

# 사이버보안 AI · 빅데이터 챌린지 2023

CybersecurityAI Big Data Challenge 2023

## 대회안내서

주최



과학기술정보통신부

주관



한국인터넷진흥원

# Contents



1 A트랙 | SI기반 네트워크 웹 공격 분류

2 대회 참가방법

CHAPTER

01

# A트랙 | AI기반 네트워크 웹 공격 분류

주최



과학기술정보통신부

주관



한국인터넷진흥원

# Contents

## 1 A트랙 | 시 기반 네트워크 웹 공격 분류

- 1) 대회 일정
- 2) 데이터셋 소개
- 3) 도전 과제
- 4) 결과물 제출
- 5) 평가방식

구분	날짜	대회방식	시간		내용
학습셋	'23. 9. 19(화)	학습셋 배포	9. 19(화) ~ 10. 13(금) 18:00		대회플랫폼 온라인 배포
예선	'23.10.19(목)	예선셋 배포	10:00 ~ 24:00	840'	대회플랫폼 온라인 배포
	'23.10.20(금)	온라인 기술경연	9:30 ~ 10:00	30'	예선셋 압축 패스워드 공개
			10:00 ~ 17:00	420'	경연진행
본선	'23.11.15(수)	본선셋 배포	10:00 ~ 24:00	840'	대회플랫폼 온라인 배포
	'23.11.16(목)	온라인 기술경연	9:30 ~ 10:00	30'	본선셋 압축 패스워드 공개
			10:00 ~ 17:00	420'	온라인 기술경연
			17:00 ~ 18:00	60'	소스코드 제출
	'22.11.17(금)	오프라인 발표평가	13:00 ~ 17:00	240'	오프라인 발표평가(7개팀)

## 데이터셋 예시

Log_Num	payload	label	action
0	GET /forum1_professionnel.asp?n=/.WWW"/.WWW"/.WWW"/.WWW"/.	System_Cmd_Execution	
1	POST /owa/auth/logon.aspx?replaceCurrent=1%22%29%20AND%	System_Cmd_Execution	
2	GET /goods/goods_search?display_type=list&arr_search_list%5B0%	SQL_Injection	
3	GET / HTTP/1.1WrWnWrWn	HOST_Scan	
4	GET /sub_04_1_read.php?page=1&id=31%29%3BSELECT%20%2A9	System_Cmd_Execution	
5	POST /member/login HTTP/1.1WrWnContent-Length: 197WrWnCac	Vulnerability_Scan	
6	GET /board/?category=&gdviewer=1&goods_seq=69&id=goods_r	System_Cmd_Execution	
7	GET /board/board_list?code=welfare&search_type=title%20AND%	SQL_Injection	

## 데이터셋 구성

- 학습셋) 웹 방화벽(WAF) 로그 학습셋 45,000건(라벨포함)
- 예선셋) 웹 방화벽(WAF) 로그 학습셋 10,000건
- 본선셋) 웹 방화벽(WAF) 로그 학습셋 12,826건

※ 예·본선 데이터셋은 데이터셋 구축 및 검증 과정에서 일부 변경될 수 있음

## 데이터셋 설명

- 로그유형 : 웹방화벽(WAF) 로그
- 공격 유형(라벨) : 9개\*
  - \* Path disclosure, Vulnerability\_scan, System\_cmd\_execution, Host\_scan, SQL\_injection, Automatically\_searching\_infor, Cross\_site\_scripting, Directory\_indexing, Leakage\_through\_nw
- 제공필드 : payload 관련정보만 제공

## 데이터셋 배포

챌린지 플랫폼을 통해 데이터셋 배포

## 도전 주제

AI를 통해 웹 방화벽 로그를 분석하고, 비정상 행위를 분류하라

## 문제 풀이

- ① 약 9개의 공격유형으로 라벨링된 WAF 로그가 데이터셋으로 주어진다.
- ② 주어진 학습셋으로 AI모델을 학습시켜
- ③ 예/본선셋의 각 로그를 9개의 공격유형으로 분류한다.

