공개출처정보(OSINT) 솔루션 개발

팀 명 : Joongsint

지 도 교 수 : 이병천 교수님

팀 장 : 우제혁

팀 원 : 노무승

송태현

이예준

이정호

이종엽

2024. 11.

중부대학교 정보보호학과

목 차

1. 서론

1.1. 연구 배경

대한민국은 사이버 보안을 비롯한 IT 분야에서 세계를 선도하고 있다. 그러나 인터넷에 연결된 기기와 모바일 기기 사용이 증가하면서 사이버 공격의 주요 대상이 되고 있다. 2021년 CONCERT 회원사를 대상으로 실시한 설문 조사에서 응답자의 36.4% 이상이 데이터 유출을 가장 심각한 침해로 꼽았다. 또한 한국인터넷진흥원(KISA)의 '기업 규모별 사이버 보안 침해 사고 신고 현황'에 따르면, 매년 중소기업의 침해 사고 신고 건수가 증가하고 있는 추세이다.

현대 산업 환경에서 중소기업은 핵심 기술 유출에 더욱 취약하다. 해커들은 대기업에 직접적인 공격이 어려울 경우 협력업체나 하청업체인 중소기업을 공격 대상으로 삼아, 내부 직원의 신분을 도용하여 대기업에 접근한다. 중소기업은 보안 인프라 구축이나 보안 인력 확보에 금전적인 부담을 겪고 있어 보안 취약성이 높아지고, 이는 외부 공격자의 침입과 내부 정보 유출의 위험을 증가시킨다. 그 결과 핵심 기술 정보의 무단 유출로 경쟁력 하락과 재정적 피해를 입을 수 있다.

또한 중소기업의 데이터와 핵심 기술이 유출되고 있음에도 불구하고, 정보 보안 전담 인력이 없는 경우가 많으며 보안 위협에 대한 경각심도 낮은 편이다. 중소기업 기술 보호 울타리의 '최근 3개년 중소·중견·대기업 기술 보호 역량 점수 분포'에 따르면, 중소기업은 중견·대기업에 비해 기술 보호 역량이 현저히 부족한 것으로 나타났다. 취약한 비율이 중견기업은 약 10%, 대기업은 약 3%인 반면, 중소기업은 40% 이상이 취약하거나 위험한 것으로 집계되었다.

중소기업을 대상으로 한 주요 사이버 공격으로는 악성코드 유포, 랜섬웨어 유포, 소셜 미디어 해킹, APT 공격 등이 있으며, 대부분 인터넷에 공개된 정보를 활용한 사회공학 기법을 이용한다.

1.2. 연구 목적 및 필요성

이러한 보안 위협을 예방하기 위해서는 효과적인 보안 위협 탐지 솔루션이 필요하다. 현재의 OSINT(Open Source Intelligence) 도구들은 주로 정보 수집에 초점을 맞추고 있으며, 보안 위협 정보를 제대로 탐지하거나 수집하지 못하는 한계가 있다. 따라서 중소기업이 직면한 보안 취약성을 개선하고 핵심 기술과 데이터를 보호하기 위해 보안 위협 탐지를 위한 OSINT 솔루션을 제안한다. 이 솔루션을 통해 중소기업은 미리 보안 위협을 탐지하여 보안 수준을 향상시킬 수 있으며, 기존 도구들의 한계를 보완하여 효과적인 대응 방안을 제공할 수 있다.

2. 관련 연구

2.1. 중소기업의 보안 위협

산업 보안은 산업 기술을 다양한 위험요소로부터 다방면으로 유출을 방지하는 활동을 의미한다.

국가 차원의 산업 보안 활동은 주로 기술 유출 차단 목적의 산업 스파이 색출 활동으로 이루어지 며, 기업 차원의 산업 보안 활동은 산업 기술 유출 방지와 함께 기업의 영업기밀을 보호하는데 목 적이 있다. 하지만, 산업 보안에 있어서 중소기업은 대기업에 비해 상대적으로 취약할 수밖에 없는 요인들을 가지고 있으며 실제로 피해 규모도 대기업에 비해 심각한 수준으로 나타나고 있다. 과학 기술정보통신부에서 공개한 22년 사이버 보안 위협 분석 및 23년 전망 발표'에 따르면, 2022년 한 국인터넷진흥원에 접수된 침해 사고 신고 건수가 전년 대비 약 16배 증가하였다고 발표하였다. 그 뿐만 아니라 피해 발생 분포를 확인해 보면 중소기업이 약 90%의 비율을 차지하고 있는 것을 확 인할 수 있다. 따라서 이와 같은 보안 사고가 증가하고 있으며 비교적 보안이 취약한 중소기업들 은 피해가 심한 것을 확인할 수 있다. 한국은 중소기업이 전체 기업의 99.9%를 차지하고 있으며 전체 기업 종사자의 87.9%가 중소기업에서 일하고 있다. 중소기업은 국가 경제의 버팀목이며 국민의 일터이다. 따라서 중소기업에서 개발된 핵심 기술들이 유의한 보안 관리를 통해서 외부로 유출 되지 않도록 정부 차원과 기업 차원에서 중층적인 보안 관리 장치가 마련돼야 한다.

2.2. 소스코드 유출 위협 및 보안 패치의 중요성

기술력이 핵심이 되는 중소기업에서는 AI 등 디지털 신기술 활용이 증가함에 따라 공개형 소프트웨어인 오픈소스의 활용이 비약적으로 증가하고 있다.

1990년대부터 소스 코드 유출은 존재했으며 기업에 큰 피해를 끼치고 있었으나, 최근 들어 디지 털 전환으로 소스 코드 유출 위험과 그로 인한 영향은 더욱 커진 상황이다. 일례로 게임사의 경우 소스 코드가 유출된 경우 해킹롬 파일을 제작하여 무단으로 게임을 이용할 수 있어, 게임 사업을 영위하기 어려울 정도로 큰 비즈니스 타격을 입게 된 사례가 존재하기도 한다. 이와 더불어 기업 의 이미지 또한 실추되게 되어 경제적 피해가 발생하기도 한다. 실제로 스냅챗은 소스 코드 유출 사고로 주가가 하루 동안 3.4% 하락했다.

