테스트 해본 코드

1. 사용자가 Microsoft Word 문서를 복사하는 경우 (차단)

```
<and>
  <equal>
    <evtSrcFileExt />
    <string value="docx" />
  </equal>
  <in>
    <evtOperationType />
    <list>
      <constOpFileCopy />
    </list>
  </in>
</and>
```

복사를 하고 붙여 넣기를 했을 때 파일 생성이 되지 않아 정상 동작임을 확인

2. 이동식 드라이브에 파일 또는 폴더 쓰기 (차단)

```
<and>
  <equal>
    <evtDestDriveType />
    <constDriveRemovable />
  </equal>
  <in>
    <evtOperationType />
    <constOpFileWrite />
  </in>
</and>
```

이동식 디스크에서 파일 쓰기 차단이 되는 것을 확인을 하였으나 , 폴더 생성까지 막아버림

3. 이동식 드라이브에 파일 또는 폴더 복사 (차단)

```
<and>
  <equal>
    <evtDestDriveType />
    <constDriveRemovable />
  </equal>
  <in>
    <evtOperationType />
    <constOpFileCopy />
  </in>
</and>
```

이동식 디스크에서 파일 복사는 안되는 것을 확인했으나 폴더는 복사가 잘 됨

4. 이동식 드라이브에 파일 이름변경(차단)

```
<and>
  <equal>
    <evtDestDriveType />
    <constDriveRemovable />
  </equal>
  <equal>
    <evtOperationType />
    <constOpFileRename />
  </equal>
</and>
```

이동식 디스크에서 파일,폴더 이름 변경이 안되는 것을 확인

5. 이동식 드라이브에 파일 삭제 (차단)

```
<and>
  <or>
    <equal>
      <evtDestDriveType />
      <constDriveRemovable />
    </equal>
    <equal>
      <evtSrcDriveType />
      <constDriveRemovable />
    </equal>
  </or>
  <in>
    <evtOperationType />
    <constOpFileDelete />
  </in>
</and>
```

이동식 디스크에서 파일 삭제할 경우 안됨 하지만 폴더는 정상적으로 동작을 안함 삭제가 잘 됨.

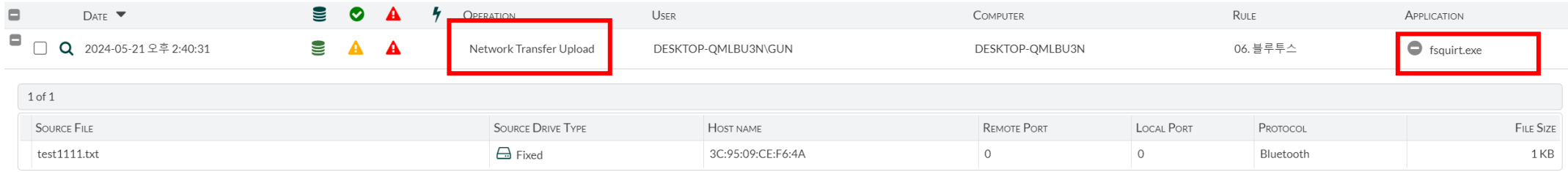
6. 프로그램 실행(차단)

```
<and>
  <equal>
    <curProcessImageName />
    <string value="Notion.exe" />
  </equal>
  <equal>
    <evtOperationType />
    <constOpAppStart />
  </equal>
</and>
```

노션 프로그램 실행이 안되는 것 확인 완료

7. 블루투스를 이용한 파일 전송(차단)

```
<and>
  <equal>
    <evtProtocolType />
    <constProtocolBluetooth />
  </equal>
  <like expr="%fsquirt.exe%">          //블루투스 프로세스
    <curProcessImageName />
  </like>
  <in>
    <evtOperationType />
    <list>
      <constOpNetTransferUpload />
    </list>
  </in>
</and>
```



Date	Operation	User	Computer	Rule	Application
2024-05-21 오후 2:40:31	Network Transfer Upload	DESKTOP-QMLBU3N\GUN	DESKTOP-QMLBU3N	06. 블루투스	fsquirt.exe

