



Threat Protection Profile

2021. 02

WAPPLES 탐지 룰

• Custom Rule

- 패턴 검증 방법까지 사용자 정의를 통하여 공격 트렌드의 변화에 따라 효율적이고 강력한 보안 유지
 - 논리적인 룰: 설정 (패턴, 검증, 검사 위치)들의 조합으로 다수, 다양한 룰을 정의
 - 신속한 적용: 신규 취약점을 이용한 공격을 즉각적으로 막을 수 있음
 - 사용자 맞춤형 기록: 효율적인 취약점 관리를 위한 룰 이름 및 탐지 패턴 설정이 가능

탐지 위치		
Request or Status Line	Method	
	Path	
	Query	Key(name)
		Value
	Status Code	
Header Lines		
Body		

다양한 탐지 위치가 존재함

사용자 정의로 설정

패턴 등록

패턴 그룹 이름: t2

검증 방법: Simple

탐지 근거: 테스트용입니다.

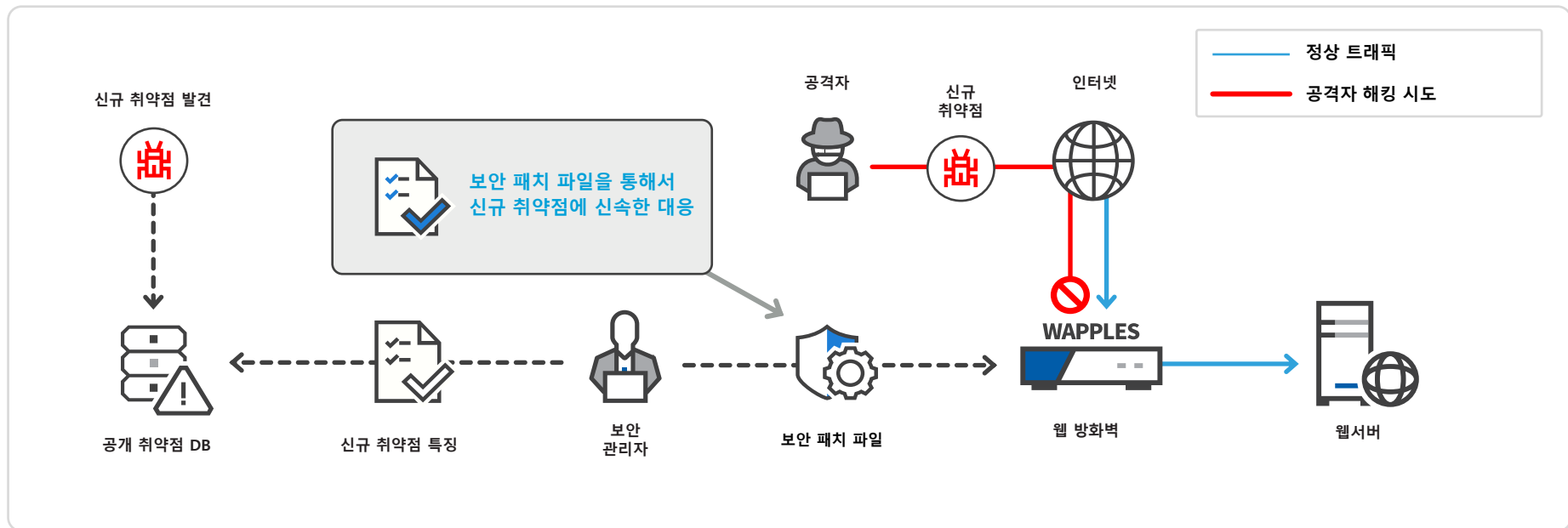
Q 검색...

