「2021 사이버보안 AI · 빅데이터 활용 경진대회」 대회 안내서

2021. 9. 10.

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

목 차

Ⅰ 대회 개요

□ 대회목적

o 사이버보안 분야 AI 응용 및 빅데이터 분석 등 AI·빅데이터 활용 기술 경쟁의 場 「사이버보안 AI·빅데이터 활용 경진대회」 개최

□ 대회개요

o 대 회 명 : 2021 사이버보안 AI·빅데이터 활용 경진대회

o 주 최 : 과학기술정보통신부

o 주 관 : 한국인터넷진흥원

o 참가대상 : 사이버보안 AI·빅데이터에 관심있는 국민 누구나

※ 개인 또는 4인 이내 팀 구성

□ 운영방식

①참가접수 → ②온라인 예선 → ③온라인 본선 (발표 평가) → ④ 수상자 발표 및 시상

□ 트랙운영 : 기술경연 트랙 2종, 아이디어 공모트랙 1종 운영

구분	분야	운영트랙	대회 내용
A트랙	AI	AI기반 파워쉘 악성 스크립트 탐지	• AI 기반의 정상/악성 파워쉘 스크립트 탐지
B트랙	빅데이터	침해사고 Threat Hunting	• 침해사고 빅데이터 분석을 통한 위협 탐지
C트랙	아이디어 공모	AI·빅데이터 활용 아이디어 공모	• 정보보호 분야에서의 AI기반 빅데이터 활용 아이디어 공모

□ 트랙별 운영일정(안)

o A트랙 : AI기반 파워쉘 악성 스크립트 탐지

1 신청접수	⇒	2 학습 데이터셋 배포	⇒	3 예선	⇒	4 본선		⇒	4 시상식 및 성과공유회
신청서 제출		데이터셋 온라인 배포		온라인 (7팀 선발)		온라인	발표평가		수상자 시상 및 성과공유
9/6(월) ~ 9/24(금)		9/28(화) ~ 10/15(금)		10/22(금)		11/18(목)	11/19(금)		12/1(수)

o B트랙 : 침해사고 Threat Hunting

1 신청접수	⇒	2 샘플 데이터셋 배포	⇒	3 예선	⇒	4 본선		⇒	4 시상식 및 성과공유회
신청서 제출		데이터셋 온라인 배포		온라인 (7팀 선발)		온라인	발표평가		수상자 시상 및 성과공유
9/6(월) ~ 9/24(금)		9/28(화) ~ 10/15(금)		10/22(금)		11/18(목)	11/19(금)		12/1(수)

※ 예·본선 데이터셋은 대회 5~7일 전 사전 배포 예정(팀장 메일을 통해 다운로드 링크 제공)

o C트랙 : 사이버보안 AI·빅데이터 활용 아이디어 공모

1 신청접수	⇒	2 예선	⇒	3 서면평가	⇒	4 본선	⇒	4 시상식 및 성과공유회
신청서 제출		아이디어 공모문서 사무국 접수		서면평가 (7팀 선발)		발표평가		수상자 시상 및 성과공유
9/6(월) ~ 9/24(금)		10/18(월) ~ 10/22(금)		10/25(월) ~ 10/29(금)		11/17(수)		12/1(수)

□ 시상 내역

o 시상 / 상금 : 과학기술정보통신부장관상 2점, 한국인터넷진흥원상 7점, **총 2,700만원 상당 상금 시상**

※ 상금에 대한 제세공과금은 수상팀 부담

구분	운영트랙	구분	훈격	상금
A트랙	AI기반 파워쉘 악성 스크립트 탐지	대상	과학기술정보통신부 장관상	500만원
		최우수상	한국인터넷진흥원장상	300만원
		우수상	한국인터넷진흥원장상	200만원
B트랙	침해사고 Threat Hunting	대상	과학기술정보통신부 장관상	500만원
		최우수상	한국인터넷진흥원장상	300만원
		우수상	한국인터넷진흥원장상	200만원
C트랙	AI·빅데이터 활용 아이디어 공모	최우수상	한국인터넷진흥원장상	300만원
		우수상	한국인터넷진흥원장상	200만원
		우수상	한국인터넷진흥원장상	200만원