2.3. OSINT 이론 배경

OSINT(공개 출처 정보)는 온라인상에 공개된 정보를 수집하고 분석하여 인텔리전스를 얻는 방법론으로, 인터넷, 소셜 미디어, 공공 기록 등 다양한 출처에서 정보를 수집한다. OSINT는 인터넷 검색 엔진, 소셜 미디어 분석 도구, 데이터베이스 검

색 등을 통해 정보를 수집하고, 이러한 과정에 서 신뢰할 수 있는 인텔리전스를 제공하기 위해 정보의 신뢰성과 타당성을 평가한 후 데이터 분석 및 시각화 기술을 활용하여 유용한 인텔리전스를 도출한다. 이를 통해 기업이나 조직은 위협 정보 및 시장 동향 등 다양한 정보를 확보할 수 있으며, 특히 보안 분야에서 그 중요성이 더욱 부각된 다. KISA에서는 사이버 위협 인텔리전스(CTI)를 효과적으로 사용하기 위해 필수적인 정보 공유를 NVD, DNS 등의 24개의 위협 정보 수집 시스템 채널로 구성된 OSINT를 기반으로 개발 중에 있 다. 또한, ISEC 2020와 K-CTI 2023에서 'OSINT를 이용한 기업 보안 강화 방안(Feat. Recorded Future)'를 주제로 다크 웹, 크리덴셜 등 새롭게 떠오르는 공격 형태에 대해 효과적인 대응 방안과

'OSINT 기반의 Attack Surface 모니터링(멀웨어&CVE 위협 정보)'에 대해 다뤘다.

이처럼 OSINT는 사이버 위협에 대한 대응과 사전 예방에 도움을 줄 수 있으며, 사이버 보안 전략의 일부로서, 공격 탐지, 위협 예측, 취약점 분석 등 다양한 보안 목적을 달성하는 데에 중요 한 역할을 할 수 있다.

2.4. 기존 OSINT 솔루션 분석 및 연구

OSINT 기술은 데이터 수집에 유용하지만 다양한 분야의 데이터 수집을 위해서는 여러 서비스 를 연결된 방식으로 사용해야 한다. 따라서 다양한 소스에서 고품질 정보를 수집하고 추론을 개선 하기 위해 자동화된 도구가 개발되었다. 기존의 OSINT 자동화 도구들의 성능을 확인하기 위해 기존의 중소기업을 대상으로 실험하는 것은 보안상의 문제가 된다. 따라서, 모의 기업을 구축하여 실제 기업과 동일하게 회사 도메인 및 SNS 서비스 등 다양한 정보를 공개적으로 노출시켰으며, 이를 통해 모의 기업의 데이터 수집에 대한 정확성을 분석하였다.

2.4.1. THE HARVESTER

THE HARVESTER는 기본적으로 이름, 이메일, IP, 다양한 검색엔진에 조사되는 하위 도메인 및 URL들을 찾아주는 역할을 하지만 도메인을 입력했을 때 IP 이외의 도메인들은 수집하지 못했 다. 또한 서블릿 기반의 웹에서는 데이터를 수집하지 못하는 한계점이 존재했다.[표 2] 또한 서블 릿 기반의 웹에서는 데이터를 수집하지 못했다. 따라서 goole.com, microsoft.com 등의 대기업 이 외에 잘 알려지지 않은 중소기업은 정보 수집이 수월하게 이뤄지지 않는 한계가 존재했다.

2.4.2. SPIDER FOOT

SPIDER FOOT은 사용 가능한 거의 모든 데이터 소스와 통합되고 다양한 데이터 분석 방법을 활용하여 해당 데이터를 쉽게 탐색할 수 있는 도구로서 DNS, Whois, IP, 이메일 주소, 소셜 미디어 등 229개의 다양한 모듈을 사용해서 정보를 수집한다. SPIDER FOOT는 기본적으로 도메인, 이메일, 휴대폰 번호 등을 입력하여 정보를 수집한다. 따라서 모의 기업 도메인 주소를 입력해본 결과 15시간이 소요되었으며 총

597개의 데이터가 수집 되었다.

2.4.3. Maltego

Maltego는 58개 이상의 데이터 소스에 액세스하여 도메인, 이메일, 전화번호 등의 데이터를 입 력하여 데이터를 수집한다. 따라서 모의 기업과 관련된 도메인 주소 및 이메일 전화번호, 소스 코 드가 담긴 GitHub 프로필 등의 데이터를 입력해 본 결과 다음과 같은 결과가 도출되었다.

Maltego는 각 모듈을 하나씩 사용해야 한다는 불편함이 있으며, 제대로 된 데이터 수집이 이뤄지 지 않았다. 또한 도메인 등록 기관의 이메일과 전화번호를 수집하는 등 관련 없는 데이터들을 수 집하여 별도의 분석이 필요했다. 결과적으로 maltego는 편리한 UI와 빠른 속도를 가지고 있지만, 추가적인 분석이 필요한 한계점이 있다.

2.4.4. Shodan

Shodan은 검색 결과를 통해 각 기기가 어떤 소프트웨어나 하드웨어를 사용하고 있는지, 또 어떤 버전을 사용하는지 등의 정보를 얻을 수 있어 사용자가 이를 바탕으로 잠재적인 취약점이나 위 험을 파악할 수 있다. Shodan의 사용 방법은 다양한 검색 필터링과 함께 키워드를 조합하여 원하 는 결과를 얻을 수 있다. 그러나 단일 필터링이나 검색을 위한 키워드가 부족한 경우 결과에 대한 정확도가 현저히 떨어지는 경우가 나타나며, 필터링과 키워드를 다양하게 조합하여 사용해도 도출 되는 결과가 동일하여 얻을 수 있는 데이터의 다양성이 떨어지는 한계가 있다.

2.4.5. recon-ng

Recon-ng는 오픈소스의 웹 기반 정보 수집 도구로 정보 수집을 자동화하고 결과물을 저장하거 나, 다른 도구를 이용한 분석 작업에 적용할 수 있도록 지원한다. Recon-ng는 쉽고 편리하게 사용 할 수 있는데, 명령어를 통해 모듈을 읽고 실행하며, 정규 표현식을 사용하여 데이터를 분석하고 조작할 수 있다. 그러나 모의 기업의 도메인을 입력하면 잘 알려진 유명한 기업들에 비해 공개된 데이터들을 출력해 오는 부분이 부족했다.[표 6] 이처럼 중소기업에 관련된 입력 데이터 값을 대상 으로는 만족스러운 정보를 수집하기가 힘들다는 한계가 존재한다.

2.4.6. FOCA

FOCA (Fingerprinting Organizations with Collected Archives)는 Microsoft Windows 운영체제 에서 실행되며, 기술 요소 및 메타데이터에서 정보를 추출한다. FOCA는 또한 같은 회사 또는 사 이트에 올린 여러 문서 및 파일 간의 관계를 통해 특정 주소 또는 조직의 다른 정보를 생성한다.

