K-Shield Jr.

머신러닝을 활용한

네트워크 이상탐지

Outsider

김태영, 박수곤, 송지민, 유다정, 이기훈

Contents

K-Shield Jr.

01

프로젝트 개요

- ✓ 배경
- ✓ 관련연구
- ✓ 목표
- ✓ 역할

02

CICIDS 2017

- ✓ 진행순서
- ✓ 데이터 수집
- ✓ 전처리
- ✓ 모델링 (KNN)
- ✓ 한계점, 중단이유

03

KISA challenge 2019

- ✓ 진행순서
- ✓ 데이터 수집
- ✓ 전처리
- ✓ 모델링
- ✓ 추후 연구방안

04

SIEM + ELK 시스템

- ✓ 진행순서
- ✓ 환경구축
- ✓ 네트워크 구성도
- ✓ 특징공학
- ✓ 모델링
- ✓ 시각화

05

결론& 추후계획

#1 배경

Machine learning

- ✓ **Supervised**
- ✓ **Unsupervised**
- ✓ **Deep learning**

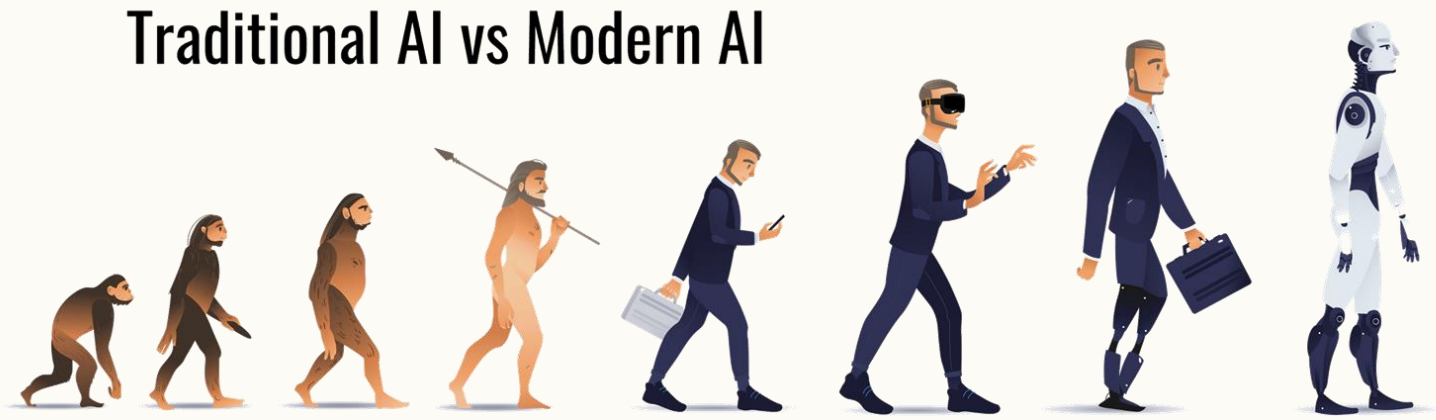
AI
(Artificial intelligence)

Curated

- ✓ **knowledge**

Reverse

- ✓ **Engineering brain**



#1 배경

소셜 미디어와 , 인터넷의 발전으로 인한 **데이터**와 **정보**의 **가치 상승**

안전하게 **보관**, 보호라는 방안과 **고민과 관심도의 상승**

손실로 인한 **사회**, **경제적 문제와 심각성 증가**

기업의 **빅데이터**, 인공지능의 **활용**, **연구**로 인한 **분석**, **보안** 활용시 **효율성과 필요성 제기**

#1 배경

K-Shield Jr.

사람

수집 ▶ 정제 ▶ 탐색 ▶ 모델링 ▶ 해석

기계

수집 ▶ 전처리 ▶ 모델학습 ▶ 예측

#1 배경

K-Shield Jr.

금융 업계의 머신러닝 도입, 사기 방지부터 시작하라

좋아요 19개 | 입력 : 2019-06-24 11:04

#정보보호 #정보

각종 IT 기술 빠르게

사기 방지 전문가들

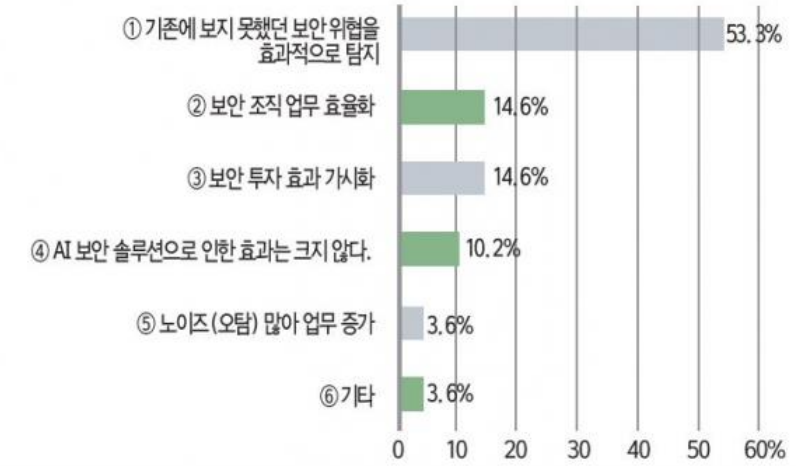
HOME > 뉴스 > 보안

[2020 보안 담당자 설문조사③] AI 보안 솔루션 '긍정'

김선애 기자 | 승인 2020.02.04 09:00 | 댓글 0

> AI 보안 솔루션, 보안 탐지 효과 높다 평가하면서도 도입은 '주저'
> "AI 악용공격 우려 높지만 진화하는 공격 방어 위해 필요"

〈그림 6〉 AI 활용 보안 솔루션 효과는



(자료 : 네트워크타임즈 '2020 보안 담당자 설문조사')

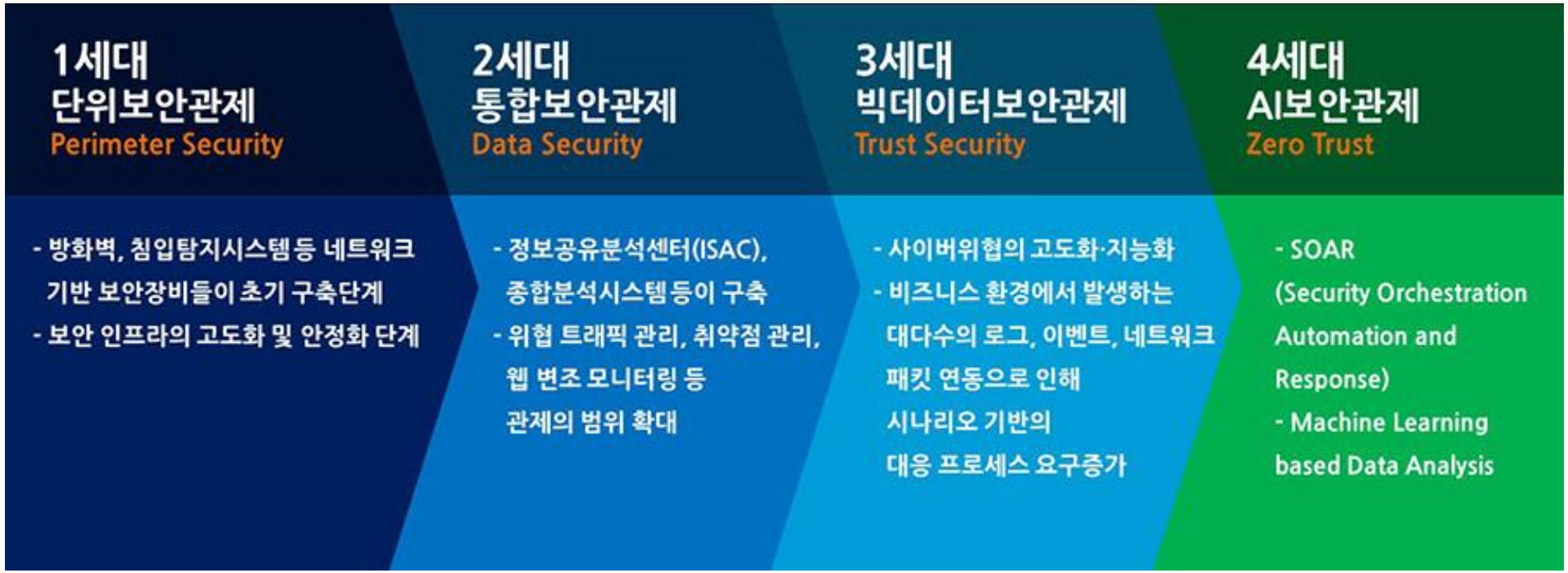
#1 배경

빠르게 발전하는 IT산업시대에서 **네트워크**를 통한 사이버 공격들이 점점 고도화됨에 따라

신종 또는 변종 공격방식을 탐지하기 위해 **머신러닝에 침입 탐지 시스템**을 접목한 기술들이

최근에 주목받고 있다.

