K-사이버 시큐리티 챌린지

2020. 07. 17.

이 새 움 선임연구원

한국인터넷진흥원

Contents

I. 배경 – 사이버보안 대응환경 변화

사회 전반의 ICT 융합 가속화

※ 스마트시티 · 자동차 · 의료 · 공장 · 농장 등 전통산업과 ICT 융합으로 다양한 서비스 등장

신규기기(IoT) 연결로 보안위협 대상의 폭증 및 복잡

※ 인터넷에 연결되는 기기가 기하급수로 증가

사이버보안을 위한 전통적 대응방식은 한계에 도달

※ 유사/변종 악성코드 급증 등으로 기존 시그니처(탐지규칙) 기반 탐지로는 대응불가

KISA

I. 배경 – 사이버보안 대응환경 변화

하루에 발생한 침해사고(2017)

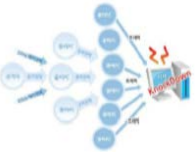
악성코드 활동 : 23,883건
(안랩 탐지 8,717,194건)

랜섬웨어 피해 : 16건
(KISA 피해상담 5,825건)

홈페이지 변조 : 5건
(KISA 탐지 1,724건)

홈페이지 악성코드 유포 : 37건
(KISA 탐지 · 조치 13,347건)

신규 취약점 : 4.32건
(KISA 탐지 · 신고 · 분석 1,577건)



DDoS 공격 : 1.25건
(KISA 탐지 · 신고 551건)

피싱 · 파밍 사이트 : 35건
(KISA 탐지 · 조치 12,683건)

스미싱 메시지 : 1,376건
(KISA 탐지 · 조치 502,027건)

I. 배경 – 사이버보안 대응환경 변화

AI 혁명 : 알파고 vs. 이세돌(1/2)

※ 출처 : 바둑TV

I. 배경 – 사이버보안 대응환경 변화

AI 혁명 : 알파고 vs. 이세돌(2/2)

알파고 시리즈의 성능 비교 자료: 네이처

엘로(ELO)는 바둑 실력을 수치화한 점수로 클수록 고수. GPU와 TPU는 각각 그래픽 연산 전용 프로세서와 인공지능용 칩을 말함.

이름	공개 시점	전적	엘로(ELO)	학습법	하드웨어
알파고 판	2015년 10월	판후이 2단에게 5-0 승리	3144	딥러닝, 강화학습	GPU 176개, TPU 4개
알파고 리	2016년 3월	이세돌 9단에게 4-1 승리	3739	딥러닝, 강화학습	GPU 176개, TPU 4개
알파고 마스터	2017년 5월	커제 9단에게 3-0 승리	4858	딥러닝, 강화학습	TPU 4개
알파고 제로	2017년 10월	알파고 리에 100-0, 알파고 마스터에 89-11 승리	5185	강화학습	TPU 4개

※ 출처 : 동아일보

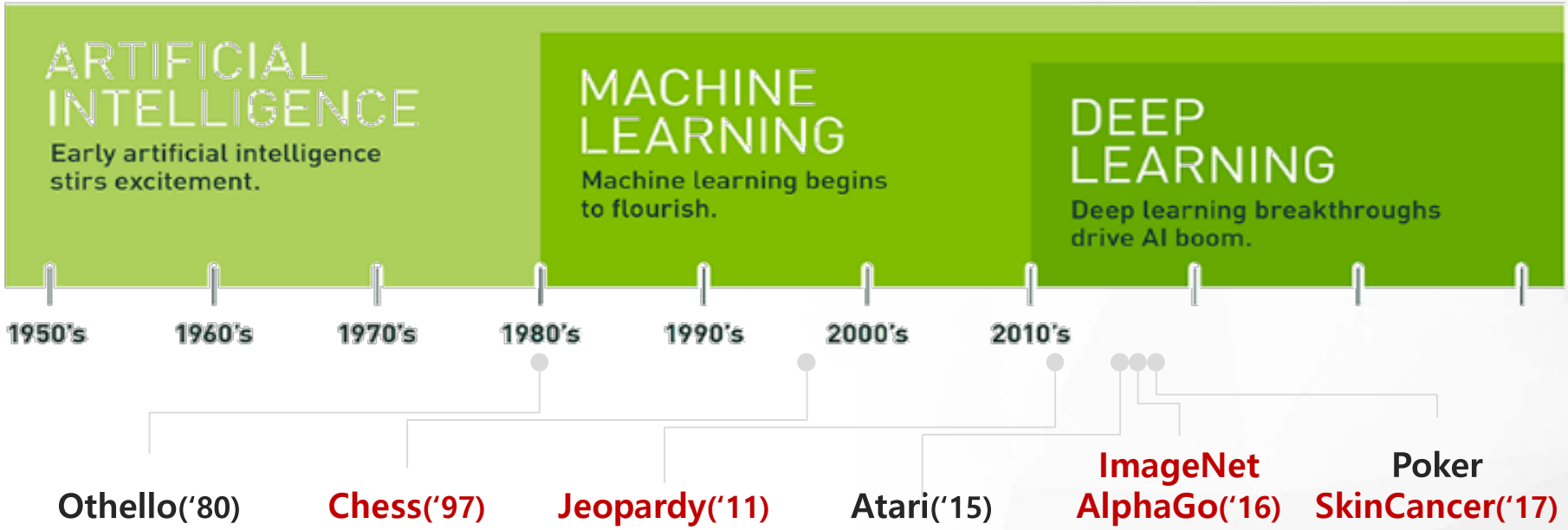
I. 배경 – 사이버보안 대응환경 변화

AI 발자취(1/2)

정의: **인간 지능**의 본질을 규명하고, 이를 **인공적으로 재현**하려는 기술

인지 · 학습 · 추론 · 행동

※ 스스로 지능을 발전시키는 **학습단계(강화학습) 수준**이며, 새로운 상황을 추론하고 행동하는 단계로 발전中



※ 이미지 출처 : https://www.nvidia.com

I. 배경 – 사이버보안 대응환경 변화

AI 발자취 : 전문분야 인공지능 활용사례 (2/2)

※ 출처 : 위키트리

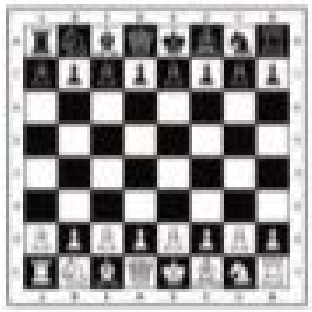
※ 출처 : 한계레

I. 배경 – 사이버보안 대응환경 변화

AI 능력 및 현황

- Artificial Narrow Intelligence (ANI, Weak AI) : 인간의 지능을 모방하여 특정한 문제를 해결
- Artificial General Intelligence (AGI, Strong AI) : 인간처럼 생각(사고·감정·창의)하여 문제를 해결
- Artificial Super Intelligence (ASI, Super AI) : 인간을 초월한 지능 보유

현재



ANI: Chess Program

2040년

AGI: Human Level Intelligence

2060~70년

ASI: Superintelligence

※ 출처 : Superintelligence: Paths, Dangers, Strategies (2014)

I. 배경 – 사이버보안 대응환경 변화

AI 활용분야

개인 맞춤형 상품 추천 서비스

자율주행자동차

금융·법률·의료 및 사이버보안 등
최신 정보 파악·조언

자동 통·번역 서비스

공장에서 제조공정 통합관리

인공지능 전투로봇

산불·지진·홍수 및 사이버 침해사고 등
재해·사고 예측 서비스

에너지 효율을 높인 스마트 빌딩

I. 배경 – AI 기반 사이버보안 개선분야

AI 활용으로 **새로운 공격에 대응**하고, **단순반복 및 수작업 대체**

인텔리전스

보안위협 **정보 급증 및 복잡**

각종 보안위협
분석 및 연계를 통해
의사결정 지원

대응시간

사람에 의한 **수동 분석 및 대응**
(수주~수개월 소요)

침해사고 **대응시간 단축**

정확도

제로데이 취약점 및 변종 확산
및
규칙(시그너처) 기반 탐지 한계

이상징후·공격시도 등
탐지 정확도 향상

I. 배경 – AI 기반 사이버보안 개선분야

AI 기반 사이버보안 전망

23%

plan to invest in cyber AI

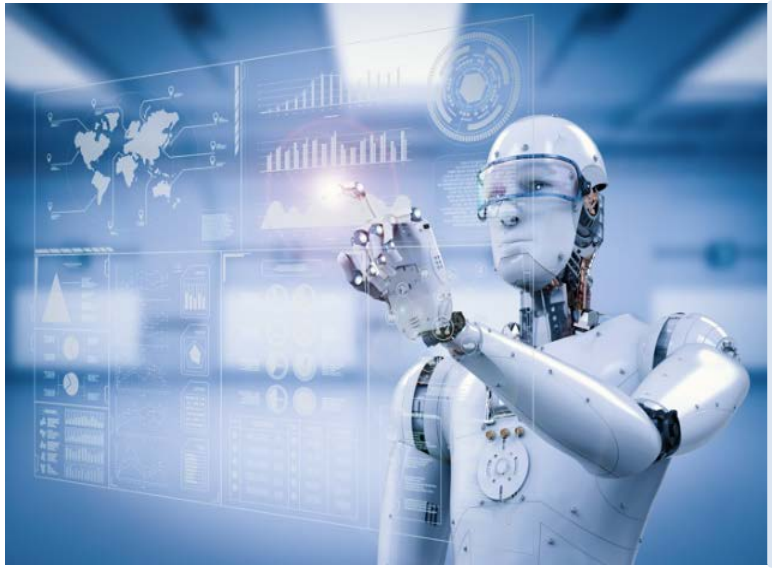
85%

of all cyber attacks predicted by using AI

36.1%

is the expected yearly market growth between 2016 and 2024 for AI

※ 출처 : Global Opportunity Report 2017



- 非정상 · 악성 행위 탐지 및 공격 저지
- 제로데이 취약점 제거
- 사람의 분석 능력 및 결과 보강
- 보안 반복작업 자동화

I. 배경 – R&D 데이터 공유 필요성

- 우수한 정보보호 기술 연구·검증 등을 위해서는 **양질의 데이터 확보가 필수**
- 특히 AI시대, **기계 학습에 필요한 데이터**가 인공지능 기술의 **품질**을 좌우