또한, FOCA는 PDF, HTML, Word, Excel 등과 같은 다양한 문서에서 메타데이터 수

집하는 것을 중점을 두고 있다. 하지만 입력 데이터로는 오직 도메인만을 입력할 수 있으며, 모의 기업의 도메 인을 입력하여 도출된 결과로는 다음과 같이 ip, 도메인, 서버 버전에 대한 정보를 가져온다.[표 기 그러나 이용자들이 이용할 수 있는 입력 데이터 값의 한계와 수집되는 데이터의 다양성이 부족하 다는 한계를 가지고 있다.

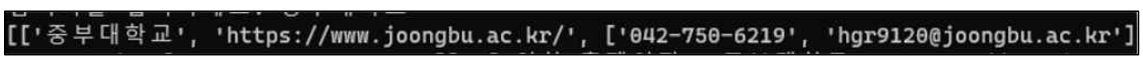
3. 본론

3.1. SNS 모듈

기존의 OSINT 도구의 특징은 SNS에 검색한 사용자의 프로필이 있는지만 찾아주는 역할이 대 부분이었다.따라서 관련 프로필인지 중요 데이터가 유출되었는지는 직접 분석해야 했다. 하지만 보고서에서 제안하는 OSINT 솔루션은 기존의 한계점을 보완해서 데이터 스크래핑 기술을 통해 존재하는 프로필의 이미지, 이름, 소개 글, 가입일, 해당 기업의 위치, 관련 이메일과 전화번호 등을 나타내주기도 하며, 소셜미디어 플랫폼에만 있는 기업의 스케줄 및 포스팅된 게시물들과 기업 관 련 해시태그까지 확인 가능하다. 결과적으로 해당 기업 태그 데이터들을 수집해서 관련 데이터 수집의 범위와 정확성을 높였으며, 수집된 데이터들을 확인하여 민감한 기업 관련 기밀 데이터들이 공개되었는지 파악한다. 따라서, 노출된 이메일과 전화번호 및 비공개회의 일정 등의 정보들을 관리하여 APT 공격에 대응할 수 있다.

3.2. 검색엔진 모듈

보고서에서 소개되는 OSINT 솔루션의 또 다른 검색엔진 모듈은 특정 기업의 정보 수집을 위 해 검색엔진 API를 사용한다. 기존의 검색엔진을 활용한 OSINT 도구들보다 더 세부화된 수집 범위와 데이터 마이닝 기법을 통해 사용자는 해당 기업에 대한 정보를 정확하게 수집하게 된다. 일반적으로 다른 OSINT 도구는 검색 결과 URL과 URL 소개 데이터를 수집하는 것 이외의 정보를 수집하지는 않는다. 하지만 보고서에서 소개하는 검색엔진 모듈은 검색되는 URL 링크 및 URL 소개 데이터를 수집한 뒤, 수집된 URL에 접속하여 각 페이지에서 노출되는 이메일 및 전화번호를 수집해오며 사용자가 지정한 키워드 존재 확인 단계까지 진행된다. 이처럼 OSINT 솔루션의 검색 엔진 모듈은 대량의 정보를 효율적으로 분석하고 처리할 수 있는 능력을 보유하고 있다.



[그림 1 검색엔진 모듈 수집 예시]

3.3. 도메인 모듈

기존의 OSINT 도구들은 수집하고자 하는 도메인을 입력받게 되어 해당 도메인의

서버 및 열려 있는 포트를 대상으로 인텔리전스를 수집하였다. 하지만 보고서에서 소개하는 OSINT 솔루션은 노출되어 있는 정보 수집에 초점을 맞췄다. 도메인 모듈은 입력받은 도메인을 기준으로 데이터 스크래핑 기술을 통해 해당 도메인의 웹 리소스를 수집한다. 웹 리소스에 존재하는 모든 키워드 및 전화번호, 이메일 데이터를 텍스트 마이닝 기법을 통해 분석하고 가공한다. 추가로 각 URL의 정보를 쉽게 확인하기 위해, 해당하는 URL의 화면을 캡처해서 어떻게 구성되었는지 사용자에게 제 공한다. 또한 키워드 필터링 기술을 활용해 노출되면 안 되는 키워드들을 지정하여 노출되어 있는 지 확인 가능하며 관련 없는 페이지를 수집 단계에서 제외하여 효율적인 기능을 향상시켰다. 이를 통해서 기업을 대표하는 페이지에서 원하지 않은 정보가 노출되어 있는지 파악할 수 있으며 기업 의 정보 노출 수준에 대해 확인이 가능하다. 또한, 숨겨져 있는 URL 및 주석 관리를 못한 소스 코드 또한 발견할 수 있어 이후 APT 공격 및 다양한 보안 공격을 대비할 수 있게 해준다.

[그림 2 도메인 모듈 수집 예시]

3.4. 깃허브 모듈

기존의 OSINT 도구들은 특정 도메인을 입력받아 해당 서버와 열려 있는 포트 등의 인텔리전스를 수집하는 데 초점을 맞춘다. 그러나 제공된 코드의 OSINT 솔루션은 노출된 정보의 수집에 중점을 둔다.

이 코드에서는 GitHub에서 특정 사용자 이름을 기반으로 공개된 리포지토리와 그 내부의 파일을 분석한다. 이를 통해 웹 리소스에 존재하는 모든 키워드, 전화번호, 이메일 등의 데이터를 수집하고, 텍스트 마이닝 기법을 활용하여 분석 및 가공한다. 또한, 노출되면 안 되는 키워드를 사용자로부터 입력받아 해당 키워드가 포함된 정보를 탐지한다.

추가적으로, 소스코드 내에 숨겨져 있는 주석이나 관리되지 않는 코드 부분을 발견하여 기업이 원하지 않는 정보가 공개되어 있는지를 파악할 수 있다. 이는 기업의 정보 노출 수준을 확인하고, 이후 발생할 수 있는 APT 공격이나 다양한 보안 위협에 대비할 수 있게 해준다.

이 솔루션은 불필요한 페이지나 정보를 수집 단계에서 제외함으로써 효율성을 높인다. 웹 리소스의 구조를 이해하기 쉽게 각 URL의 화면을 캡처하여 제공하는 기능

은 포함되어 있지 않지만, PDF 파일 등의 중요한 문서 링크를 수집하여 추가적인 정보 유출을 방지한다.