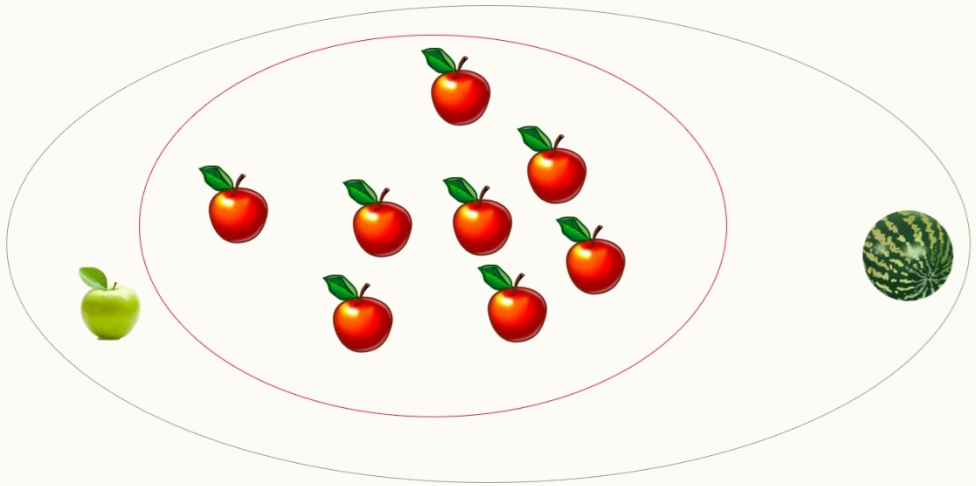
#1 배경


1세대
단위보안관제
Perimeter Security
- 방화벽, 침입탐지시스템 등 네트워크 기반 보안장비들이 초기 구축단계
- 보안 인프라의 고도화 및 안정화 단계
2세대
통합보안관제
Data Security
- 정보공유분석센터(ISAC), 종합분석시스템 등이 구축
- 위협 트래픽 관리, 취약점 관리, 웹 변조 모니터링 등 관제의 범위 확대
3세대
빅데이터보안관제
Trust Security
- 사이버위협의 고도화·지능화
- 비즈니스 환경에서 발생하는 대다수의 로그, 이벤트, 네트워크 패킷 연동으로 인해 시나리오 기반의 대응 프로세스 요구증가
4세대
AI보안관제
Zero Trust
- SOAR (Security Orchestration Automation and Response)
- Machine Learning based Data Analysis

#1 배경

“이상(Anomaly)이란?”

정상과 비정상(이상)의 구분은 주관적 개념일 뿐이다.



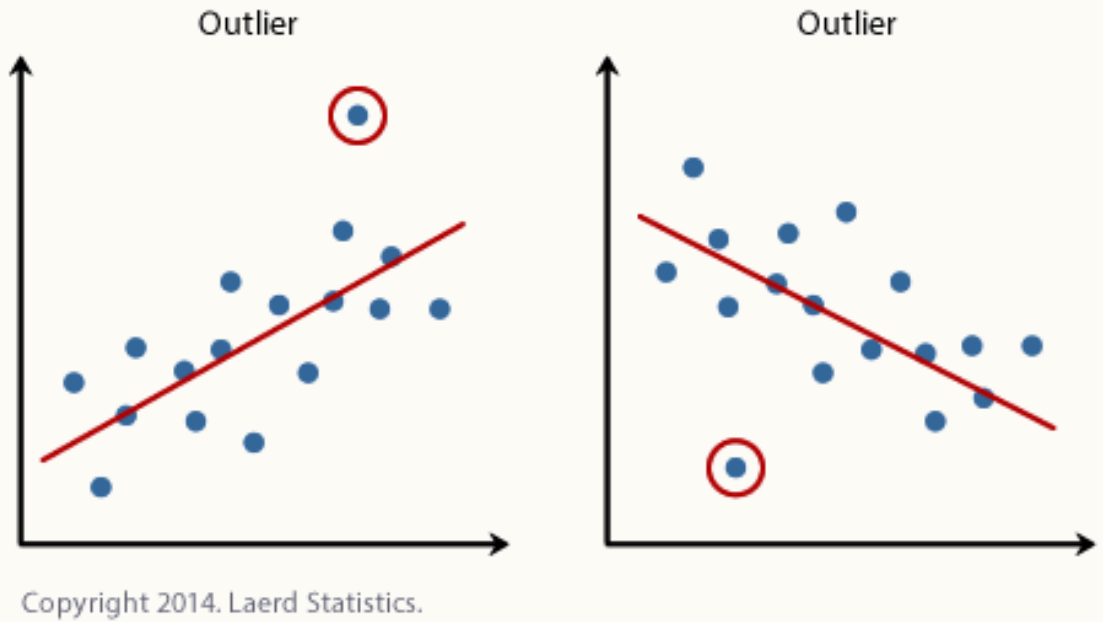
사과의 경계 주위에 청사과와 수박이 있다.

→ “과연 수박도 모양만 봤을 때는 동그란데 사과라고 해야 하나?”

#1 배경

이상 탐지(anomaly detection)란 자료에서 예상과는 다른 패턴을 보이는 개체 또는

자료를 찾는 것을 일컫는다.



#1 관련연구

- Evaluation of Network Intrusion Detection with Features Selection and Machine Learning Algorithms on CICIDS-2017 Dataset

  - Mr. Shailesh Singh Panwara, Dr. Y. P. Raiwanib, Mr. Lokesh Singh Panwarc

- IOT 환경에서의 오토인코더 기반 특징 추출을 이용한 네트워크 침입 탐지 시스템

  - 정보처리학회논문지. 소프트웨어 및 데이터 공학

- 머신러닝을 활용한 IDS 구축 방안 연구

  - 한국소프트웨어 감정평가 학회 논문지

#1 목표

K-Shield Jr.

- **비지도학습**을 기반으로 알려지지 않은 위협과 기존에 없던 행위에 대한 판별을 탐지한다.
- 로그 시각화를 통한 Anomaly detection **탐지율 향상** 시킨다.
- **이상 치**에 대한 명세 정리 및 속성별 유형을 파악한다.
- 로그와 다양한 이벤트를 머신러닝을 통한 학습을 통해, 관제 인력이 파악하기 힘든 공격징후를 파악하여 **오탐을 줄일 수 있는 방향**으로 활용

#2 역할

데이터 수집

1.네트워크 침입 시나리오 데이터 수집

데이터 분석

1.데이터셋 패턴 분석

2.중요 데이터 선별

모델링

1.모델 튜닝

2.학습 모델 성능 평가

3. 최적화

#2 역할

K-Shield Jr.

김태영	박수곤	송지민	유다정	이기훈
● CICIDS2017 데이터셋 전처리 ● 피쳐추출 ● KNN 알고리즘 적용	● 자료조사 ● ELK구축	● CICIDS2017 데이터셋 전처리 ● KISA Challenge 2019 데이터셋 전처리 ● 피쳐추출 ● 모델링	● CICIDS2017 데이터셋 피쳐추출 ● SIEM & ELK 구축 ● 가상환경 네트워크 데이터 수집 ● 특징 추출 ● 모델링	● CICIDS2017 데이터셋 수집

#2 수행일정

K-Shield Jr.

구분	추진내용	프로젝트 기간(주간)									
		1	2	3	4	5	6	7	8	9	10
계획	팀구성 / 주제설정	◆									
조사	기능 정의/ 명세		◆	◆							
설계	데이터 수집			◆	◆		◆			◆	
	환경구축			◆	◆				◆	◆	
분석	데이터 분석				◆	◆	◆	◆	◆	◆	◆
	특징 공학					◆	◆	◆	◆	◆	◆
	모델링								◆	◆	◆
종료	시각화										◆

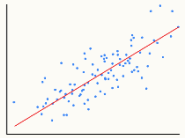
K-Shield Jr.

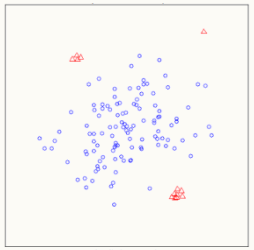
#02 CICIDS 2017

1주차~5주차

#2 진행순서

Intrusion Detection Evaluation Dataset (CICIDS2017)





