PHÂN TÍCH HÀNH VI NGƯỜI DÙNG VÀ THỰC THỂ VỚI MẠNG NƠ-RON TỰ TỔ CHỨC TĂNG CƯỜNG

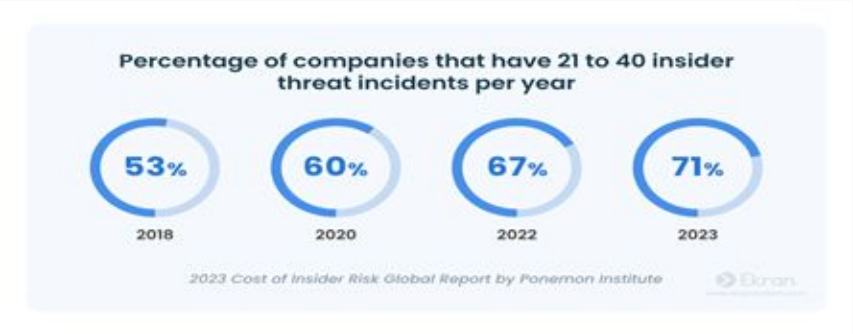
Nguyễn Tấn Kiệt - 230202009

Tóm tắt

- Lớp: CS2205.CH181
- Link Github:
- Link YouTube video:
- Họ và Tên: Nguyễn Tấn Kiệt

Giới thiệu

- ●Từ năm 2019 đến năm 2024, số lượng tổ chức báo cáo các cuộc tấn công nội bộ đã tăng từ 66% lên tới 76%
- ●70% số người được hỏi bày tỏ lo ngại về rủi ro nội bộ trong môi trường làm việc kết hợp giữa làm việc tại nhà và trên văn phòng
- ●Chỉ 16% tổ chức cho rằng mình cực kỳ hiệu quả trong việc xử lý các mối đe dọa nội bộ, cải thiện so với 11% vào năm 2019

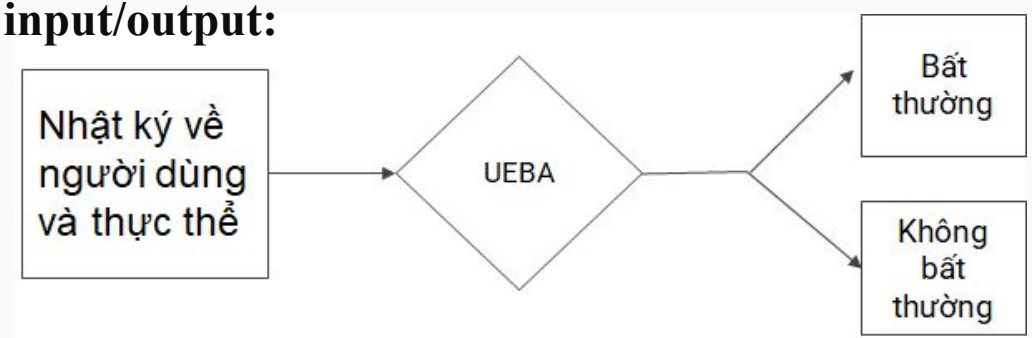


Giới thiệu

Phân tích hành vi người dùng và thực thể (UEBA) là một phương pháp giám sát an ninh mạng sử dụng **kỹ thuật học máy** để phân tích hành vi của người dùng và thực thể trong mạng nhằm xác định các hành vi bất thường tiềm ẩn mối đe dọa an ninh mạng.

- Tập trung vào hành vi của người dùng, thực thể
- Các mối quan hệ tương tác của người dùng với người dùng, người dùng với thực thể

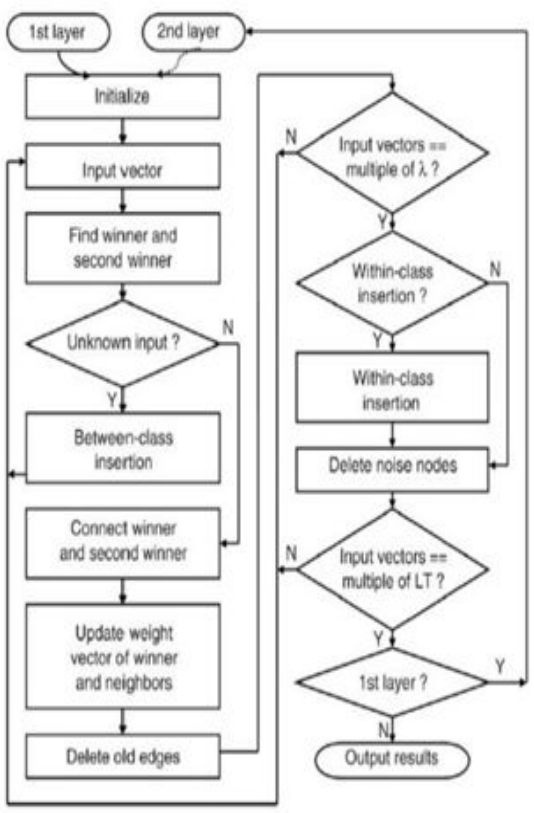
input/output:



Giới thiệu

Mạng nơ-ron tự tổ chức tăng cường (SOINN) là một mô hình mạng nơ-ron tự tổ chức có khả năng học và phân loại dữ liệu không giám sát.

- Tự tổ chức
- Học tập liên tục
- Khả năng giải thích cao
- Hiệu quả về tính toán

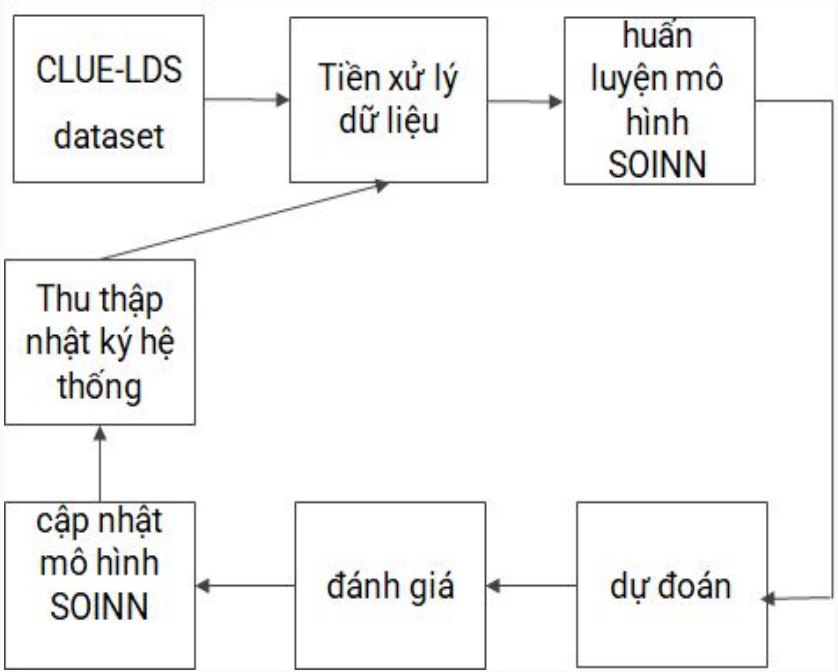


Mục tiêu

- Nghiên cứu và so sánh các phương pháp cho bài toán phân tích hành vi người dùng và thực thể dựa trên mô hình mạng nơ-ron tự tổ chức tăng cường
- Huấn luyện, dự đoán mô hình có khả năng cảnh báo bảo mật với độ chính xác cao theo thời gian thực
- Tích hợp vào hệ thống quản lý sự kiện và thông tin bảo mật mã nguồn mở ELK như một phần chiến lược quản lý các sự kiện bảo mật tập trung

Nội dung và Phương pháp

- Xây dựng và đánh giá các mô hình, biến thể dựa trên SOINN
- Sử dụng bộ dữ liệu CLUE-LDS cho lần train đầu tiên
- Sử dụng độ đo Silhouette để đánh giá mô hình
- Huấn luyện liên tục mô hình trong thời gian thực bằng việc tận dụng khả năng học tiệm tiến của mô hình



Kết quả dự kiến

- Hiểu được hành vi người dùng và thực thể trong hệ thống mạng doanh nghiệp
- Mô hình dự đoán thời gian thực đạt hiệu suất cao
- Có khả năng triển khai và tích hợp vào hệ thống quản lý sự kiện và thông tin mã nguồn mở ELK

Tài liệu tham khảo

- Ren, Jing, et al. "SOINN Intrusion Detection Model Based on Three-Way Attribute Reduction." Electronics 12.24 (2023): 5023.
- Landauer, Max, et al. "A User and Entity Behavior Analytics Log Data Set for Anomaly Detection in Cloud Computing." 2022 IEEE International Conference on Big Data (Big Data). IEEE, 2022.