SEMI_PROJECT

팀 프로젝트 발표

다크웹 유출 정보 알림 및 OSINT 수집 시스템 개발

구름 딥다이브 정보보호 11회차
김지은 | 조수민 | 이우진 | 이순우

K-Digital Training

고용노동부 KSQA KOREATECH 직업능력심사평가원

목차 LIST

01 프로젝트 개요 PROJECT

- **프로젝트 주제**

Telegram

랜섬웨어 그룹이 다크웹에 유출한 leak 데이터와 Telegram 상의 OSINT 기법을 통해 공격자 프로파일링을 수행하여,

그 분석 결과를 Discord DM으로 전송하는 통합 보안 분석 시스템

01 프로젝트 개요 PROJECT

- **주제 선정 배경**

1. 증가하는 사이버 범죄

2. 정보의 중요성

3. 신속한 위협 대응

현재 사이버 범죄가 기하급수적으로 증가하고 있으며, 공격 기법은 날로 정교해지고 있습니다. 이로 인해 다크웹과 텔레그램 등 다양한 플랫폼에서 유출되는 보안 정보는 공격자 형태와 관련 인프라를 파악하는데 결정적인 역할을 합니다.
사이버 위협은 실시간으로 변화하기 때문에 이에 따른 빠르게 대응할 수 있는 체계가 필수적이라고 생각했습니다

01 프로젝트 개요 PROJECT

- 활용 장비 및 재료(개발 환경)

elasticsearch

Google Cloud Platform

python™

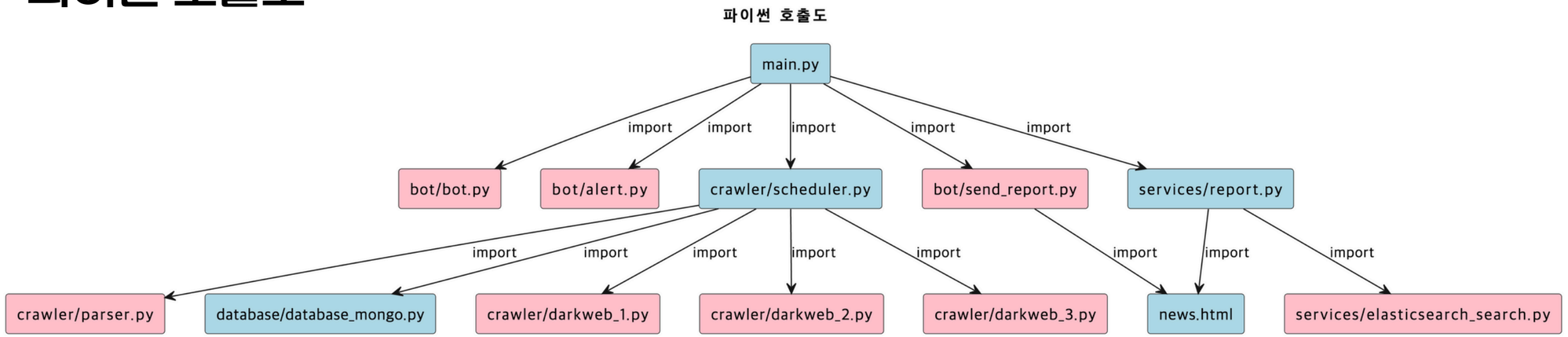
docker

mongoDB

01 프로젝트 개요 PROJECT

- 프로젝트 구조

파이썬 호출도



01 프로젝트 개요 PROJECT

- 기대 효과

  - 개인 정보 및 기밀 데이터 유출 여부 조기 탐지
  - 키워드 검색을 이용해 특정 공격 사전 경고 가능
  - 유출 정보를 분석해 피해 동향 분석 용이
  - 모니터링 자동화로 효율성 증가 및 비용 절감

