CSCF | CYBER STRATEGY CONSULTING FIRM

" 사이버 보안의 올바른 방향을 제시합니다."

CSSCAN 사용자 매뉴얼

CONTENTS

"사이버 보안의 올바른 방향을 제시합니다."

“NON-AGENT 방식의 다중플랫폼을 지원하는 최적의 거버닝 솔루션”

CSSCAN은 에이전트가 필요 없는 다중 플랫폼 지원, 최신 반응형 UI 및 효율적인 리포팅을 통해 최적의 거버닝 솔루션을 제공합니다.

AGENTLESS | 다중 플랫폼 지원 | 최신 UI 적용 | 효율적인 리포팅

효율적인 Non-Agent 방식

- 간편한 구축과 신속한 도입: 에이전트가 필요 없는 시스템은 복잡한 설치 과정이나 지속적인 유지 관리가 필요 없습니다. 이로 인해 시스템을 빠르게 도입하고 즉시 사용할 수 있으며, IT 인프라에 대한 부담을 크게 줄일 수 있습니다.
- 시스템 자원의 효율적 활용: 에이전트가 없음으로 인해 추가적인 소프트웨어 컴포넌트가 시스템 자원을 소모하지 않습니다. 이는 특히 자원이 제한적인 환경에서 중요하며, 전체적인 시스템 성능을 향상시키고, 운영 비용을 절감할 수 있습니다.

Windows / Mac PC 지원

- 범용적인 솔루션 제공: 다양한 운영 체제와 하드웨어 플랫폼에서 CSSCAN를 사용할 수 있어, 조직 내 여러 기술 스택을 갖춘 환경에서도 통합된 관리 솔루션을 제공합니다. 이는 IT 인프라의 복잡성을 줄이고 관리를 통합할 수 있는 이점을 제공합니다.
- 일관된 관리와 사용자 경험: 모든 플랫폼에서 일관된 인터페이스와 기능을 제공함으로써 사용자가 다양한 시스템과 장비를 쉽게 관리할 수 있습니다. 이는 교육 및 지원 비용을 절감하고, 사용자 만족도를 높일 수 있습니다.

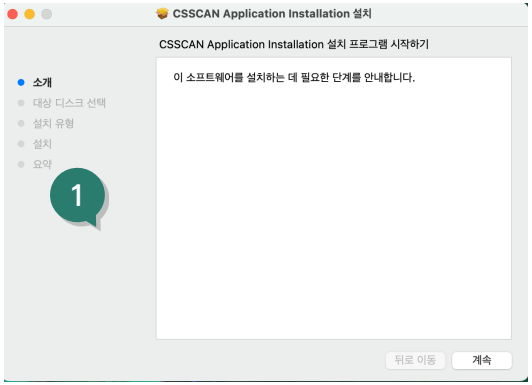
효과적인 Dashboard 지원

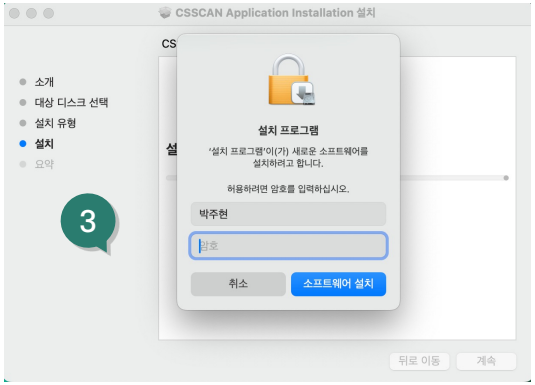
- 고급 사용자 인터페이스: 현대적인 디자인 원칙과 사용자 경험(UX) 최적화를 적용하여 사용자가 직관적으로 시스템을 이해하고 조작할 수 있게 합니다. 이는 사용자의 학습 곡선을 낮추고, 작업 효율성을 높입니다.
- 다양한 장치에서의 접근성: 반응형 웹 디자인을 통해 사용자가 데스크톱, 랩톱, 태블릿, 스마트폰 등 다양한 장치에서 동일한 사용성을 경험할 수 있습니다. 이는 현장에서의 실시간 데이터 접근과 수정을 가능하게 하여 업무의 유연성을 크게 향상시킵니다.

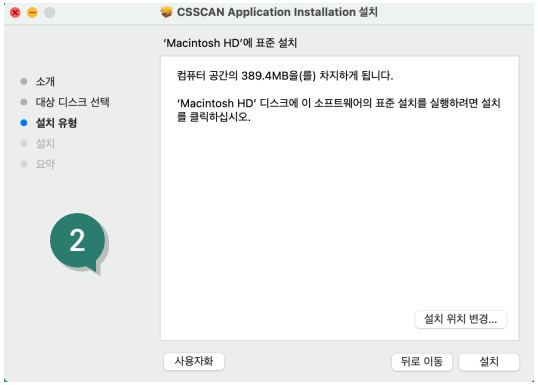
컨설팅 템플릿 적용

- 강력한 데이터 시각화: 사용자는 시각적인 대시보드를 통해 복잡한 데이터와 메트릭을 쉽게 해석하고 분석할 수 있습니다. 이는 복잡한 정보를 빠르게 파악하고, 효과적으로 의사소통하는 데 도움을 줍니다.
- 커스텀 검색 및 적응형 템플릿: 사용자는 강력한 검색 기능과 다양한 컨설팅 템플릿을 이용하여 필요한 정보를 즉시 검색하고, 특정 비즈니스 요구에 맞게 리포팅 형식을 맞춤 설정할 수 있습니다. 이는 효과적인 의사결정 지원과 전략적 인사이트 제공을 가능하게 합니다.

