



Splunker

운영2팀 - 관제시스템

Team Leader

김민경

WBS 제작
대시보드 개발
AES 복호화
보고서 작성
발표

김도연

취약점 탐색
공격 탐지 쿼리 개발
시나리오 수행
제안서 제작

박용현

공격 탐지 쿼리 개발
경고 등록
이벤트 처리 흐름도 제작
보고서 작성

박준희

WBS 제작
공격 탐지 쿼리 개발
시나리오 수행
제안서 제작

구분	주요 Task			산출물	5월											6월										
	대분류	소분류	3주차		4주차					5주차					1주차					2주차					3주차	
				17	20	21	22	23	24	27	28	29	30	31	3	4	5	6	7	10	11	12	13	14	17	18
1. 설계	1.1 kick-off	1.1.1 프로젝트 계획 수립	프로젝트 수행계획서																							
	1.2 WBS 수립	1.2.1 WBS 작성	WBS																							
	1.3 사전 준비	1.3.1 Splunk 이해 및 SPL 스크립트																								
	1.4 환경 설계	1.4.1 아키텍처 구성	아키텍처																							
2. 구축	2.1 SIEM(Splunk) 구축	2.1.1 Forwarder(hwd), Indexer(idk), Searcher(sch), Master 설치 2.1.2 fed → idk ↔ master ↔ sch 연동																								
	2.2 WEB 구축	2.2.1 GnuBoard (웹서버) 설치 2.2.2 Splunk와 연동하여 로그 수집																								
	2.3 공격 환경 구축	2.3.1 OS (Kali Linux) 구축 2.3.2 취약점 스캔 도구 설치																								
		3.1.1 GnuBoard 취약점 조사 3.1.2 취약점 자동 진단 수행 (공격성 트래픽 발생 등) 3.1.3 공격성 트래픽 탐지 시나리오 개발	GnuBoard 버전별 취약점 리스트 취약점 진단 결과 리포트																							
3. 개발	3.1 Splunk 탐지 시나리오 개발	3.2.1 웹 서버 로그 분석 3.2.2 Splunk 탐지 쿼리 생성 3.2.3 Splunk 경고 등록	로그 분석 결과 Draft																							
	3.2 Splunk 탐지 쿼리 생성	3.3.1 Splunk 대시보드 구성 3.3.2 Splunk 대시보드 검증																								
	3.3 Splunk 대시보드 구성																									
4. 검증	4.1 침해사고 모의 공격 수행 (1)	4.1.1 침해사고 사례1 기획 4.1.2 Chrome 익스텐션 자동완성 파일 복호화 4.1.3 피싱사이트 제작 4.1.4 XSS 공격 수행 4.1.5 Splunk 경고 발송 검증	Mail, csv 파일																							
	4.2 침해사고 모의 공격 수행 (2)	4.2.1 침해사고 사례2 기획 4.2.2 DDos 공격 수행 4.2.3 Splunk 경고 발송 검증	Mail, csv 파일																							
	4.3 결과 보고	4.3.1 관제 활동 결과보고서 작성	관제 활동 보고서																							
		5.1.1 프로젝트 발표 자료 제작 (PPT) 5.1.2 프로젝트 발표 자료 제작 (스크립트)	프로젝트 제안서 발표 스크립트																							
5. 총합	5.1 발표 준비	5.2.1 프로젝트 발표 5.2.2 프로젝트 수정																								
	5.2 발표																									

집중수행

이전 Task 미완료시 보완 수행

진행수행

이전 Task 미완료시 보완 수행

SPLUNK를 통한 SIEM 기반 보안관제 시스템

2024. 06.

SECUI



목차

I

사업 수행 방안

1. 추진 배경
2. 수행 방안

II

T사 적용 사례

1. 사전 환경
2. 공격 파악 과정
3. 유출 과정 전개
4. 결과

III

기대 효과

1. 기대 효과



Chapter

I

사업 수행 방안

1. 추진 배경

2. 수행 방안



splunk> SIEM 기반 보안 관제 시스템

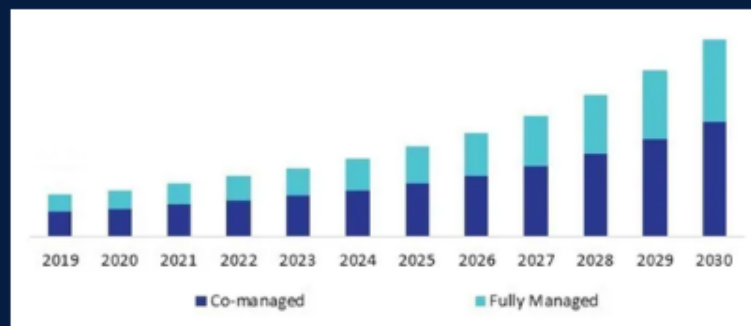
빅데이터
분석

맞춤형
대시보드

자동화된
실시간
경고

체계적인
산출물

자동화된 탐지를 바탕으로
신속성 및 안정성 향상



Global Managed SIEM Services Market

AS-IS

ESM

- 단기 이벤트성 위주 분석
- IP, Port 기반 네트워크 계층 탐지
- 알려진 시그니처 중심의 분석

TO-BE

SIEM - Splunk

- 빅데이터 수준의 장시간 심층 분석
- 수집한 데이터들의 상관 관계 분석
- ESM 대비 탐지 정확도 개선

“맞춤형 최적화를 통한
안정성 및 신뢰성 향상”

구축, 분석, 조치, 보고

01

사전 준비

- 고객사 운영현황 인터뷰
- 로그 수집 대상 산정
- Splunk 구축
(Forwarder, Indexer, Searcher, Master)