☐	패턴 검증 순서	패턴	PART	REGEX	대소문자 구분
☐	Q	Q		(All)	(All)
☒	수정 1	test	requestline	☐	☐
☒	수정 2	abc	requestheader	☐	☐

보안 패치

• Threat Protection Profile (TPP)

- WAPPLES가 제공하는 탐지 룰로 차단할 수 없는 공격에 대해 긴급으로 대응하기 위한 보안 기능
- 기존 탐지 룰으로 대응 불가 시, 해당 취약점을 대응 하기 위한 Custom Rule을 이용한 형태
- 취약점 대응을 위한 보안 패치 파일을 자동/수동 업데이트 할 수 있는 기능
 - 보안 패치 파일은 펜타 시큐리티시스템에서 배포하며, 그 외 파일은 적용할 수 없음
 - 장비에 별도의 추가 설정 또는 설치 과정 없이 적용 가능
 - 5.0.12.26 이상 버전부터 기능 사용 가능



1. Threat Protection Profile

자동 업데이트

Threat Protection Profile 자동 업데이트

- **TPP 자동 업데이트 적용 조건**

- 자동 업데이트 기능은 5.0.12.31 이상 버전부터 가능
- WAPPLES 관리도구 IP로 펜타시큐리티시스템 자동 업데이트 서버에 접근 가능해야함
 - 자동 업데이트 서버 정보 (218.145.29.168:443)
- 자동 업데이트 기능은 장비의 유효성 검사를 위해서 제품 ID의 형식을 검증함
 - Appliance 의 경우 **W**XXXXXX-XXXXXXX (글자의 자릿수는 상관 없음)
 - VM의 경우 **WVX**-XXXXXX-XXXXXX (글자의 자릿수는 상관 없음)
 - 제품ID 형식과 다를 경우에는 자동 업데이트 불가
- 자동 업데이트 적용 불가 조건
 - PLS 연동 설정이 활성화(ON) 되어 있을 때
 - ✓ 양방향 동기화에서는 어느 한쪽이 우선하여 동기화 될지 알 수 없기 때문에, PLS 동기화 환경에서 자동 업데이트 ON 시 장애 발생 가능성이 높음
 - ✓ PLS 동기화 환경에서는 수동 업데이트 활용 권고
 - WAPPLES Control Center와 연동(ON) 되어 있을 때
 - ✓ WCC에서 현재 자동 업데이트 기능을 지원하지 않음
 - 향후 버전에서는 PLS 연동 시에도 자동 업데이트를 지원 되도록 개선 될 예정

Threat Protection Profile 자동 업데이트

• TPP 자동 업데이트 주기 및 영향도

- TPP 파일 서버에 보안 패치 파일 업데이트 시, 익일 새벽 3시 35분에 자동으로 패턴 업데이트
- 패턴이 새롭게 추가되어 자동 업데이트 된 경우, 실제 정책에 적용되기 전이기 때문에 서비스 영향도 없음
- 정책에 적용 중인 TPP 패턴이 새롭게 업데이트 되어 다시 받아온 경우는 정책 리로딩 작업이 발생
 - Rule_Change 이벤트가 발생함으로 탐지엔진이 설정을 재로딩하게 됨 (= 정책을 수정 후 저장하는 정도의 영향도)

보안 설정 > Threat Protection Profile (Threat Protection Profile을 관리합니다.)

자동 업데이트 ☒ ON 즉시 업데이트

⚠ 파일 업로드를 할 수 없습니다.

업데이트된 시각: 2021-01-20 09:09:51

업로드

삭제

☐	룰	버전	설명
	Q	Q	Q
	상세 WP-EDB-47144	1-0	Web Ofisi Rent a Car 3 - 'klima' SQL Injection
	상세 WP-EDB-47199	1-0	WebIncorp ERP - SQL injection
	상세 WP-EDB-47205	1-0	Rest - Cafe and Restaurant Website CMS - 'slug' SQL Injection
	상세 WP-EDB-47284	1-0	Web Wiz Forums 12.01 - 'PF' SQL Injection