"인공지능 경쟁력 핵심은 양질의 데이터 확보"

아이뉴스24

본문듣기 | 설정

기사입력 2016-03-20 13:33 기사원문

5 4

지능정보기술과 산업 활성화를 위한 방안으로 양질의 데이터 확보 필요

<아이뉴스24>

[김국배기자] 산학연 전문가들은 인공지능 등 지능정보기술과 산업 활성화를 위한 방안으로 양질의 데이터 확보를 꼽았다.

미래창조과학부와 정보통신기술진흥센터는 지난 18일 오후 경기도 성남시 분당구 네이버 그린팩토리에서 '지능정보산업 발전전략 추진을 위한 후속조치'를 주제로 '제7차 ICT정책 해우소'를 열었다.

해우소에는 삼성전자와 LG전자, SK텔레콤, KT, 네이버 등의 기업들과 관련 연구소, 학계 전문가들이 참석했다.

◇ 미래창조과학부는 지난 18일 '지능정보산업 육성을 위한 전략'을 주제로 제7차 ICT 정책해우소를 개최했다. [사진=미래부]

"인공지능, 선택 아닌 필수…'빅데이터' 중요"

"기술 개발보다 활용에 초점 맞춰야…인재 양성 시급"

[뉴스토마토 박진아기자] 이세돌 9단과 구글 알파고의 바둑 대결로 인공지능에 대한 관심이 급증한 가운데, 인공지능 관련 전문가들이 "인공지능은 기업의 선택이 아닌 필수"라고 강조하며 "빅데이터 확보가 중요하다"고 입을 모았다.

빅데이터 중요

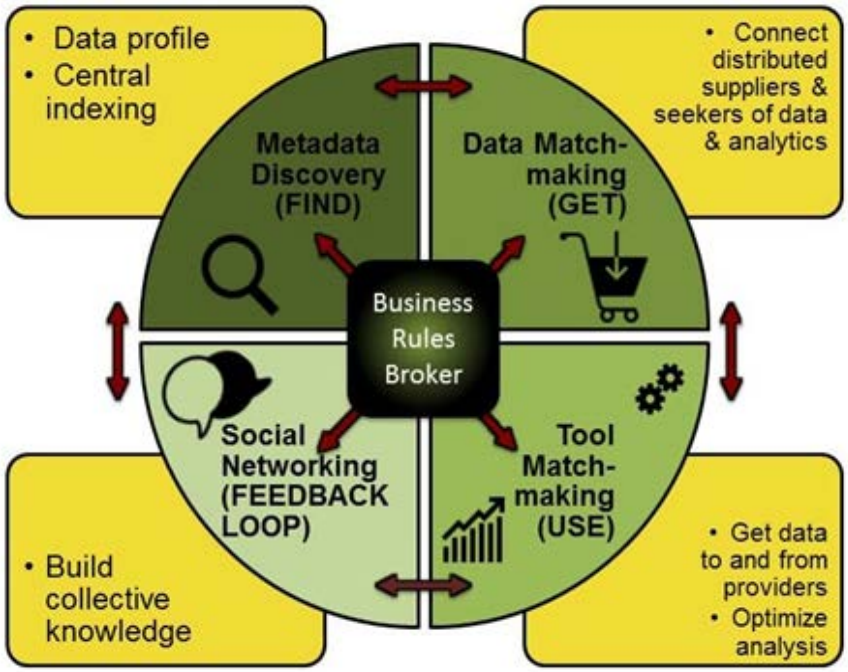
대한상공회의소가 24일 서울 세종대로 대한상의회관에서 '인공지능 기술 트렌드와 기업 활용전략' 주제로 개최한 경영아카데미에서 최승진 포스텍 컴퓨터공학과 교수가 '머신러닝과 딥러닝: 인공지능을 위한 궁극적인 방법인가?'라는 주제 발표를 하고 있다. 사진/대한상의

대한상공회의소가 24일 서울 세종대로 상의회관에서 개최한 '인공지능 기술 트렌드와 기업 활용전략' 경영아카데미에서 최승진 포스텍 컴퓨터공학과 교수는 "인공지능이 학문적 연구대상에서 산업의 도구적 가치로 이동하고 있다"며 "인공지능을 모르는 기업은 이를 선택한 기업을 절대로 따라잡을 수 없을 것"이라고 말했다.

최 교수는 '머신러닝과 딥러닝: 인공지능을 위한 궁극적인 방법인가'라는 주제 발표를 통해 "인공지능 중에서 '머신러닝(machine learning)'은 고객서비스 개선과 더불어 단순 반복적인 업무를 대체할 수 있다는 점에서 가치가 있다"며 "미국 IT산업의 요충지인 실리콘밸리 뿐 아니라 전세계 IT기업들이 관심을 기울이는 이유"라고 말했다. 머신러닝은 인공지능의 연구 분야 중 하나로 컴퓨터가 스스로 각종 데이터를 수집하고 학습하는 기술을 뜻한다. 기존의 인공지능은 사람이 갖고 있는 지식을 빠른 시간내 프로그래밍을 통해 그대로 입력시키는 반면, 머신러닝은 컴퓨터 스스로 활발히 더 적은 프로그래밍을 통해 스스로 일을 한다.

II. 동향 – 데이터 공유 사례 – IMPACT (1/2)

- **미 국토안보부(DHS) 지원으로 사이버 보안 연구에 필요한 데이터(1페타 이상) 공유**
  ※ 국토안부부(DHS) 내 과학기술국(S&T), 사이버보안부서(CSD)에서 운영
- **데이터 검색, 데이터&분석 도구 매칭, 데이터 공유, 소셜 서비스 제공**



기능	설 명
메타데이터검색	정보 제공자와 사용자가 인터페이스와 엔진을 사용하여 메타데이터 검색
데이터&도구 매칭	사용자와 데이터를 중앙 인터페이스를 이용하여 연결시키고 관련 도구 매칭
데이터 공유	해당 데이터의 정책 및 절차를 검토하여 정상적인 데이터 접근 권한을 가진 연구원과 공유
소셜 네트워크 (Feedback)	정보 제공자-사용자-연구원 등 사용자 간의 피드백을 통해 데이터, 도구, 분석 모델에 대한 정보를 최적화

[IMPACT(The Information Marketplace for Policy and Analysis of Cyber-risk & Trust) 구성도]

II. 동향 – 데이터 공유 사례 – IMPACT (1/2)

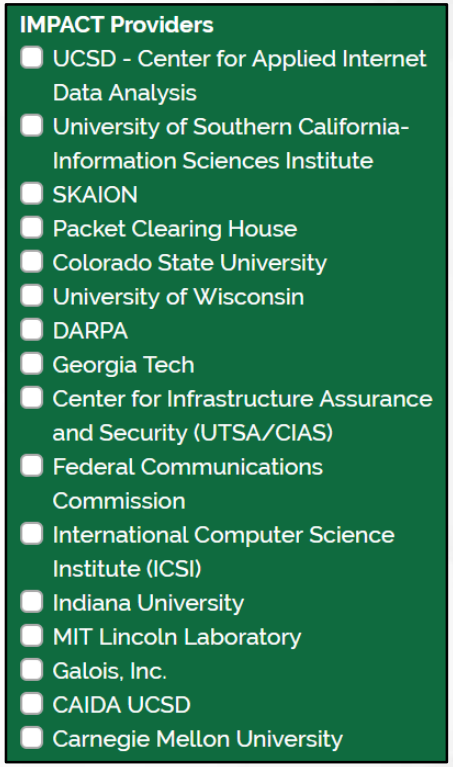
- 악성 트래픽, BGP 트래픽 등 네트워크 관련 데이터와 분석 도구를 주로 공유
- 미 학계·산업계·비영리단체·정부기관과 7개 국가가 참여하여 데이터셋 구축

※ DHS가 인정한 호주, 캐나다, 이스라엘, 일본, 네델란드, 싱가로프, 영국에서만 데이터 공유·이용 가능

[IMPACT 데이터셋 종류]

