THÔNG TIN CHUNG CỦA NHÓM

- Link YouTube video của báo cáo (tối đa 5 phút): *https://youtu.be/rw2PtjydjYM*
- Link slides (dạng .pdf đặt trên Github của nhóm): *https://github.com/tructt41/CS2205.CH201/blob/main/Slide%20-%20AN%20AGENTIC%20AI-DRIVEN%20FRAMEWORK%20FOR%20CLOUD%20LOG%20SECURITY%20AND%20MISCONFIGURATION%20MITIGATION%20IN%20MULTI-CLOUD%20ENVIRONMENTS.pdf*
- *Mỗi thành viên của nhóm điền thông tin vào một dòng theo mẫu bên dưới*
- *Sau đó điền vào Đề cương nghiên cứu (tối đa 5 trang), rồi chọn Turn in*
- *Lớp Cao học, mỗi nhóm một thành viên*

- Họ và Tên: Trần Thanh Trực
- MSSV: 250202023

- Lớp: CS2205.CH201
- Tự đánh giá (điểm tổng kết môn): 7.5/10
- Số buổi vắng: 2
- Link Github: https://github.com/tructt41/CS2205.CH201

ĐỀ CƯƠNG NGHIÊN CỨU

TÊN ĐỀ TÀI (IN HOA)

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

TÊN ĐỀ TÀI TIẾNG ANH (IN HOA)

AN AGENTIC AI-DRIVEN FRAMEWORK FOR CLOUD LOG SECURITY AND MISCONFIGURATION MITIGATION IN MULTI-CLOUD ENVIRONMENTS

TÓM TẮT *(Tối đa 400 từ)*

Nghiên cứu này tập trung giải quyết thách thức về an ninh bảo mật trong môi trường Multi-Cloud (AWS và OpenStack), nơi 65–70% sự cố xuất phát từ sai cấu hình (misconfiguration). Trong khi cơ sở hạ tầng mã nguồn (IaC) giúp triển khai nhanh nhưng cũng dễ tạo ra các lỗ hổng bảo mật nếu thiếu cơ chế kiểm soát. Đề tài đề xuất khung nghiên cứu Cashify Cloud Log Security Framework, tích hợp Agentic AI đóng vai trò trợ lý phân tích SOC (SOC Analyst Assistant). Hệ thống sử dụng kỹ thuật RAG (Retrieval-Augmented Generation) kết hợp với các mô hình Deep Learning (Transformer, LSTM) để phát hiện bất thường và đưa ra gợi ý khắc phục dựa trên các bộ tiêu chuẩn quốc tế như OWASP và CSA. Dữ liệu thực nghiệm được kế thừa từ bộ dataset chuẩn CAshify Cloud Log Security (ACM 2024) kết hợp với log thực tế từ môi trường testbed. Kết quả mong đợi là một hệ thống có khả năng giảm tỷ lệ báo động giả, tối ưu hóa thời gian phản ứng (Time-to-detect) và cung cấp báo cáo hỗ trợ ra quyết định cho con người (Human-in-the-loop).

GIỚI THIỆU *(Tối đa 1 trang A4)*

Sự bùng nổ của điện toán đám mây đã biến AWS và OpenStack thành hạ tầng lõi của nhiều doanh nghiệp. Tuy nhiên, sự phức tạp trong quản lý đa nền tảng dẫn đến các rủi ro lớn về sai cấu hình IAM, S3 bucket hay các thiết lập mạng (SG/NACL). Các hệ thống SIEM truyền thống dựa trên luật (rule-based) hiện nay bộc lộ hạn chế trong việc mở rộng và xử lý lượng log khổng lồ.

Khoảng trống nghiên cứu hiện nay nằm ở việc thiếu một khung làm việc tích hợp giữa triển khai IaC an toàn và khả năng phân tích log thông minh bằng AI. Sự xuất hiện của Agentic AI mở ra cơ hội mới, cho phép LLM kết hợp với RAG để không chỉ phát hiện mà còn giải thích lý do bất thường (reasoning). Nghiên cứu này không hướng tới sự tự động hóa hoàn toàn để tránh rủi ro thực thi sai, mà tập trung vào mô hình "Trợ lý ảo" hỗ trợ chuyên gia SOC, đảm bảo tính an toàn và minh bạch qua cơ chế human-in-the-loop.

