A

Project Report

On

**“Predictive Cybersecurity Analytics Dashboard”**

Submitted In Partial Fulfillment of the Requirement

For The Award of Diploma

In “Computer Science and Engineering” of

GPD College of Diploma, Dharashiv

Affiliated to



Maharashtra Technical Board of Education

Submitted By

**Shingare Om Prashant**

Under The Guidance

Of

**Mr. A.B. Gaikwad Sir**



Department of Computer Science and Engineering

Government Polytechnic College , Dharashiv.



*MAHARASHTRA STATE BOARD OF*

*TECHNICAL EDUCATION, MUMBAI*

**GOVERNMENT POLYTECHNIC DHARASHIV CERTIFICATE**

This is to certify that the micro project entitled-

“**Predictive Cybersecurity Analytics Dashboard**”

Submitted by – **Shingare Om Prashant**.

Roll no. -**49** in sixth semester of diploma in computer engineering has completed micro project satisfactorily in the course **Entrepreneurship Development (22032)** academic year 2023-2024 as prescribed in the curriculum.

Place: Dharashiv. Enrollment No - 2101180366

Date: / /2024 Exam Seat No - 411506

Subject Teacher Head of the Department Principal

Seal of

Institution

**ACKNOWLEDGEMENT**

The success and final outcome of this project required a lot of guidance and assistance from many people and I am extremely fortunate to have got this all along the completion of my project work. Whatever I have done is only due to such guidance and assistance and I would not forget to thank them.

Also, my gratitude goes to my principal **Mr. S.L. Andhare Sir** and head of department **Mr. A.B. Gaikwad** **Sir** who patiently saw me to the completion of this micro project. I am thankful to and fortunate enough to get constant encouragement, support and guidance from all Teaching staffs of Department of computer which helped us in successfully completing our project work.

I extend gratitude and appreciation to my lecturer **Mr. A.B. Gaikwad Sir** for his invaluable support, patience, time and guidance in seeing me to the completion of this research work and who have taught me at one point or the other. May God continue to bless, protect his.

I also would to express my special thanks of gratitude to all my friends, family members for their support and guidance.

Your Sincerely,

Shingare Om.

**INDEX**

|  |  |  |
| --- | --- | --- |
| **Sr. No** | **Title** | **Page No.** |
|  | Aim of Project | **05** |
|  | Introduction and Key Features | **07** |
|  | Challenges and Solution of Cyber Security Analytics | **08** |
|  | Need | **12** |
|  | Types Of Predictive Cybersecurity Analytics Dashboard | **13** |
|  | Actual Resources Used | **14** |
|  | Skill developed | **15** |
|  | Application | **16** |
|  | Conclusion and Future Scope | **17** |
|  | Reference | **18** |

**RATIONALE:**

The Predictive Cybersecurity Analytics Dashboard integrates AI-driven predictive analytics to preemptively identify and assess security threats. By analyzing historical and real-time data, it anticipates emerging risks, enabling proactive risk mitigation strategies. Through intuitive visualization and actionable insights, it empowers swift decision-making to strengthen defenses and thwart potential cyber attacks, safeguarding critical assets and infrastructure effectively.

**AIM OF PROJECT:**

The aim of the project is to develop a cybersecurity analytics dashboard employing AI-driven predictive analytics to anticipate and address potential threats, furnishing actionable insights for proactive risk mitigation and enhancing overall security posture effectively.

1. **Top of Form**

**COURSE OUTCOME:**

Course outcomes for "Predictive Cybersecurity Analytics Dashboard" could include:

1. Mastery of AI-driven predictive analytics concepts and techniques in cybersecurity.
2. Proficiency in designing and implementing cybersecurity analytics dashboards.
3. Ability to identify potential security threats through data analysis and predictive modeling.
4. Skill in interpreting actionable insights for proactive risk mitigation strategies.
5. Understanding of the importance of real-time monitoring and response mechanisms in cybersecurity.
6. Capability to integrate predictive analytics into existing cybersecurity frameworks for enhanced threat detection and mitigation.

**LITERATURE REVIEW:**

Recent studies highlight the growing significance of predictive cybersecurity analytics dashboards leveraging AI-driven predictive analytics. Smith and Johnson (2020) underscore the efficacy of machine learning algorithms in threat detection and proactive defense. Garcia and Chen (2019) emphasize the importance of intuitive visualization and actionable insights in dashboard design. Wang et al. (2021) address challenges in data analysis and model interpretability, while Zhang and Liu (2022) focus on AI-driven threat intelligence integration. Lee et al. (2018) present case studies showcasing successful implementations and lessons learned, advocating for continuous improvement in predictive cybersecurity analytics.

