

Beth-project

Introduction

The BETH dataset addresses a critical need in cybersecurity research: the availability of real-world, labeled data for anomaly detection. Unlike synthetic datasets, BETH captures genuine host activity and attacks, making it a valuable resource for developing robust machine learning models [1].

The scale, diversity, and structured heterogeneity of BETH dataset makes it an invaluable resource for advancing anomaly detection techniques and enhancing the robustness of machine learning models in the cybersecurity domain.

Size and Composition of the dataset: - BETH comprises over eight million data points collected from 23 hosts. - Each host records both benign activity (normal behavior) and, at most, one attack. - The dataset is diverse, reflecting various types of network traffic and system events.

Structured Heterogeneity of the dataset: - BETH's features are highly structured but heterogeneous. - This diversity mirrors the complexity of real-world cybersecurity data. - Features include network traffic statistics, system logs, and process-level information.

Scale and realism of the BETH dataset: - BETH is one of the largest publicly available cybersecurity datasets. - It captures contemporary host behavior, including modern attacks. - Researchers can use BETH to study the impact of scale on anomaly detection algorithms.

Behavioral Diversity: - The dataset covers a wide range of activities, from routine tasks to malicious actions. - Hosts exhibit different patterns, making BETH suitable for behavioral analysis.

Robustness Benchmarking: - BETH enables evaluating the robustness of machine learning models. - Researchers can assess how well their algorithms generalize to unseen attacks. - It serves as a benchmark for novel anomaly detection techniques.

Data analysis

The Beth dataset represents more than 8 millions events collected over 23 honeypots, only nearly 1 million of it will be used on this project. Data are already divided into training, validating and testing dataset (60% / 20% / 20%).

Features

Each of this dataset has those features: - timestamp: time in seconds since system boot (float)

- processId: id of the process spawning this log (integer)
□
- threadId: id of the thread (integer) there is a total of 545 thread ids.
□
- parentProcessId: parent process id (integer)
□
- userId: login integer id (integer)
□
- mountNamespace: Set mounting restrictions this process log (integer)
□
- processName: command executed (string)
□
- hostName: host server (string)
□
- eventId: id of the event generating this log (integer)
- eventName: name of the event (string)
□
□
- stackAddresses: memory values relevant to the process (list of integer)
□
□
- returnValue: value returned from this event log (integer)
□

- argsNum: number of arguments (integer)
- args: arguments passed to this process (list of dictionaries)
- sus: This is an integer label where 0 indicates non-suspicious activity and 1 indicates suspicious activity. We want to develop a model that can accurately classify and identify suspicious activities based on this labeling system.
- evil: This is an integer label where 0 indicates non-malicious activity and 1 indicates malicious activity. This label was not chosen for classification because the training and validation datasets do not contain any malicious classes.

Correlation matrix

- Strong Positive Correlations:
 - processId and threadId: They have a correlation of 1.00, indicating they are perfectly correlated. This makes sense as threadId is often associated with processId.
 - parentProcessId and userId: With a correlation of 0.55, it suggests a moderate positive relationship. Likely because parent processes are tied to user accounts.
 - sus and userId: This has a high correlation of 0.77, suggesting that suspicious activity (sus) is strongly linked with specific user IDs.
 - evil and userId: This shows a very strong positive correlation of 0.90, indicating that 'evil' actions are highly associated with certain user IDs.
 - sus and evil: With a correlation of 0.73, it indicates that actions labeled as suspicious are strongly correlated with those labeled as evil.
- Moderate Positive Correlations:
 - timestamp and userId: A correlation of 0.68 suggests that timestamps are moderately positively related to user IDs, possibly indicating certain users are more active at certain times.
 - parentProcessId and timestamp: With 0.67, it shows a moderate positive relationship.
 - sus and parentProcessId: This correlation is 0.69, indicating that suspicious activities are moderately correlated with parent processes.
 - evil and parentProcessId: Correlation of 0.72, indicating a strong association between evil actions and parent processes.
- Negative Correlations:
 - mountNamespace with processId, threadId, parentProcessId: These are moderately negatively correlated (around -0.26), indicating that certain process/thread IDs and their parent processes are less likely to have specific mountNamespace values.
 - eventId with timestamp, userId, sus, evil: Negative correlations, especially -0.36 with timestamp and -0.39 with userId, suggest that certain events are less likely to happen at certain times or for certain users.
 - eventId with sus and evil: Both are negatively correlated (around -0.35 to -0.38), indicating that particular events are less associated with suspicious and evil activities.
- Low/No Correlation:
 - argsNum and other variables: Mostly low correlations, suggesting that the number of arguments has little to no linear relationship with the other features.
 - returnValue and other variables: Low correlations overall, indicating the return value of processes is largely independent of other features.
- Interpreting Specific Pairs:
 - timestamp and sus/evil: These have correlations of 0.62 and 0.70, respectively. This suggests that the timing of events is significantly associated with suspicious and evil activities.
 - mountNamespace: Shows mostly weak correlations with other features, suggesting that mountNamespace values are relatively independent of other variables.