저장

취소

Threat Protection Profile 자동 업데이트

- TPP 자동 업데이트 방법

- [보안 설정] → [보안 패치] → [Threat Protection Profile]
- 자동 업데이트 ON 설정 후 저장

2. Threat Protection Profile 수동 업데이트

Threat Protection Profile 수동 업데이트

- **TPP 수동 업데이트 적용 조건**

- 수동 업데이트 기능은 5.0.12.26 이상 버전부터 가능

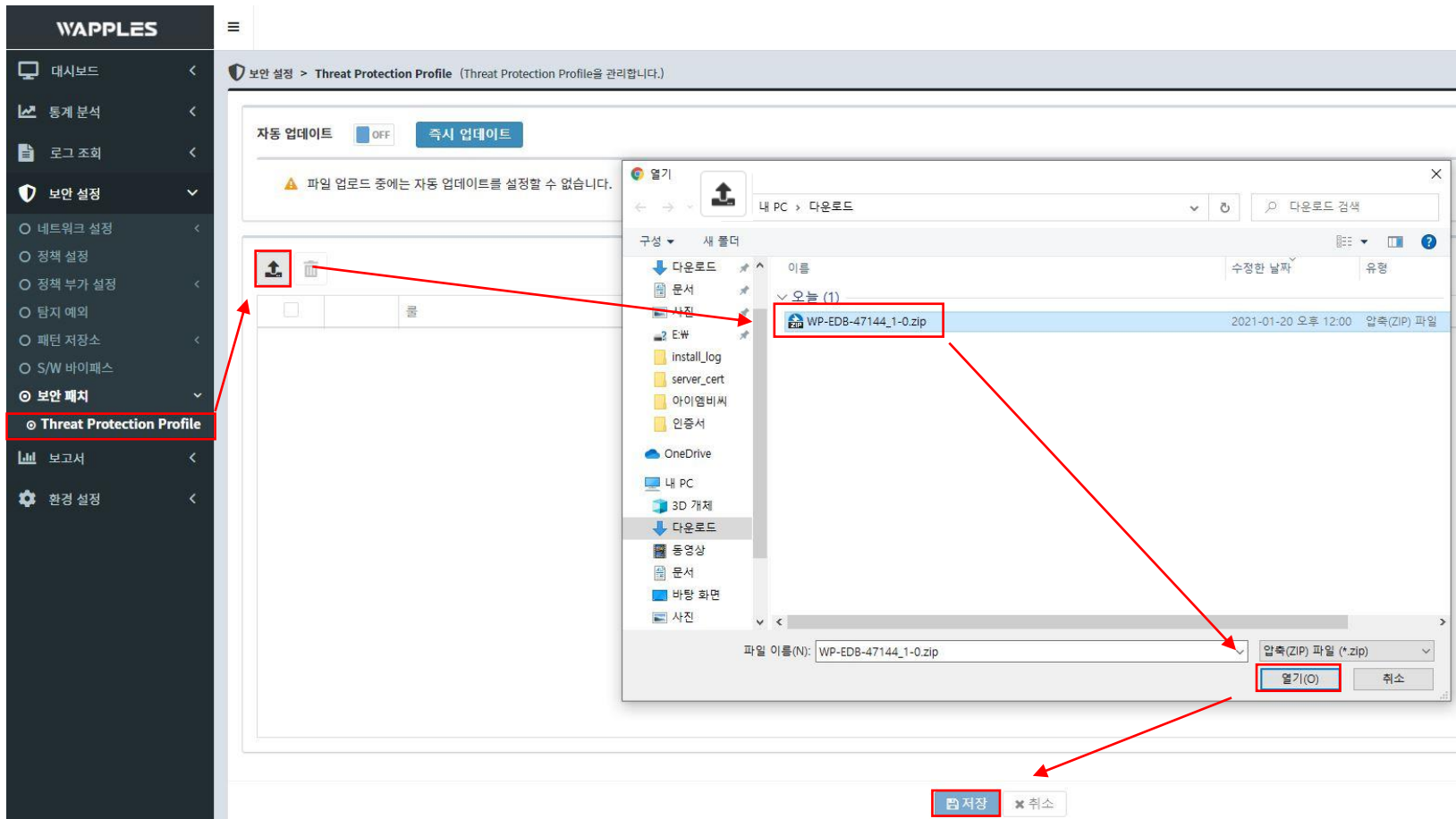
- **TPP 수동 업데이트 영향도**

- 자동 업데이트와 영향도는 같음
- TPP 패턴을 새롭게 다운로드 한 경우는 실제 정책에 적용되기 전이기 때문에 서비스 영향도 없음
- 정책에 적용 중인 TPP 패턴을 새롭게 업데이트 할 경우 정책 리로딩 작업이 발생
 - Rule_Change 이벤트가 발생함으로 탐지엔진이 설정을 재로딩하게 됨 (= 정책을 수정 후 저장하는 정도의 영향도)

