00. 보안 진단 툴

첫번째로는 ai를 사용하지 않은 툴이다.

ai가 그리 코딩에 쓸만하지 않을때, 그리고 한참 python을 업무에 활용해보고 싶을때 집에서 틈틈히 만들었다.

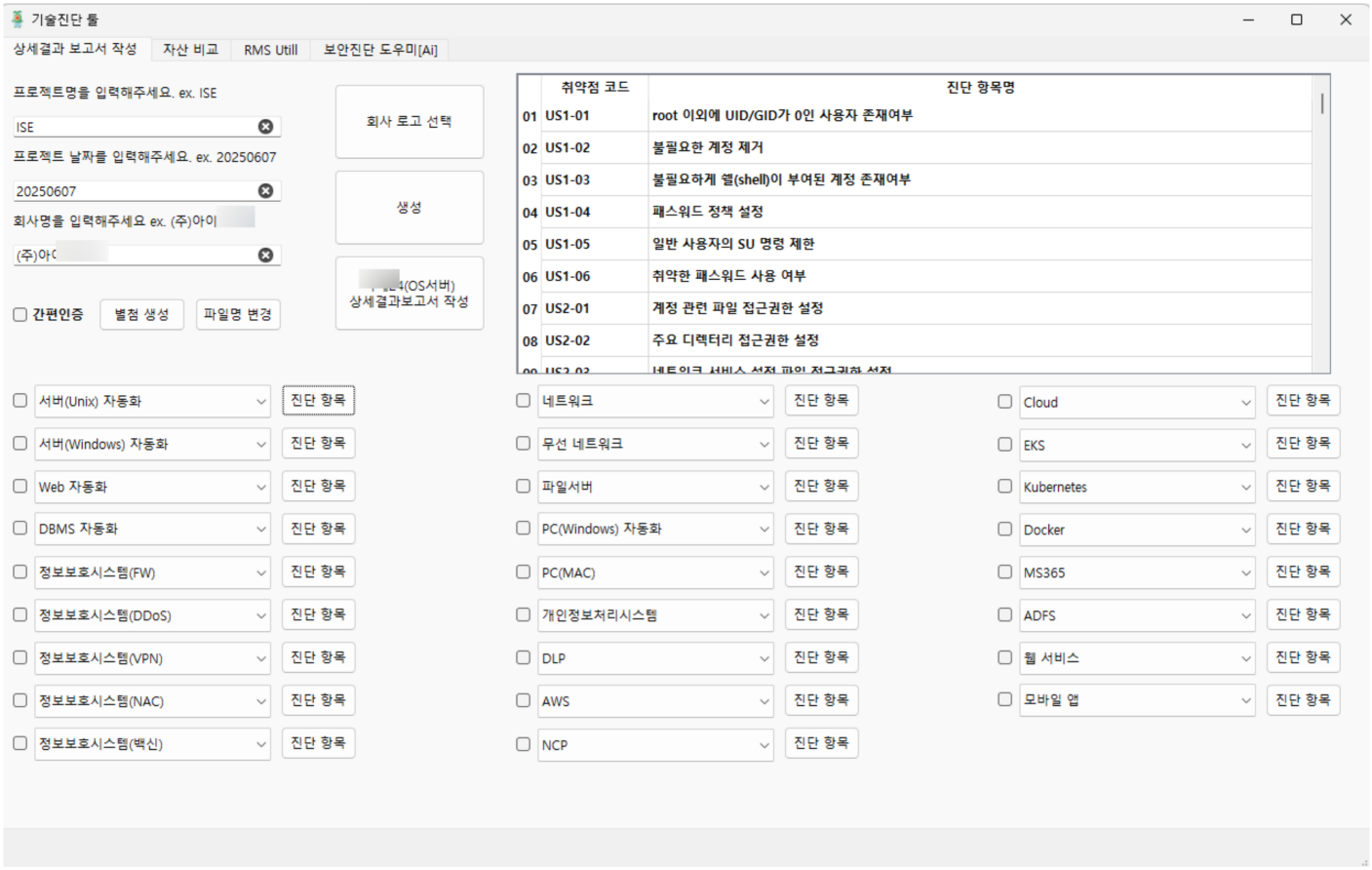
요즘엔 필요한 툴은 다 ai가 쉽게 만들어 주지만, 뭔가 기왕 ai 없이 시작한거 이 프로그램의 유지보수는 항상 직접하고 있다.

네이버 블로그에 이전에 정리해둔 내용을 가져왔다.

*이후 이것저것 추가가 됐지만 패스-

파이썬 + QT Designer 를 사용하여 GUI로 사용하는 툴을 만들었다.

이전에 개발해서 쓰고 있던 프로그램을 계속 업데이트 해서 쓰고 있는데 그냥 근황 겸 남겨본다 .