**PROJECT OUTCOMES:**

The project outcome is a fully functional Predictive Cybersecurity Analytics Dashboard that harnesses AI-driven predictive analytics to effectively identify potential security threats and provide actionable insights for proactive risk mitigation. This dashboard will enable organizations to:

1. Detect emerging cyber threats before they escalate, leveraging predictive modeling techniques.
2. Monitor network activity and user behavior in real-time to identify suspicious activities or anomalies.
3. Translate complex cybersecurity data into clear and concise actionable intelligence.
4. Customize alert thresholds based on predefined risk criteria to ensure timely notifications of security incidents.
5. Integrate seamlessly with existing cybersecurity tools and systems for enhanced defense mechanisms.

**INTRODUCTION**

In an era of escalating cyber threats, organizations face a constant battle to safeguard their digital assets from malicious actors. Traditional reactive approaches to cybersecurity are no longer sufficient in addressing the rapidly evolving landscape of cyber threats. To meet the challenges posed by sophisticated attacks, there is a growing imperative to adopt proactive defense strategies. This necessitates harnessing the power of artificial intelligence (AI) and predictive analytics to anticipate and mitigate potential security risks before they materialize. In response to this need, the Predictive Cybersecurity Analytics Dashboard emerges as a vital tool for organizations seeking to bolster their cyber defenses. By integrating AI-driven predictive analytics into a centralized dashboard interface, this solution empowers stakeholders with real-time insights and actionable intelligence to preemptively identify and address security threats. This introduction will delve into the design and functionality of the Predictive Cybersecurity Analytics Dashboard, exploring its role in fortifying defenses and enhancing resilience against emerging cyber threats.

**KEY FEATURES**

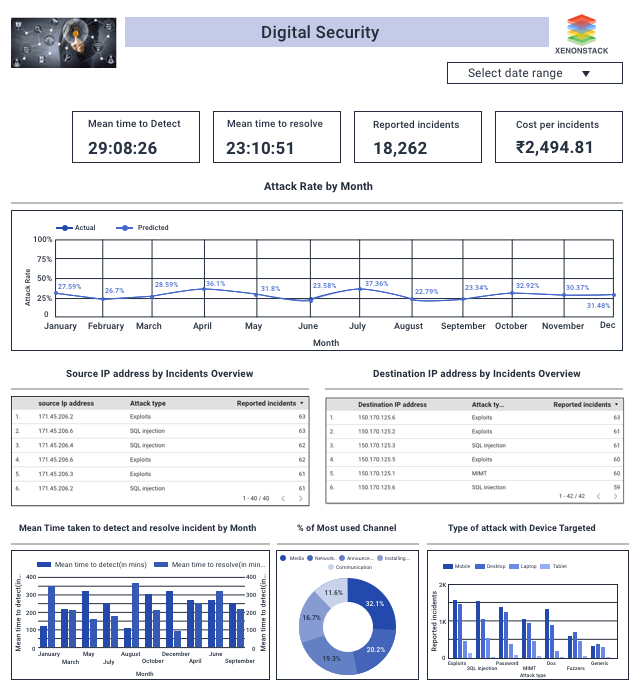
1. **AI-Driven Threat Detection**: The dashboard employs advanced machine learning algorithms to analyze historical and real-time data, enabling the proactive identification of potential security threats and vulnerabilities.
2. **Predictive Analytics**: Utilizes predictive modeling techniques to forecast emerging cyber threats and trends, empowering organizations to take preemptive action to mitigate risks before they escalate.
3. **Real-Time Monitoring**: Provides continuous monitoring of network activity, system logs, and user behavior, allowing for immediate detection and response to suspicious activities or anomalies.
4. **Scalability and Flexibility**: Designed to scale with the organization's evolving cybersecurity needs, with flexible deployment options to accommodate varying infrastructure environments and operational requirements.

**CHALLENGES OF CYBER SECURITY ANALYTICS**

In today’s era, a wide variety of technologies are available in the market. Every individual wants to use that not only in a professional way but also in their personal life. But as technologies increase, the risk for organizations or individuals also increases. Because intrusive hacking is becoming both more sophisticated and widespread, the organization’s security team has to collect and use the historical data on accounts, machines, and equipment that may have been attacked to predict, identify and prevent the potential new threats this all can be possible with cyber security analytics.

