

실무형 프로젝트 회의

K-Shield 주니어 보안사고 분석대응 7기

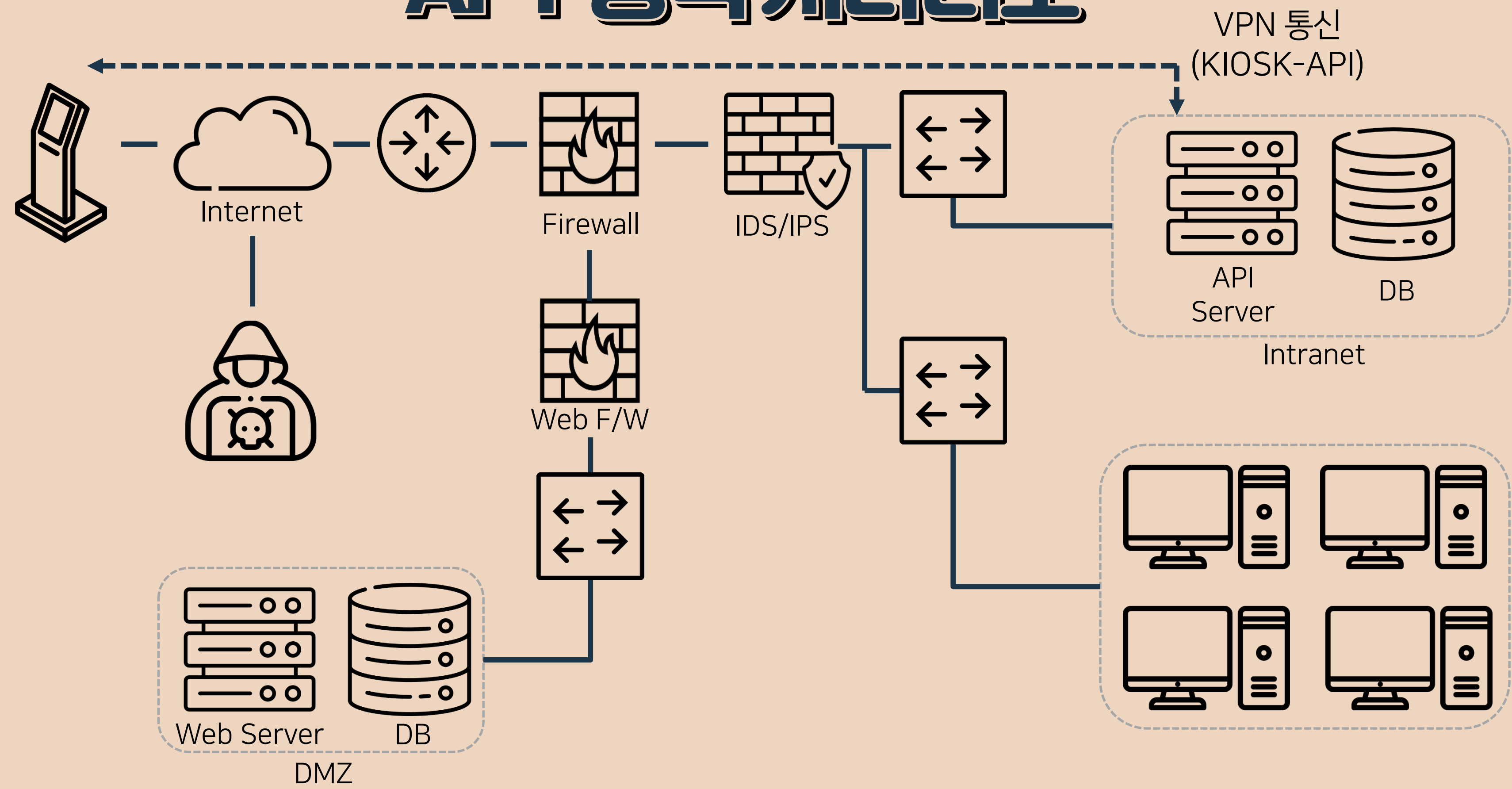
2021. 09. 25
5조 R&B

APT 공격

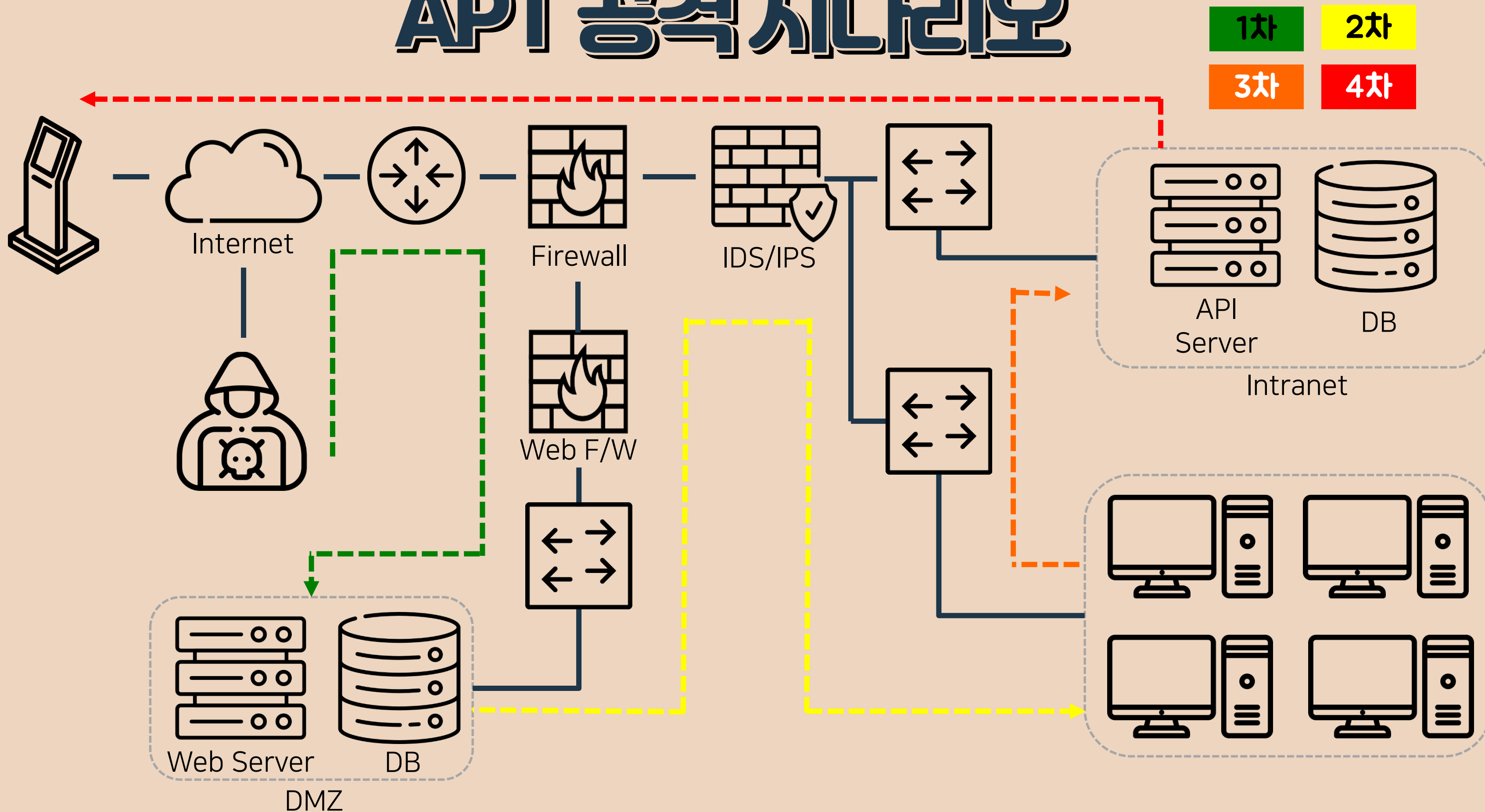
APT 목표

맥도날드 키오스크를 사용하는 이용자(대상)의