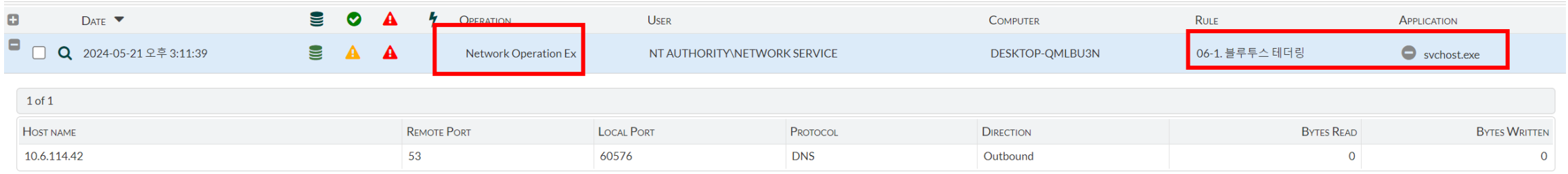
1 of 1

Source File	Source Drive Type	Host name	Remote Port	Local Port	Protocol	File Size
test1111.txt	Fixed	3C:95:09:CE:F6:4A	0	0	Bluetooth	1 KB

노트북으로 블루투스를 통한 파일 전송 차단 됨을 확인.

9. 블루투스를 이용한 테더링 (차단)

```
<and>
   <like expr="%Bluetooth Device%">
    <evtAdapterName />
  </like>
  <in>
    <evtOperationType />
    <list>
      <constOpNetwork />
      <constOpNetworkEx />
    </list>
  </in>
</and>
```



Date	Operation	User	Computer	Rule	Application
2024-05-21 오후 3:11:39	Network Operation Ex	NT AUTHORITY\NETWORK SERVICE	DESKTOP-QMLBU3N	06-1. 블루투스 테더링	svchost.exe

1 of 1

Host name	Remote Port	Local Port	Protocol	Direction	Bytes Read	Bytes Written
10.6.114.42	53	60576	DNS	Outbound	0	0

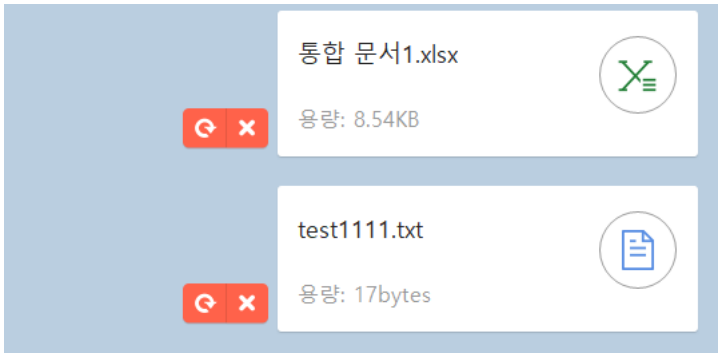
아이폰과 노트북을 사용하여 블루투스 테더링 사용 차단 확인.

10. Kakatalk을 이용한 파일 업로드(차단)

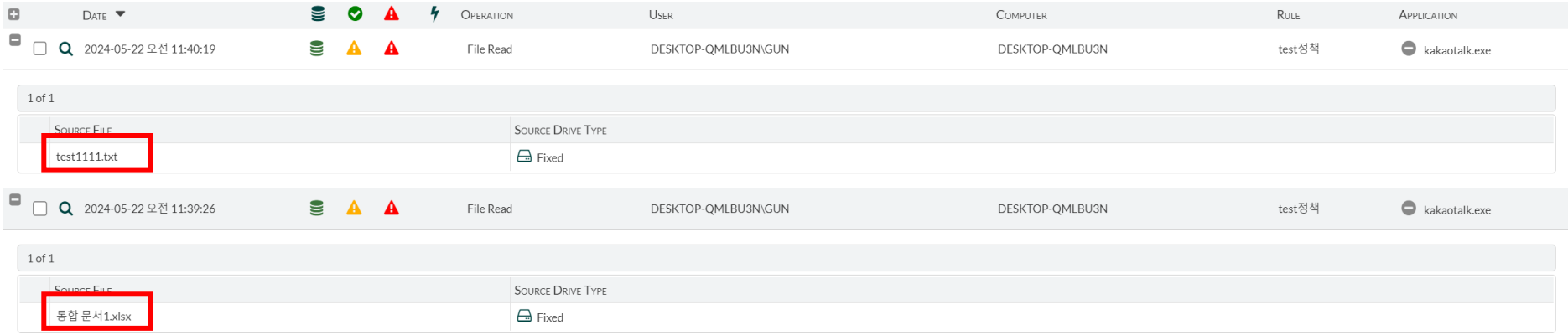
```
<and>

  <not>
    <equal>
      <evtSrcFileExt />
      <string value="" />
    </equal>
  </not>

  <not>
    <in op="like" match="any">
      <evtSrcFilePath />
      <list>
        <string value="%₩appdata₩roaming₩%" />
        <string value="%₩appdata₩local₩%" />
        <string value="%₩appdata₩locallow₩%" />
        <string value="%₩prefetch₩%" />
        <string value="%₩windows₩%" />
        <string value="%₩program files (x86)₩kakao₩%" />
      </list>
    </in>
  </not>
  <in>
    <curProcessImageName />
    <list>
      <string value="KakaoTalk.exe" />
    </list>
  </in>
  <equal>
    <evtOperationType />
    <constOpFileRead />
  </equal>
</and>
```