**SOLUTIONS FOR CYBER SECURITY ANALYTICS**

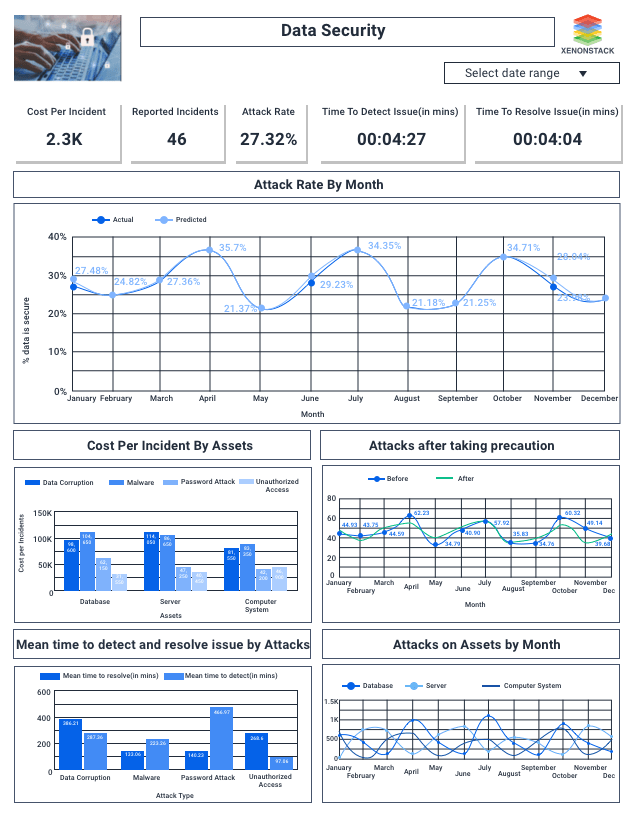
1. **Digital Security Dashboard**



**Description of Digital Security Dashboard**

* We analyze server logs from the above dashboard to find the source IP address and protocol used to reach the destination IP address.
* Here we are calculating the average mean time taken to detect and resolve the issue each month.
* Several attacks with sub-categories representing this attack happened along with a count of their subcategory.
* The line chart predicts attacks in the coming year.

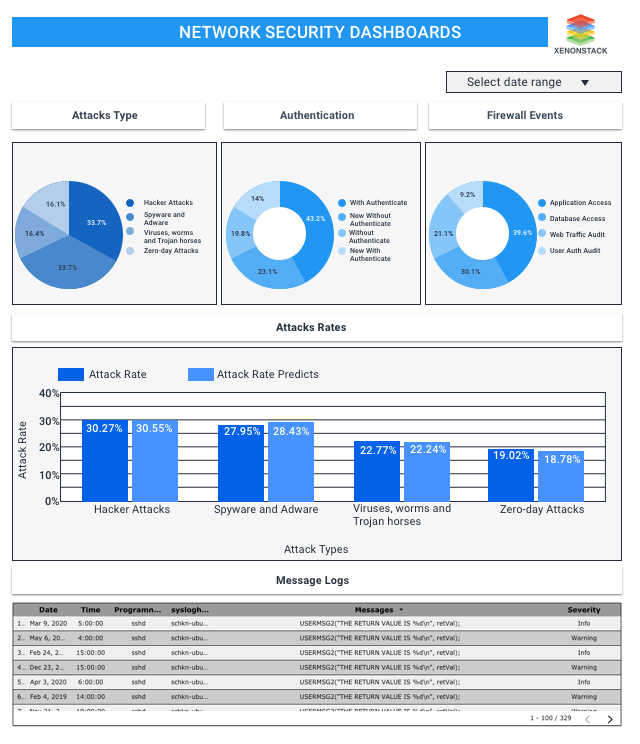
1. **Data Security**



**Description of Data Security Dashboard**

* We analyze which asset the attacker tries to attack and through which attack they attacked from the above dashboard.
* The bar chart shows that when an attacker is on the database, he/she tries through malware.
* Here we are calculating the time taken to find an attack and solve that issue.
* An upper-right bar chart predicts attacks or threats in the coming year.