## A트랙 | 분류정확도 | Macro f1-score

Macro f1-score : N개의 클래스에 대해, 각 클래스별 f1-score 합의 평균

$$\text{분류정확도} = \sum_{i=1}^N \frac{f1\ Score_i}{N} \quad (N: The\ Number\ of\ Classes)$$

## 트랙 운영

- 예선
    - 운영방식 : 기술경연, 서면평가
    - 제출물 : 답안지(기술경연), 기술보고서(서면평가)
  - 본선
    - 기술경연, 발표평가
    - 제출물 : 답안지(기술경연), 발표자료(발표평가), 소스코드
- ※ 소스코드 제출 시간 : '23.11.16.(목) 18시까지

## 유의사항

- 수상자 대상으로 소스코드를 검증하고 평가기준 미달 시 실격
- 소스코드 : .ipynd | google colab에서 재현 가능한 소스코드
- AI 대회이므로, 패턴매칭\* 으로 분류 금지
  - \* 패턴매칭 예시 : 특정 패턴일때 특정 라벨로 판단
- 부정행위, 실격처리 등 관련 대회규칙은 대회요강 확인 필수
- 대회규칙에 위반된 결과물 제출시 수상에서 제외될 수 있음



## 답안지 작성요령

	A	B
1	Log_Number	label_action
2	0	System_Cmd_Execution
3	1	System_Cmd_Execution
4	2	SQL_Injection
5	3	HOST_Scan
6	4	System_Cmd_Execution
7	5	Vulnerability_Scan
8	6	System_Cmd_Execution
9	7	SQL_Injection
10	8	HOST_Scan
11	9	HOST_Scan

- Log\_Number : WAF 개별로그 식별자
- Label\_action : WAF 로그의 공격위협 분류
- 답안지명 : ./A\_Track\_팀명.csv
- 소스코드는 반드시 google colab에서 실행되어야 함

## 기술보고서 작성요령

사이버보안 AI 역량데이터 설문지 2022  
<A트랙 : AI기반 악성코드 위협 분류>

☐ AI 학습 구성도

아래의 방법론을 기반으로 데이터 분석 - 분류 모델링 전 과정에 대한 AI 모델링 구성도

☐ 방법론

기타 추가적인 방법론에 대한 항목 추가 가능

1. 데이터 분석

데이터 전처리, 데이터 초기 분석 방법 등

1.1

-

※

1.2

2. feature

분류를 위해 선정한 feature, 선정 기준(이유), feature 별 중요도 등

2.1

-

※

3. AI 모델링

AI 알고리즘 구성, AI 알고리즘 선정 기준(이유), 파라미터 튜닝 등

3.1

-

※

2

## &lt;기본항목&gt;

1. 데이터 분석
2. Feature 선정
3. AI 모델링
4. 분류 결과(분류정확도)
5. 현장 적용을 위한 모델의 개선방안  
(필수항목)
6. 결론

※ 기본항목은 변경 가능(평가항목 참고)  
 ※ 활용도구 명시 必  
 ※ 외부데이터 활용시, 해당 내용 포함 必  
 ※ 출처 명시 必

👉 발표자료는 기술보고서 핵심내용으로 구성(15분 발표분량)



👉 평가방식은 평가위원회 의견에 따라 공개 가능한 수준으로만 공지됩니다.

## 평가지표

- 예선 | 분류정확도(60%) + 순위별 차등점수\* (10%) + 서면평가(30%)

\* 순위별 차등점수 : 1~3등 : 10점 | 4~6등 : 8점 | 7~9등 이하 6 | 10등 이하 4점

- 본선 | 분류정확도(80%) + 발표평가(20%)
- 분류정확도 | Macro f1-score

## 평가방법

- 블라인드 평가 | 평가위원회는 팀정보를 모르는 상태에서 평가진행
- 최고 최저 제외 평균 | 평가위원(8인 내외) 평가점수 중 최고 및 최저 점수 제외한 평균점수 반영
- 학생팀의 경우 서면/발표평가 가산점 2점 부여

## 평가항목 - 서면/발표평가

NO.	평가항목	배점
1	데이터 구성의 이해 & feature 엔지니어링	20
2	데이터 전처리기술	30
3	AI 기술수준	30
4	현장 적용을 위한 모델의 개선 방안	20