기본 예외시킬 경로이고 추가하고 싶은 프로세스의 경로 추가



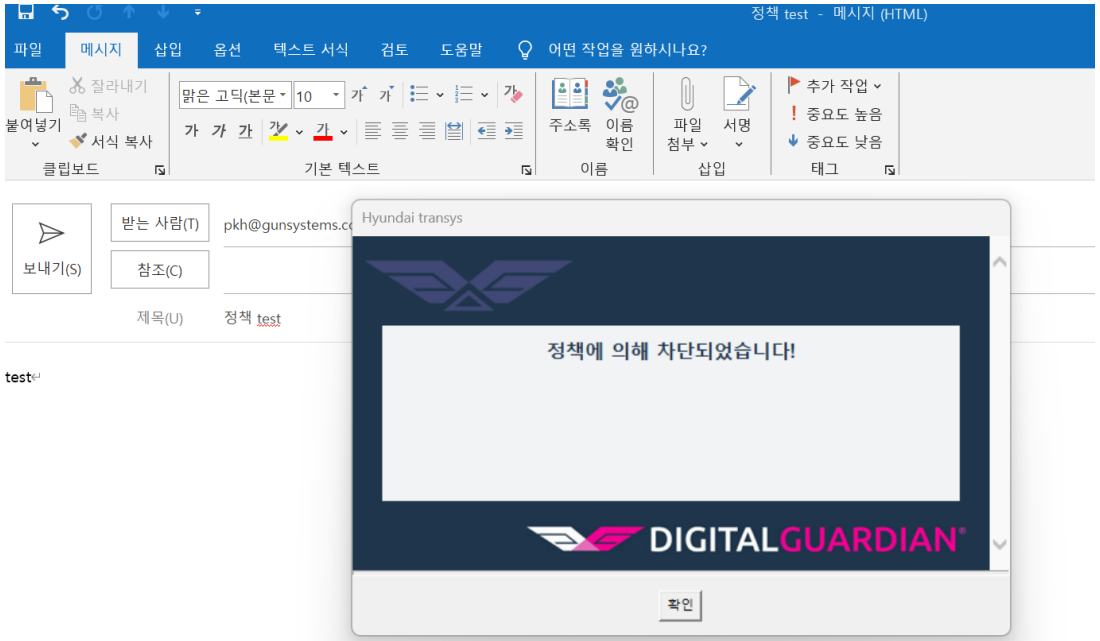
11. 웹 브라우저 실행(차단)

```
<and>
<or>
  <like expr="Firefox Setup%">
    <curProcessImageName />
  </like>
  <like expr="Firefox20Setup%">
    <curProcessImageName />
  </like>
 <like expr="firefox%">
    <curProcessImageName />
  </like>
<or>
<equal>
    <evtOperationType />
    <constOpAppStart />
  </equal>
</and>
```

Firefox 실행 안되는 거 확인 (크롬,웨일 지원 안함)

12. Outlook 첨부파일 (차단)

```
<in>
  <evtOperationType />
  <list>
    <constOpMailAttach />
  </list>
</in>
```



Date	Operation	User	Computer	Rule	Application
2024-05-23 오후 3:16:49	Attach Mail	DESKTOP-QMLBU3N\GUN	DESKTOP-QMLBU3N	test정책	outlook.exe

