O24Sec

Object-Oriented Clustering for Security Monitoring

객체 중심 보안관제로그 오탐제거

2021 캡스톤 18조

팀 “맬러리를 찾아서”

김민송 장우혁

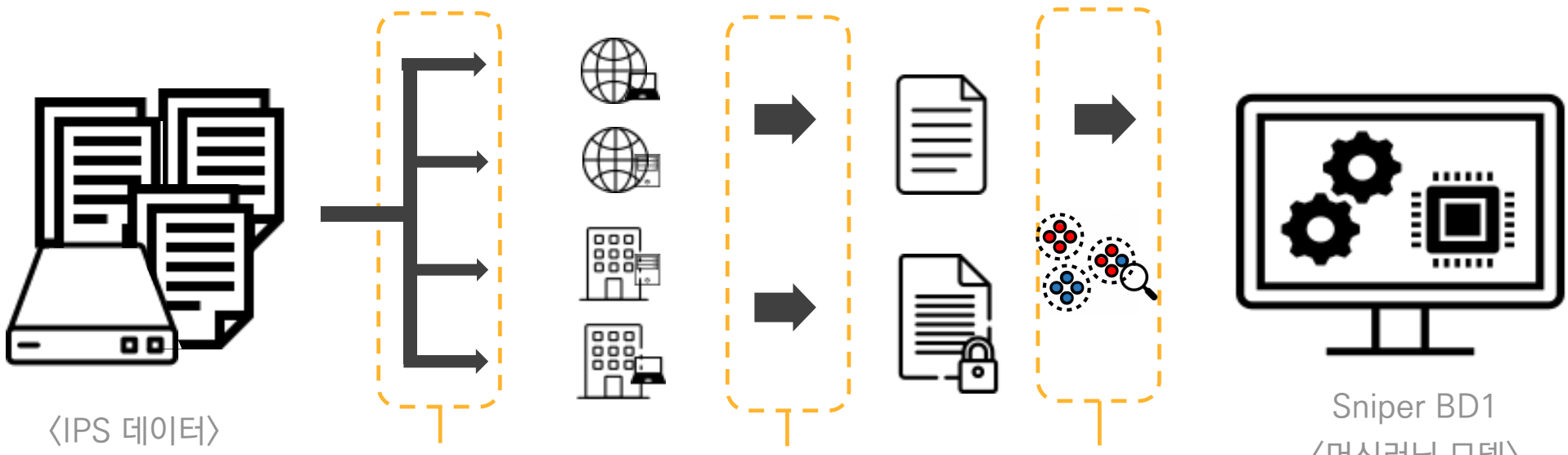
지도 : 윤명근 교수님

프로젝트 소개

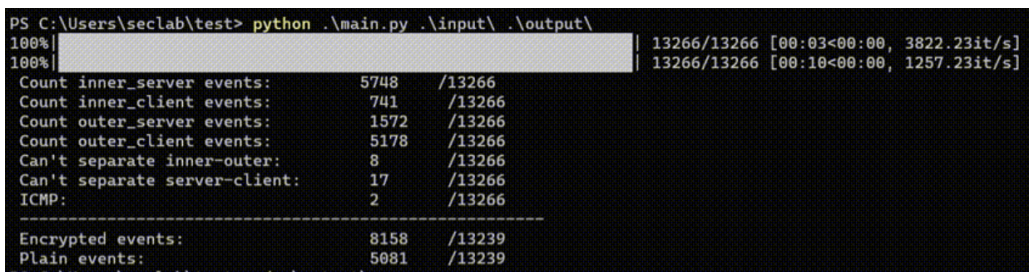
정보보호기업 ‘윈스’의 보안관제제품 SNIPER BD1에서 사용하는
머신러닝 모델의 성능 및 보안관제의 효율성을 위해
해당 제품에서 발생하는 보안관제로그 데이터 분석 및 처리를 돕는 기술을 개발한다.

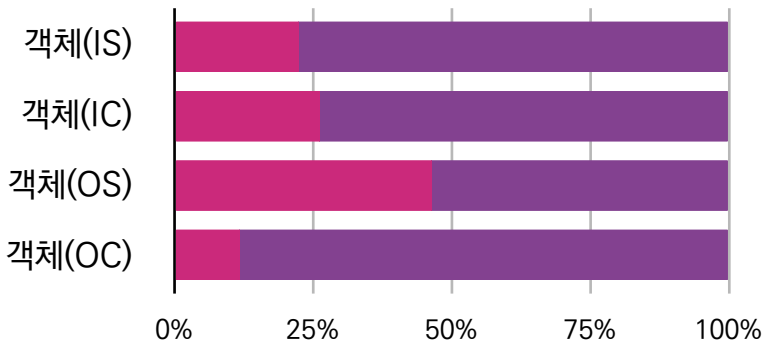
1. **보호대상 객체식별** 자동화 기술
2. 보안관제로그의 **암호화 여부 판별** 기술
3. 객체별 유사도 기반 클러스터링 –〉 **학습 데이터 정합(오탐 제거)**

프로젝트 개요



주요 기술





1. 비식별화된 통신 이벤트 데이터들의 5-Tuple(IP, Port, Protocol)
만을 사용하여 제품 기준으로 내부/외부 IP를 판단하고 역할(서버/클라이언트)에
따라 모든 데이터를 4분할 하는 자동 분류 기술

2. 각 통신 이벤트의 페이로드(실질적인 데이터의 내용) 길이와 복잡도(Entropy)
사이의 관계를 정규분포와 비교하여, 해당 데이터의 페이로드 암호화 여부를
판별하는 기술

3. 4분류 후 유사도 기반으로 클러스터링된 데이터가 각 객체별 최소 50% 이상
압축되었다. 실제 업무에서 정탐 오탐의 라벨 정합을 주어진 차트로
분석할 수 있다.

〈군집화 데이터 제공〉

	A	B	C	D	E	F	G	H	I	J
1	Cluster	DetectN	Result	_id	Payload	label_P(	DetectN	diffrent		
5233	1547		0	e06b2ecb-				["b'953'"]		
5234	1547		0	f9808adb-				["b'3980'"]		
5235	1547		0	f0fdc411-4				["b'64498'"]		
5236	1547		0	67aa372b-				["b'SM-G965N'", "b'59745'"]		
5237	1547		0	11b4e606-				["b'64498'"]		
5238	1547		0	2cf7501b--				["b'21942'"]		
5239	1547		0	69bbfb24-				["b'35701'"]		
5240	1547		0	13c614cd-				["b'953'"]		
5241	1547		0	a9f30000-(				["b'4030'"]		
5242	1547		0	17b1a019-				["b'64498'"]		
5243	1547		0	a3330350-				["b'21942'"]		
5244	1547		0	8b53ba8a-				["b'953'"]		
5245	1547		0	9e705bda-				["b'4005'"]		
5246	1547		0	4d2727b3-				["b'64498'"]		
5247	1547		0	4d9478d9-				["b'21942'"]		
5248	1547		0	37cb5b65-				["b'35488'"]		

Special thanks to mentor Seong Ick Moon

github.com/kookmin-sw/capstone-2021-18

youtu.be/wjlrlJas8TQ