MAC Install

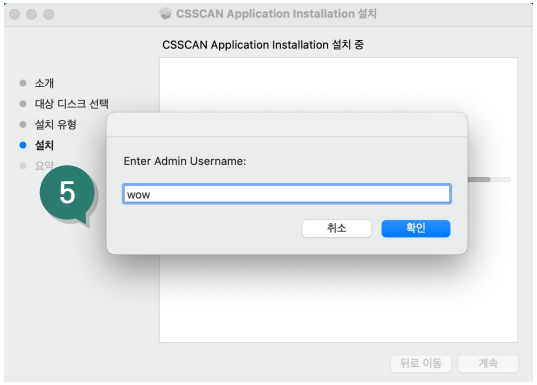

CSSCAN Application Installation 설치
CSSCAN Application Installation 설치 프로그램 시작하기
소개
대상 디스크 선택
설치 유형
설치
요약
이 소프트웨어를 설치하는 데 필요한 단계를 안내합니다.
1
뒤로 이동
계속

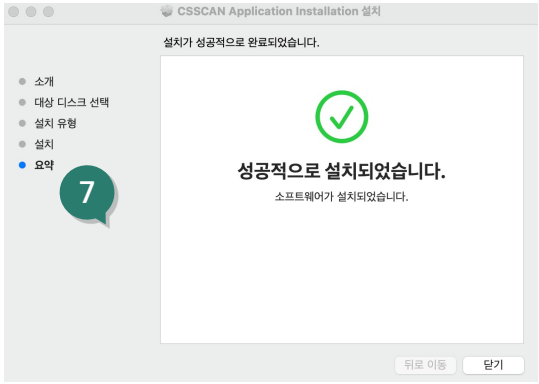

CSSCAN Application Installation 설치
소개
대상 디스크 선택
설치 유형
설치
요약
3
설치 프로그램
'설치 프로그램'이(가) 새로운 소프트웨어를 설치하려고 합니다.
허용하려면 암호를 입력하십시오.
박주현
암호
취소
소프트웨어 설치
뒤로 이동
계속

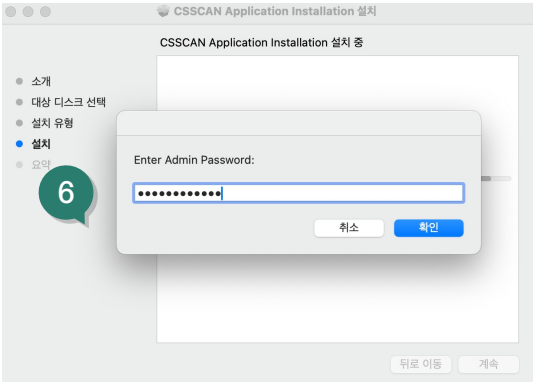

CSSCAN Application Installation 설치
'Macintosh HD'에 표준 설치
소개
대상 디스크 선택
설치 유형
설치
요약
2
컴퓨터 공간의 389.4MB을(를) 차지하게 됩니다.
'Macintosh HD' 디스크에 이 소프트웨어의 표준 설치를 실행하려면 설치를 클릭하십시오.
설치 위치 변경...
사용자화
뒤로 이동
설치


CSSCAN Application Installation 설치
CSSCAN Application Installation 설치 중
소개
대상 디스크 선택
설치 유형
설치
요약
4
'설치 프로그램'에서 'System Events'을(를) 제어하려고 합니다. 제어를 허용하면 'System Events'에 있는 문서 및 데이터에 접근이 허용되며 해당 앱에서 동작을 수행할 수 있게 됩니다.
허용 안 함
허용
뒤로 이동
계속

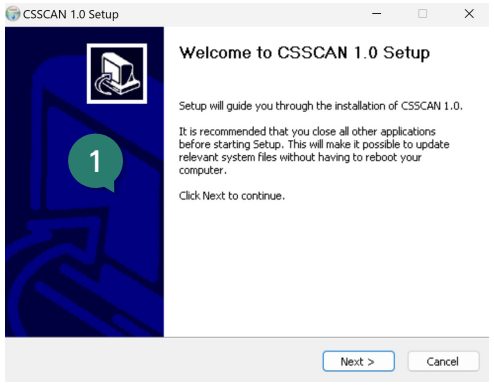
MAC Install

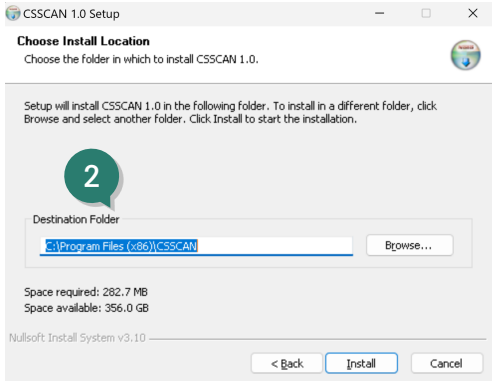

CSSCAN Application Installation 설치
CSSCAN Application Installation 설치 중
소개
대상 디스크 선택
설치 유형
설치
요약
5
Enter Admin Username:
wow
취소
확인
뒤로 이동
계속

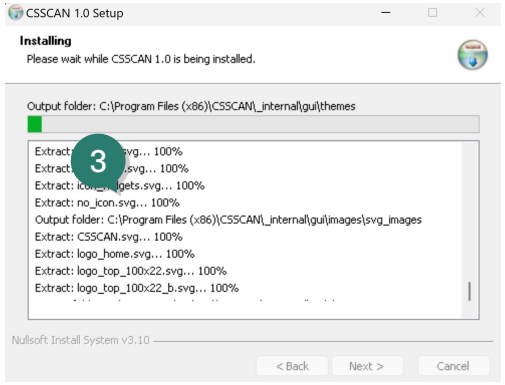

CSSCAN Application Installation 설치
설치가 성공적으로 완료되었습니다.
소개
대상 디스크 선택
설치 유형
설치
요약
7
성공적으로 설치되었습니다.
소프트웨어가 설치되었습니다.
뒤로 이동
닫기

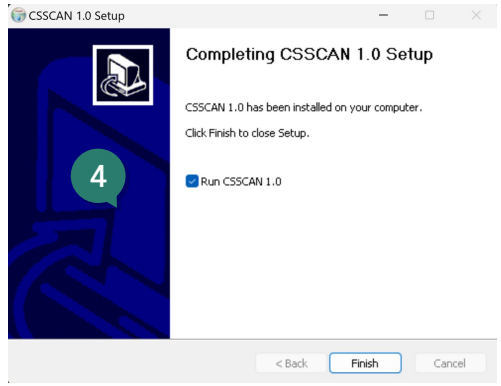

CSSCAN Application Installation 설치
CSSCAN Application Installation 설치 중
소개
대상 디스크 선택
설치 유형
설치
요약
6
Enter Admin Password:
취소
확인
뒤로 이동
계속