자료조사

- 머신러닝 보안 동향 분석
- 머신러닝 공부

데이터 수집/ 분석

- CICIDS 2017

feature 추출

- Feature 추출
- Feature 선정

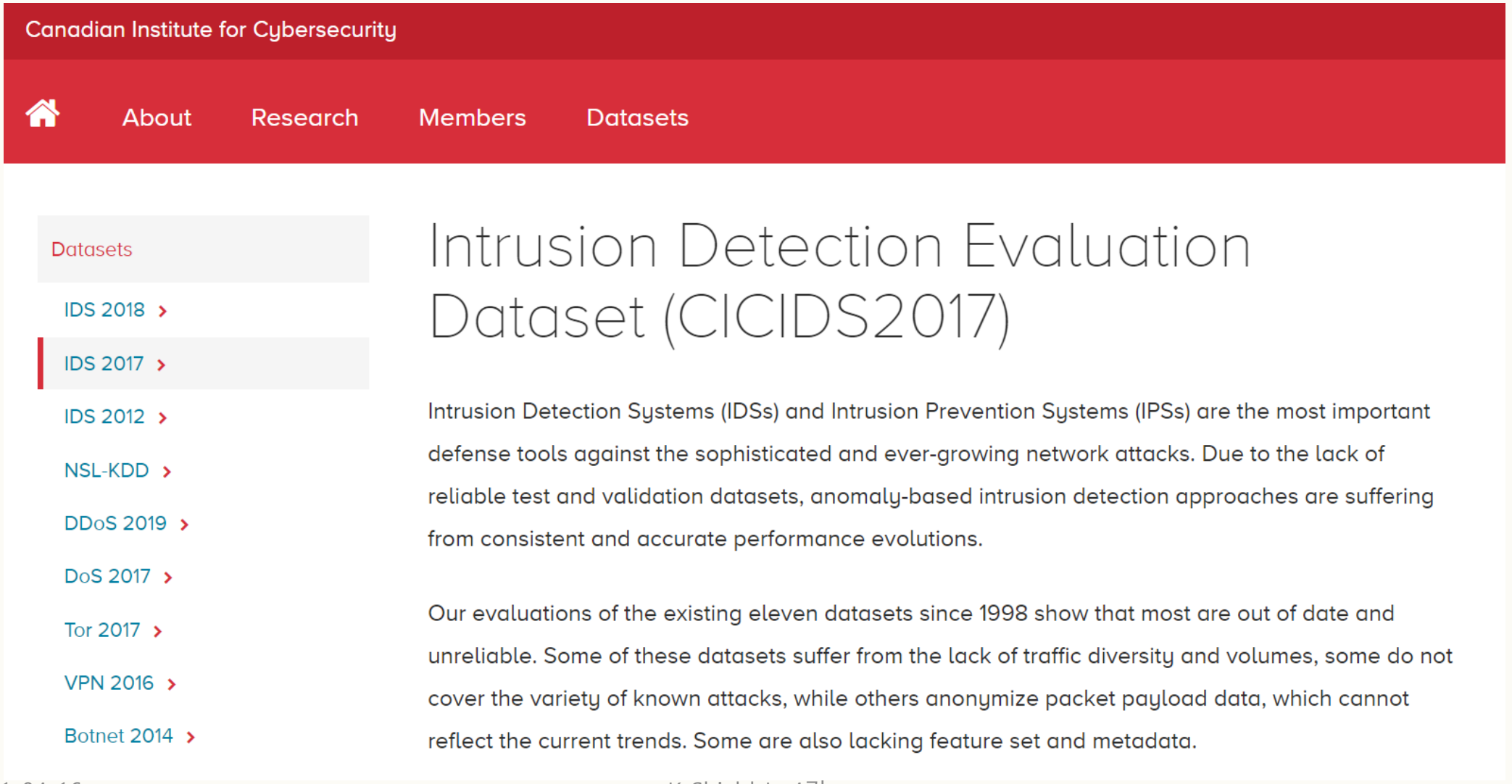
모델링

- 알고리즘
- 최적화

CICIDS2017

#2 데이터 수집

K-Shield Jr.



#2 데이터수집

이름	수정한 날짜	유형	크기
Friday-WorkingHours-Afternoon-DDos.pcap_ISCX	2020-06-18 오후 1:03	Microsoft Excel ...	93,110KB
Friday-WorkingHours-Afternoon-PortScan.pcap_ISCX	2020-06-18 오후 1:03	Microsoft Excel ...	98,354KB
Friday-WorkingHours-Morning.pcap_ISCX	2020-06-18 오후 1:03	Microsoft Excel ...	72,854KB
Monday-WorkingHours.pcap_ISCX	2020-06-18 오후 1:04	Microsoft Excel ...	225,887KB
Thursday-WorkingHours-Afternoon-Infilteration.pcap_ISCX	2020-06-18 오후 1:03	Microsoft Excel ...	105,019KB
Thursday-WorkingHours-Morning-WebAttacks.pcap_ISCX	2020-06-18 오후 1:04	Microsoft Excel ...	64,950KB
Tuesday-WorkingHours.pcap_ISCX	2020-06-18 오후 1:04	Microsoft Excel ...	168,801KB
Wednesday-workingHours.pcap_ISCX	2020-06-18 오후 1:04	Microsoft Excel ...	276,140KB

#2 데이터 분석

파일 이름	요일	유형
Monday-WorkingHours	월요일	정상 데이터
Tuesday-WorkingHours	화요일	정상, 공격
Wednesday-WorkingHours	수요일	공격
Thursday-WorkingHours-morning	목요일	공격
Thursday-WorkingHours-afternoon		공격
Friday-WorkingHours-morning	금요일	공격
Friday-WorkingHours-Afternoon_PortScan		공격
Friday-WorkingHours-Afternoon_DDos		공격

CICIDS2017

#2 데이터 수집

K-Shield Jr.

	Destination Port	Flow Duration	Total Fwd Packets	Total Backward Packets	Total Length of Fwd Packets	Total Length of Bwd Packets	Fwd Packet Length Max	Fwd Packet Length Min	Fwd Packet Length Mean	Fwd Packet Length Std	Bwd Packet Length Max	Bwd Packet Length Min	Bwd Packet Length Mean	Bwd Packet Length Std	Flow Bytes/s	Flow Packets/s	Flow IAT Mean	Flow IAT Std
0	54865	3	2	0	12	0	6	6	6.00000	0.00000	0	0	0.00000	0.00000	4000000.00000	666666.66670	3.00000	0.00000
1	55054	109	1	1	6	6	6	6	6.00000	0.00000	6	6	6.00000	0.00000	110091.74310	18348.62385	109.00000	0.00000
2	55055	52	1	1	6	6	6	6	6.00000	0.00000	6	6	6.00000	0.00000	230769.23080	38461.53846	52.00000	0.00000
3	46236	34	1	1	6	6	6	6	6.00000	0.00000	6	6	6.00000	0.00000	352941.17650	58823.52941	34.00000	0.00000
4	54863	3	2	0	12	0	6	6	6.00000	0.00000	0	0	0.00000	0.00000	4000000.00000	666666.66670	3.00000	0.00000

```
        Destination Port  Flow Duration  ...  Idle Min   Label
0                  54865              3  ...         0  BENIGN
1                  55054            109  ...         0  BENIGN
2                  55055             52  ...         0  BENIGN
3                  46236             34  ...         0  BENIGN
4                  54863              3  ...         0  BENIGN
...                  ...            ...  ...       ...     ...
692698                53          32215  ...         0  BENIGN
692699                53            324  ...         0  BENIGN
692700             58030             82  ...         0  BENIGN
692701                53        1048635  ...         0  BENIGN
692702                53          94939  ...         0  BENIGN

[2830743 rows x 79 columns]
```

```
1  label_list = df[df.columns[-1]]
2  label_type = list(set(label_list))
3  for i in label_type:
4      print(i)
```

```
FTP-Patator
PortScan
DoS Slowhttptest
Bot
Infiltration
SSH-Patator
DDoS
Heartbleed
DoS GoldenEye
DoS Hulk
Web Attack  Sql Injection
BENIGN
Web Attack  XSS
Web Attack  Brute Force
DoS slowloris
```

CICIDS 2017 Dataset

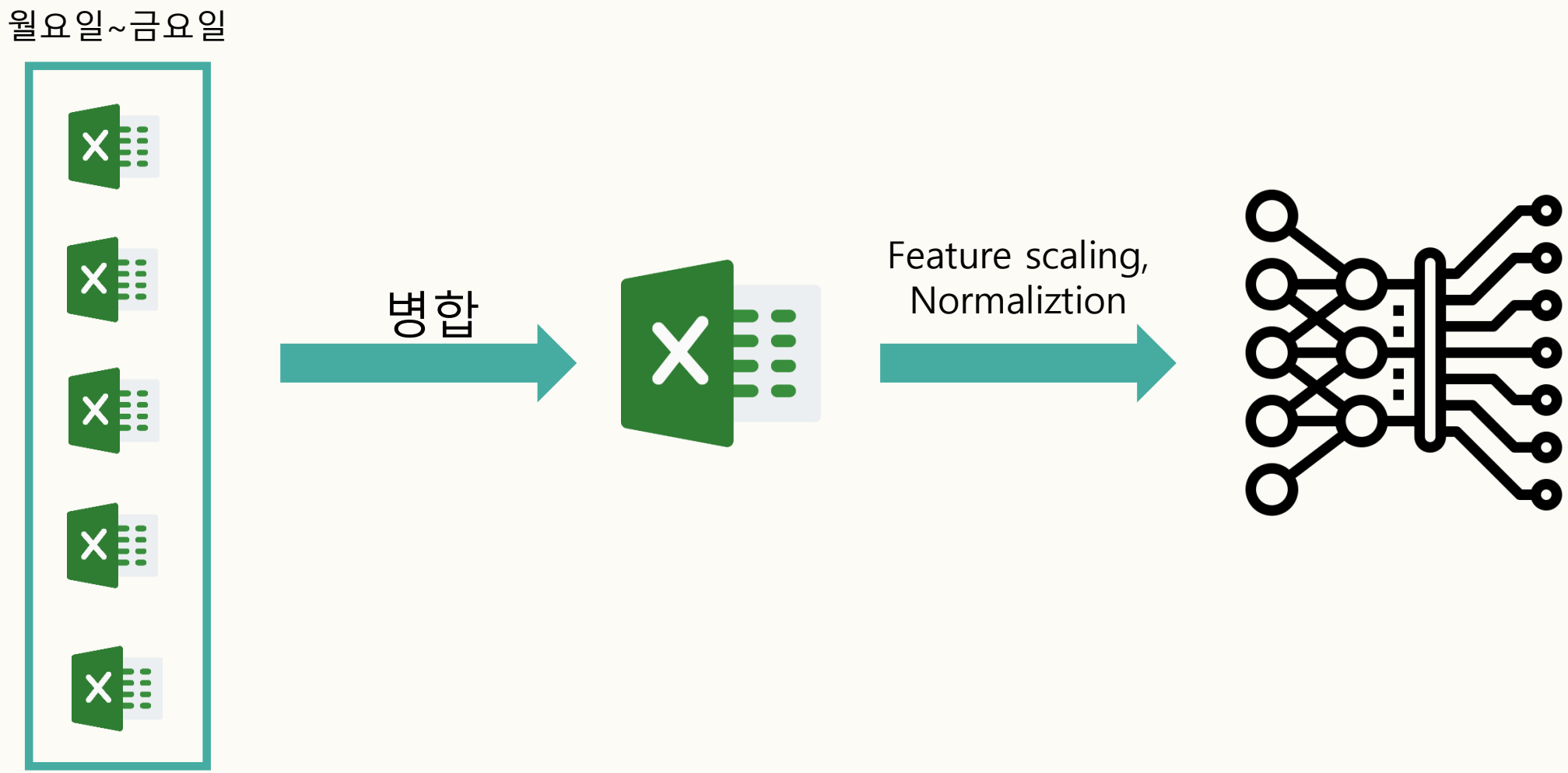
CICIDS2017

#2 데이터 분석

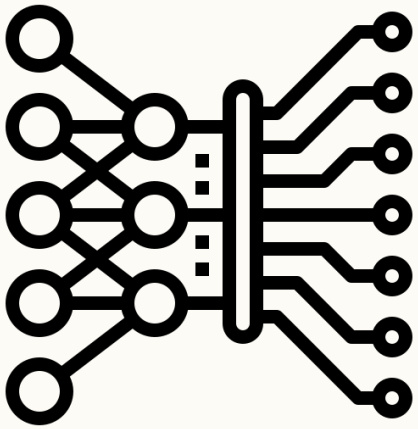
K-Shield Jr.