02 팀 구성 및 역할 TEAM MEMBER

팀장

김지은

프로젝트 기획

DB가공, 삽입

수집 데이터 검증 기능 구현

키워드 검색 기능 구현

개발 환경 구성

조수민

웹 크롤러 작성

리포트 스케줄러 작성

일일 리포트 데이터 검색

DB, 엘라스틱서치 검색

이우진

웹 크롤러 작성

크롤러 스케줄러 작성

HTML 템플릿 제작

크롤러 DB 연동

★응원단장★

부팀장

이순우

텔레그램 크롤러 작성

디스코드 봇 기능 구현

키워드 알림 기능 구현

일일 리포트 전송 기능 구현

프로그램 기능 통합

03 프로젝트 진행과정 WORK FLOW

STEP 01

주제 및 목표 설정

프로젝트 기획
프로젝트 기간별 계획

STEP 02

사전 조사

기술 스택 및
크롤링 사이트 조사

STEP 03

코드 개발

개별 코드 개발

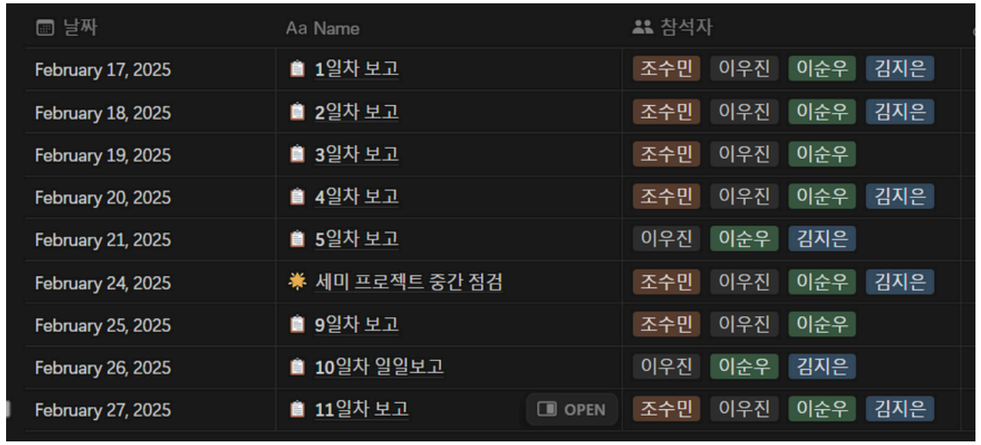
STEP 04

테스트

코드 통합 및
실행 테스트

03 프로젝트 진행과정 (회의)

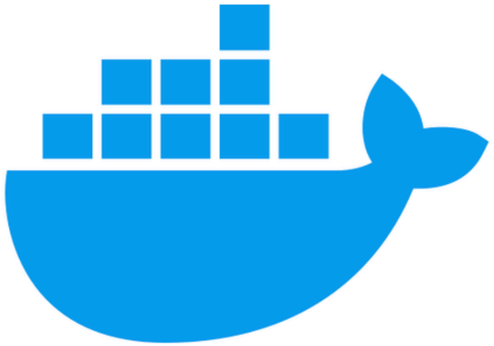
Notion 평일 15시 회의, 개별 진행도 공유



날짜	Aa Name	참석자
February 17, 2025	1일차 보고	조수민 이우진 이순우 김지은
February 18, 2025	2일차 보고	조수민 이우진 이순우 김지은
February 19, 2025	3일차 보고	조수민 이우진 이순우
February 20, 2025	4일차 보고	조수민 이우진 이순우 김지은
February 21, 2025	5일차 보고	이우진 이순우 김지은
February 24, 2025	세미 프로젝트 중간 점검	조수민 이우진 이순우 김지은
February 25, 2025	9일차 보고	조수민 이우진 이순우
February 26, 2025	10일차 일일보고	이우진 이순우 김지은
February 27, 2025	11일차 보고 OPEN	조수민 이우진 이순우 김지은