신용카드 정보 탈취 후 흔적 삭제

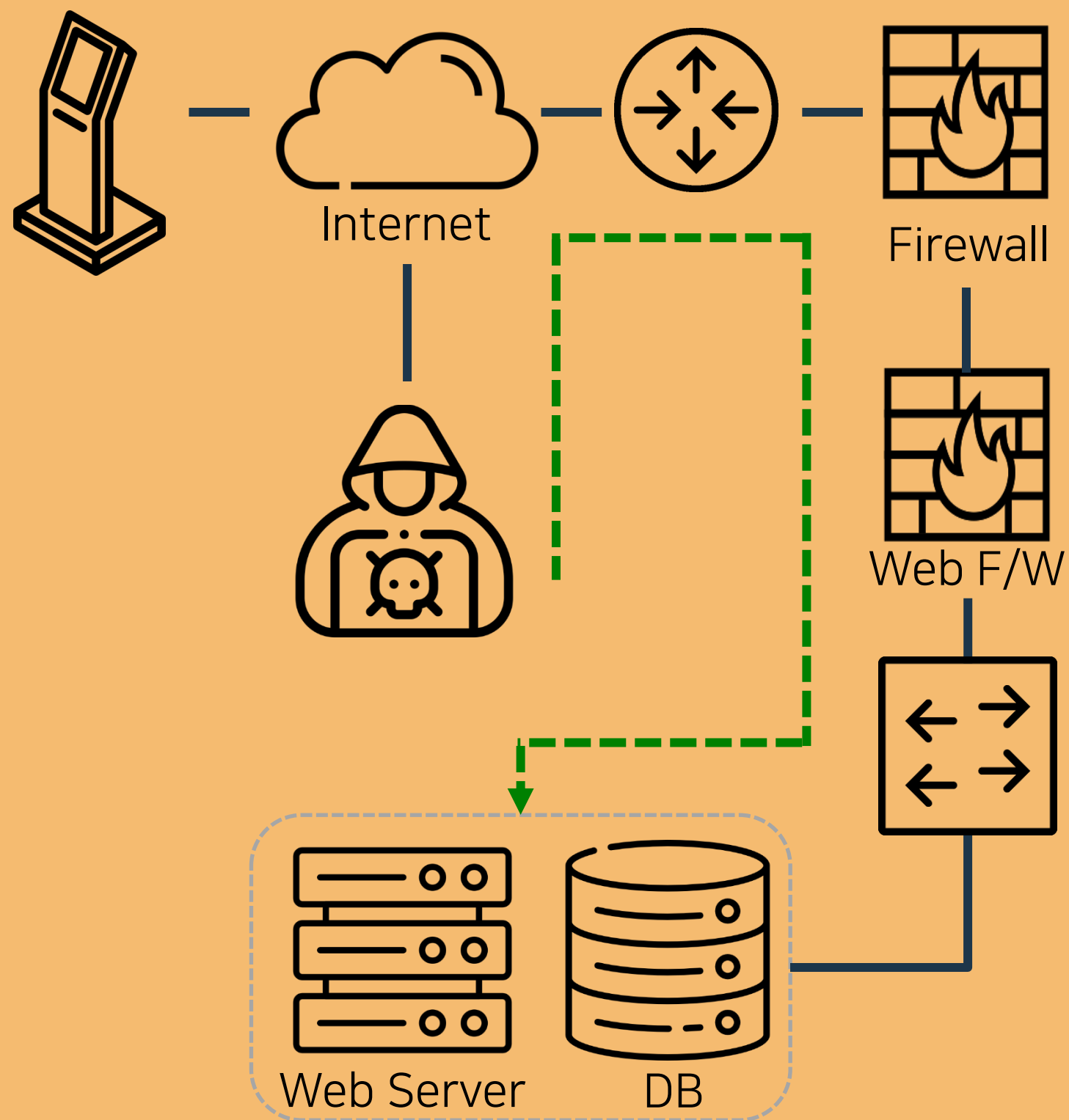
APT 공격 시나리오



APT 공격 시나리오



침투 과정



1차 침투 : HACKER -> DMZ

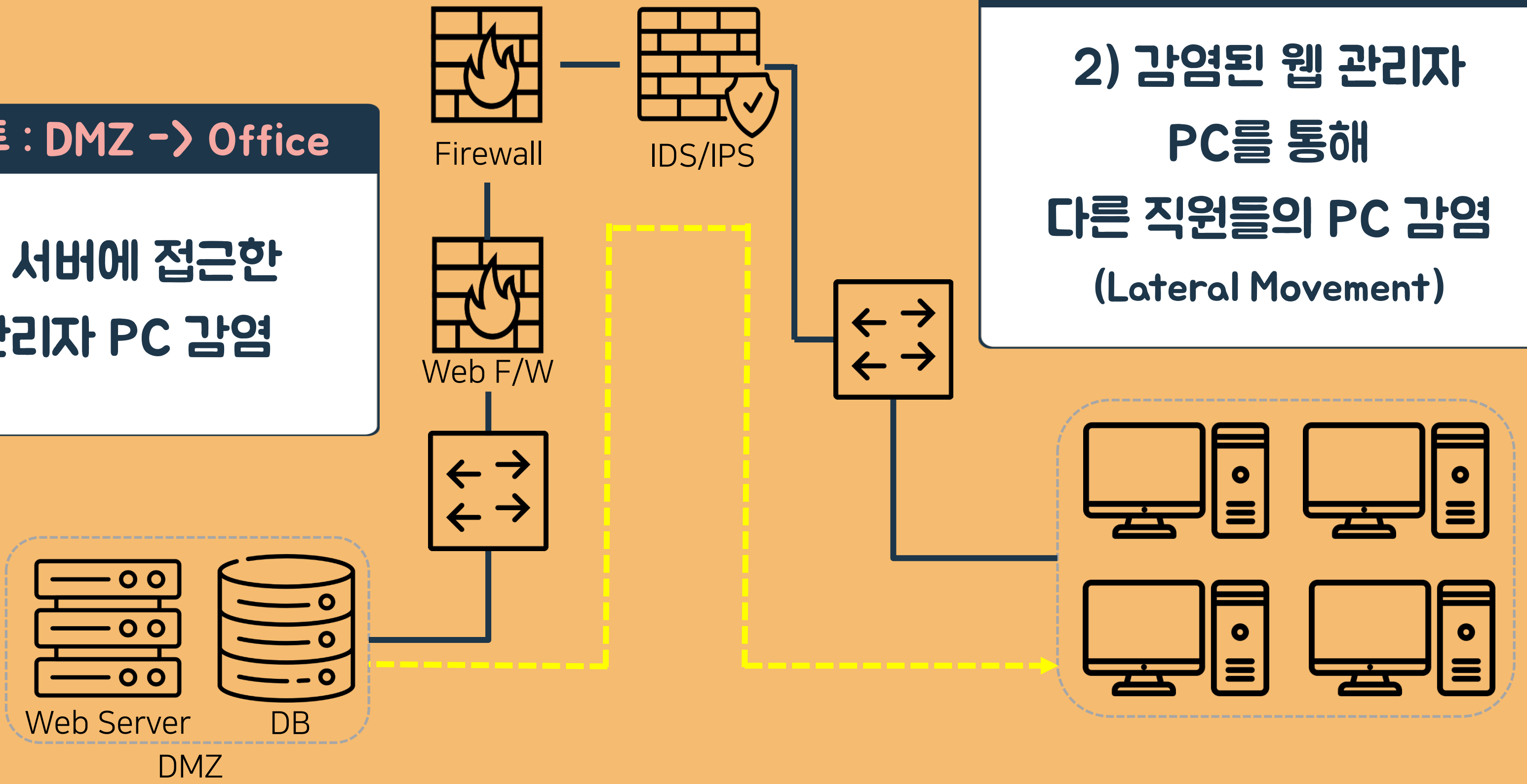
웹 서버 감염

키오스크의 배너 창에 있는
