A CLIENT-ORIENTED MACHINE LEARNING SYSTEM FOR NETWORK SECURITY OPERATIONS CENTER

Ms. Karumudi Hari Chandana #1, Ms. Munnangi Lakshmi Teja #2,
Ms. Kapa Amrutha #3, Ms. Urati Sai Bhavya #4
#1 Student, Dept Of IT, Qis College of Engineering and Technology, Ongole, Prakasam (Dt)
#2 Student, Dept Of IT, Qis College of Engineering and Technology, Ongole, Prakasam (Dt)
#3 Student, Dept Of IT, Qis College of Engineering and Technology, Ongole, Prakasam (Dt)
#4 Assistant professor, Dept Of CSE, Qis College of Engineering and Technology, Ongole, Prakasam

Abstract

So as to guarantee an organization's Internet security, SIEM (Security Information and Event Management) framework is set up to streamline the different preventive advancements and banner cautions for security occasions. Inspectors (SOC) explore alerts to decide whether this is valid or not. In any case, the quantity of alerts as a rule isn't right with the larger part and is more than the capacity of SCO to deal with all mindfulness. Along these lines, pernicious plausibility. Assaults and bargained hosts might not be right. AI is a conceivable way to deal with improving the wrong positive rate and improving the profitability of SOC experts. In this article, we make a client driven specialist learning structure for the Internet Safety Functional Center in the genuine authoritative setting. We examine ordinary information sources in SOC, their work process, and how to process this information and make a viable AI framework. This article is gone for two gatherings of per users. The principal aggregate is keen specialists who have no information of information researchers or PC security fields yet who architect ought to create AI frameworks for machine wellbeing. The second gatherings of guests are Internet security specialists that have profound information and aptitude in Cyber Security, yet do Machine learning encounters don't exist and I'd like to make one independent from anyone else. Toward the finish of the paper, we utilize the record for instance to exhibit full strides from information gathering, name creation, include building, AI calculation and test execution assessments utilizing the PC worked in the SOC generation of Seyondike.

Keywords: *Machine learning, Internet Safety Functional Center, AI framework.*

I. INTRODUCTION

Digital security episodes will cause huge budgetary and notoriety impacts on big business. So as to identify noxious exercises, the SIEM (Security Information and Event The board) framework is worked in organizations or government. The framework relates occasion logs from endpoint, firewalls, IDS/IPS (Interruption Detection/Prevention System), DLP (Data Loss Security), DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), Windows/Unix security occasions, VPN logs and so on. The security occasions can be gathered into various classes [1]. The logs have terabytes of information every day. From the security occasion logs, SOC (Security Operation Focus) group grows alleged use cases with a pre-decided seriousness dependent on the analysts encounters. They are commonly rule based connecting at least one pointers from various logs. These standards can be organize/have based or time/recurrence based. On the off chance that any pre-characterized use case is activated, SIEM framework will create an alarm progressively. SOC investigators will at that point explore the alarms to choose whether the client identified with the alarm is unsafe (a genuine positive) or not (false positive). In the event that they discover the alarms to be suspicious from the examination, SOC experts will make OTRS (Open Source Ticket Request System) tickets.

After starting examination, certain OTRS tickets will be raised to level 2 examination framework (e.g., Co3 System) as serious security episodes for further examination and remediation by Incident Reaction Team. Be that as it may, SIEM normally produces a great deal of the alarms, yet with an extremely high false positive rate. The quantity of alarms every day can be many thousands, substantially more than the limit with respect to the SOC to research every one of them. Along these lines, SOC may explore just the cautions with high seriousness or smother a similar sort of alarms. This could conceivably miss some extreme assaults. Thusly, a progressively insightful and programmed framework is required to distinguish hazardous clients. The AI framework sits amidst SOC work process, joins distinctive occasion logs, SIEM alarms and SOC investigation results and creates exhaustive client chance score for security activity focus. Rather than straightforwardly diving into substantial measure of SIEM alarms and attempting to discover needle in a pile, SOC investigators can utilize the hazard scores from AI framework to organize their examinations, beginning from the clients with most noteworthy dangers. This will incredibly improve their efficiency,optimize their activity line the board, and at last upgrade the undertaking's security.

In particular, our methodology builds a structure of usercentric AI framework to assess client hazard dependent on ready data. This methodology can give security examiner a complete hazard score of a client and security investigator can center on those clients with high hazard scores.

II EXISITING 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.

Disadvantages:

1. Firewalls can be difficult to configure correctly.
2. Incorrectly configured firewalls may block users from performing actions on the Internet, until the firewall configured correctly.
3. Makes the system slower than before.
4. Need to keep updating the new software in order to keep security up to date.
5. Could be costly for average user.
6. The user is the only constant

III PROPOSED SYSTEM

User-centric cyber security helps enterprises reduce the risk associated with fast-evolving end-user realities by reinforcing security closer to end users. User-centric cyber security is not the same as user security. User-centric cyber 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 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 confidential data. Main scope of this project in reduces the unwanted data for the dataset.