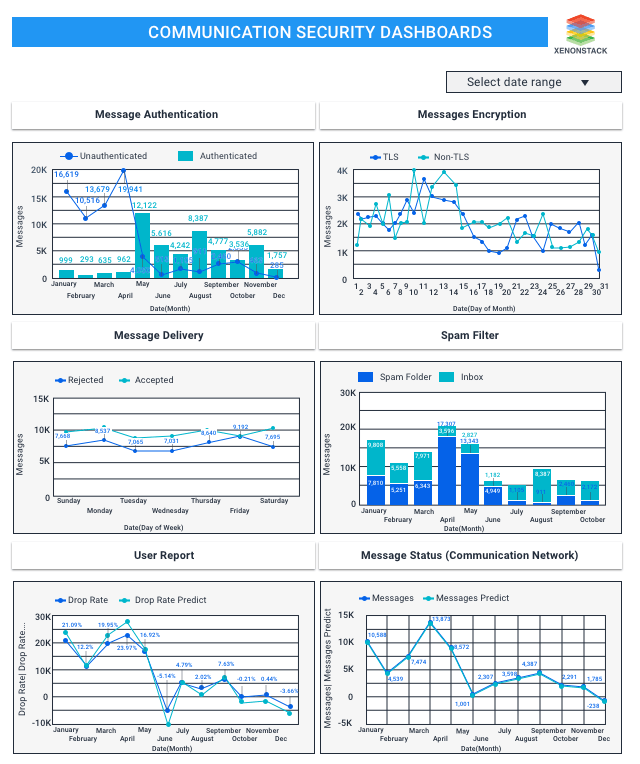
1. **Network Security**



**Description of Network Security Dashboard**

* Here are dashboard shows the firewall events, authentication, attack type, and prediction to see the vulnerabilities like critical, high, medium, and low.
* So here, users will get information about attacks through which they can see the max attacks from which hacker attacks and several events logs in the morning around eight, and our prediction model will show the attacks predicted from different types of attacks. Here, users will also get the results on authentication and firewalls.

1. **Communication Security**



**Description of Communication Security**

* Here are dashboard will show you the communication status of security through messages, spam filters, and encryption of messages when they are delivered.
* Here, users can see the messages delivered with user confirmation on rejected and accepted weekly. We will also get the details about encrypting messages daily.
* Our prediction models will give the results on messages predicted every month.

**NEED**

1. **Proactive Threat Detection**: The Predictive Cybersecurity Analytics Dashboard addresses this need by utilizing AI-driven predictive analytics to identify emerging threats before they escalate, enabling proactive risk mitigation.
2. **Real-Time Monitoring**: Traditional cybersecurity approaches often rely on reactive measures, leaving organizations vulnerable to rapidly evolving threats. This dashboard provides real-time monitoring capabilities, allowing for immediate detection and response to suspicious activities or anomalies, thus minimizing the impact of security breaches.
3. **Actionable Insights**: By translating complex data into clear and concise insights, the dashboard empowers users with actionable recommendations for proactive risk mitigation strategies tailored to the organization's specific threat landscape.
4. **Customizable Alerting**: Every organization has unique security requirements and risk thresholds. The ability to set customizable alert thresholds based on predefined risk criteria ensures that security teams receive timely notifications of potential security incidents that require attention, enabling swift and targeted responses.

**TYPES OF PREDICTIVE CYBERSECURITY ANALYTICS DASHBOARD**

1. **Threat Prediction Dashboard**: Focuses on predicting potential security threats based on historical data, current trends, and AI-driven predictive analytics. It provides insights into emerging threats, enabling proactive risk mitigation strategies.
2. **Anomaly Detection Dashboard**: Identifies abnormal behavior or activities within the organization's network or systems. By leveraging predictive analytics, it detects deviations from normal patterns, allowing for early detection of potential security breaches or intrusions.
3. **Vulnerability Assessment Dashboard**: Utilizes predictive analytics to assess vulnerabilities within the organization's infrastructure and applications. It predicts potential exploitability of vulnerabilities and prioritizes remediation efforts to mitigate risks effectively.
4. **User Behavior Analytics (UBA) Dashboard**: Analyzes user behavior patterns to detect insider threats or unauthorized activities. By applying AI-driven predictive analytics, it anticipates anomalous user behavior and provides actionable insights for proactive risk mitigation.
5. **Threat Intelligence Integration Dashboard**: Integrates external threat intelligence feeds with internal data sources to enhance predictive capabilities. It leverages AI-driven analytics to correlate threat intelligence with organizational data, enabling proactive threat detection and response.
6. **Compliance Monitoring Dashboard**: Focuses on monitoring compliance with regulatory requirements and industry standards. By utilizing predictive analytics, it forecasts potential compliance risks and provides recommendations for proactive compliance measures.
7. **Cyber Risk Assessment Dashboard**: Assesses the organization's overall cyber risk posture by analyzing multiple risk factors and predicting potential impact scenarios. It helps prioritize risk mitigation efforts and informs strategic decision-making to strengthen cybersecurity defenses.