구분	설명
New Insider Threat Data	Lincoln 연구실(MIT)에서 내부자 위협에 대한 12가지 시뮬레이션을 진행한 데이터셋
Wisconsin's Web Cookies Data	상위 100,000개의웹 사이트(2013. 11~ 2015. 04, Alexa)에서 수집된 웹 쿠키 데이터 세트
Merit's Network Scanners from Darknet	DarkNet 스캐닝을 통해 관찰된 IP주소, 패킷의 수에 대한 데이터 셋 매일 업데이트되며 네트워크 구성 오류 등 다른 유형의 정보도 포함
An Empirical Study of Web Cookies	상위 100,000개의 웹 사이트(Alexa)에서 약 320만 개 이상 수집된 쿠키 데이터 세트 제공
Dataset Spotlight: Certificates Data	상위 1,000,000개 사이트(Alexa), 피싱 사이트(PhishTank), 은행 웹사이트의 인증서 필드의 데이터 세트 제공

[최근 공유된 데이터셋]



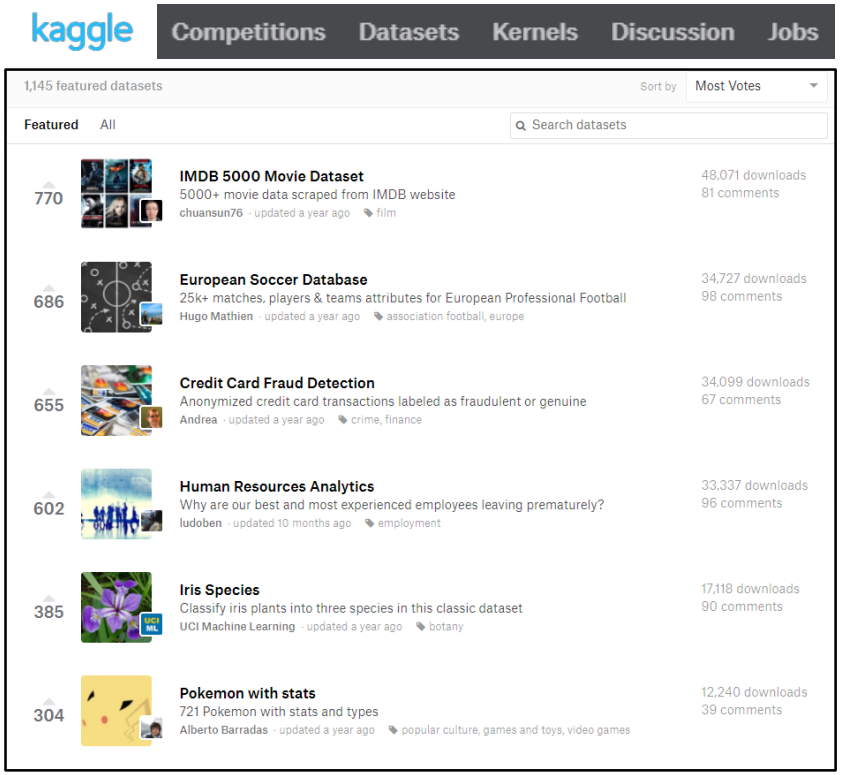
[주요 데이터셋 제공자]

II. 동향 – 데이터 공유 사례 – Kaggle

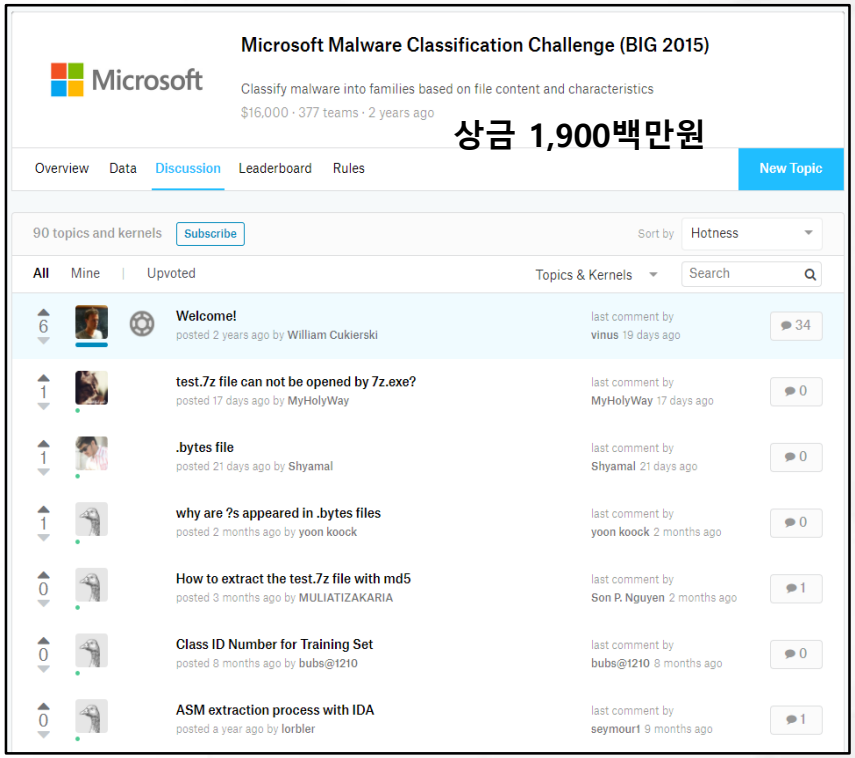
- 구글이 운영('17년 3월 인수)하는 개방형 데이터 공유 및 문제해결 대회 플랫폼

  ※ 누구나 현실의 문제와 데이터를 제공하고, AI 알고리즘 등을 활용한 문제 해결 우승자를 포상

- MS사가 500G(10,868개) 악성코드 샘플을 공유하고, 기계학습 알고리즘을 활용해 악성코드를 9개 그룹으로 분류하는 대회(malware classification challenge) 개최('15)



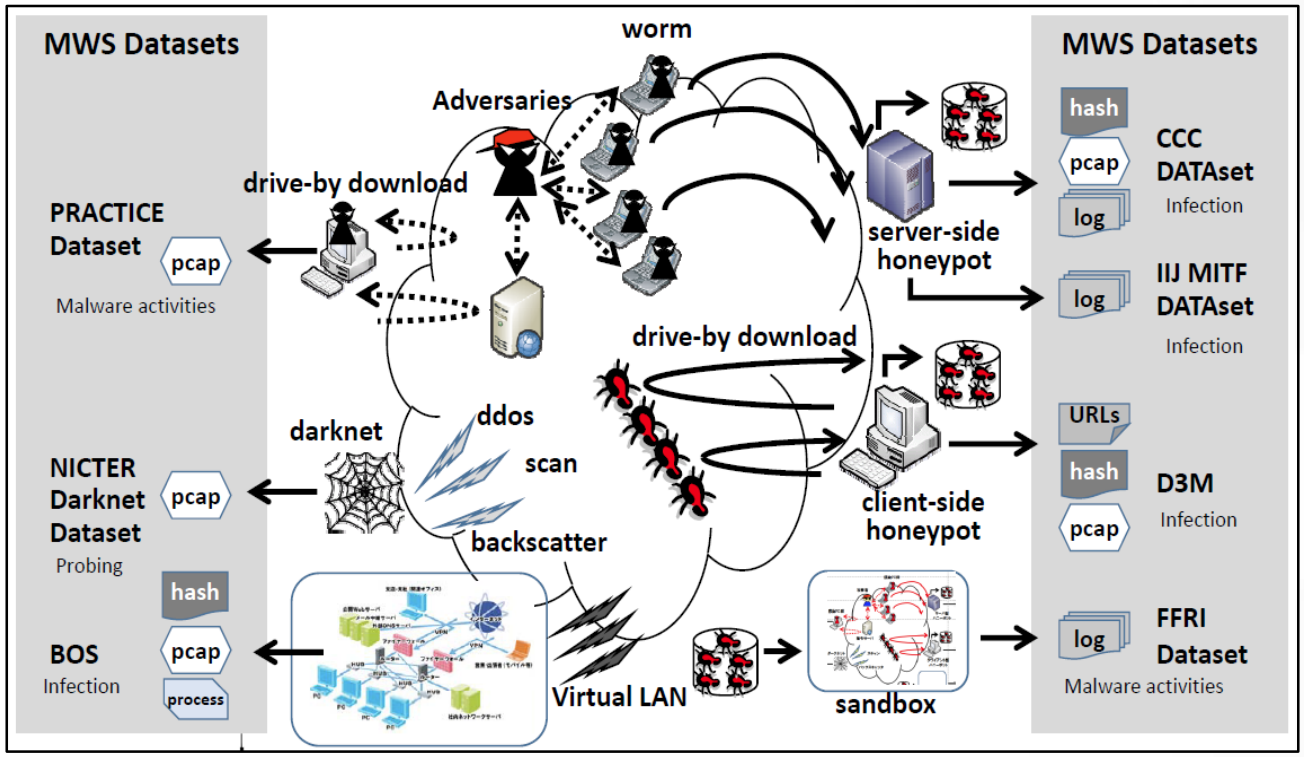
[Kaggle Top5 데이터셋]



[MS사 Malware Classification Challenge]

II. 동향 – 데이터 공유 사례 – MWS

- 일 기관 등이 보유한 악성코드 데이터를 공유해 분석결과 등을 경쟁하는 대회('08~)
  ※ JPCERT/CC, IPA, AIST, NICT 등과 일본 컴퓨터보안학회가 공동으로 대회 개최
- 악성코드 유포부터 감염, 확산(네트워크 트래픽 등)및 분석결과 등의 데이터로 구성