따라서 이 코드는 기업이 대표하는 페이지나 GitHub 리포지토리에서 원치 않는 정보가 노출되어 있는지를 효과적으로 파악하고, 보안 수준을 향상시킬 수 있는 OSINT 솔루션을 구현한다.

who	repository	path	content
songtaehyeon	SCP_mentoring	test.md	email : truebird@gmail.com
songtaehyeon	SCP_mentoring	test.md	phone : 010-0101-0101
songtaehyeon	SCP_mentoring	test.md	IP : 112.32.112.53
songtaehyeon	SCP_mentoring	test.md	api : testinday
songtaehyeon	SCP_mentoring	test.md	id : test
songtaehyeon	SCP_mentoring	test/history/may.py	#birnil_api : im_birnil
songtaehyeon	SCP_mentoring	test/history/truebird/OMG.C	//sEcond_ID : QueenCArd
songtaehyeon	SCP_mentoring	test/history/truebird/OMG.C	TEST_PW : P.ar CHU
songtaehyeon	SCP_mentoring	test/history/truebird/test.md	api : jaaja
songtaehyeon	SCP_mentoring	test/history/truebird/test.md	pw : sadsada
songtaehyeon	test	README.md	api = test
songtaehyeon	test	README.md	nu = 010-7749-4724

[그림 3 깃허브 모듈 수집 예시]

3.5. Report 모듈

보고서에서 제시하고 있는 OSINT 솔루션은 사용자들이 수집한 데이터를 로그 형태로 저장하여 사용자의 편의성을 강화하였다. 이 로그들은 Report 페이지에서 확인 가능하다. 사용자가 Report 페이지에 처음 접속하게 되면, 초기에 설정했던 폴더들을 선택할 수 있는 기능을 제공한다.

사용자가 특정 폴더를 선택하고 조회를 실행하면, 도메인, GitHub 모듈을 통해 수집했던 데이터들이 하나의 페이지에서 볼 수 있다.[그림 3] 페이지 안에 데이터들을 보고서 양식으로 된 PDF 파일로 변환시켜 데이터의 활용성을 높이는 기능도 있다. 따라서 사용자가 수집된 다양한 데 이터를 한눈에 파악하고, 이를 PDF 파일로 저장하여 쉽게 공유할 수 있다. 이와 같은 사용자 중심 적인 기능을 통해 보고서의 OSINT 솔루션의 데이터 관리 효율성을 높였다.

[그림 4 데이터 통합 조회 결과 페이지]

4. 검증 및 결과

4.1. 모의 기업 구축 및 데이터 수집

제안하는 OSINT 솔루션의 정확도 평가를 실제 중소기업을 대상으로 수행할 경우, 법적인 문제 와 민감 정보에 대한 우려가 있기 때문에 모의 중소기업을 자체 제작하여 검증을 진행했다. 기업 민감 정보에 대한 예민함 때문에 많은 기업들이 JavaScript 서블릿이나 SPA를 사용하여 데이터 스크래핑을 어렵게 만드는데, 이와 같은 환경에서도 보고서에서 제시하는 OSINT 솔루션을 검증 할 수 있도록 SPA 페이지로 모의 기업을 구축했다. 따라서 보고서의 모의 중소기업은 실제 기업 과 유사한 특성을 가지며, 회사 도메인, SNS, 블로그, 소스 코드, 숨겨둔 서버 등의 정보를 공개적 으로 노출시켜 제안된 솔루션의 정확도를 평가했다.

[그림 5 구축된 모의 기업 웹 사이트]

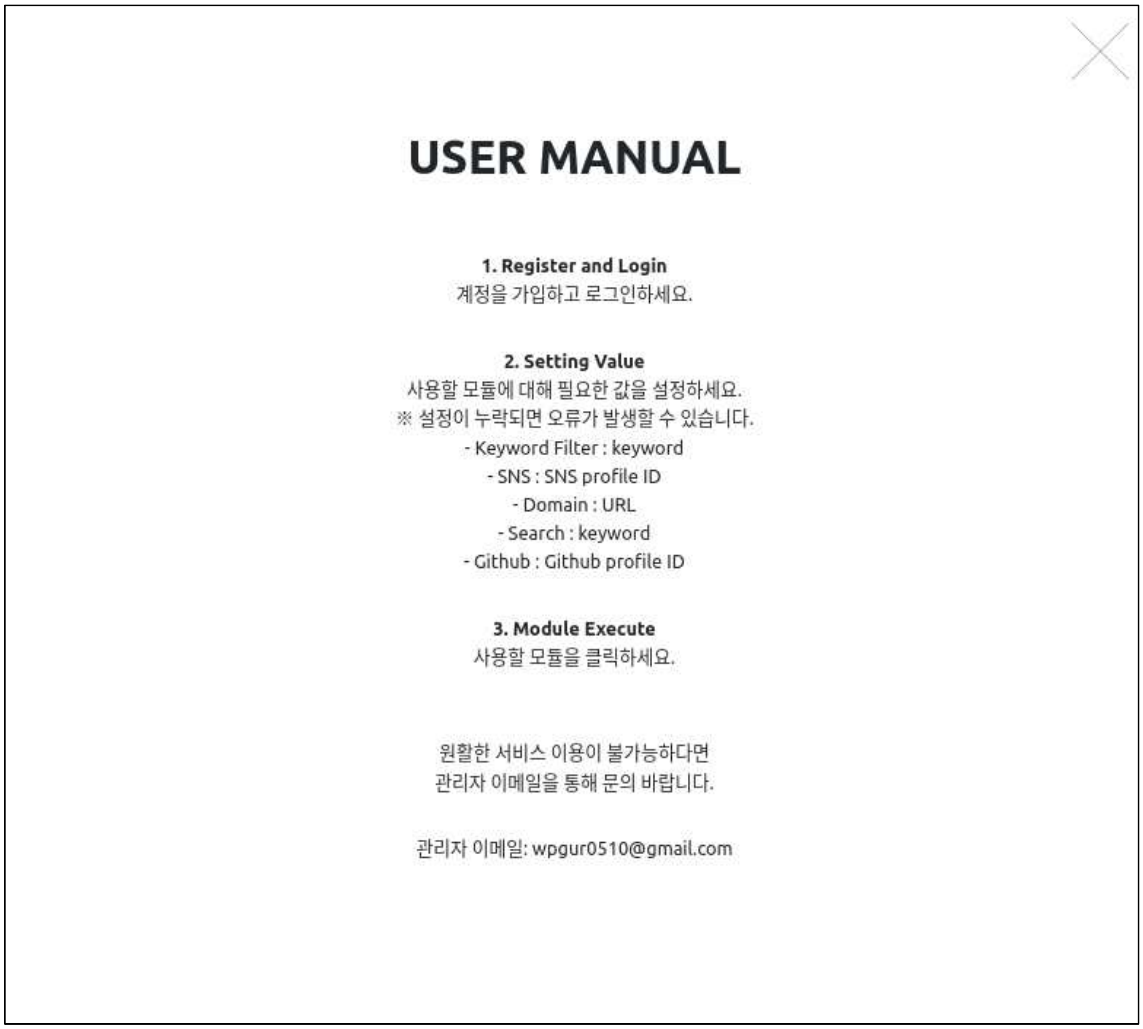
도메인, 검색엔진 모듈은 URL을 기반으로 데이터 수집했으며, URL 주소를 입력하여 성공적으로 이메일, 전화번호및 키워드를 추출했다.

