ML 데이터기반의 효과적인
Insight분석역량을 가진

데이터 전문가,
최동욱 입니다.

데이터 분석 역량

빅데이터 기반 플랫폼 운영경험 및 다수의 보안솔루션 운영경험을 통한 이상행위 / 침해사고 대응에 핵심적인 역량.

Python 개발 역량

LLM기반 LangChain 활용, ML기반 데이터 분석 등, 다수의 Python 프로그램 개발 역량을 통해 업무 자동화 및 효율화, 개선 및 정보활용 역량

프로젝트 리더 역량

부서 내 파트장 역할 및 프로젝트 리더 수행경험을 통한 책임감 역량

이상행위, 악성코드 분석 / 침해사고 대응 역량

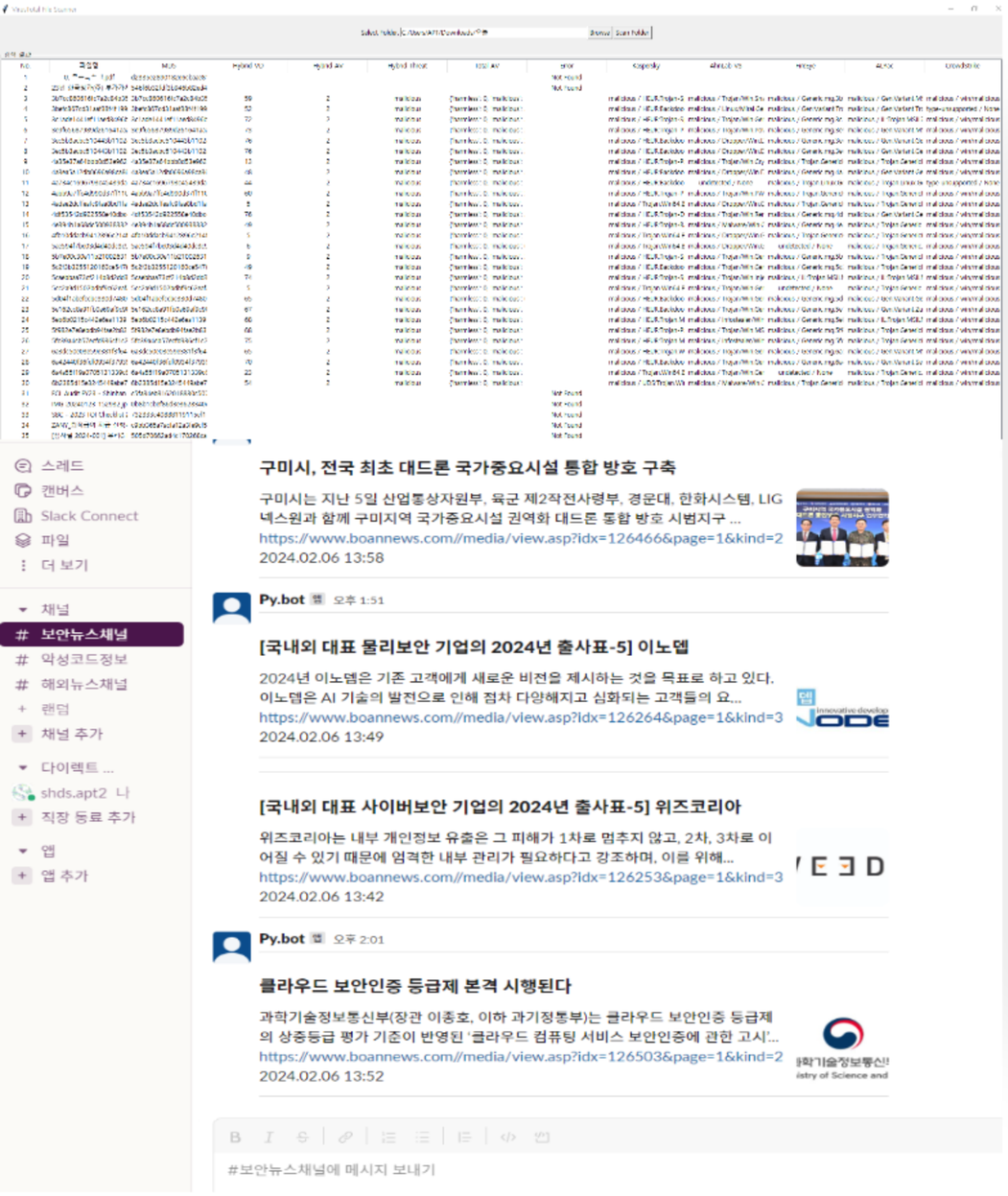
- CVE 취약점 기반 침해사고(RCE, Fileupload) 대응 - 사고발굴, 원인조사, 대응조치, 이행점검, 보고
- 악성코드 파일 상세 분석(정적분석 및 동적분석, 상세 포렌식 및 파일행위 여부) - 샌드박스환경구성, 다양한 분석Tool 응용 및 개발
- 최신 APT 위협 분석 및 악성메일 유포 최신 기법 동향 연구
- APT 보안솔루션 장비 구축 & 운영 (Trellix NX, EX, FX / Ahnlab MDS, DarkTrace NDR)
- APT 보안솔루션 미탐지(신규) 악성 패턴 반영 및 버그 조치
- 운영 고도화 (CustomRule 제작 고도화, 탐지구성 및 탐지로직 고도화)

