

AI를 통한 비정상 웹로그 탐지 시스템



장혜선



21.06.30

목차



개요



프로젝트 소개



계획

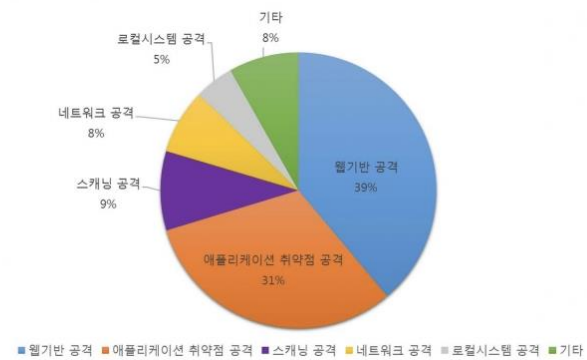
1. 개요

안랩, '2019년 사이버 공격 통계' 발표... "웹기반애플리케이션 취약점 공격이 전체 70%"

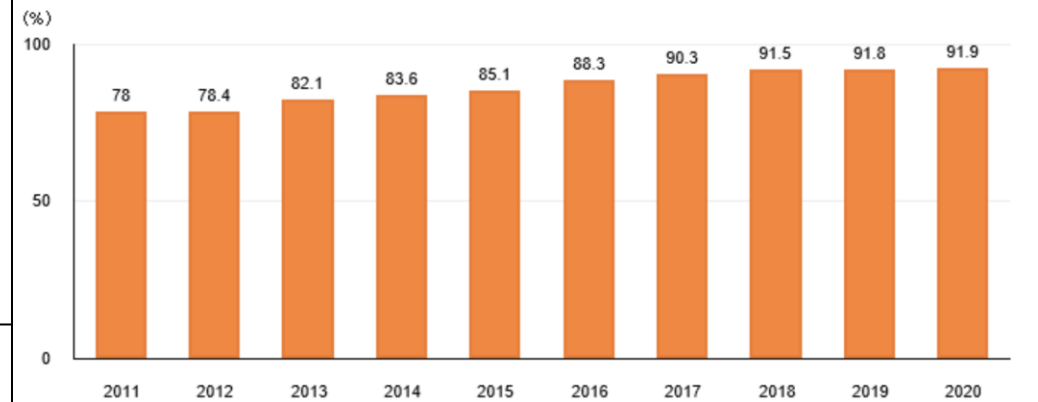
☞ 문성훈 기자 | ☎ 승인 2020.01.16 16:07

산업군별 공격타지 비율은 '미디어'·'게임'·'공공'·'유통'·'법률/세무' 순
'제조'·'중공업' 등 대규모 산업시설 겨냥한 공격 시도도 전년 대비 125% 증가

안랩 2019년 사이버 공격 동향 통계 (공격 유형별)



인터넷 이용률



2-1. 프로젝트 요약

목표

ai를 이용하여 능동적으로 공격을 탐지하고 관리자에게 메일을 전송하여 알리는 프로그램 개발

의의

여러 웹 서버에서 통합적으로 사용할 수 있는 서비스

산출물

결과보고서, 프로그램, 오픈소스, ELK Stack, 계획서

2-1. 자원 및 개발환경



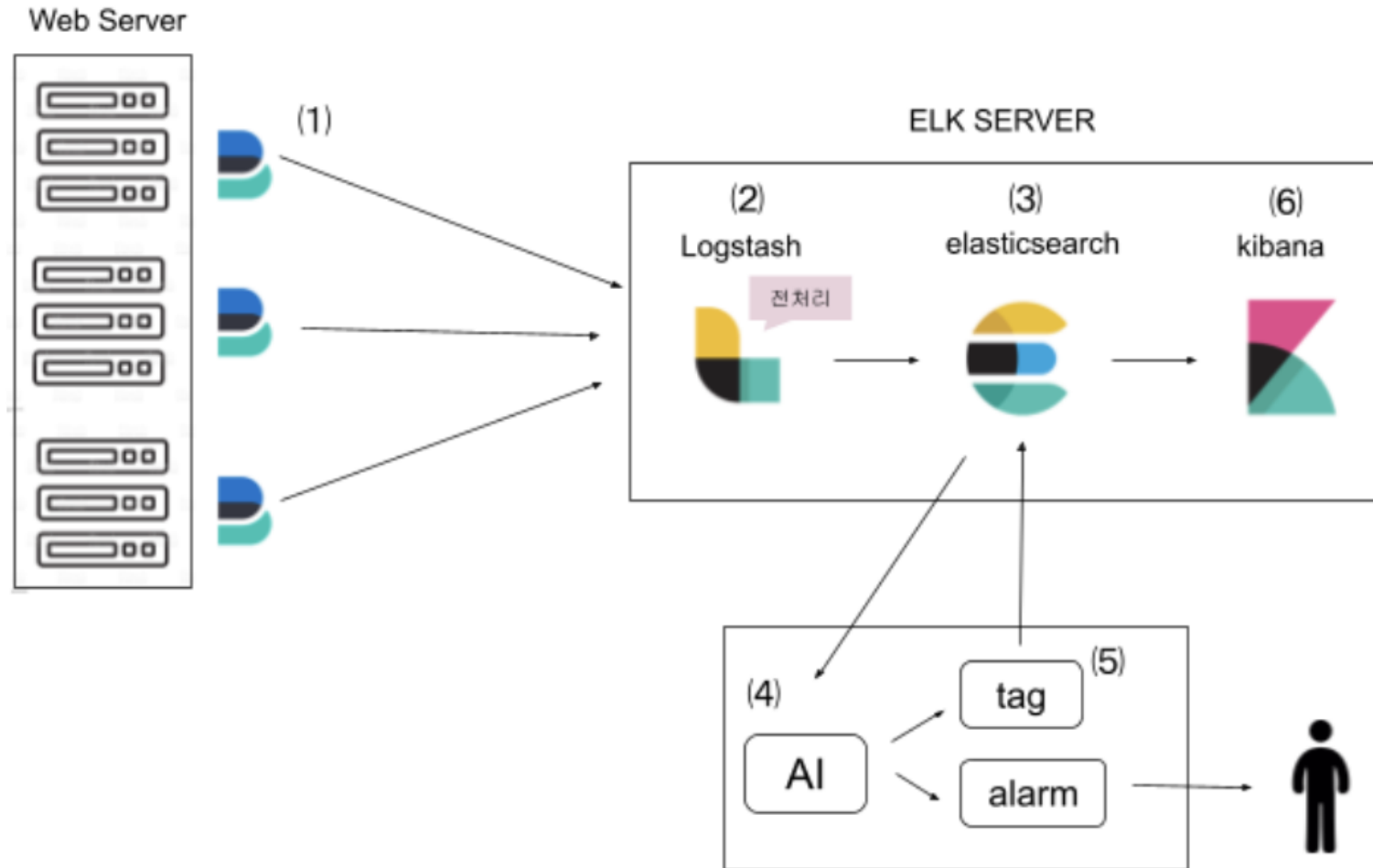
Apache



JEUS[®]



2-2. 구조도



3. 계획

계획 분류	7월				8월				9월				10월			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
사전 공부																
로그 수집																
데이터 전처리																
AI 모델 구현																
성능 테스트																



TensorFlow

감사합니다.