Windows Install





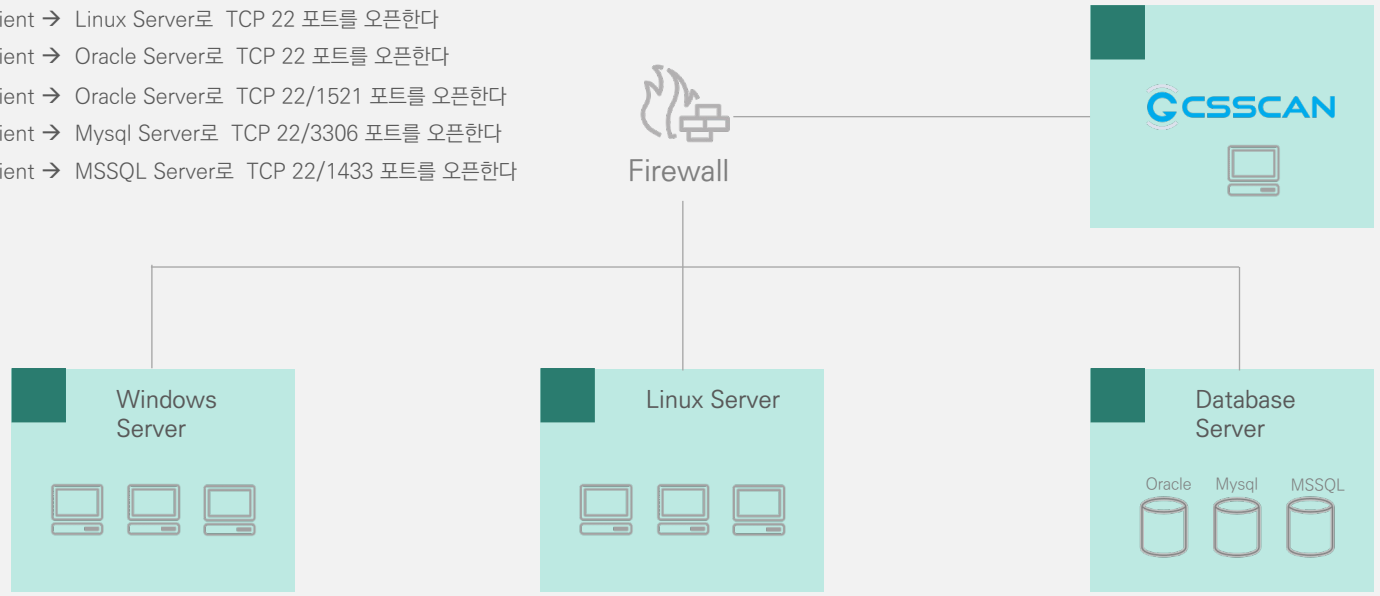




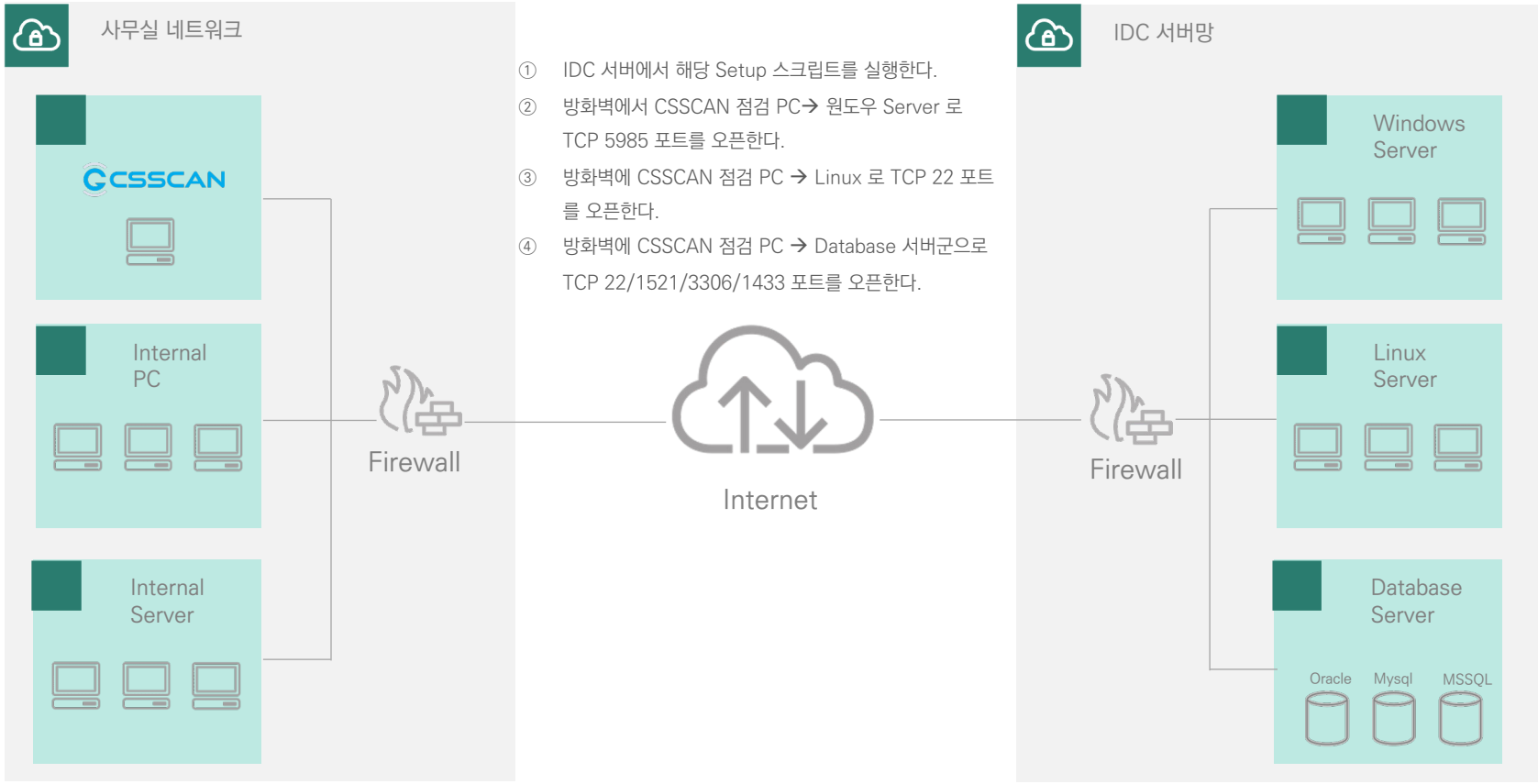
Broadcast 점검 구성

회사 네트워크(Broadcast network)