공격유형		개수	퍼센티지
Benign		2,273,097	80.3004%
Ddos		128,027	4.5227%
Port Scan		158,930	5.6441%
Bot		1,966	0.0695%
Infilteration		36	0.0013%
웹 공격	Brute Force	2,180	0.0770%
	SQL Injection		
	XSS		
FTP-Patator		7,938	0.2804%
SSH-Patator		5,897	0.2083%
Dos-GoldenEye		10,293	0.3636
Dos-Hulk		231,073	8.1630%
Dos-Slowhttptest		5,499	0.1943%
Dos-Slowloris		5,796	0.2048%
Heartbleed		11	0.0004%

#2 전처리



#2 모델링



TEST D: 0.2
Training D: 0.8

36 features

ANN

적용결과

99%
accuracy

#2 한계점

- 1. 정상 데이터와 공격 데이터의 비율

  -> 정상 데이터가 압도적으로 많음

- 2. 데이터셋 자체의 문제점으로 인한
  실제 네트워크 환경 적용의 어려움

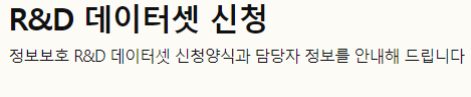
  -> 패킷에 공격 유형이 주기적으로 되어 있음

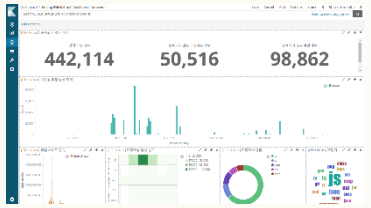
K-Shield Jr.

#03 KISA Challenge 2019

6주차~9주차

#3 진행순서





자료조사

- 비지도 알고리즘 학습

데이터 수집/ 분석

- KISA challenge 2019

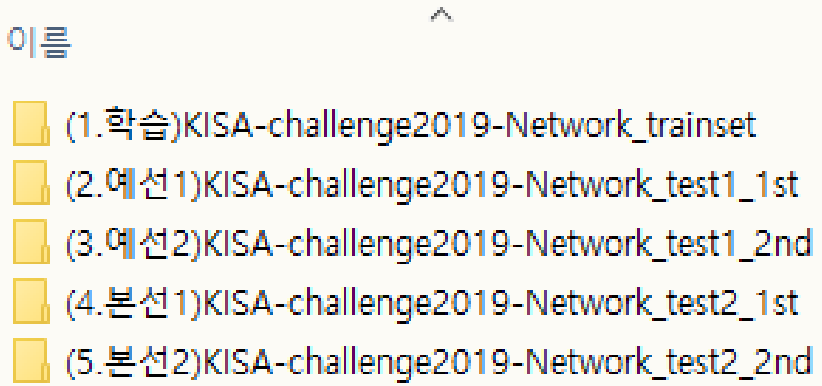
feature 추출

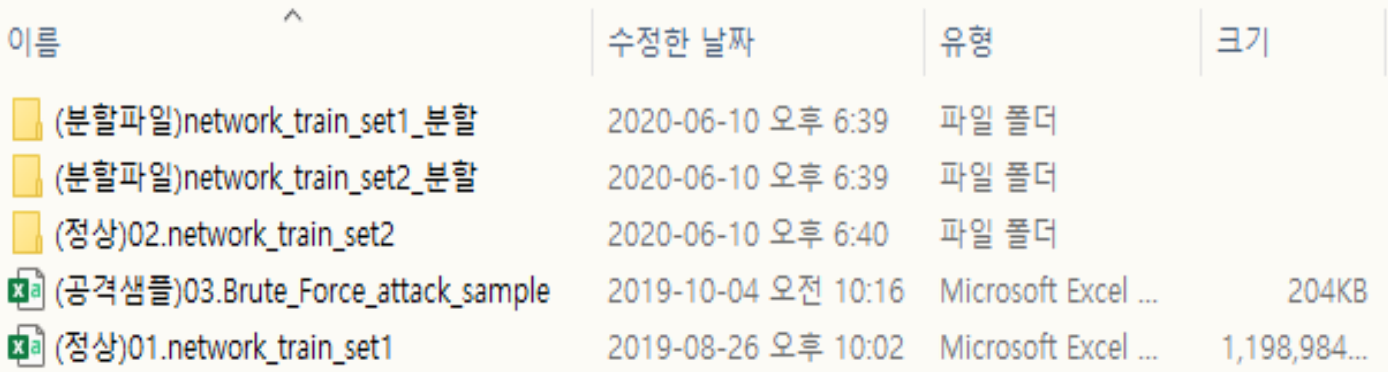
- Feature 추출
- Feature 선정

모델링

- 알고리즘
- 최적화

#3 데이터수집


이름
(1.학습)KISA-challenge2019-Network_trainset
(2.예선1)KISA-challenge2019-Network_test1_1st
(3.예선2)KISA-challenge2019-Network_test1_2nd
(4.본선1)KISA-challenge2019-Network_test2_1st
(5.본선2)KISA-challenge2019-Network_test2_2nd


이름
수정한 날짜
유형
크기
(분할파일)network_train_set1_분할
2020-06-10 오후 6:39
파일 폴더
(분할파일)network_train_set2_분할
2020-06-10 오후 6:39
파일 폴더
(정상)02.network_train_set2
2020-06-10 오후 6:40
파일 폴더
(공격샘플)03.Brute_Force_attack_sample
2019-10-04 오전 10:16
Microsoft Excel ...
204KB
(정상)01.network_train_set1
2019-08-26 오후 10:02
Microsoft Excel ...
1,198,984...

#3 데이터 분석

	학습			예선 1	예선 2
	train_set1	train_set2	공격_sample	test1_1st	test1_2nd
_ws.col.Protocol	55개	32개	2개	56개	58개
ip.src	9517개	9610개	2개	8481개	10373개
ip.dst	9568개	9825개	2개	8540개	6919개
Tcp.srcport	28920개	29920개	118개	37030개	
Tcp.dstport	28889개	28880개	118개	36920개	

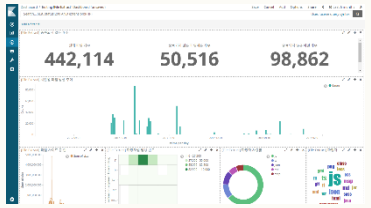
- ARP, CDP 프로토콜에는 해당 ip.src와 ip.dst가 존재하지 않는다.

K-Shield Jr.