02

로그 분석

- 로그 수집 및 분석
- 대시보드 구축
- 공격 탐지 시나리오 개발
- 공격 탐지 쿼리 생성
- Splunk 경고 등록

03

실시간 탐지

- 365일 24시간 모니터링
- 정확한 탐지 쿼리를 통한
즉각적인 경고 발송

04

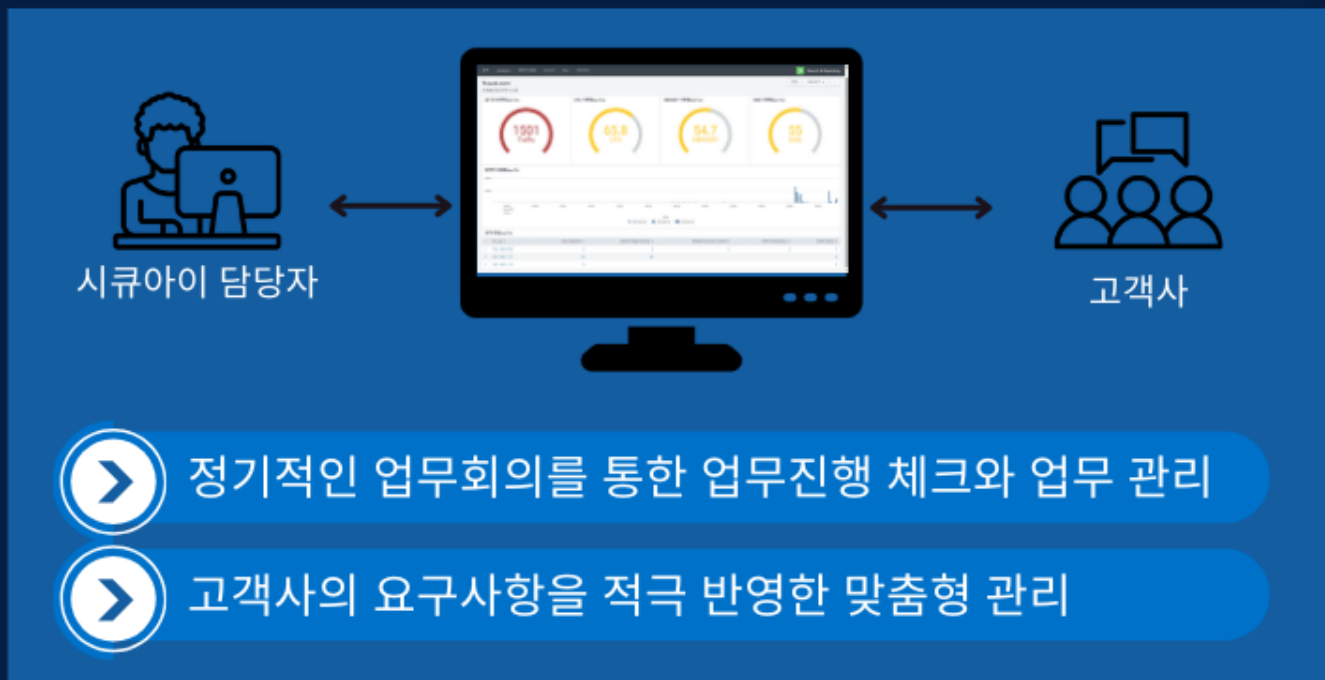
결과 보고

- 공격 관련 로그 csv 파일
- 보안관제 일일 보고서

보안관제 이벤트 처리 프로세스



전문인력을 통하여 업무를 효율적으로 수행하고, 의사소통 및 협조체계 강화



R & R 관리기준	SECUI	고객사
웹서버 방화벽 권한 및 정책 관리		O
Splunk 탐지 시나리오 정리 및 로그 분석	O	
권고안 제안 및 산출물관리	O	
최종 적용 후 내역 검토	O	O

Chapter

II

T사 적용 사례

- XSS로 인한 피싱 사이트 리다이렉트
- DDoS

1. 사전 환경

2. 공격 파악 과정

3. 유출 과정 전개

4. 결과



T사 (TRAVELDOTCOM) 개인 정보 유출 사고 예방

사고 예방 프로세스

01
등록

고객사 현황을 기반으로
공격 탐지 쿼리 등록

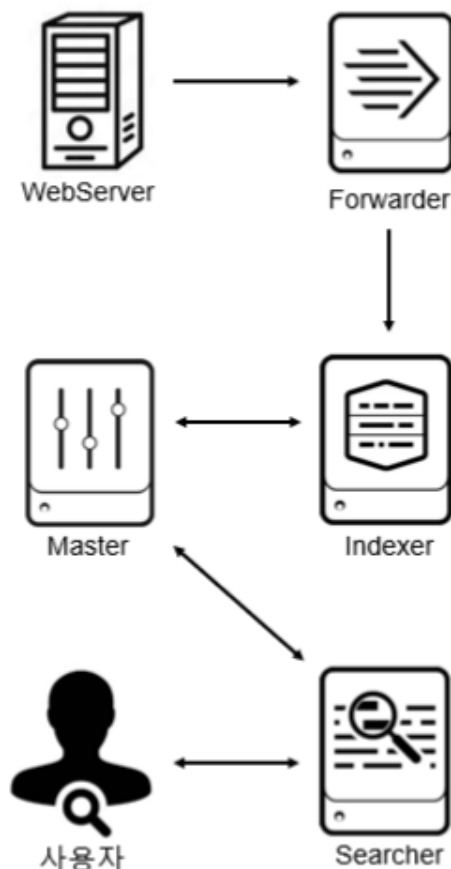
02
탐지

공격 징후 탐지 시 경고 발생

03
보고

해당 결과 고객사 리포팅

T사의 Splunk 아키텍처



6월 9일 3시 9분, 공격자 관리자 페이지 접근
3시 20분, 경고 메일 발송



▼ T사 홈페이지 관리자와 담당 관제센터에서 자동 경고 메일 수신

client_time	src_ip	status	method	url
[09/Jun/2024:03:18:56]	192.168.1.17	200	POST /adm/ajax.token.php HTTP/1.1	http://192.168.1.16/adm/menu_list.php
[09/Jun/2024:03:18:52]	192.168.1.17	200	GET /adm/menu_list.php HTTP/1.1	http://192.168.1.16/adm/menu_list.php
[09/Jun/2024:03:17:21]	192.168.1.17	200	GET /adm/board_list.php HTTP/1.1	http://192.168.1.16/adm/board_list.php
[09/Jun/2024:03:17:01]	192.168.1.17	200	GET /adm/sms_adminv/config.php HTTP/1.1	http://192.168.1.16/adm/config_form.php
[09/Jun/2024:03:16:10]	192.168.1.17	200	GET /adm/mail_list.php?mem=%27select*frommember HTTP/1.1	
[09/Jun/2024:03:14:34]	192.168.1.17	200	GET /adm/member_list.php HTTP/1.1	192.168.1.16/adm/member_list.php
[09/Jun/2024:03:13:57]	192.168.1.17	200	GET /adm/mail_list.php?id=%27or1=1 HTTP/1.1	
[09/Jun/2024:03:13:04]	192.168.1.17	200	GET /adm/mail_list.php?%3Cscript%3Ealert(1)%3C/script%3E HTTP/1.1	
[09/Jun/2024:03:12:51]	192.168.1.17	200	GET /adm/mail_list.php?%3Cscript%3Ealert(1)%3C/script%3E HTTP/1.1	
[09/Jun/2024:03:11:33]	192.168.1.17	200	GET /adm/mail_list.php HTTP/1.1	
[09/Jun/2024:03:09:40]	192.168.1.17	200	GET /adm/board_list.php?board=%3Cscript%3Elocation.href=	
[09/Jun/2024:03:09:28]	192.168.1.17	200	%22http://192.168.1.17/traveldotcom%22%3C/script%3E HTTP/1.1	192.168.1.16/adm/board_list.php
[09/Jun/2024:03:09:22]	192.168.1.17	200	GET /adm/config_form.php HTTP/1.1	http://192.168.1.16/adm/config_form.php
[09/Jun/2024:03:09:12]	192.168.1.17	200	GET /adm/ HTTP/1.1	http://192.168.1.16/

▼ 메일에 첨부된 CSV 파일 확인

경고 등록

경고 편집

설정

경고

근무 외 시간 Admin 페이지 접근 시도 탐지

설명

근무 외 시간에 관리자 페이지 접근 (주말)

검색

index=web_server method=*/adm*

|table client_time, src_ip, status, method, url

경고 유형

예약됨

실시간

크론 스케줄로 실행 ▼

시간 범위

마지막 20 분 ▶

크론 표현식

00,20,40 *** 0,6

취소

저장

트러거 작업

작업 추가 +

트러거되는 경우

이메일 보내기

받는 사람

0098121@naver.com, monitor24365@secui.com

성폭로 구분된 이메일 주소 리스트입니다.