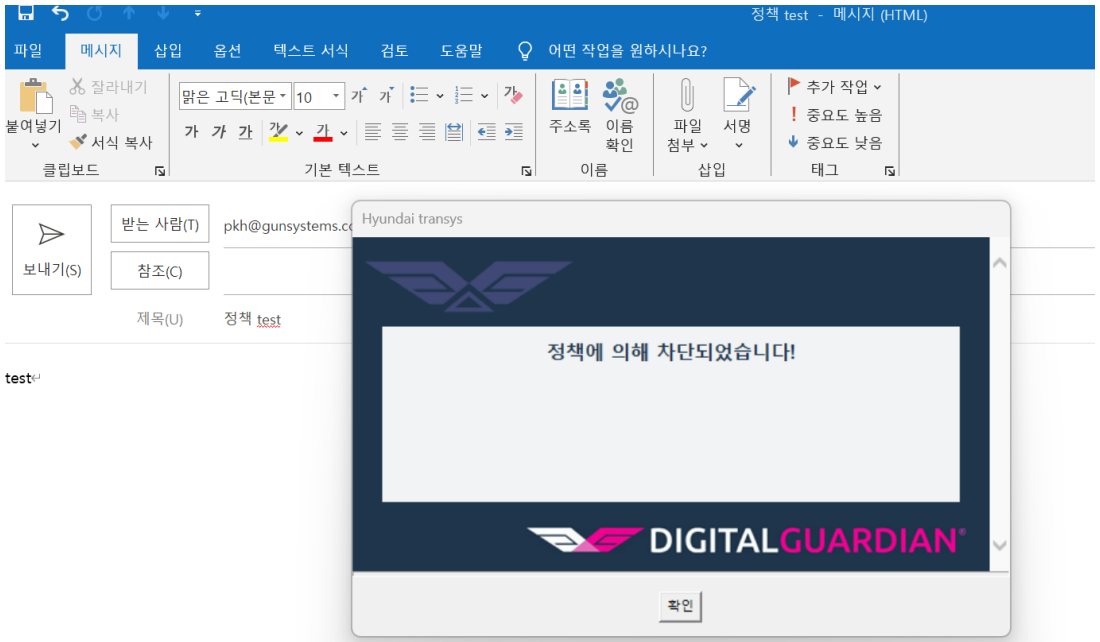
1 of 1

Source File	Source Drive Type	Destination File	File Size
test1111.txt	Fixed		1 KB

파일 첨부 안되는 것 확인

13. 메일 보낼 시(차단)

```
<equal>
  <evtOperationType />
  <constOpSendMail />
</equal>
```



Date	Operation	User	Computer	Rule	Application
2024-05-23 오후 3:22:11	Send Mail	DESKTOP-QMLBU3N\GUN	DESKTOP-QMLBU3N	test정책	outlook.exe

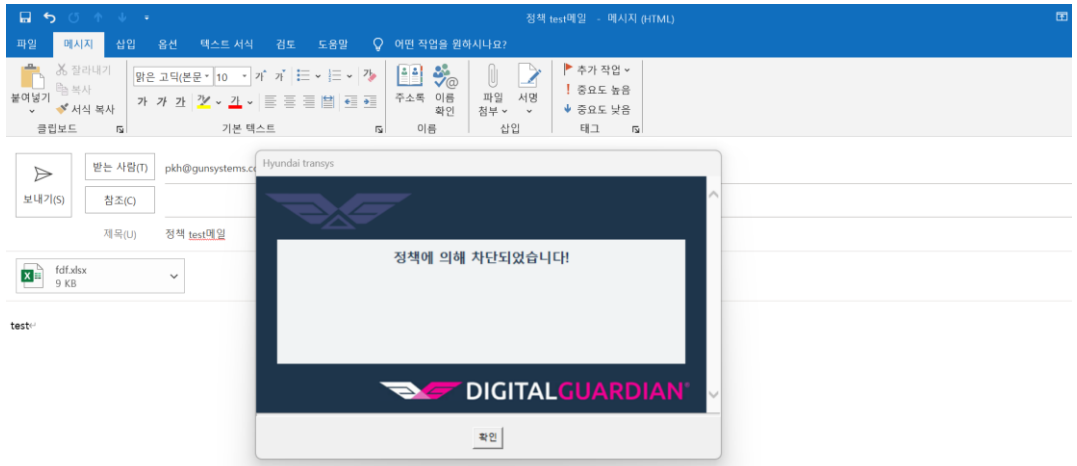
From: pkh@gunsystems.co.kr
Subject: 정책 test메일

1 of 1

Source File	Source Drive Type	Destination File	File Size
message body	Fixed	message body	

14. Outlook txt첨부파일만 (차단)

```
<and>
  <equal>
    <evtSrcFileExt />
    <string value="txt" />
  </equal>
  <equal>
    <evtOperationType />
    <constOpMailAttach />
  </equal>
</and>
```



Date	Operation	User	Computer	Rule	Application
2024-05-23 오후 3:34:58	Attach Mail	DESKTOP-QMLBU3N\GUN	DESKTOP-QMLBU3N	test정책	outlook.exe

1 of 1

Source File	Source Drive Type	Destination File	File Size
test1111.txt	Fixed		1 KB

Source File Extension 를 이용해 소스 파일 확장자를 txt로 선언 했고
엑셀파일은 첨부가 정상적으로 되지만 txt파일은 첨부가 안됨