II 대회 운영

□ 참가자격

o 사이버보안 AI·빅데이터에 관심있는 국민 누구나(개인 또는 4인이내 팀 구성)

※ 참가팀의 팀장은 본인의 소속을 증명할 수 있는 서류(재직(학) 증명서 등) 제출 必

□ 대회 절차

o **(참가신청)** 대회 누리집(https://aibigdatasec.kr) 內 접수페이지를 통해 참가신청

o **(접수기간)** 9/6(월) 10:00 ~ 9/24(금) 18:00

※ 접수기간 내에 접수된 건에 한하여 인정(방문, 우편접수 불가)

o **(사전 설명회)** 대회 참가 희망자를 위한 사전 설명회(9.3. 14시, 온라인) 추진

구 분	내 용
일시 / 방법	ㅇ 9. 3.(금) 14:00~15:00 / 유튜브*, 네이버 TV**를 통한 스트리밍 ㅇ 채널명 : kisa_streaming *유튜브 채널: https://www.youtube.com/watch?v=LpvjyXpSx_E **네이버 TV 채널: https://tv.naver.com/v/22238106
주요내용	ㅇ 대회 신청방법, 신청절차, 유의사항 등 대회 참여 필요한 사항 ㅇ 트랙별 출제방향, 운영 방안 등 안내 및 질의 응답

□ 문의처

o 「2021 사이버보안 AI·빅데이터 활용 경진대회」 운영사무국

- E-mail. aibigdata@cmcom.kr, / Tel. 070-4849-7022

1 A트랙 : AI기반 파워쉘 악성 스크립트 탐지

□ 개요

o **(도전과제)** AI 및 빅데이터 분석 기술을 활용하여 정상/악성 파워쉘 스크립트 탐지 모델을 개발하라!

□ 진행방식

o 온라인 예선을 통해 선발된 탐지율 상위 7개팀에 대해 본선 진출권 부여

학습셋 배포		예선		본선	
일정	방식	일정	방식	일정	방식
9/28(화) ~ 10/15(금)	온라인	10/22(금)	온라인 기술경연	11/18(목)	온라인 기술경연
				11/19(금)	발표평가

o **(발표평가)** 팀에서 발표자 1인을 선정, 발표자만 오프라인 심사장에 참석하여 발표 및 평가위원회 심사

※ 오프라인 심사장에 팀원 참석 여부는 코로나19 상황을 고려해 추후 결정 후 공지 예정

□ 데이터셋

o (학습셋) 정상/악성 파워쉘 스크립트 10,000개

o (예선셋) 정상/악성 파워쉘 스크립트 5,000개

o (본선셋) 정상/악성 파워쉘 스크립트 5,000개

※ 데이터셋 수량은 데이터셋 검증결과에 따라 추후 변경될 수 있음

□ 제출문서

o **(예선)** 결과파일(csv), 기술보고서

- **(결과파일)** 탐지결과를 ID와 Result를 포함하여 csv로 구성

※ ID: 파일명 | Result: 정상 0, 악성 1

	A	B
1	ID	라벨
2	파일명.ps	1/0
3		
4		
5		
6		

<결과파일 구성>

- **(기술보고서)** 제공된 양식의 필수항목*에 따른 개발기술 설명서 작성
  * 필수항목: 서론, 사용 feature, AI 모델, 프로그램 설명 등
  ※ 기술보고서는 부정행위 검증 및 발표평가의 참고자료로 활용 예정

o **(본선)** 결과파일(csv), 발표자료(ppt)

- **(발표자료)** 필수항목에 따른 개발기술에 대한 발표자료(15분 분량)

□ 평가방식

o **(예선)** 탐지율*(100%)

o **(본선)** 탐지율(80%) + 발표평가(20%)

* 탐지율 : $F1score = 2 \times \frac{Precison \times Recall}{Precision + Recall}$

2 B트랙 : 침해사고 Threat Hunting

□ 개요

o **(도전과제)** 침해사고 데이터로부터 이상행위를 탐지하고, 공격자의 특성 및 침해사고의 흐름을 분석하며 대응방안을 제시하라!

