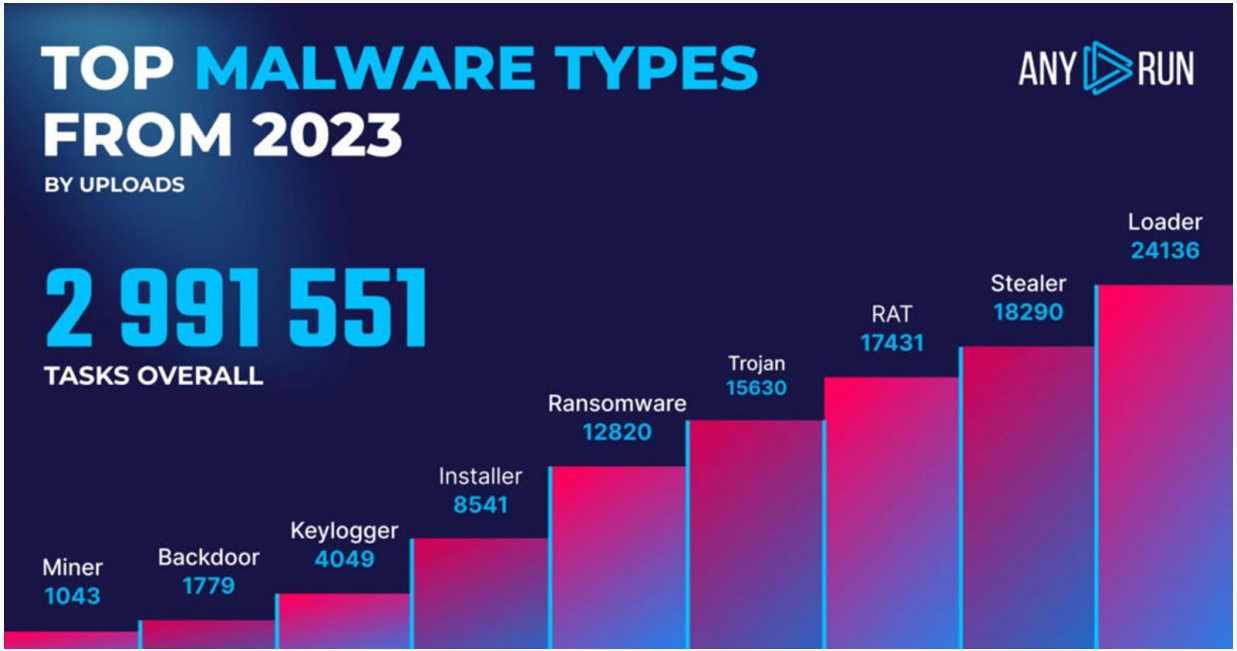
Ứng Dụng Natural Language Processing(NLP) Để Thu Thập Tri Thức An Ninh Mạng Trên Trình Duyệt Web

Sử Chấn Hoài Bảo - 230202003

Tóm tắt

- Lớp: CS2205.CH181
- Link Github:
- Link YouTube video:
- Ảnh + Họ và Tên: Sử Chấn Hoài Bảo
- Tổng số slides không vượt quá 10