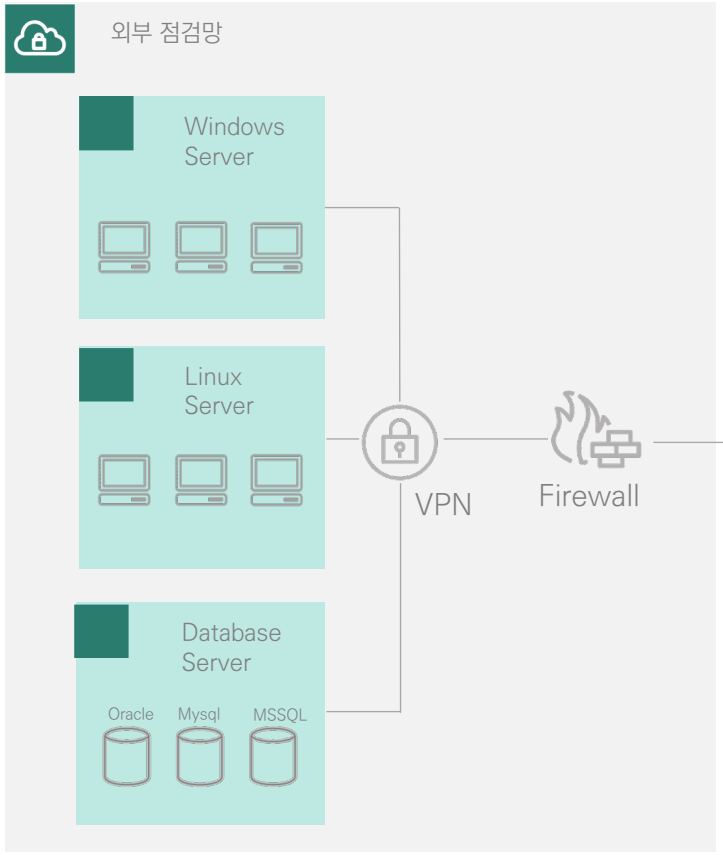
① CSSCAN Client → Windows Server 로 TCP 5985 포트를 오픈한다.
② CSSCAN Client → Linux Server로 TCP 22 포트를 오픈한다
③ CSSCAN Client → Oracle Server로 TCP 22 포트를 오픈한다
④ CSSCAN Client → Oracle Server로 TCP 22/1521 포트를 오픈한다
⑤ CSSCAN Client → Mysql Server로 TCP 22/3306 포트를 오픈한다
⑥ CSSCAN Client → MSSQL Server로 TCP 22/1433 포트를 오픈한다



IDC 서버망 점검 구성


사무실 네트워크
CSSCAN
Internal PC
Internal Server
Firewall
① IDC 서버에서 해당 Setup 스크립트를 실행한다.
② 방화벽에서 CSSCAN 점검 PC→ 원도우 Server 로 TCP 5985 포트를 오픈한다.
③ 방화벽에 CSSCAN 점검 PC → Linux 로 TCP 22 포트를 오픈한다.
④ 방화벽에 CSSCAN 점검 PC → Database 서버군으로 TCP 22/1521/3306/1433 포트를 오픈한다.
Internet
Firewall
IDC 서버망
Windows Server
Linux Server
Database Server
Oracle
Mysql
MSSQL

외부망 서버 점검 구성



① CSSCAN 점검 랩탑에서 외부 점검망으로 VPN 으로 접속한다.

② 외부 점검망 서버에서 해당 Setup 스크립트를 실행한다.

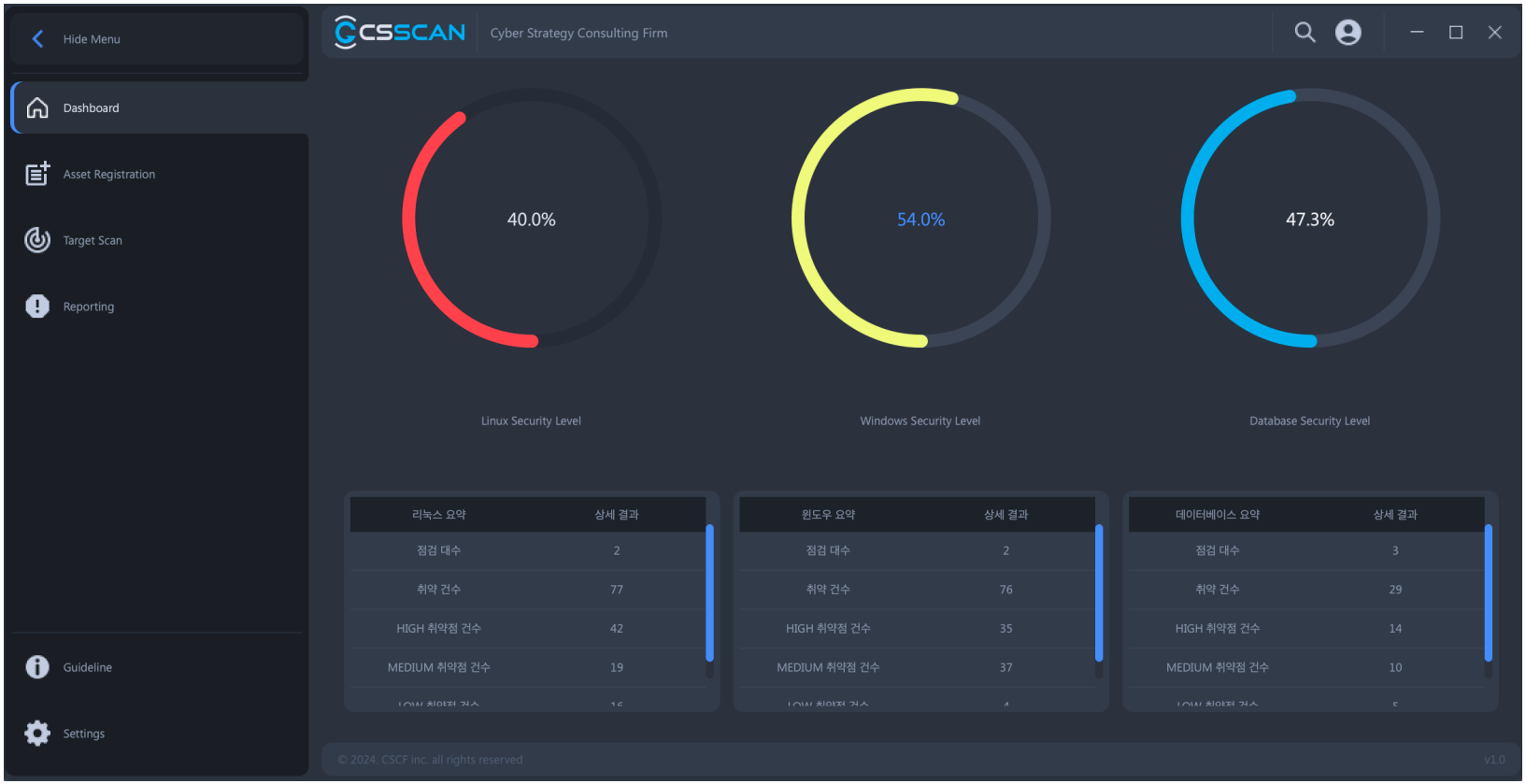
③ 외부 점검망 방화벽에서 CSSCAN 점검 랩탑 → 원도우 Server 로 TCP 5985 포트를 오픈한다.

