과학기술정보통신부 보도자료 다시 대한민국! 새로운 국민의 나라

보도시점 2024. 7. 26.(금) 14:00 (2024. 7. 27.(토) 조간) 배포 2024. 7. 26.(금) 09:00

“진화하는 사이버 위협 대응에 인공지능 활용은 선택이 아닌 필수”

- 「2023년 사이버보안 인공지능 데이터셋 구축 결과 및 우수성과 공유회」 개최
- ’23년 침해사고, 위협 헌팅, 위협 인텔리전스 분야 6억 건 구축
- 구축한 인공지능 데이터셋 실증으로 사이버보안 대응체계 고도화 지원

과학기술정보통신부(장관 이종호, 이하 ‘과기정통부’)와 한국인터넷진흥원(원장 이상중, 이하 ‘KISA’)은, 국내 기업들이 나날이 복잡하고 지능화되는 사이버 공격에 대비해 **인공지능(AI)을 활용**하여 효과적으로 대응할 수 있도록 **‘사이버보안 인공지능 데이터셋 구축 성과 공유회’**를 **7월 26일(금)에 개최**(장소: 로얄파크 컨벤션) 하였다.

※ 사이버보안 인공지능 데이터셋 : AI기술을 활용한 보안제품·서비스 개발을 위해 필요한 정상·공격 데이터(악성코드, IP 등)를 수집·분석·가공(비식별화, 라벨링 등)하여 모아둔 인공지능 학습용 데이터

인공지능·디지털 기술이 나날이 발전과 진화를 거듭할수록 사이버 공격도 또한 일상화, 대규모화되고 있는 동시에, 기존 보안기술을 우회하고 무력화시키는 **신·변종 위협도 지속 증가**하고 있다. 국내 보안기업들은 사이버위협에 효과적으로 대응하기 위해 **인공지능 기술을 보안에 도입**하려고 노력하고 있으나, **양질의 인공지능 학습용 데이터 부족 등으로 어려움**을 겪어왔다.

이에 과기정통부와 한국인터넷진흥원은, 인공지능 **기술을 활용한 보안제품·서비스 개발에 필요한 데이터셋*을** ’21년부터 구축하고, 이를 **기업 및 기관에서 실증·활용할 수 있도록 지원**하여 인공지능 기술 적용을 촉진하고, 사이버 침해사고 대응에 지능화 역량을 강화할 수 있도록 힘쓰고 있다.

* (21년) 악성코드, 침해사고 2개 분야, 8억건 구축
(22년) 애플리케이션보안, 능동형 보안관제, 위협 프로파일링 3개 분야, 6억건 구축
(23년) 최신 침해사고, 위협 인텔리전스, 위협 헌팅 3개 분야, 6억건 구축

’23년도에는 △**최신 침해사고, △위협 헌팅*, △위협 인텔리전스**** 3개 분야에 **6억 건의 인공지능 데이터셋을 구축**했으며, 이를 바탕으로 공공, 금융, 보안 등 40개 수요 기업·기관에 **구축한 데이터셋을 활용·실증**함으로써, **기업들의 금품 요구 악성 프로그램(랜섬웨어) 등 공격행위 탐지력 향상, 분석 정확도 제고 등에 개선 효과**가 나타났다.

* 미래 발생가능한 잠재적 공격(위협)에 선제적 대응 가능한 탐지 툴(패턴) 데이터셋

** 현존하거나 향후 발생할 수 있는 공격의도, 목적, 기법 등의 분석, 대응 등을 위한 데이터셋

< ’23년 주요실증 및 개선효과 사례 >

○ **(광주광역시청)** 랜섬웨어 감염 예방을 위해 직원 PC 보안 솔루션에 AI 데이터셋을 적용하여 지방자체단체 중 최초로 인공지능기반 보안체계 도입

- 24종의 금품요구 악성 프로그램(랜섬웨어) 대응 모의훈련 결과, 24종 모두 정탐하여 기존 대비 탐지성능 40% 향상

○ **(여기어때)** 웹페이지 모니터링을 통해 수집되는 보안 이벤트(이상 사용자 등)를 탐지하고, 정오탐 분류를 자동화하기 위한 웹로그 분석 인공지능 모델 지원

