**A black background with white text

Description automatically generated with medium confidence**

**Dissertation Proposal Form**

**Date of Submission:**

|  |  |
| --- | --- |
| **Name** | Charan Kumar Naidu Mallarapu |
| **Student Id** | 220166249 |
| **Module Code** | COM7042M |
| **Project Title** | CyberShield: Fortifying Betting Security Through IDS & ELK Integration |
| **Supervisor Name** | Dr. Soonleh Ling |
| **Supervisor Approval** | Yes |
| **Supervisor Signature** |  |

**Section 1: Academic**

*This section helps Academic staff assess the viability of your project. It also helps identify the most appropriate supervisor for your proposed research. This proposal will be referred to as a point of discussion by your supervisor in seminar sessions.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NAME:** Charan Kumar Naidu Mallarapu | **STUDENT NUMBER:** 220166249 | | | | |
| **PROPOSED TITLE OF PROJECT:**  CyberShield - Fortifying Betting Security Through IDS & ELK Integration | | | | | |
| **BRIEFLY DESCRIBE YOUR FIELD OF STUDY:**  This project focuses on enhancing the cybersecurity measures in online sports betting industry. This is achieved by integrating two key technologies: Intrusion Detection System (IDS) and Elasticsearch, Logstash, Kibana (ELK Stack).  The IDS is used to monitor network traffic for patterns indicative of cyberattacks, such as unusual login attempts, outbound connections to known malicious domains, or sudden spikes in traffic. On the other hand, ELK is a powerful platform that collects and processes data from multiple data sources, stores that data in one centralized data store, and provides a set of tools to analyse the data.  This project aims to address common cybersecurity challenges in the industry, such as unauthorised access, DDoS attacks, Real time monitoring, Automated responses and robust logging. By integrating IDS and ELK, the goal is to enhance the ability to detect and respond to these cybersecurity challenges, ultimately strengthening the overall security posture of organizations in online sports betting industry.  The field of study to be used for this project is as follows:  **Cyber Security**  Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It encompasses various categories, including network security, application security, information security, and operational security. Cybersecurity measures aim to protect systems, applications, computing devices, sensitive data, and financial assets against a wide range of cyber threats, from simple computer viruses to sophisticated ransomware attacks.  The cybersecurity landscape in the betting industry is critical due to the sensitive nature of financial transactions, personal information, and the constant threat of cyber-attacks. The betting industry is an attractive target for cybercriminals, making cybersecurity a top priority. Continuous monitoring, proactive measures, and a commitment to staying ahead of emerging threats are essential for maintaining a secure and trustworthy betting platform.  **Data Science**  Data science is a cross-disciplinary field that utilizes scientific methods, algorithms, and systems to extract insights and knowledge from both structured and unstructured data. Drawing on expertise from areas such as statistics, computer science, machine learning, and domain-specific knowledge, data science aims to uncover patterns, make predictions, and provide valuable support for decision-making processes.  Data science models can analyse historical betting data to identify patterns and trends. Predictive analytics allows the industry to forecast outcomes, set odds, and make informed decisions on betting markets. Data-driven models can analyse historical data, current market conditions, and other relevant factors to optimize odds and payouts. This ensures that the odds offered by the betting platform are competitive, reflecting the underlying probabilities accurately. Also, data science techniques, including anomaly detection and pattern recognition, are applied to identify fraudulent activities and enhance security. | | | | | |