MWS Dataset

	2008	2009	2010	2011	2012	2013	2014
CCC DATAset [server-side honeypot]	☑	☑	☑	☑	☑	☑	
MARS for MWS [malware dynamic analysis]	☑	☑	☑				
D3M [client-side honeypot]			☑	☑	☑	☑	☑
IIJ MITF DATAset [server-side honeypot]					☑		
PRACTICE Dataset [malware behavior analysis]						☑	
FFRI Dataset [malware sandbox analysis]						☑	☑
NICTER Darknet Dataset [darknet monitoring system]						☑	☑
Behavior Observable System (BOS) [observing threat actors]							☑

'08년 Server Honeypot 데이터 공유
'10년 Client Honeypot 데이터 추가
'13년 악성코드 행위 분석 결과 추가
'13년 다크넷 모니터링 데이터 추가

[MWS(anti-Malware engineering WorkShop) 데이터셋 구성]

II. 동향 – 데이터 공유 사례 – 삼성

- 우수 AI 분야 아이디어와 데이터 분석 능력을 겨루는 삼성 AI 챌린지 개최('18)

  ※ AI 해커톤과 데이터 챌린지 2개 트랙으로 구성

- 과거 교통사고 데이터셋 분석을 통해 미래 교통사고 예측 데이터 챌린지

II. 동향 – 데이터 공유 사례 – IITP

- AI 기술을 활용해 사회문제를 해결하기 위한 AI R&D 챌린지 개최('17~)

※ 대회 입상 시 상금(총 6백만원)이 지급되고, 입상팀이 후속 연구를 진행할 수 있도록 R&D 사업 지원(총12억)

- '17년 가짜 뉴스 찾기, '18년 합성 사진 찾기를 위한 데이터 배포 및 우수 기술 경쟁

샘플 데이터셋의 규모 : 총 1,200개 이미지

- 세부 임무별 문제범위 내 출제 경향을 파악할 수 있도록 샘플데이터 제공(4월 20일(금) 제공 예정)
  - 임무① : 총 400개 (생성 이미지 200개, 정상 이미지 200개)
  - 임무② : 총 800개 (합성 이미지 300개, 정상 이미지 500개)
- 제공된 샘플 데이터셋의 생성/합성 이미지의 범위가 본선대회의 생성/합성 이미지 전체를 의미하는 것은 아니며, 공고문의 문제 범위내에서 다양한 방법으로 생성/합성된 이미지를 대상으로 본선대회 진행 예정
- 샘플 데이터셋은 총괄책임자 이메일로 배포 예정

인공지능 기술을 활용한 '합성사진 찾기'

- 참가자(팀)은 '다른 사람이 거짓된 사실을 믿도록 하기 위해 만들어진 사진'으로, 명의 도용, 명예 훼손, 사실 왜곡 등 각종 사회적 혼란을 초래하는 것을 방지할 수 있는 기초 및 요소기술 개발을 통한 해결방안 제시

출처 : 2018년도 AI 챌린지 1차 워크숍 발표자료

II. 동향 – 국외 챌린지

DARPA

챌린지명	연도	분야	주요 특징
그랜드 챌린지 (Grand Challenge)	'04~'05	자율 주행차	• (목표) 사막에서 운행 가능한 자율주행차를 개발하여 10시간 이내에 목표지점 도달 • (상금) 목표달성 시 1등 200만 달러 지급
어번 챌린지 (Urban Challenger)	'07	자율 주행차	• (목표) 도시에서 운행 가능한 자율주행차를 개발하여 6시간 이내에 목표지점 도달 • (상금) 1등 200만 달러, 2등 100만 달러, 3등 50만 달러
로보틱스 챌린지 (Robotics Challenge)	'12~'15	로봇	• (목표) 재난구조를 위한 휴머노이드 로봇개발 • (상금) 1등 200만 달러, 2등 100만 달러, 3등 50만 달러
사이버 그랜드 챌린지 (Cyber Grand Challenge)	'16	사이버 보안	• (목표) 인공지능(AI)을 활용한 사이버 해킹·보안 기술개발 • (상금) 1등 200만 달러, 2등 100만 달러, 3등 75만 달러
주파수 협력 챌린지 (Spectrum Collaborative Challenge)	'16~'19	무선 주파수	• (목표) 무선 주파수의 효과적인 활용을 위한 기술개발 • (상금) 1등 200만 달러, 2등 100만 달러, 3등 75만 달러

※ 챌린지에 따라 트랙 수, 이름, 트랙별 지원방안이 다르며, DARPA의 당해연도 예산 편성에 따라 예산지원 트랙의 지원하는 팀 수와 금액을 결정

II. 동향 – 국외 챌린지

- 사이버 그랜드 챌린지(CGC) 운영사례 분석
- 예산을 지원받는 “Funded Track”과 예산 지원을 받지 않는 “Open Track”으로 추진

Funded Track

- 챌린지와 관련된 기술개발 지원사업을 기획·공고하고, 복수의 수행기관들을 선정해 예산 지원
- 프로젝트는 보통 2~3 단계로 지원
- 단계별 종료 후에는 Preliminary Event와 같은 단계평가를 거쳐 일정 기준을 충족하는 경우만 차기 단계를 지원

Open Track

- DARPA의 예산지원 없이 연구자들이 스스로 기술개발을 추진해 참가하는 트랙
- 예선이나 결선경기에 참가하기 위해서는 DARPA가 정해놓은 일정 기술수준을 충족해야 함
- DARPA 개최 행사에 기술 시연을 하거나 챌린지에 따라 동영상을 찍어 제공함

II. 동향 – 국외 챌린지

구글 – Kaggle

- 2010년 시작된 최대 규모의 데이터 과학자, 머신러닝 연구자 오픈 커뮤니티 플랫폼
- 1만개 이상의 기업이 서비스를 이용 중이며, 약 100만 명의 데이터 과학자와 머신러닝 연구자가 활동

- **기업·단체에서 데이터와 해결과제를 등록하고, 많은 연구자들이 문제해결 솔루션을 개발하고 경쟁**
- **캐글은 참여자의 실시간 순위표 공개, 정보 공유를 통해 경쟁심리를 자극하는 동시에 경쟁 팀 간의 협력도 유도**
  - ⇒ 팀 간에 알고리즘을 비교할 기회를 제공하여 경쟁자 간 발생하는 잘못된 결과로의 쏠림, 각 팀의 한계, 실패 문제 등을 해소
- **경진대회는 참여자들이 실력을 발휘하고, 기업들은 우수한 참여자들을 스카웃하는 창구로도 활용**

II. 동향 – 국내

정보통신기획평가원(IITP) - 인공지능(AI) R&D 그랜드 챌린지

- 인공지능(AI) SW(알고리즘, 데이터)와 HW(드론, 로봇 등) 융합을 통한 AI 원천기술 고도화 및 재난·안전 등 사회문제 해결형 경진대회
- 사회적 현안에 대한 공모를 통해 AI를 활용한 해결과제 제시

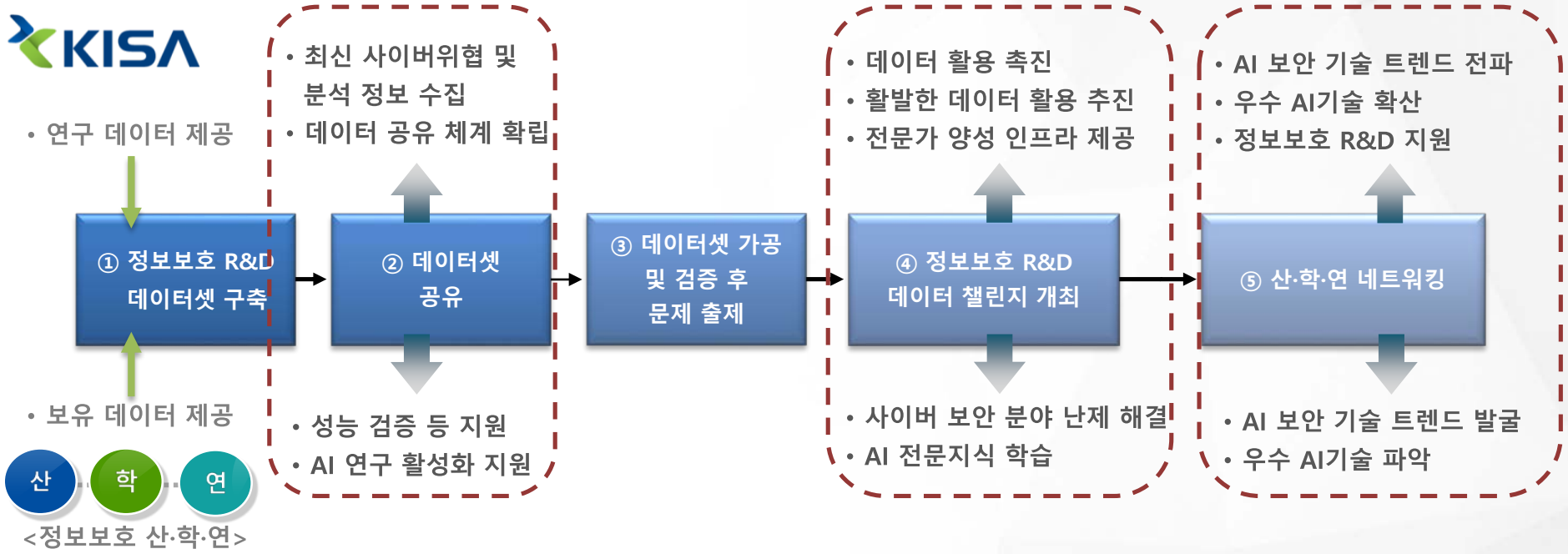
- '18년 가짜뉴스 찾기 : 최근 SNS 등의 발달로 "속이는 것을 목적으로 만들어진 이야기"인 가짜뉴스가 전 세계적인 문제로 부상됨에 따라, 이를 퇴치하기 위한 챌린지 추진
- '18년 합성사진 판별 : 악의적 비방을 목적으로 특정 인물의 합성 사진을 제작하여 배표하는 사회문제를 해결하기 위한 챌린지 추진

