SUMMER INTERNSHIP COURSE

2024-25

SYNOPSIS

1. Basic Information

Name of Student	Krishna Sharma
Roll Number	AP22110010128
Branch	CSE
Name of Internship station/ Company	Zeronsec
Location	Onsite
Date of Joining	30th May
Address of the Company	1st Floor, Plot-3, Navjivan Society - 2, Ajwa Road, Vadodara, Gujarat 390006
Project Title	Log Parser

Project Purpose (One sentence only - about 10/12 words, describing the anticipated change. What is the immediate outcome or direct benefit the project will achieve resulting from the activities and outputs). It should not contain project details which can be described elsewhere on the form.
The project aims to automate log parsing for improved efficiency and accuracy in cybersecurity operations.

What is the situation/status in the company before the project was given to you?	Indicators of success *(evidence: how we will know the purpose (above) has been achieved?*	What is the progress till date?
Before the project was assigned, the cybersecurity team at Zeronsec was manually parsing logs using regular expressions and Grok patterns. This process was time-consuming, error-prone, and often struggled to handle complex or evolving log formats. The manual approach hindered the team's efficiency in identifying security threats and responding to incidents.	The success of the project will be measured by the following indicators: ● **Improved efficiency:** A significant reduction in the time required for log parsing compared to manual methods. ● **Enhanced accuracy:** Increased accuracy in extracting relevant	The project has successfully progressed through the following stages: ● **Data collection and preparation:** A diverse dataset of log data was gathered and preprocessed for model training. ● **Model development and training:** A machine learning

	information from log data. ● **Scalability:** The ability of the model to handle increasing volumes of log data without compromising performance. ● **User satisfaction:** Positive feedback from the cybersecurity team regarding the usability and effectiveness of the log parser tool.	model, specifically an LSTM-based model, was developed and trained on the prepared dataset. ● **Model evaluation:** The model's performance was evaluated using appropriate metrics, demonstrating promising results. ● **Integration and testing:** The model was integrated into the existing cybersecurity infrastructure and tested in real-world scenarios.

Outputs: Please list here all of the outputs (specific deliverables) you expect the project activities to deliver.

Outputs *(The results of project activities. These should be sufficient to achieve the project purpose.)*	1. A trained and optimized machine learning model capable of parsing diverse log formats. 2. A user-friendly interface for interacting with the model and visualizing extracted information. 3. Comprehensive documentation outlining the project's methodology, results, and recommendations.
Main Activities *(List the tasks to be done to deliver the outputs.)*	1.1 **Data acquisition and preprocessing:** Collecting, cleaning, and preparing log data for model training. 1.2 **Model selection and development:** Choosing a suitable machine learning algorithm and designing the model architecture. 1.3 **Model training and tuning:** Training the model on the prepared dataset and optimizing its hyperparameters. 2.1 **Model evaluation and testing:** Assessing the model's performance and addressing any issues 2.2 **Integration and deployment:** Integrating the model into the existing cybersecurity infrastructure.

	2.3 **Documentation and reporting:** Creating comprehensive documentation and reports summarizing the project's findings.

Brief Background of the Project

(**500 words max**. Please include the rationale, the context and relevant/expected work to be conducted in this area)

The increasing volume and complexity of log data have made manual parsing methods unsustainable for modern cybersecurity operations. The need for an automated and efficient log parsing solution has become paramount. This project aimed to address this challenge by leveraging machine learning techniques to extract valuable information from log data. By automating the log parsing process, the project sought to improve the efficiency, accuracy, and scalability of log analysis, ultimately enhancing the organization's ability to detect and respond to security threats.

Kshorne.

Signature of Student:

(I confirm that all relevant project related information has been shared and I agree that I shall work towards the goals set in this form)