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

Tác giả Nguyễn Tấn Kiệt

Trường Đại học Công nghệ Thông tin

What ?

Chúng tôi xin giới thiệu một thuật toán phát hiện bất thường hành vi của người dùng và thực thể :

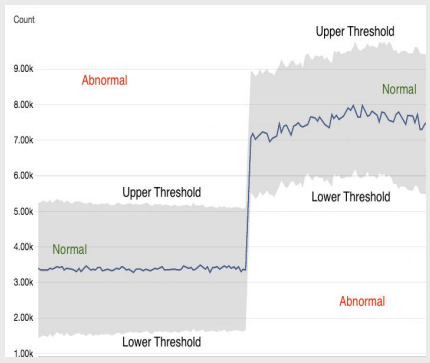
- Đề xuất phương pháp giám sát và phân tích hành vi người dùng và thực thể trong mạng doanh nghiệp
- Đã đánh giá các thuật toán dựa trên SOINN để xác định người dùng độc hại
- Tích hợp vào hệ thống SIEM mã nguồn mở

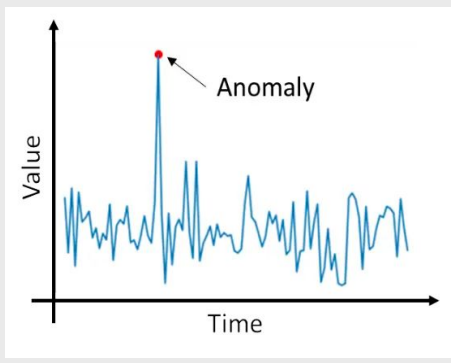
Why ?

- Phân tích hành vi của người dùng và thực thể rất quan trọng đối với bảo mật doanh nghiệp, cung cấp thông tin chi tiết quan trọng để xác định các tài khoản bị xâm nhập và những người nội bộ độc hại.
- Hầu hết các công cụ phân tích hành vi của người dùng và thực thể đều tập trung vào quy tắc dựa trên phương pháp thống kê và các tập luật

Overview

Thu thập dữ liệu → tạo mức ngưỡng → Phát hiện bất thường → Đánh giá mức rủi ro





Description

1. Thu thập dữ liệu

- Thu thập nhật ký người dùng từ nhiều hệ thống khác nhau như : email, truy cập trang web, xác thực, đối tượng chia sẻ, …

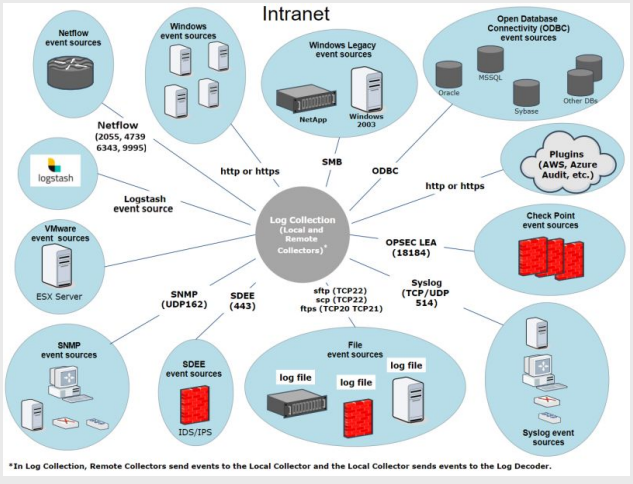


Figure 1. Thu thập nhật ký người dùng từ nhiều nơi

2. Tạo mức ngưỡng

- Chúng tôi đã sử dụng các thuật toán học máy để phân tích thông tin được thu thập và thiết lập đường cơ sở về hồ sơ hành vi của người dùng và thực thể thông thường nhằm phân biệt giữa các hoạt động thông thường và các sự kiện bất thường

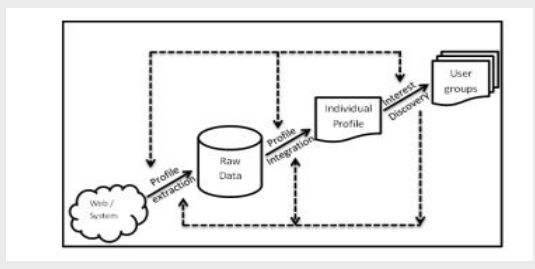


Figure 2. User and entity profiling

3. Anomaly detection

- UEBA có thể bắt đầu xác định những sai lệch so với đường cơ sở đó. Các điểm bất thường có thể bao gồm các kiểu truy cập bất thường, truyền dữ liệu không thường xuyên hoặc các hoạt động khác đi chệch khỏi các quy tắc đã thiết lập.

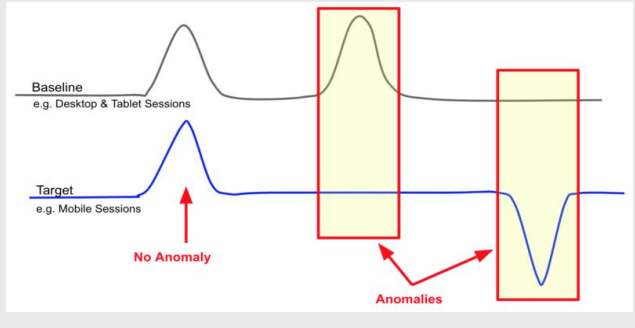


Figure 3. Đường cơ sở và sự bất thường của hành vi

4. Đánh giá mức độ rủi ro

- Chuyển đổi điểm bất thường thành điểm rủi ro
- Điểm rủi ro cao cho thấy một sự kiện cần được chú ý ngay lập tức, trong khi điểm thấp hơn có thể biểu thị rằng cần phải điều tra thêm.

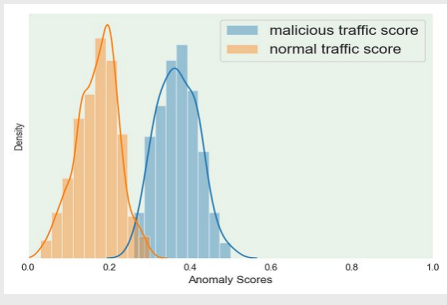


Figure 4. Điểm cơ sở và điểm bất thường

NII

Nguyễn Tấn Kiệt – Trường Đại học Công nghệ Thông tin

TEL : 0358223020 Email : kietnt.18@grad.uit.edu.vn