- 실증기간(약 2개월) 중 웹방화벽에서 탐지된 약 52만 건의 공격 이벤트의 정오탐 분류를 자동화하고(정탐률 99.85%) 분석시간 단축(10→1분)

○ **(한국전력공사)** 공급망 타깃 공격 적시 대응 등을 위해 상시 위협 분석이 가능하도록 네트워크 기반 인공지능 모델 지원

- 실증기간(약 2개월) 중 수집된 약 2천만 건의 트래픽과 약 8만 건의 파일을 대상으로 보안에 취약한 프로토콜, 파일 위험성 식별 등 사내 정보기술 인프라의 위험성을 진단하여 보안정책에 반영

이번 **성과공유회**는 사이버보안 분야 인공지능 데이터 활용, 관련 기술개발 등에 관심이 있는 기업·기관들에게 **데이터셋 구축 결과·우수사례 등을 공유**하고, **활용방안 등을 모색**하고자 마련된 자리로, 인공지능 **시대의 사이버보안 기술 및 위협에 대한 전문가 강연**(부산대 김호원 교수, 코난테크놀로지 임완택 상무), **인공지능 데이터셋 활용사례 발표**(광주광역시, 여기어때 등) 등으로 진행되었다.

과기정통부 정창림 정보보호네트워크정책관은 “**민간에서 획득이 어려운 양질의 사이버보안 인공지능 데이터셋을 정부가 지원하여 구축**하고, 이에 **민간의 창의력과 기술력을 결합한 실증·활용**으로, 우리 보안산업 발전에 **큰 동반상승 효과**가 생길 것으로 기대”된다며,

“과기정통부는 앞으로도 사이버보안 인공지능 데이터셋을 지속적으로 구축·고도화하여 국내 사이버보안 시장 경쟁력을 강화하고 **우리 기업들이 세계 인공지능 보안 기술을 선도할 있도록 적극 지원**하겠다.”고 밝혔다.

담당 부서	정보보호네트워크정책관 사이버침해대응과	책임자	과장	최광기	(044-202-6460)
		담당자	사무관	한지용	(044-202-6463)
			주무관	김지환	(044-202-6469)
관련 기관	한국인터넷진흥원 AI위협데이터대응팀	책임자	팀장	이규생	(02-405-5438)
		담당자	책임	김주혁	(02-405-5305)

붙임1 **성과공유회 안내문**

주최 과학기술정보통신부 Ministry of Science and ICT

주관 KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY

2024 사이버보안 AI 데이터셋 우수 활용 성과공유회

2023년도 구축 ▲최신 침해사고 ▲위협 인텔리전스 ▲위협 헌팅 분야

2024. 7. 26(금)
13:30~17:30

용산 로얄파크 컨벤션 3층 로얄홀

사전등록

참여 혜택
- 사전등록 후 행사 참여 시 소정의 기념품 증정

주요 내용
- AI 기술 동향 및 AI 시대의 사이버 위협 대응 전략 발표
- 2023년 사이버보안 AI 데이터셋 구축 결과 및 우수 활용사례 공유
- 2023년 사이버보안 AI 데이터셋 우수 활용 사례집 배포 및 2024년 실증 참여 상담 부스 운영

