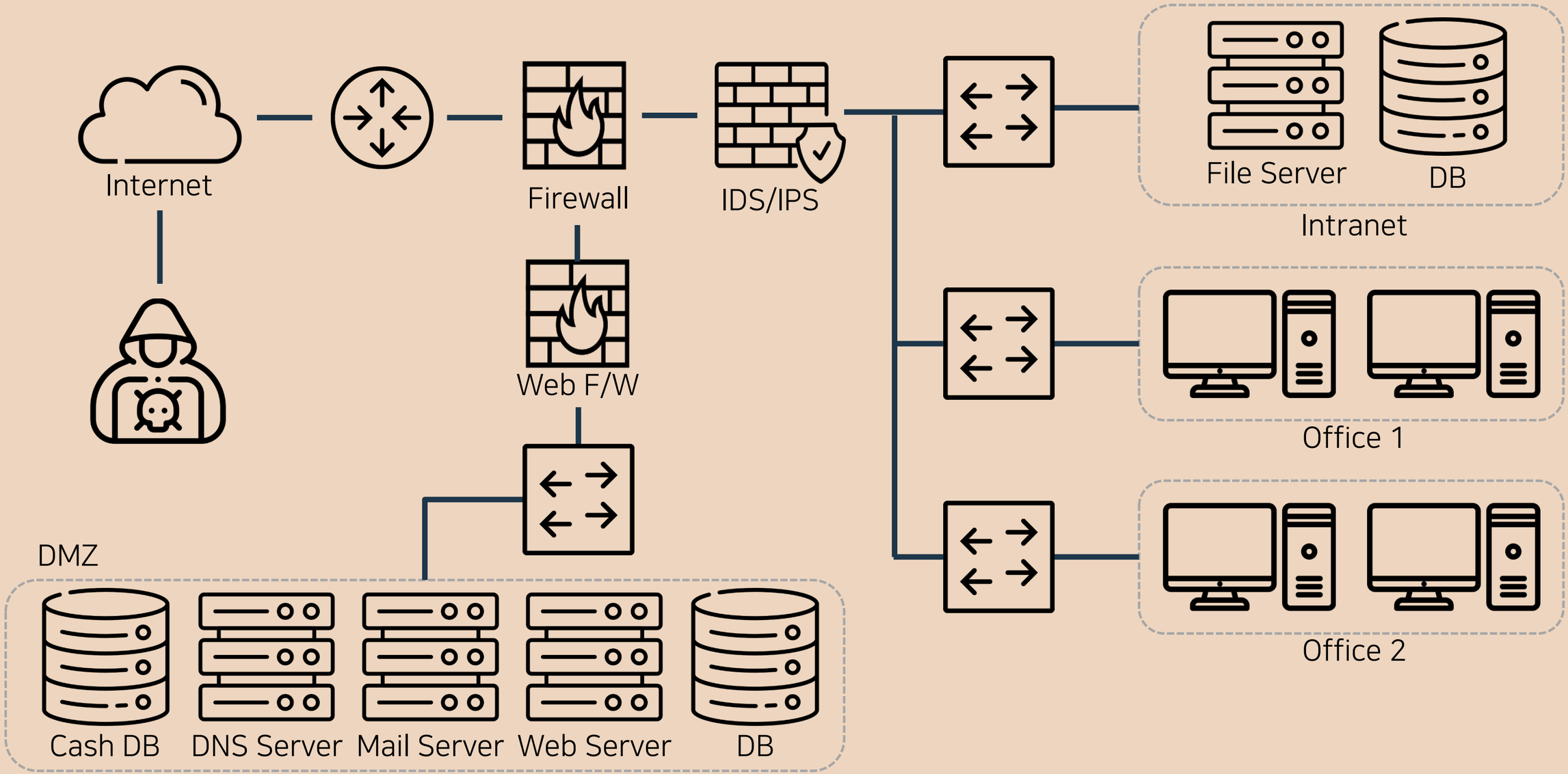
# 실무형 프로젝트 회의

## K-Shield 주니어 보안사고 분석대응 7기

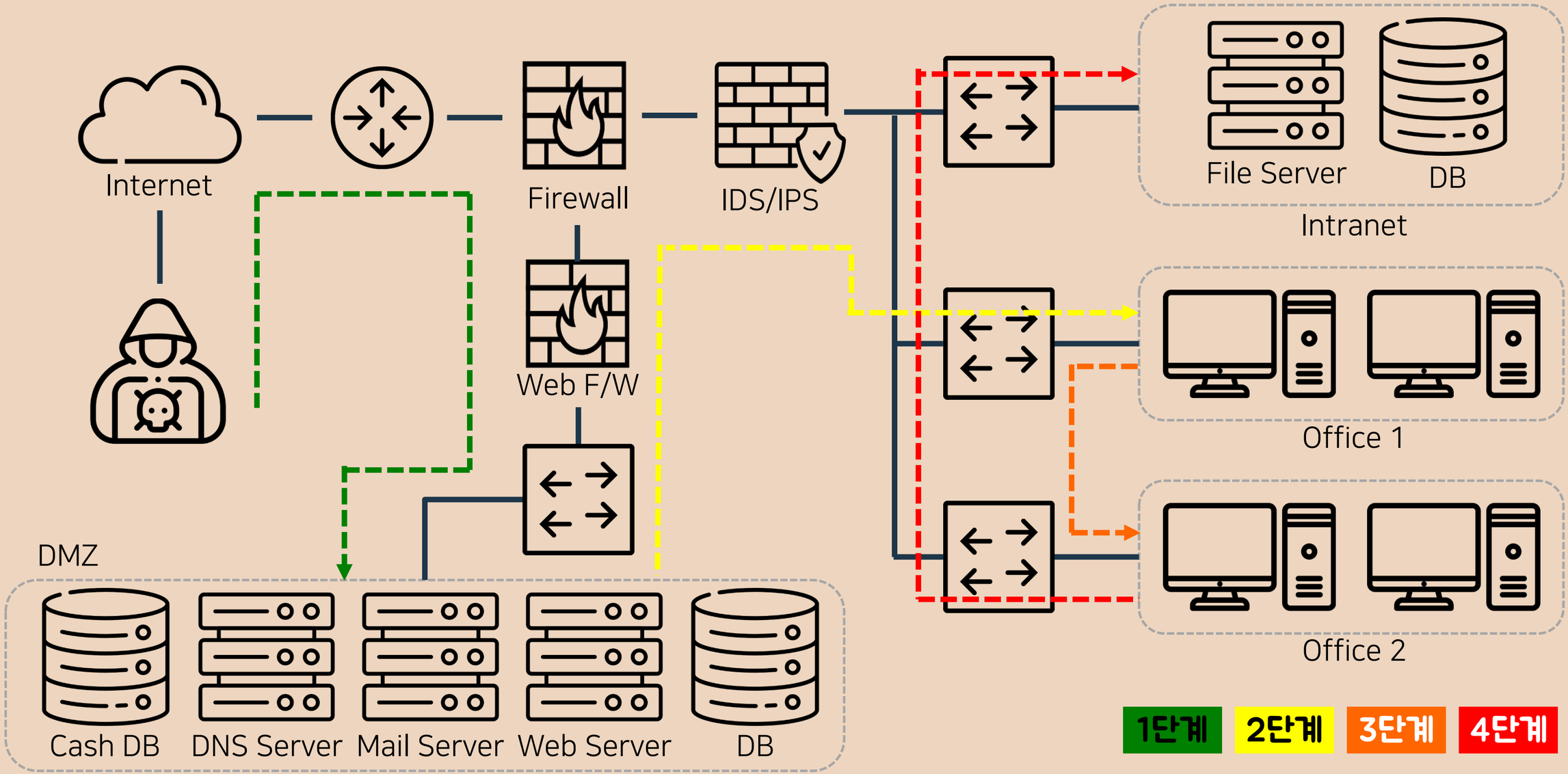
2021. 10. 03

5조 R&B

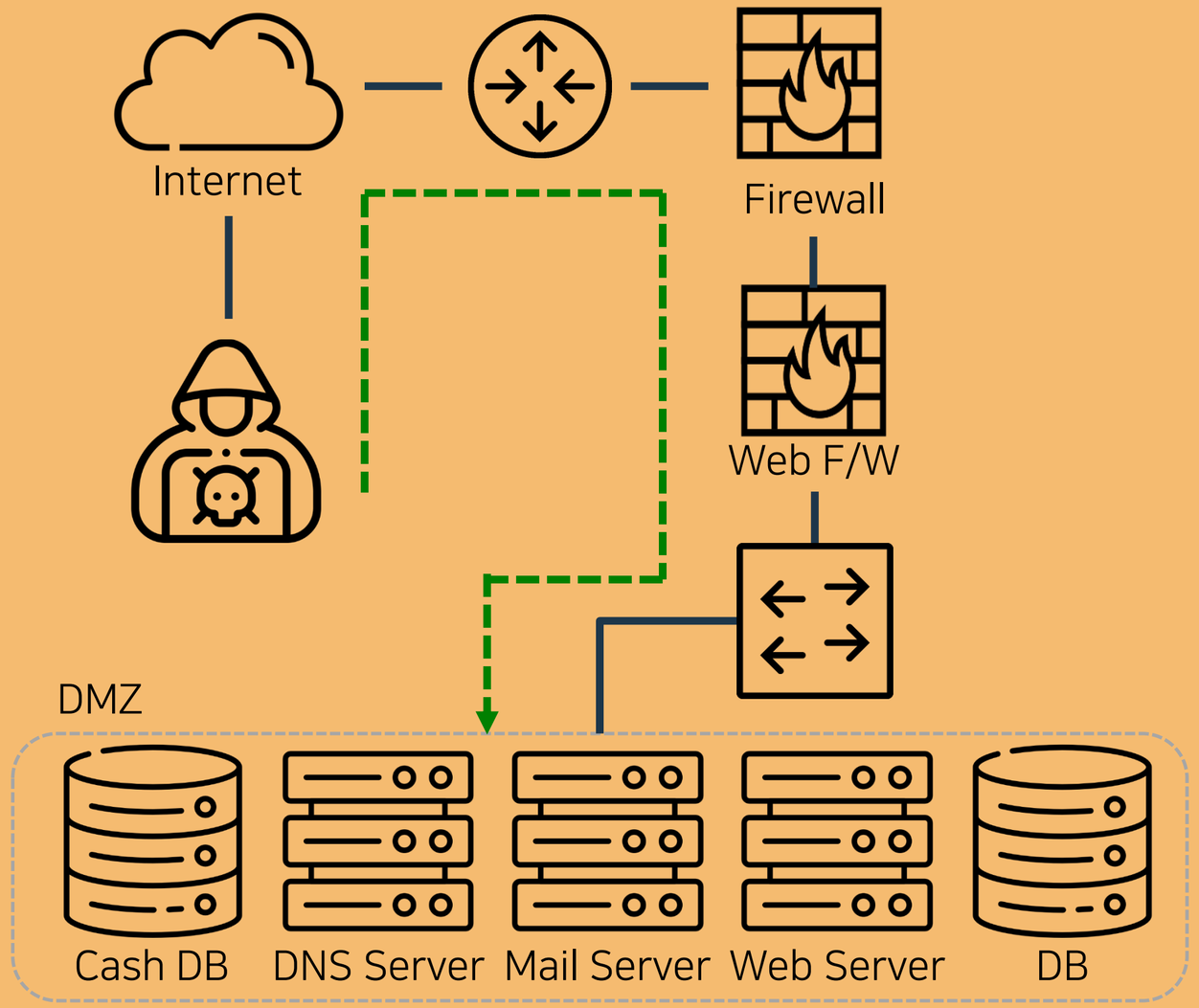