15. 테더링(차단)

```
<and>
<or>
   <like expr="%NDIS%">   //안드로이드 기기 테더링 어뎁터
     <evtAdapterName />
   </like>
   <like expr="%Remote%"> //테더링시 공유 폴더 탐지
     <evtAdapterName />
   </like>
   <like expr="%Apple%"> //애플 기기에 대한 테더링 어뎁터
     <evtAdapterName />
   </like>
 </or>
 <in>
   <evtOperationType />
   <list>
     <constOpNetwork />
     <constOpNetworkEx />
   </list>
 </in>
</and>
```

Date	Operation	User	Computer	Rule	Application
2024-05-24 오전 11:04:34	Network Operation Ex	DESKTOP-QMLBU3N\GUN	DESKTOP-QMLBU3N	05. 테더링	msedge.exe

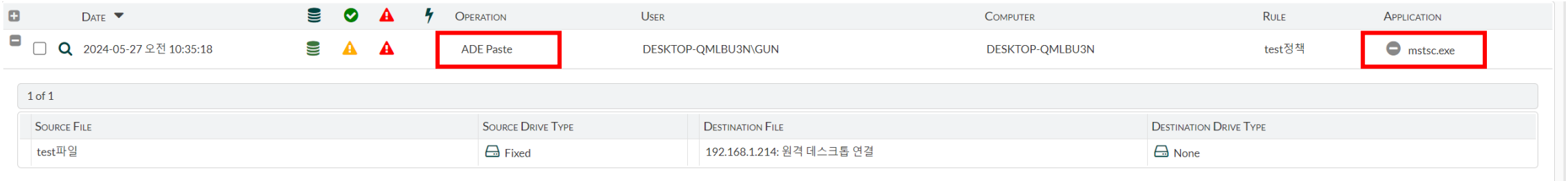
1 of 1

Host name	Remote Port	Local Port	Protocol	Direction	Bytes Read	Bytes Written
224.0.0.251	5353	5353	UDP	Outbound	0	0

테더링시 장치관리자에 apple 로 시작하는 어뎁터 인식 확인과 동시에 테더링 차단

16. PC 에서 MSTSC 파일 붙여넣기(차단)

```
<and>
  <equal>
    <evtSrcDriveType />
    <constDriveFixed />
  </equal>
  <equal>
    <curProcessImageName />
    <string value="mstsc.exe" />
  </equal>
  <in>
    <evtOperationType />
    <list>
      <constOpFileCopy />
      <constOpFileMove />
      <constOpAdePaste />
    </list>
  </in>
</and>
```



Date	Operation	User	Computer	Rule	Application
2024-05-27 오전 10:35:18	ADE Paste	DESKTOP-QMLBU3N\GUN	DESKTOP-QMLBU3N	test정책	mstsc.exe

1 of 1

Source File	Source Drive Type	Destination File	Destination Drive Type
test파일	Fixed	192.168.1.214: 원격 데스크톱 연결	None

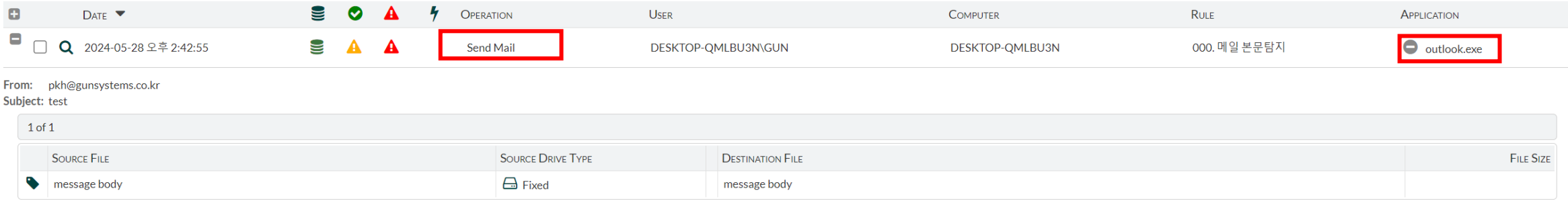
바탕화면 TXT문서를 원격서버에 파일 붙여넣기 안되는 것 확인
소스파일 확인해보면 붙여넣은 문서가 아니라 폴더가 찍힘 즉 바탕화면에서 원격으로 옮기는건 막지 못함 폴더에서 원격으로 넘겨야만 차단 이유를 찾아볼 필요가 있음

->확인해보니 드라이브타입을 <constDriveUnknown /> 바꿔보니 바탕화면에서 붙여넣은 것 차단 확인

17. Outlook 본문 키워드 (차단)

```
<and>
  <equal>
    <evtSrcFilePolicyTag /> (정책 불러오는 것)
    <string value="test" />
  </equal>
  <in>
    <evtOperationType />
    <list>
      <constOpSendMail />
    </list>
  </in>
</and>
```