| **WHAT QUESTION DOES YOUR PROJECT SEEK TO ANSWER?**  This project seeks to answer the following questions:   1. Can integration of Intrusion Detection System (IDS) and Elasticsearch, Logstash, Kibana (ELK) enhance the cybersecurity measures in the online sports betting industry?   By leveraging IDS and ELK, organizations can effectively detect and respond to common cybersecurity threats such as data breaches, unauthorised access DDoS attacks, ultimately strengthening the overall security posture of the online sports betting platforms.   1. How can we implement an effective real-time unauthorized access detection technique, to promptly identify and respond to potential security threats in a computer system or network?   By training the system with historical data, it can promptly identify deviations from normal behaviour, enabling swift responses to potential security threats in a computer system or network.   1. What are the potential benefits of IDS and ELK integration for online sports bettings beyond cybersecurity enhancement? | | | | | |
| **WHAT HYPOTHESIS ARE YOU SEEKING TO TEST?**  Here are some potential hypotheses:  Null hypothesis(H0): Online betting industry that effectively implement IDS and ELK integration will experience a reduction in cybersecurity incidents.  Alternative hypothesis(H1): Online betting industry that fail to implement IDS and ELK integration will be at a higher risk of experiencing cyberattacks, leading to data breaches, financial losses, and reputational damage. | | | | | |
| **WHAT ARE THE PROBABLE PROJECT OUTCOMES?**  The probable project outcomes are:  **Encompassing enhanced cybersecurity**  Effective implementation of IDS and ELK integration can significantly strengthen the cybersecurity posture of online betting industry, reducing the likelihood of cyberattacks and minimizing their impact.  **Improved data analytics**  Integration of IDS and ELK provides valuable insights into user behaviour and betting patterns which enables betting industry to optimize their strategies and operations.  **Optimized operational efficiency.**  IDS and ELK integration can contribute to improved operational efficiency in several aspects such as Automated Tasks and Processes, Streamlined Communication and Collaboration, Reduced Downtime and Maintenance Costs.  Potential publication in international conferences. | | | | | |
| **PLEASE PROVIDE A BRIEF BIBLIOGRPAHY OF 2-4 KEY TEXTS FOR YOUR STUDY (USE HARVARD REFERENCE STYLE)**   1. ESPN.com. (2022). *Source: FBI probing attack of online sportsbooks*. [online] Available at: <https://www.espn.com/sports-betting/story/_/id/35156137/source-fbi-investigating-cyberattack-online-sportsbooks> [Accessed 12 Dec. 2023]. 2. ‌Bace, R. and Mell, P. (n.d.). NIST Special Publication on Intrusion Detection Systems NIST Special Publication on Intrusion Detection Systems. [online] Available at: <https://apps.dtic.mil/sti/tr/pdf/ADA393326.pdf>. 3. Amoany, E. (n.d.). An introduction to monitoring using the ELK Stack. [online] Enable Sysadmin. Available at: <https://www.redhat.com/sysadmin/what-is-elk-stack>. 4. Stellmacher, D., Shrimpton, H. and Camilleri, E. (2021). Cyber and Gambling Cyber security in the gambling and lottery sector. [online] Available at: <https://www.ncsc.gov.uk/files/NCSC-Cyber-and-Gambling-report-2021.pdf>. 5. www.feedconstruct.com. (n.d.). *The Data Behind Sports Betting - Machine Learning and Data Science*. [online] Available at: <https://www.feedconstruct.com/blog/the-data-behind-sports-betting-machine-learning-and-data-science#:~:text=Data%20science%20is%20a%20field%20that%20provides%20methods> [Accessed 12 Dec. 2023]. | | | | | |
| **PLEASE NAME ANY MEMBER OF THE ACADEMIC TEAM YOU HAVE DISCUSSED THIS POTENTIAL PROJECT:**  NA | | | | | |
| ***(staff use only) Project Approved by Academic Team?*** | | YES |  | NO |  |
| *Any other Academic Staff comments*  ***Student can proceed with the project based on the current status of RP but the following comments need to be considered:***   1. ***The key questions should be clearly mapped to a set of performance metrics which will be helpful during the project execution later.*** 2. ***System architecture diagram needs to be improved to incorporate ELK and other components of the proposed system.*** 3. ***It is desirable to include the research methodology, system development details and project milestones, please provide some elaboration on the project timeline in Figure 4.*** 4. ***The technical outputs of the project need to be improved to ensure the right project deliverables.***   ***Student needs to take all the above into consideration when executing the project.*** | | | | | |