□ 진행방식

o 온라인 예선의 탐지점수 및 서면평가 결과로 선발된 상위 7개팀에 대해 본선 진출권 부여

<table>
<tr><th colspan="2">학습셋</th><th colspan="2">예선</th><th colspan="2">본선</th></tr>
<tr><th>일정</th><th>방식</th><th>일정</th><th>방식</th><th>일정</th><th>방식</th></tr>
<tr><td rowspan="3">9/28(화)
~
10/15(금)</td><td rowspan="3">온라인</td><td rowspan="2">10/15(금)</td><td rowspan="2">(온라인)
예선 데이터셋 배포</td><td>11/12(금)</td><td>(온라인)
본선 데이터셋 배포</td></tr>
<tr><td>11/18(목)</td><td>온라인
기술경연</td></tr>
<tr><td>10/22(금)</td><td>온라인
기술경연</td><td>11/19(금)</td><td>발표평가</td></tr>
</table>

o **(발표평가)** 팀에서 발표자 1인을 선정, 발표자만 오프라인 심사장에 참석하여 발표 및 평가위원회 심사

※ 오프라인 심사장에 팀원 참석 여부는 코로나19 상황을 고려해 추후 결정 후 공지 예정

□ 데이터셋

o **(학습셋)** 침해사고 로그 데이터(json) + 라벨파일*

- 전체 이벤트 약 4만건, 공격 이벤트 약 30건

* 라벨파일: 탐지된 각 공격로그에 대해 MITRE ATT&CK v7에 매핑되는 공격기법으로 라벨링

o (예선셋) 침해사고 로그 데이터(json)

- 전체 이벤트 약 12만건, 공격 이벤트 약 60건

o (본선셋) 침해사고 로그 데이터(json)