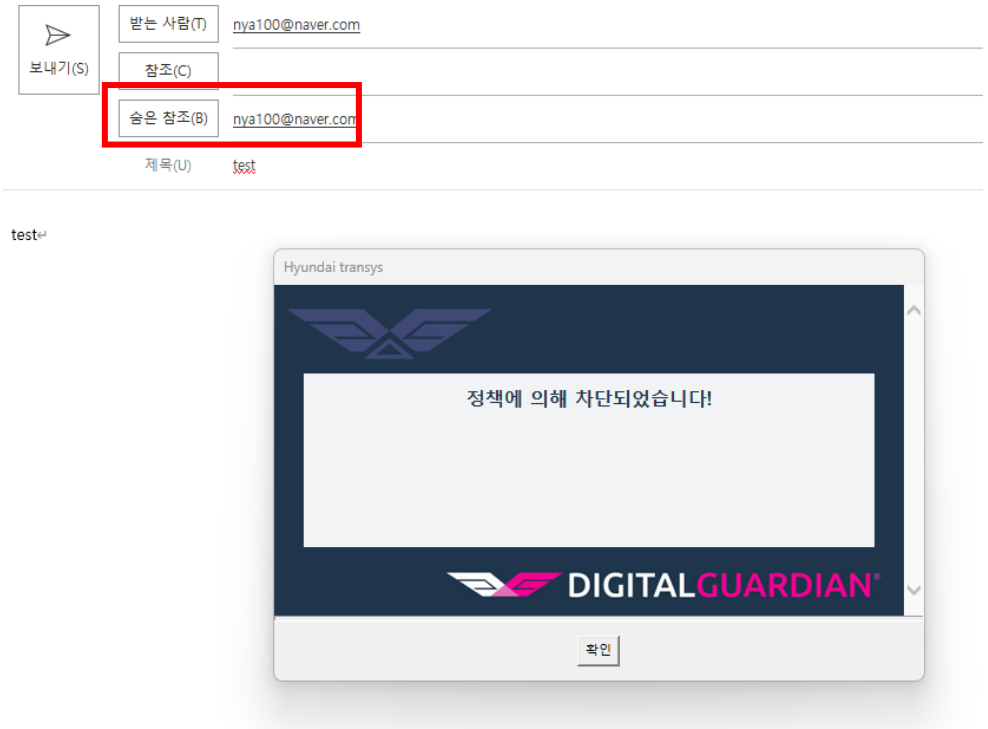
<evtSrcFileEntityFrequency name> 규칙이름 불러오는 것

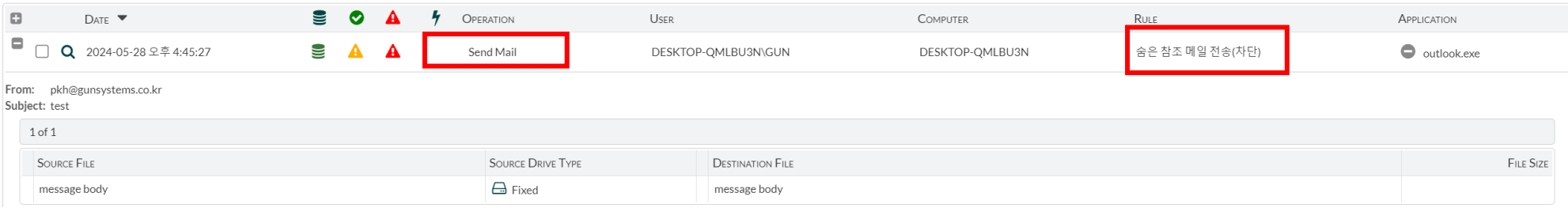


Outlook 메일 본문에 설정한 키워드 "Kwang" 가 포함되면 차단 되는 것 확인.