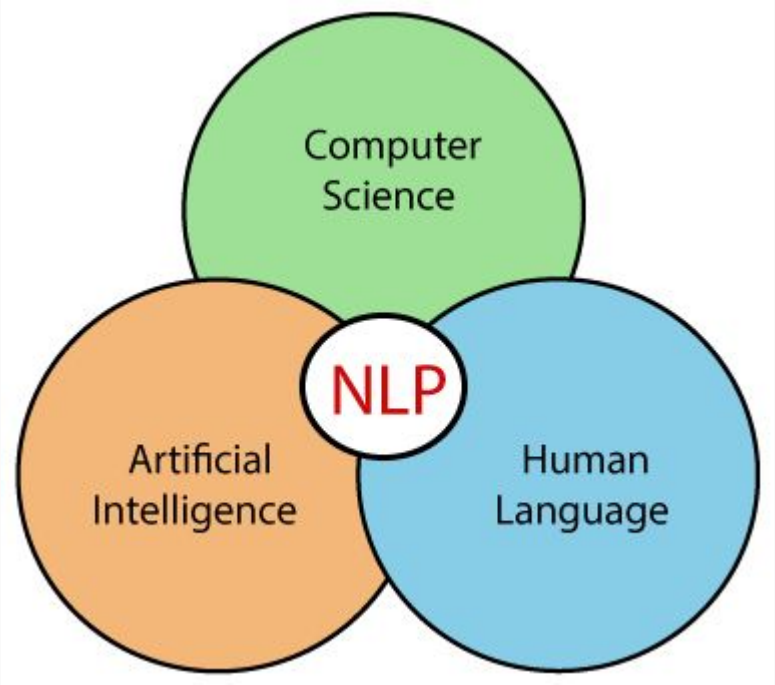
Giới thiệu



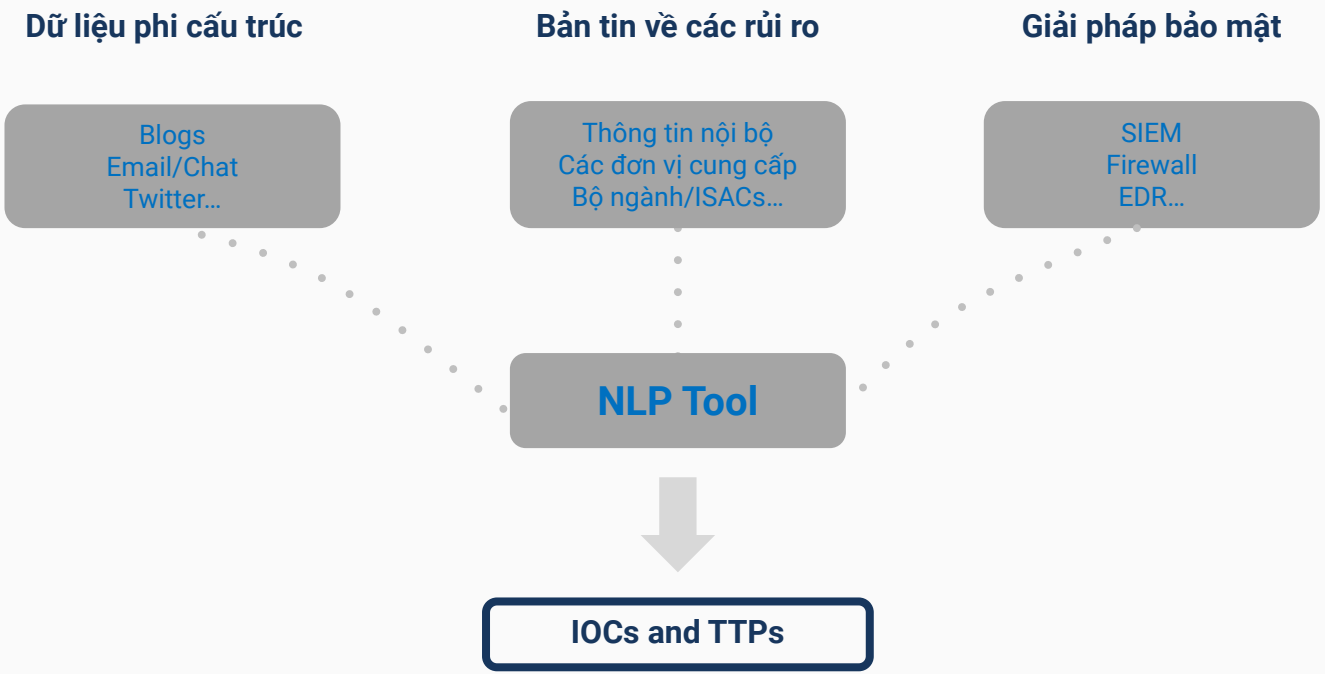
- Ai đang nhắm vào tổ chức của chúng ta?
- Tổ chức của chúng ta có bị tấn công hay chưa?
- Tổ chức của chúng ta đang bị tấn công bằng phương thức nào?