# APT 공격 시나리오


Internet
Firewall
IDS/IPS
File Server
DB
Intranet
Web F/W
Office 1
DMZ
Office 2
Cash DB
DNS Server
Mail Server
Web Server
DB

# APT 공격 시나리오


Internet
Firewall
IDS/IPS
File Server
DB
Intranet
Web F/W
Office 1
Office 2
DMZ
Cash DB
DNS Server
Mail Server
Web Server
DB
1단계
2단계
3단계
4단계

# 침투 과정




## 1단계

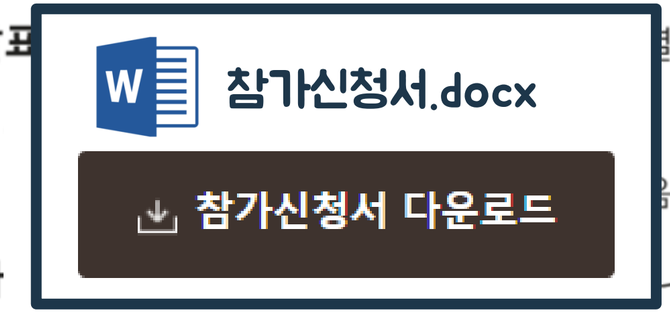
### 참가신청서 작성 후 접수

**공모일정**

결과발표 ... 별통보)