광고에 악성코드를 유포

침투 과정

2차 침투 : DMZ -> Office

1) 웹 서버에 접근한
웹 관리자 PC 감염

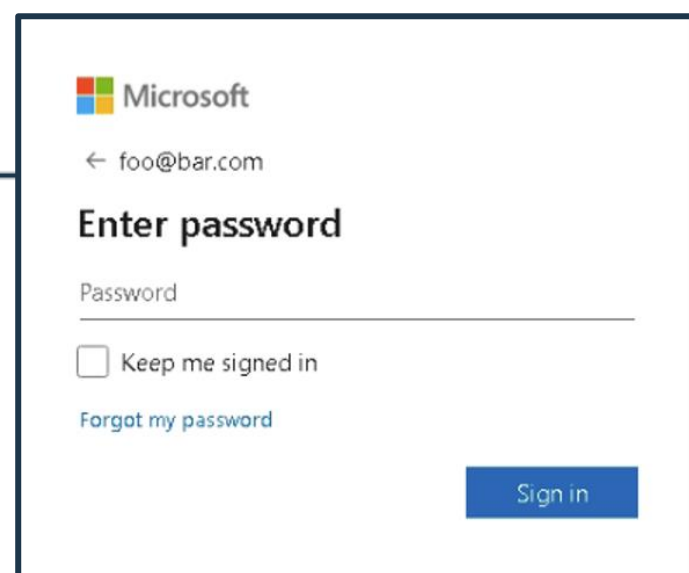


2차 침투 : DMZ -> Office

2) 감염된 웹 관리자
PC를 통해
다른 직원들의 PC 감염
(Lateral Movement)

