iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

CYBERSECURITY THREAT INTELLIGENCE PLATFORM USING AIML

Mrs. Novera Habeeb,
Associate Professor, Department of Artificial Intelligence and Machine Learning,
J.B. Institute of Engineering and Technology, Hyderabad, Telangana, India

Gugulothu Yakub,
Jatoth Anil Nayak, Kethavath Akhil Kumar,
Doddi Manikanta, Vaditya Raju,
Students, Department of Artificial Intelligence and Machine Learning,
J.B. Institute of Engineering and Technology, Hyderabad, Telangana, India

[1] noverahabeeb543@gmail.com [2] yakubnayakguguloth4@gmail.com [3] jatothanilnayak2@gmail.com [4] akhilkumarkethavath@gmail.com [5] vadithyaraju34@gmail.com[6]

ABSTRACT

It has a major concern modern era continuously in terms of sophistication and scale traditional antivirus software are heavily reliant on signature-based detection and pre-defined rule sets to identify malicious activity while these methods in identifying known fail new cyberattacks zero-day ai-driven moreover extensive adoption of cloud computing iot devices and remote work spaces has brought new challenges making traditional incapable end-to-end focuses an ai-driven cybersecurity system strengthens through automation envisioned system uses machine learning algorithms behavior anomaly detect more precisely system is able to scan large amounts of security logs correlate predict security breaches before are able to cause extensive damage big analytics artificial system reduces false positives minimizes time active contemporary it environments.

1. INTRODUCTION

The fast pace of technological development has led to a greater dependence on digital platforms for communication data storage and business while this digital revolution has many advantages it has subjected individuals various types have targeting systems banks personal therefore critical the of digital assets be a fundamental part of contemporary computing one of the largest problems with legacy solutions predefined rule sets and signature-based detection legacy can detect only known attacks and do a poor job detecting new or unknown attacks cyber criminals always attack in order to circumvent legacy security controls left constantly struggling to stay protected legacy security controls also generate large numbers of alarms most are false positives teams are usually overwhelmed by alarms leads to delays in uncovering and acting legitimate growing sophistication together failings legacy has an imperative artificial machine learning are among the top cybersecurity technologies they are able handle sets learn may present a breach ai powered are unlike because are able to learn and continuously and become more effective in protecting through ai powered solutions able improve at detecting and preventing cyber threats in real time reducing financial loss data exposure and reputation damage.

2. LITERATURE SURVEY

Literature survey this literature survey presents recent research on cybersecurity threat intelligence ai-based solutions the purpose of survey is to review past research determine their contributions mention research legacy controls primarily on signature-based detection whereby predefined known attacks are used a number of studies have examined the effectiveness legacy controls snort ids roesch 1999 as an older system ids snort uses known attack signatures in detecting known attacks firewall-based security cheswick bellovin 1994 firewalls have been used for years to block unauthorized access to networks in contrast to traditional measures systems learn patterns attacks detection deep learning sharma et al 2020 researchers proposed a malware classification system

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

based on deep learning with higher accuracy compared to conventional antivirus software the study demonstrated that malware behavior could be identified more efficiently with the help of convolutional neural networks cnns and recurrent neural networks anomaly detection systems ahmed et al 2019 the study examined unsupervised ml techniques detecting system clustering like k-means and db scan identified patterns were likely ai-powered threat intelligence 2021 researchers proposed an ai powered threat intelligence system that collects processes logs actionable attack framework 2018 a globally recognized framework classifies cyberattack use to analyze adversary stance al 2020 the authors considered whether virus total ibm x-force were beneficial it was determined from the study real-time enhance security visibility but must be supported with automated correlation functions to remove false positives these studies highlight the requirement in-real-time ai-driven predictive modeling to neutralize efficiently.