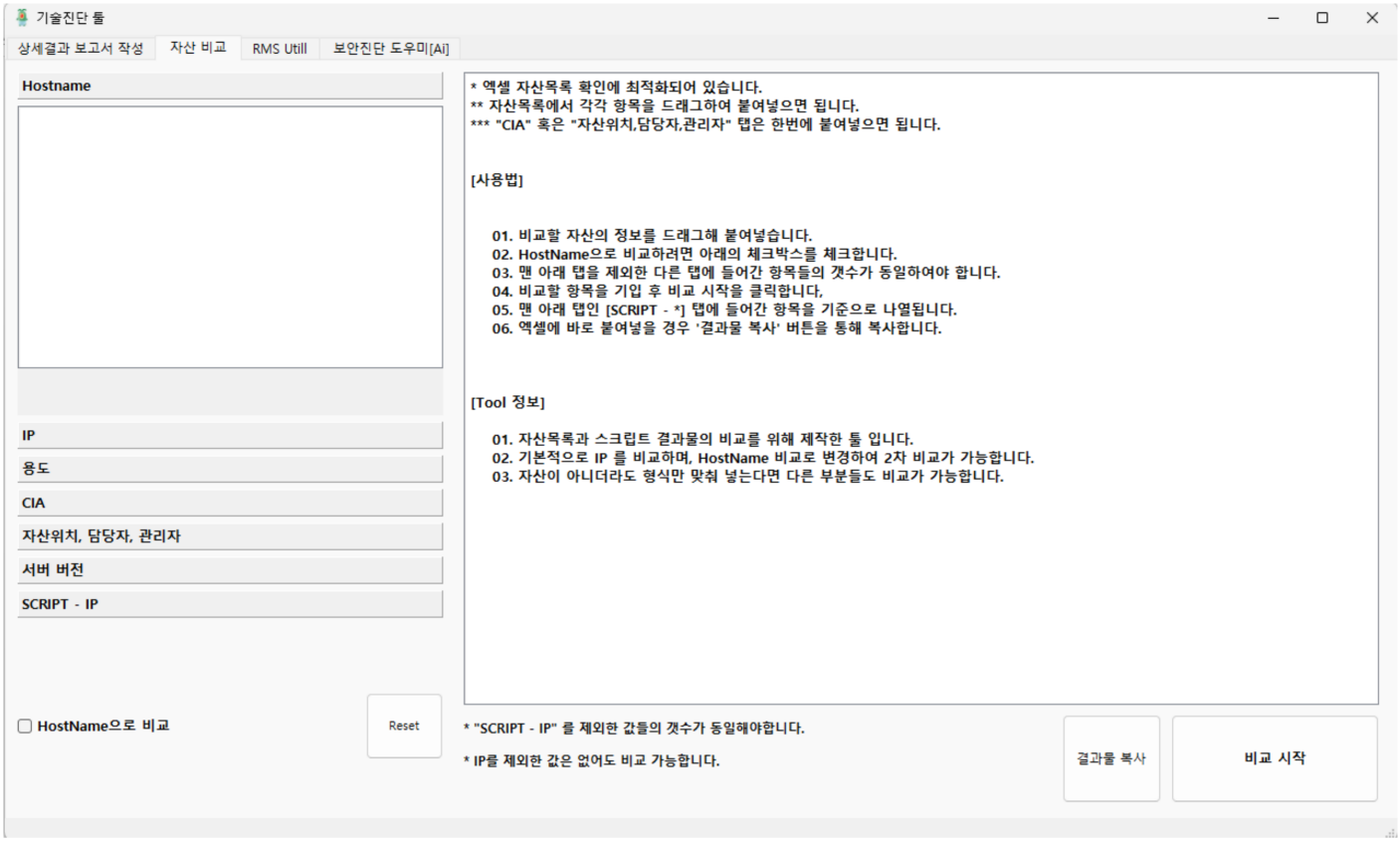
첫번째 탭은 , 자산 종류 별로 엑셀 보고서 파일을 만들어야하는데 회사 로고를 넣거나 , 날짜 , 자산종류 명 등등

엑셀파일을 매번 생성하기 귀찮아서 만들었다 .

라이브러리는 **win32com** 을 주로 사용했다 .

이미지 크기 조절 , 화질 조절하는거에 되게 애먹었던 기억이 ..

보고서를 열 몇개씩 만들 일들이 꽤 많은데 편하게 사용했다 .



두번째 탭은 , 자산 진단을 하다보면 회사 자산의 수정 여부를 파악하는데 시간이 너무 많이 들어서 만든 툴이다 .