**Section 2: Technical**

*This section is designed to help the technical team ensure the appropriate equipment to support each project has been ordered. It also exists to help you fully ascertain the technical requirements of your proposed project. In filling out this section please note that we do not ‘buy’ major items of equipment for student projects. However, if a piece of equipment has a use to the department beyond the scope of a single project, we will consider purchasing it. Though purchasing equipment through the university is often a slow process.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PLEASE DESCRIBE YOUR PROJECT IN TECHNICAL TERMS:**  The main aim of this project is to build an integrated system with IDS and ELK for online betting platforms to detect and prevent cybersecurity threats this project combines various technologies and strategies to enhance the ability to detect, respond to, and analyse security threats in real-time, with a particular focus on unauthorized access prevention, continuous monitoring, and automated incident response.  The key challenge is to detect an intrusion continuously and provide an automated response. Intrusions can occur from both internal and external sources. Internal intrusions may involve unauthorized access from friends, partners, employees, or even disgruntled clients who have gained access to the networking system. External intrusions, also known as internet attacks, involve intrusions from outside the network system.  **System Architecture**    Figure : Typical IDS System Architecture  A typical intrusion detection system (IDS) architecture consists of three main components:  1. **Sensors:** Sensors collect data from the network or host systems. They can be either software-based or hardware-based. Software-based sensors are installed on the target systems, while hardware-based sensors are deployed on the network infrastructure.  2. **Centralized Collection and Analysis Engine**: The centralized collection and analysis engine receives data from sensors and analyses it for signs of intrusion. It can use various detection techniques, such as signature-based detection, anomaly-based detection, and stateful protocol analysis.  3. **Response Engine**: The response engine acts if it detects an intrusion. The actions can include generating alerts, triggering firewalls to block malicious traffic, or isolating infected hosts.  A diagram of a computer network  Description automatically generated  Figure : Overall CyberShield System Architecture (not a good diagram)  This is the overall system architecture where we place a NIDS (Network IDS) agent which is integrated with IDS and ELK this agent will continuously monitor and Continuous monitoring involves a vigilant watch over the network's activities, akin to having a security guard on constant duty. If any unusual or potentially harmful activity is detected, the system can take immediate action. Automated responses alleviate the need for human intervention in addressing potential security issues. The system can take immediate action to minimize the impact of security incidents, expediting responses and reducing the workload on human operators.  Robust logging entails maintaining a detailed record of all events that occur within the computer system. These logs provide a comprehensive record in case of security incidents, allowing for a thorough analysis of the event's nature, occurrence, and potential prevention strategies. It's akin to a detective reviewing a crime scene diary to understand what happened, how it happened, and how to prevent similar incidents from occurring in the future.    Figure : Proposed CyberShield System Architecture process  This is the process diagram of implementation for fortifying betting security through IDS & ELK integration involves several key stages. Here's a step-by-step breakdown followed from Data Ingestion Layer to Alerts notifications several tools will be used for this project and are mentioned below.  **The following tools are used in the CyberShield project:**  **AlienVault:**   * Purpose: Threat Intelligence * Brief Description: AlienVault is utilized for gathering and analysing threat intelligence, helping the system stay updated on current and emerging cybersecurity threats.   **Snort:**   * Purpose: IDS (Intrusion Detection System) Framework * Brief Description: Snort functions as an IDS framework, actively monitoring and analysing network traffic for signs of unauthorized access or potential security threats.   **ELK Stack:**   * Purpose: Monitoring & Logging * Brief Description: ELK Stack, consisting of Elasticsearch, Logstash, and Kibana, is employed for real-time monitoring, logging, and visualization of system data, enhancing the system's ability to detect and respond to security incidents.   **Ansible:**   * Purpose: Automation * Brief Description: Ansible is used for automating various tasks, such as configuration management and deployment, streamlining processes and reducing the need for manual intervention.   **KDDCUP 99 dataset:**   * Purpose: Anomaly Detection System * Brief Description: The KDDCUP 99 dataset is utilized for training and testing anomaly detection systems. It provides a set of data to help develop and assess the system's ability to identify abnormal patterns or activities in network traffic.   These tools and datasets collectively contribute to the overall functionality of the "CyberShield" project, covering aspects such as threat intelligence, intrusion detection, monitoring, logging, automation, and the development of anomaly detection systems.  **PROJECT TIMELINE**    Figure 4  Provide a little bit of explanation  System development details not very clear. | | | | |
| **WHAT EXISTING LAB EQUIPMENT DO YOU NEED ACCESS TO UNDERTAKE YOUR PROPOSED PROJECT:**  Computer systems, Virtual machines. | | | | |
| **PLEASE LIST ANY MINOR EQUIPMENT YOU MUST PURCHASE TO COMPLETE YOUR RESEARCH PROJECT: (eg, switches, resistors, raspberry pi, Arduino etc)**  NA | | | | |
| **PLEASE LIST ANY MAJOR EQUIPMENT YOU REQUIRE TO COMPLETE YOUR RESEARCH PROJECT ALONG WITH LINKS TO WHERE IT MAY BE PURCHASED (eg a Drone, mobile phone etc).**  NA | | | | |
| **HAVE YOU DISCUSSED THE FEESIBILITY OF YOUR PROJECT WITH A MEMBER OF THE TECHNICAL TEAM? IF SO, WHO?**  NO | | | | |
| ***(staff use only) Project Approved by Technical Team?*** | YES |  | NO |  |
| Please comment on the Feasibility of the project: | | | | |