CHAPTER

02

# 대회 참가방법

주최



과학기술정보통신부

주관

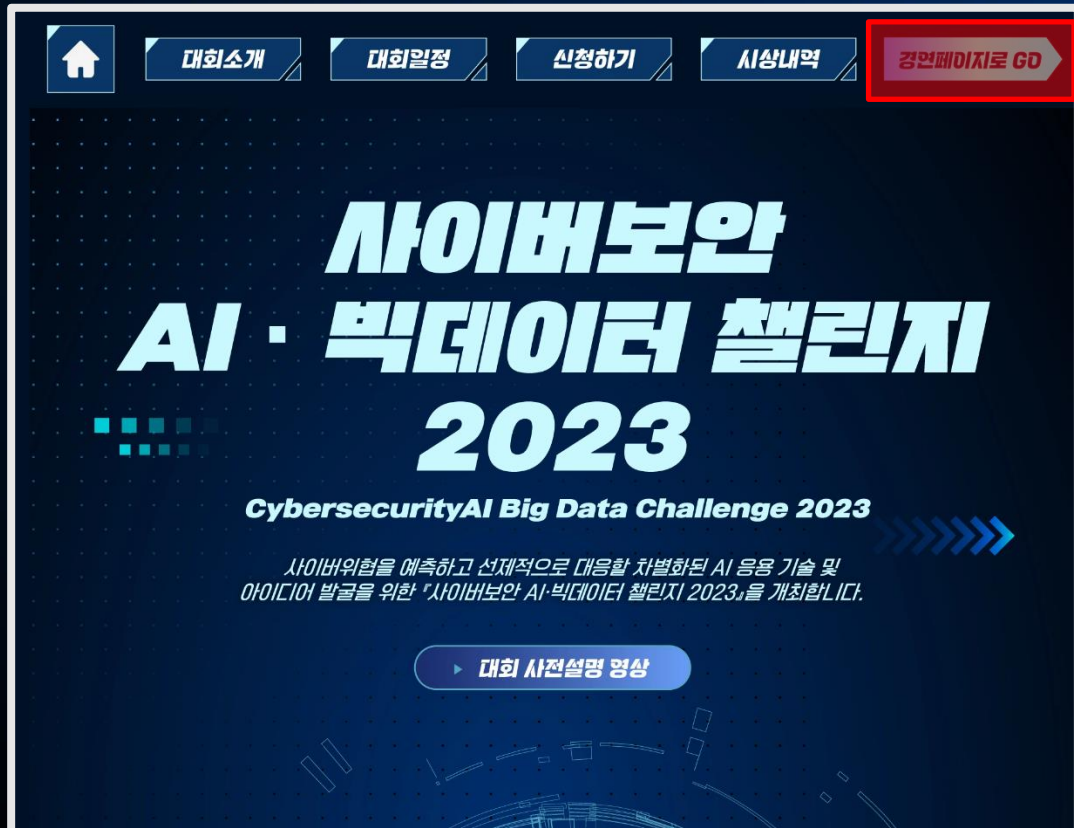


한국인터넷진흥원

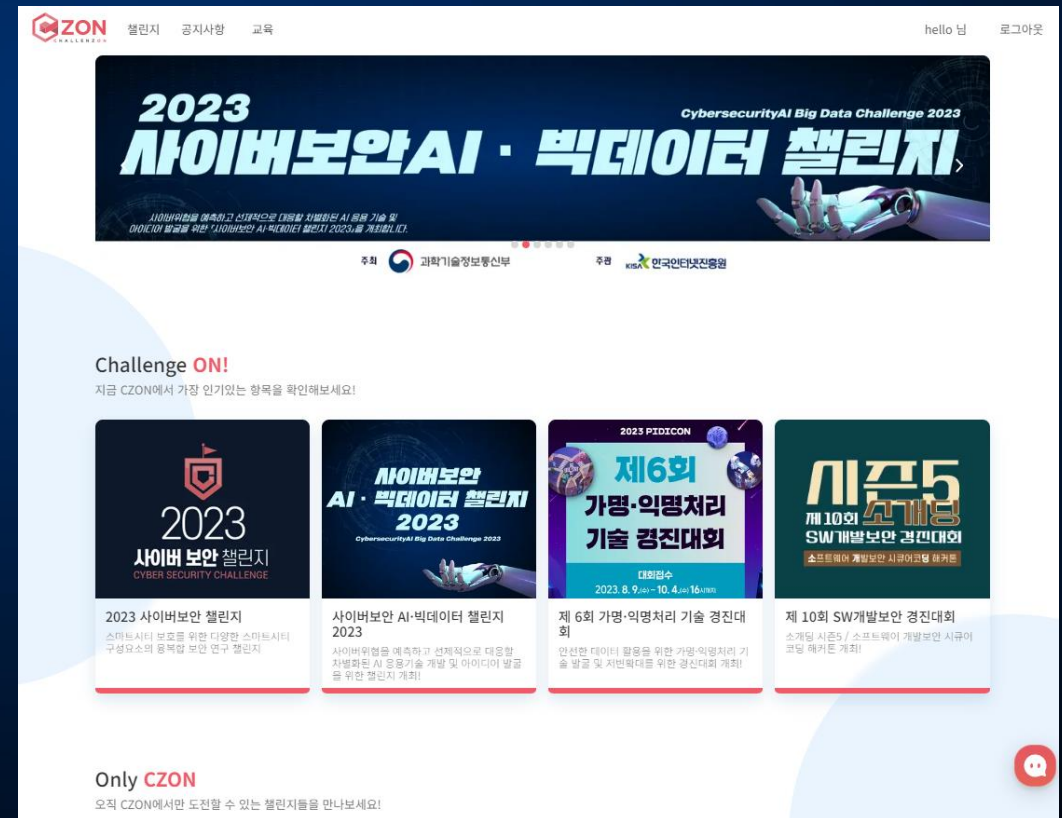
# 01 경연플랫폼 접속방법 - 챌린지 플랫폼

- 경진대회 홈페이지 | 대회소개, 대회일정, 신청접수, 시상내역, 대회자료(대회요강, 설명자료 등) 다운로드 등 대회 운영 홈페이지
- 챌린지 플랫폼 | 데이터셋 배포, 결과물 제출, 리더보드, 대회 공지사항 등 대회 참가 플랫폼

## 경진대회 홈페이지



## CZON(Challenge ON) 챌린지 플랫폼





## 회원가입 / 로그인

### 탭 설명

### 챌린지 참가 방법

### 팀 구성

### 제출방법

CZON.IO

## 회원가입 / 로그인

○ CZON 접속 (<https://czon.io>) ▶ 회원가입 버튼 클릭 ▶ 회원가입 페이지에 접속

**CZON 약관 동의**  
CZON을 이용하기 위해 약관에 동의하십시오.

- ☒ 모든 약관에 동의합니다.
- ☒ 이용약관에 동의합니다. (필수)
- ☒ 개인정보 수집·이용에 동의합니다. (필수)
- ☒ 마케팅 수신동의 수신에 동의합니다. (선택)

**동의합니다**

**1. 약관 동의**  
CZON을 이용하기 위해 약관에 동의하세요.

**이메일**  
CZON 계정에서 사용할 이메일 주소를 입력하십시오.

이메일:

**인증번호**

인증번호를 입력하십시오.  
인증번호를 받지 못한 경우, 이메일을 확인하십시오.  
인증번호를 받지 못한 경우, 이메일을 확인하십시오.  
인증번호를 받지 못한 경우, 이메일을 확인하십시오.

**인증번호 받기**

**2. 이메일 인증번호 발송/인증**  
CZON 계정에서 사용할 이메일 주소를 입력하세요.

**비밀번호**  
CZON 계정에서 사용할 비밀번호를 입력하십시오.

비밀번호:

비밀번호를 확인하십시오.  
비밀번호를 확인하십시오.  
비밀번호를 확인하십시오.

**비밀번호 확인**

**3. 비밀번호 입력 및 확인**  
CZON 계정에서 사용할 비밀번호를 입력하세요.

**이름**  
본인의 이름을 입력하십시오.

이름:

**성명**

성명:

**이메일**

이메일:

**비밀번호**

비밀번호:

**비밀번호 확인**

비밀번호 확인:

**가입하기**

**4. 사용자 성함 입력**  
본인의 이름을 작성해주세요.

**닉네임**  
CZON 계정에서 사용할 닉네임을 입력하십시오.

닉네임:

**닉네임 확인**

**5. 닉네임 입력**  
CZON 계정에서 사용할 닉네임을 입력하세요.

**정보확인**  
입력한 정보가 올바른지 확인하십시오.

이메일:

비밀번호:

비밀번호 확인:

닉네임:

**확인**

**6. 입력한 정보 확인 후 가입하기**  
입력한 정보로 계정이 가입됩니다.

**CZON 가입을 축하합니다!**

회원가입 완료  
지금 바로 로그인하여 활동하세요!