④ 외부 점검망 방화벽에 CSSCAN 점검 랩탑 → Linux 로 TCP 22 포트를 오픈한다.

⑤ 외부 점검망 방화벽에 CSSCAN 점검 랩탑 → Database 서버군으로 TCP 22/1521/3306/1433 포트를 오픈한다.

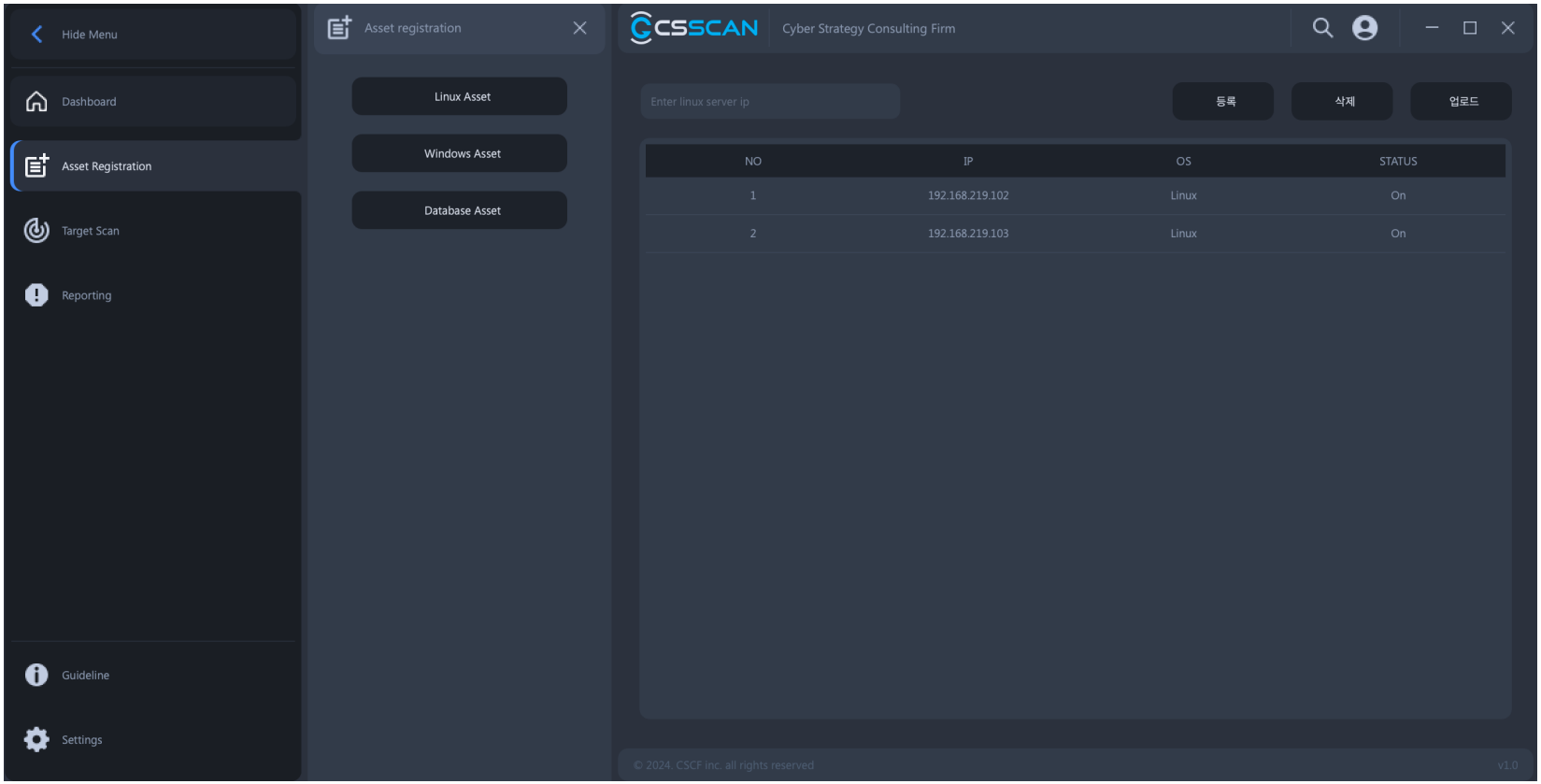
사용자 인터페이스 소개

Dashboard 화면



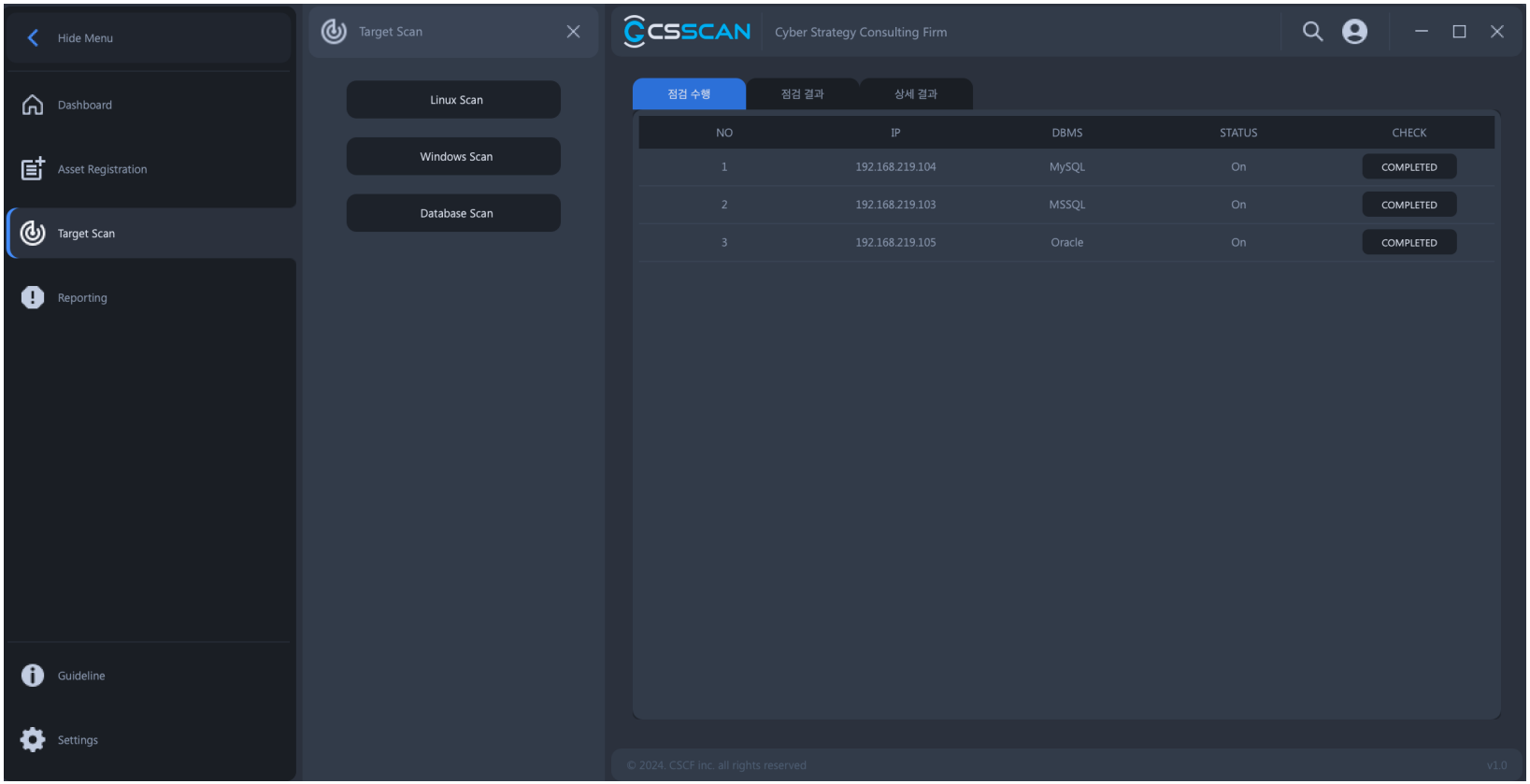
사용자 인터페이스 소개