18. Outlook 숨은 참조 메일 보낼 시(차단)

```
<and>
  <equal>
    <evtMailRecipientTypes />
    <constMailBCC />                -> BCC = 숨은 참조
  </equal>
  <equal>
    <evtOperationType />
    <constOpSendMail />
  </equal>
</and>
```

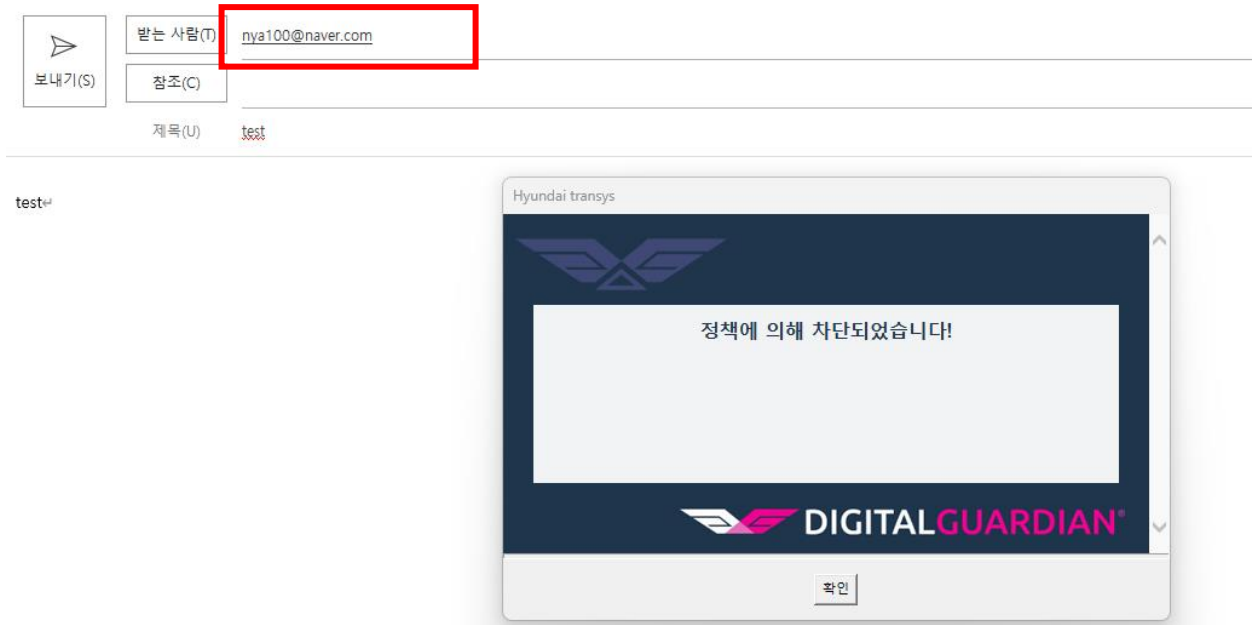


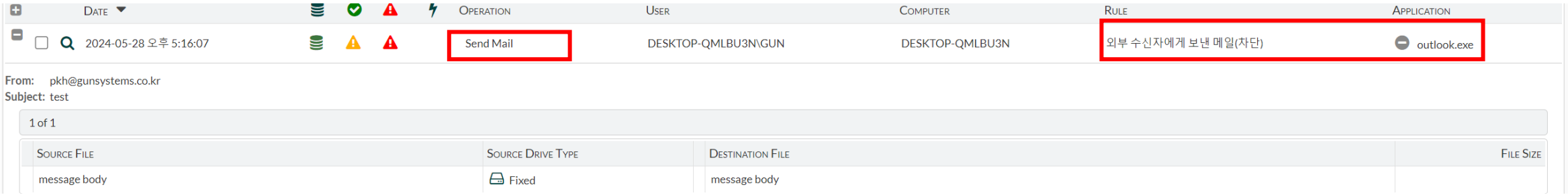


Outlook 메일 숨은 참조 메일 보낼 시 차단 확인

19. Outlook 외부 사용자에게 메일 전송(차단)

```
<and>
  <not>
     <like expr="%gunsystems.co.kr">
      <evtMailRecipients/>
    </like>
  </not>
  <equal>
    <evtOperationType/>
    <constOpSendMail/>
  </equal>
</and>
```