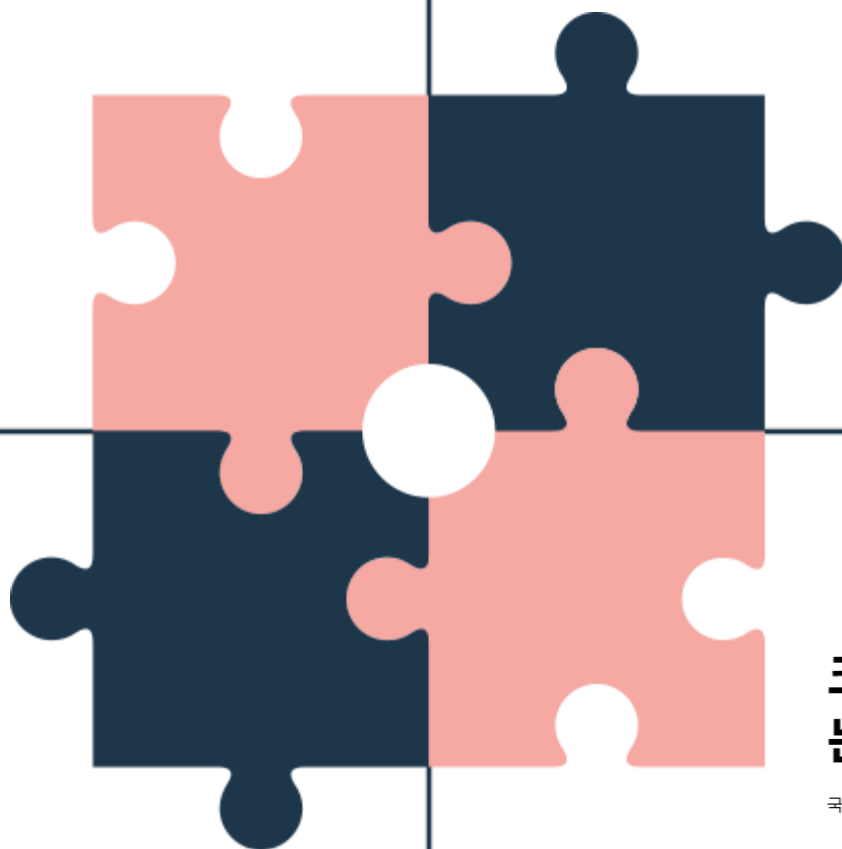
침투 과정

원격지에서 관리자의 크리덴셜 얻기



웹 서버에 접근할 때
로그인 하는 페이지로 위장해서 빼오기

웹 서버에 업데이트 파일인 척
악성코드 파일을 올려놓고 관리자 PC
감염시키기



크롬을 이용해 원격으로 윈도우 패스워드를 훔칠 수 있는 취약점 발견 돼

국내외 보안동향 · by 알약(Alyac) · 2017. 5. 18. 15:45

<https://blog.alzac.co.kr/1102>

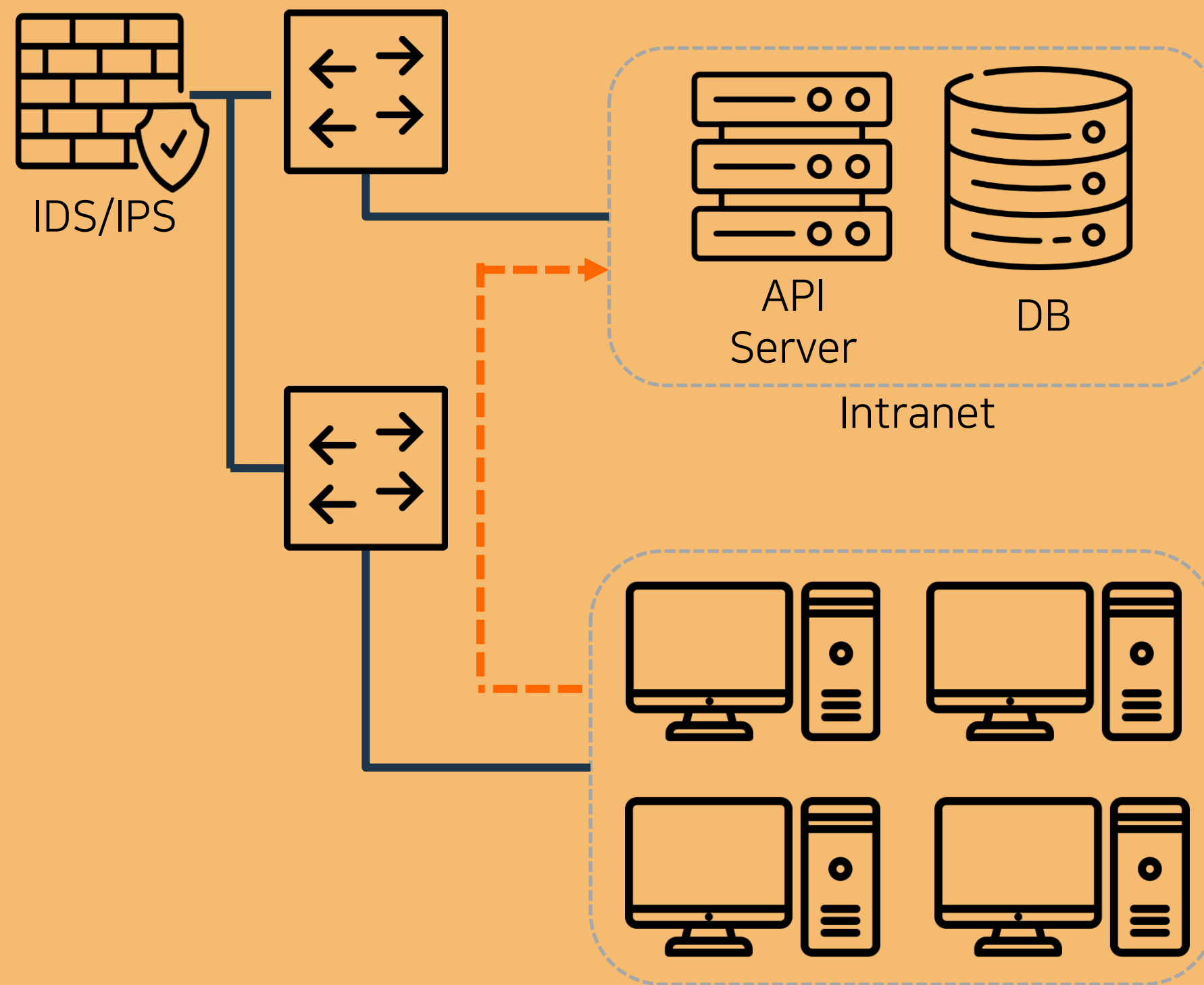
크롬을 이용하여 크리덴셜 훔치기

침투 과정