점검 Asset 등록

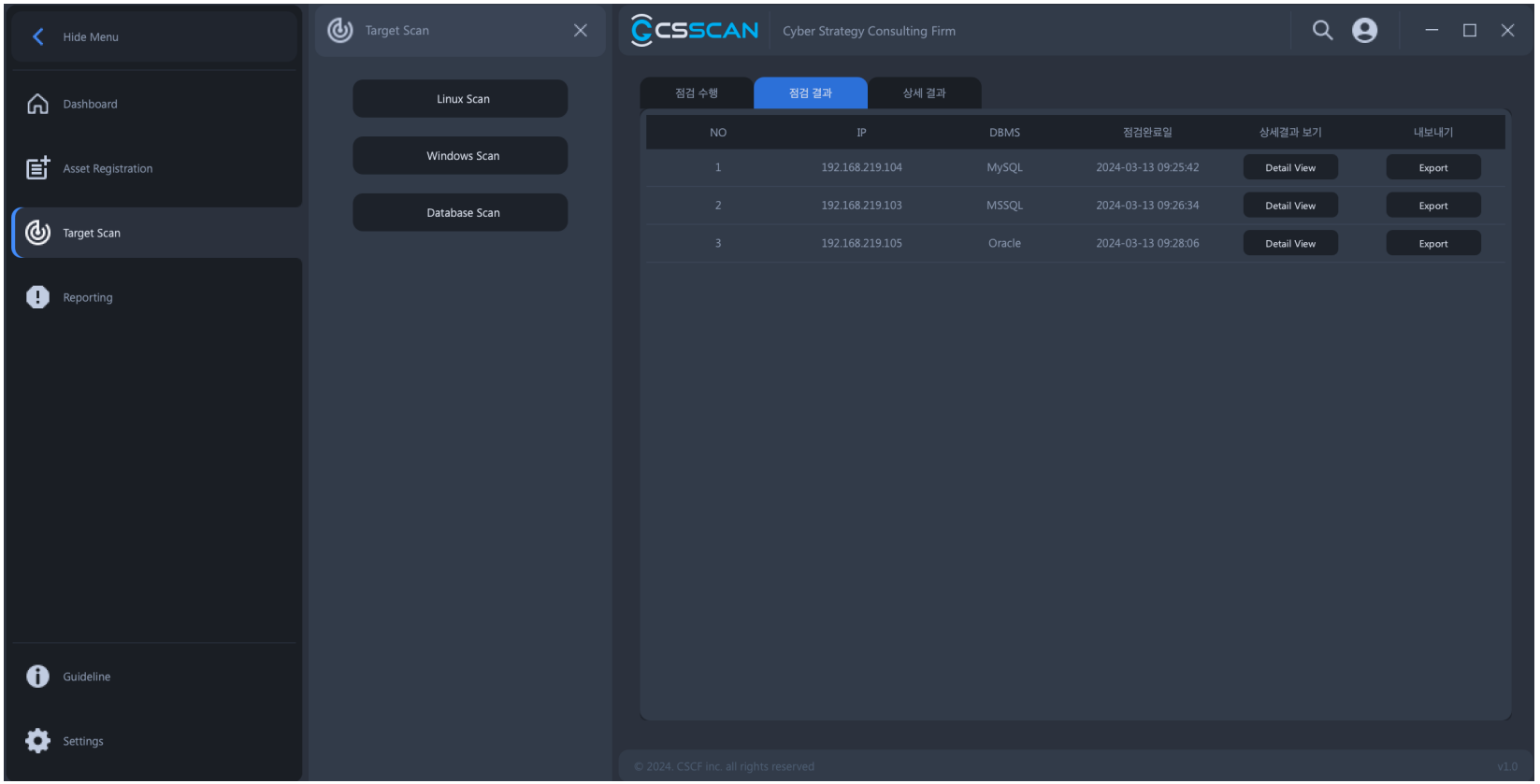


사용자 인터페이스 소개

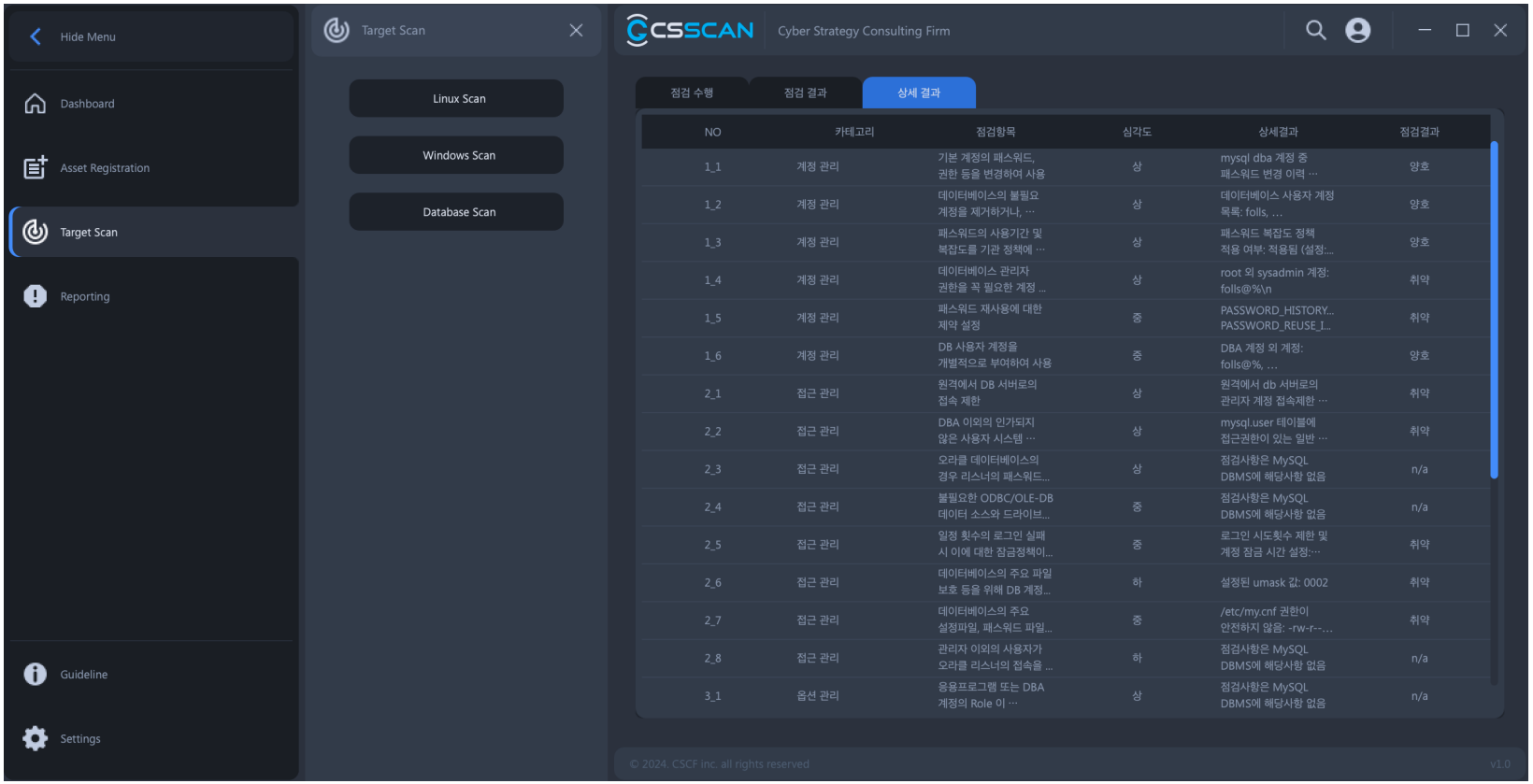