Threat Protection Profile 수동 업데이트

• TPP 수동 업데이트 방법 #1

- [보안 설정] → [보안 패치] → [Threat Protection Profile]
-  클릭 후 보안 패치 파일 업로드
 - 원하는 보안 패치 파일만 적용하는 방식



Threat Protection Profile 수동 업데이트

- TPP 수동 업데이트 방법 #2

- [자동 업데이트 OFF] → [즉시 업데이트] → [확인]
 - TPP 파일 서버에 올라와 있는 모든 보안 패치 파일을 즉시 적용하는 방식

The screenshot displays the 'Threat Protection Profile' management page. At the top, a navigation bar shows '보안 설정 > Threat Protection Profile (Threat Protection Profile을 관리합니다.)'. Below this, the '자동 업데이트' (Automatic Update) section is highlighted with a red box, showing a toggle switch set to 'OFF' and a '즉시 업데이트' (Update Now) button. A red arrow points from the '즉시 업데이트' button to a confirmation dialog box. The dialog box contains the text: '192.168.63.155 내용: 설정한 내용은 반영되지 않습니다. 즉시 업데이트를 실행하시겠습니까?' (192.168.63.155 content: The set content will not be reflected. Do you want to run the immediate update?). The dialog has '확인' (Confirm) and '취소' (Cancel) buttons. Below the update section, a warning message states: '⚠ 파일 업로드 중에는 자동 업데이트를 설정할 수 없습니다.' (⚠ Cannot set automatic update while uploading files). At the bottom, there is a table with columns for '선택' (Select), '이름' (Name), '버전' (Version), and '설명' (Description). The table is currently empty, and a message '데이터 없음' (No data) is displayed at the bottom right.

3. Threat Protection Profile

정책 적용 방법

Threat Protection Profile 정책 적용 방법

- 자동/수동 업데이트를 통해 TPP 파일 다운로드 이후
 - [보안 설정] → [정책 설정] → Threat Protection Profile을 추가할 정책을 클릭
 - [룰 추가] 클릭
 - [룰 추가 방식 선택]에서 [Threat Protection Profile] 클릭

WAPPLES

보안 설정 > 정책 (WAPPLES에서 사용함 정책과 웹 사이트를 설정합니다.)

정책 목록

정책 설정 : TEST

+ 룰 추가

룰 추가 방식 선택

Threat Protection Profile

직접 입력

정책/웹 사이트	룰	탐지
6.무조건 차단	수정	버퍼 공격 탐지
5.PCI-DSS 보안 정책	수정	탐지
4.고급 보안 정책	수정	사용자 정의
3.표준 보안 정책	수정	탐지
2.기본 보안 정책	수정	탐지
1.탐지만 하고 차단 안 함	수정	2차 수준 차단
0.탐지없이 통과	수정	안전한 형식만 접근 가능
✓ TEST	수정	파일 Include 탐지
192.168.40.245:80	수정	사용자 정의
		탐지 안 함
		탐지 안 함
		탐지
		URL 공격 탐지
		탐지 안 함
		주민등록번호 및 신용카드 번호 탐지(한국)

룰 저장 취소

Threat Protection Profile 정책 적용 방법

• TPP 정책 적용 방법

- [룰 추가] 설정 화면 하단에 사전에 업로드한 보안 패치 파일 목록이 출력됨
- 출력된 목록 중 적용할 Profile을 클릭하면 화면 상단 [룰] 란에 선택한 Profile이 반영됨
- 필요에 따라 [대응 설정/위험도]를 설정한 후 [적용] → [저장]을 순차적으로 클릭

