



2022 다학제간캡스톤 디자인 #35팀 최종 발표

버그바운티 플랫폼
가상 네트워크 환경 구축 프로젝트

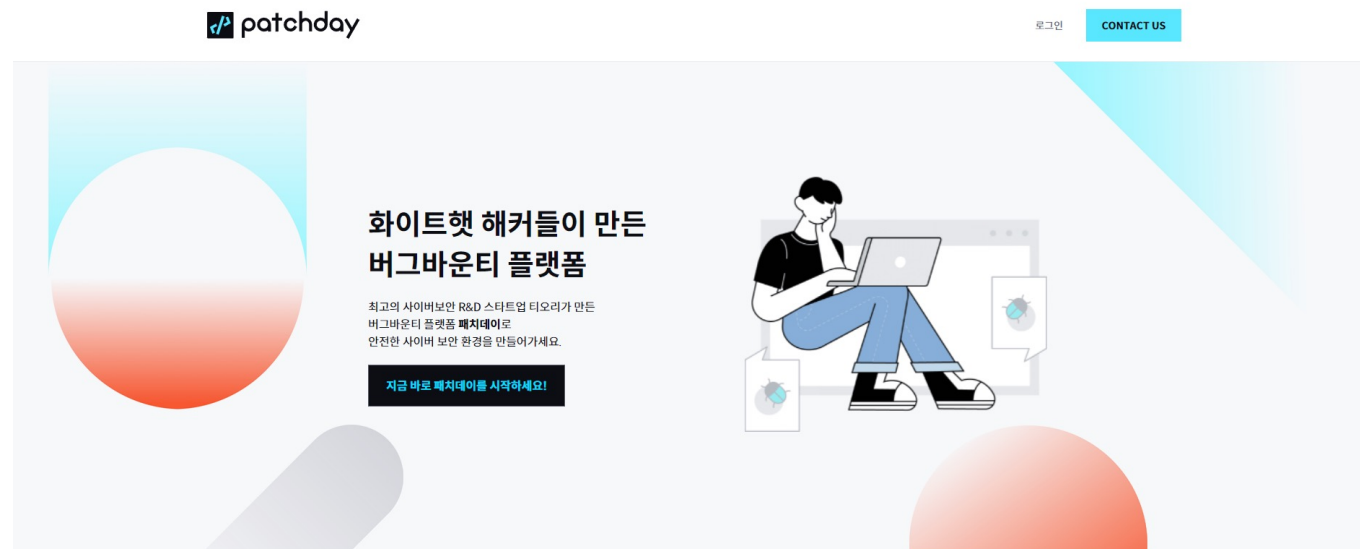
산학기관 및 서비스 소개



사이버 보안 R&D 스타트업



버그바운티 플랫폼 서비스





프로젝트 소개

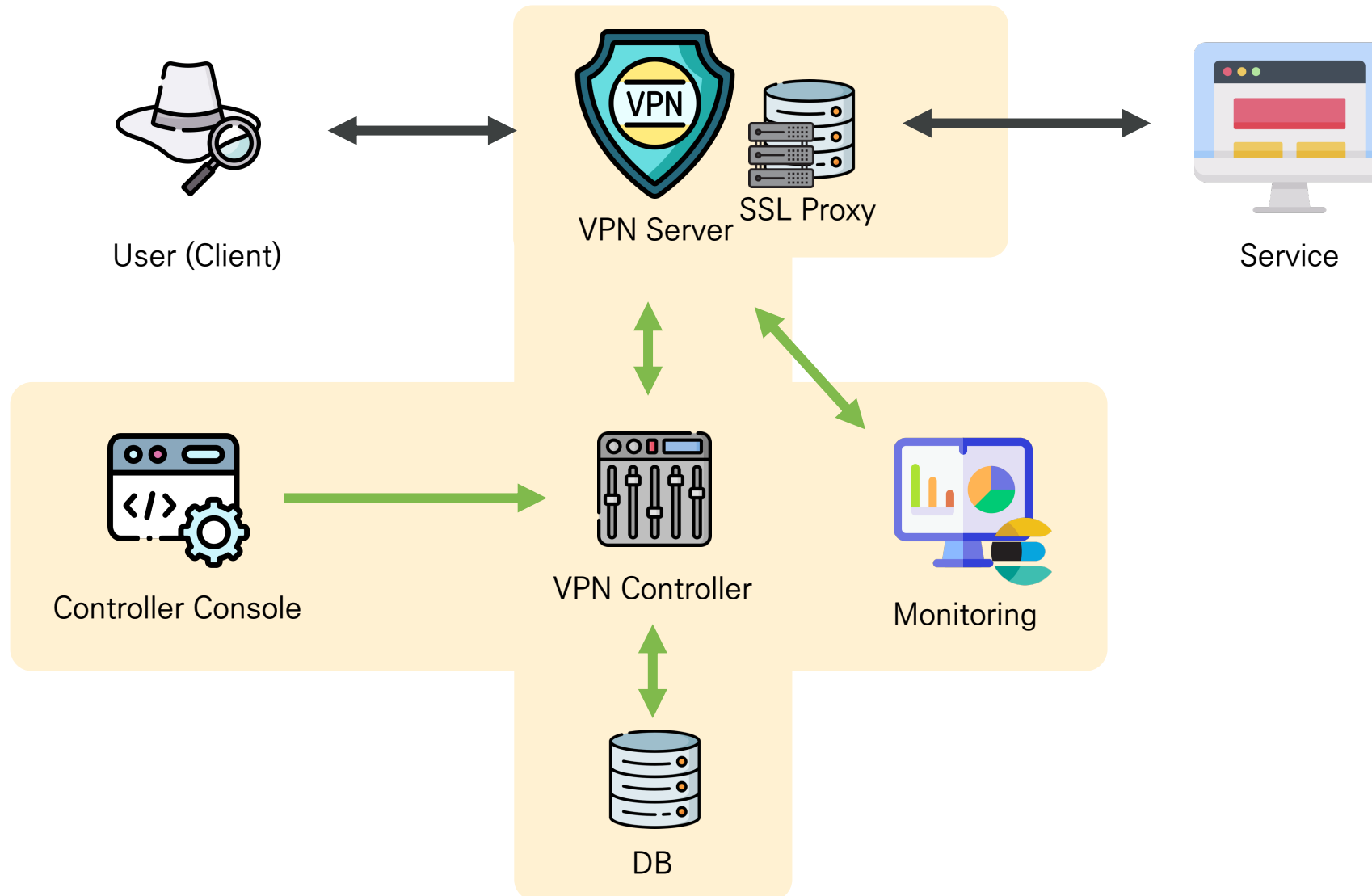
버그바운티 플랫폼

VPN Gateway 인프라 구축

버그바운티 참여 유저의 모의해킹 시도 현황 파악 및
관련 데이터 수집



프로젝트 구조





프로젝트 수행 설명

목표

- 1 VPN Gateway Infra 구축
- 2 VPN Controller 개발
- 3 트래픽 대시보드 및 조회 페이지 구축

프로젝트 수행 결과_VPN Gateway Infra