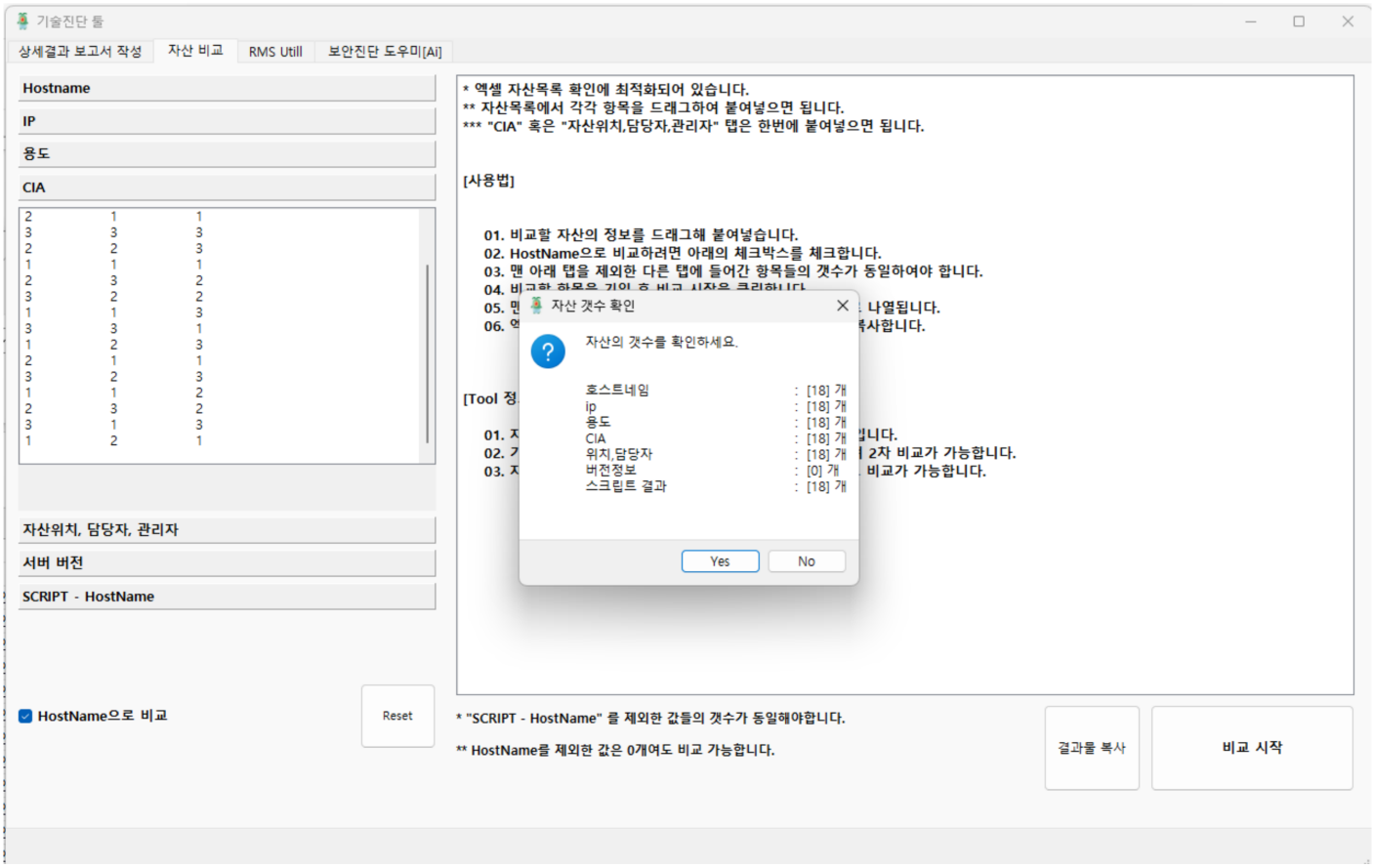
기준이 되는 항목을 맨 아래 탭에 넣으면 매칭하고 싶은 행을 가져온다 .