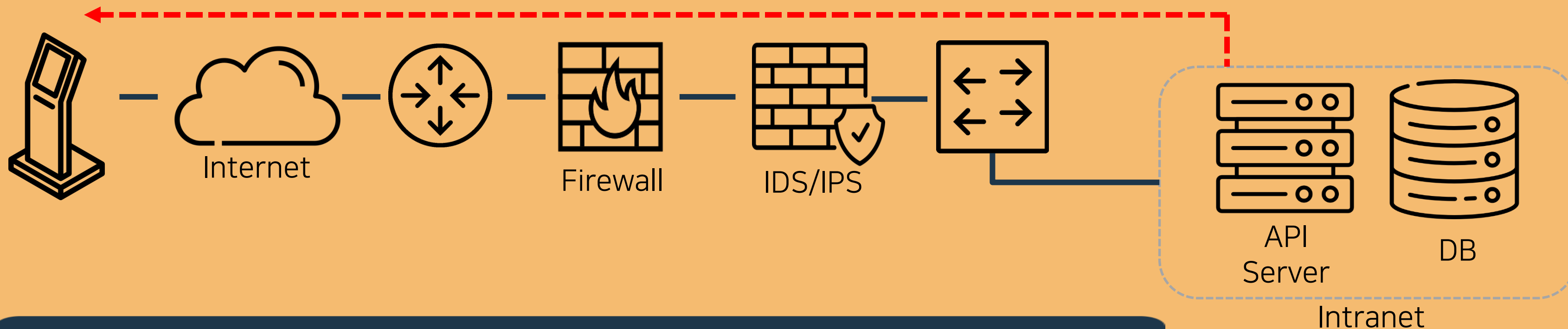
3차 침투 : Office -> INTRA

API 서버 감염

서버 구축을 REST API로 선택
→ REST API의 취약점을 이용



침투 과정

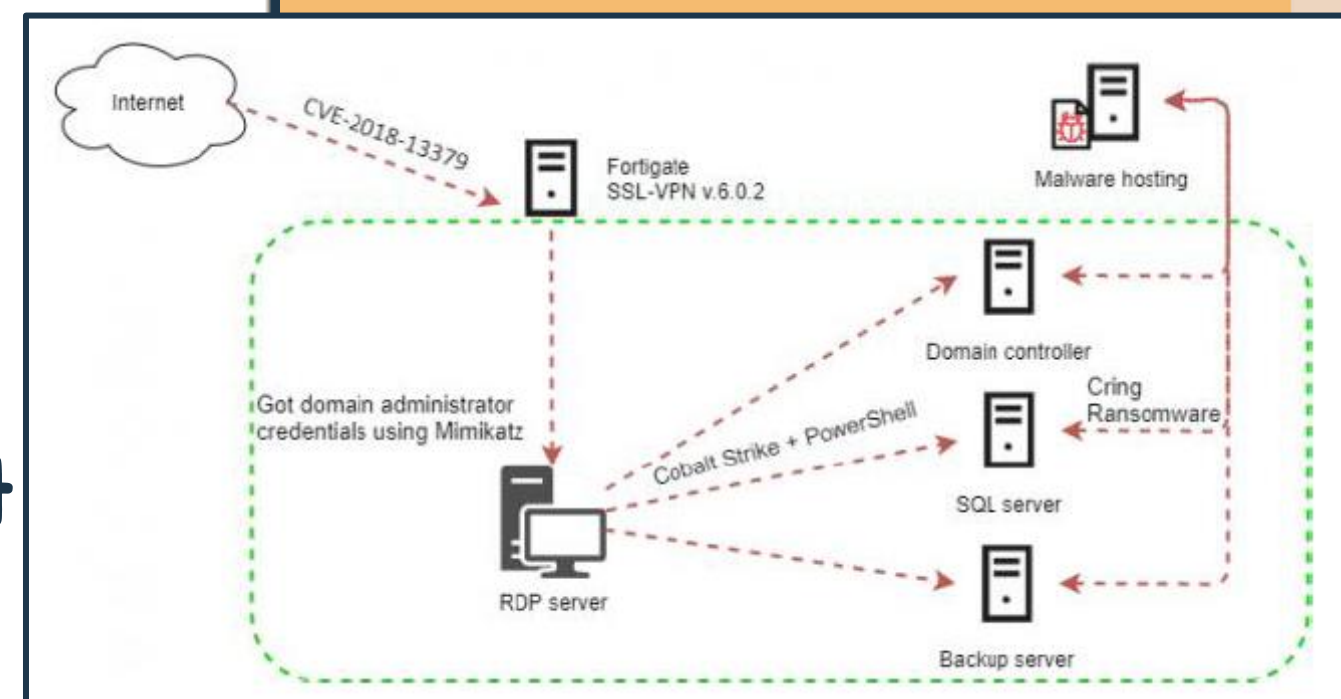


4차 침투 : INTRA -> KIOSK

API 서버와 VPN으로 연결된 키오스크 감염

< CVE-2018-13379 >

SSL VPN 웹 포털에서 제한된 디렉토리("Path Traversal")에 대한 경로 이름의 부적절한 제한을 사용하면 인증되지 않은 공격자가 특수하게 조작된 HTTP 리소스 요청을 통해 다운로드할 수 있음