포문으로 표시된 이메일 주소는 검색 시점에만 유효성이 검사됩니다.

CC 및 BCC 표시

우선순위

높음 ▼

제목

[긴급] 근무 외 시간 관리자 페이지

이메일 제목, 수신한 횟수 메시지는 검색 결과에 따라 색소를 삽입하는 포문이 포함될 수 있습니다. 자세히 알아보기

메시지

비 근무시간 관리자 페이지 접근이 발생하였습니다.
관리자 본인이 맞는지 확인 부탁드립니다.

포함

☒ 경고 링크

☒ 결과 링크

☐ 검색 문자열

☐ 인라 테이블

☐ 트리거 조건

☒ CSV 첨부

☐ 트리거 시간

☐ PDF 첨부

☒ 빈 첨부 파일 허용

유형

HTML 및 일반 ... 일반 텍스트

▼ 경고 - 근무 외 시간 Admin 페이지 접근 시도 탐지

6월 9일 3시 23분, 피싱사이트 확인

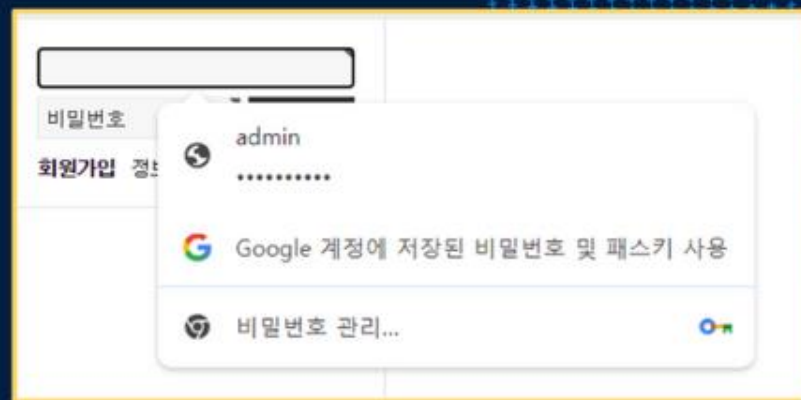


▼ T사를 모방한 피싱 사이트



▼ 메인페이지에 삽입된 리다이렉트 소스코드

InfoStealer 유포

T사의 관리자
계정 탈취

▼ Chrome 패스워드 자동완성 기능

문서작업 프로그램 불법 설치 파일 위장한 악성코드 주의보

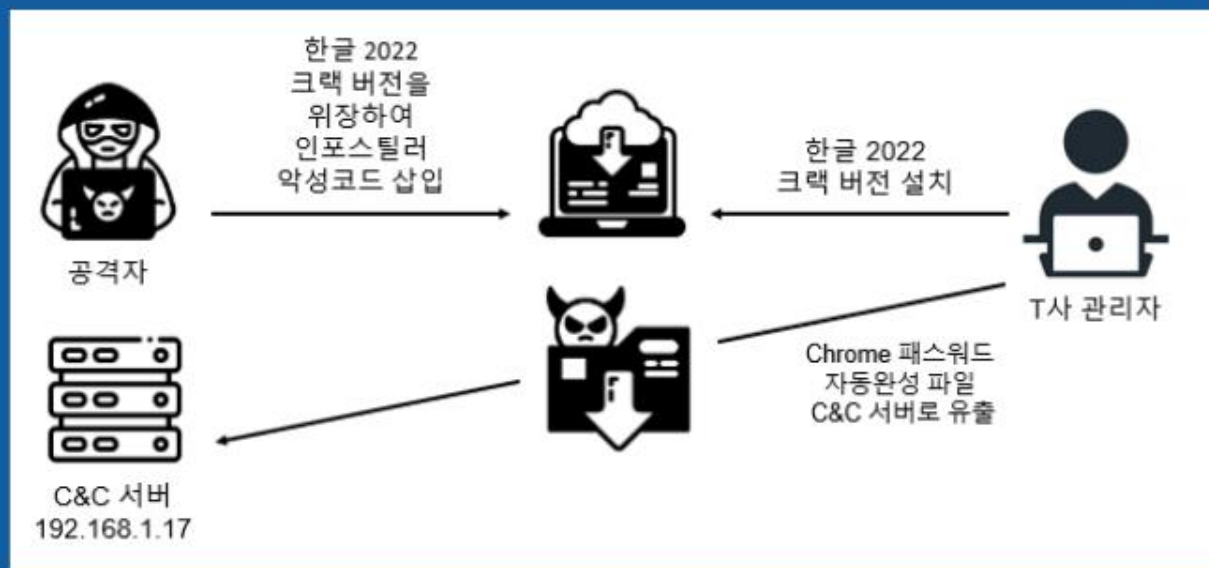
최근 '브라우저 자동 로그인' 기능 악용한 계정정보 탈취 범죄 급증

일례로 지난 2월 국가정보원은 국가·공공기관 정보 서비스 이용자 1만 3,000개 가량의 개인정보가 다 크웹에 유출됐다고 밝혔다. 해당 공격은 사용자의 아이디와 비밀번호 등 개인정보를 탈취하는 악성코드인 인포스틸러(Infostealer)를 활용한 것으로 드러났다. 공격자는 각종 콘텐츠 및 파일이 오가는 웹하드, P2P 사이트, 블로그 등에 인포스틸러를 은닉한 불법 소프트웨어를 유통하는 방식으로 악성코드를 퍼트렸다. 인포스틸러를 활용해 사용자의 아이디, 패스워드 등 개인정보를 탈취한 것이다.