3.METHODOLOGY

the methodology applied in project is systematic and structured to ensure an intelligent monitoring system capable once the problem is determined second is preprocessing quality quantity are the only two parameters on which the efficiency of any machine learning-based system depends for project are gathered related repositories sniffers simulated contain behavior and system activity logs for the purpose of ensuring high-quality data preprocessing steps are carried out such as duplicate removal handling missing values numerical value normalization and feature selection for model training preprocessed performance machine final phase of the methodology focuses on future improvements an evolving domain are constantly being evade security for long-term effectiveness the system can be upgraded with sophisticated deep learning algorithms threat systems future improvement can include the addition behavioral improving alert mechanisms cloud-based systematic approach system is made highly efficient scalable and identify real time through machine learning able to learn new thereby be adaptive in responding to potential emerging through of a user-friendly dashboard experts are able to monitor network activity effectively while the backend and database modules are make system operate methodology followed in this system for cybersecurity monitoring is a structured and integrated one to develop an efficient smart anomaly given the increasing sophistication and complexity of the is also designed through the implementation of machine learning and behavior analysis.

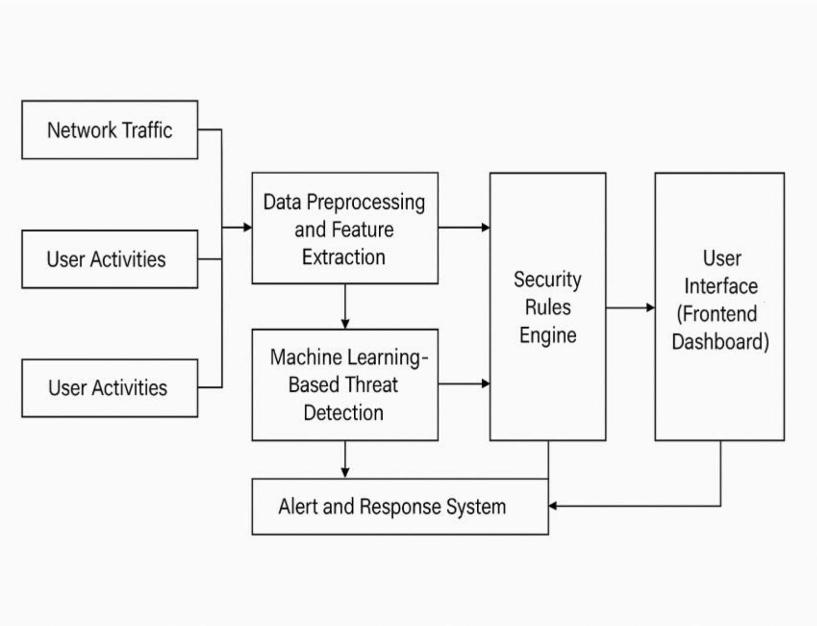
Network Traffic
User Activities
User Activities
Data Preprocessing and Feature Extraction
Machine Learning-Based Threat Detection
Security Rules Engine
User Interface (Frontend Dashboard)
Alert and Response System

Figure 6.1 System Architecture Block Diagram

The image system architecture block diagram the final phase of the methodology focuses of future enhancements ever-evolving field attackers develop new bypass ensure long-term effectiveness the system can be enhanced advanced deep learning models networks response mechanisms future improvements may incorporating behavioral enhancing alert mechanisms immediate detected threats cloud-based infrastructures broader coverage image.