**로그인**

**7. 회원가입 완료**  
CZON에 로그인이 가능합니다.





회원가입 / 로그인

탭 설명

챌린지 참가 방법

팀 구성

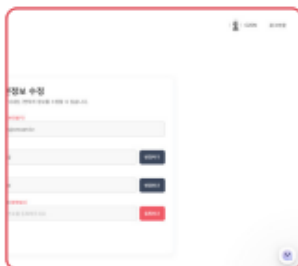
제출방법

CZON.IO

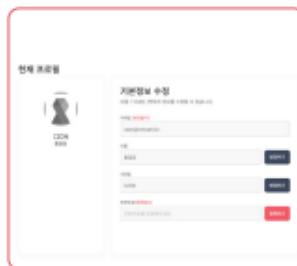
## 기본정보수정

CZON 로그인 ▶ 프로필 사진 클릭 ▶ 마이페이지에 접속

인증할 전화번호 입력 ▶ 전화번호 인증번호 발송 ▶ 인증번호 인증 ▶ 인증 완료 여부 확인



**1. 프로필 사진을 클릭**  
오른쪽 상단에 있는 프로필 사진을 클릭하세요.



**2. 마이페이지에 접속**  
이름/이메일/연락처 정보를 수정할 수 있습니다.



**3. 인증할 전화번호 입력**  
전화번호를 입력하시고 인증번호를 발송하세요.



**4. 인증 완료 여부 확인**  
인증번호를 인증하고 완료 여부를 확인하실 수 있습니다.







회원가입 / 로그인

챌린지 탭 소개

챌린지 참가 방법

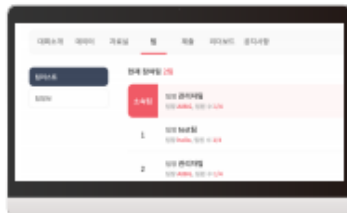
팀 구성

제출방법

CZON.IO

## 챌린지 탭 소개

### 팀 | 제출



#### 팀\_팀 리스트

##### 챌린지 활동을 위한 팀을 구성함

챌린지를 진행하기에 앞서 팀을 구성해야 합니다.  
본인이 소속한 팀의 팀명과 팀장, 팀원 수를 확인할 수 있습니다.  
본 대회에 어떤 팀이 참가했는지 볼 수 있습니다.  
※ 개인(1인) 팀의 경우 개인으로 팀을 생성해야 합니다.  
※ 구성할 수 있는 최대 팀원 수는 대회마다 상이합니다.



#### 팀\_팀 정보

소개수령: 팀 소개 수령  
팀 삭제: 팀의 멤버가 없을 경우 팀을 삭제함  
팀원 리스트: 팀장, 팀원리스트 출력 / 팀장과 팀원의 합은 총 인원을 넘을 수 없음  
추방하기: 팀 멤버를 선택하고 '추방하기' 클릭 시 팀에서 해당 멤버를 제거함  
승인하기: 신청리스트에서 신청자 선택 후 클릭 시 신청자를 팀 멤버로 등록함  
거절하기: 신청리스트에서 신청자 제거



#### 제출

##### 챌린지 결과물을 업로드 할 수 있음

제출할 수 현황: 최대 제출 횟수 및 제출 현황 조회 가능  
선택된 파일: 제출하기 전 업로드할 파일 확인  
※ 한 번 제출한 파일은 취소할 수 없습니다.





회원가입 / 로그인

챌린지 탭 소개

챌린지 참가 방법

팀 구성

제출방법

CZON.IO

## 챌린지 탭 소개

제출 | 리더보드 | 공지사항



### 제출

챌린지 결과물을 업로드 할 수 있음

제출 정보 : 제출 정보를 통해 업로드한 결과물의 채점결과를 조회할 수 있음  
※ private 점수의 경우 대회 종료 시 공개됩니다.  
※ 파일 형식 : csv 파일만 가능



### 리더보드

현재 대회 순위 조회

public / private : 카테고리 별 순위 조회 가능  
※ public : 일부 데이터에 대한 예과 결과 채점 점수  
※ private : 나머지 데이터에 대한 예과 결과 채점 점수  
※ private 점수의 경우 대회 종료 시 공개됩니다.