'19년 : "인공지능과 로보틱스를 활용하여 복합 재난상황에서 골든타임 내에 신속하게 인명을 구조하라"를 주제로 진행

⇒ '19년부터 '22년까지 4개년에 걸쳐 총4단계로 진행
(트랙별 시나리오) 1단계[테스트베드(실내)환경] → 2단계[테스트베드(실내)환경]
→ (통합시나리오) 3단계[테스트베드(실외)환경] → 4단계[테스트베드(실외)환경]

III. K-사이버 시큐리티 챌린지 - 프로세스

- 정보보호 산·학·연이 공유한 연구 데이터를 통해 **최신 사이버 위협 동향 파악**
- **사이버 보안 AI 기술 트렌드 분석** 및 사이버 보안 업무에 활용 가능한 **AI 기술 전파**
  산업계 및 지역 대학 등에 **사이버 보안 AI 적용·연구 지원(컨설팅)**
- 정보보호 산·학·연이 쉽게 구할 수 없는 연구 데이터 공유를 통해 **AI 연구 활성화 지원**



III. K-사이버 시큐리티 챌린지 - 데이터셋

국내 정보보호 R&D 데이터셋 공유 웹 페이지 구축('17~)

※ 정보보호산업진흥포털 內 공유 페이지 생성 및 공유 신청자를 대상으로 오프라인 데이터셋 공유

R&D 데이터셋 목록

데이터셋 그룹	데이터셋	제공자	소개
악성코드 데이터셋	PC악성코드	한국인터넷진흥원 세인트시큐리티	악성코드 변종탐지, 그룹분류 기술
	지능형 악성코드	안랩, 하우리, 세인트시큐리티	2017 정보보호 R&D 데이터 챌린지 대회의 지능형 악성코드
	대용량 정상, 악성파일 1 (2017 예선)	한국인터넷진흥원, 하우리, 세인트시큐리티	2017 정보보호 R&D 데이터 챌린지 대회의 대용량 정상, 악성파일
	대용량 정상, 악성파일 2 (2017 본선)	한국인터넷진흥원, 하우리, 세인트시큐리티	2017 정보보호 R&D 데이터 챌린지 대회의 대용량 정상, 악성파일
	대용량 정상, 악성파일 3 (2018)	한국인터넷진흥원, 안랩, 이스트시큐리티, 하우리, 세인트시큐리티	2018 정보보호 R&D 데이터 챌린지 대회의 악성코드
	대용량 정상, 악성파일 4 (2019)	한국인터넷진흥원, 안랩, 이스트시큐리티, 하우리, 세인트시큐리티	2019 정보보호 R&D 데이터 챌린지 대회의 악성코드
	VX Heaven 악성코드	호서대학교	VX heaven에서 배포하는, 15개의
	메모리 상주 악성코드	한양대학교	실행파일 없이 메모리 상에 상주
안드로이드 앱 데이터셋	정상/악성앱	고려대학교	다양한 악성앱 repository에서 수
	오탐/제로데이 악성앱	고려대학교	Andro-Profiler에서 오진한 앱과 제로데이 악성앱 셋
	대용량 악성·정상앱 1 (2018)	고려대학교	2018 정보보호 R&D 데이터 챌린지 대회의 악성·정상 앱
차량 데이터셋	Car Hacking 데이터셋	고려대학교	DoS attack, fuzzy attack, spoofing the drive gear, spoofing the RPM gauge를 포함하는 자동차 해킹 데이터셋
	차량 이상징후 탐지	고려대학교	2017 정보보호 R&D 데이터 챌린지 대회의 "차량 이상징후 탐지" 트랙 본선에 활용된 정상 및 3종의 차량 공격시도 패킷 데이터
	차량 주행 데이터 (2018)	고려대학교	2018 정보보호 R&D 데이터 챌린지 대회의 "차량 주행 데이터 기반 도난 탐지"에 활용된 700km 차량 주행 데이터
	자동차용 네트워크 데이터 (2019)	고려대학교	"자동차용 침입탐지 2019"에 활용된 3개 차종의 정상 및 공격 데이터
기타	스크립트 난독화 도구	한국인터넷진흥원	난독화된 자바 스크립트 해제 기술 성능평가에 활용된 원본 스크립트, 난독화된 스크립트, 난독화 도구 4종 분석자료
	취약한 바이너리셋 1 (2018)	한국인터넷진흥원	"AI기반 취약점 자동탐지"에 활용된 취약점이 포함된 바이너리 95개
	취약한 바이너리셋 2 (2019)	한국인터넷진흥원	"AI기반 취약점 자동탐지 2019"에 활용된 취약점이 포함된 바이너리 60개
	네트워크 패킷 데이터	한국인터넷진흥원, 안랩, 한국전력공사	"AI기반 네트워크 위협탐지 2019"에 활용된 약 60GB의 패킷을 가공한 파일
	게임유저 액션로그 데이터	고려대학교	"게임봇 탐지 2019"에 활용된 약 3주치의 AION 게임유저 액션 로그

KISA

III. K-사이버 시큐리티 챌린지 - 2017

악성코드, 정상·악성 앱, Car Hacking 데이터셋을 활용한 챌린지 대회 개최

(KISA) 악성코드 선제대응 챌린지

- 백신사 제공 300개 지능형 악성코드
  ※ 백신사에서 분석에 어려움을 겪고 있는 대표 샘플로 구성
- 자유 기술경쟁(악성코드 공격/방어 기술)
- 1위 KISA 원장상(상금 300만원)

(KISA) 악성코드 탐지 챌린지

- 백신사, KISA 정상·악성코드 3만개
  ※ 랜덤한 방식으로 수집된 정상·악성코드 샘플로 구성
- 악성코드 탐지 정확도 경쟁
- 1위 KISA 원장상(상금 300만원)

(고려대) 차량 이상징후 탐지 챌린지

- 자동차 정상·공격 네트워크 트래픽
  ※ 실제 자동차에서 수집된 네트워크 트래픽
- 실시간 자동차 공격 탐지 정확도 경쟁
- 1위 정보보호학회 회장상(상금 300만원)

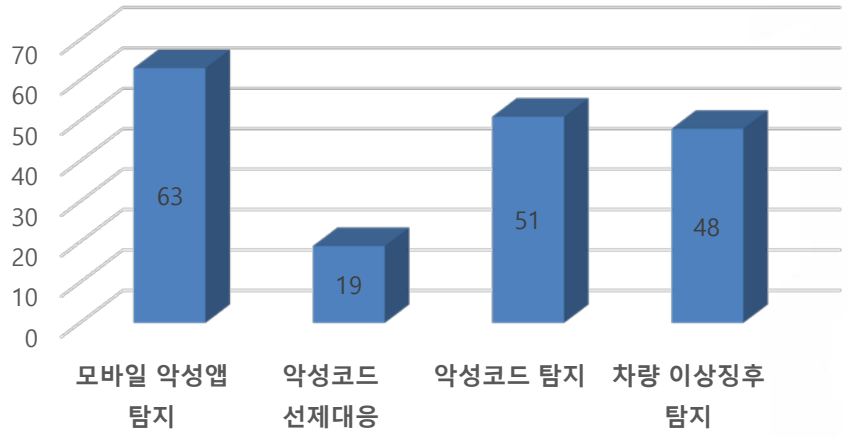
(고려대) 악성앱 탐지 챌린지

- 모바일 정상·악성 앱 8천개
  ※ 앱 스토어에서 수집된 정상·악성 앱
- 모바일 악성 앱 탐지 정확도 경쟁
- 1위 NC소프트 대표이사상(상금 300만원)