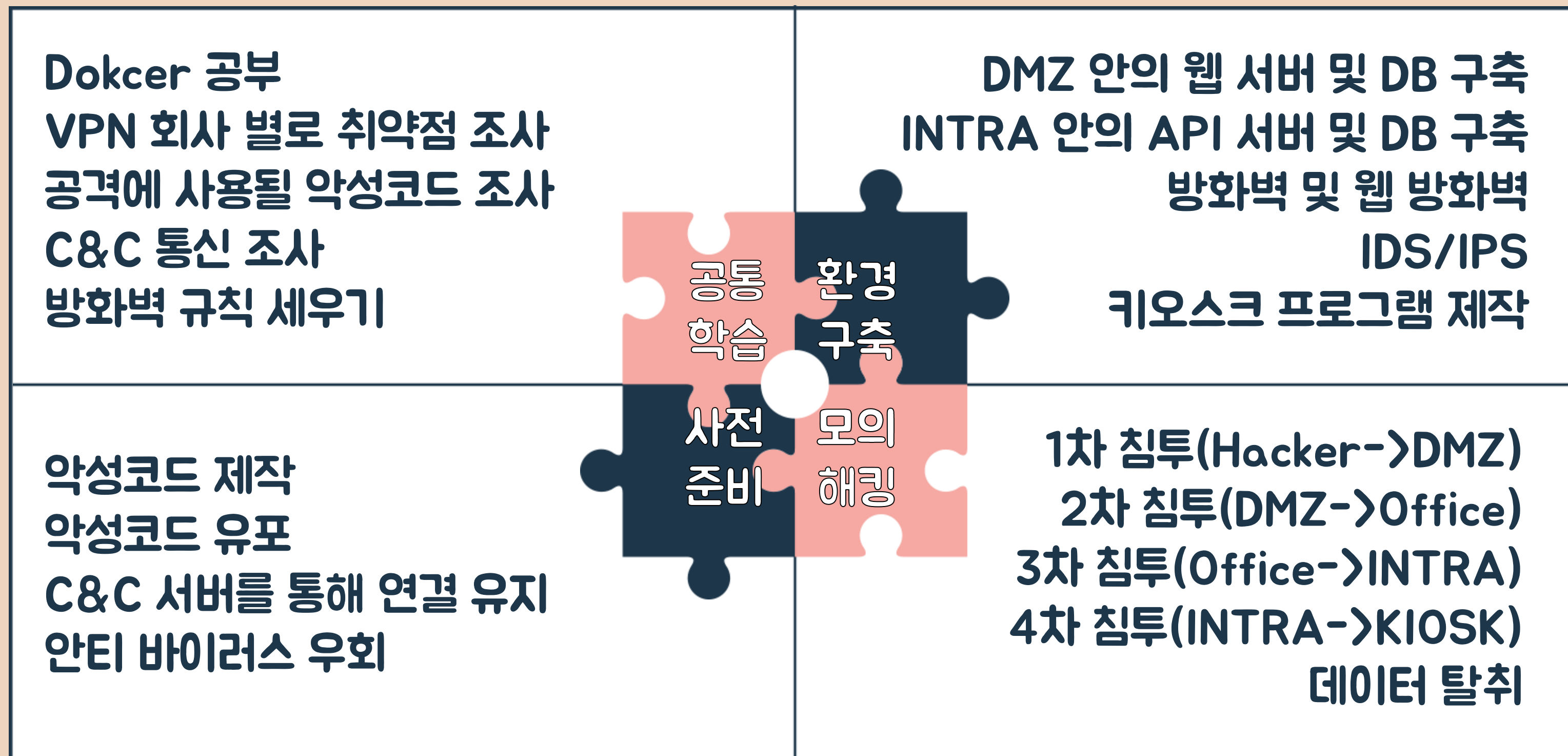
침투 이후

키오스크에서 결제정보 데이터를 획득하여
공격자에게 전달

* 데이터 전달 루트 *

(키오스크 -> API 서버 -> 관리자 PC -> 공격자)

APT WBS



APT WBS

방화벽 룰

1) 내부->외부 : 허용