### 공지사항

공지사항 : 안내사항 또는 유의사항 안내  
시스템 : 시스템 점검 또는 기능추가 안내  
이벤트 : 챌린지 별 이벤트 참가방법 안내







○ 회원가입 / 로그인

○ 챌린지 탭 소개

● 챌린지 참가 방법

○ 팀 구성

○ 제출방법

CZON.IO

## 챌린지 참가 방법

### 대회 참가 프로세스



#### 챌린지 참가

참가신청 중인 챌린지에 접속  
챌린지 내의 [참가하기] 버튼을 클릭



#### 챌린지 참가

추가정보 (소속, 유형)를 입력  
대회 참여 약관에 동의  
작성완료 버튼을 클릭



- 회원가입 / 로그인
- 챌린지 탭 소개
- 챌린지 참가 방법
- 팀 구성
- 제출방법

CZON.IO

## 팀 구성

### 팀 생성 | 팀 참가



#### 팀 생성

챌린지 활동을 위한 팀을 구성함

팀 탭 내의 [팀 생성하기] 버튼 클릭

팀 생성하기 창에 정보 입력

[생성] 버튼 클릭

#### 팀 참가

챌린지 활동을 위한 팀을 구성함

현재 참여팀 확인

[참가신청] 버튼으로 팀 참가

- 경진대회 홈페이지 | 대회소개, 대회일정, 신청접수, 시상내역, 대회자료(대회요강, 설명자료 등) 다운로드 등 대회 운영 홈페이지
- 챌린지 플랫폼 | 데이터셋 배포, 결과물 제출, 리더보드, 대회 공지사항 등 대회 참가 플랫폼

## 플랫폼 메인페이지

Challenge ON!  
지금 CZON에서 가장 인기있는 항목을 확인해보세요!

Only CZON  
오직 CZON에서만 도전할 수 있는 챌린지들을 만나보세요!

사이버 보안 AI·빅데이터 챌린지 2023 [A트랙] - 예선  
27,000,000원  
참가 신청 시작 D-22

## 예선/본선 페이지

사이버 보안 AI·빅데이터 챌린지 2023 [A트랙] - 예선  
참가 신청 시작 D-22

사이버 보안 AI·빅데이터 챌린지 2023 [A트랙] - 예선  
사이버 보안 AI·빅데이터 챌린지 2023 [A트랙] - 예선  
사이버 보안 AI·빅데이터 챌린지 2023 [A트랙] - 예선

대회소개 | 데이터 | 자료실 | 팀 | 제출 | 리더보드 | 공지사항

【대회소개】  
과학기술정보통신부와 한국인터넷진흥원에서는 사이버보안 AI 응용기술의 혁신을 선도할 아이디어와 AI 우수인재 발굴을 위해 사이버보안 AI·빅데이터 챌린지 2023을 개최하오니 관심있는 분들의 많은 참여 바랍니다.

【참가자격】  
사이버보안 AI 빅데이터 활용에 관심이 있는 대한민국 국민 누구나  
\* 개인 또는 단체(4인 이하)로 참여 가능

【대회일정】

	A트랙	B트랙	C트랙
예선	2023. 09. 15(월) ~ 2023. 12. 07(목)		
본선			

- 경진대회 홈페이지 | 대회소개, 대회일정, 신청접수, 시상내역, 대회자료(대회요강, 설명자료 등) 다운로드 등 대회 운영 홈페이지
- 챌린지 플랫폼 | 데이터셋 배포, 결과물 제출, 리더보드, 대회 공지사항 등 대회 참가 플랫폼

## 데이터 다운로드 페이지 (예선/본선 동일)

사이버 보안 AI·빅데이터 챌린지 2023 [A트랙] - 예선

참가 신청 시작 D-22

AI를 통해 웹 방화벽 로그를 분석하고, 비정상 행위를 분류하라!

2023. 09. 15(월) ~ 2023. 12. 07(목)

₩ 27,000,000원

과학기술정보통신부 | 한국인터넷진흥원

참가시작전

대회소개 **데이터** 자료실 팀 제출 리더보드 공지사항

데이터 소개

### 사이버보안 AI·빅데이터 챌린지 2023

[ 데이터 소개 ]

로그유형 : 웹방화벽(WAF) 로그

[ 학습셋 ] [다운로드](#)

## 자료실 다운로드 페이지 (답안지, 기술보고서, 발표자료)

사이버 보안 AI·빅데이터 챌린지 2023 [A트랙] - 예선

참가 신청 시작 D-22

AI를 통해 웹 방화벽 로그를 분석하고, 비정상 행위를 분류하라!