Machine Learning Algorithm

In our system, we tried several machine learning algorithms [3][4][5][6][7], including Multi-layer Neural Network (MNN) with two hidden layers, Random Forest (RF) with 100 Ginisplit trees, Support Vector Machine (SVM) with radial basis function kernel and Logistic Regression (LR). In our practice, we find that Multi-layer Neural Network and Random Forest work pretty well for our problem. Some validation results from these models will be shown later.

ADVANTAGES:

1)Protects system against viruses, worms, spyware and other
2) Protection against data from theft.
3) Protects the computer from being hacked.
4) Minimizes computer freezing and crashes.
5) Gives privacy to users.
6) Securing the user-aware network edge
7) Securing mobile users' communications '
8) Managing user-centric security

IV SYSTEM ARCHITECTURE

The complete structure and its components of our proposed system is given by

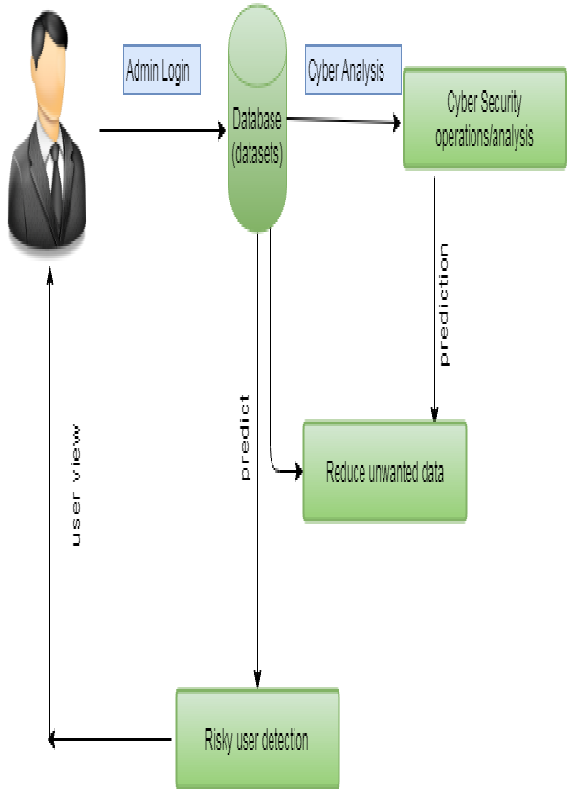

Fig: System structure

CYBER ANALYSIS

Cyber threat analysis 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 data reduplication, 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

V CONCLUSION

In this paper, we present a user-centric machine learning system which leverages big data of various security logs, alert information, and analyst insights to the identification of risky user. This system provides a complete framework and solution to risky user detection for enterprise security operation center. We describe briefly how to generate labels from SOC investigation notes, to correlate IP, host, and users to generate user-centric features, to select machine learning algorithms and evaluate performances, as well as how to such a machine learning system in SOC production environment.

VI REFERENCES

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

[2] X.Li and B "Learning to classify text using positive and unlabeled Data", Proceedings of the 18th international joint conference on Artificial intelligence, 2003

[3] 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.

[4] 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.

[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.

[7] 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.

Authors Profile

Ms. **Karumudi Hari Chandana** pursuing B.Tech in Information Technology from Qis College Of Engineering and Technology (Autonomous & NAAC 'A' Grade), Ponduru Road, Vengamukkapalem, Ongole, Prakasam Dist, Affiliation to Jawaharlal Nehru Technological university, Kakinada in 2015-19, respectively.

Ms. **Munnangi Lakshmi Teja** pursuing B.Tech in Information Technology from Qis College Of Engineering and Technology (Autonomous & NAAC 'A' Grade), Ponduru Road, Vengamukkapalem, Ongole, Prakasam Dist, Affiliation to Jawaharlal Nehru Technological university, Kakinada in 2015-19, respectively.

Ms. **Kapa Amrutha** pursuing B.Tech in Information Technology from Qis College Of Engineering and Technology (Autonomous & NAAC 'A' Grade), Ponduru Road, Vengamukkapalem, Ongole, Prakasam Dist, Affiliation to Jawaharlal Nehru Technological university, Kakinada in 2015-19, respectively.

Ms. **Urati Sai Bhavya** has received her B.Tech and M.Tech. She is dedicated to teaching field from last 2 years. She has guided 3 groups of U.G students. At present she is working as Asst.Professor in Qis College of Engineering And Technology,