Github와 SNS 모듈은 사용자 Profile ID를 기반으로 데이터 수집을 진행한다. SNS 모듈은 앞서 생성한 모의 기업의 Profile ID를 입력하여 데이터를 수집했고, Gitllub 모듈은 도메인 모듈에 서 수집한 ID를 기반으로, 해당하는 ID의 모든 Repository를 순회하여 IP, 이메일, 전화번호, 그리 고 사용자가 입력한 특정 문자열이 포함하는 데이터가 모두 수집되었다.

5.서비스 안내

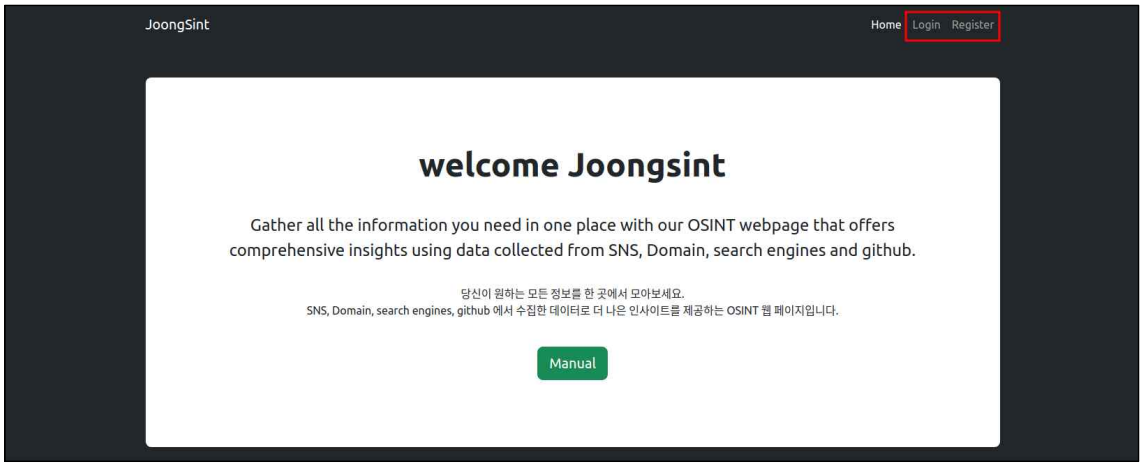
5.1. 서비스 활용 및 사례

OSINT 솔루션 활용 방법은 아래와 같다. 제공되는 OSINT 솔루션의 원활한 솔루션을 위한 매뉴얼이 상세하게 기입되어 있다.



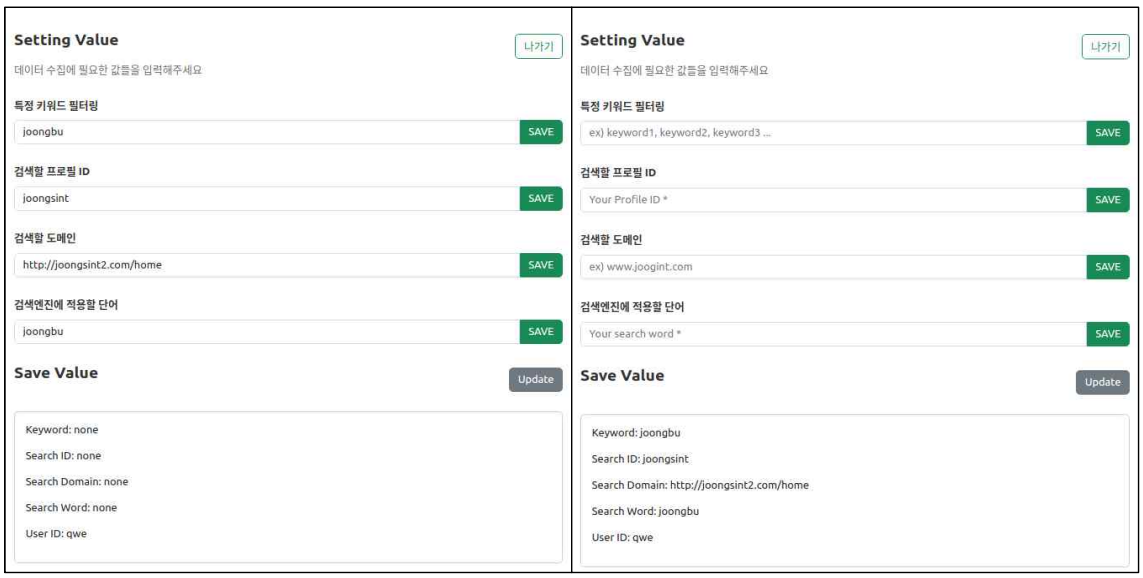
[그림 6 사용 매뉴얼 안내]

회원가입 및 로그인 프로세스는 개인화된 맞춤형 서비스 제공을 위한 필수 단계이다. 사용자는 SNS, 검색 엔진, 깃허브와 같은 다양한 모듈에 접근하기 위해 로그인 절차를 완료해야 한다. 또한,사용자 등록은 레포트 모듈을 통해 각 모듈 사용 결과를 종합적으로 확인할 수 있는 기능이 제공된다.

