

한 주 연 010 2650 5357 galbitangnamnam@naver.com

경기도 수원시 권선구



01 About Me

2015.09 ~ 2019.07 보하이대학교 신문방송학과 (졸업)

02 Education

2023.06~2024.01 DB보안 솔루션 (JAVA, C/C++)개발자 양성 2023.09~2023.10 문제해결을 위한 자바 코딩 챌린지(к기초디지털역량) Address

GitHub (프로젝트)

https://github.com/JUYEON919/TeamProject.git

GitHub (개인)

JUYEON919 (juyeon han) (github.com)

E-mail

wndus5357@naver.com

Q 기술 스택

03

01 Backend

Spring Boot

MyBatis

Thymeleaf

Lombok

O2 Programming Languages

Java

HTNL5

CSS3

JavaScript

C

C++

Collaborations

Git Hub

Serv

04

Server / DB / OS

Apache Tomcat

Spring

MariaDB

MySQL

Linux (Ubuntu, Rocky)

Tools/Performance Test

Eclipse

DBeaver

WireShark

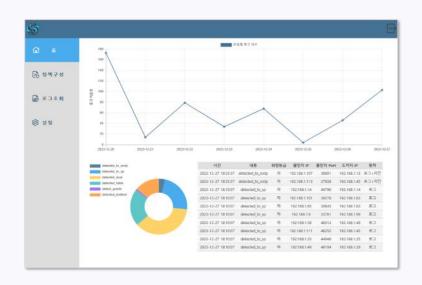
GDB

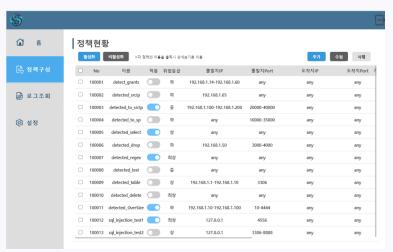
JQuery

VirtualBox

tcpdump

Q Sentinel팀 프로젝트





데이터베이스 공격 탐지 및 차단 서비스

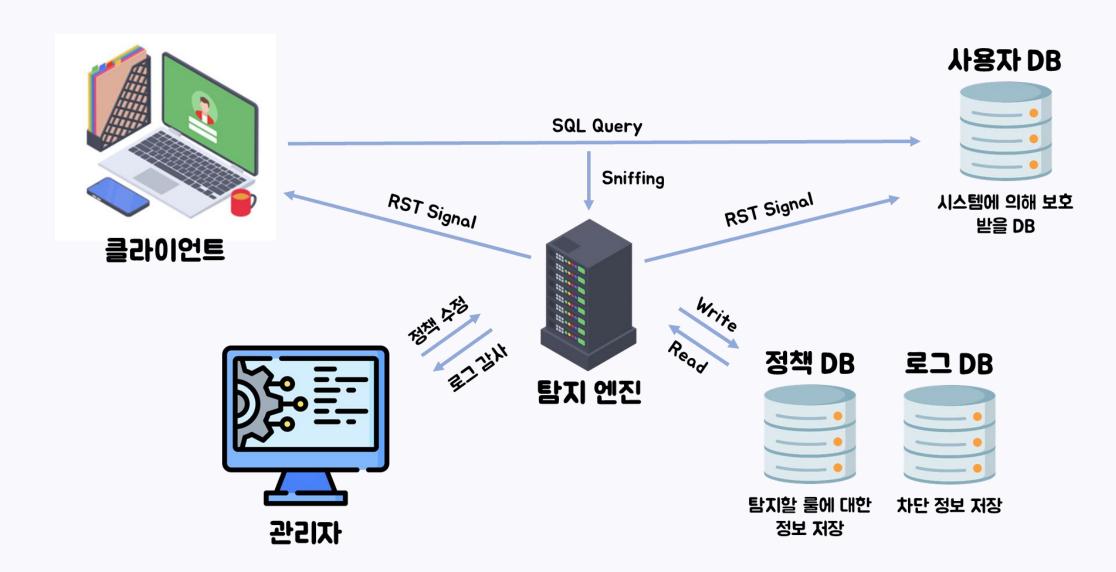
작업 기간	2023. 11. 07 ~ 2023. 12. 28 (2개월)
인력 구성	5명(엔진구현 4 / 화면구성 2)
프로젝트 목적	데이터베이스 공격을 탐지하고 차단하는 프로그램을 구현
맡은 역할 <i>/</i> 주요 업무 및 상세 역할	탐지엔진구현의 정책룰을 읽어와 필터링, 행동기반탐지엔 진 구현 보안 관리자 페이지 화면 구성 목업 기획부터 프론트엔드 기 능 구현까지 전담하여 업무 수행
사용언어 및 개발 환경	C/C++, Java, Html5, CSS3, Javascript, MariaDB, Rocky Linux, Wireshark, GitHub, spring, GDB, Val grind, jQuery, Thymeleaf, Lombok, Tcpdump
느낀점	화면구성 작업시에 Git으로 협업하면서 작업을 해서 git사용 의 편리함과 중요성을 배웠다
참고 자료	Github 링크(화면구성 소스코드) https://github.com/JUYEON919/TeamProject.git