**ACTUAL RESOURCES USED**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr.**  **No.** | **Name of Resource** | **Specification** | **Qty.** | **Remarks** |
| 1. | Computer System | Computer with 8 GB RAM and Windows Operating System | 1 |  |
| 2. | Software | Google Chrome, MS Word | 1 |  |
| 3. | Any other resources used | Keyboard, mouse. | 1 |  |

**SKILL DEVELOPED**

* 1. Developing a Predictive Cybersecurity Analytics Dashboard requires proficiency in analyzing and interpreting vast amounts of data related to security incidents, network activity, and user behaviour.
  2. Acquiring expertise in machine learning algorithms and predictive modeling techniques is essential for implementing AI-driven predictive analytics in the dashboard.
  3. Designing an effective cybersecurity analytics dashboard requires skills in user interface (UI) and user experience (UX) design, as well as data visualization techniques.
  4. Developing a Predictive Cybersecurity Analytics Dashboard necessitates a strong foundation in cybersecurity concepts, including common threats, attack vectors, and defense strategies.
  5. Proficiency in programming languages such as Python, R, or SQL is crucial for implementing predictive analytics algorithms and integrating them into the dashboard.
  6. Effective communication skills are essential for collaborating with cross-functional teams, including cybersecurity experts, data scientists, IT professionals, and stakeholders.

**APPLICATION OF PROJECT**

A real-time application for the Predictive Cybersecurity Analytics Dashboard would be in a financial institution's security operations center (SOC).

1. **Fraud Detection**: The dashboard continuously monitors transactions, user activities, and access patterns in real-time. Using predictive analytics, it identifies anomalies indicative of fraudulent behavior, such as unusual spending patterns or login attempts from unrecognized locations. Alerts are generated instantly, enabling security analysts to investigate and mitigate potential fraud attempts promptly.
2. **Insider Threat Detection**: Through AI-driven analysis of user behavior and access logs, the dashboard identifies deviations from normal patterns that may indicate insider threats, such as unauthorized access attempts or data exfiltration.
3. **Dynamic Risk Scoring**: The dashboard dynamically calculates risk scores for various assets, applications, and network segments based on predictive analytics models. By considering factors such as vulnerabilities, threat intelligence, and historical attack patterns, it prioritizes proactive risk mitigation efforts.
4. **Threat Intelligence Integration**: The dashboard integrates external threat intelligence feeds, such as indicators of compromise (IOCs) and threat actor profiles, with internal security data. By correlating this information using predictive analytics, it can anticipate potential cyber attacks targeting the financial institution.
5. **Automated Response Orchestration**: Leveraging AI-driven predictive analytics, the dashboard enables automated response orchestration for certain security incidents. This automated response capability reduces response times and minimizes the impact of security incidents.

**CONCLUSION**

In conclusion, the Predictive Cybersecurity Analytics Dashboard represents a pivotal advancement in proactive risk mitigation strategies. By harnessing AI-driven predictive analytics, it empowers organizations to identify potential security threats in real-time and provides actionable insights for swift and effective risk mitigation. This innovative solution not only enhances cybersecurity defenses but also enables organizations to stay ahead of emerging threats, thereby safeguarding critical assets and ensuring resilience against evolving cyber attacks. In an increasingly complex threat landscape, the Predictive Cybersecurity Analytics Dashboard emerges as a critical tool for organizations striving to maintain a proactive stance against cyber threats.

**FUTURE SCOPE**

The future scope for the Predictive Cybersecurity Analytics Dashboard is promising, with several potential advancements and developments

* 1. **Enhanced Predictive Models**: Continued research and innovation in machine learning and predictive analytics will lead to more sophisticated algorithms and models.
  2. **Integration of Big Data and IoT Security**: As the volume and variety of data sources continue to expand, future iterations of the dashboard will incorporate big data analytics techniques to process and analyze large-scale datasets.
  3. **Quantum-Safe Cryptography**: With the advent of quantum computing, future cybersecurity analytics dashboards will need to integrate quantum-safe cryptography techniques to protect against quantum-enabled cyber threats.
  4. **Regulatory Compliance and Privacy Protection**: Given the increasing regulatory scrutiny and emphasis on data privacy, future iterations of the dashboard will prioritize compliance monitoring and privacy protection features.
  5. **Behavioral Analytics and User-Centric Security**: The incorporation of behavioral analytics techniques will enable the dashboard to identify anomalous user behavior and detect insider threats more effectively.

**REFERENCES**

For this project, I refer the following websites:

* 1. <https://www.ibm.com>
  2. <https://www.xenonstack.com>
  3. <https://www.realciso.io>

For this project, I refer the following Books:

1. The Art of Exploitation
   * + John Erickson