https://any.run/cybersecurity-blog/malware-trends-2023/

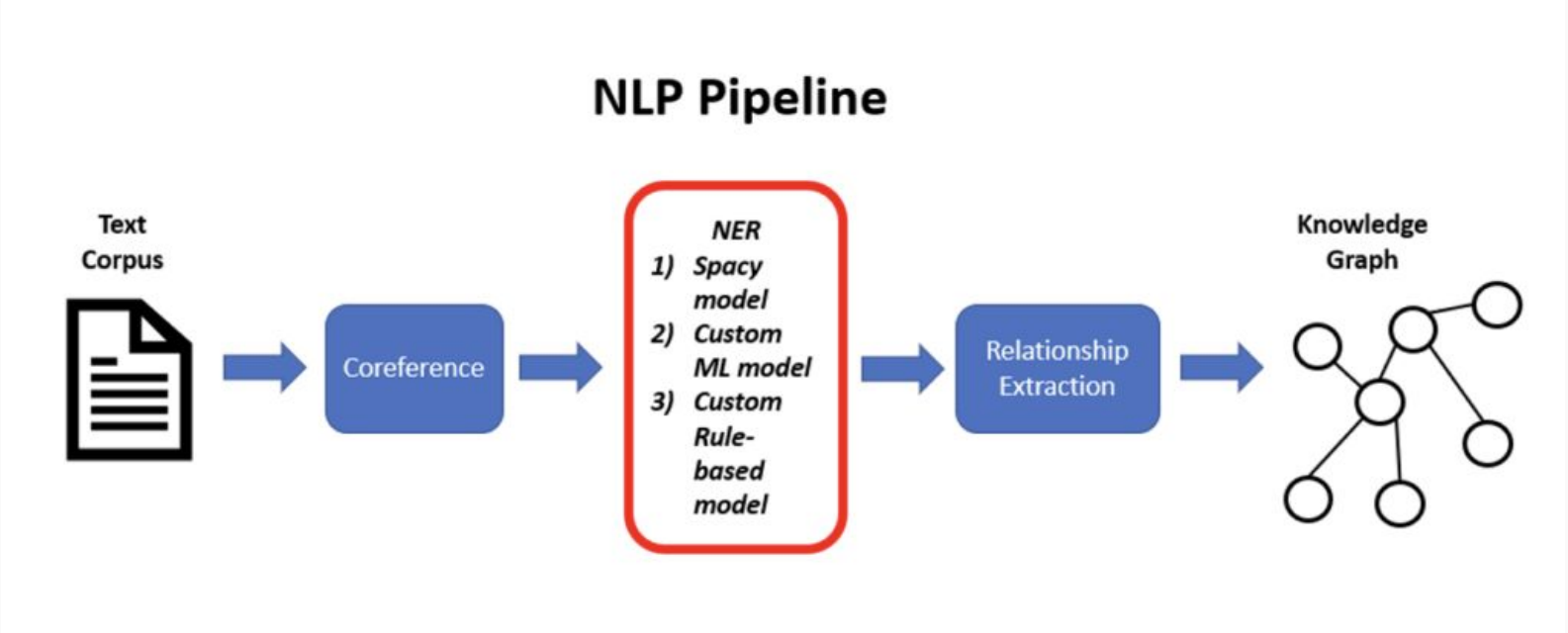
Giới thiệu


Computer
Science
NLP
Artificial
Intelligence
Human
Language

Mục tiêu


Dữ liệu phi cấu trúc
Bản tin về các rủi ro
Giải pháp bảo mật
Blogs
Email/Chat
Twitter...
Thông tin nội bộ
Các đơn vị cung cấp
Bộ ngành/ISACs...
SIEM
Firewall
EDR...
NLP Tool
IOCs and TTPs