예를 들어보면

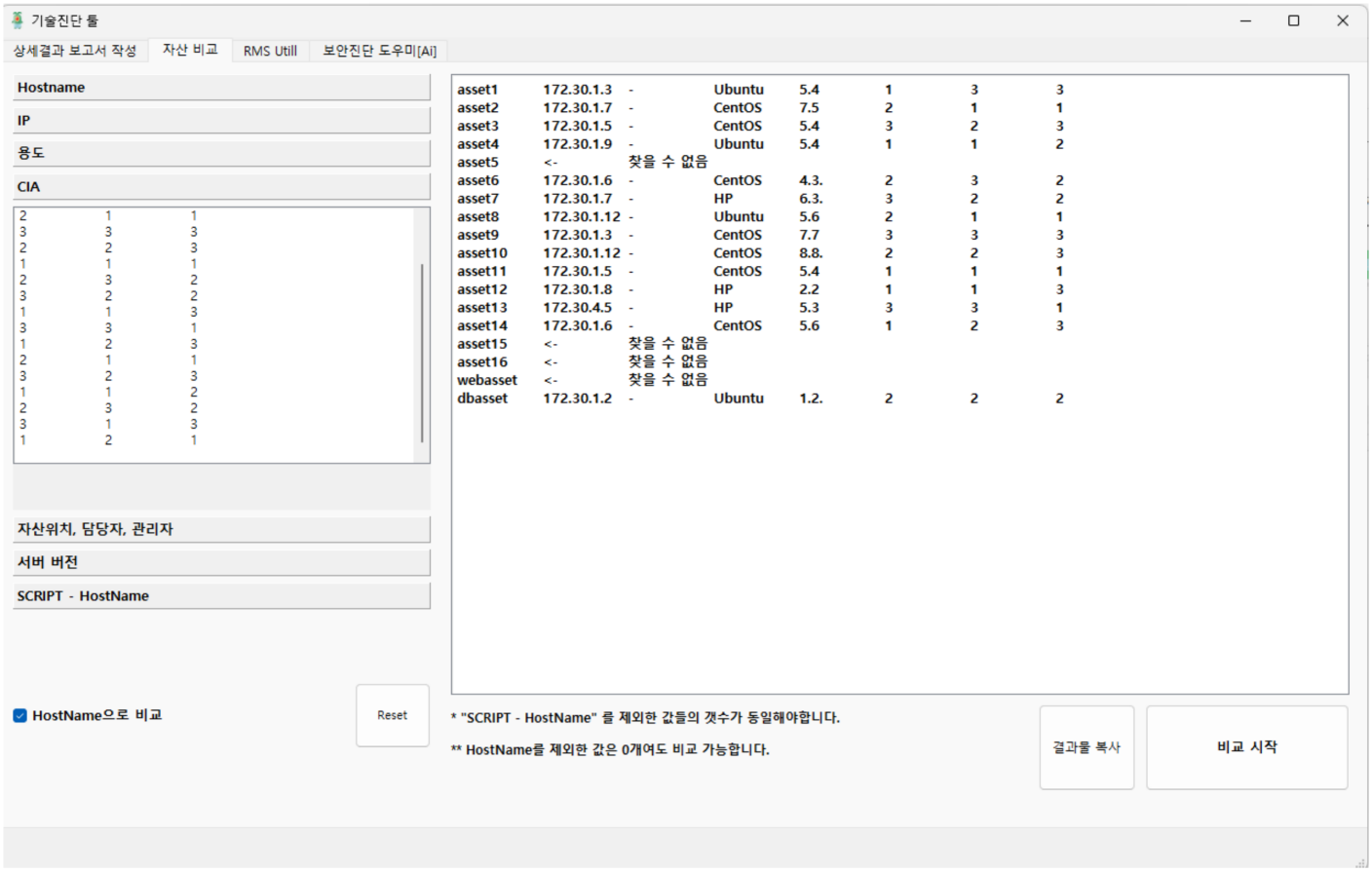
자산목록								제공받은 스크립트 결과(기준)
자산	종류	IP	버전	C	I	A		자산
webaseet	Ubuntu	172.30.1.1	1.2.	3	2	1		asset1
dbasset	Ubuntu	172.30.1.2	1.2.	2	2	2		asset2
asset1	Ubuntu	172.30.1.3	5.4	1	3	3		asset3
asset8	Ubuntu	172.30.1.12	5.6	2	1	1		asset4
asset9	CentOS	172.30.1.3	7.7	3	3	3		asset5
asset10	CentOS	172.30.1.12	8.8.	2	2	3		asset6
asset11	CentOS	172.30.1.5	5.4	1	1	1		asset7
asset6	CentOS	172.30.1.6	4.3.	2	3	2		asset8
asset7	HP	172.30.1.7	6.3.	3	2	2		asset9
asset12	HP	172.30.1.8	2.2	1	1	3		asset10
asset13	HP	172.30.4.5	5.3	3	3	1		asset11
asset14	CentOS	172.30.1.6	5.6	1	2	3		asset12
asset2	CentOS	172.30.1.7	7.5	2	1	1		asset13
asset3	CentOS	172.30.1.5	5.4	3	2	3		asset14
asset4	Ubuntu	172.30.1.9	5.4	1	1	2		asset15
asset32	Ubuntu	172.30.1.7	4.3.	2	3	2		asset16
asset33	Ubuntu	172.30.1.8	6.3.	3	1	3		webasset
asset34	Ubuntu	172.30.1.1(	2.2	1	2	1		dbasset

왼쪽이 제공받은 자산목록이고 오른쪽에 왼쪽의 자산 정보를 옮겨야 할때

하나하나 매칭해가면서 붙여넣기가 너무 귀찮다 .