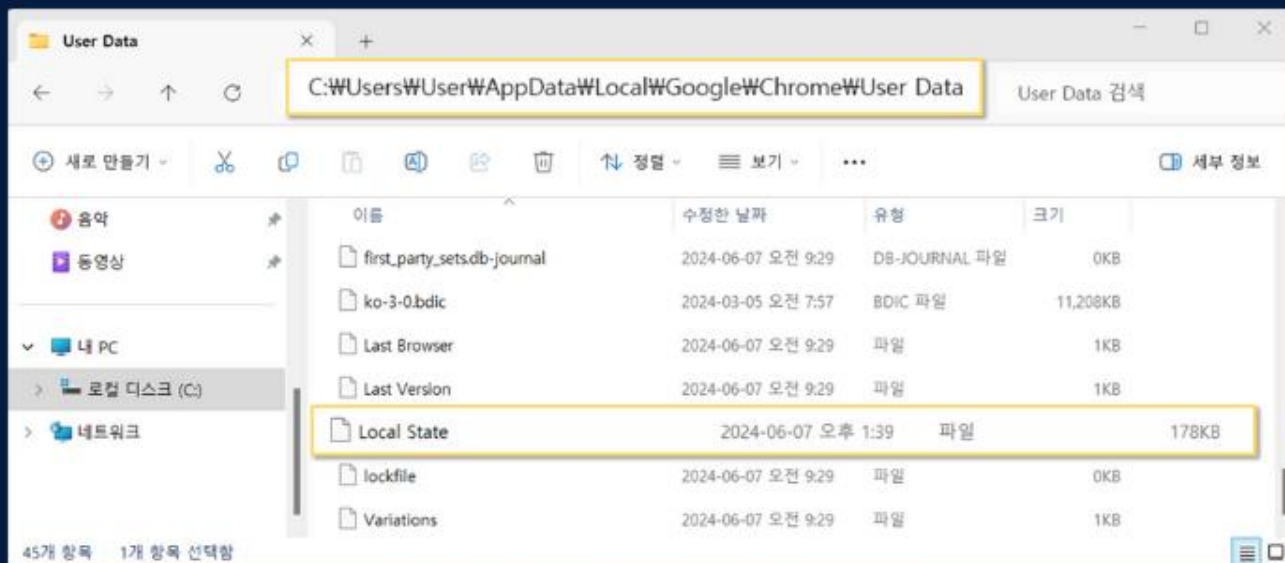
II

T사 적용 사례

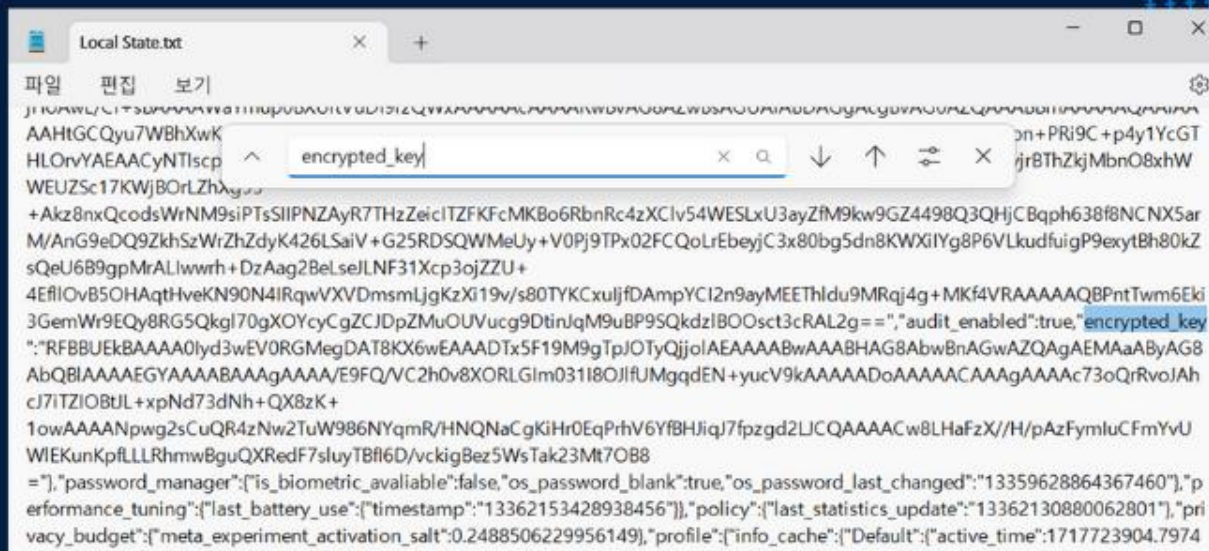
유출 과정 전개 - XSS로 인한 피싱 사이트 리다이렉트



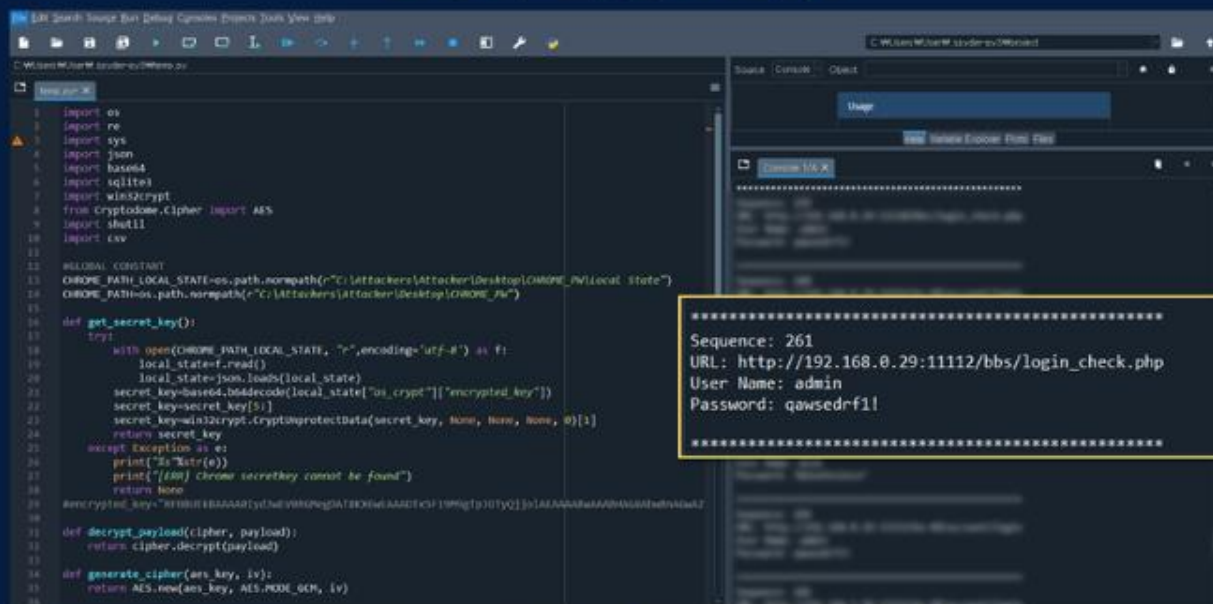
▼ T사 관리자 Chrome의 패스워드 자동완성 파일 탈취 과정



▼ 패스워드 자동완성 파일 저장 위치



▼ 암호화된 계정 정보 존재 확인



▼ 파일 복호화를 통해 관리자 계정 탈취 성공

II T사 적용 사례 유출 과정 전개 - XSS로 인한 피싱 사이트 리다이렉트

XSS 공격을 통해 Redirect

트래블 닷컴

전체메뉴

호텔

더보기

국내여행

더보기

최고관리자님

관리자 모드

쪽지 0

포인트 600

스크랩

정보수정

로그아웃

▼ 탈취한 계정으로 T사 관리자 로그인

ADMINISTRATOR

관리자정보 | 기본환경 | 부가서비스 | 커뮤니티 | 로그아웃

환경설정 | 회원관리 | 게시판관리 | SMS 관리

기본환경설정 | 관리자환경설정 | 테이블설정 | 메뉴설정 | 메일 테스트 | 팝업레이어관리 | 세션파일 일괄삭제 | 캐시파일 일괄삭제 | 컴쳐파일 일괄삭제 | 쉼네일파일 일괄삭제 | phpinfo | Browsercap 업데이트 | 접속로그 변환 | 부가서비스

메뉴설정

주의! 메뉴설정 작업 후 반드시 확인을 누르셔야 저장됩니다.