- SPL기반(Splunk) 침해 위협, 침해 행위에 대한 탐지 기법(시그니처), 취약점 탐지 기법 - 고도화 및 개발
- SPL기반(Splunk) 응답 값을 통한 상관 분석 룰 제작, 악성코드 감염 신호 탐지 및 분석, 탐지 기법의 최적화 및 고도화 활동
- DDoS 공격 초동 조치 대응, 회선 우회, 공격 유입 분석 업무, DDoS 공격 트래픽 분석, 차후 대응 방안 고도화
- DDoS 탐지, 대응, 분석 가이드라인 매뉴얼 제작

Network Enginner 역량

- Field Trouble Shooting - Packet 분석 및 네트워크 상태, 장비 상태 분석, Traffic 분석을 통한 조치
- Site Maintenance - 장비 분석, 상태 분석, 네트워크 분석을 통한 결과 보고
- 신규 Configuration - Consulting을 통한 신규 구성 정의(Design) 및 Configuration 지원
- Firewall 설정 - 통신 관계 분석(Third Party), Firewall Dump 분석, Traffic 분석 및 Policy 정의 및 구성 및 Configuration 지원 업무
- Security (보안 적용) - 네트워크 장비 (L2, L3) 보안 취약점 분석, 보안 기능 설정 업무
- DCS 업체 Standard Configuration에 따른, Cisco L2, L3 Switch Configuration을 위한 설정 가이드 제작
- 다수의 해외 Trouble Shooting 출장 경험

Python 개발 역량



#1. Local 환경 LLM기반 LangChain 기능을 통한 인공지능 ChatGPT 기능 구현

#2. OpenAPI(Virustotal, hybrid) 연동을 통해 파일 MD5(hash)값 기반 대량 파일 악성 정보값 출력 프로그램 개발

#3. 국내 보안 동향, 해외 보안 동향, 악성코드 정보 동향을 각 사이트별 데이터 수집 후 번역기모듈 연동 및 Slack 프로그램 API를 통해, Slack 채널 별 정보 수집 개발

#4. 정보보안과 관련된 입찰정보에 대한 조달청 나라장터 API를 통해 입찰공고 별 Slack 전송 정보 수집 개발

#5. 신규 생성된 Malware파일 자료 수집 후, 보안솔루션(장비)로 송부하여 악성탐지 결과 조회 자동화 프로그램 개발

#6. 기타 그외 Speech to Text(STT) 음성녹음 프로그램, 부동산조회 프로그램 등등

감사합니다.

CONTACT

최동욱

010-9958-1419

https://github.com/donguk0207