03 프로젝트 진행과정

25.02.17.	|	프로젝트 기획
25.02.18. - 25.02.23.	|	개발 환경 구성 크롤러 제작

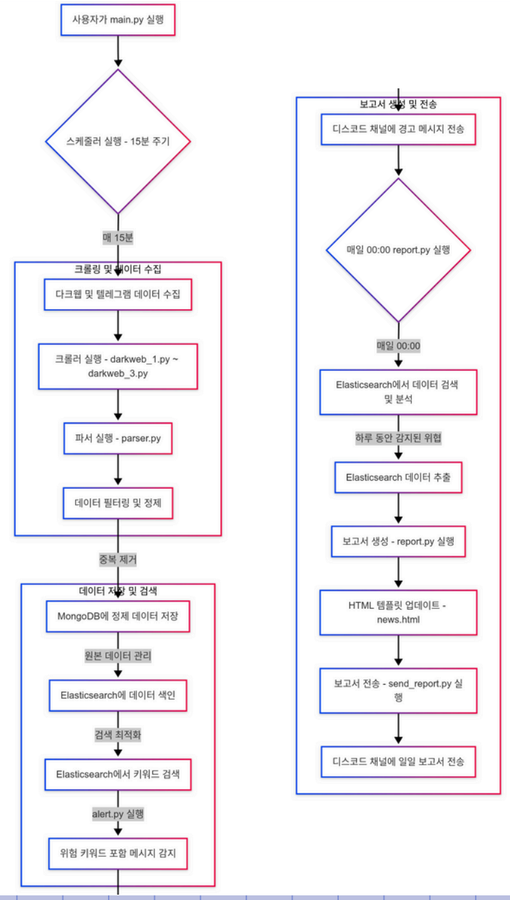


git

03 프로젝트 진행과정

25.02.24. | 프로그램 흐름도 및 호출도 작성
개발 업무 분담

25.02.24. | 코드 작성 및 취합
-
25.02.28. GCP
테스트 진행

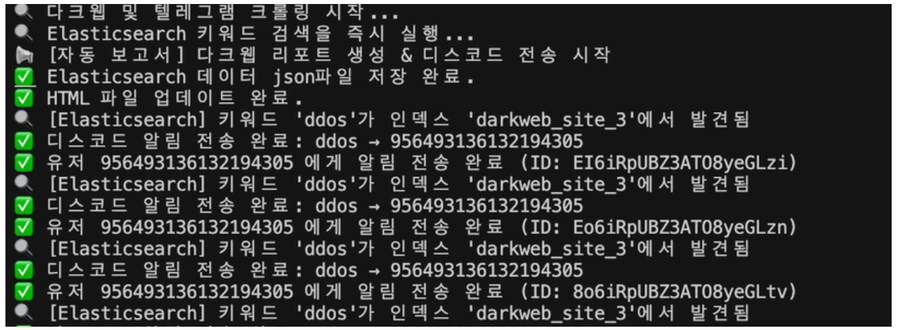


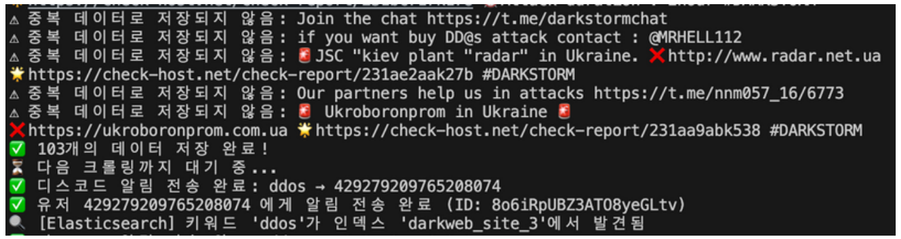
03 프로젝트 진행과정

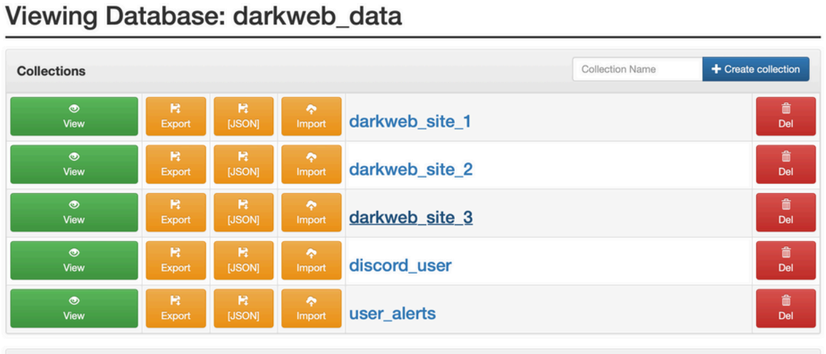
	17	18	19	20	21	22	23	24	25	26	27	28
프로젝트 기획												
사전 조사 및 개발 환경 구성												
크롤러 및 파서 개발												
프로그램 진행도 및 흐름도 작성												
코드 통합 및 테스트												

04 프로젝트 수행 결과

크롤링 및 데이터 저장







_id	title	description	source	alert_sent
67c08e2bb21a213a7cd17d98	Makesworth Accountants	Makesworth Accountants is multi-award-winning acc…	darkweb_1	false
67c08e2bb21a213a7cd17d99	Lakeshore Title Agency	Lakeshore Title Agency has closed over $100 milli…	darkweb_1	false
67c08e2bb21a213a7cd17d9a	Grupo Vargas	Laboratorios Vargas stands out in the pharmaceuti…	darkweb_1	false
67c08e2bb21a213a7cd17d9b	Retemex	Retemex is a virtual mobile operator in Mexico, o…	darkweb_1	false
67c08e2bb21a213a7cd17d9c	Brontoo Technology Solutions	Brontoo Technology Solutions India Private Limite…	darkweb_1	false
67c08e2bb21a213a7cd17d9d	nursing.com	NURSING.com is an all-in-one online platform desi…	darkweb_1	false