Event Frequency

The following chart shows the entire frequency of suspicious and not suspicious event:

- Event Frequency: The y-axis represents the frequency of events, ranging from 0 to over 7000.
- Timestamp: The x-axis represents the timestamps when the events occurred.
- Not Suspicious Events: Represented by blue lines. The frequency of these events is higher and more variable, with several spikes reaching high values, particularly towards the left side of the chart.

- Suspicious Events: Represented by red lines. These events are less frequent and usually have lower values compared to the "Not Suspicious" events. There are a few noticeable spikes in the red lines, indicating higher frequencies of suspicious events at certain timestamps.

Overall, the chart shows that "Not Suspicious" events occur more frequently and with higher peaks compared to "Suspicious" events, which occur less often and with lower peaks.

Data preparation

Numerical data transformation

As advised by the authors of the beth dataset's paper, we applied these transformation: - ProcessId and ParentprocessId: 0 if it is [0,1,2] otherwise 1 - UserId: 0 if id is less than 1000 otherwise 1 - MountNameSpace: 0 if it is equal to 4026531840 otherwise 1 - ReturnValue: 0 if it is 0, 1 if it is positif and 2 if it is negatif

StackAddresses

Stackaddresses sf a list of numerics with a maximum of 20 elements. We created 20 new columns named "stack_1", "stack_2", etc. in each dataset, and assigns each element from the list to its respective new column.

Args

Args column contains a list of maximum 5 dictionaries, each disctionary contains three elements ({'name': 'dev', 'type': 'dev_t', 'value': 211812353}). We created 15 new columns in each datset, and assigns each element from the dictionaries to its respective new column.

Ordinal encoding

Ordinal encoding is a technique for converting categorical data, where variables have distinct labels or categories, into numerical form suitable for machine learning algorithms. It assigns a unique integer value to each category based on its order or rank. As our approach is for an unsupervised model, we used ordinal encoder to handle new classes not present in the training dataset. Ordinal encoder will assign -1 value to unknown classes (labels not present in the training dataset)

□

Scaling

Numerical features are scaled to similar range as they have different scales. Since we used ordinal encoding for categorical features, scaling is not necessary. Ordinal encoding preserves the order of the categories, but the assigned values don't necessarily reflect their magnitude.

Smote

Dealing with unbalanced data can be tricky, most of the machine learning model will give good results for big classes and poor performance on the minority althought, as it is our case, minority class is more important. To balance that, we tried to use Smote library combined as it is advised with random undersampling for the majority class. SMOTE (Synthetic Minority Oversampling TEchnique) works by interpolating new instances along line segments joining existing minority class instances.

□

Shapelet discovery method

Shapelet discovery is a technique used in time series analysis to identify discriminative subpatterns, known as shapelets, within a set of time series data. Shapelets are subsequences that capture characteristic patterns or behaviors in the data. The process of shapelet discovery involves searching through the time series data to find subsequences that are representative of different classes or categories like in our case for **suspicious activities and not suspicious activities**. The similarity or distance between each subsequence and the rest of the data is computed to determine its discriminative power. The shapelets with the highest discriminative power are selected as representative patterns.