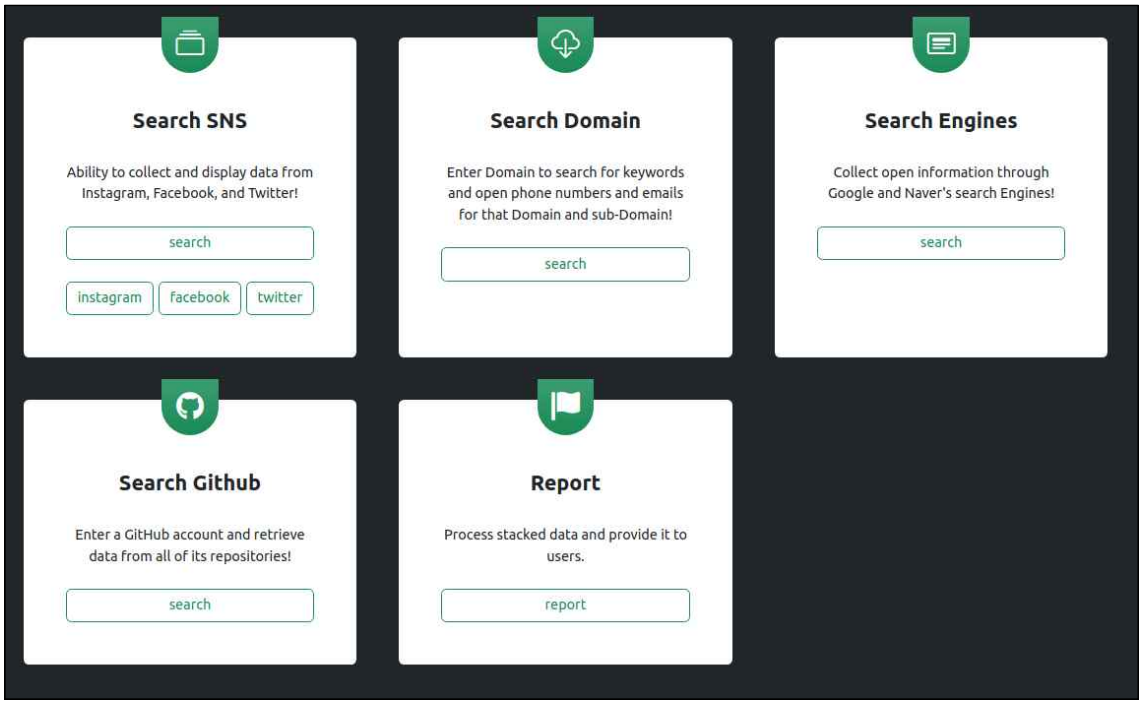


[그림 7 로그인 및 회원 가입]

정보 수집을 위한 각 모듈에 대해 필요한 키워드와 URL 등을 체계적으로 정의하여, 효과적인 데이터 수집과 분석을 위한 기반을 마련한다.

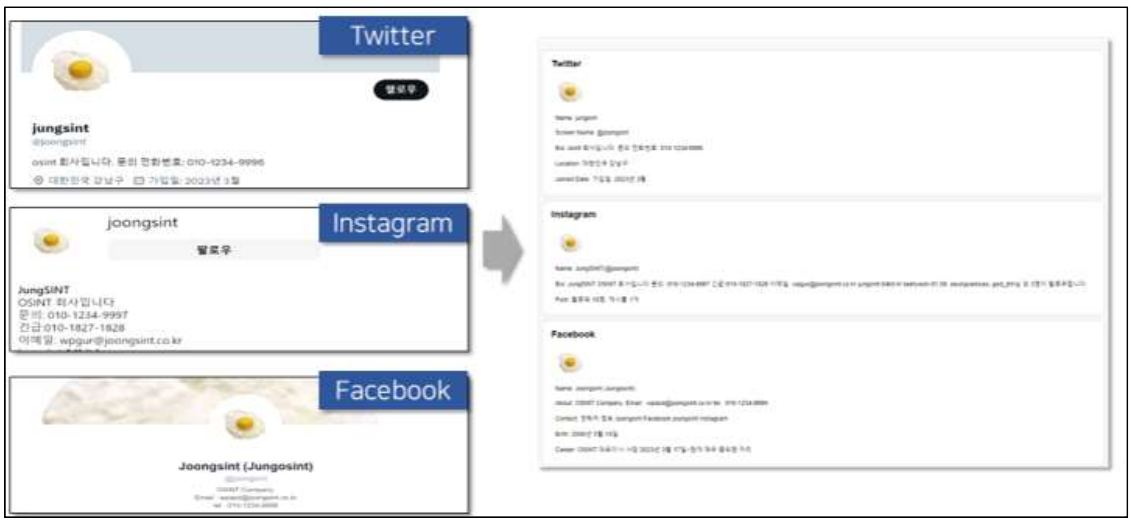


[그림 8 데이터 수집을 위한 설정]



[그림 9 제공 모듈]

SNS 모듈의 경우 저장된 프로필 ID를 기반으로 Twitter, Instagram, Facebook을 통한 데이터 수집을 진행한다. 해당 OSINT 솔루션의 경우 데이터 스크래핑 기술을 통해 존재하는 프로필의 이미지, 이름, 소개 글, 가입일, 위치, 관련 이메일과 전화번호 등을 나타내주기도 하며, 소셜 미디어 플랫폼에만 있는 기업의 스케줄 및 포스팅된 게시물들과 기업 관련 해시태그까지 확인할 수 있다.

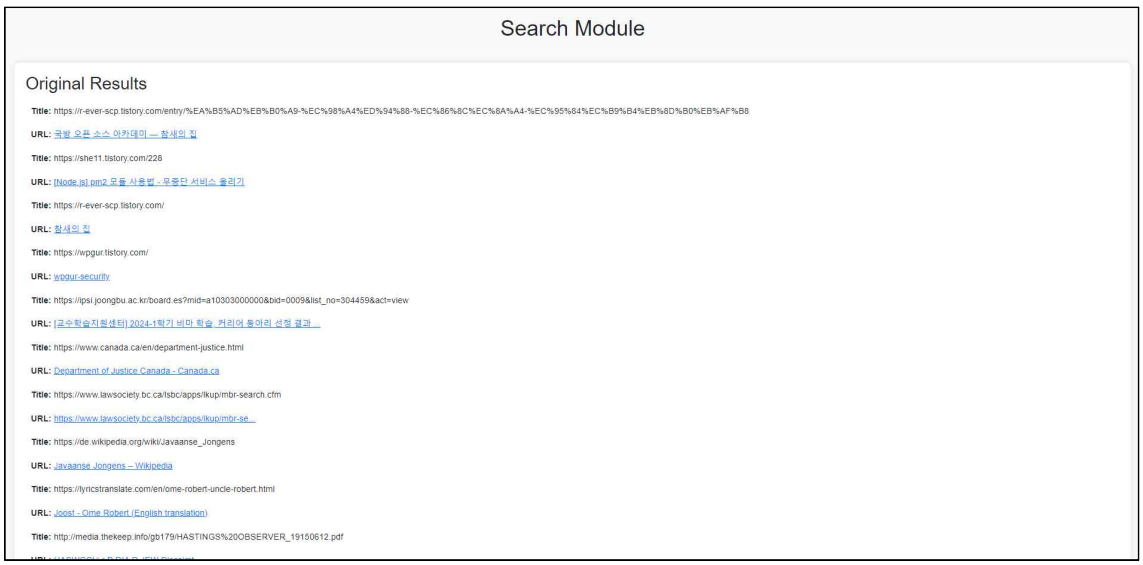


[그림 10 SNS 모듈 사용 결과]

