ỨNG DỤNG PHÁT HIỆN HÀNH VI BẤT THƯỜNG CỦA NGƯỜI DÙNG TRONG MẠNG DOANH NGHIỆP

Huỳnh Trần Trọng Nghĩa - 250101047

Tóm tắt

- Lớp: CS2205.CH201
- Link Github: https://github.com/nghiahuynh8620/CS2205.CH201
- Link YouTube: https://youtu.be/8iREqJGTmyA
- Họ và Tên: Huỳnh Trần Trọng Nghĩa
- MSHV: 250101047

Giới thiệu

- Trong mạng doanh nghiệp, các chuỗi hành động “hợp lệ” nhưng bất thường theo ngữ cảnh có thể là dấu hiệu Account Takeover hoặc Insider Threat.
- Rule - signature dễ triển khai nhưng khó bao phủ các hành vi tinh vi và biến thể mới.
- UEBA baseline học hành vi người dùng để phát hiện sự bất thường và ưu tiên cảnh báo.
- Mục tiêu: hỗ trợ SOC Blue Team phát hiện sớm và rút ngắn thời gian điều tra nhờ cảnh báo có ngữ cảnh & giải thích.

Mục tiêu

- Xây dựng bộ dữ liệu & pipeline tiền xử lý log: chuẩn hoá, làm sạch, ghép nguồn, gom theo timestamp; thiết kế bộ đặc trưng UEBA.
- Thiết kế – huấn luyện – so sánh mô hình phát hiện bất thường: Supervised Learning, Deep Learning, tối ưu giảm cảnh báo sai.
- Xây dựng demo tra cứu - cảnh báo và đánh giá định lượng và cung cấp tài liệu tái lập (reproduce).

Nội dung và Phương pháp

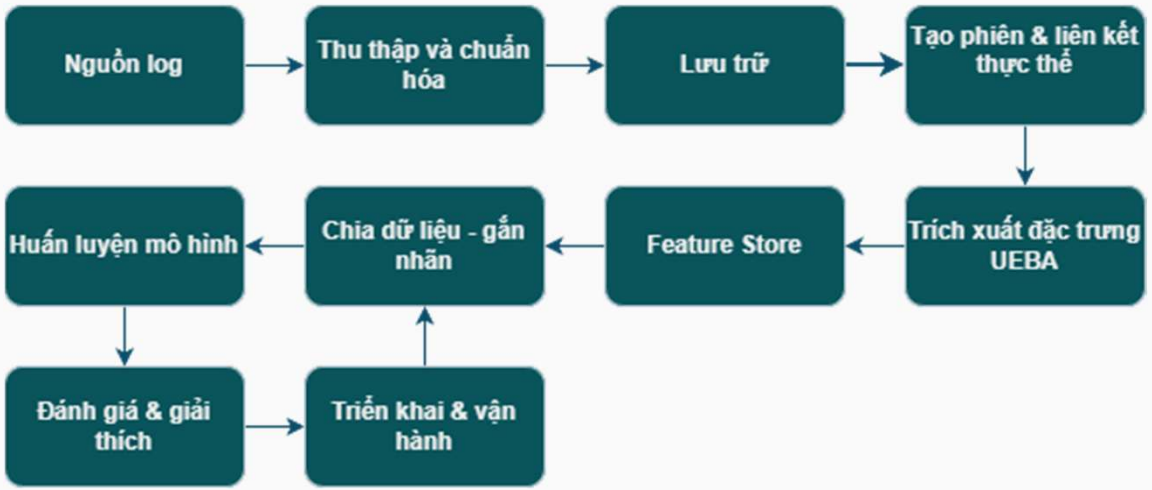
- Dữ liệu và tiền xử lý:
  - Nguồn dữ liệu: AD - SSO (login), file access, proxy - network, endpoint- process, email, USB audit
  - Chuẩn hoá schema: user - host - action - resource - timestamp
  - Làm sạch: loại trùng, xử lý thiếu, đồng bộ timezone.
  - Gom theo timestamp (5 phút/1 giờ/1 ngày) để tạo bảng sự kiện & bảng đặc trưng.

Nội dung và Phương pháp

- Mô hình & Đánh giá
  - Baseline Supervised Learning: Random Forest , XGBoost có xử lý mất cân bằng (sampling/weight).
  - Deep Learning: Autoencoder, Transformer tự giám sát cho chuỗi sự kiện hoặc Embedding log.
  - Đánh giá time-based split; metrics: Precision/Recall/F1, PR-AUC/ROC-AUC, FPR; + thời gian suy luận
  - Giải thích: feature importance/SHAP (tree-based) hoặc phân rã reconstruction error (AE).

Nội dung và Phương pháp

- Pipeline tổng thể:



Kết quả dự kiến & Demo

- Bộ dữ liệu chuẩn hoá (hoặc dataset công khai đã chuẩn bị) + mã nguồn ETL/feature engineering.
- Tối thiểu 3–4 baseline + 2 mô hình DL; bảng so sánh định lượng & phân tích lỗi.
- Demo tra cứu theo user/timestamp: điểm bất thường, ngữ cảnh sự kiện, giải thích và xuất danh sách cảnh báo.
- Báo cáo + slide + hướng dẫn chạy/tái lập

Tài liệu tham khảo

[1]. David Alvarez Muniz, Luis Perez Miguel, et al.: Design and Generation of a Dataset for Training Insider Threat Prevention and Detection Models: The SPEDIA Dataset. Computers & Security 2025: 104743.
[2]. W. Feng, et al.: Multi-Granularity User Anomalous Behavior Detection. Applied Sciences 2024, 15(1):128.
[3]. Crispin Almodovar, Fariza Sabrina, Sarvnaz Karimi, et al.: LogFiT: Log Anomaly Detection Using Fine-Tuned Language Models. IEEE Transactions on Network and Service Management 2024, 21(2):1715-1723.

Tài liệu tham khảo

[4]. S. Song, et al.: Confront Insider Threat: Precise Anomaly Detection in Behavior Logs Based on LLM Fine-Tuning. COLING 2025.
[5]. (Scientific Reports): System log anomaly detection based on contrastive learning and retrieval augmented. Scientific Reports 2025.
[6]. Max Landauer, Florian Skopik, et al.: Cloud-based User Entity Behavior Analytics Log Data Set (CLUE-LDS). Zenodo 2022.