메뉴추가

메뉴	영크	상태	순서	PC사용	모바일사용	관리
전체메뉴<script>loc:11112/bbs/board.php?co_table=aaa	사용안함	0	사용함	사용함	추가 삭제	
전체메뉴<script>location.href="http://192.168.1.17/traveldotcom"</script>						

▼ 관리자 페이지에서 XSS 공격을 통해 피싱 사이트로 리다이렉트

개인정보 유출 사고 피해 최소화 및 사후 관리

01

2024/06/09 03:09
공격자가 관리자 페이지 접근


02

2024/06/09 03:09~
다양한 웹공격 시도

03

2024/06/09 03:20
관리자 페이지 접근 경고 메일 발송

04

 2024/06/09 03:23 ~
피싱사이트 확인
T사 사용자 개인정보 유출 위험성 발생

05

2024/06/09 03:26
고객사에 조치 요청

06

2024/06/10 11:00
고객사에 리포팅 및 솔루션 제안

공격 발생 17분 내
파악 및 조치 요청

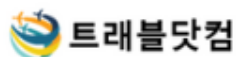


▼ 고객사 리포팅



▼ 추가 솔루션 제안

SECUI



보안관제 일일 보고서

SECUI

보고주기

[O] 일일 [I] 주간 [L] 월간

기본 정보

담당자	보안운영 ○○○ 프로	일 시	2024/06/09(월)
-----	-------------	-----	---------------

탐지 결과

최초탐지시간	2024/06/09(월) 03:20:00	위협등급	상
공격IP	192.168.1.17/한국	목적지IP	192.168.1.16
Action	Allow	탐지시나리오	근무 외 시간 Admin 페이지 접근 시도 탐지

탐지내용

[03:09:12] 공격IP 관리자 페이지 접근
[03:09:40~03:26:50] 웹 공격 시도_XSS, SQLI 공격, 파라미터 변조 로그 70건 발생
[03:20:00] suspicious_admin_access 시나리오 알림이 발생하여 외부 공격자의 접근 사실 인지
[03:23:20] 트래블닷컴 접속 시 메인 페이지와 유사한 피싱사이트로 리다이렉트되는 점을 확인하여 웹 프록시 툴로 소스코드 분석_메뉴 네비게이션 바에서 XSS 구문 확인
[03:26:50] 공격자의 IP를 확인 후 트래블닷컴 보안 담당자에게 블랙리스트 추가 요청 및 취약점이 확인된 위치 전달
[03:28:05] 블랙리스트IP로 등록되어 공격 종료

조치 결과

조치 내용

외부 IP(192.168.1.17)에서 관리자 페이지 접근이 확인되었으며 약 20분간 웹 공격시도가 지속적으로 발생하였습니다. 해당 공격 중 XSS가 성공 피싱사이트로 리다이렉션이 확인되었습니다. 고객사에게 연락하여 해당 IP 차단하였지만, 취약점이 보완된 것은 아니라 추가적인 조치가 필요하여 현재 CERT에 연계하여 분석 중입니다.

특이 사항

- 상단에 웹방화벽이 없어 상세로그 확인이 불가능 하므로, 시큐아이 파트너솔루션인 Monitorapp 사의 AIWAF 추가 권고 드립니다.
- menu_list.php Line79 - [해뉴] 폼이 사용자의 입력 값을 이스케이프 처리하도록 get_sanitize_input 함수 사용을 권고 드립니다.

AS-IS

```
<input type="text" name="me_name[]" value="<?php echo $me_name; ?>" id="me_name">?php echo $i; ?>" required class="required tbl_input full_input">
```

TO-BE

```
<input type="text" name="me_name[]" value="<?php echo get_sanitize_input($me_name); ?>" id="me_name">?php echo $i; ?>" required class="required tbl_input full_input">
```