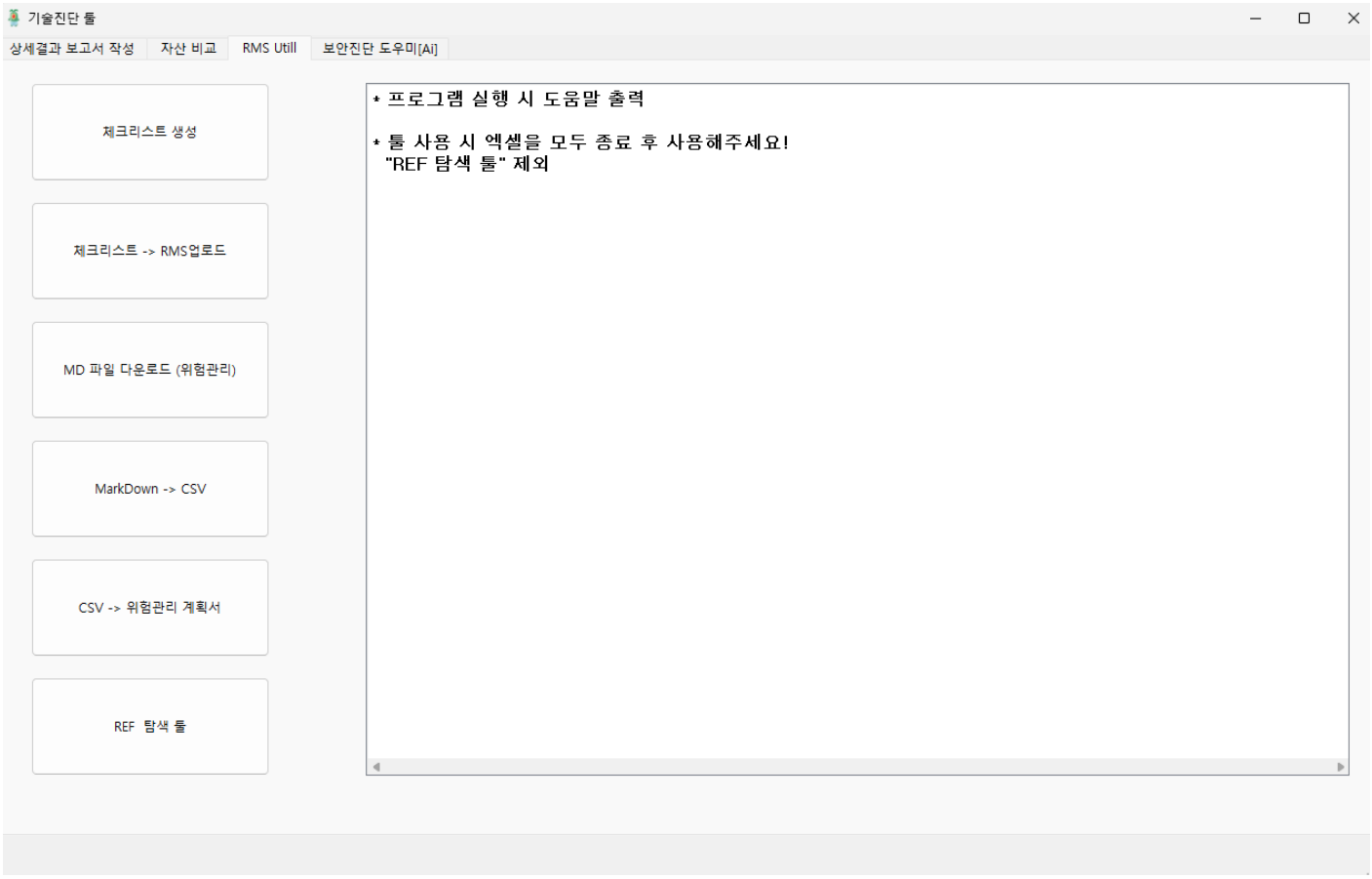


값을 넣고 비교시작을 누르면 갯수를 파악하고 (기준을 제외한 값들은 갯수가 같아야한다 .)



맨 아래에 넣은 데이터에 관련 정보를 가져와준다 .

굳이 자산 정보가 아니여도 엑셀에 있는 값들을 복사해 넣으면 비교가 되므로 이곳저곳에서 잘 활용 중



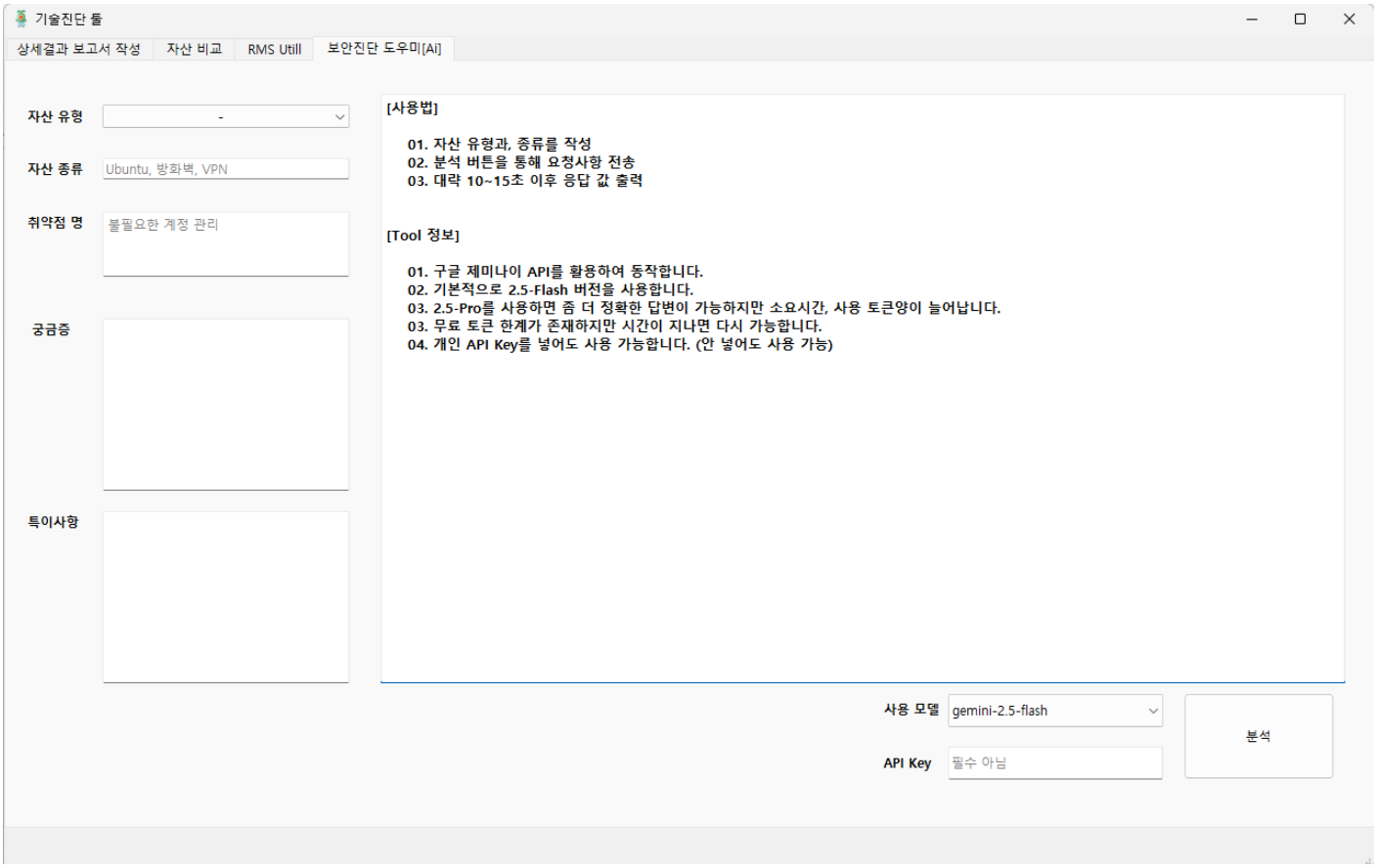
```
* 프로그램 실행 시 도움말 출력

* 툴 사용 시 엑셀을 모두 종료 후 사용해주세요!
  "REF 탐색 툴" 제외
```