2023. 09. 15(월) ~ 2023. 12. 07(목)

₩ 27,000,000원

과학기술정보통신부 | 한국인터넷진흥원

참가시작전

대회소개 데이터 **자료실** 팀 제출 리더보드 공지사항

자료실 소개

[ 자료실 소개 ]

※ 사이버 보안 AI·빅데이터 챌린지 자료실입니다.

[ 자료 다운로드 ] [다운로드](#)

- 결과파일 [답안]
- 기술보고서



## 예·본선 기술경연 진행방식

- **결과물 제출** | 답안지, 기술보고서는 챌린지 플랫폼에 업로드 제출
- **답안지 제출기회** | 경연시간 內 총 5회까지 제출 가능
- **최종결과** | 가장 **마지막**에 제출한 답안지의 점수로 결과반영
- **기술보고서** | 경연시간 內 **마지막 제출된** 보고서로 평가 실시
- **서면평가** | 제출받은 보고서로 평가위원회 서면평가 별도 실시
- **리더보드** | 리더보드를 통해 팀별 실시간 분류정확도 비교경쟁

## 리더보드 확인 방법 (경연플랫폼)

대회소개	데이터	자료실	팀	제출	리더보드	공지사항
PUBLIC	PRIVATE					
순위	팀명	점수	제출시간			
1	null2root	0.97008	2022-10-21 13:21:46.802545			
2	빅마우스	0.96192	2022-10-21 15:55:40.93787			
3	Xransformer	0.96187	2022-10-21 14:34:55.86616			
4	네모세모	0.9573	2022-10-21 16:57:15.139417			

## 본선 발표경연 진행방식

- **결과물 제출** | 발표자료는 챌린지 플랫폼에 업로드 제출
- **발표자료** | 제출시간 內 **마지막 제출된** 자료로 평가 실시  
※ 제출시간 : 11.16(목), 17:00까지
- **오프라인 평가** | 오프라인 심사장에 참석하여 발표 평가
- **진행방식** | 발표자료 제출의 역순으로 발표  
※ 팀별 발표시간 별도 공지예정
- **평가시간** | 15분 발표 + 10분 질의 (±5분)

## 유의사항

- 본선진출팀/수상자 발표는 부정행위 확인 및 결과 집계 후, **대회 홈페이지**를 통해 발표
- 이의제기에 따라 수상팀은 변경될 수 있음
- 대회규칙 내 이의제기 기간 이후에는 이의신청 받지 않음  
(이의신청 기간 : 수상자 발표 후 2일 이내)
- 제출 마감시간 이후에는 결과물 제출받지 않음(시간엄수)

## 챌린지 플랫폼의 제출 탭을 통해 결과물 제출

대회소개 데이터 자료실 팀 **제출** 리더보드 공지사항

제출횟수 현황 3/5

클릭하여 제출할 파일을 선택해주세요.

선택된 파일

파일명	확장자	용량

제출하기

제출정보  
private 전수는 대회 종료 후 공개됩니다.

제출순서	제출자	제출일자	파일명	public	private	기타 메시지
24	SYSNAR	2022-08-23T17:14:29.607712	example_team3csv	-	-	채점대기
23	SYSNAR	2022-08-23T17:02:06.647148	example_team3csv	-	-	채점대기
22	SYSNAR	2022-08-22T14:48:18.576135	test_answer (1)csv	1	-	채점완료
21	SYSNAR	2022-08-19T10:00:34.478165	test_answer (1)csv	1	-	채점완료
20	SYSNAR	2022-08-16T16:57:17.348619	test (1)csv	-	-	채점오류

결과물 제출 탭

제출할 파일을 찾아서 선택 혹은  
드래그&드롭하여 업로드

선택한 파일 리스트 확인

제출하기 버튼을 클릭하여 제출

※ 한 번 제출한 제출물은 수정이 불가하오니, 유의하시어 업로드 바랍니다.

횟수별 제출물 정보 확인

# 사이버보안 AI · 빅데이터 챌린지 2023

CybersecurityAI Big Data Challenge 2023

## 기타 챌린지 문의



홈페이지 內 채널톡

[aibigdata@cmcom.kr](mailto:aibigdata@cmcom.kr) / 070-4849-4535

주최



과학기술정보통신부

주관



한국인터넷진흥원