Sentinel 데이터베이스 설계

			olicy_db.ips_policy	Table フ	술서		작성일	20231125	Page
			s_ips_manager				작성자	Sentinel	
Des	cription	남시물 1	설정 테이블						
No	Attril	bute	Data Type	Length	Null	KY	Default		iption
1	detected_no		int	6	N	PK		룰번호	
2	detected_name		varchar	50	N			룰 이름	
3	cont	ent1	varchar	255	Υ		null	탐지 문구 1	
4	content2		varchar	255	Υ		null	탐지 문구 2	
5	cont	ent3	varchar	255	Υ		null	탐지 문구 3	
6	6 enable		int	1	N		1	0 : 룰 실행 X 1 : 룰 실행 O	
7	src	_ip	varchar	15	Υ		0		
8	src_port		int	5	Υ		0		
9	action		int	1	N		0	0 : 로그 1 : 로그+차단	
10	lev	⁄el	int	1	N		0	위험순위	
11	base_	time	int	11	Υ		0	행동 탐지 기준	초
12	base_	_limit	int	11	Υ		0	행동 탐지 기준	퀴리 수
13	end_	time	date		N		1	유효기간	
14	det	tail	varchar	255	Υ			탐지 내용	
15	to_	sip	varchar	15	1		0	범위입력시 sip	
16	to_	sp	int	5	Υ		0	범위입력시 sp	
17	dst	_ip	varchar	15	Υ		0	탐지할 IP	
18	base	_size	int	11	Υ		0	행동 탐지 기준	데이터 사이즈
19	dst_	port	int	5	N			Destination Por	t

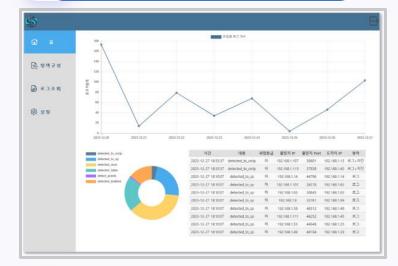
1	Name	S_ips_log_	_db.log_YYYYMMDD	Table フ	수서		작성일	20231125	Page
S	ystem	dbm	s_ips_manager	ps_manager				Sentinel	
Des	cription	탐지결과 .	로그 테이블						
No	Attr	ibute	Data Type	Length	Null	KY	Default	Description	n
1	log_	index	int	11	N	PK		로그 번호	
2	detec	ted_no	int	6	N			탐지 룰 번호	
3	detecte	ed_name	varchar	50	N			탐지 룰 이름	
4	ti	me	timestamp		N			기록 시간	
5	ac	tion	int	1	N			탐지 행동 유형	
6	sr	c_ip	varchar	15	N			Source IP	
7	pack	et_bin	varbinary	3000	N			패킷 내용	
8	le	evel	int	5	N			위험순위	
9	src	_port	int	5	N			Source Port	
10	ds	st_ip	varchar	15	N			Destiny IP	
11	dst	_port	int	5	N			Destiny Port	
비고	1								
	ра	cket에서 더	이터를 뽑을 수 있지	만 검색할 때 용	이하게	하기위	해 src_ip	를 따로 저장	