세번째는 회사에서 개발 중인 솔루션에서 아직 불편한 부분들이 있어서 좀 편하게 할 수 있는 기능들을 넣어두었다.

솔루션에서 지원하면 안 쓸 기능들이기 때문에 대강대강 만들어서 붙여둠

1. 진단 체크리스트 (엑셀) 생성 기능
2. 진단완료한 체크리스트를 솔루션에 업로드하기 편한 csv로 변환해줌
3. 보고서 제작을 위한 데이터를 솔루션에서 다운로드 받아줌
4. 솔루션에서 받은 markdown 파일을 csv로 변환
5. csv파일을 사용해 엑셀 보고서 생성
6. 진단 시 스크립트 결과파일을 분석하기 편한 프로그램 실행 (ai가 만들어줌 ㅋㅋ)



사용 모델 gemini-2.5-flash

[사용법]

01. 자산 유형과, 종류를 작성
02. 분석 버튼을 통해 요청사항 전송
03. 대략 10~15초 이후 응답 값 출력

[Tool 정보]

01. 구글 제미나이 API를 활용하여 동작합니다.
02. 기본적으로 2.5-Flash 버전을 사용합니다.
03. 2.5-Pro를 사용하면 좀 더 정확한 답변이 가능하지만 소요시간, 사용 토큰양이 늘어납니다.
03. 무료 토큰 한계가 존재하지만 시간이 지나면 다시 가능합니다.
04. 개인 API Key를 넣어도 사용 가능합니다. (안 넣어도 사용 가능)

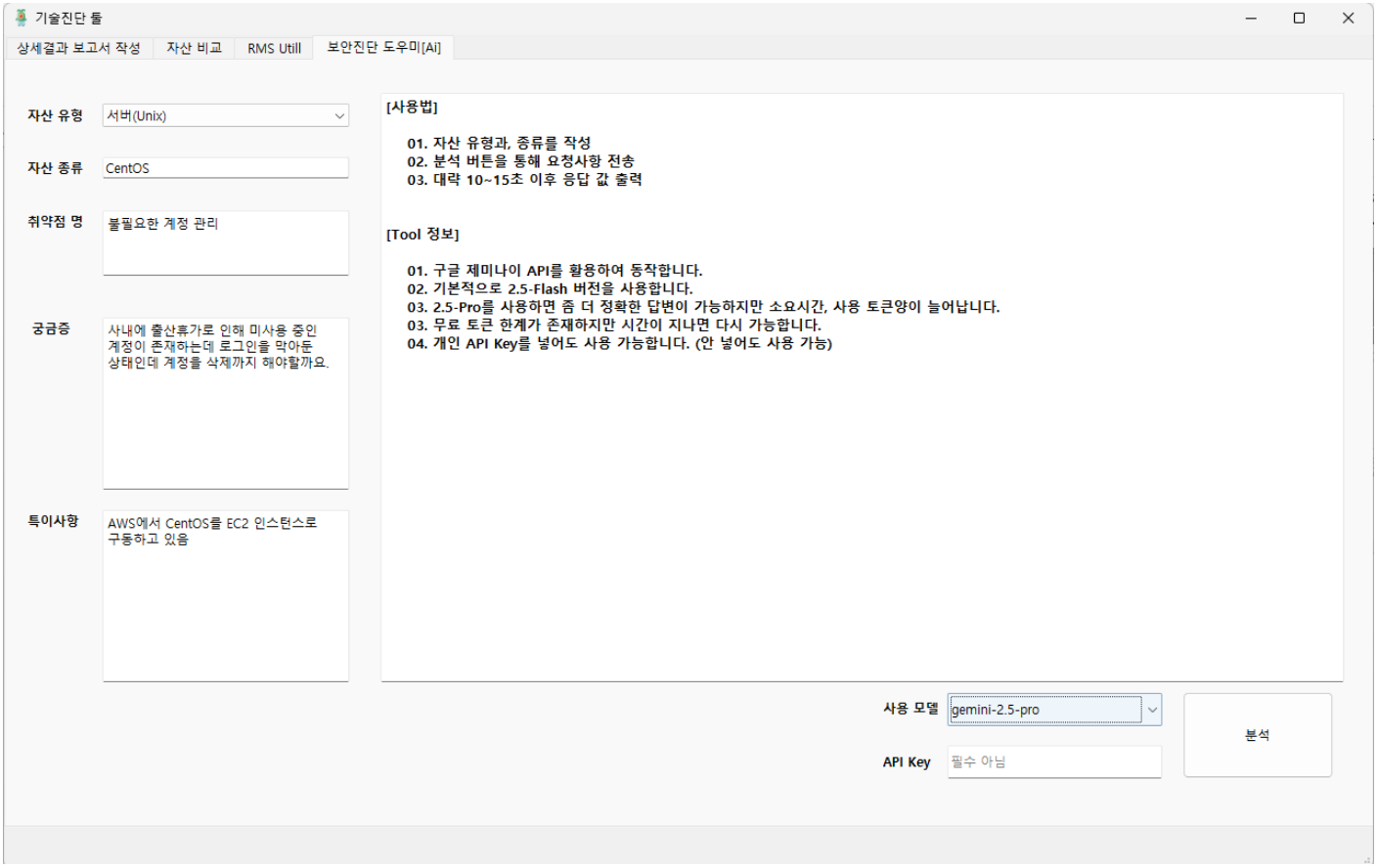
네번째 탭은 보안 컨설팅 진단을 할때 궁금한 점들을 빠르게 물어보기 위해 세팅해둔 **ai** 도우미 탭이다.