내부 컴퓨터는 외부 인터넷으로 사용할 수 있게 한다.

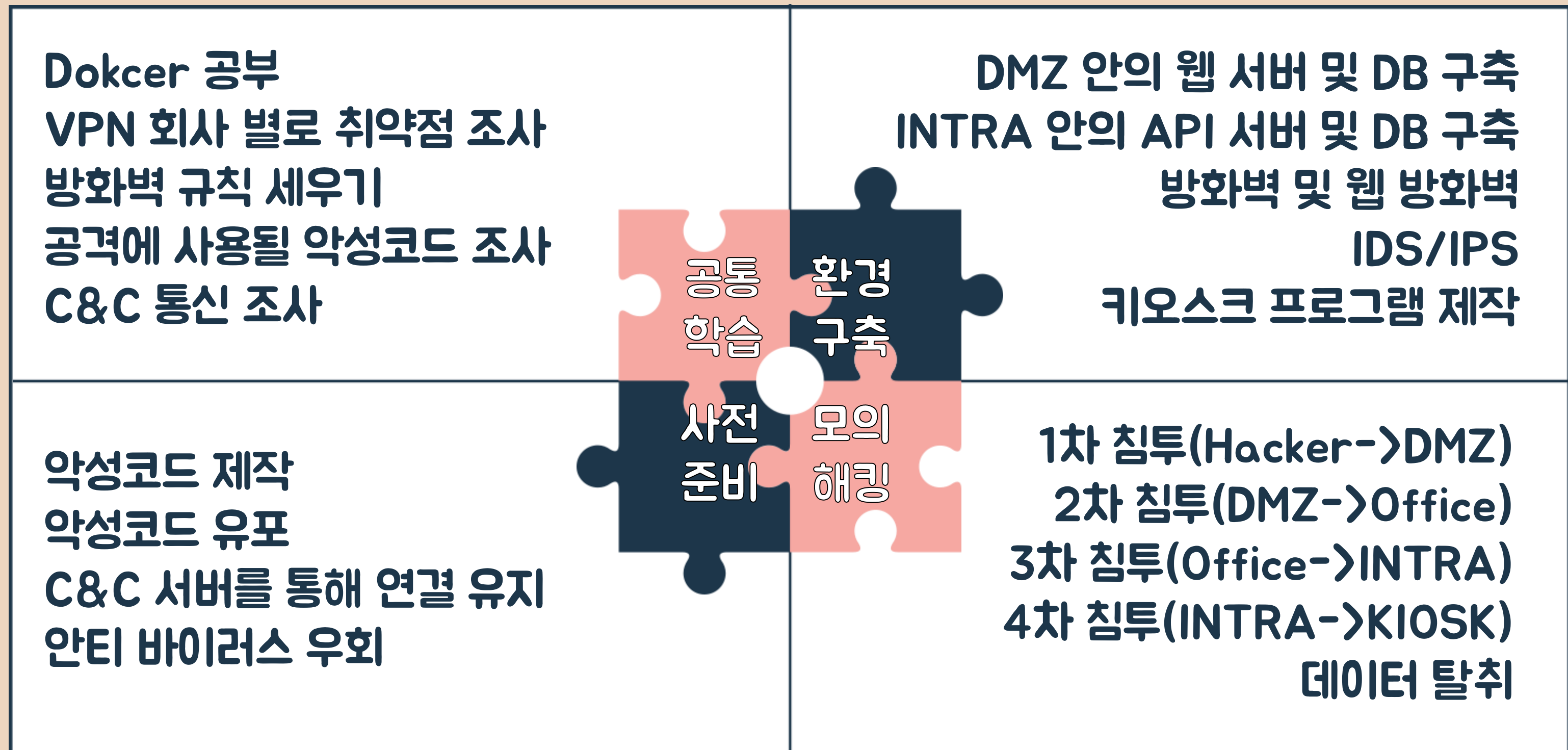
2) 외부->내부 : 차단

외부 컴퓨터는 내부에 접속할 수 없도록 한다.

3) 외부->DMZ, 내부->DMZ : 허용

외부 컴퓨터가 방화벽 서버의 공인 IP로 웹 서비스를 요청할 때는 내부에 있는 웹 서버가 서비스 한다.