	Name S_manag		ge_user.user_info	Table 7	작성일	20231125	Page		
S	System Manager_User			lable >	12/1		작성자	Sentinel	
Description IPS_MANAGER 유저정보				테이블					
No	No Attribute		Data Type	Length Null KY		KY	Default	Description	
1	persor	nal_no	int	11	N	PK		고유번호	
2	ic	t	varchar	50	N			아이디	
3	passv	word	char	64	N			비밀번호	
4	sa	lt	varchar	20	N		·	임의 해시 데이	터



Q Sentinel팀 프로젝트 - 화면구성

01 홈 메인 페이지



01 설정 페이지

파일 설정	설정
DB NIC:	
DB IP:	
DB Port:	
비밀번호 변경	비밀번호 변경
비밀번호 변경	비밀번호 변경
•	비일번호 변경

01 정책 현황 페이지

9	성화	비활성화 포각 정	책의 이름	을 클릭시 상세	보기로 이동		추가	수정 삭제
	No	이름	적용	위험등급	출발지IP	출발지Port	도착지IP	도착지Por
	100001	detect_grants		하	192.168.1.14-192.168.1.60	any	any	any
	100002	detected_srclp		하	192.168.1.65	any	any	any
	100003	detected_to_srcIp		중	192.168.1.100-192.168.1.200	20000-40000	any	any
	100004	detected_to_sp		하	any	10000-35000	any	any
	100005	detected_select		상	any	any	any	any
	100006	detected_drop		하	192.168.1.50	3000-4000	any	any
	100007	detected_regex		최상	any	any	any	any
	100008	detected_test		중	any	any	any	any
	100009	detected_table		상	192.168.1.1-192.168.1.10	3306	any	any
	100010	detected_delete		최상	any	any	any	any
	100011	detected_OverSize		하	192.168.1.10-192.168.1.100	10-4444	any	any
	100012	sql_injection_test1		최상	127.0.0.1	4556	any	any
	100013	sql_injection_test2		상	127.0.0.1	3306-8888	any	any

	이름을 입력하세요.	참지 패턴	20
#선 정보 출발지 P (-P 범위): 출발지 Port (-Port 범위): 도착지 P:	┃ 정책 상세 정보 ┃ 탐지 정책 기본 정보		당지 패턴
도착지 Port 장택 등작 등작설정:	합지명 유효기간: 위립등급: 세선 정보 출범지 P (4P 범위):	detect_grants	기준복수 @ 프용한 100 회 발생 제작점의 나 용 contents 합력하세요. Content1: grant content2: show
	출발지 Port [-Port 범위]: 도착지 IP: 도착지 Port 정책 등작	any any any	집 당지 내용 설명 절관 설명
	동작설정:	E2 v	有点 今後

01

로그 조회 페이지

필	터										
		any		위험등급:	위험등급: 전체		•	동작:	전체		•
		any		도착지 IP	:	any		시작 지점 날짜:	2023-12-27	00:00	.00
출발	지 Port:	any		도착지 Po	ort:	any		종료 지점 날짜:	2024-01-04	23:59	59
										조 회	초기화
No	И	간	내용	위험등급	Ŷ	발지 IP	출발지 Port	도착지 IP	도착지 Port	동작	버튼
1	2023-12-2	7 14:27:18	detected_testbed	상	192	168.1.65	9918	192.168.1.14		로그+자단	상세보기
2	2023-12-2	7 14:29:03	detected_dual	최상	192.1	68.173.37	1628	192.168.13.73		로그+차단	상세보기
3	2023-12-2	7 14:29:03	detected_dual	최상	192.1	68.203.87	1629	192.168.213.27		로그+차단	상세보기
4	2023-12-2	7 14:29:03	detected_dual	최상	192.	168.79.21	1630	192.168.249.19		로그+자단	상세보기
5	2023-12-2	7 14:29:03	detected_dual	최상	192	168.11.61	1631	192.168.71.49		로그+차단	상세보기
6	2023-12-2	7 14:29:03	detected_dual	최상	192.1	68.187.85	1632	192.168.9.65		로그+차단	상세보기
7	2023-12-2	7 14:29:03	detected_dual	최상	192.1	68.213.47	1633	192.168.227.99		로그+자단	상세보기
8	2023-12-2	7 14:29:03	detected_dual	최상	192.1	68.157.79	1627	192.168.1.41		로그+차단	상세보기
9	2023-12-2	7 14:30:23	detected_dual	최상	192.1	68.203.87	1629	192.168.213.27		로그+차단	상세보기
10	2023-12-2	7 14:30:23	detected_dual	최상	192.1	68.173.37	1628	192.168.13.73		로그+자단	상세보기