Chapter

II

T사 적용 사례

- XSS로 인한 피싱 사이트 리다이렉트

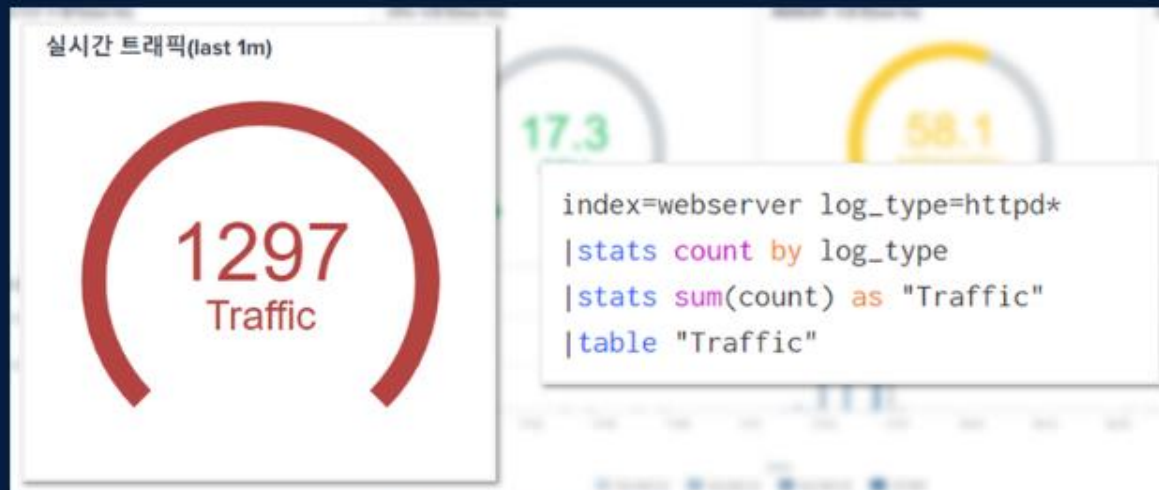
- DDoS

1. 사전 환경

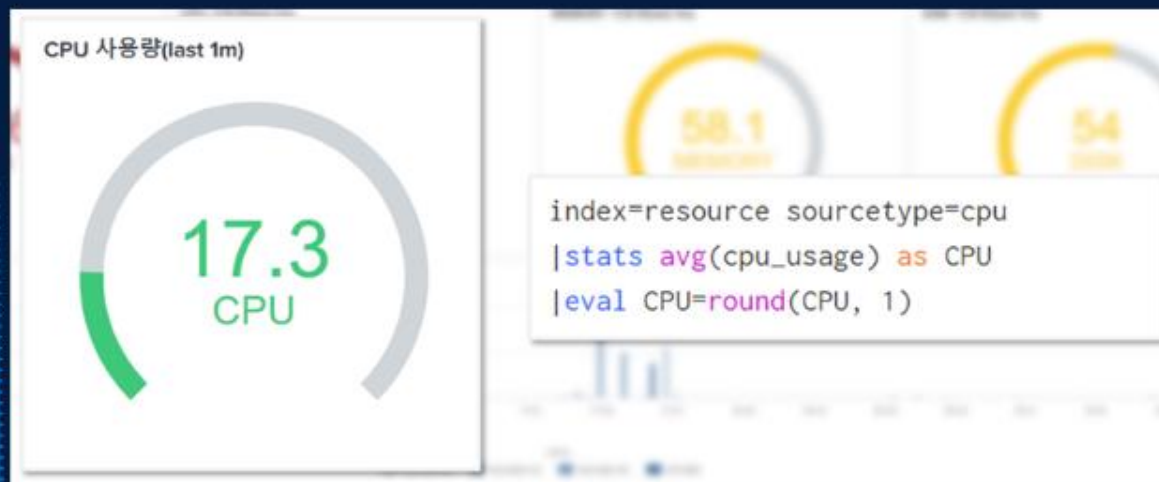
2. 공격 파악 과정

3. 결과

대시보드 구축

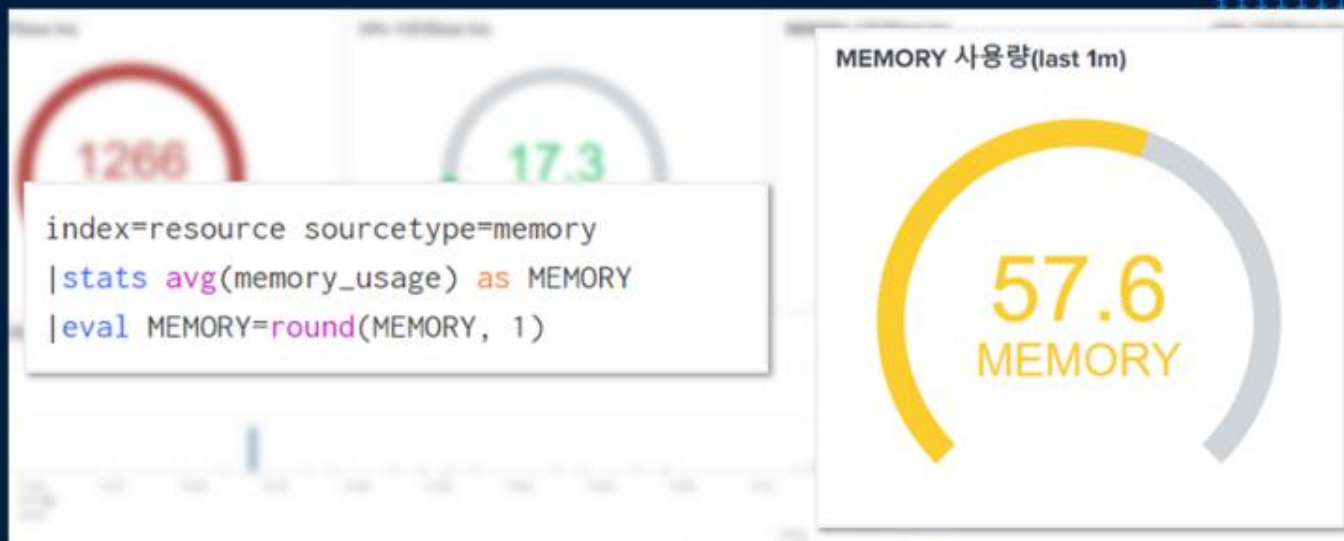


▼ 실시간 트래픽 (Last 1m)

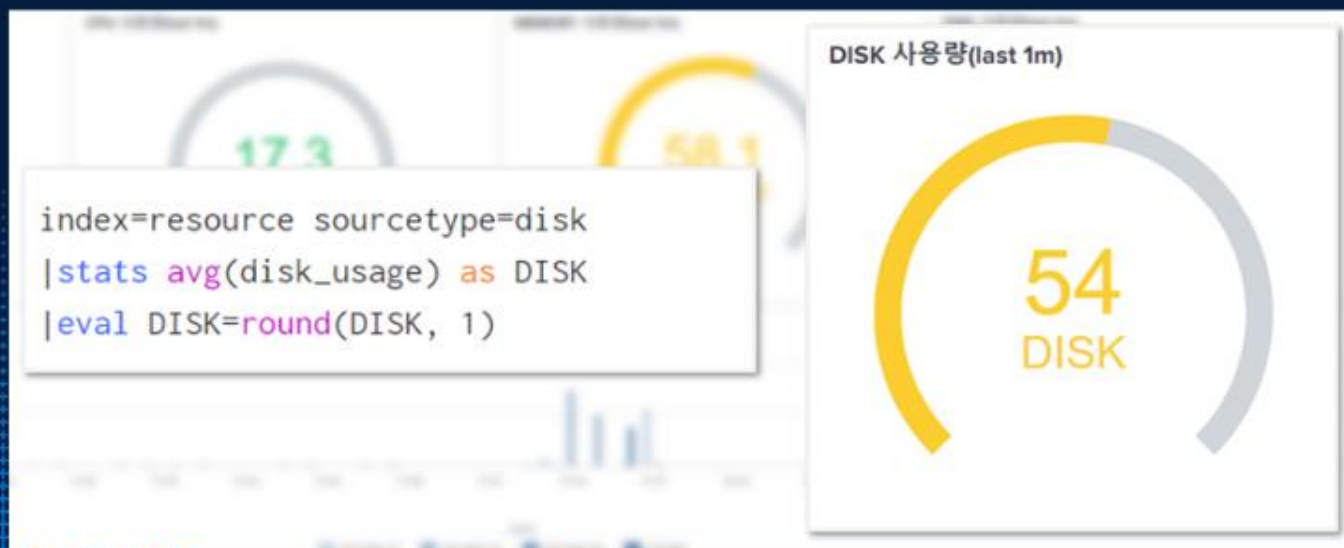


▼ CPU 사용량 (Last 1m)