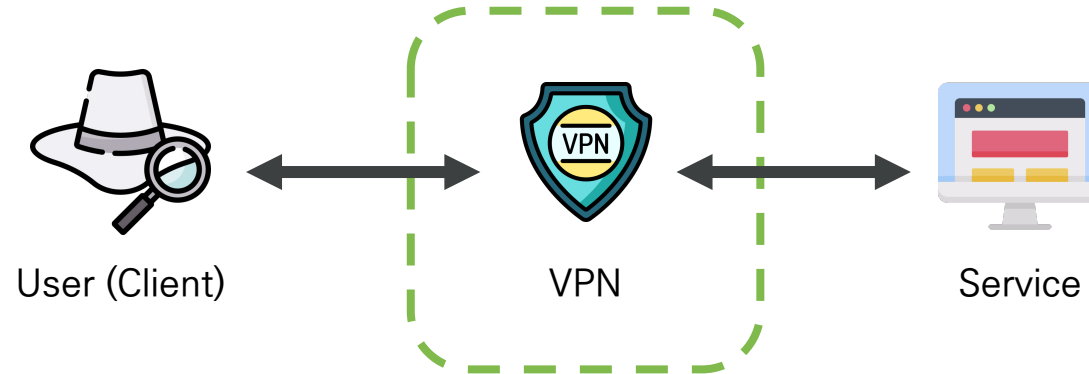


유저가 직접 서비스에 취약점 분석활동 수행



취약점 분석수행 여부 확인 어려움

프로젝트 수행 결과_VPN Gateway Infra



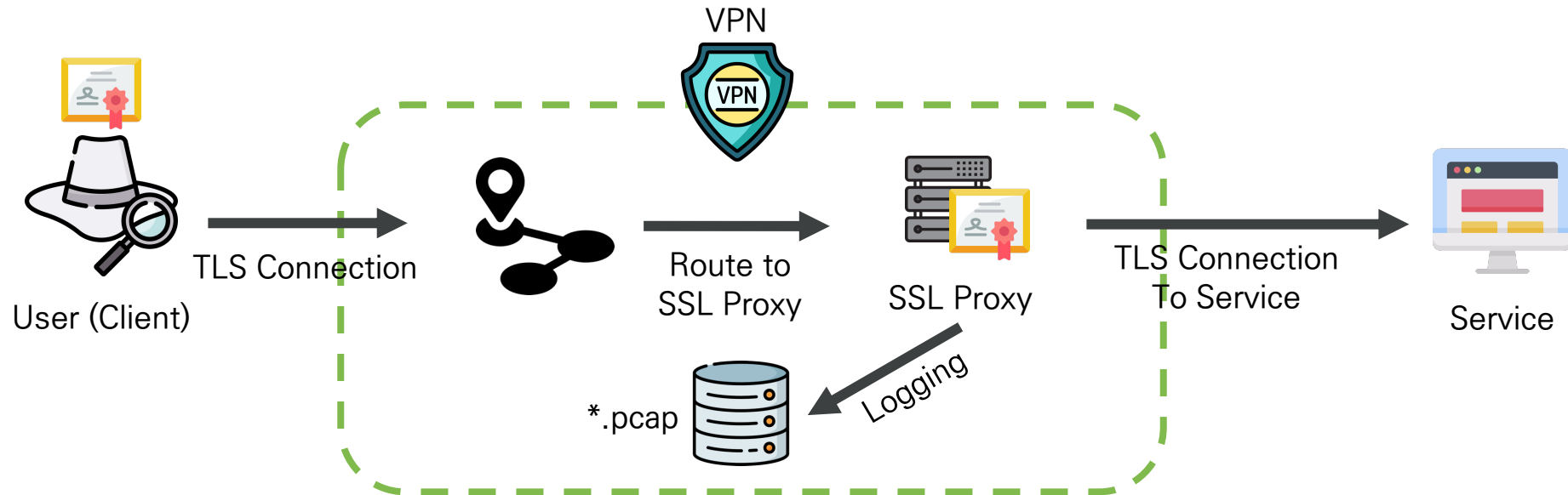
VPN을 통해 대상 서비스에 접속하여 버그바운티 활동을 수행
플랫폼이 유저의 버그바운티 활동여부를 식별할 수 있음

OpenVPN + AWS Instance

버그바운티 프로그램 서비스에만 라우팅

프로젝트 수행 결과_VPN Gateway Infra

TLS Cleartext



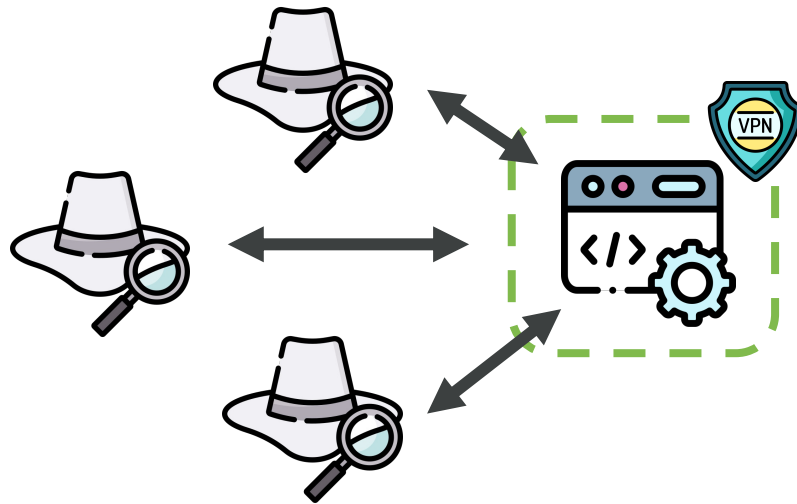
암호화된 TLS 패킷에 대해 Cleartext를 얻을 필요성

클라이언트의 요청이 VPN 서버에 SSL Proxy로 라우팅 후 Cleartext 획득,
이후 서비스로 다시 TLS 연결 수립 후 전송

Strip된 패킷 데이터는 별도의 pcap 로그로 저장
사후 사고분석 등 제한적 용도로 사용

프로젝트 수행 결과_VPN Controller

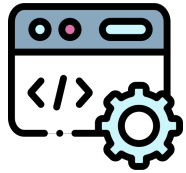
VPN Controller



OpenVPN 제공 Protocol을 사용한 VPN 관리 도구
각 유저의 인증, 접속 제어, 인증서 관리, VPN 세션 관리, VPN 로그 기록
컨트롤러 API + 웹 대시보드

프로젝트 수행 결과 _VPN Controller

VPN Controller



VPN 관리 프로토콜 파싱	VPN agent
인증, 세션 관리, 유저 관리	VPN Monitor
DB연동, 데이터 제공	Store Manager
API 제공	Gateway Manager