시 상

참가자 ... 나




**접수방법** e-mail (csteam@hanwha.com) 접수

**제출서류** 1. 참가신청서 (한화손해보험 홈페이지에서 다운로드)
2. 제출보고서 (자율양식)

# 침투 과정

디지털 취약계층 서비스 아이디어 공모전

참 가 신 청 서

| | | | |
|---|---|---|---|
| 응모 내용 요약 | 아이디어 내용 (간략히) | | |

※ 제출보고서(자율양식)를 간략히 요약하여 작성

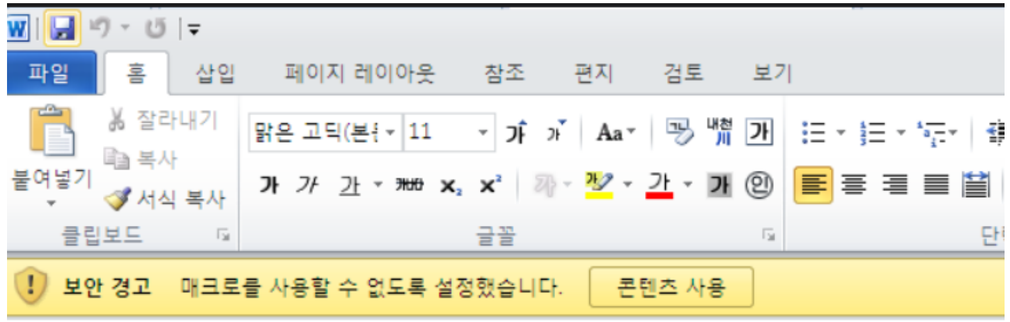
**〈 CVE-2018-0802 〉**

**Microsoft Office 메모리 손상 취약점**

**메모리에서 개체가 처리되는 