II T사 적용 사례 사전 환경 - DDoS

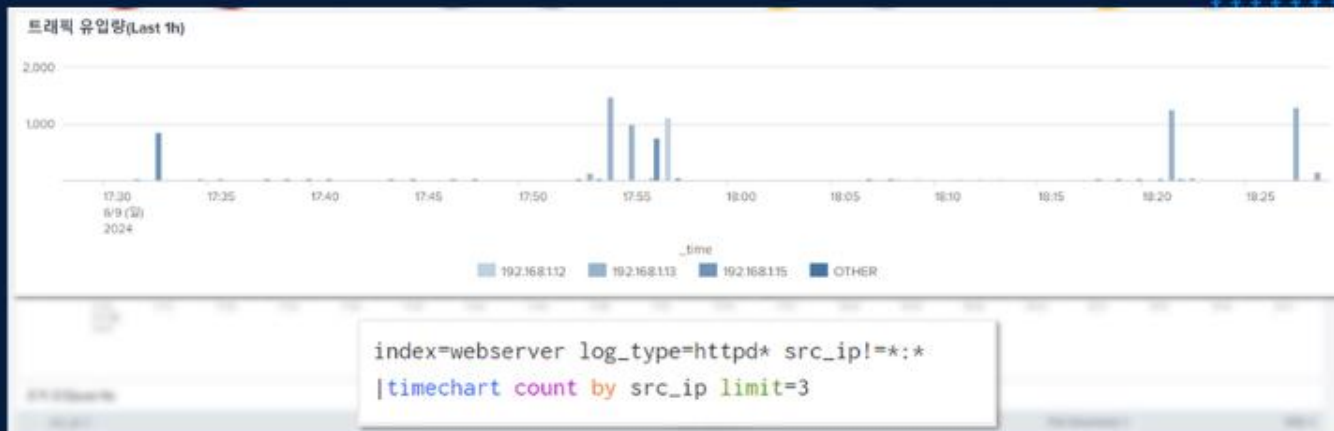


▼ MEMORY 사용량 (Last 1m)

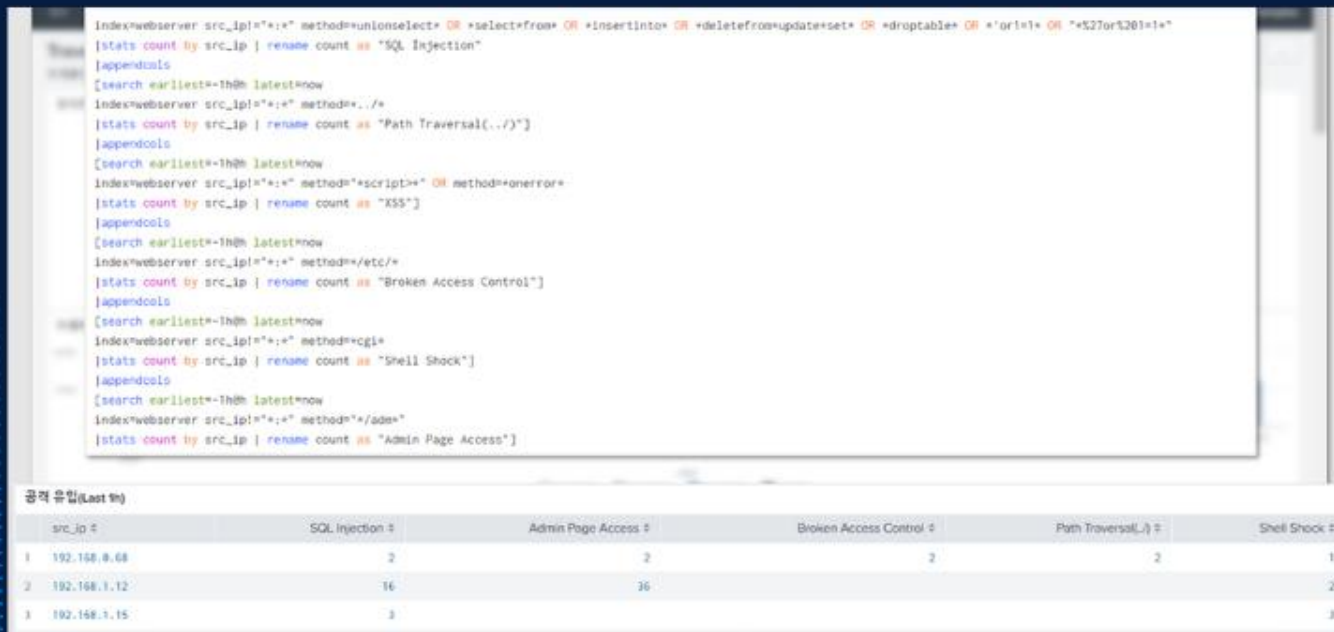


▼ DISK 사용량 (Last 1m)

II T사 적용 사례 사전 환경 - DDoS

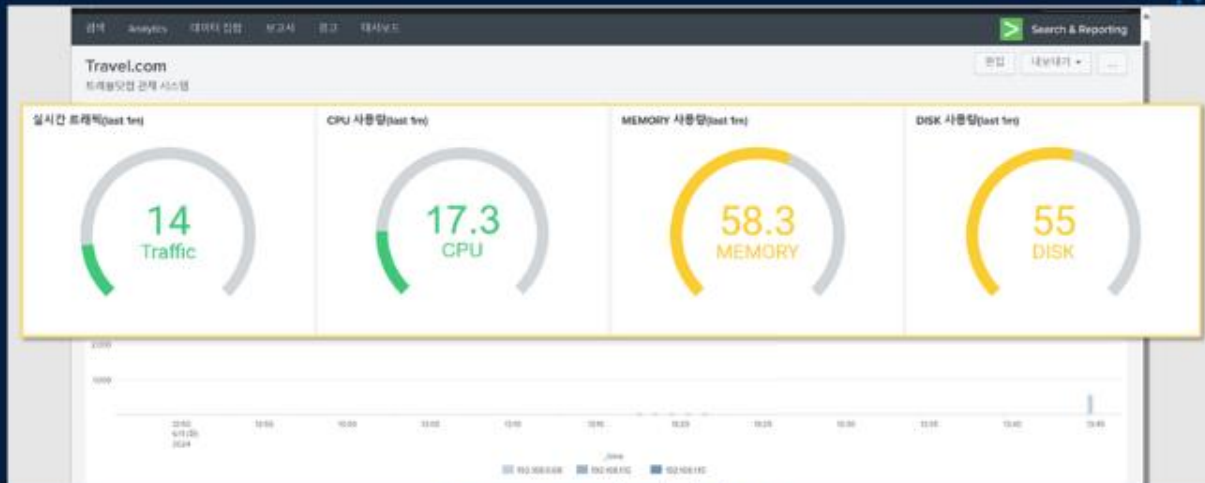


▼ 트래픽 유입량 (Last 1h)