#04 SIEM + ELK 시스템

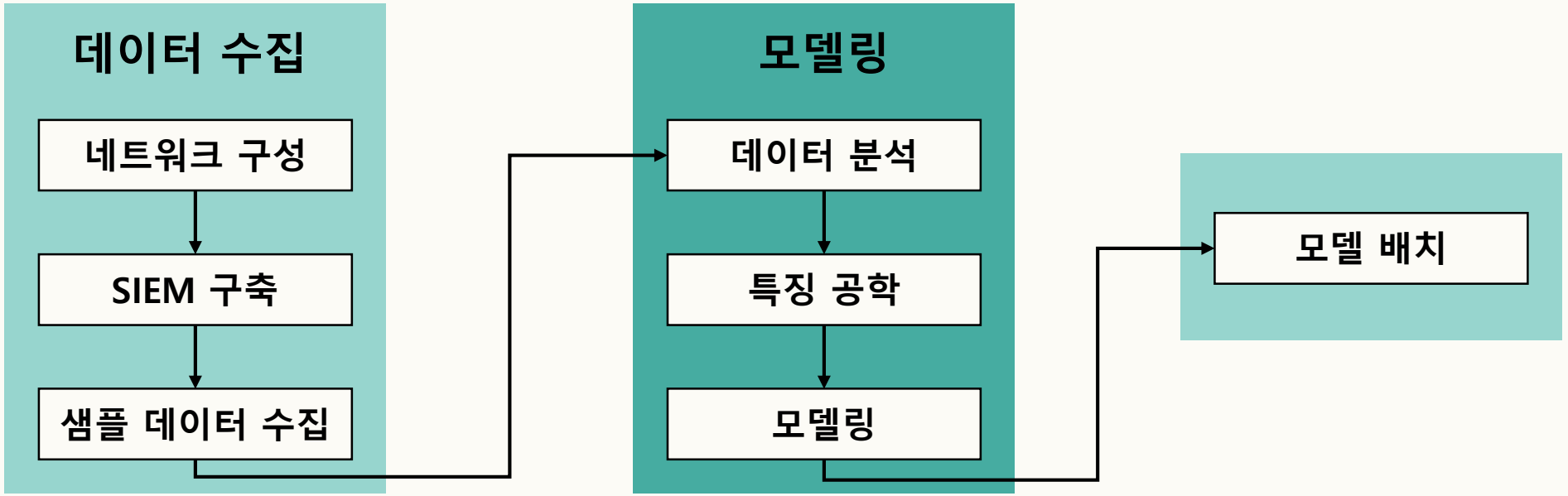
9주차~10주차

#4 진행순서



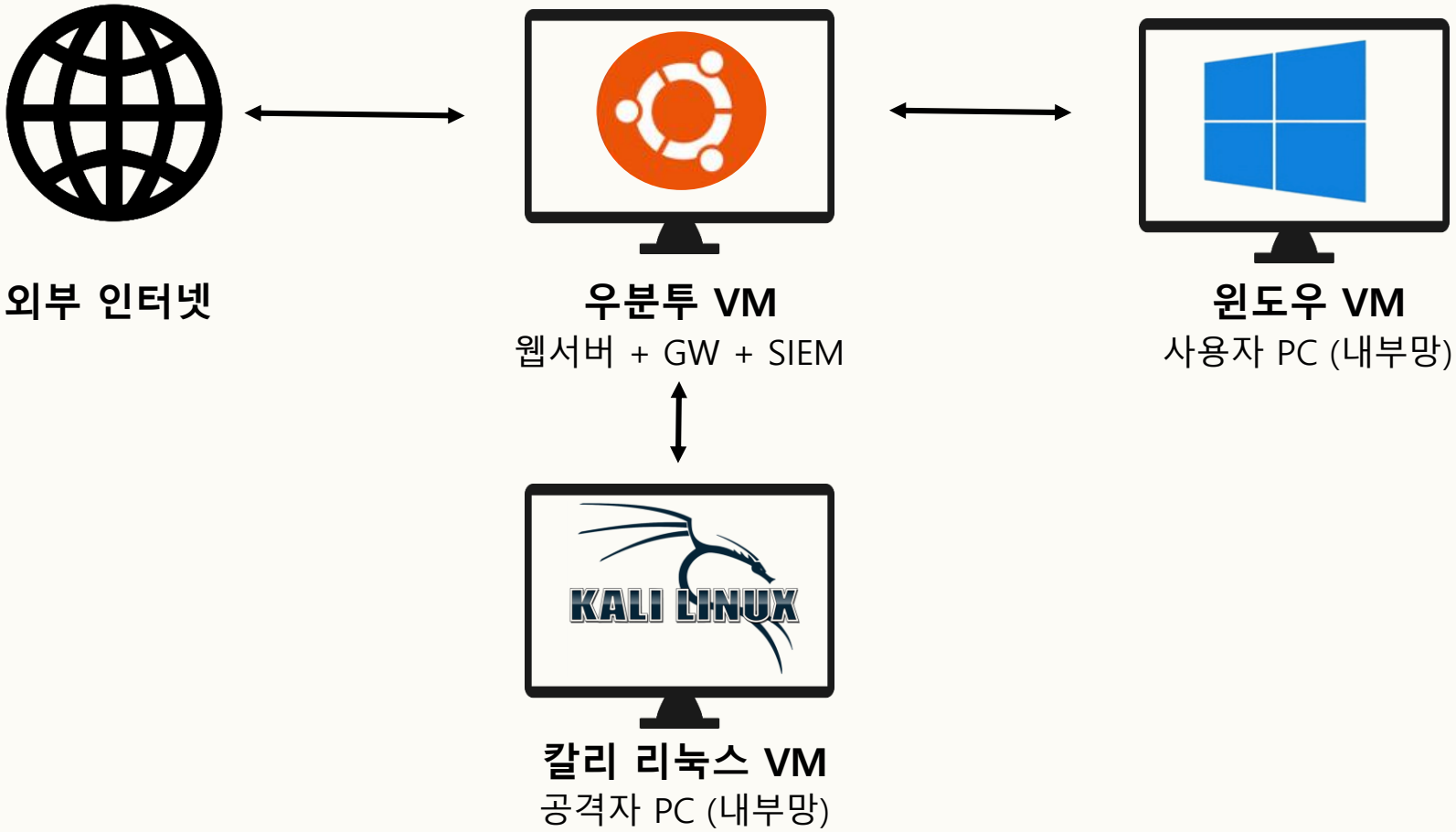
자료조사	데이터 수집/ 분석	feature 추출	모델링
▪ ELK스택 ▪ SIEM 구축	▪ 가상머신을 통해 네트워크 트래픽 생성 ▪ 칼리리눅스 (메타스플로잇)	▪ IDS 로그 탐지 ▪ Elasticsearch DSL ▪ 인덱스 생성/저장	▪ 비지도학습 ▪ UI제작