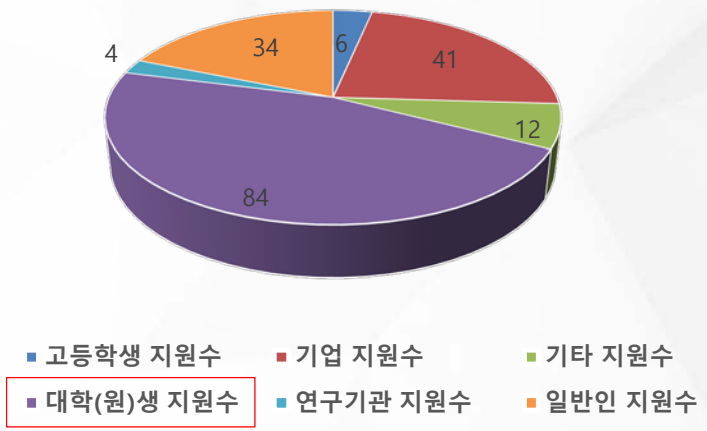
III. K-사이버 시큐리티 챌린지 - 2017

총 181개팀(372명)이 참여하여 온라인 예선 진행

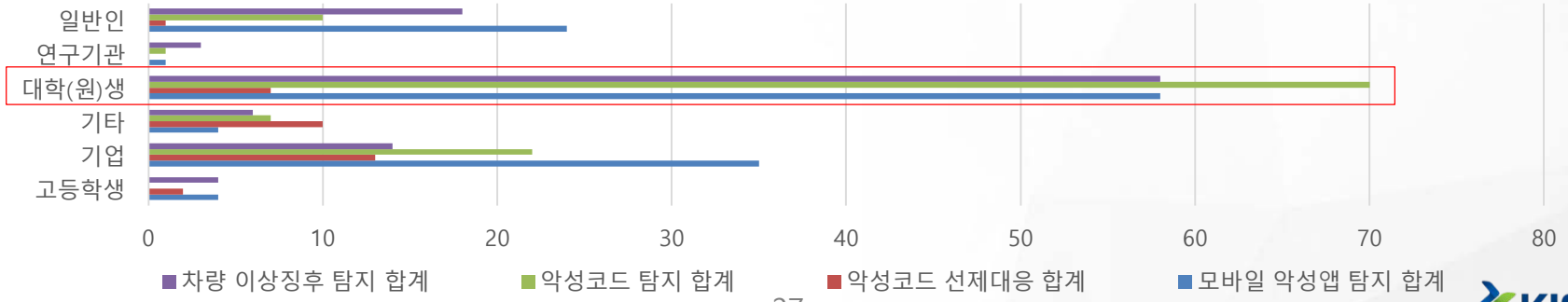
트랙별 참가 팀 현황



참가 팀 구분



트랙별 참가자 현황



III. K-사이버 시큐리티 챌린지 - 2017 결과

20팀 본선 진출, 최종 7개 수상팀 선정('17.12.8)

악성코드 탐지 기술 챌린지

- 백신사, KISA 정상·악성코드 3만개
  ※ 랜덤한 방식으로 수집된 정상·악성코드 샘플로 구성
- (1위) AI기술을 활용해 본선 당일 새롭게 공개된 악성·정상 코드를 1만 5천개를 88.66% 정확도로 탐지

악성앱 탐지 기술 챌린지

- 모바일 정상·악성 앱 8천개
  ※ 앱 스토어에서 수집된 정상·악성 앱
- (1위) AI기술을 활용해 본선 당일 새롭게 공개된 모바일 정상·악성앱 4천개를 87.24% 정확도로 탐지

차량 이상징후 탐지 기술 챌린지

- 자동차 정상·공격 네트워크 트래픽
  ※ 실제 자동차에서 수집된 네트워크 트래픽
- (1위) AI기술을 활용해 본선 당일 새롭게 공개된 차량 정상 운행, 공격 시도 행위를 91.44% 정확도로 탐지

III. K-사이버 시큐리티 챌린지 - 2018

- 2개 신규 트랙 추가, 악성코드 탐지 트랙 대학(원)생-일반 부문으로 이원화
- 권역별 오프라인 예선 개최, 악성코드 탐지 트랙 1박 2일 본선 개최

[KISA] 악성코드 탐지

- 백신사, KISA 정상·악성코드 5만개
- 정상/악성코드 탐지 정확도 경쟁
- 1위 KISA 원장상(상금 300만원)

[KISA] 취약점 자동 탐지

- 취약한 바이너리 95개
- 자동 취약점 탐지 기술 경쟁
- 1위 과기부 장관상(상금 300만원)

[학회] 안드로이드 악성앱 탐지

- 정상·악성 앱 11,000개
- 정상/악성앱 탐지 정확도 경쟁
- 1위 정보보호학회 회장상(상금 300만원)

[학회] 차량 도난 탐지

- 720KM 주행 데이터
- 차량 운전자 구분 정확도 경쟁
- 1위 정보보호학회 회장상(상금 300만원)

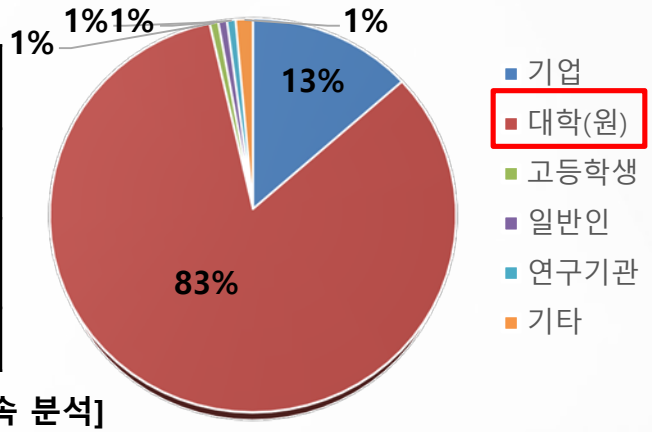
III. K-사이버 시큐리티 챌린지 - 2018

참가자 분석

트랙		팀(개)	인원(명)	비율(%)
AI기반 악성코드 탐지	일반(제한없음)	18	37	47.32
	대학(원)생	32	104	
AI기반 취약점 자동탐지		14	42	14.09
AI기반 안드로이드 악성앱 탐지		33	68	22.82
차량주행 데이터 기반 도난탐지		27	47	15.77
합계		**124**	**298**	**100**

[2018년 챌린지 참가자 현황]

구분	기업	대학(원)	고등학생	일반인	연구기관	기타	합계(명)
일반부문 (제한없음)	19	13	1	1	1	2	37
대학(원) 부문	-	104	-	-	-	-	104
합 계	19	117	1	1	1	2	141



[악성코드 탐지 트랙 참가자 소속 분석]

III. K-사이버 시큐리티 챌린지 - 2018 결과

32팀 본선진출, 4개 트랙 1~3위(총 15팀) 선정

악성코드 탐지_일반

순위	팀명	탐지율
1	정성균 개인팀	96.83%
2	F1	94.48%
3	너울	93.41%
4	Maybe	91.51%
5	양버터팀	41.84%

악성코드 탐지_대학(원)

순위	팀명	탐지율
1	KMU InfoSec	96.1%
2	S&D	95.84%
3	이상 SDS	95.46%
4	MALSECOM	94.67%
5	Chuiup Sicuejo	94.39%
6	갓보성	91.85%
7	Hawkis	91.79%

안드로이드 악성앱 탐지

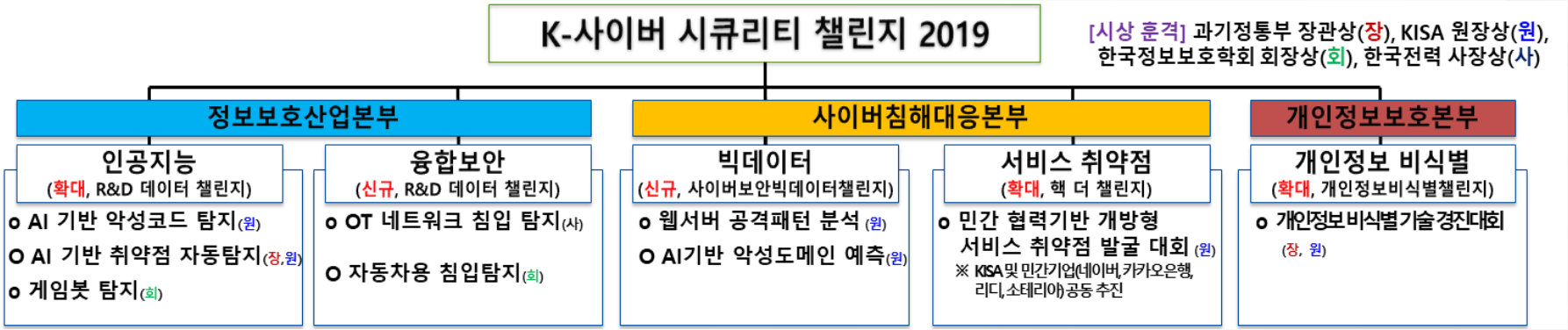
순위	팀명	탐지율
1	너의3대는?	97.53%
2	유홍렬	95.85%
3	고려대&연세대	94.33%
4	MLCS	94.23%
5	뉴테크	93.95%
6	노위캔	91.38%
7	AA	89.33%
8	한명이사라졌어요	87.6%

차량주행 데이터기반 도난 탐지

순위	팀명	분류정확도
1	태듕	49.98%
2	IMLAB	42.45%
3	차도둑들	36.19%
4	고려대 & 연세대	35.58%
5	오투랩스	32.06%

III. K-사이버 시큐리티 챌린지 - 2019

인공지능, 융합보안, 빅데이터, 서비스 취약점, 개인정보 비식별 등 국내 최대 규모의 사이버보안 경연대회 'K-사이버 시큐리티 챌린지 2019' 개최