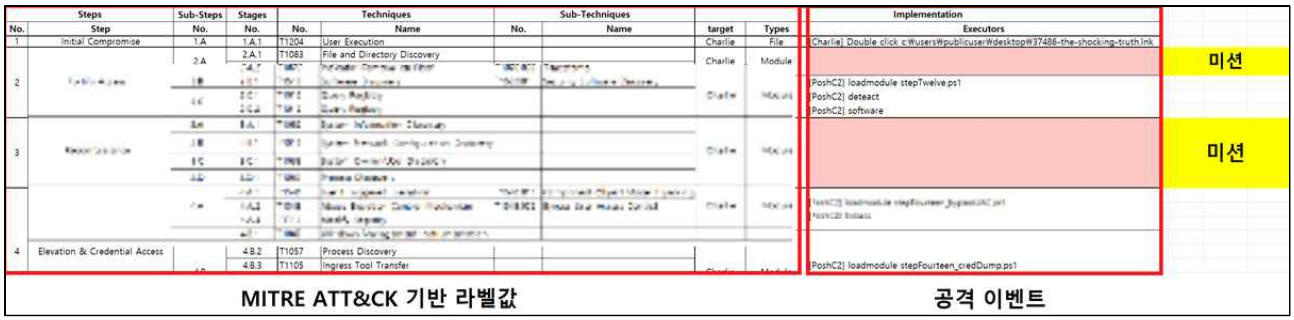
- 전체 이벤트 약 19만건, 공격 이벤트 약 60건

□ 제출문서

o (예선) 결과파일(csv), 기술보고서

- (결과파일) 공개된 라벨값*을 참고하여, 데이터셋으로부터 미션에 해당하는 공격로그를 탐지하여, 탐지한 로그를 csv로 구성

* 라벨값: 탐지된 각 공격로그에 대해 MITRE ATT&CK v7에 매핑되는 공격기법으로 라벨링



- (기술보고서) 제공된 양식의 필수항목에 따른 침해사고 분석과정 및 대응방안 작성

※ 필수항목: 데이터 분석방법, 침해사고 개요도, 타임라인, IoC정보, 대응방안 등

※ 기술보고서는 부정행위 검증 및 서면평가에 활용

o (본선) 결과파일(csv), 발표자료(ppt)

- (발표자료) 필수항목에 따른 침해사고 분석 방법론에 대한 발표자료(15분 분량)

□ 평가방식

o (예선) 탐지점수(70%) + 서면평가(30%)

o (본선) 탐지점수(70%) + 발표평가(30%)

※ 데이터셋으로부터 공격 흐름을 추적·분석하고, 그 안에서 실제 공격을 탐지해 내는 방법론 도출 필요

3 C트랙 : 사이버보안 AI · 빅데이터 활용 아이디어 공모

□ 개요

o **(공모주제)** 사이버보안 분야에서 AI를 통해 빅데이터를 활용할 수 있는 방안에 대한 아이디어를 발굴하라!

<예 시>

1. 국민 생활 밀착형 보안 서비스(보이스 피싱 방지, 스팸방지 등) 발굴을 위한 AI·빅데이터 활용 아이디어
2. AI 성능 향상을 위한 AI 데이터셋 구축(수집·가공·생성·활용 등) 아이디어
3. AI·빅데이터 활용을 통한 사이버보안 난제 해결 아이디어 등

□ 진행방식

o 서면평가를 통해 선발된 상위 7개팀에 대해 본선 진출권 부여

예선		서면평가		본선	
일정	방식	일정	방식	일정	방식
10/18(월) ~ 10/22(금)	(온라인) 아이디어 보고서 제출	10/25(월) ~ 10/29(금)	평가위원회 서면평가	11/17(수)	발표평가

o **(발표평가)** 팀에서 발표자 1인을 선정, 발표자만 오프라인 심사장에 참석하여 발표 및 평가위원회 심사

※ 오프라인 심사장에 팀원 참석 여부는 코로나19 상황을 고려해 추후 결정 후 공지 예정

※ 아이디어 도용, 타 공모전에서 이미 채택된 아이디어 등 문제 발견 시, 수상에서 제외될 수 있음

□ 제출문서

o **(예선)** 자유양식으로, PPT파일 30페이지 이내로 아이디어 기술

※ 팀 당 1개의 아이디어 공모문서 제출을 원칙으로 함

o **(본선)** 예선 제출자료를 15분 발표분량으로 수정하여 제출

※ 발표자료 수정 여부는 자유이나, 발표시간은 약 15분으로 제한 함

□ 평가방식

o **(예선)** 서면평가(100%)

o **(본선)** 예선결과(80%) + 발표평가(20%)

※ 본선에서는 예선의 서면평가 결과를 80%로 반영

Ⅲ. 대회 규정

□ 신청 및 접수

o 사이버보안 AI·빅데이터에 관심있는 국민 누구나(개인 또는 4인이내 팀 구성)

※ 참가팀의 팀장은 본인의 소속을 증명할 수 있는 서류(재직(학) 증명서 등) 제출 必

o 접수기간 : ‘21. 9. 6.(월) 10:00 ~ ’21. 10. 15.(금) 18:00까지

o 신청방법 : 경진대회 누리집(https://aibigdatasec.kr)을 통해 접수

o 심사 및 서류 탈락(결격) 사유

- 참가신청 기간 외에 참가접수 요청 팀
- 참가신청서 내 일부 내역이 누락된 팀

※ 참가신청서 작성 내역으로 해당 신청인(팀원 포함)을 식별할 수 없을 경우 해당

- 참가신청 서류 목록의 전부 또는 일부가 누락된 팀
- 참가신청 서류를 허위로 작성하여 제출한 팀
- 부정행위(치팅)*가 확인될 경우 본선진출, 입상 등에서 심사탈락