#4 환경구축



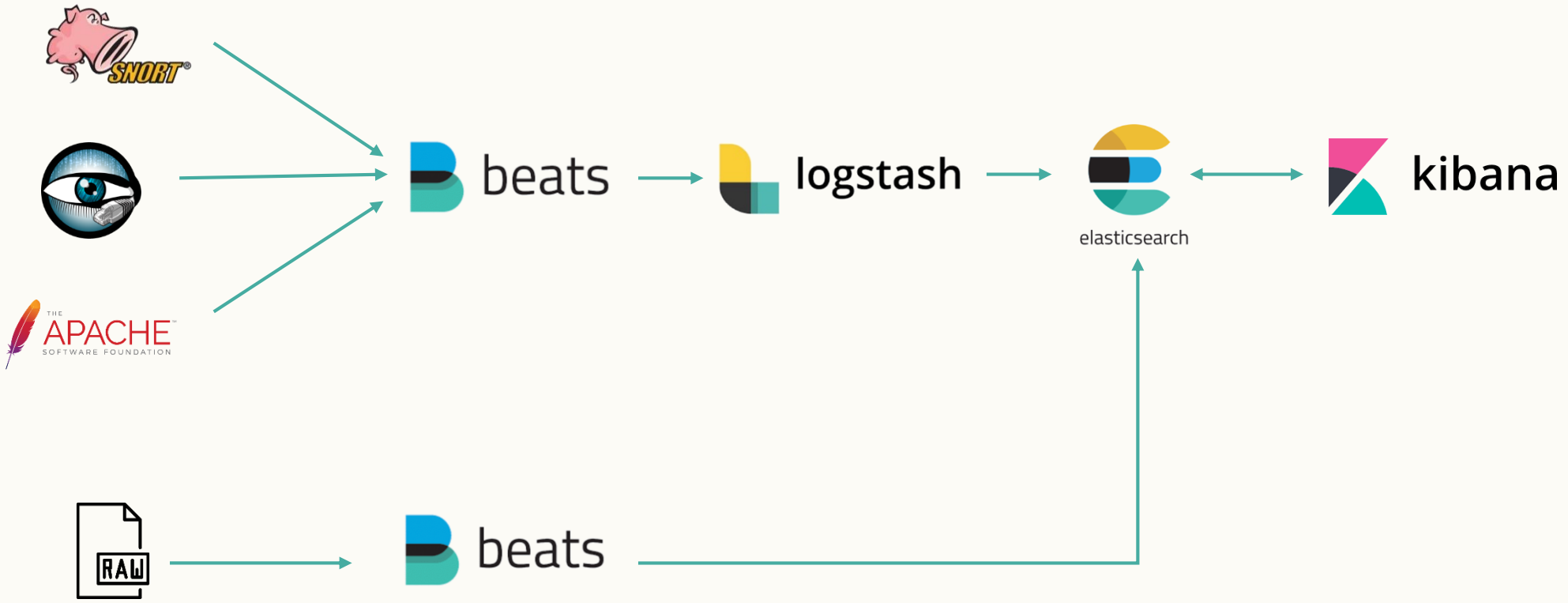
프로젝트 진행 과정

#4 네트워크 구성도



가상머신을 이용한 프로젝트 실습 환경 구성

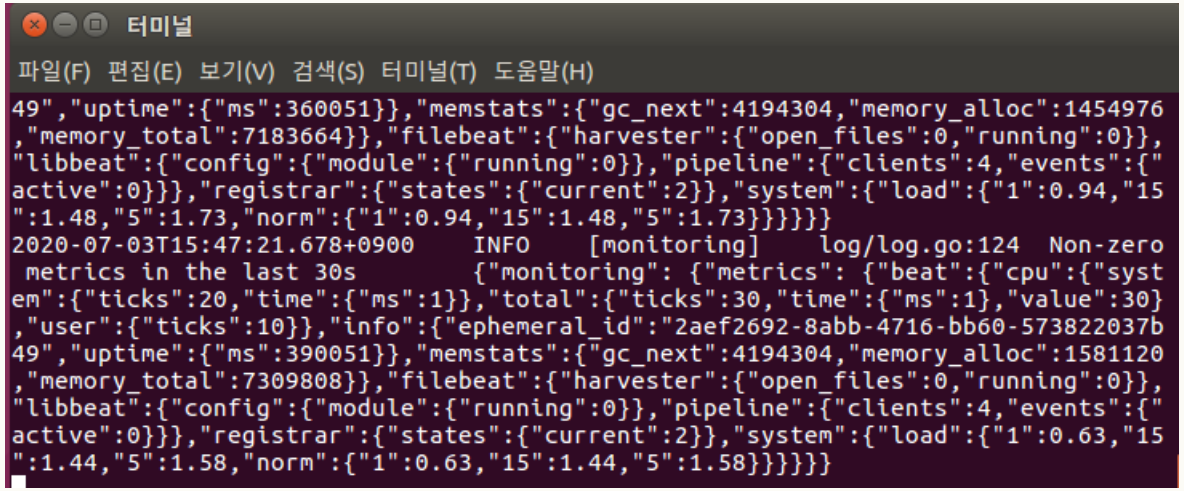
#4 환경구축



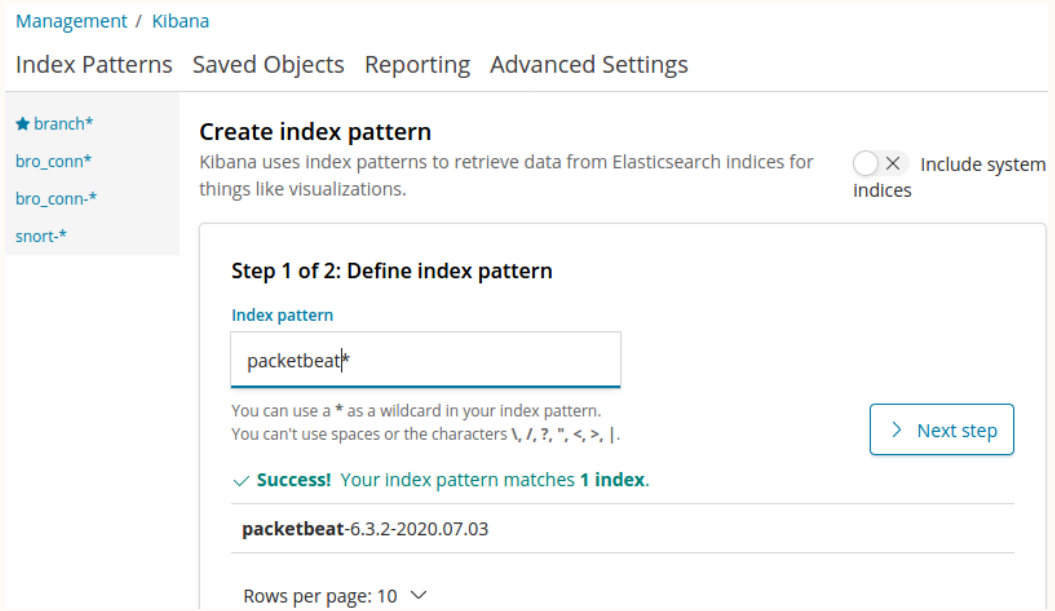
ELK 스택을 활용한 데이터 수집 체계

#4 특징공학

K-Shield Jr.



자동화 스크립트 실행결과

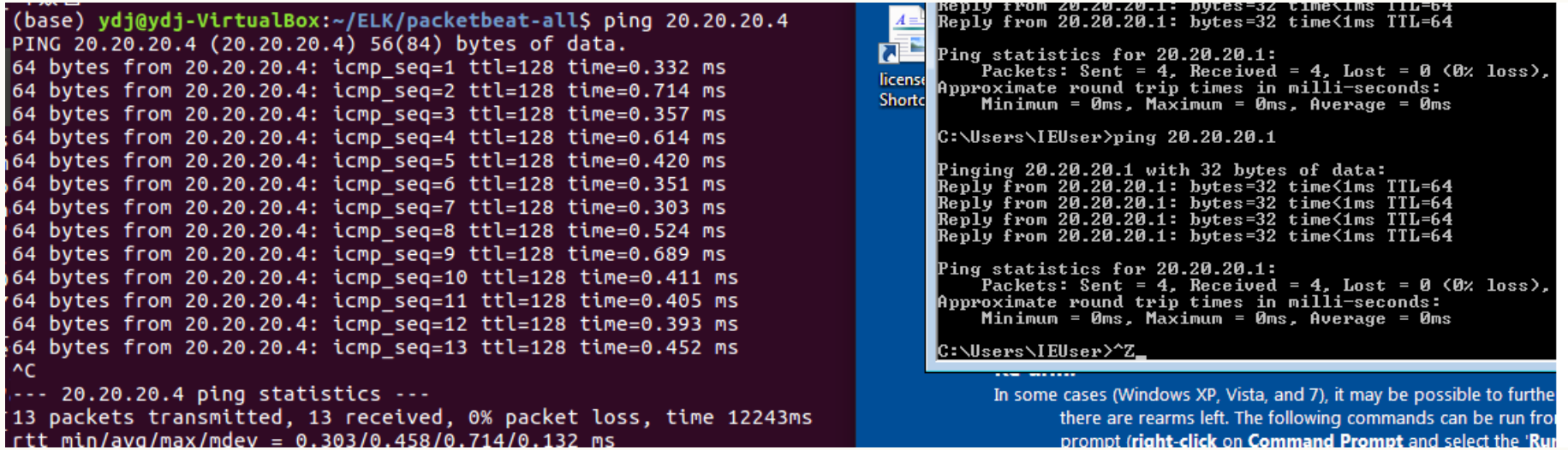


로그 수집 결과

#4 특징공학

K-Shield Jr.

1. 초기 학습데이터

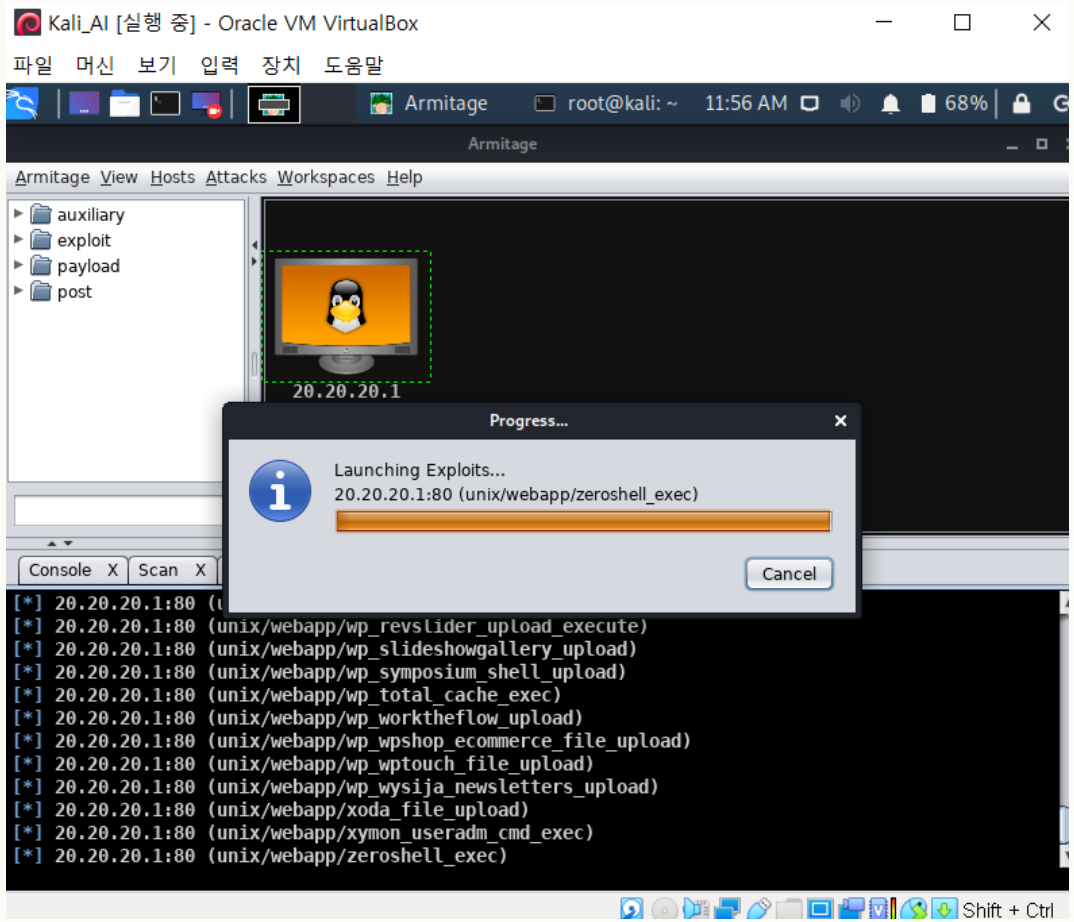


윈도우 <-> 우분투 ping 실행

#4 특징공학

K-Shield Jr.

2. 초기 학습데이터

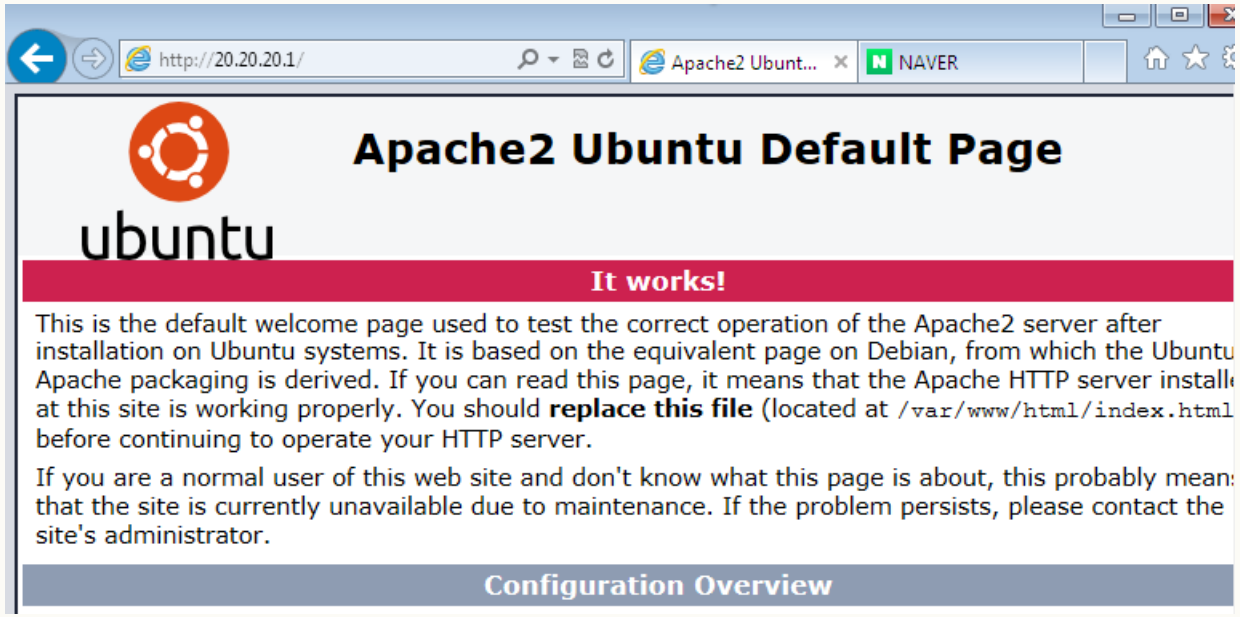


칼리리눅스-> 우분투 스캐닝 & 무차별 공격 수행

#4 특징공학

K-Shield Jr.