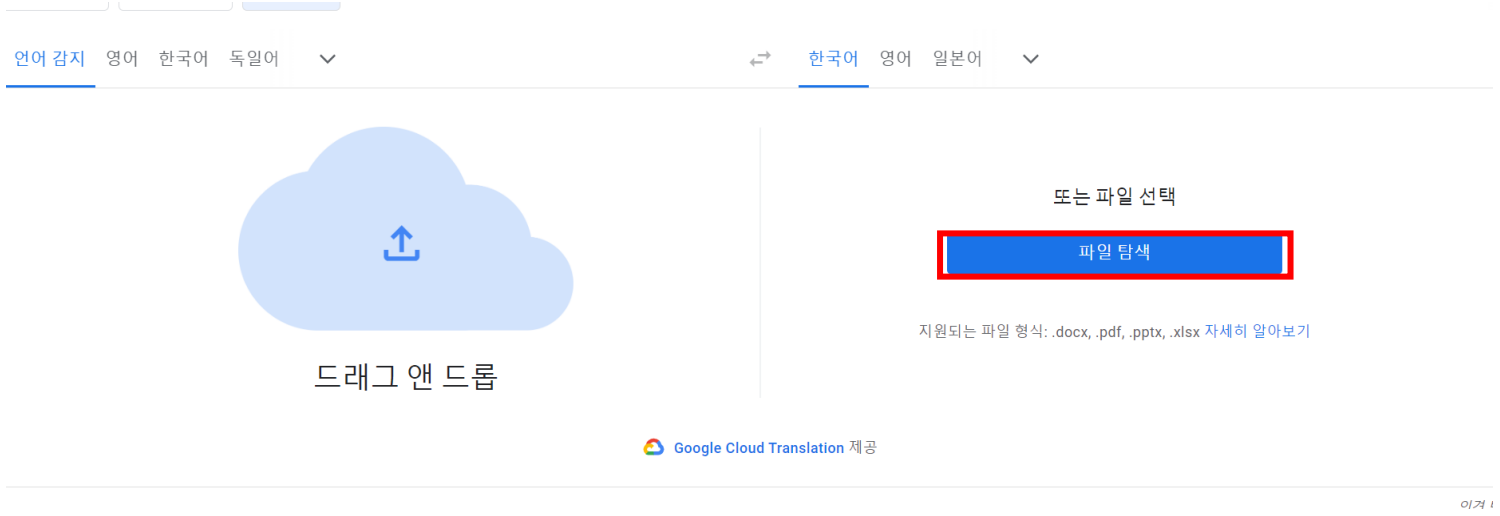




Outlook을 이용해 외부 메일인 nya100@naver.com은 차단이 되었고 , 코드에 예외처리 한 내부 메일은 정상적으로 메일 전송 확인

20. 크롬을 이용하여 구글 번역기 파일 업로드(차단)

```
<and>
  <in op = "like" match = "any">
    <evtSrcFilePath />
    <list>
      <string value = "%₩%" />
    </list>
  </in>
  <or>
    <in op="like" match="any">
      <curProcessAddressBar/>
      <list>
        <string value="%translate.google.co.kr%" />
      </list>
    </in>
    <in op="like" match="any">
      <evtDomain/>
      <list>
        <string value="%translate.google.co.kr%" />
      </list>
    </in>
  </or>
  <in>
    <evtOperationType />
    <list>
      <constOpFileOpen />
      <constOpNetTransferUpload />
    </list>
  </in>
</and>
```



파일 탐색기 버튼이 눌리지 않음을 확인

21. 크롬,엣지 이용하여 파일 업로드(차단)

```
<and>
  <in op="like" match="any">
    <evtDomain/>
    <list>
      <string value="%nextpcb.com%" />
      <string value="%papago.naver.com%" />
      <string value="%clients6.google.com%" />
      <string value="%push.clients6.google.com%" />
    </list>
  </in>
  <in>
    <curProcessImageName />
    <list>
      <string value="chrome.exe" />
      <string value="msedge.exe" />
    </list>
  </in>
  <in>
    <evtOperationType />
    <list>
      <constOpNetTransferUpload />
    </list>
  </in>
</and>
```

해당 사이트들 문서 업로드 안되는거 확인 완료

22. 스크린 캡쳐(차단)

```
<or>
  <in>
    <evtOperationType />
    <list>
      <constOpAdePrintScreen />
      <constOpAdeScreenCapture />
    </list>
  </in>

  <and>
    <equal>
      <curProcessImageName />
      <string value="lightshot.exe" />
    </equal>
    <in>
      <evtOperationType />
      <list>
        <constOpFileSaveAs />
        <constOpFileWrite />
        <constOpAdePrintScreen />
        <constOpAdeScreenCapture />
      </list>
    </in>
  </and>
</or>
```

첫 번째 경우: 컴퓨터에서 스크린샷을 찍는 명령을 실행하는 경우.

두 번째 경우: 컴퓨터에서 SnippingTool.exe 프로그램이 실행 중이고, 파일을 저장하거나 쓰거나, 스크린샷을 찍는 명령을 실행하는 경우.

Date	Operation	User	Computer	Rule	Application
2024-05-30 오후 4:35:40	File Write	DESKTOP-QMLBU3N\GUN	DESKTOP-QMLBU3N	캡쳐 차단	snippingtool.e

1 of 1

Source File	Source Drive Type	Destination File	Destination Drive Type	File Size
settings.dat.log1	Fixed		None	

캡처 도구 실행 안되는 것 확인 완료