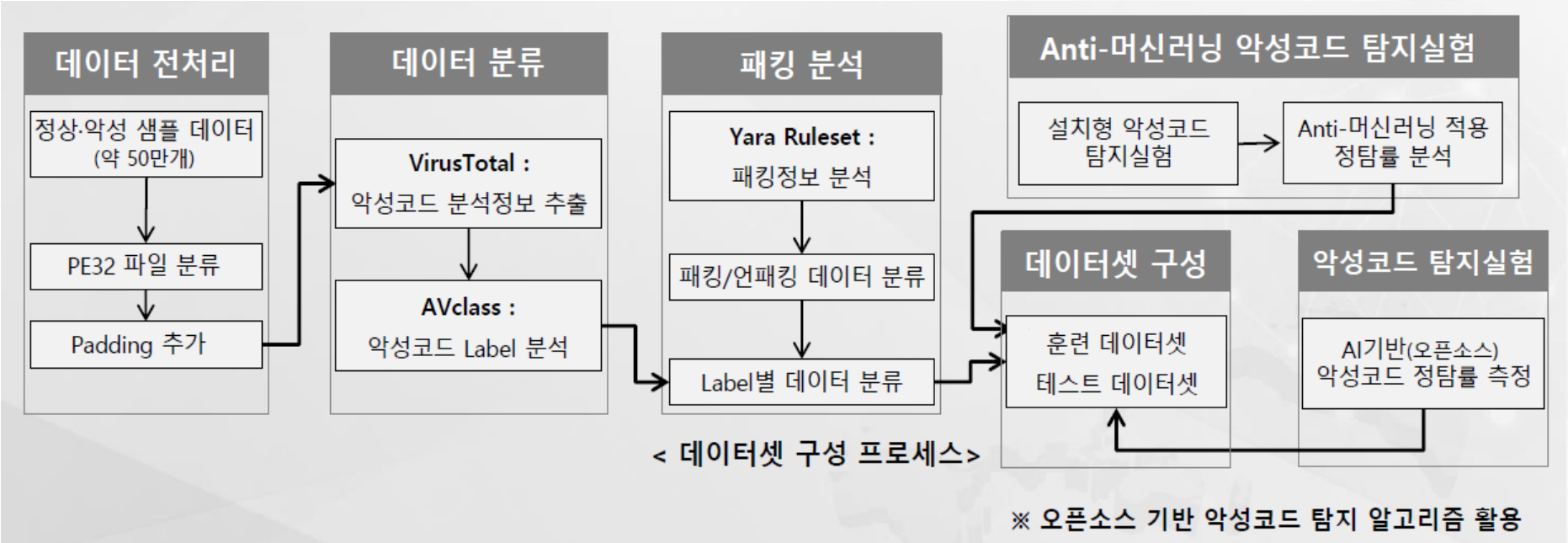
- **369개팀(총 730명)이 트랙별 예선·본선을 거쳐 우수 32개팀 입상**

	인공지능			융합보안		빅데이터		서비스 취약점	개인정보 비식별
	악성코드 탐지	취약점 자동탐지	게임 봇 탐지	OT 네트워크 침입탐지	자동차 침입탐지	웹 서버 공격패턴 분석	악성 도메인 예측	취약점 발굴 대회	비식별 기술경진
참가	40팀 (124명)	11팀 (32명)	40팀 (81명)	27팀 (77명)	38팀 (78명)	20팀 (58명)	19팀 (50명)	126팀 (126명)	48팀 (104명)
수상	3팀 (12명)	3팀 (11명)	3팀 (14명)	3팀 (11명)	3팀 (11명)	3팀 (10명)	3팀 (9명)	4팀 (4명)	7팀 (22명)

III. K-사이버 시큐리티 챌린지 - 2019

- AI를 이용한 악성코드 탐지 트랙
- 변별력 확보를 위해 패킹(약 30%), Anti-머신러닝 악성코드(약 2%) 포함
- 실험결과를 바탕으로, 본선 데이터셋에 신규데이터(10%) 포함

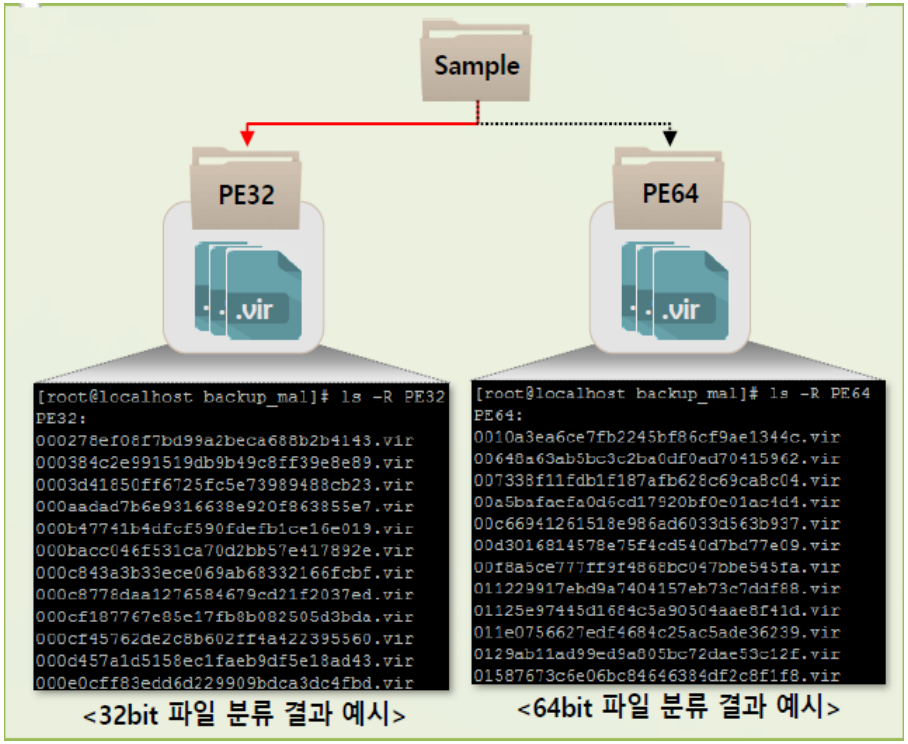
※ KISA와 국내 백신 4사(안랩, 세인트시큐리티, 이스트시큐리티, 하우리)가 제공한 정상·악성 데이터 약 50만개 활용



III. K-사이버 시큐리티 챌린지 - 2019

- AI를 이용한 악성코드 탐지 트랙
- 데이터 전처리

  - PE32, PE64 파일 분류 및 대회용 시그니처 KISA 삽입



<32bit 파일 분류 결과 예시>

<64bit 파일 분류 결과 예시>

Padding 추가

- 정상·악성 데이터 끝에 대회용 시그니처인 KISA (4byte Padding)를 추가한 형태로 공유
- 파일명은 MD5 해쉬값, 확장자는 .vir

```
000cf45762de2c8b602ff4a422395560.vir
001da0dcd43214567e5b95405f7538bb.vir
00285555ddd4cf729db70bc62ccba665.vir
002ecf83540369333f5c17bb2867f3b2.vir
00366e05529ad18c3f743dabd4e11a86.vir
004263064fc93ebf27ef4a3f5213cfee.vir
```

<대회용 데이터 파일명 예시>

```
00093E70  E0 76 09 61 57 D9 66 57 A9 4C 8B 4A 98 B9 DD 09  àv.aWUfWŒL‹J˜¹Ý.
00093E80  E1 08 D9 84 B4 F1 2F 58 CF 1F 2F 73 9A AC 66 29  á.Ù„´ñ/XÏ./sš¬f)
00093E90  8E 17 29 71 DB 0C 0A 10 3E 1C 63 AA 8E AF 4F F3  Ž.)qÛ...>.cªŽ¯Oó
00093EA0  59 DD 21 CC 68 04 EB 6A CC D4 45 F9 51 A4 38 8F  YÝ!Ìh.ëjÌÔEùQ¤8.
00093EB0  38 37 66 27 95 AD 8A C4 3A 28 93 7F 3C A9 F6 B2  87f'•.ŠÄ:("."<©ö²
00093EC0  37 56 6C 69 21 8D FA 84 D7 D9 69 75 8F 1C 05 08  7Vli!.ú„×Ùiu....
00093ED0  85 FF 2F 34 7A 9C D7 8D D4 F6 F3 C4 30 AC 70 67  …ÿ/4zœ×.ÔöóÄ0¬pg
00093EE0  7A 00 00 00 00 00 00 00 4B 49 53 41              z.......KISA
```

<시그니처 추가한 대회용 데이터 - Hex 코드>

KISA

III. K-사이버 시큐리티 챌린지 - 2019

데이터챌린지 2017 vs 2018 vs 2019 비교

	순위	모델	알고리즘	분류	정탐률(%)	평균 정탐률(%)
2017	1	앙상블	Gradient Boosting (XGBoost)	머신러닝	87.92	78.1
	2	단일모델	ANN	딥러닝	85.467	
	3	단일모델	DNN	딥러닝	78.747	
	4	앙상블	Random Forest	머신러닝	75.7665	
	5	앙상블	Random Forest	머신러닝	62.6	
2018	1	앙상블	XGBoost, LightGBM	머신러닝	96.86	95.78
	2	앙상블	Random Forest	머신러닝, 딥러닝	96.1	
	3	앙상블	Random Forest	머신러닝	95.84	
	4	앙상블	Fast KNN, DNN 등	머신러닝, 딥러닝	95.46	
	5	앙상블	Random Forest	머신러닝	94.67	
2019	1	앙상블	CNN, LSTM	딥러닝	99.3	97.49
	2	앙상블	LightGBM, Random Forest	딥러닝	98.79	
	3	앙상블	XGBoost	머신러닝	97.69	
	4	앙상블	XGBoost, LightGBM	머신러닝	96.48	
	5	앙상블	XGBoost, LightGBM	머신러닝	95.2	