방식으로 인해 원격 코드 실행 취약점**

## 워드 문서 공격 방법

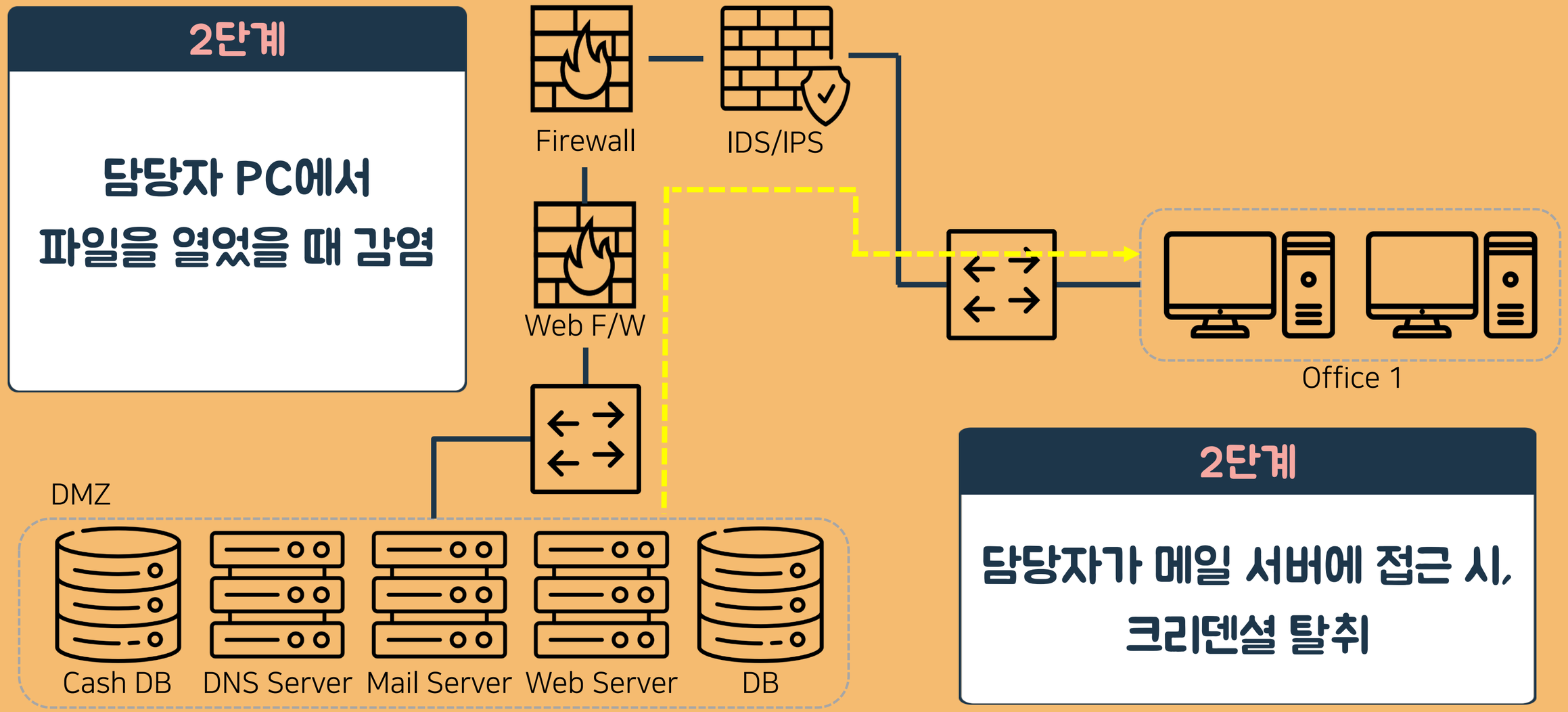
**MS Office 편집기 프로세스에서의 취약점을 이용**



# 침투 과정

## 2단계

담당자 PC에서
파일을 열었을 때 감염




## 2단계

담당자가 메일 서버에 접근 시,
크리덴셜 탈취

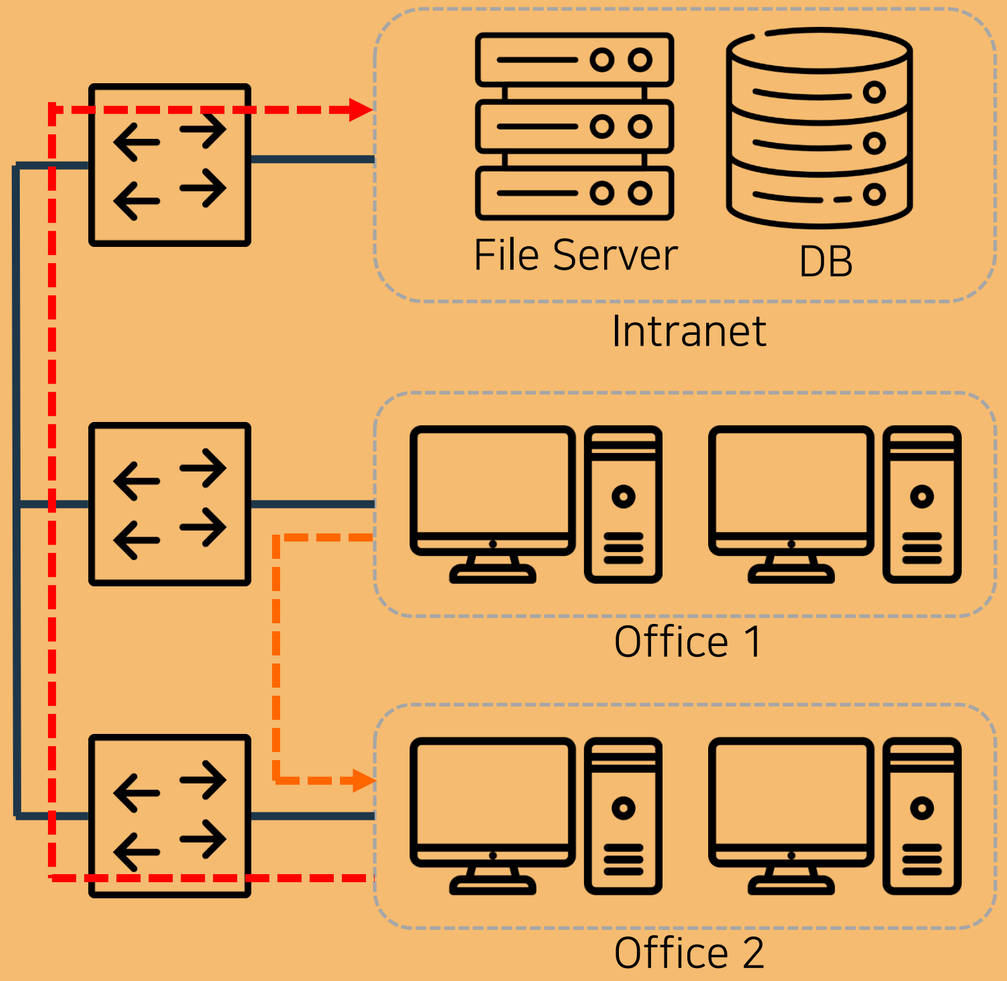
# 침투 과정

## 3단계

탈취한 메일 계정으로
다른 부서의 사원에게 메일 전송

## 4단계

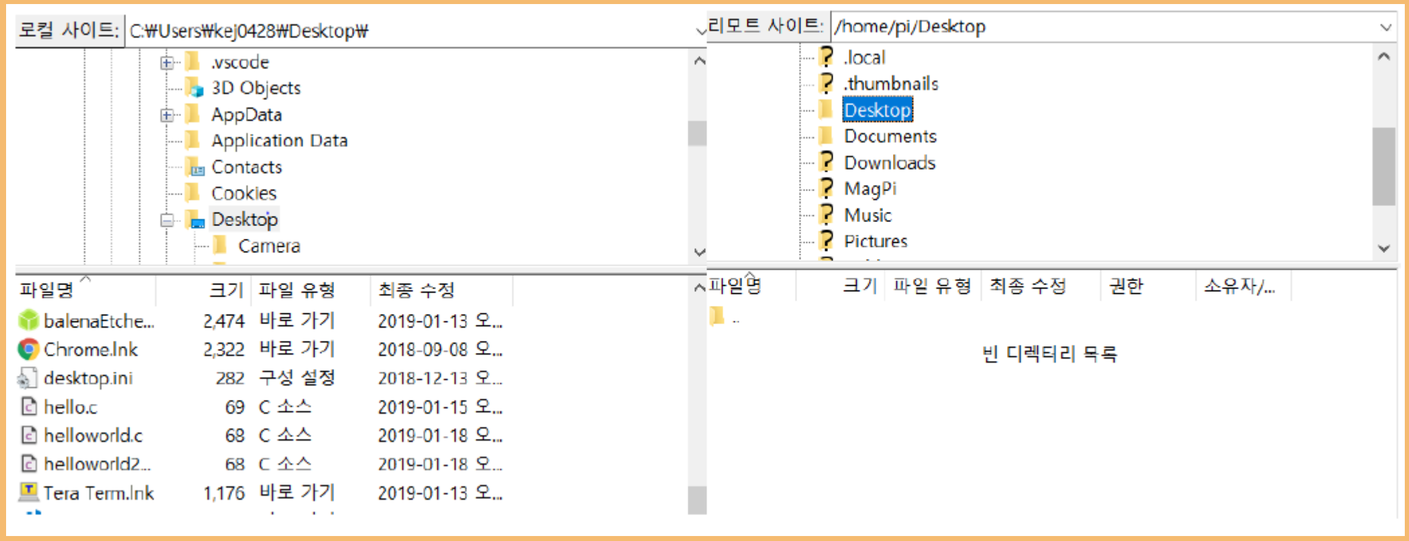
Office 2의 파일 서버 계정으로
침투 후 중요 파일 접근