프로젝트 수행 결과 _VPN Controller

VPN Agent_Management protocol parse

```
<pd_openvpn_agent.vpn_monitor.Handler object at 0x7f4c31627f40>>, (b'n_clients', b'0'), {})  
<pd_openvpn_agent.vpn_monitor.Handler object at 0x7f4c31627f40>>, (b'untrusted_port', b'53741'), {})  
<pd_openvpn_agent.vpn_monitor.Handler object at 0x7f4c31627f40>>, (b'untrusted_ip', b'██████████'), {})  
<pd_openvpn_agent.vpn_monitor.Handler object at 0x7f4c31627f40>>, (b'common_name', b'██████████'), {})  
<pd_openvpn_agent.vpn_monitor.Handler object at 0x7f4c31627f40>>, (b'password', b'1'), {})  
<pd_openvpn_agent.vpn_monitor.Handler object at 0x7f4c31627f40>>, (b'username', b'user'), {})  
<pd_openvpn_agent.vpn_monitor.Handler object at 0x7f4c31627f40>>, (b'IV_SS0', b'webauth,openurl,crttext'), {})  
<pd_openvpn_agent.vpn_monitor.Handler object at 0x7f4c31627f40>>, (b'IV_GUI_VER', b'0CmacOS_3.3.5-4310'), {})  
<pd_openvpn_agent.vpn_monitor.Handler object at 0x7f4c31627f40>>, (b'IV_CIPHERS', b'AES-256-GCM:AES-128-GCM:CHACHA20-POLY1305'), {})
```

VPN 관리용 프로토콜 포트와 소켓통신 후 Listen
커맨드 메시지를 버퍼에서 읽어 정규식으로 파싱
파싱된 데이터로 핸들링

프로젝트 수행 결과 _VPN Controller

VPN Agent_Management protocol parse

```
>[COMMAND]:[CONTENT]
>[COMMAND]:ENV, [ENV_VALUE]
...
>[COMMAND]:END
```

Command Msg



Type	->	COMMAND
Handle Method	->	CONTENT
Env Values	->	ENV_VALUE

Parsed data



```
_topics = {
  b"BYTECOUNT": "_handle_bytecount",
  b"ECHO": "_handle_echo",
  b"STATE": "_handle_state",
  b"CLIENT": "_handle_client",
  ...
}

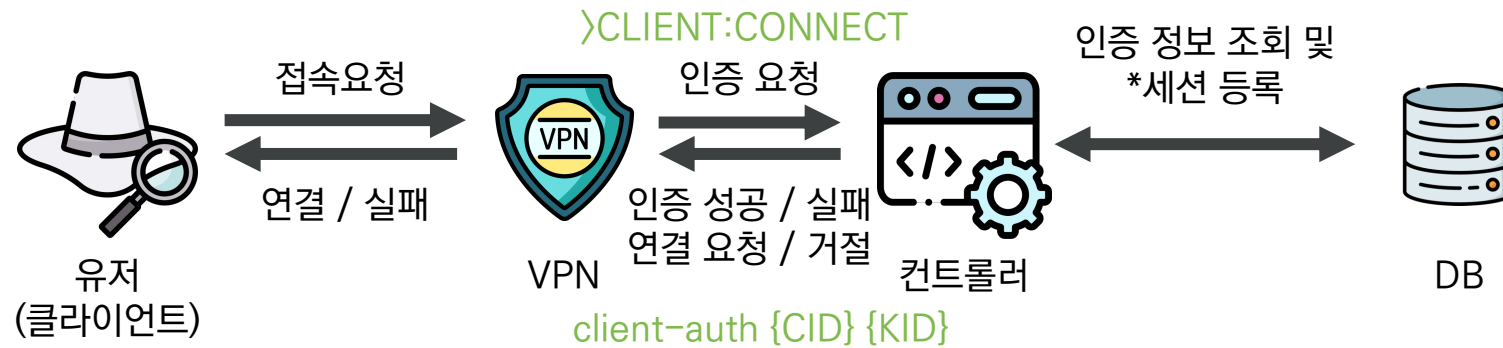
_client_topics = {
  b"CONNECT": "_handle_client_connect",
  b"REAUTH":
    "_handle_client_cr_response",
  b"ENV": "_handle_client_env",
  ...
}
```

Handle methods

VPN 관리용 프로토콜 포트와 소켓통신 후 Listen
커맨드 메시지를 버퍼에서 읽어 정규식으로 파싱
파싱된 데이터로 핸들링

프로젝트 수행 결과 _VPN Controller

VPN moitor_VPN 연결 요청된 사용자에게 대한 인증 및 연결 수립



VPN에서 인증요청
컨트롤러에서 접속 요청 유저 유효 여부 검증
유효한 유저는 성공 응답 반환, 세션 등록

프로젝트 수행 결과 _VPN Controller

Store

id	sso_user_id	x509_common_name	username	password	created_at	updated_at	is_valid	invalidated_at
2					2022-05-21 11:14:51.249847	2022-05-21 11:14:51.249847	t	
1					2022-05-20 12:58:09.86103	2022-05-20 12:58:09.86103	t	
3					2022-05-23 05:48:14.048602	2022-05-23 05:48:14.048607	t	
4					2022-05-23 06:04:44.089272	2022-05-23 06:04:44.089276	t	
5					2022-05-23 06:06:21.485813	2022-05-23 06:06:21.485817	t	
6					2022-05-23 07:12:47.982543	2022-05-23 07:12:47.982547	t	
9					2022-05-23 07:16:23.115688	2022-05-23 07:16:23.115692	t	
11					2022-05-23 08:11:32.339605	2022-05-23 08:11:32.339609	f	
13					2022-05-23 08:50:18.978458	2022-05-23 08:50:18.978461	t	
12					2022-05-23 08:31:50.862718	2022-05-23 08:31:50.862722	f	
14					2022-05-23 13:16:07.60943	2022-05-23 13:16:07.609437	t	
(11 rows)								