III. K-사이버 시큐리티 챌린지 - 2019

AI를 이용한 악성코드 탐지 트랙

데이터챌린지 2017 vs 2018 vs 2019 비교

	2017					2018				
정탐률 순위	1	2	3	4	5	1	2	3	4	5
모델	앙상블	단일모델	단일모델	앙상블	앙상블	앙상블	앙상블	앙상블	앙상블	앙상블
알고리즘	XGBoost	ANN	DNN	Random Forest	Random Forest	Gradient Boosting	CNN, 엘라스틱서치	Random Forest	Fast KNN, DNN 등	Random Forest
분류	머신러닝	딥러닝	딥러닝	머신러닝	머신러닝	머신러닝	머신러닝 딥러닝	머신러닝	머신러닝 딥러닝	머신러닝
정탐률(%)	87.92	85.467	78.747	75.7665	62.6	96.86	96.1	95.84	95.46	94.67

KISA

III. K-사이버 시큐리티 챌린지 - 2020

AI, 빅데이터 등 혁신 보안기술 분야 산·학·연 보안전문가간 기술 경쟁의 場 'K-사이버 시큐리티 챌린지 2020' 개최

※ '19년 대비 신기술 분야 신규 4개, 참여규모 확대 2개, 개선 1개 등 총 10개 트랙

- **AI보안, 빅데이터, 개인정보 등 4개 분야 10개 트랙 개최**

※ 예선(10~11월)은 자율적(트랙별 특성이나 참가자 규모 등에 맞춰 온/오프라인)으로 개최하고, 본선 대회(11.26~27: 오프라인)는 통합 개최

구분	운영 트랙		대회 내용
AI 보안	신규	자동차 해킹 공격/방어	• 자동차 주행 데이터셋 기반 AI 모델 적용한 해킹탐지/방어 기술경쟁
	확대	악성코드 탐지	• 정상/악성 데이터셋 기반 AI 모델 적용한 악성코드 탐지 기술경쟁
	개선	취약점 자동탐지	• 취약점이 포함된 데이터셋 기반 취약점 패치, 자동공격 기술경쟁
	-	게임봇 탐지	• 게임 로그 데이터 기반 게임봇 탐지 기술경쟁
	신규	악성 이메일 탐지	• 데이터셋 기반 AI 모델 적용한 악성 이메일 탐지 기술경쟁
빅데이터	신규	웹스크랩핑 이상탐지	• 웹 접속로그 데이터 기반 웹스크랩핑 이상접근 분석경쟁
	-	데이터셋 Idea 공모	• 보안 분야에 활용성이 높은 독창적인 새로운 데이터셋 공모
	신규	데이터활용Idea 공모	• 미개방 빅데이터 분석을 통한 민간데이터 활용가치 발굴 경진대회
취약점 발굴	확대	핵 더 챌린지	• KISA, 네이버 등 개방형 취약점(대상:홈페이지) 발굴 대회
개인정보	-	개인정보 비식별	• 개인정보 데이터셋 기반 가명·익명 처리 기술경쟁

III. K-사이버 시큐리티 챌린지 - 2020

챌린지 트랙별 추진계획 (1/5)

- **자동차 해킹 공격/방어 기술개발(신규)**
  - ⇒ 목표 차량에 대해 **차량 네트워크 공격**을 진행하고, 기계학습 기반 차량용 IDS(Intrusion Detection System)로 해당 **공격**을 **탐지**하는 공방형 경진대회
  - ⇒ 차량 네트워크 공격 수행 시 트래픽 캡처 및 공격 시점 라벨링 등을 통한 데이터셋 개발
  - ⇒ **네트워크 공격/방어 성공률** 등을 고려하여 우수팀 선정·평가

- **AI기반 악성코드 탐지(확대)**
  - ⇒ 대용량의 정상/악성코드를 활용하여 대회 참가자가 개발한 **AI기반 악성코드 탐지**시스템을 통해 과탐, 미탐이 적은 팀을 선발
  - ⇒ 악성코드 분류 및 분석정보 기반의 데이터셋으로 정상/악성코드 4만개 수준
  - ⇒ **악성코드 탐지율** 및 **발표점수**를 기반으로 우수팀 선정·평가

III. K-사이버 시큐리티 챌린지 - 2020

챌린지 트랙별 추진계획 (2/5)

- **AI기반 취약점 자동탐지(개선)**
  - ⇒ 참가자가 개발한 취약점 자동탐지·공격 시스템을 활용하여 취약점을 찾아 자신의 서버에 패치하고, 경쟁자 서버에 취약점을 찾아 공격 진행
  - ⇒ 사이버 취약점 진단기준(CWE) 기반의 취약점이 포함된 SW 실행파일 활용
  - ⇒ 취약점 탐지율 및 발표점수를 기반으로 우수팀 선정·평가

- **AI기반 게임봇 탐지(유지)**
  - ⇒ 참가자가 개발한 AI기반 게임봇 탐지 시스템을 활용하여 게임 유저 데이터에서 정해진 시간 내에 게임봇 탐지를 많이 한 팀 선발
  - ⇒ 실제 게임회사에서 운용중인 MMORPG 게임유저의 게임로그 데이터셋 활용
  - ⇒ 게임봇 탐지정확도 및 발표점수를 기반으로 우수팀 선정·평가

III. K-사이버 시큐리티 챌린지 - 2020

챌린지 트랙별 추진계획 (3/5)

- **AI기반 악성 이메일 탐지(신규)**

  ⇒ 정상/악성 메일간의 차이를 분석하여 특정 패턴을 파악하여 고도화된 **피싱 공격의 탐지율·예측 정확도**가 높은 팀 선발

  ⇒ 정상 및 악성으로 구성된 약 100만건의 이메일 데이터 활용(추후 확정)

  ⇒ **정상·악성 및 스팸·스피어 피싱 예측정확도**와 **발표**를 기반으로 우수팀 선정·평가

- **웹 스크랩핑* 이상 탐지(신규)**

  ⇒ 웹 스크랩핑에 대한 **정상·이상 로그**를 **분석**하여 발생건수, 탐지율이 높은 팀 선발

  ⇒ 정상 및 악성으로 구성된 약 100GB 수준의 웹서버 접근로그(추후 확정)

  ⇒ **이상 접근유형분석, 이상징후 탐지, 데이터 시각화, 발표**를 기반으로 우수팀 선정·평가

  * 금융, 포털 등의 피싱 웹사이트 제작 과정에서 악용되는 크롤링 기술

KISA

III. K-사이버 시큐리티 챌린지 - 2020

챌린지 트랙별 추진계획 (4/5)

- **사이버보안 인공지능 데이터셋 아이디어 공모(유지)**
  - ⇒ 사이버보안 분야 인공지능 데이터셋에 대한 아이디어와 그 활용 예시 들을 제안하는 데이터셋 경진대회 개최
  - ⇒ 사이버보안 인공지능 이용활성화에 도움이 되는 데이터셋 구축 아이디어 발굴
  - ⇒ 실용성·범용성·데이터 수집/가공 용이성을 기반으로 평가

- **데이터 활용 아이디어 공모(신규)**
  - ⇒ 미개방 데이터의 활용가치 확산 및 새로운 데이터 서비스 시장 창출을 위한 아이디어와 최신 데이터 기술 접목 사례 발굴
  - ⇒ 한국데이터산업진흥원(KDATA)에서 제공하는 미개방 공공·민간 데이터 활용
  - ⇒ 분석보고서에 대한 서면 심사 및 발표에 대한 대면 평가로 우수팀 선정·평가

III. K-사이버 시큐리티 챌린지 - 2020

챌린지 트랙별 추진계획 (5/5)

- **핵 더 챌린지(확대)**

  ⇒ 기업·기관의 자발적 보안 수준 향상 및 IoT·융합보안 등 생활 속 ICT 안전 구현을 위한 취약점 발굴·조치 모델 확산 필요

  ⇒ KISA 및 민간기업 3개 홈페이지 대상→ KISA 및 민간기업 4개 홈페이지로 대상 확대

  ⇒ 취약점 발견 및 조치를 기반으로 우수팀 선정·평가

- **개인정보 비식별(유지)**

  ⇒ 안전하게 처리된 개인정보 더미데이터를 가명·익명처리하고, 가명·익명정보의 유용성 및 안정성이 우수한 팀 선발

  ⇒ 30~100만명 규모의 안전하게 처리된 개인정보 형태의 더미데이터 활용

  ⇒ 가명·익명 처리 데이터의 유용성 및 안전성을 기반으로 우수팀 선정

III. K-사이버 시큐리티 챌린지 - 2020

K-사이버 시큐리티 챌린지 2020 설명회

- 행사명: K-사이버 시큐리티 챌린지 2020 설명회
- 일 시: 2020년 9월 11일(금), 10:00 ~ 12:00
- 장 소: 세종대학교 대양 AI홀(예정)
- 세부 내용

  ⇒ AI보안 기술개발 트랙 운영계획 소개

  ⇒ 사이버보안 빅데이터 부문 운영계획 소개

  ⇒ 취약점 발굴(핵 더 챌린지) 트랙 운영계획 소개

  ⇒ 개인정보 비식별 트랙 운영계획 소개

- 참석대상: K-사이버 시큐리티 챌린지 2020대회에 관심있는 정보보호 관련 대학(원)생, 재직자, 일반인 등

감사합니다