프로그램

시간	주요내용	발표자
13:30~13:40	개회 및 참석자 소개	이규생 팀장(KISA)
13:40~13:45	인사말씀	과학기술정보통신부
13:45~13:50	환영사	한국인터넷진흥원
세션 I	초청발표: AI 기술 동향 및 AI 시대의 사이버 위협 대응 전략	
13:50~14:10	생성형 AI 기반의 취약성 탐지 및 대응 기술 사례 소개	김호원 교수(부산대학교)
14:10~14:30	생성형 AI(LLM)의 개요, 개발 방향 그리고 RAG	임완택 상무(코난테크놀로지)
14:30~14:50	휴식 (Coffee Break)	
세션 II	AI 데이터셋 구축 및 활용 사례	
14:50~15:10	사이버보안 AI데이터셋 구축 사업 추진전략 및 23년 결과 공유	최보민 선임(KISA)
15:10~15:30	AI를 활용한 랜섬웨어 탐지 및 대응 사례	임동우 주무관(광주광역시)
15:30~15:50	능동형 사이버 침해예방 체계 전환을 위한 AI 데이터셋 활용 보안관제 운영 사례	윤진환 CISO(여기어때컴퍼니)
15:50~16:10	휴식 (Coffee Break)	
16:10~16:30	AI 기반 인텔리전스 보고서 TTP 자동 추출 기술	최창희 선임(국방과학연구소)
16:30~16:50	지능형 보안관제 체계 구축을 위한 AI 모델 구현	양봉열 대표(로그프레소)
16:50~17:10	위협 인텔리전스 데이터셋 구축 및 LLM 기반 위협 대응 자동화	김기홍 대표(샌즈랩)
17:10~17:30	Q&A 및 폐회	

문의처 02-405-5305, 5206 aidata@kisa.or.kr

붙임2 사이버보안 AI 데이터셋 구축 현황

연도	분야	주요 내용
2021	악성코드 분야	• **[정의]** KrCert 및 국내외 보안장비에서 수집한 다양한 유형의 악성·정상파일을 분석 및 가공하여 AI데이터로 구축 • **[활용]** AI기반 백신(Anti-virus) 및 악성코드 분석 서비스에 활용
	침해사고 분야	• **[정의]** 최신 해킹 사건을 재현을 통해 각종 보안장비에서 발생한 보안 로그를 수집 및 가공하여 AI데이터로 구축 • **[정의]** 방화벽 및 침입 탐지 시스템(IDS/IPS) 등 솔루션 개발 및 AI를 기반 네트워크 이상 시나리오 분석 등에 활용
2022	애플리케이션 보안 분야	• **[정의]** 취약한 애플리케이션의 프로그램을 개발하는 소스코드를 수집 및 가공하여 AI데이터 형태로 구축 • **[활용]** AI기반 소스코드 취약점 진단 도구개발 등에 활용
	능동형 보안관제 분야	• **[정의]** APT 공격기법을 재현하여 각종 보안관제 장비에서 발생하는 인증우회, 비인가 접속시도 등 보안이벤트를 수집 및 가공하여 AI데이터로 구축 • **[활용]** EDR, SOAR 등 AI기반 APT 보안 제품개발 및 기업 IT인프라로 유입되는 공격행위 탐지, 위험도 산정 등에 활용
	위협 프로파일링 분야	• **[정의]** 킴수키, 라자루스, APT29 등 조직화된 공격그룹과 연관된 위협정보(File, IP/URL, 도메인 등)를 수집 및 가공하여 AI데이터로 구축 • **[활용]** AI를 이용하여 유사·연관 공격 분류 및 공격그룹 식별 등에 활용
2023	최신 침해사고 분야	• **[정의]** '21년도 구축된 악성코드 및 침해사고 데이터를 신규 위협 데이터를 활용하여 업데이트 및 최신화
	위협 인텔리전스 분야	• **[정의]** 특정 산업, 국가 및 사회 이슈(국가분쟁, 재난 등)를 타깃 삼는 공격과 연관된 위협정보(File, IP/URL, 도메인)를 수집 및 가공하여 AI데이터로 구축 • **[활용]** XAI(설명가능한 AI) 기술과 접목하여 공격 의도, 목적 등에 대한 해석을 자동으로 생성해주거나, 유사 공격의 예측/예방 기술 개발에 활용
	위협 헌팅 분야	• **[정의]** 최신 공격(악성코드, 보안이벤트)에 대한 탐지 패턴을 수집 및 가공하여 AI데이터 형태로 구축 • **[활용]** AI를 활용해 알려지지 않은 신·변종 위협에 대해 실시간 탐지룰/패턴을 자동으로 제작해주는 기술 개발에 활용