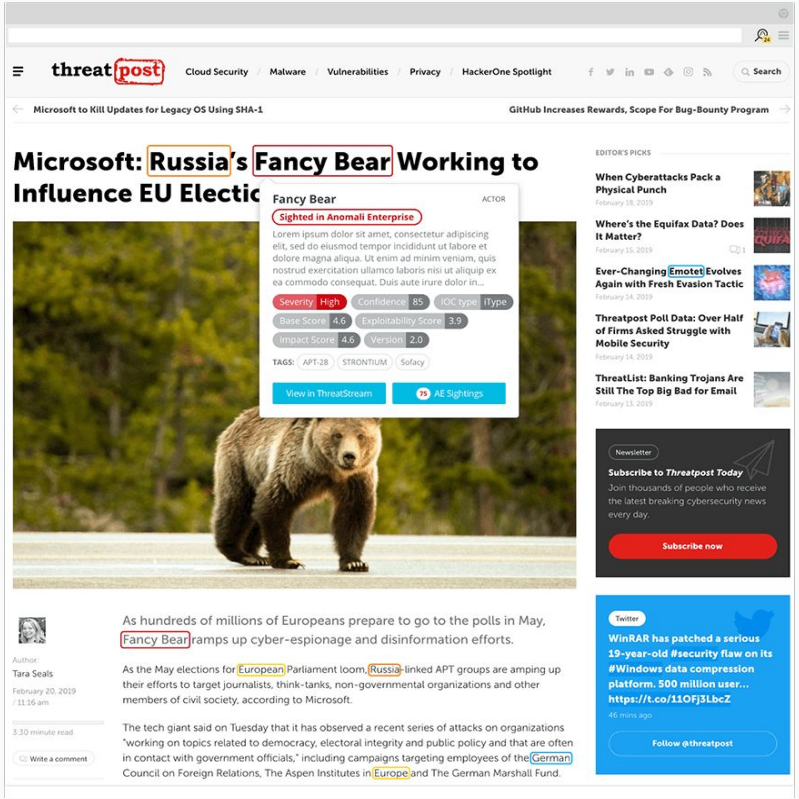
Nội dung và Phương pháp

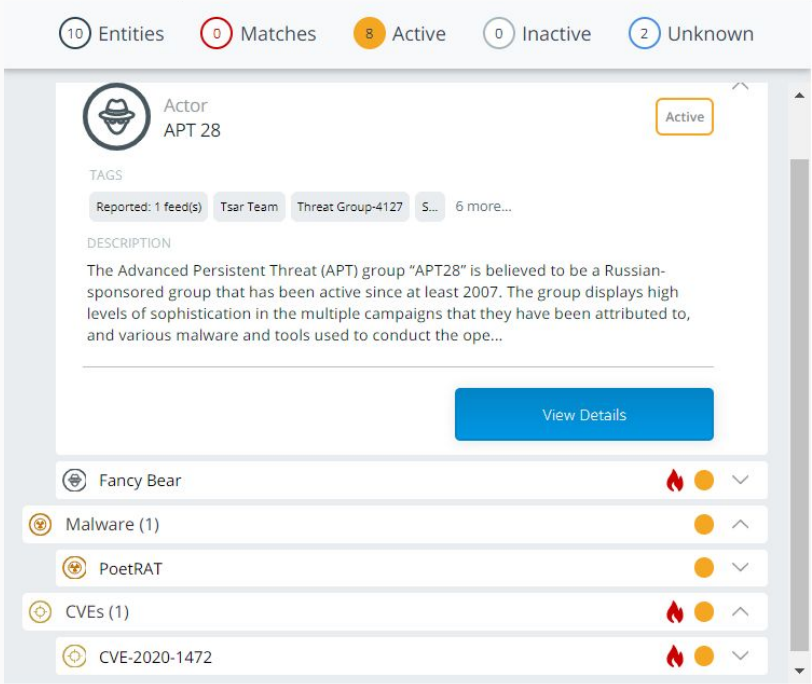


Nội dung và Phương pháp

STT	Nội dung
1	Xác định vấn đề và mục tiêu phát triển
2	Thu thập dữ liệu
3	Xử lý dữ liệu
4	Xây dựng mô hình NLP phù hợp
5	Triển khai và đánh giá
6	Tinh chỉnh và cải tiến

Kết quả dự kiến





Tài liệu tham khảo

[1]. M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh, J. Horn, S. Mangard, P. Kocher, D. Genkin, et al., “Meltdown: Reading kernel memory from user space,” in 27th { USENIX } Security Symposium ({ USENIX } Security 18), pp. 973–990, 2018.

[2]. C. Sauerwein, I. Pekaric, M. Felderer, and R. Breu, “An analysis and classification of public information security data sources used in research and practice,” Computers & security, vol. 82, pp. 140–155, 2019.

[3]. B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, “Mitre att&ck: Design and philosophy,” Technical report, 2018.

[4]. M. R. Rahman, R. Mahdavi-Hezaveh, and L. Williams, “A literature review on mining cyberthreat intelligence from unstructured texts,” in 2020 International Conference on Data Mining Workshops (ICDMW), pp. 516–525, IEEE, 2020.