3. 초기 학습데이터



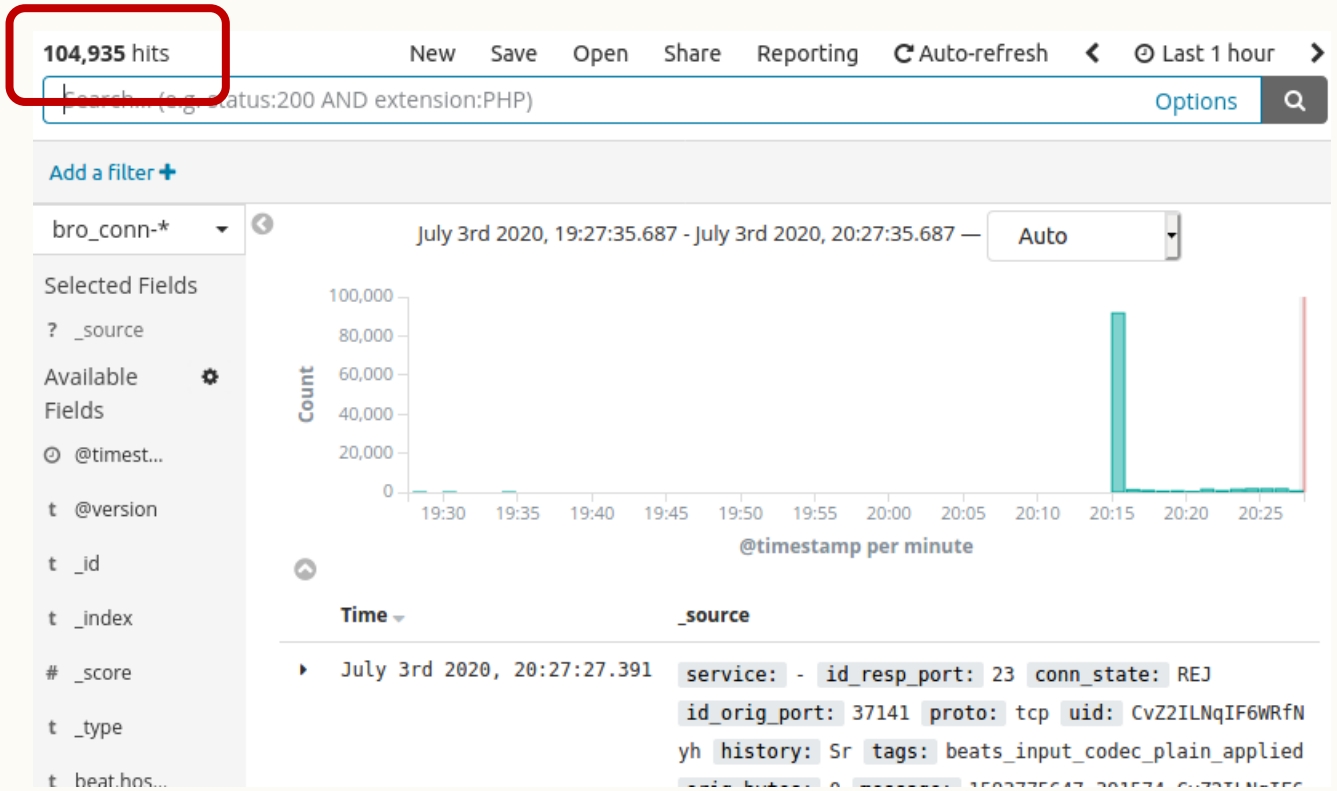
윈도우 -> 우분투 웹서버 접속

#4 특징공학

4. 초기 학습데이터

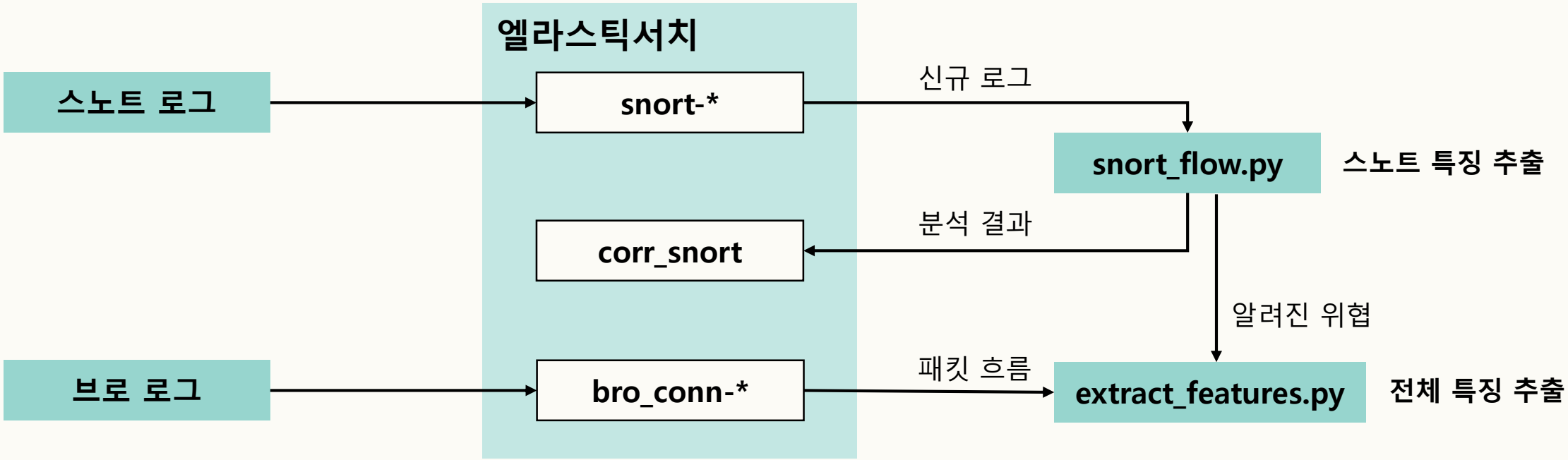
윈도우 -> 인터넷 브라우징 사용

#4 특징공학



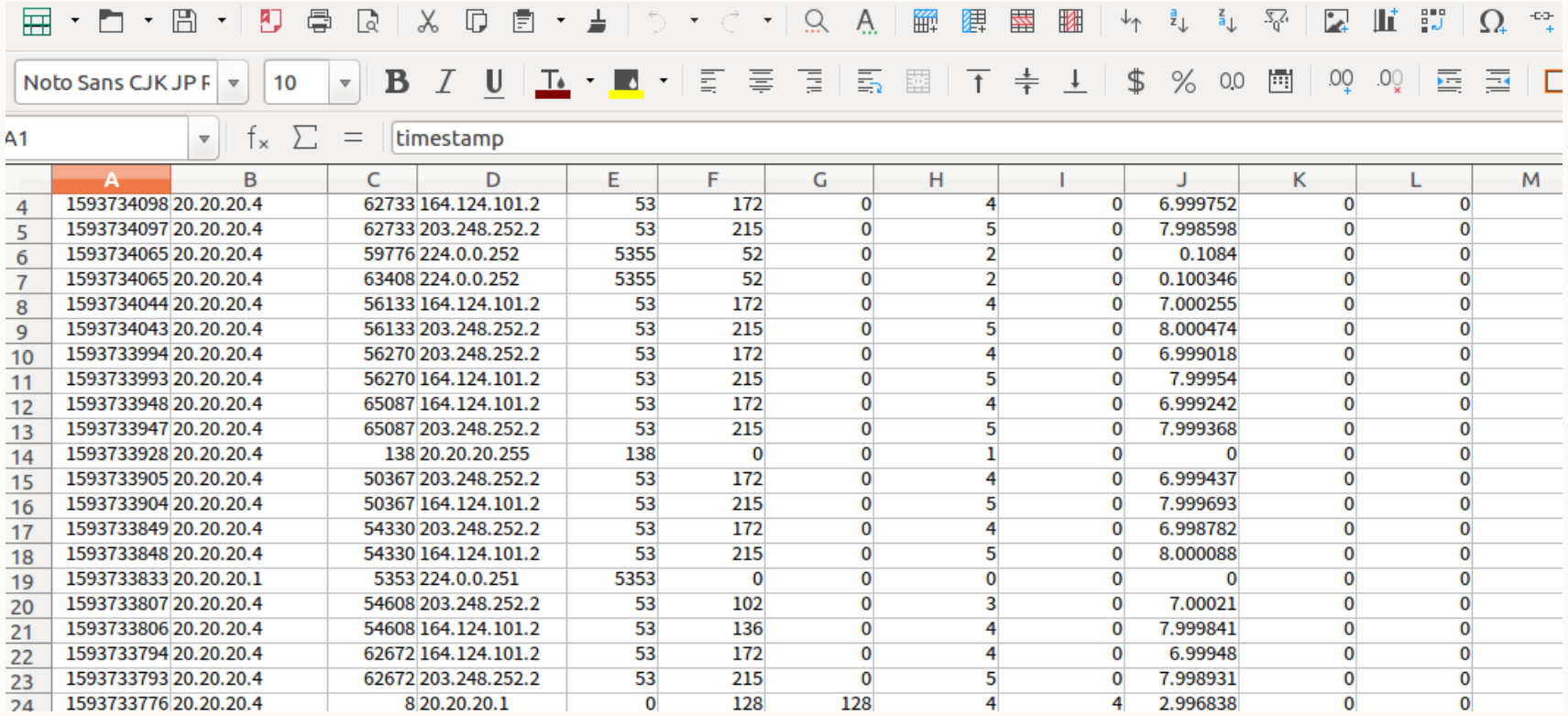
키바나에서 데이터 정상 수집

#4 특징공학



로그파일, 엘라스틱서치와 특징 추출
모듈 관계 및 흐름도

#4 특징공학

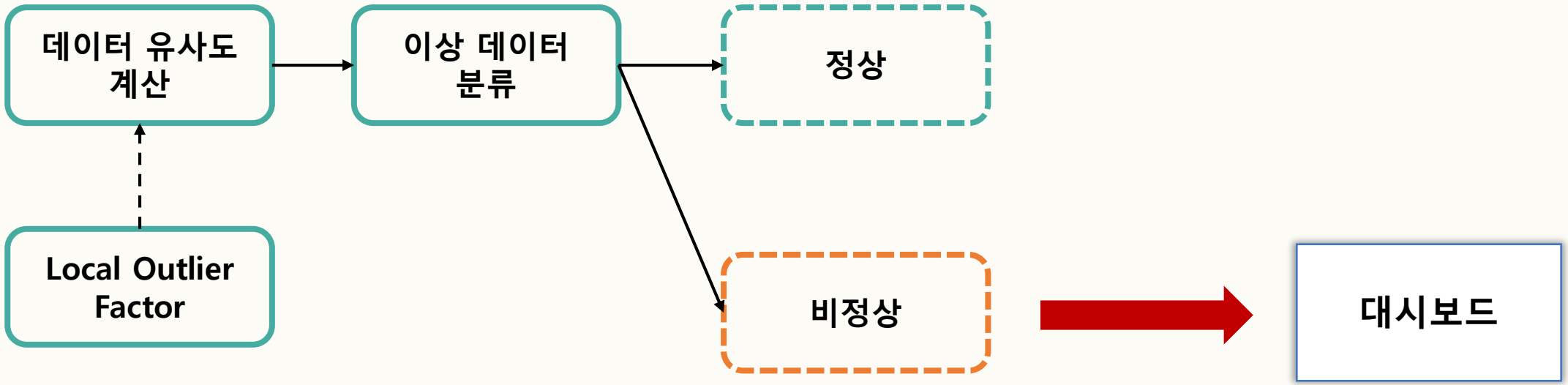


Noto Sans CJK JP F | 10 | A1 | timestamp

	A	B	C	D	E	F	G	H	I	J	K	L	M
4	1593734098	20.20.20.4	62733	164.124.101.2	53	172	0	4	0	6.999752	0	0	
5	1593734097	20.20.20.4	62733	203.248.252.2	53	215	0	5	0	7.998598	0	0	
6	1593734065	20.20.20.4	59776	224.0.0.252	5355	52	0	2	0	0.1084	0	0	
7	1593734065	20.20.20.4	63408	224.0.0.252	5355	52	0	2	0	0.100346	0	0	
8	1593734044	20.20.20.4	56133	164.124.101.2	53	172	0	4	0	7.000255	0	0	
9	1593734043	20.20.20.4	56133	203.248.252.2	53	215	0	5	0	8.000474	0	0	
10	1593733994	20.20.20.4	56270	203.248.252.2	53	172	0	4	0	6.999018	0	0	
11	1593733993	20.20.20.4	56270	164.124.101.2	53	215	0	5	0	7.99954	0	0	
12	1593733948	20.20.20.4	65087	164.124.101.2	53	172	0	4	0	6.999242	0	0	
13	1593733947	20.20.20.4	65087	203.248.252.2	53	215	0	5	0	7.999368	0	0	
14	1593733928	20.20.20.4	138	20.20.20.255	138	0	0	1	0	0	0	0	
15	1593733905	20.20.20.4	50367	203.248.252.2	53	172	0	4	0	6.999437	0	0	
16	1593733904	20.20.20.4	50367	164.124.101.2	53	215	0	5	0	7.999693	0	0	
17	1593733849	20.20.20.4	54330	203.248.252.2	53	172	0	4	0	6.998782	0	0	
18	1593733848	20.20.20.4	54330	164.124.101.2	53	215	0	5	0	8.000088	0	0	
19	1593733833	20.20.20.1	5353	224.0.0.251	5353	0	0	0	0	0	0	0	