04 프로젝트 수행 결과

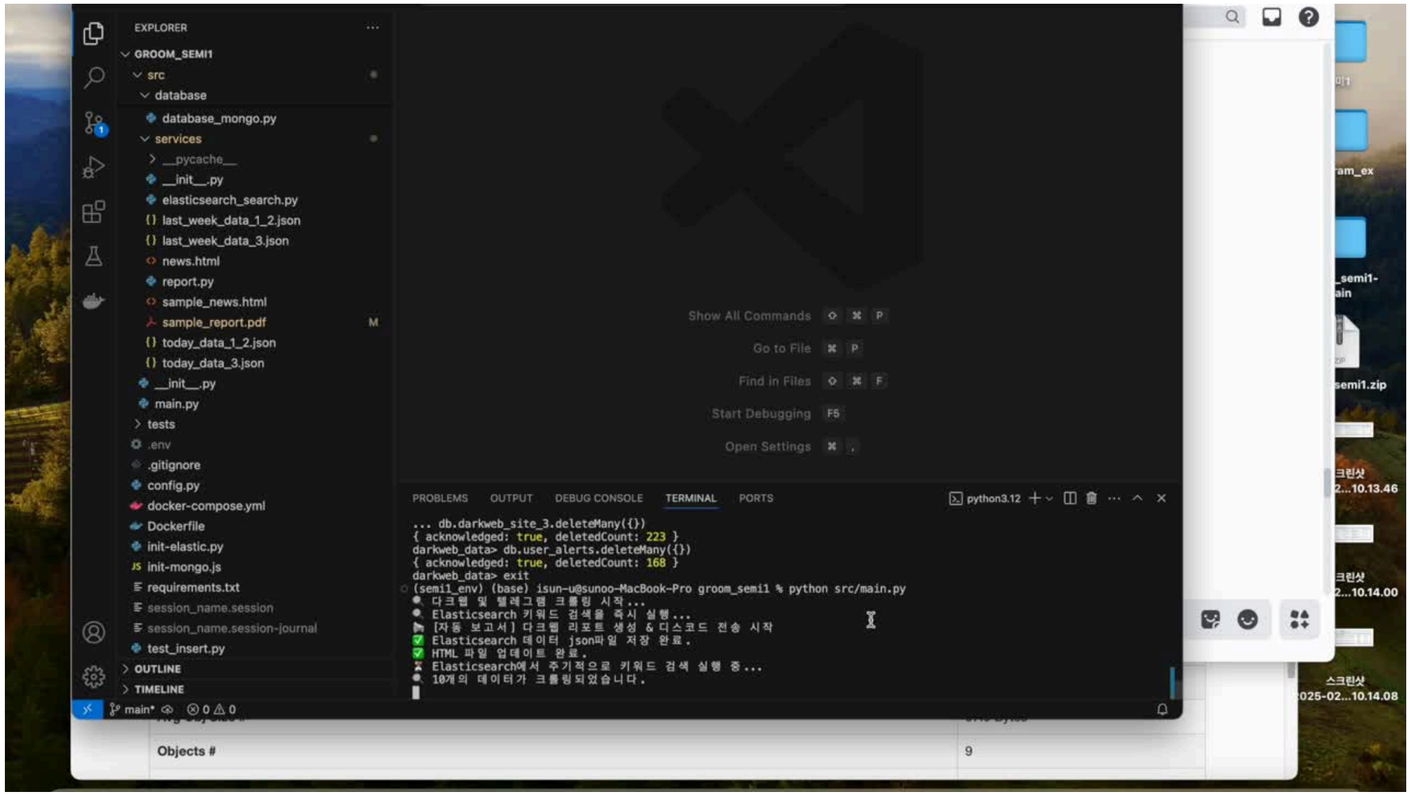
실시간 키워드 알림

keyword_bot_test 앱 오늘 오후 11:24
키워드 `ddos` 가 포함된 메시지 감지됨!

시간: 2025-02-16 08:24:31
내용: 👷ddos services menu : 1- DDos attack on protected website for 2hours 💲Price : $25 2- DDos attack on protected website for 1 Day 💲 Price : $60
3-DDos attack on protected website for 1 week 💲 price : $250 4- DDOS attack on protected website for 1month 💲 price : $600 💲
Payment methods : crypto 📞Contact to purchase : @MRHELL112
키워드 `ddos` 가 포함된 메시지 감지됨!

리포트 전송

04 프로젝트 수행 결과 시연 동영상



04 프로젝트 수행 결과

leak 데이터가 많이 없는 게 아쉽고
짧은 시간이었는데도 팀원들과 같이
프로젝트 만드는 과정이 좋았습니다.

05 자체 평가 의견

(팀장) 김지은

로그인이나, 자체 capcha 등 부가적인게 필요해서 활발한 leak 정보를 못 얻은게 아쉬움

(팀원) 이우진

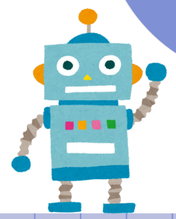
다크웹 사이트 들어가서 해킹 당할까 조금 무서웠지만 실제 leak 데이터를 확인하는 좋은 시간이었습니다.

(팀원) 조수민

계획했던 기능 대부분 구현했지만 코드 최적화, 프로그램 확장성에 대한 생각을 많이 못해 아쉬웠습니다.

(부팀장) 이순우

프로젝트를 기획하고 코드를 구현하면서 여러 데이터를 다룰 수 있는 좋은 경험이었습니다.



06 향후 개선방향

- 개선사항 1 — leak 데이터 다크웹 추가
- 개선사항 2 — Report 데이터 시각화 추가 (통계 자료)
- 개선사항 3 — 전체 DB 내용을 확인할 수 있는 웹서버 운영

07 질문과 답변 Q & A

궁금한 점이 있다면 자유롭게 질문해 주세요.

THANK YOU

감사합니다