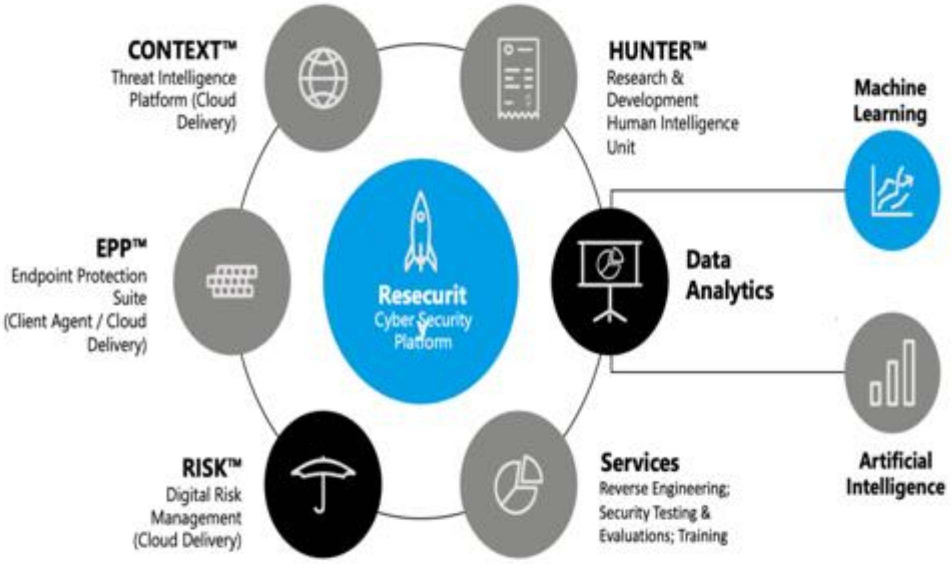
CONTEXT™
Threat Intelligence Platform (Cloud Delivery)
HUNTER™
Research & Development Human Intelligence Unit
Machine Learning
EPP™
Endpoint Protection Suite (Client Agent / Cloud Delivery)
Resecurit
Cyber Security Platform
Data Analytics
RISK™
Digital Risk Management (Cloud Delivery)
Services
Reverse Engineering; Security Testing & Evaluations; Training
Artificial Intelligence

Figure 6.2 **Cybersecurity threat intelligence using AIML**

4. APPLICATIONS

The monitoring a tool safeguarding confidential network infrastructures from possible cyber attacks with of iot devices on rise has emerged as a top agenda for individuals organizations and governments enterprises hold huge amounts of customer data financial data and intellectual property making them a soft target for cyber attacks such cyber attacks particularly on the above-mentioned sectors have disastrous consequences ranging from leakage of espionage sabotage monitoring system assists in the robustness national detecting unauthorized access government the system is highly beneficial in detecting advanced persistent threats apts where sophisticated techniques are employed by hackers to infiltrate sensitive systems over a long duration of time leveraging the strengths of anomaly government agencies proactive steps towards position cyber criminals employ fraudulent transactions identity theft and account takeover techniques to attack financial institutions this system of is required for monitoring banking transactions abnormal spending patterns fraud.

5.CONCLUSION

The cybersecurity monitoring system developed in this project is highly effective detecting log using with the assistance of a flask-based backend a react js- based frontend and mongodb as overall objective of the system is malicious activity alert thus reducing the possibility minimizes human intervention time immediate there vast scope for development and enhancements in the future the system can be deployed on cloud platforms such as aws, azure or google cloud to enhance accessibility and scalability overall the suggested system monitoring project is a robust foundation automated combining techniques it provides a cost-effective scalable infrastructure further enhancements and developments the system can be developed into an extremely advanced ai-based solution for that counter cyber.

REFERENCES

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

1. Good fellow i bengio y courville a 2016 deep learning mit press a textbook that encompasses the deep learning principles architectures and applications which can be useful to learn ai-based anomaly
2. Bishop c m 2006 pattern recognition springer the book gives thorough information on machine learning methods statistical pattern recognition and probabilistic models to cybersecurity.
3. Stallings w 2017 cryptography and network security principles and practice pearson provides basic principles methods encipherment controls which form the core of network infrastructure protection.
4. Mcgregor j d sykes d a 2001 a practical guide to testing object-oriented software addison-wesley discusses software testing methodologies such as security testing in developing robust software.
5. Sommerville i 2015 software engineering pearson provides software engineering best practices like system design procedures and secure code practices that apply to creating cyber security solutions.
6. Provos n holz t 2007 virtual honeypots from botnet tracking to intrusion detection addison-wesley explains the application of honeypots in identifying gathering attack methods.
7. Tanenbaum a s wetherall d 2019 computer networks pearson covers networking fundamentals protocols intrusion tools included in cybersecurity systems.
8. Schutt r oneil c 2013 doing data science straight talk from the frontline oreilly media provides insights into data science techniques like feature engineering and predictive analytics used in cybersecurity anomaly detection.
9. Scarfone k mell p 2007 guide to intrusion detection and prevention systems idps national institute of standards and technology nist explores architectures methods used in the identification of network traffic-based cyber attacks.