# 침투 과정

파일 서버 구성

-> 다른 부서로 접근 불가

# 악성코드 기능

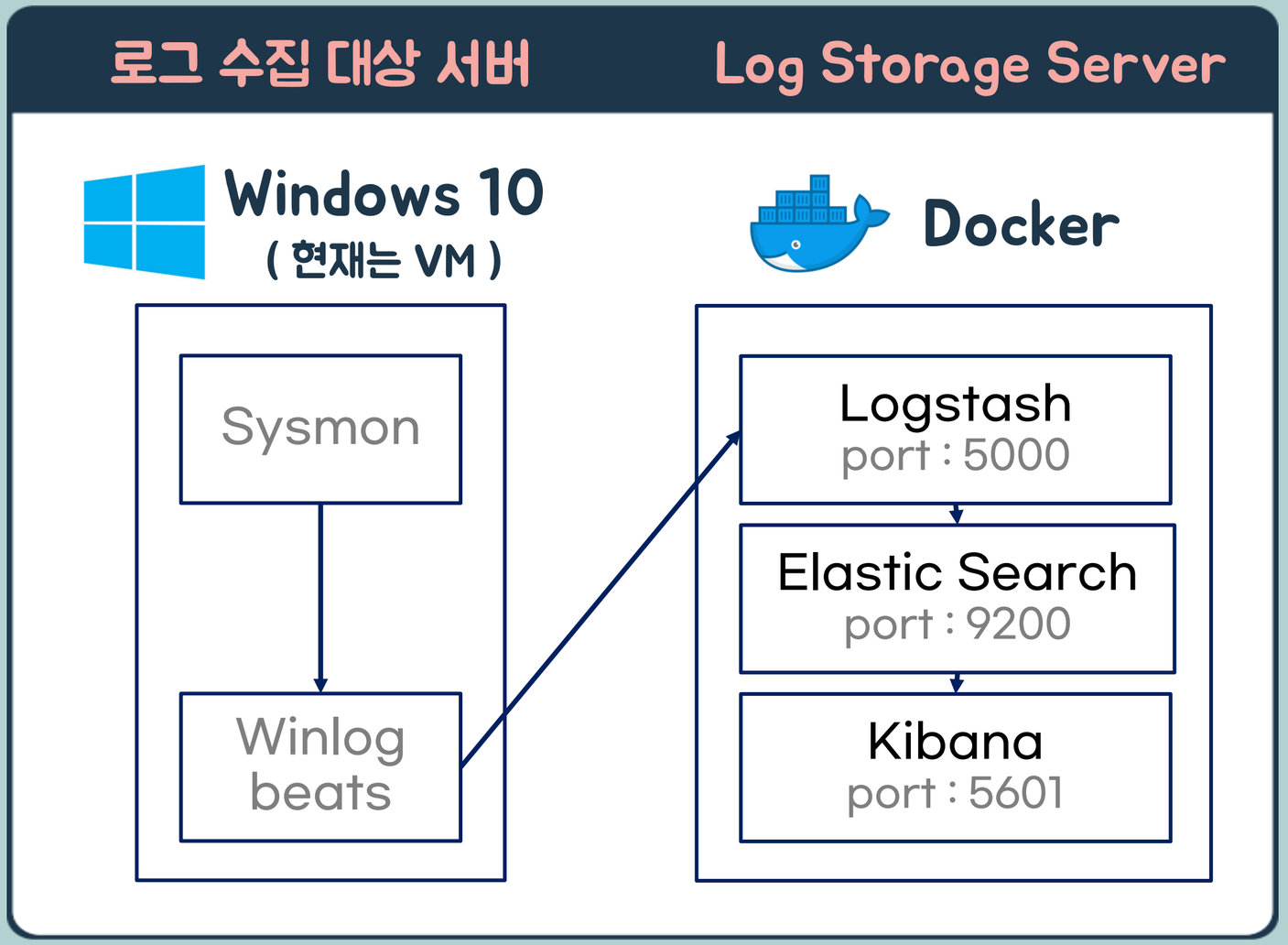
## 기능

- C&C 연결
- 키 캡처, 스크린 캡처
- 파일 업로드 & 다운로드
- UAC 우회
- 레지스터 등록

## 추가해야할 기능

- 윈도우 디펜더 우회
- 문서형 악성코드

# EDR 팀 환경 구성


로그 수집 대상 서버
Log Storage Server
Windows 10
( 현재는 VM )
Docker
Sysmon
Winlog beats
Logstash
port : 5000
Elastic Search
port : 9200
Kibana
port : 5601