20	1593733807	20.20.20.4	54608	203.248.252.2	53	102	0	3	0	7.00021	0	0	
21	1593733806	20.20.20.4	54608	164.124.101.2	53	136	0	4	0	7.999841	0	0	
22	1593733794	20.20.20.4	62672	164.124.101.2	53	172	0	4	0	6.99948	0	0	
23	1593733793	20.20.20.4	62672	203.248.252.2	53	215	0	5	0	7.998931	0	0	
24	1593733776	20.20.20.4	8	20.20.20.1	0	128	128	4	4	2.996838	0	0	

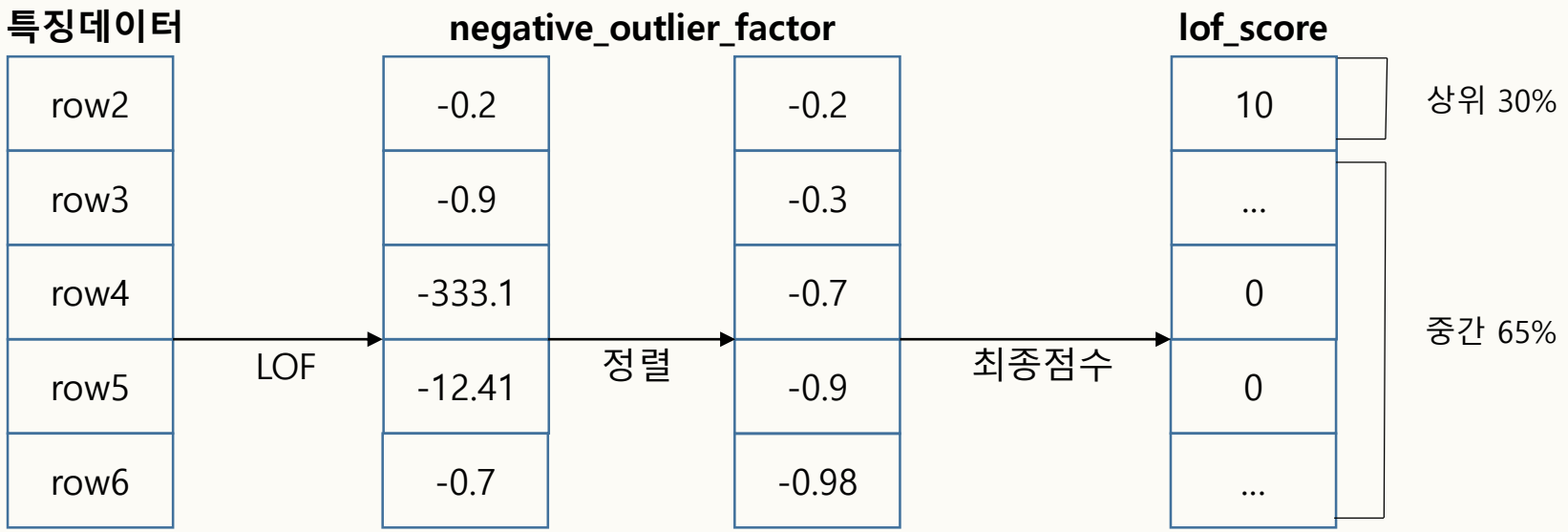
특징추출 결과 feature.csv

#3 데이터 분석



비지도 기반 모델 구조

#4 모델링



특징 데이터 이상 여부

#4 모델링

K-Shield Jr.

P	Q	R	S	T	U	V
high	medium	low	snort_src_cnt	snort_dst_cnt	lof_score	anomal_score
11	0	23	23	0	-0.839611087	1
0	0	23	23	0	-0.839611087	0
10	0	23	23	0	-0.839611087	1
0	0	23	23	0	-0.839611087	0
1	0	23	23	0	-0.839611087	1
31	0	23	23	0	-0.839611087	1
31	0	23	23	0	-0.8465030173	1
31	0	23	23	0	-0.8465030173	1
31	0	23	23	0	-0.8465030173	1
0	0	23	23	0	-0.8465030173	0
0	0	23	23	0	-0.8465030173	0
0	0	23	23	0	-0.8465030173	0
0	0	23	23	0	-0.9524552215	0
0	0	23	23	0	-0.9524552215	0
0	0	23	23	0	-0.9524552215	0
0	0	23	23	0	-0.9524552215	0
11	0	23	23	0	-0.9524552215	1
11	0	23	23	0	-0.9524552215	1

Anomaly_feature.csv

K-Shield Jr.

#05 결론 및 추후 계획

#5 결론 및 추후 계획

A

네트워크 행위에 따라 정상, 악성, 이상 유무 파악

-> 공격유형

(dos , arp 스푸핑 ....)

B

행위 파악 중점 , 가중치와 공격에 따른 학습 기준 파악

-> 트래픽과 통신 기준

C

분류 식별에 따른 불필요한 데이터 삭제, 검출

-> 프로토콜, ip , tcp...

#5 결론 및 추후 계획

A

SIEM&ELK를 통해 구축한 코드를 하나로 합쳐 구동

B

이상탐지 엔진을 배치모드/ 학습모드 구축

C

이상탐지 로그 시각화를 통한 대시보드 제작

K-Shield Jr.

머신러닝을 활용한

네트워크 이상탐지

감사합니다!

Outsider

김태영, 박수곤, 송지민, 유다정, 이기훈

K-Shield Jr.

머신러닝을 활용한

네트워크 이상탐지

Q&A

Outsider

김태영, 박수곤, 송지민, 유다정, 이기훈