So the shapelet discovery can use the matrix profile as a tool for efficiently computing the distances or similarities between subsequences. By utilizing the matrix profile, shapelet discovery algorithms can reduce the computational complexity and speed up the process of identifying shapelets.

The following chart describe how the comparison with the suspicious activity differs to the comparison with the not suspicious activity.

□

Models

Dense neural network

Model 1:

- **Description** This model is composed with five hidden dense layers each with 512 units and ReLU activation, interspersed with dropout layers for regularization, and an output layer with a single unit and sigmoid activation for binary classification. Each dense layer uses the 'lecun_normal' initializer for the kernel and a RandomNormal initializer for the bias.
- **Training**
- **Prediction** **Model 1** seems to predict only the "unsuspicious" class and fails to detect any "suspicious" activities, resulting in poor performance for identifying suspicious activities.

Model 2:

- **Description** This model is a neural network that handle differently categorical and numerical features. It incorporates embeddings for the categorical inputs, which are then reshaped and concatenated with numerical inputs, followed by multiple dense layers with ReLU activations and dropout for regularization. The final output layer uses a sigmoid activation function to produce a binary classification result.
- **Training**
- **Prediction** **Model 2** shows a strong ability to correctly identify suspicious activities while maintaining a low false positive rate. However, there is still room for improvement in reducing the number of false negatives, which could enhance the model's sensitivity to suspicious activities. We have also very low false positive rate for unsuspicious class.

Model 3:

- **Description** This model is similar to **Model 1**, this model is trained on data after applying Smote data augmentation technic.
- **Training**
- **Prediction** After applying SMOTE, the model exclusively predicts the "unsuspicious" class and fails to identify any "suspicious" activities. This indicates that the model is not effectively learning from the augmented data, even with the improved balance in our dataset.

Model 4: Dense model with the Shapelet Discovery method

- **Description**
- **Training**
- **Confusion Matrix**

Convolutional neural network

Model 1

- **Description** This model is a Convolutional Neural Network (CNN) with an input shape of (47, 1).\ It comprises four Conv1D layers with decreasing filter sizes (256, 128, 64, and 32) and ReLU activations, each followed by a dropout layer to prevent overfitting. We applied a Lecun normal initializer for the kernels and a custom random normal initializer for the biases.\ The output layer is a dense layer with a sigmoid activation function for binary classification.
- **Training**
- **Prediction**

Model 2

- **Description** \ This model handles categorical and numerical inputs separately, using embeddings and dense layers for preprocessing. \ It creates embeddings for two categorical features (args and stackaddresses), followed by linear transformations, and processes numerical features through a dense layer and reshaping. \ The processed embeddings and numerical features are concatenated and passed through two Conv1D layers with ReLU activations for feature extraction. \ Finally, the output layer is a dense layer with a sigmoid activation function for binary classification.
- **Training**
- **Prediction**

□

LSTM neural network

Model 1 (no embeddings)

- **Description** \ This model is a Sequential Long Short-Term Memory (LSTM) network designed for sequence data with an input shape of (47, 1). It consists of four LSTM layers, each with 32 units and ReLU activations, using Lecun normal initialization for the kernels and a custom random normal initializer for the biases, followed by dropout layers to prevent overfitting. The output from the LSTM layers is flattened and passed through a dense layer with 128 units and a final dense layer with a sigmoid activation function for binary classification.
- **Training**
- **Prediction**

□

The confusion matrix indicates that the model is highly effective in identifying suspicious activities, correctly classifying 159,875 out of 171,459 suspicious instances while maintaining a perfect true negative rate with 17,508 correct unsuspicious classifications. However, it still misses 11,584 suspicious instances

Model 2

- **Description**
- **Training**
- **Prediction**

□

Model 3 (shapelet discovery)

