KHUNG KIỂM SOÁT AN NINH LOG VÀ GIẢM THIỂU SAI CẤU HÌNH CLOUD DỰA TRÊN AGENTIC AI TRONG MÔI TRƯỜNG MULTI-CLOUD

Trần Thanh Trực - 250202023

Tóm tắt

- Lớp: CS2205.CH201
- Link Github của nhóm: https://github.com/tructt41/CS2205.CH201
- Link YouTube video: https://youtu.be/rw2PtjydjYM

Trần Thanh Trực
250202023

Giới thiệu

- **Bối cảnh (The Context):**
  - Sự dịch chuyển mạnh mẽ sang mô hình Multi-Cloud (AWS, OpenStack) làm gia tăng độ phức tạp trong quản lý cấu hình.
  - Theo các nghiên cứu mới nhất (như CAShift 2025), các cuộc tấn công dựa trên sai cấu hình (Misconfiguration) ngày càng tinh vi và khó phát hiện do sự thay đổi liên tục của dữ liệu log (Normality Shift).

Giới thiệu

- **Vấn đề nghiên cứu (Problem Statement):**
  - Sự bùng nổ dữ liệu: Lượng log khổng lồ từ đa nền tảng khiến việc phân tích thủ công trở nên bất khả thi.
  - Hạn chế của SIEM truyền thống: Các hệ thống dựa trên luật (rule-based) thường xuyên bỏ lỡ các biến thể tấn công mới hoặc tạo ra quá nhiều báo động giả.
  - Khoảng trống kỹ thuật: Thiếu một cơ chế tích hợp có khả năng vừa phát hiện bất thường bằng Deep Learning, vừa giải thích và gợi ý khắc phục bằng AI (Agentic AI).
- **Giải pháp đề xuất:**
  - Ứng dụng khung nghiên cứu tích hợp: Sử dụng mô hình DeepLog để phát hiện và Agentic AI để đóng vai trò "trợ lý phân tích" giúp tự động hóa quy trình phản ứng an ninh.

Mục tiêu

- **Mục tiêu chính:** Xây dựng khung kiểm soát an ninh (Framework) tự động phát hiện và gợi ý khắc phục sai cấu hình trên môi trường Multi-Cloud (AWS & OpenStack).
- **Mục tiêu cụ thể:**
  - Tích hợp các bộ dữ liệu chuẩn (CAShift, AWSCTD, OpenStack) để huấn luyện mô hình phát hiện tấn công và bất thường cấu hình.
  - Ứng dụng Agentic AI (LLM + RAG) để phân tích ngữ nghĩa log, giảm tỷ lệ báo động giả (False Positive) từ các hệ thống truyền thống.
  - Đề xuất cơ chế phản ứng tự động dựa trên tri thức từ các bài báo khoa học (như DeepLog) để hỗ trợ chuyên gia SOC ra quyết định.

Nội dung nghiên cứu

- **Phân tích và Khai thác dữ liệu Log đa nguồn:**
  - AWS Security: Khai thác dữ liệu từ AWSCTD và CAShift để nhận diện các hành vi leo thang đặc quyền và tấn công khai thác cấu hình sai (Misconfiguration attacks).
  - OpenStack Security: Sử dụng dữ liệu từ Loghub và nghiên cứu của Kalaki et al. (2023) để phân tích các log hệ thống hạ tầng đám mây dùng riêng.
  - Tiền xử lý: Áp dụng phương pháp phân tách log (Log Parsing) dựa trên các kỹ thuật trong bài báo Loghub để chuẩn hóa dữ liệu log thô thành dữ liệu cấu trúc.

Nội dung nghiên cứu

- **Xây dựng mô hình phát hiện bất thường:**
  - Deep Learning Core: Triển khai kiến trúc DeepLog (LSTM/Transformer) để học chuỗi sự kiện log bình thường và phát hiện các sai lệch (Anomaly Detection).
  - Normality Shift: Giải quyết bài toán thay đổi hành vi log theo thời gian dựa trên các kết quả thực nghiệm mới nhất từ bài báo CAShift (FSE 2025).
  - Tối ưu hóa: Sử dụng thuật toán Robust PCA cải tiến (theo Kalaki et al.) để tăng cường khả năng phát hiện trong môi trường nhiễu.

Phương pháp nghiên cứu

- **Quy trình thực hiện (Pipeline):**
  - Data Ingestion: Thu thập log từ môi trường thử nghiệm (Testbed) và Dataset.
  - Detection Engine: Kết hợp Ensemble Learning (DeepLog + Robust PCA).
  - Reasoning Layer (Agentic AI): Sử dụng RAG (Retrieval-Augmented Generation) truy vấn cơ sở dữ liệu tri thức từ các paper để giải thích lỗi.
  - Evaluation: Đánh giá bằng bộ chỉ số chuyên biệt cho Cloud Security (Precision, Recall, F1-score).

Hệ thống Agentic AI trong Security

- **Vai trò của Agent:** Đóng vai trò là một "Chuyên gia SOC ảo".
- **Chức năng:**
  - Tự động tóm tắt các cảnh báo phức tạp từ Deep Learning thành ngôn ngữ tự nhiên.
  - Truy xuất (Retrieve) các giải pháp khắc phục từ thư viện tài liệu bảo mật.
  - Tương tác với quản trị viên để xác nhận việc rollback cấu hình sai.

Kết quả dự kiến

- **Về mặt công nghệ:** Một hệ thống (Prototype) có khả năng giám sát log thời gian thực trên cả AWS và OpenStack.
- **Về mặt hiệu năng:**
  - Đạt độ chính xác (F1-score) > 90% trên bộ dữ liệu CAShift.
  - Giảm 50% thời gian phân tích thủ công của nhân viên SOC nhờ trợ lý Agentic AI.
- **Về mặt học thuật:** Hoàn thiện báo cáo nghiên cứu và có tiềm năng công bố trên các hội thảo về An toàn thông tin.

Tài liệu tham khảo

- J. Yu, X. Xie, et al. CAShift: Benchmarking Log-Based Cloud Attack Detection under Normality Shift. FSE 2025.
- P. Kalaki, et al. Anomaly detection on OpenStack logs based on an improved robust principal component analysis model. Softw. Pract. Exp. 2023.
- S. He, et al. Loghub: A Large Collection of System Log Datasets towards Automated Log Analytics. CoRR 2020.
- D. Ceponis, et al. Towards a Robust Method of Dataset Generation for AWSCTD. BJMC 2018.
- M. Du, et al. DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning. ACM CCS 2017.