도메인 모듈의 경우 입력받은 도메인을 기준으로 데이터 스크래핑 기술을 통해 해당 도메인의 웹 리소스를 수집한다. 또한 키워드 필터링 기술을 활용하여 사용자가 지정한 특정 키워드가 웹 페이지에 노출되는지를 확인할 수 있는 기능을 제공하여 사용자에게 민감한 정보나 원치 않는 콘텐츠의 노출을 방지하는 데 기여한다.

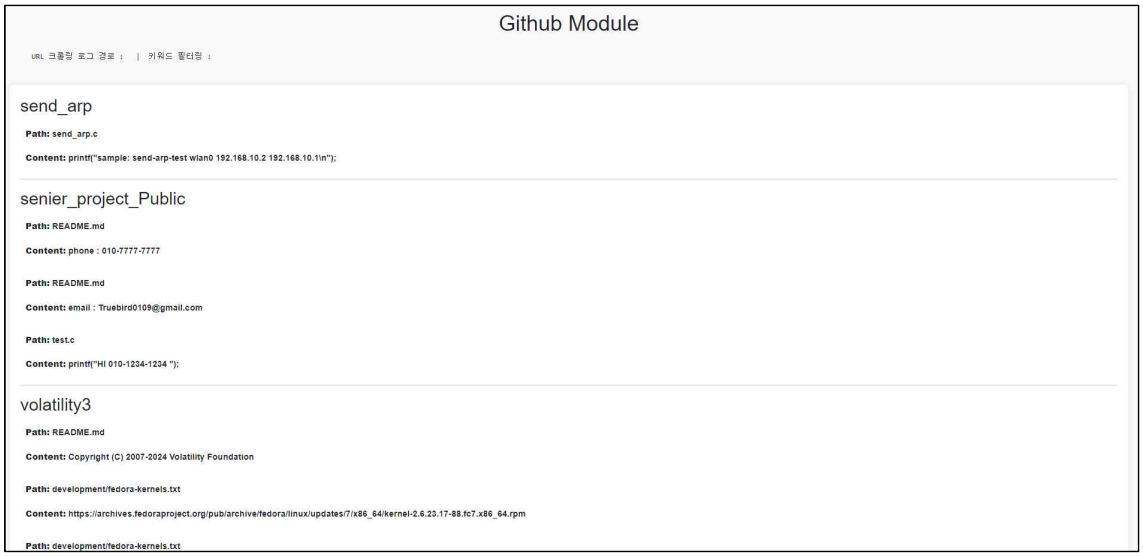
[그림 11 도메인 모듈 사용 결과]

검색 엔진 모듈은 검색엔진 API를 사용하여 기존의 검색엔진을 활용한 OSINT 도구들보다 더 세부화된 수집 범위와 데이터 마이닝 기법을 통해 사용자는 해당 기업에 대한 정보를 정확하게 수집하게 된다.



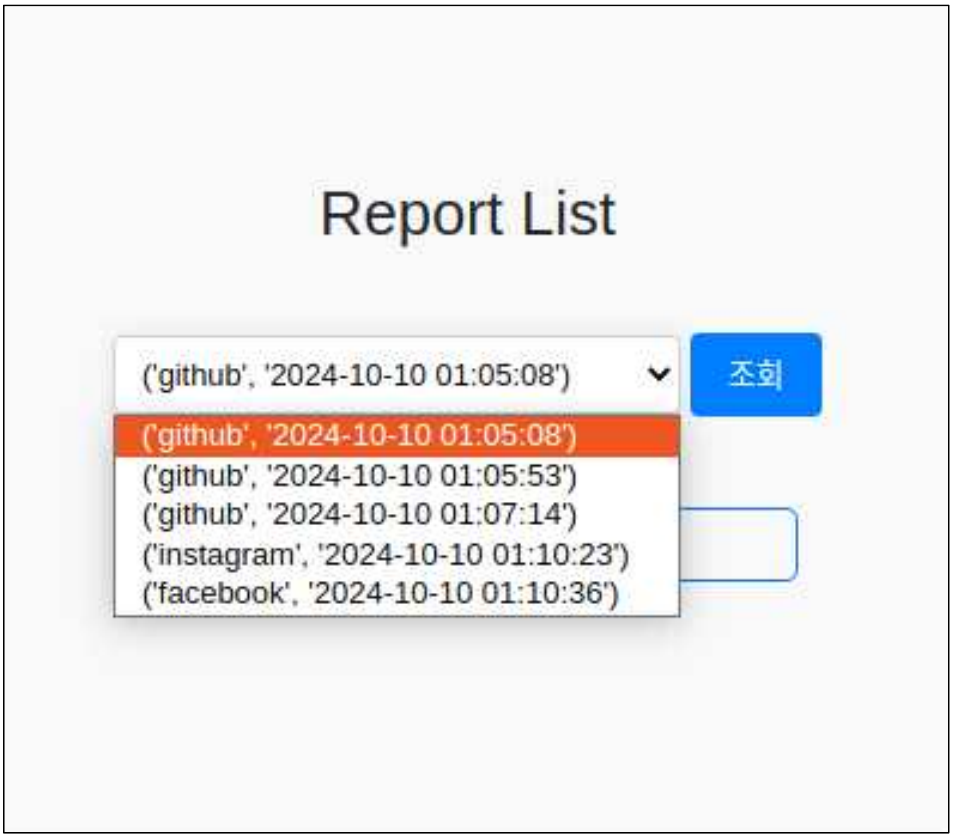
[그림 12 검색 엔진 모듈 사용 결과]

GitHub 모듈의 경우 GitHub 저장소를 분석하여 지정된 키워드나 IP 주소, 전화번호, 이메일과 같은 패턴을 검색하며, 발견된 PDF 파일의 링크를 수집하여 최종적으로 분석 결과를 웹 페이지에 표시하며 GitHub 관리 부주의로 인해 빈번히 일어나는 소스코드 유출에 대해 적극적으로 예방할 수 있다.