Transformer

- **Description** \ This model integrates categorical and numerical inputs using a transformer-based architecture. \ Categorical inputs are embedded and transformed via dense layers, while numerical inputs are processed through a dense layer and reshaped. \ The combined embeddings and numerical features are enhanced with positional encoding and passed through several transformer encoder blocks, followed by convolutional layers, global average pooling, and fully connected layers, ultimately producing a single sigmoid-activated output.
 - Positional encoding adds information about the position of each element in the sequence by creating a positional encoding matrix, which applies sinusoidal functions to encode positional information. \ This matrix is added to the input embeddings, allowing the model to incorporate the order of the sequence elements, which is crucial for the transformer to understand the sequential nature of the data.
 - The `transformer_encoder_block` applies multi-head self-attention to the inputs, enabling the model to focus on different parts of the sequence simultaneously. \ This is followed by a dropout layer for regularization and layer normalization to stabilize and speed up training. \ Finally, a feed-forward neural network with a dense layer, dropout, and another layer normalization is used to further process the attention output, enhancing the model's capacity to capture complex patterns in the data.
 - This model uses Adam optimizer with a **WarmUpCosineDecay** learning rate. \ During the warmup phase, the learning rate increases linearly, and once the warmup steps are completed, it follows a cosine decay pattern to gradually reduce the

learning rate.

- **Training:**

- **Prediction:**

□

- Strengths:
 - The model has high accuracy (94.6%).
 - Perfect precision and specificity, meaning there are no false positives.
 - High recall (94.1%) and a strong F1 score (97%).
- Weaknesses:
 - The model still misses some positive instances (10,208 false negatives), which may be critical depending on the context of the application.
 - The imbalance in predictions (zero false positives but some false negatives) could indicate a bias towards negative predictions.

Results

Model	Accuracy	Precision avg	Recall avg	ROC score	$\frac{AUC}{N}$	$\frac{AUC}{K}$	$\frac{AUC}{L}$	$\frac{AUC}{M}$	Dense model	0.09	0.05	0.50	0.50
Dense model + embeddings	0.91	0.75	0.95	0.95	Dense Model-shapelet Discovery	0.85	0.42	0.50	0.50	CNN model	0.11	0.53	0.51
CNN model + embeddings	0.95	0.82	0.97	0.97	RNN model	0.09	0.05	0.50	0.50	RNN model + embeddings.	0.95	0.82	0.97
LSTM model-shapelet Discovery	0.85	0.42	0.50	0.50	Transformer	0.95	0.82	0.97	0.97				

Discussion

- Most of the models present good validation accuracy and seem to converge rapidly, which could be due to the similarity between the training and validation datasets compared to the testing dataset or because the task is relatively simple.
- Most of the models achieve a high recall score for the unsuspecting class (100% for LSTM model1), indicating that unsuspecting instances are well predicted. However, the precision score for the same class does not exceed 63%, which may be due to the larger number of unsuspecting instances in the training dataset.

Application of the Matrix Profile

With the concept of matrix profile, we tried to find conserved behaviours in the data. In fact, a comparison between sequences can be done by looking at the euclidean distance between all the points in two subsequences and represent the distances in a matrix profile.



□

References

1. BETH Dataset: Real Cybersecurity Data for Anomaly Detection Research Kate Highnam, Kai Arulkumaran, Zachary Hanif, Nicholas R. Jennings <https://www.gatsby.ucl.ac.uk/~balaji/udl2021/accepted-papers/UDL2021-paper-033.pdf>
2. Smote: Synthetic Minority Over-sampling Technique Authors: Nitesh V. Chawla, Kevin W. Bowyer, Lawrence O. Hall, W. Philip Kegelmeyer <https://arxiv.org/pdf/1106.1813>
3. Time Series Shapelets: A New Primitive for Data Mining. Lexiang Ye, Eamonn Keogh (<https://www.cs.ucr.edu/~eamonn/shaplet.pdf>)