id	user_id	initial_public_peer_address	initiated_at	reset_request_id
d2e5fb71-8d85-4083-99b9-d9d39447d17a	14	61.82.	2022-05-23 13:29:59.619514	
bc93513d-49ab-43fa-bf71-175a99756478	14	61.82.	2022-05-23 13:22:11.602012	100
81eaf494-8e81-45a9-8d61-f5808a94e988	14	61.82.	2022-05-23 13:20:08.075899	99
c0ad6772-5bbd-411e-bdbb-6fa1aaa20340	14	61.82.	2022-05-23 13:18:10.696073	97
3afe9983-092a-41e2-b8a7-3e1a4e5bbb2b	14	61.82.	2022-05-23 13:16:22.457639	

id	user_id	session_id	issued_at
40		b11b3d13-5077-4c50-a40a-5374b050be3f	2022-05-23 05:20:20.738545
41		e87eae6c-0e1d-451f-bd6c-44a9f16f6b52	2022-05-23 05:28:59.197958
42		51a01fce-c06b-4805-bb8f-bbed119acac1	2022-05-23 05:36:05.858937
43		bdb4d34d-2030-4a51-a56c-fc188a707295	2022-05-23 05:38:37.038902

유저정보, 세션 정보, 이벤트 정보 등
VPN 이벤트 로깅

프로젝트 수행 결과 _VPN Controller

Gateway Manager_API

유저 목록, 세션목록 등 데이터 조회

웹 인터페이스로 컨트롤러 명령 전송

세션 종료

인증서 발급

유저 비활성화

```
[
  {
    "expired_at": "None",
    "initial_public_peer_address": "██████████",
    "initial_public_peer_port": 1194,
    "initiated_at": "2022-05-20 13:04:32.714371",
    "private_gateway_address": "10.8.0.2",
    "private_source_address": "10.8.0.1",
    "reset_request_id": null,
    "session_id": "bc04cbae-471d-48b5-99f1-71fb1541b7bf",
    "user_id": 1
  },
  {
    "expired_at": "None",
    "initial_public_peer_address": "██████████",
    "initial_public_peer_port": 1194,
    "initiated_at": "2022-05-20 13:18:03.553600",
    "private_gateway_address": "10.8.0.2",
    "private_source_address": "10.8.0.1",
    "reset_request_id": null,
    "session_id": "6a88441c-6286-4f2c-bb28-fea7b008201b",
    "user_id": 1
  },
  {
    "expired_at": "None",
    "initial_public_peer_address": "██████████",
    "initial_public_peer_port": 1194,
    "initiated_at": "2022-05-20 13:28:02.481715",
    "private_gateway_address": "10.8.0.2",
    "private_source_address": "10.8.0.1",
    "reset_request_id": null,
    "session_id": "ccee8cea-4466-4241-a0fa-05183a5f914e",
    "user_id": 1
  },
  {
    "expired_at": "None",
    "initial_public_peer_address": "██████████",
    "initial_public_peer_port": 1194,
    "initiated_at": "2022-05-20 13:31:01.004483",
    "private_gateway_address": "10.8.0.2",
    "private_source_address": "10.8.0.1",
    "reset_request_id": null,
    "session_id": "4c821907-8c8a-41b8-9aa7-8ea0723bd85f",
    "user_id": 1
  }
],
```

프로젝트 수행 결과 _VPN Controller

Session & user management

Admin

홈

프로그램 관리

벤더 관리

세션 관리

보고서 관리

VPN 관리

결제 관리

개인정보 보호정책

이용약관

Contact us

대시보드

유저 관리

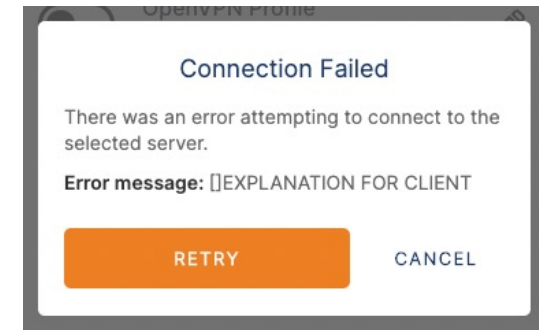
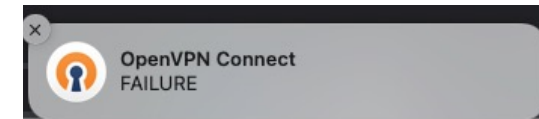
전체 세션	활성화 된 세션	전체 유저	차단 유저
41	1	11	2