APT WBS



EDR 진행 상황

kkggy Update yalarule

1 contributor

89 lines (69 sloc)

Yara

yara

악성코드의
VirusTotal에
단순 Text St
Yara는 멀티
rule 파일 =

dks1013 [21091]

1 contributor

75 lines (66 sloc)

- 파일 리스
- 악성코드가 시
- 웹페이지에 들
- 사용자 웹브러
- 감염 장소는
- 이미 설치되어
- 엑셀이나 워드
- 시그니처 매칭
- 사용자가 실행
- 방어법 : 지능
- 로깅 - 파워셸
- 로컬 그룹정책
-
- Living off t
- LotL 공격 (저
- 희생자가 보유

wespito [210919] fileles

1 contributor

422 lines (292 sloc)

Fileless

1. Code Inject

- Shellcode
- 합법 프로
- DLL inject
- 프로세스

t0paz-2357 Update [210913] ELK.md

1 contributor

33 lines (26 sloc) | 1.63 KB

ELK

ELK (ElasticSearch, Logstash, Kibana) 란?

ElasticSearch - 분석 및 저장 기능을 담당
Logstash - 수집 기능
Kibana - 이를 시각화하는 도구

전체적으로 접근성과 용이성이 좋아 최근 가장 핫한 로그 및 데이터 분석 도구이다.
[공식 사이트](#)

ELK 사용법

- [ELK Introduction](#)
- [ELK Installation](#)
- [ELK 기본사용법](#)

EDR 탐지 구현

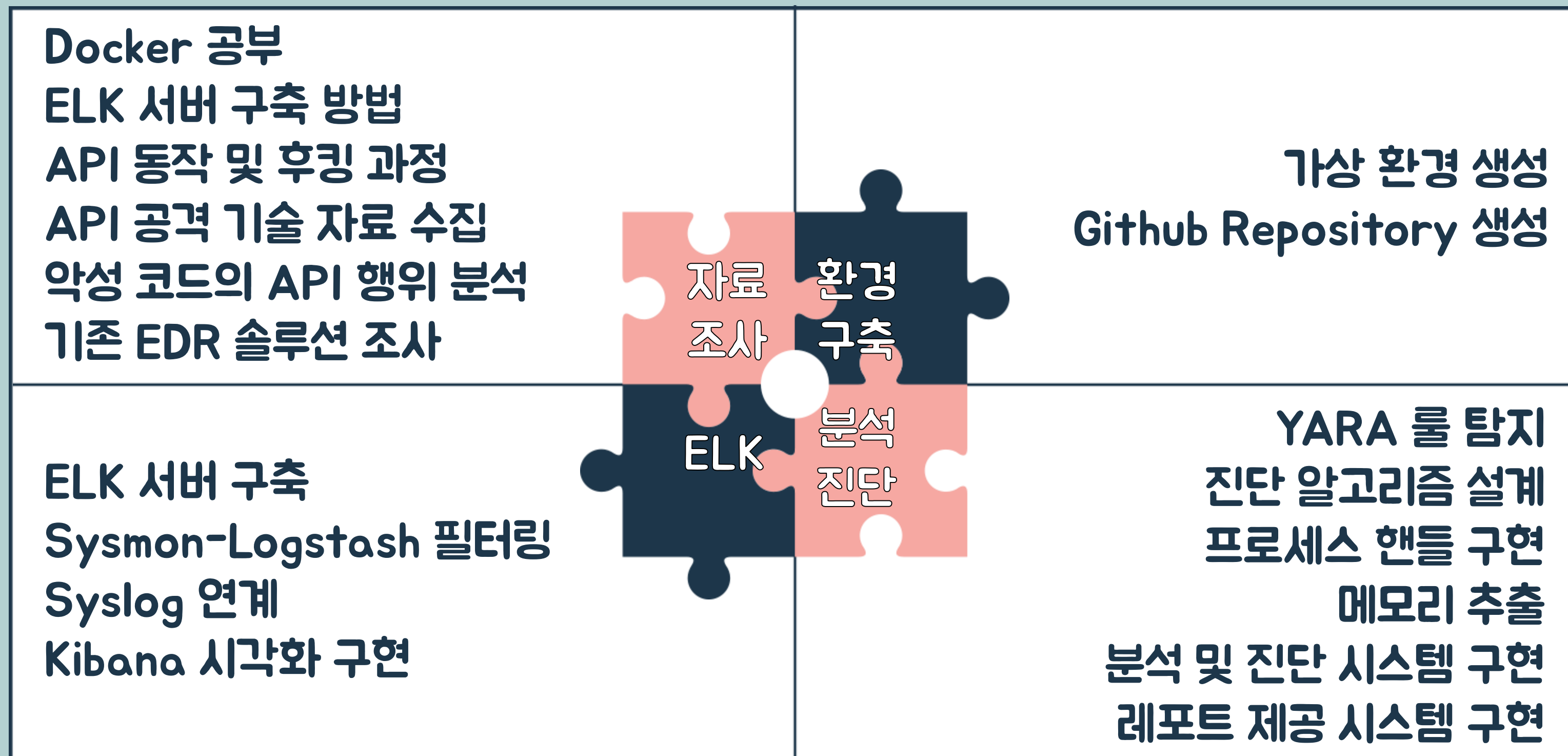
기 초

- 1) Sysmon + ELK 서버 구축 : EDR의 기본 틀 마련
- 2) Syslog 연계(APT 팀의 구축 환경 고려)
: DMZ 존 + 인트라넷망 + 워크존 모두 탐지하기 위해
- 3) Yara rule 작성

심화 - APT 공격에 자주 사용되는 Fileless 공격 탐지 구현

- | | |
|---|---|
| 1) DLL injections,
Reflective DLL injections,
Process hollowing | 2) LotL (Living of the Land)
3) 지속성 공격 |
|---|---|

EDR WBS



감사합니다