* 예시) AI를 기반으로 하지 않고 검색엔진을 사용해 파워쉘 스크립트 정상/악성 탐지하는 행위, 참가팀원 이외의 인원의 도움을 받거나 참여하는 행위 등

o 중복참여

- 팀원은 2개 트랙 이상 참여 가능하나, 팀장은 타 트랙에 중복 참여 불가능 함
- 중복참여 시, 2개 이상 트랙 모두 본선에 진출할 경우, 한 개 트랙의 본선에만 최종 참여 가능하며 이에따른 팀의 결원은 충원이 불가함

※ ex) 트랙1, 트랙2 모두 본선 진출권을 획득한 팀원 A는 트랙1 참여팀 또는 트랙2 참여팀 둘 중 하나의 팀에만 참여 가능. A가 트랙1 팀 선택할 경우, 트랙2 팀은 A의 결원으로 처리하여 본선 진행

o 평가위원 제척사항

- 평가위원의 경우 소속기업 및 기관 참여시 평가위원에서 제척함

o 기타

- 참가신청 서류를 허위로 작성하여 제출한 경우 참가자격 박탈 등 관련 규정에 따라 조치
- 팀장의 경우 소속을 증빙할 수 있는 재학(휴학)증명서 및 재직증명서 제출 必

□ 유의 사항

o 여기서 참가자란 참가한 팀, 팀 전원, 팀 內 개별 팀원 등을 포함함

o 참가자가 제안한 아이디어는 타사 또는 타기관에 제안이력이 없어야 하며, 참가자가 직접 창안하거나 전적인 권리를 갖고 있어야 함

o 참가자가 제출한 아이디어 및 수상작에 대한 **제3자의 저작권, 특허권, 초상권 등의 지적재산권 및 정보의 무단 사용 등으로 발생할 수 있는 법적문제에 대한 책임은 응모자 및 수상자**에게 있으며, 추후 문제 발생 시 수상취소 및 상금 환수 조치함

o 주요 평가 기준 및 항목만 공개하며, 평가위원회를 통한 세부 평가한 내용 및 과정 등 관련 자료는 공개하지 아니함

o 아래의 경우, 수상 이후라도 수상취소 및 상금회수를 조치하며, 이와 관련하여 발생 할 수 있는 모든 민·형사상의 책임은 본인에게 있음

- 자신이 속한 조직 등의 **사업 아이디어 및 사업 중이거나 사업화를 위해 준비 중인 아이디어로 공모** 한 경우
- **타 경진대회, 공모전 등에서 이미 채택된 아이디어인 경우**
- 참가신청서 등 제출 서류를 사실과 다르게 허위로 작성한 경우
- 참가자격에 준하지 않은 자가 대회에 참가한 경우
- 타 경진대회 수상작, 대리작 및 타인의 저작물을 도용한 경우

o 경진대회의 참가작에 대한 저작권은 참가자에게 있으며, KISA는 참가자와 협의를 통해 제3자에게 공개하거나 공유가 가능함

※ KISA는 수상작에 한하여 수상자와 협의하여 간행물 및 보도자료를 배포할 수 있음

o 제출한 경진대회 관련 서류는 선정여부를 불문하고 반환하지 않음

o 접수 결과 등에 따라 시상 규모는 변경 될 수 있음

o 상금에 대한 제세공과금은 수상자 부담을 원칙으로 함

o 개인이 아닌 팀으로 참가하여 수상할 경우, 상금은 대표자에게 지급되며 상금의 분배와 관련된 사항은 참가자 상호간 협의에 따라 결정할 사항으로 과학기술정보통신부와 한국인터넷진흥원은 이에 관여하지 않음