패킷정보					
thernet Header	패킷 상세	정보			
Destination MAC Addr: 00:E0:81:4C:D4:62 Ource MAC Addr: 00:0E:0C:00:CD:7B Thernet Type: 0x0800	CD 78 08 00 40 00 80 06 C0 A8 D5 18	00 E0 81 4C D4 62 00 0E 0C 00 CD 78 08 00 45 00 00 76 6C 9F 40 00 80 06 6C 19 C0 A8 CB 57 C0 A8 D5 18 06 5D 05 F1 E3 ED D1 0F C7 57 94 E5 D1 18 FC E6			
P Header		9A EC 50 18 FC E6 00 53 00 00 06 00			
Irelation. 4 Interface Tempts 5 Specification 1200 Interface Tempts 123 Interface Tempts 123 Interface Tempts 125 Interface Tempts 126 Interface Te	01 12 01 01 7F FF FF FF C 00 00 00 12 20 2A 20 46 41 4C 01 01				
TCP Header	위험등급:	정보 없음	처리방법 : 정보 없음		
ource Port: 1629 Destination Port: 1521 equence Number: 3824013583 Icknowledgment Number: 3344407276	내용:				

Q Sentinel팀 프로젝트 - 트러블이슈

01 로그인 화면



문제 관리자의 로그인 정보에대한보 안 및 사용자 정보 안정성이 부 족함

원인 관리자의 로그인정보를 평문으로 저장하는 형식을이용함

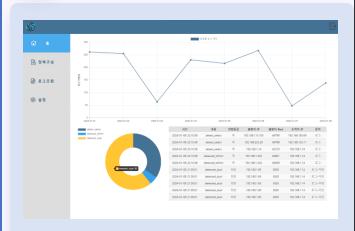
보안 및 사용자 정보 안정성이 부족하다고 판단하여 비밀번호 와 무작위 솔트값을 해시화하 여 저장하고 비교하도록 구현했 습니다.

```
$(document).ready(function () {
    var logNames = {};
    var logCounts = {};
    function formatLogTime(logTime) {
        var date = new Date(logTime);
        var formattedTime = date.toLocaleString('en-US', {
            year: 'numeric',
            month: '2-digit',
            day: '2-digit',
            hour: '2-digit'
            minute: '2-digit',
            second: '2-digit',
            hour12: false // 24시간 형식
        var parts = formattedTime.split(', ');
        var datePart = parts[0].split('/').reverse().join('-'); // Reformatting date
        var timePart = parts[1];
       return datePart.replace(/(\d+)-(\d+)-(\d+)/, '$1-$3-$2') + ' ' + timePart;
```

```
function fetchLogs(date) {
   var dd = String(date.getDate()).padStart(2, '0');
   var mm = String(date.getMonth() + 1).padStart(2, '0');
   var yyyy = date.getFullYear();
   var dateStr = vvvv + '-' + mm + '-' + dd;
   $.ajax({
       url: '/admin/menu/home/api/log'.
       type: 'GET',
       data: {
           date: dateStr
       success: function (data) {
           if (data.length === 0) {
               date.setDate(date.getDate() - 1);
               fetchLogs(date);
           } else {
               var tbody = $('#lTable');
               var logNames = {};
               var topTenLogs = data.slice(0, 10);
               topTenLogs.forEach(function (log) {
                   var row = $('');
                   row.append($('').text(formatLogTime(log.time)));
                   row.append($('').text(log.detected_name));
                   var resultLevel = '';
                   switch (log.level) {
                           resultLevel = '전체';
                           break;
                       case 0:
                           resultLevel = '하';
                           break;
                       case 1:
                           resultLevel = '중';
                           break;
                       case 2:
                           resultLevel = '상';
                           break;
                       case 3:
                           resultLevel = '최상';
                           break;
```