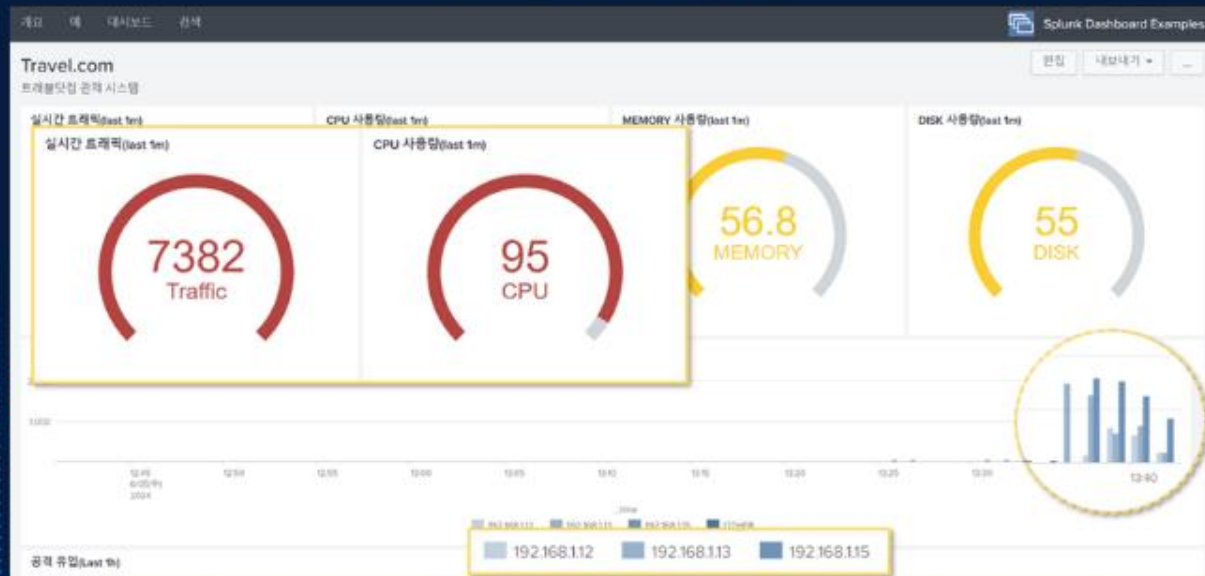


▼ 웹공격 유입 (Last 1h)

6월 5일 13시 35분, DDoS 발생



▼ DDoS 공격 전 대시보드



▼ DDoS 공격 후 대시보드

13시 35분, 경고 메일 발송

경고 만들기

설정

제목

외부 트래픽 과다 접근 탐지 (N:11분/7,000건)

설명

실시간 분당 7,000건 이상의 접근 탐지

검색

```
index=web_server log_type=*http*
|stats count by src_ip
|where count > 7000
```

앱

Search & Reporting (search) ▼

권한

비공개 앱에서 공유됨

경고 유형

예약됨 실시간

크론 스케줄로 실행 ▼

시간 범위

마지막 1분 ▶

크론 표현식

*/*1****

취소

저장

경고 편집

트리거 작업

트리거되는 경우

이메일 보내기

받는 사람

qkrdydgus987@naver.com
 ,monitor24365@secui.com

우선순위

정상 ▼

제목

Splunk Alert: \$name\$공격이 감지 !

메시지

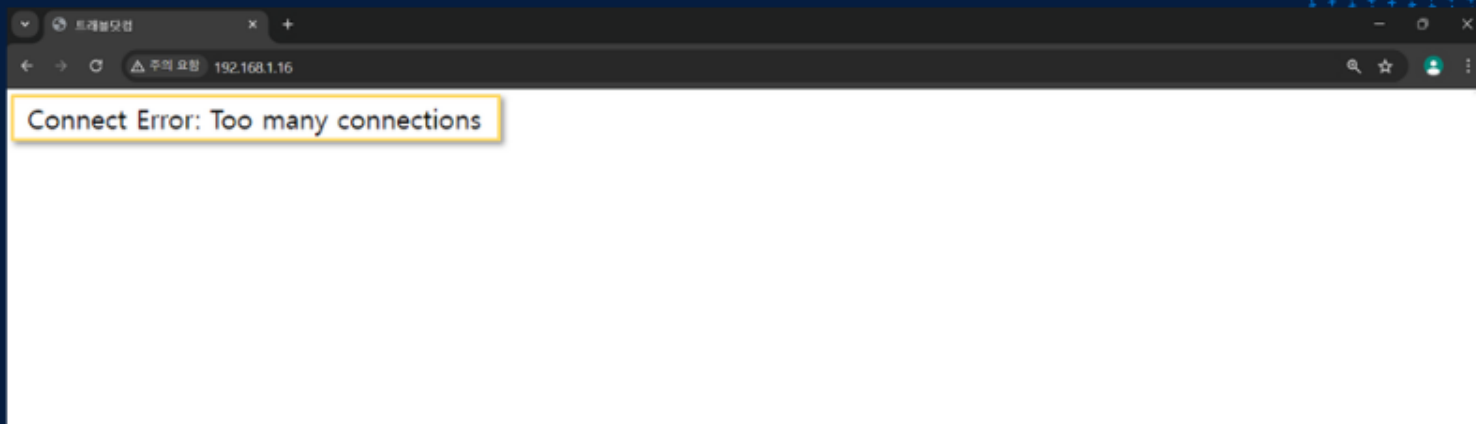
' \$name\$ ' 공격으로 의심되는 접근
 이 확인되었습니다.

▼ 경고 - 외부 트래픽 과다 접근 방지 (N:11분/7,000건)

src_ip	count
192.168.1.13	7005

▼ 메일에 첨부된 CSV 파일

13시 38분, T사 웹서비스 단절



▼ DDoS 공격으로 T사 홈페이지 서비스 단절



▼ 서비스 단절 후 대시보드

서비스 마비로 인한 피해 최소화 및 사후 관리

01

2024/06/05 13:35
DDoS 발생

02

2024/06/05 13:35
대시보드 확인, DDoS 경고 메일 발송

03

⚠ 2024/06/05 13:38
T사 웹서비스 단절

04

2024/06/05 13:38
IP 차단 요청

05

2024/06/05 13:45
모든 공격자 IP 차단 완료

06

2024/06/05 13:50
T사 웹 서버 리소스 정상 범주로 복구

공격 발생 10분 내
파악 및 조치 요청



▼ 고객사 리포팅



▼ 정상 범주로 복구된 T사 웹서버



▼ 추가 솔루션 제안

Chapter

III

기대 효과

1. 기대 효과

구축부터 분석, 조치 서비스를 제공하여 보안 관제 시스템 최적화

자동화된 실시간 경고

- ✓ 정확한 탐지 쿼리를 통한 즉각적인 경고 발송
- ✓ 메일, SMS, 텔레그램 등 다양한 알림 지원



실시간 경고



대시 보드

맞춤형 대시보드

- ✓ 다양한 차트, 그래프를 활용한 공격 현황 파악
- ✓ 고객사 니즈를 충족하는 맞춤형 대시보드 제작



솔루션

추가 솔루션 제안

- ✓ 다양한 자사 솔루션 보유로 고객사 환경에 적합한 솔루션 컨설팅
- ✓ 자사의 제품 뿐만 아니라 파트너사 솔루션 제안으로 체계적 대응 보장



산출물

체계적인 산출물

- ✓ 공격에 관련된 로그가 추출된 Excel 파일
- ✓ 고객사 리포팅 보고서

SECUI