**Section 3: Ethics Approval**

*This section of the form will help ascertain if you need to complete and undergo the universities research ethics approval process. Please answer all questions honestly.*

|  |  |  |
| --- | --- | --- |
| **Question** | **Yes** | **No** |
| **Does your Research involve any of the following?**  **Human participants / subjects, Human tissue, Documents** |  | **Badge Tick1 outline** |
| **Will the research require the collection of primary source material that might be considered offensive or illegal to access or hold on a computer? (e.g. studies related to state security, pornography, abuse, illegal behaviour, or terrorism).** |  | **Badge Tick1 outline** |
| **Does your research concern group which may be construed as terrorist or extremist?** |  | **Badge Tick1 outline** |
| **Will the research involve visual/vocal methods where participants may be identified?** |  | **Badge Tick1 outline** |
| **Will the research involve the use of genetic data (inherited/acquired genetic characteristics resulting from the analysis of a biological sample)?** |  | **Badge Tick1 outline** |
| **Will the study require the co-operation of a gatekeeper to give access to, or to help recruit, participants? (eg, headteacher or group leaders publicising your work)** |  | **Badge Tick1 outline** |
| **Will it be necessary for participants to take part in the study without their knowledge or consent at the time?** |  | **Badge Tick1 outline** |
| **Will the study involve recruitment of patients through the NHS?** |  | **Badge Tick1 outline** |
| **Will inducements be offered to participants? (eg the offer of being entered into a prize draw)** |  | **Badge Tick1 outline** |
| **Does the study involve participants who are particularly vulnerable or unable to give informed consent? (e.g. participants under 18. Adults with learning disabilities, the frail elderly, or anyone who may be easily coerced due to lack of capacity)** |  | **Badge Tick1 outline** |
| **Is there a possibility that the safety of the researcher may be in question?** |  | **Badge Tick1 outline** |
| **Will the study require participants to commit extensive time to the study?** |  | **Badge Tick1 outline** |
| **Are drugs, placebos, or any other substances to be administered to participants, or will the study involve invasive, intrusive, or potentially harmful procedures of any kind?** |  | **Badge Tick1 outline** |
| **If there are experimental and control groups, will being in one group disadvantage participants?** |  | **Badge Tick1 outline** |
| **Is an extensive degree of exercise or physical exertion involved?** |  | **Badge Tick1 outline** |
| **Will blood or tissue samples be obtained from participants?** |  | **Badge Tick1 outline** |
| **Could the study induce psychological stress or anxiety or cause harm or negative consequences beyond the risks encountered in normal life?** |  | **Badge Tick1 outline** |

*This part of Section 3 requires you to thoroughly* ***identify*** *and* ***mitigate*** *the ethical challenges of your research project. This is required to enable the computer Science ethics panel to properly consider if your proposed project requires you to submit a formal proposal to the university ethics panel.*

|  |
| --- |
| **With your answers to the previous questions in mind, please describe the main ethical challenges of your research project and how you propose to mitigate them. Your discussion may include material not covered in the above questions. Please be as through as possible:**  N/A |