Q Sentinel팀 프로젝트 - 트러블이슈

01 홈 화면



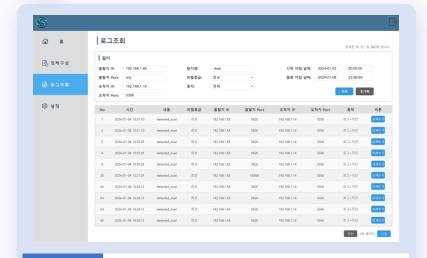
```
문제 홈 화면 페이지에서 출력하는 로 당이 오래걸리는 현상 발생 명이 오래걸리는 현상 발생 대량의 데이터를 한번에 다 가져 오는 방법때문에 로딩이 오래걸림 하달, 일주일, 하루 기간을 나누어 데이터를 불러오는 시간을 약 15초 가량 소요되던 로딩시간을 5초 이내로 단축
```

```
$(document).ready(function () {
    var logNames = {};
    var logCounts = {};
    function formatLogTime(logTime) {
        var date = new Date(logTime);
        var formattedTime = date.toLocaleString('en-US', {
            year: 'numeric',
            month: '2-digit',
            day: '2-digit',
            hour: '2-digit'
            minute: '2-digit',
            second: '2-digit',
            hour12: false // 24시간 형식
        var parts = formattedTime.split(', ');
        var datePart = parts[0].split('/').reverse().join('-'); // Reformatting date
        var timePart = parts[1];
        return datePart.replace(/(\d+)-(\d+)-(\d+)/, '$1-$3-$2') + ' ' + timePart;
```

```
function fetchLogs(date) {
   var dd = String(date.getDate()).padStart(2, '0');
   var mm = String(date.getMonth() + 1).padStart(2, '0');
   var yyyy = date.getFullYear();
   var dateStr = vvvv + '-' + mm + '-' + dd;
   $.ajax({
       url: '/admin/menu/home/api/log'.
       type: 'GET',
       data: {
           date: dateStr
       success: function (data) {
           if (data.length === 0) {
               date.setDate(date.getDate() - 1);
               fetchLogs(date);
           } else {
               var tbody = $('#lTable');
               var logNames = {};
               var topTenLogs = data.slice(0, 10);
               topTenLogs.forEach(function (log) {
                   var row = $('');
                   row.append($('').text(formatLogTime(log.time)));
                   row.append($('').text(log.detected_name));
                   var resultLevel = '';
                   switch (log.level) {
                           resultLevel = '전체';
                           break;
                       case 0:
                           resultLevel = '하';
                           break;
                       case 1:
                           resultLevel = '중';
                           break;
                       case 2:
                           resultLevel = '상';
                           break;
                       case 3:
                           resultLevel = '최상';
                           break;
```

Q Sentinel팀 프로젝트 - 트러블이슈

01 로그조회



```
문제 로그조회 페이지에서 출력하는 로딩이 오래걸리는 현상 발생

원인 대량의 데이터를 한번에 다 가져오는 방법때문에 로딩이 오래걸림

대용량의 데이터를 고속으로 처리 가능한 방법준 페이징 기술을 적용해 약 10초 가량 소요되던 로딩시간을 3초 이내로 단축시
```

프론트엔드 - 디자인









Q

프론트엔드 - 디자인