활성화 VPN 세션

세션ID	UID	유저 IP	최초 접속시간	제어
8b21b8dd-921c-42ac-9fbd-b26e7762b958	14	61.82. [REDACTED]	2022-05-23 14:12:57.985166	<button>kill</button>

최근 VPN 세션

세션ID	UID	유저 IP	최초 접속시간	활성화
dedfad99-2e75-407f-99cb-7e1158c696df	1	14.33. [REDACTED]	2022-05-23 05:12:47.538794	● 비활성화
b11b3d13-5077-4c50-a40a-5374b050be3f	1	14.33. [REDACTED]	2022-05-23 05:13:18.458007	● 비활성화
e87eae6c-0e1d-451f-bd6c-44a9f16f6b52	1	14.33. [REDACTED]	2022-05-23 05:28:29.051772	● 비활성화
51a01fce-c06b-4805-bb8f-bbed119acac1	1	14.33. [REDACTED]	2022-05-23 05:35:56.380726	● 비활성화
72b491e4-21d0-48c2-a9f4-d938cd8df661	6	14.32. [REDACTED]	2022-05-23 09:13:39.026814	● 비활성화
bdb4d34d-2030-4a51-a56c-fc188a707295	1	14.33. [REDACTED]	2022-05-23 05:38:31.701776	● 비활성화
e8811875-32d0-4e06-9206-b12d5dc1ba4c	5	14.33. [REDACTED]	2022-05-23 06:06:50.954035	● 비활성화
84c59070-867b-40ec-9c85-b4d0f5f52279	1	14.32. [REDACTED]	2022-05-23 06:46:16.654047	● 비활성화
f1b6a8d0-3da3-4a7e-8a1f0d-8b872d13470b5	1	14.33. [REDACTED]	2022-05-23 07:20:31.407545	● 비활성화

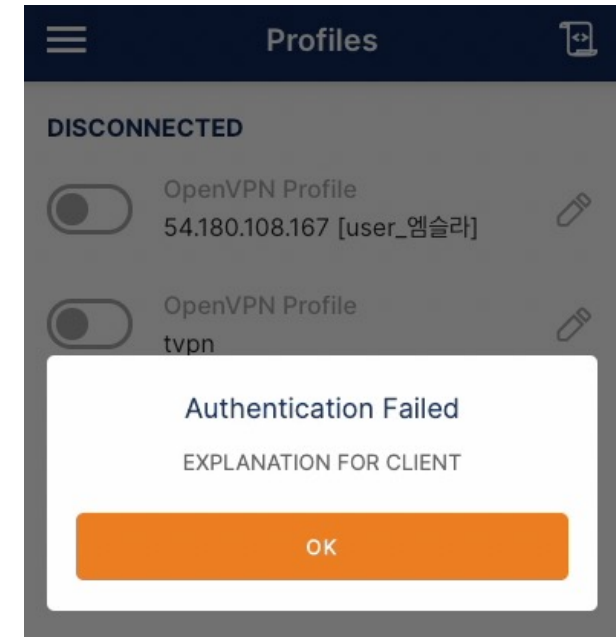


접속 세션 목록 조회 및 제어 (kill)

프로젝트 수행 결과 _VPN Controller

Session & user management


대시보드		유저 관리			
UID	CN	유저명	생성일	활성화	제어
2	127.0.0.2	msouler	2022.05.21. 20:14:51	● 활성화	revoke
1	127.0.0.1	user	2022.05.20. 21:58:09	● 활성화	revoke
3	Alice	alice	2022.05.23. 14:48:14	● 활성화	revoke
4	Bob	bob	2022.05.23. 15:04:44	● 활성화	revoke



유저 목록 조회 및 유저 비활성화

프로젝트 수행 결과 _VPN Controller

인증서(프로파일) 발급



대시보드

프로그램

인박스

Daydream

리더보드

새소식

< 내 프로필로

프로필 수정

추가정보

보안 인증

계정관리

알람 설정

초대 관리

쿠폰 등록

VPN 설정 beta

VPN 설정

VPN 서비스는 일부 프로그램과 사용자에게 적용됩니다.

활당된 인스턴스

인스턴스 #1

[Patchday TLS 인증서 다운로드](#)

발급된 인증서

발급된 인증서가 없습니다.

발급 요청

주의사항

- 패치데이 VPN을 통해 진행된 버그바운티 프로그램의 활동내역이 저장됩니다.
- VPN 인스턴스는 계정당 1개이며 활동 상황에 따라 활성화 / 비 활성화 될 수 있습니다.
- VPN을 통해 저장된 내역은 엄격한 보안을 준수하여 오직 활동 현황 파악, 통계 및 사고조사 용도로만 제한적으로 사용됩니다.
- VPN의 비 정상적 활동 내역이나 의심 정황 발견시 예고 없이 조치될 수 있습니다.