# EDR 팀 환경 구성

## 1. Sysmon, Winlogbeats 설치 -> Logstash로 전송

Mitre ATT&CK 프레임워크 매핑 필터 적용

=> 진행 완료

## 2. Syslog (Linux)에서 Logstash로 전송 (연계)

진행 중

Git에 업로드된 자료조사 파일

sysmon - logstash #1

Open dks1013 opened this issue 2 days ago · 0 comments

dks1013 commented 2 days ago • edited

sysmon - logstash 진행+방법정리

https://github.com/choisungwook/malware/tree/master/01%20blue%20team/sysmon/01%20elk%EC%84%A4%EC%B9%98%2B%EC%97%B0%EB%8F%99

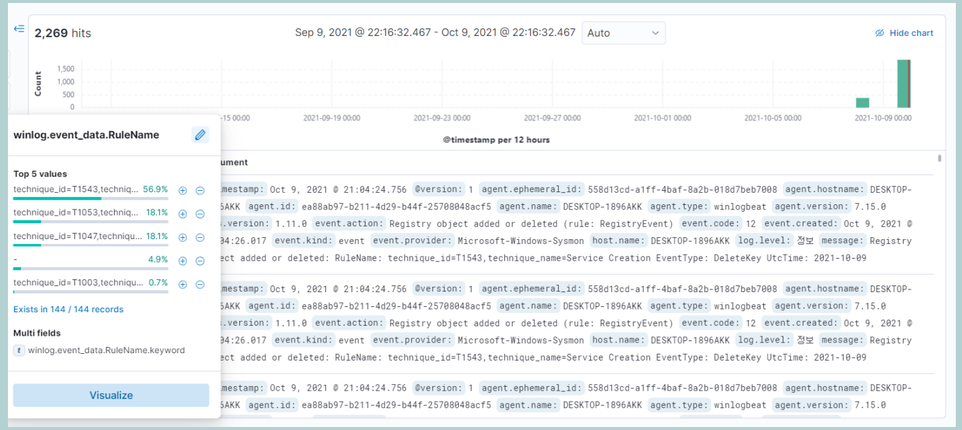
https://www.youtube.com/watch?v=4x054MeYS14

- 이용

설정변경

docker-elk/elasticsearch/config/elasticsearch.yml

```
cluster.name: "docker-cluster"
network.host: 0.0.0.0
discovery.type: single-node
```



# EDR 팀 환경 구성

## 3. Kibana 로그 대시보드, 그래프 생성 방법 조사

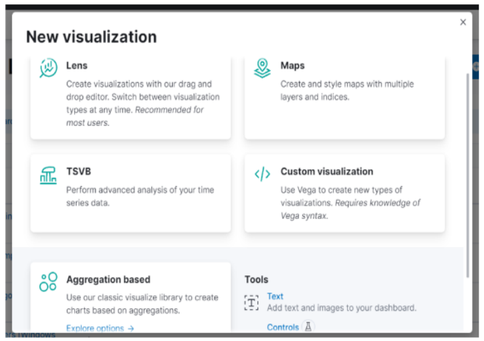
Lens, Maps, Aggregation based등의
방법으로 시각화 자료 만드는 방법 정리
=> 진행 완료

## 3. Kibana 로그 대시보드, 그래프 생성 방법 조사

log&악성 행위 수집을 위해 필요한
Dashboard 구성 요소 조사
=> 진행 중

**Git에 업로드된 자료조사 파일**

2. Visualize Library : 시각화 자




- **Lens** :
  드래그 인 드롭 에디터를 이용해 시각화를 만든다.
  언제든지 Visualizaition들의 타입을 전환할 수 있음
- **Maps** :
  여러 레이어와 인덱스들을 통해 맵 생성 가능
- **TSVB** :
  데이터를 시계열로 시각화 할 수 있음
- **Custom** :
  Vega를 사용해 새 유형의 Visualizations를 만들 수 있음. Vega 문법을 사용할 줄 알아야 함
- **Aggregation based** :
  기존 시각화 라이브러리를 사용해 집계 기반으로 차트 생성 가능