MỤC TIÊU *(Viết trong vòng 3 mục tiêu)*

- Thiết kế và triển khai khung nghiên cứu Cashify Cloud Log Security tích hợp triển khai IaC (OpenStack) và mô phỏng sai cấu hình thực tế trên AWS.
- Xây dựng mô hình phát hiện bất thường dựa trên Ensemble Deep Learning và Agentic AI pipeline để phân tích, giải thích và gợi ý khắc phục lỗ hổng.
- Đánh giá hiệu năng hệ thống thông qua việc so sánh đối đầu giữa phương pháp AI-assisted và SIEM truyền thống trên bộ dữ liệu chuẩn.

NỘI DUNG VÀ PHƯƠNG PHÁP

- Xây dựng lớp hạ tầng (IaC & Misconfig Layer): Sử dụng Ansible và Cola để triển khai OpenStack có kiểm soát an ninh. Thiết lập các kịch bản sai cấu hình thực tế trên AWS CloudTrail và VPC Flow Logs.
- Xử lý dữ liệu (ML/DL Layer): Sử dụng dataset CAshify (ACM 2024) kết hợp log tổng hợp từ testbed. Áp dụng các kỹ thuật tiền xử lý JSON, trích xuất đặc trưng và huấn luyện các mô hình như Autoencoder, LSTM và Transformer-based (LogBERT).
- Phát triển Agentic AI Layer: Xây dựng pipeline Log Ingestion → Embedding → RAG20202020. AI sẽ truy vấn Knowledge Base (OWASP, CSA) để gán nhãn mức độ nghiêm trọng và đưa ra báo cáo khuyến nghị (Recommendation Report) dưới dạng ngôn ngữ tự nhiên
- Đánh giá: Sử dụng các chỉ số Precision, Recall, F1-score và ROC-AUC để đo lường độ chính xác, đồng thời khảo sát tính hữu dụng (usability) với chuyên gia

SOC.

KẾT QUẢ MONG ĐỢI

- Một Framework bảo mật tích hợp hoàn chỉnh có khả năng hoạt động trên môi trường Multi-cloud.
- Mô hình AI SOC Assistant giúp giảm thời gian phân tích log và cung cấp các hành động khắc phục chính xác như rollback cấu hình IaC hoặc chỉnh sửa policy IAM.
- Bộ số liệu benchmark chứng minh sự vượt trội của AI-assisted SOC so với rule-based truyền thống.
- Nền tảng để phát triển thành AI Co-Pilot tích hợp vào các hệ thống SIEM/SOAR trong tương lai.

TÀI LIỆU THAM KHẢO *(Định dạng DBLP)*

[1]. Jiacheng Yu, Xiaofei Xie, Qiang Hu, Ben Zhang, et al.: CAShift: Benchmarking Log-Based Cloud Attack Detection under Normality Shift. ACM International Conference on the Foundations of Software Engineering (FSE) 2025.

[2]. Parisa Kalaki, Alireza Shameli-Sendi, Behrouz Khosravi: Anomaly detection on OpenStack logs based on an improved robust principal component analysis model and its projection onto column space. Software: Practice and Experience 53(3): 665-681 (2023).

[3]. Shilin He, Jieming Zhu, Pinjia He, Michael R. Lyu: Loghub: A Large Collection of System Log Datasets towards Automated Log Analytics. arXiv preprint arXiv:2008.06448 (2020).

[4]. Dainius Ceponis, Nikolaj Goranin: Towards a Robust Method of Dataset Generation of Malicious Activity for Anomaly-Based HIDS Training and Presentation of AWSCTD Dataset. Baltic Journal of Modern Computing 6(3): 217-234 (2018).

[5]. Min Du, Feifei Li, Guineng Zheng, Vivek Srikumar: DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning. ACM SIGSAC

Conference on Computer and Communications Security (CCS) 2017: 1285-1298.