이용약관

개인정보보호정책

새소식

Contact Us

Copyright © 2019 - 2022 Theori Inc. All rights reserved.





pd-ca.crt



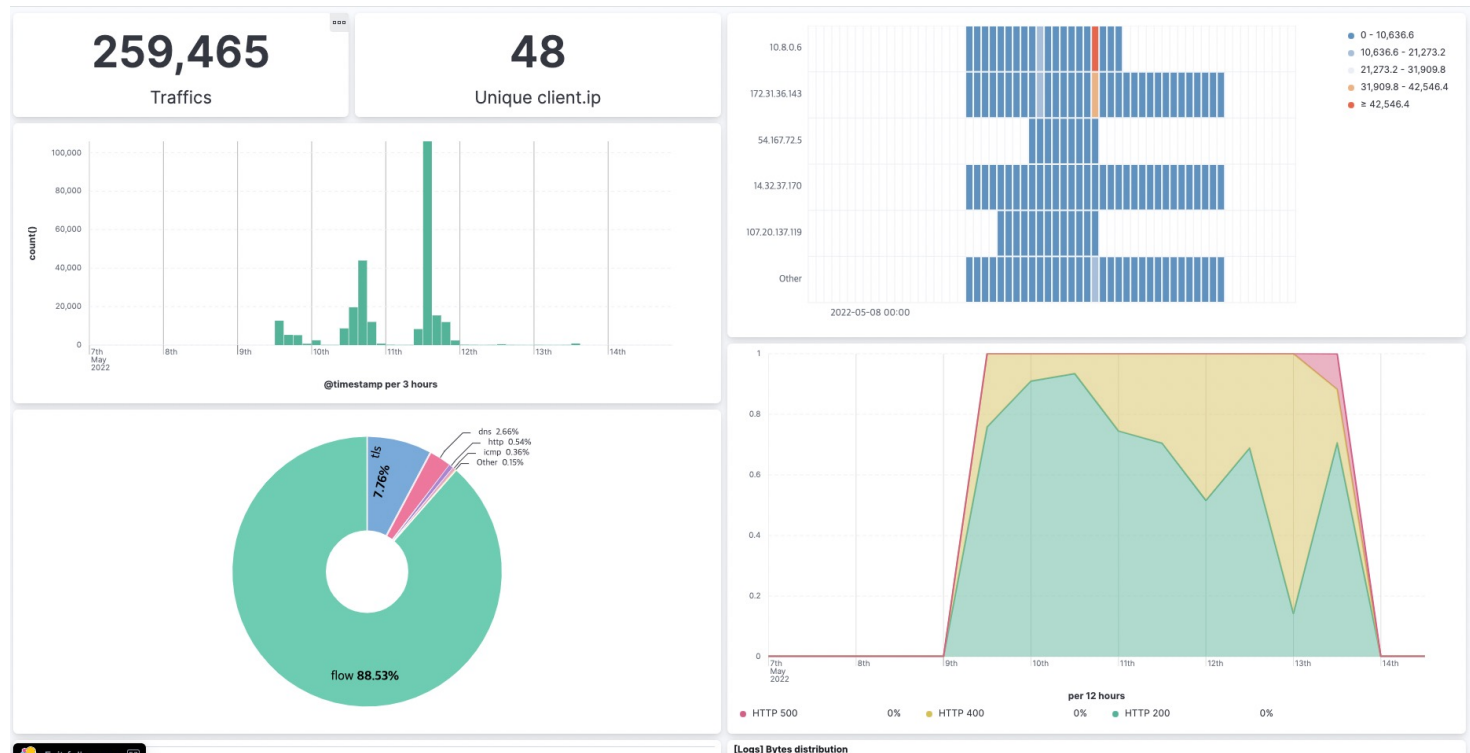
pd-01.ovpn

프로젝트 수행 결과

트래픽 대시보드 및 조회 페이지 구축

ELK Stack (Elasticsearch) 사용

인스턴스 내 In/Out bound 패킷 로깅 / 시각화



프로젝트 수행 결과

트래픽 대시보드 및 조회 페이지 구축

ELK Stack (Elasticsearch) 사용

인스턴스 내 In/Out bound 패킷 로깅 / 시각화



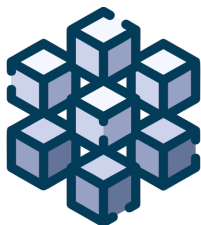
프로젝트 수행 결과

트래픽 대시보드 및 조회 페이지 구축

트래픽 알림 플러그인

플러그인이 polling 방식으로 elasticsearch에 질의
과다 트래픽 발생과 같은 이상 상황 발견 시
사내 Slack 채널에 알림을 띄워 대응하게 함

