Executive Report: Deep Learning Model for Cyber Threat Detection

Objective: The project aimed to design and implement a deep learning model to detect cyber threats in a dataset simulating real-world logs. The goal was to enhance cybersecurity by detecting malware, phishing, and denial-of-service (DoS) attacks in real-time. The BETH dataset, with the target variable `sus_label` indicating whether an event is malicious (1) or benign (0), was used for training the model.

Data Overview: The BETH dataset contains event logs with features such as `processId`, `threadId`, `argsNum`, and `returnValue`. These features were used to classify events as suspicious or benign. The dataset is preprocessed, and the target label, `sus_label`, was used for model training.

Model Development:

- Neural Network Architecture: The model was built using a feed-forward neural network consisting of three layers. The input layer had 16 units, followed by a second hidden layer with 8 units, and the output layer had a single unit for binary classification.
- Activation Functions: ReLU activation was used for the hidden layers, and the output layer applied the Sigmoid function for binary classification (0 or 1).
- Loss Function & Optimizer: Binary cross-entropy loss (`BCELoss`) was used as the loss function, with the Adam optimizer employed to update model weights during training.

Training and Results:

- Training Process: The model was trained over 20 epochs with a batch size of 32. During training, the loss gradually decreased but exhibited a negative slope, indicating the model's limited improvement. The training loss remained almost constant throughout the epochs, suggesting that the model's learning rate or architecture may need adjustments for better optimization.
- Validation Accuracy: Upon evaluating the model on the validation set, the achieved accuracy was 54%, which did not meet the target of 60%. This indicates that the model's performance on the validation set was suboptimal and struggled to generalize well.

Training Loss Over Epochs: The training loss graph displayed a negative linear decline, indicating a slow and minimal reduction in the loss function over time. The graph resembled a straight line, which suggests that the model did not make significant progress in minimizing the loss. This points to potential issues with the current training strategy, possibly due to insufficient model complexity, learning rate, or data-related factors.

Conclusion: The deep learning model for cyber threat detection demonstrated a basic capability to classify events as suspicious or benign. However, the achieved accuracy of 54% was below the target of 60%, highlighting that the model needs further refinement.

Recommendations for improvement:

- Model Architecture: Exploring more complex architectures, such as deeper networks or convolutional layers, to better capture patterns in the data.
- Hyperparameter Tuning: Adjusting the learning rate, batch size, and other hyperparameters to improve training efficiency and model performance.
- Data Processing: Implementing additional feature engineering or exploring advanced data augmentation techniques to enhance the model's training data.

Despite the challenges, the project demonstrated the potential for deep learning in detecting and mitigating cyber threats. Further experimentation and fine-tuning will be necessary to improve the model's performance and its ability to generalize to new data.