complement any store

décor, Sophisticated digital controller technology for optimum system performance

ALGORITHM:

SUPPORT VECTOR MACHINE(SVM)

"Support Vector Machine" (SVM) is a supervised machine learning algorithm which can be used for both classification or regression challenges. However, it is mostly used in classification problems. In this algorithm, we plot each data item as a point in n-dimensional space (where n is number of features you have) with the value of each feature being the value of a particular coordinate. Then, we perform classification by finding the hyper-plane that differentiate the two classes very well (look at the below snapshot). The SVM algorithm is implemented in practice using a kernel. The learning of the hyperplane in linear SVM is done by transforming the problem using some linear algebra, which is out of the scope of this introduction to SVM. A powerful insight is that the linear SVM can be rephrased using the inner product of any two given observations, rather than the observations themselves. The inner product between two vectors is the sum of the multiplication of each pair of input values. For example, the inner product of the vectors [2, 3] and [5, 6] is 2*5 + 3*6 or 28. The equation for making a prediction for a new input using the dot product between the input (x) and each support vector (xi) is calculated as follows:

$$f(x) = B0 + sum(ai * (x,xi))$$

This is an equation that involves calculating the inner products of a new input vector (x) with all support vectors in training data. The coefficients B0 and ai (for each input) must be estimated from the training data by the learning algorithm.

6. CONCLUSION

We provide a user-centered computer learning system that affects large data from various security logs, awareness information, and inspector intelligence. This method provides complete configuration and solution for dangerous user detection for the Enterprise System Operating Center. Select machine learning methods in the SOC product environment, evaluate efficiency, IO, host and users to create user-centric features. . Even with simple mechanical learning algorithms, we prove that the learning system can understand more insights from the rankings with the most unbalanced and limited labels. More than 20% of the neurological model of modeling is 5 times that of the current rule-based system. To improve the detection precision situation, we will examine other learning methods to improve the data acquisition, daily model renewal, real time estimate, fully enhance and organizational risk detection and management. As for future work, let's examine other learning methods to improve detection accuracy

REFERENCES

[1] SANS Technology Institute. □The 6 Categories of Critical Log Information□□ 2013.

[2] A. L. Buczak and E. Guven. □A survey of data mining and machine learning methods for cyber security intrusion detection□, IEEE Communications Surveys & Tutorials 18.2 (2015): 1153-1176.

[3] S. Choudhury and A. Bhowal. □Comparative analysis of machine learning

algorithms along with classifiers for network intrusion detection□, Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2015.

[4] M. J. Kang and J. W. Kang. □A novel intrusion detection method using deep neural network for in-vehicle network security□, Vehicular Technology Conference, 2016.

[5] N. Chand et al. □A comparative analysis of SVM and its stacking with other classification algorithm for intrusion detection□, Advances in Computing, Communication, & Automation (ICACCA), 2016.

[6] K. Goeschel. □Reducing false positives in intrusion detection systems using data-mining techniques utilizing support vector machines, decision trees, and naive Bayes for off-line analysis□, SoutheastCon, 2016.