[그림 13 GitHub 모듈 사용 결과]

레포트 모듈의 경우 레포트 모듈은 사용자가 선택한 특정 레포트의 결과를 데이터베이스에서 조회하여 적절한 HTML 템플릿으로 보여준다. 사용자가 제출한 선택 값을 기반으로 레포트 모듈과 날짜를 가져오고, 해당 정보를 통해 JSON 형식의 결과를 변환하여 모듈에 맞는 페이지를 렌더링한다.



[그림 14 레포트 리스트]

5.2. 추후 보완사항

다크웹 모니터링 모듈을 구축하여 특정 키워드와 패턴을 설정해 관련 게시물이나 거래를 감지할 수 있도록 하며, 불법 행위가 발견되면 즉시 경고를 발송하고 관련 기관에 보고하는 기능을 추가한다. 수집된 데이터를 분석하여 불법 행위의 추세를 파악하고 시각화하여 사용자에게 직관적인 인사이트를 제공한다. 또한, 법적 및 윤리적 문제를 고려하여 정보 수집 시 관련 법규를 준수하고 사용자 데이터 보호를 위한 조치를 마련한다. 마지막으로, 보안 전문가와 법 집행 기관과 협력하여 다크웹 정보 공유와 공동 대응 방안을 모색한다. 이러한 접근을 통해 다크웹에서의 불법 행위를 효과적으로 감지하고 예방할 수 있다. 또한, deep web 및 기업 내부 자료를 검색하는 기능을 추가하여 사용자에게 필요한 정보를 제공할 수 있도록 한다. 이 과정에서 법적 문제를 고려해야 하며, 해당 자료를 수집하기 위한 윤리적 기준을 명확히 정립해야 한다. 검색 기능은 사용자가 원하는 정보를 쉽게 찾을 수 있도록 직관적으로 설계되어야 하며, 수집된 자료는 관련 법규를 준수하여 안전하게 처리되어야 한다. 이러한 접근을 통해 deep web에서의 정보 검색과 기업 내부 자료의 활용을 효과적으로 지원할 수 있다.

6. 결론

6.1. 결론

본 연구에서는 중소기업의 사이버 보안 취약성을 해결하기 위해 새로운 OSINT 솔루션을 제안하였다. 기존의 OSINT 도구들이 정보 수집에 한정되어 있고 데이터 소스의 다양성이 부족한 반면, 본 솔루션은 SNS, 검색엔진, 도메인, GitHub 등 다양한 모듈을 통해 데이터를 수집하고 분석할 수 있는 기능을 갖추고 있다. 실험 결과, 제안된 솔루션은 기존 도구들보다 데이터의 다양성과 정확성에서 우수한 성능을 보여주었으며, 보안 위협 탐지와 예방에 효과적인 도구로 자리 잡을 수 있음을 입증하였다.

6.2. 기대 효과

제안된 OSINT 솔루션을 활용함으로써 중소기업은 보안 위협을 조기에 탐지할 수 있는 체계를 갖추게 된다. 체계적인 데이터 분석을 통해 잠재적인 사이버 공격을 사전에 발견하고 이에 효과적으로 대응할 수 있는 능력을 향상시킬 수 있다. 또한, 다양한 데이터 소스를 활용하여 보다 포괄적이고 정확한 정보를 수집함으로써 의사결정의 질을 개선할 수 있다. 이로 인해 수집된 데이터를 기반으로 한 인사이트 도출이 가능해져, 기업의 전략적 의사 결정을 보다 효과적으로 지원하게 된다. 더불어, 보안 측면에서 중요한 자산을 보호하고 중소기업의 전체적인 보안 수준을 향상시킬 수 있는 기회를 제공한다. 본 솔루션의 실용화가 이루어질 경우, 중소기

업의 사이버 보안 강화를 넘어 산업 전반의 보안 생태계에도 긍정적인 영향을 미칠 것으로 기대된다.

7. 별첨

7.1. 팀원 소개

이름	GitHub 주소	수행 파트
우제혁	https://github.com/wpgur	SNS 모듈 개발, 웹 서비스 개발
노무승	http://github.com/nms200299	SNS 모듈 개발
송태현	https://github.com/Truebird0109	깃허브, 검색 엔진 모듈 개발
이예준	https://github.com/exit1100/	도메인 모듈 개발
이정호	https://github.com/jjury	레포트 모듈 개발
이종엽	https://github.com/jonggleac	서버 DB 구축

7.2. 소스 코드

https://github.com/exit1100/JOONGSINT-2024

7.3. 시연 영상

https://youtu.be/M8LgUJ6TKaU?si=ewu2QfzQ8_TU8oKN

7.4. 참고 문헌

곽민준, 이희수, 조태웅 (2023) “Industry 4.0 시대 반도체 산업 현장의 산업보안 발전 방향 : 물리보안 통제요소를 중심으로” 한국산업보안연구학회 ,49-72
공배완 (2019) “중소기업 산업기술 보안관리 실태와 보안대책” 한국민간경비학회보
정진영, 황송이 (2023) “디지털 경제안보를 위한 소스코드 유출 방지 방안” 한국산업보안연구,119-141
이완희, 윤민우, 박준석 (2013) “인터넷 시대의 정보활동: OSINT의 이해와 적용 사례 분석” 한국경호비학회
김견한, 이슬기, 김병익, 박순태 (2019) “OSINT기반의 활용 가능한 사이버 위협 인텔리전스 생성을 위한 위협 정보 수집 시스템” 정보보호학회지
박향미, 유지연 (2015)“중소기업 산업보안 강화를 위한 한국과 미국의 관리체계 비교・분석 연구” 한국사회안전학회
김희은, 손태식 , 김두원, 한광석, 성지훈 (2021) “오픈소스 기반 APT 공격 예방 Chrome extension 개발” 아이씨티플랫폼학회
정진영, 황송이 (2023) “디지털 경제안보를 위한 소스코드 유출 방지 방안” 한국산업보안연구학회
강성록, 문미남, 신규용, 이종관 (2023) “공개출처정보를 활용한 사이버위협 평가 요소의 중요도 분석 연구 “ 한국산업보안연구학회
문형진, 취승현, 황윤철 (2016) “빅데이터를 이용한 APT 공격 시도에 대한 효과적인 대응 방안” 중소기업융합학회

7.5. 발표 자료

중부대학교 정보보호학과 졸업작품 홈페이지