룰 추가

탐지 안 함 탐지

룰
WP-EDB-47144

대응 설정

☒ 차단하지 않음

☐ 연결 끊기

☐ 오류 코드 400 Bad Request

☐ 페이지 이동 http://

위험도

0 100 0

Threat Protection Profile

룰 이름	설명
WP-EDB-47144	Web Ofisi Rent a Car 3 - 'klima' SQL Injection
WP-EDB-47199	WebIncorp ERP - SQL Injection
WP-EDB-47205	Rest - Cafe and Restaurant Website CMS - 'slug' SQL Injection
WP-EDB-47284	Web Wiz Forums 12.01 - 'PF' SQL Injection

적용 취소

4. Threat Protection Profile

상세 정보

Threat Protection Profile 상세 정보

- TPP 상세 정보

WP-EDB-47144 상세 정보	
필드	내용
룰	WP-EDB-47144
버전	1-0
사용 중인 정책	없음
설명	Web Ofisi Rent a Car 3 - 'klima' SQL Injection

✓ 닫기

- 룰
 - WP-EDB-{일련번호}
 - WP-CVE-{년도}-{일련번호}
 - 자동 생성된 룰의 이름은 수정 불가
- 버전
 - 프로파일 최초 업로드 시 '1-0' 으로 생성
 - 미탐 및 오탐에 따라 Profile이 패치 될 때마다 룰의 버전이 갱신됨
- 사용 중인 정책
 - 해당 Profile이 적용된 정책명이 표기됨
- 설명
 - 선택한 Profile에 대한 정보가 표기됨

Threat Protection Profile 상세 정보

• TPP 탐지 로그

- 기존 탐지 로그 형태와 동일함
- 탐지 근거 : 탐지한 보안 패치 파일의 설명이 표기됨

로그 조회 > 탐지 로그 (탐지 규칙에 따라 탐지한 불과 대상자의 주소, 국가 등의 정보를 제공합니다.)

검색 필터

등록 삭제 초기화

필터 목록

검색 기간 실시간(최근 5분)

숨김 로그 전체(숨김 로그 포함) 숨김 로그만

검색

추가 조건

탐지 로그

1 건 STOP 9

탐	출발지 주소	국가	웹 사이트 이름	URL	목적지 주소	시각	
상세	WP-EDB-471...	192.168.30.101:60348	? Unknown	daehwan.co.kr:443	/index.php?kategori[]=0&klima[]=...	124.53.7.10:443	2021-01-22 11:12:01

탐지 로그 상세 정보 - Chrome

주의 요함 | 192.168.30.105/log/detect/detail/1

속성

필드	내용
정책	test
로그	WP-EDB-47144
프로토콜	HTTP2
출발지 주소	192.168.30.101:60344
국가	? Unknown
웹 사이트 이름	daehwan.co.kr:443
URL	https://daehwan.co.kr/ind...
목적지 주소	124.53.7.10:443
시각	2021-01-22 11:11:51
대응	자단하지 않음
응답 코드	200
위험도	0 (하)

데이터 스트림

Unicode(UTF-8)

Raw Data Decoded Data Request Response

```
.method: GET
.authority: daehwan.co.kr
.scheme: https
.path: /index.php?kategori[]=0&klima[]=1&vites[]=1&yakit[]=1
.cache-control: max-age=0
.sec-ch-ua: "Google Chrome";v="87", " NotA Brand";v="99", "Chromium";v="87"
.sec-ch-ua-mobile: ?0
.upgrade-insecure-requests: 1
.user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Safari/537.36
.accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng/*;q=0.8,application/signed-exchange;v=b3;q=0.9
.sec-fetch-site: none
.sec-fetch-mode: navigate
.sec-fetch-user: ?1
.sec-fetch-dest: document
```

탐지 근거

Web Ofisi Rent a Car 3 - 'klima' SQL Injection

확인



KOREA www.pentasecurity.co.kr

GLOBAL www.pentasecurity.com

JAPAN www.pentasecurity.co.jp



Cybersecurity
Excellence Awards
Winner 2018



Hot Company in
Web Application
Security for 2016



SC Magazine Europe
Best SME Solution



Asian Cyber
Security Vendor
of the Year



Recognized on the
Gartner WAF
Magic Quadrant



No.1 WAF
Vendor in the
APAC Region



ICSA Labs
Certified WAF



The First and Only
CCEAL4 Certified
WAF



PCI-DSS
Compliance