gpt에 그냥 물어보면 공부 목적인지 컨설팅을 위한건지 헷갈려 할때가 많은데

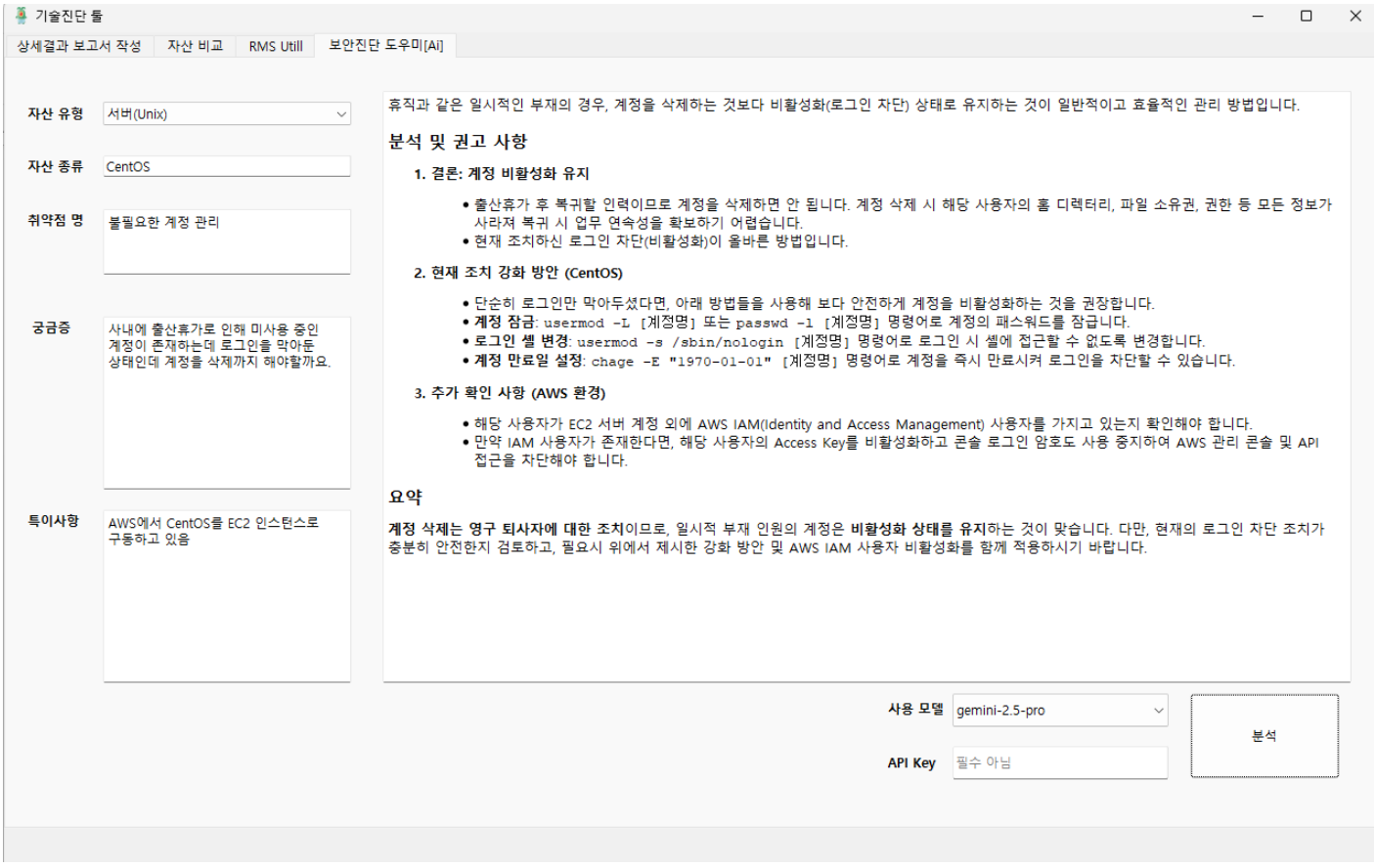
미리 코드 안에 보안 컨설턴트 페르소나를 지정해 두어 그냥 질문을 던지면 컨설턴트 입장에서의 답변을 해준다.