1. Discover : 데이터 탐색

- Discover로 들어가 데이터를 가져오고 생성된 인덱스 패턴을 확인

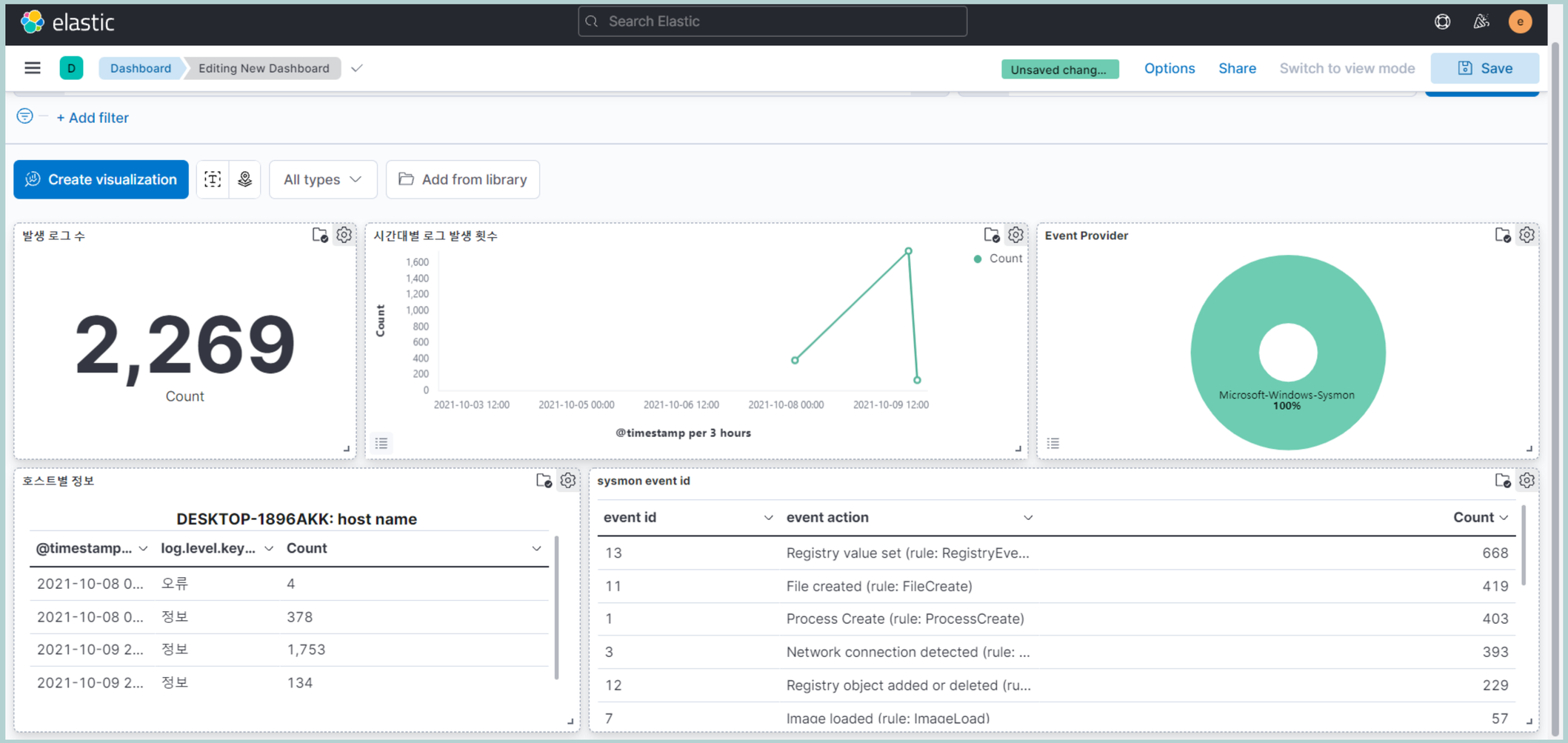
- 검색할 쿼리, 날짜 조건 입력 하여 데이터 탐색 가능
- Elastic Search 쿼리 문법 가이드
  - https://www.elastic.co/guide/en/elasticsearch/reference/7.15/query-dsl-query-string-query.html#query-string-syntax

3. Dashboard : 대시보드 생성 (예시)

[샘플 데이터의 대시보드]

- Visualize된 자료를 원하는 위치로 끌어 직접 보기 편한 위치로 배치 가능
- 시각화된 여러 유형의 데이터들을 원하는 위치에 놓아 한눈에 볼 수 있음

# EDR 팀 환경 구성


elastic
Search Elastic
Dashboard
Editing New Dashboard
Unsaved chang...
Options
Share
Switch to view mode
Save
+ Add filter
Create visualization
All types
Add from library
발생 로그 수
2,269
Count
시간대별 로그 발생 횟수
Count
1,600
1,400
1,200
1,000
800
600
400
200
0
2021-10-03 12:00
2021-10-05 00:00
2021-10-06 12:00
2021-10-08 00:00
2021-10-09 12:00
@timestamp per 3 hours
Event Provider
Microsoft-Windows-Sysmon
100%
호스트별 정보
DESKTOP-1896AKK: host name
@timestamp...
log.level.key...
Count
2021-10-08 0... 오류 4
2021-10-08 0... 정보 378
2021-10-09 2... 정보 1,753
2021-10-09 2... 정보 134
sysmon event id
event id
event action
Count
13 Registry value set (rule: RegistryEve... 668
11 File created (rule: FileCreate) 419
1 Process Create (rule: ProcessCreate) 403
3 Network connection detected (rule: ... 393
12 Registry object added or deleted (ru... 229
7 Image loaded (rule: ImageLoad) 57

# 감사합니다