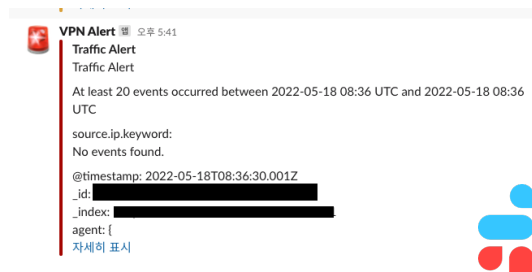
추후 Suricata 같은 IDS와 연동시 더 다양한 상황 대비



트래픽 발생



플러그인
규칙 탐색

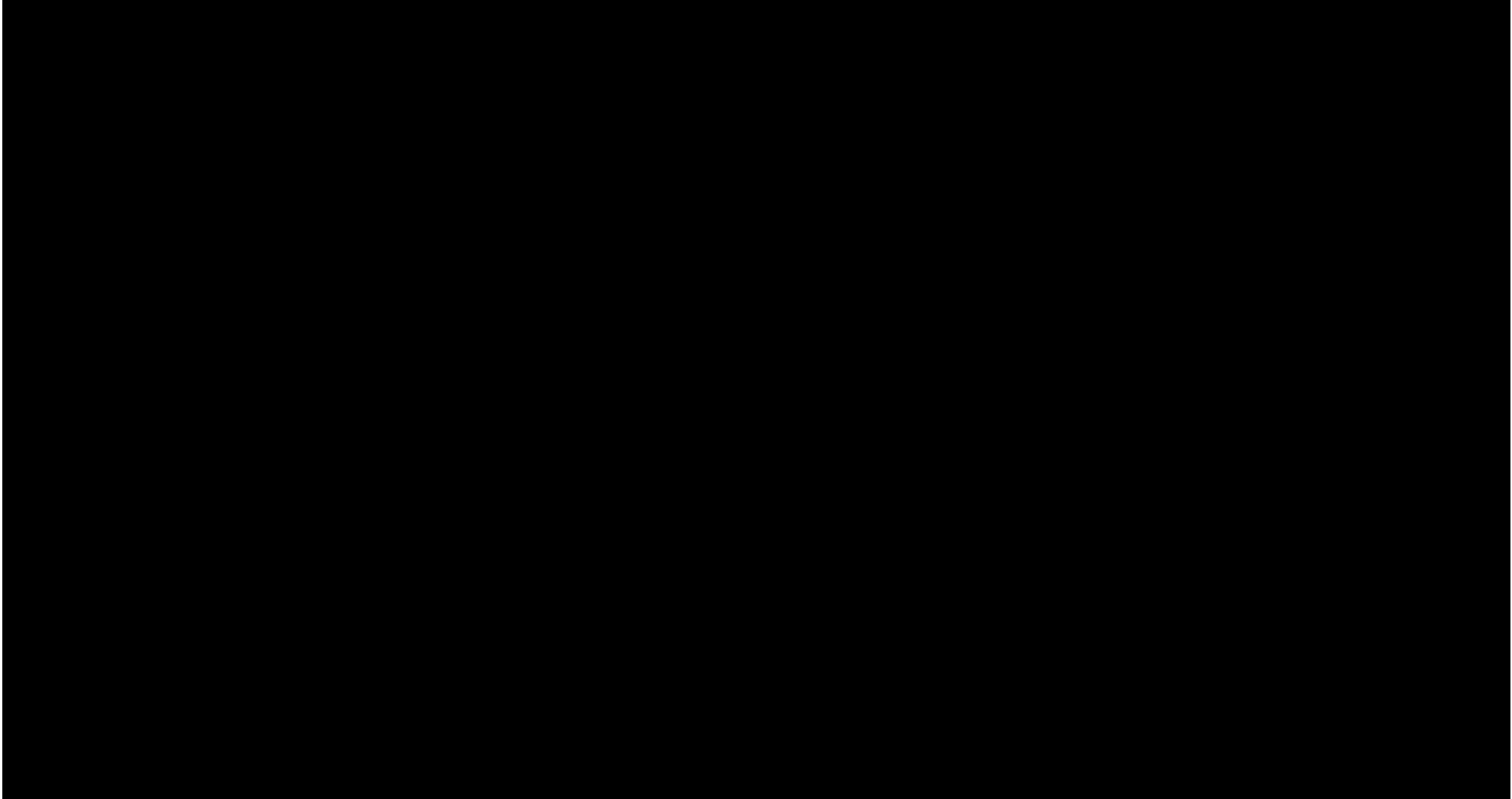


Slack에 알림 전송





프로젝트 수행 결과





프로젝트 수행 결과

기대 효과

사용자의 버그바운티 실제 활동여부를 파악 가능

벤더에 관련 자료 제공 가능

플랫폼 인사이트 가능

The image features two decorative geometric shapes. One is in the top-left corner, and the other is a larger one in the bottom-left corner. Both are composed of a blue-to-green gradient parallelogram and a white parallelogram that creates a 3D effect.

감사합니다.