제미나이 무료 **API**를 사용하고 있으며 코드자체는 별로 복잡하지 않은편이다.

*현재는 디스코드를 통해 오픈클로에게 바로바로 물어보는 중 (사용 안한지 좀 됨)


기술진단 툴
상세결과 보고서 작성
자산 비교
RMS Utill
보안진단 도우미[Ai]
자산 유형
서버(Unix)
자산 종류
CentOS
취약점 명
불필요한 계정 관리
궁금증
사내에 출산휴가로 인해 미사용 중인 계정이 존재하는데 로그인을 막아둔 상태인데 계정을 삭제까지 해야할까요.
특이사항
AWS에서 CentOS를 EC2 인스턴스로 구동하고 있음
[사용법]
01. 자산 유형과, 종류를 작성
02. 분석 버튼을 통해 요청사항 전송
03. 대략 10~15초 이후 응답 값 출력
[Tool 정보]
01. 구글 제미나이 API를 활용하여 동작합니다.
02. 기본적으로 2.5-Flash 버전을 사용합니다.
03. 2.5-Pro를 사용하면 좀 더 정확한 답변이 가능하지만 소요시간, 사용 토큰양이 늘어납니다.
03. 무료 토큰 한계가 존재하지만 시간이 지나면 다시 가능합니다.
04. 개인 API Key를 넣어도 사용 가능합니다. (안 넣어도 사용 가능)
사용 모델
gemini-2.5-pro
API Key
필수 아님
분석

□□□ □□ □□□□ □□□□ , (□□ □□□□□ □□□ □ □□□ .)


기술진단 툴
상세결과 보고서 작성
자산 비교
RMS Utill
보안진단 도우미[Ai]
자산 유형
서버(Unix)
자산 종류
CentOS
취약점 명
불필요한 계정 관리
궁금증
사내에 출산휴가로 인해 미사용 중인 계정이 존재하는데 로그인을 막아둔 상태인데 계정을 삭제까지 해야할까요.
특이사항
AWS에서 CentOS를 EC2 인스턴스로 구동하고 있음
휴직과 같은 일시적인 부재의 경우, 계정을 삭제하는 것보다 비활성화(로그인 차단) 상태로 유지하는 것이 일반적이고 효율적인 관리 방법입니다.
분석 및 권고 사항
1. 결론: 계정 비활성화 유지
• 출산휴가 후 복귀할 인력이므로 계정을 삭제하면 안 됩니다. 계정 삭제 시 해당 사용자의 홈 디렉터리, 파일 소유권, 권한 등 모든 정보가 사라져 복귀 시 업무 연속성을 확보하기 어렵습니다.
• 현재 조치하신 로그인 차단(비활성화)이 올바른 방법입니다.
2. 현재 조치 강화 방안 (CentOS)
• 단순히 로그인만 막아두셨다면, 아래 방법들을 사용해 보다 안전하게 계정을 비활성화하는 것을 권장합니다.
• 계정 잠금: usermod -L [계정명] 또는 passwd -l [계정명] 명령어로 계정의 패스워드를 잠급니다.
• 로그인 셸 변경: usermod -s /sbin/nologin [계정명] 명령어로 로그인 시 셸에 접근할 수 없도록 변경합니다.
• 계정 만료일 설정: chage -E "1970-01-01" [계정명] 명령어로 계정을 즉시 만료시켜 로그인을 차단할 수 있습니다.
3. 추가 확인 사항 (AWS 환경)
• 해당 사용자가 EC2 서버 계정 외에 AWS IAM(Identity and Access Management) 사용자를 가지고 있는지 확인해야 합니다.
• 만약 IAM 사용자가 존재한다면, 해당 사용자의 Access Key를 비활성화하고 콘솔 로그인 암호도 사용 중지하여 AWS 관리 콘솔 및 API 접근을 차단해야 합니다.
요약
계정 삭제는 영구 퇴사자에 대한 조치이므로, 일시적 부재 인원의 계정은 비활성화 상태를 유지하는 것이 맞습니다. 다만, 현재의 로그인 차단 조치가 충분히 안전한지 검토하고, 필요시 위에서 제시한 강화 방안 및 AWS IAM 사용자 비활성화를 함께 적용하시기 바랍니다.
사용 모델
gemini-2.5-pro
API Key
필수 아님
분석

이게 처음 만들어본 **GUI**가 있는 프로그램이였는데 , 많이 발전했다 싶다 ...

Revision #2
Created 2026-03-23 18:22:10 UTC by minwoo
Updated 2026-03-23 18:32:08 UTC by minwoo