Target Scan – 점검 수행



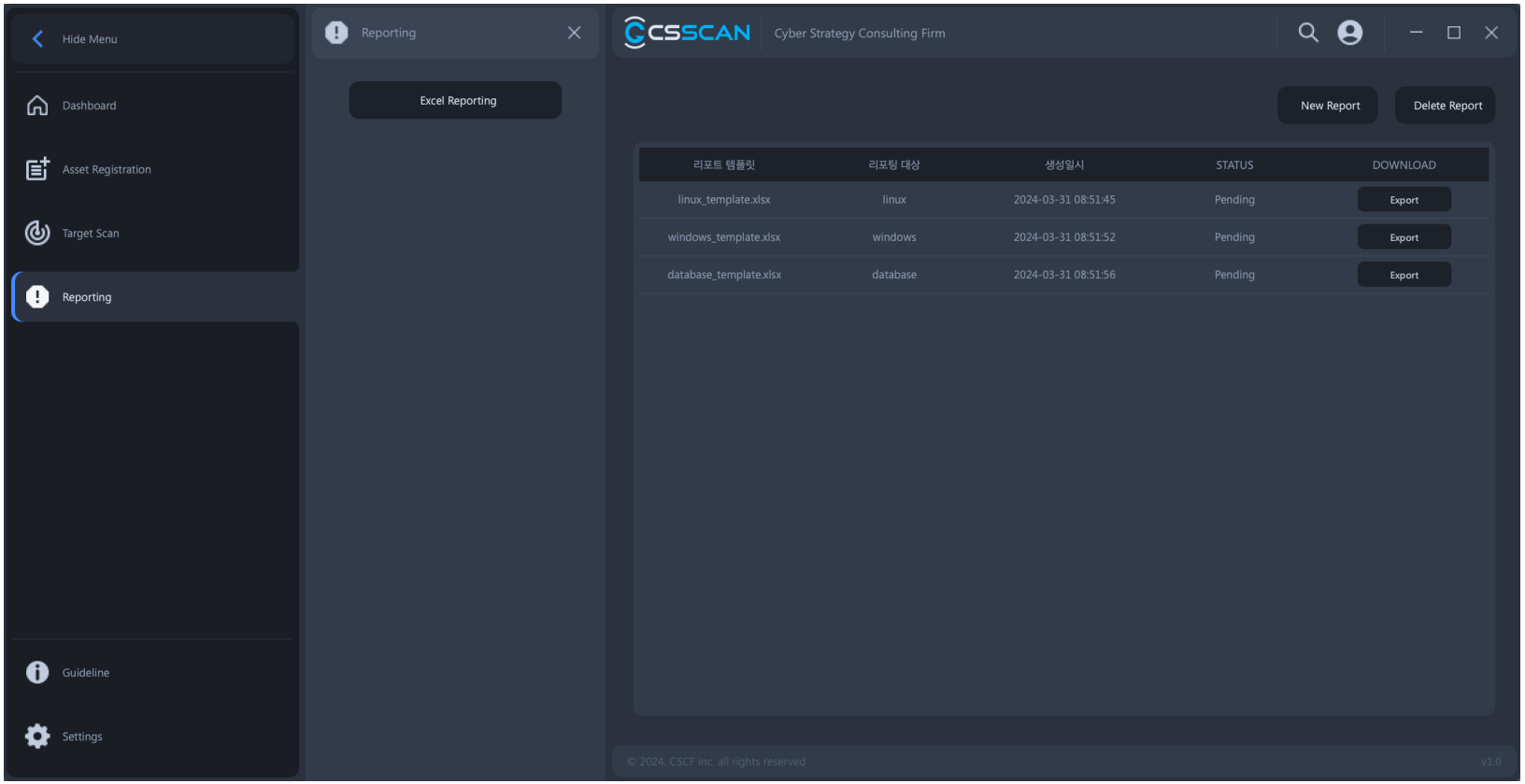
Target Scan – 점검 결과



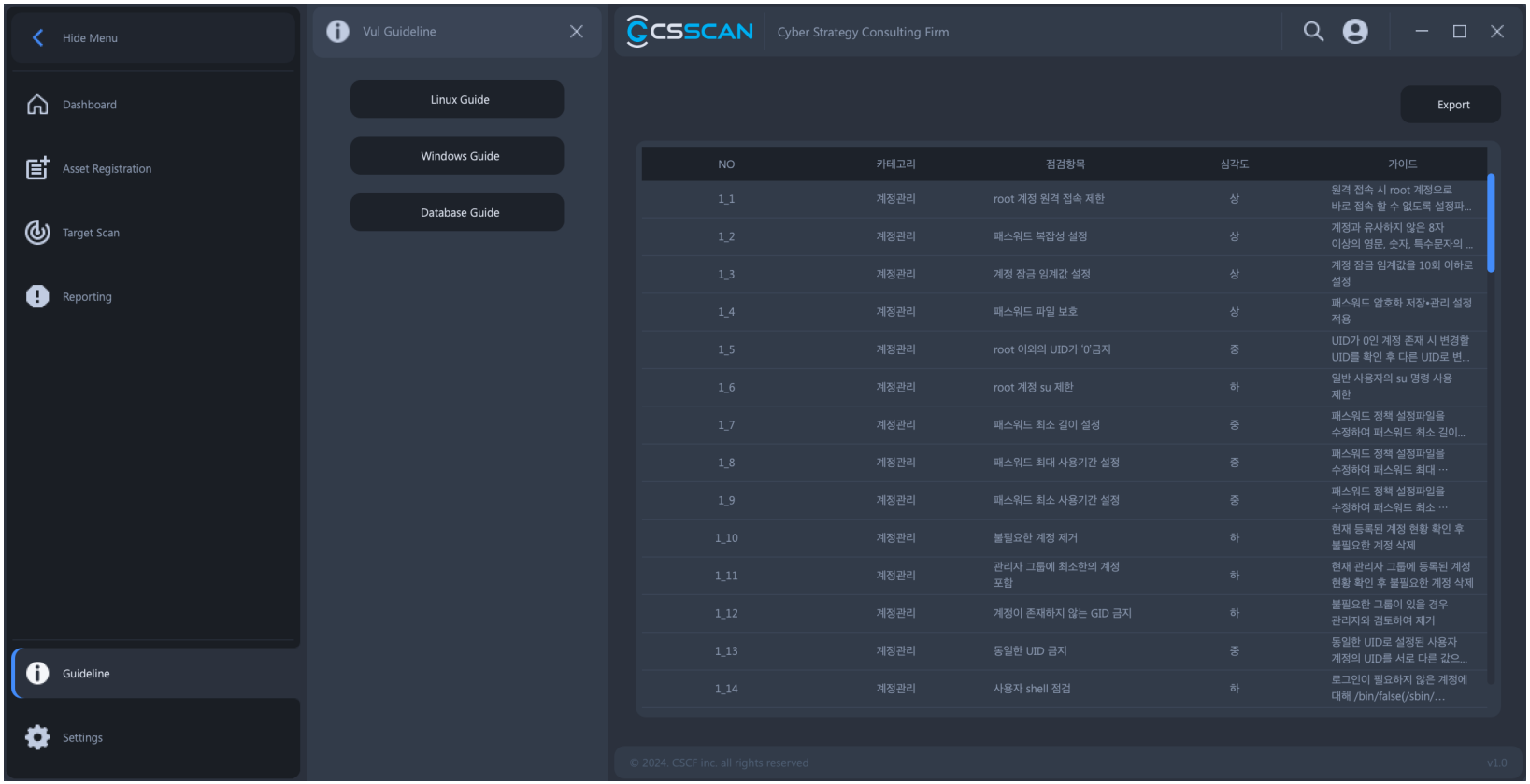
Target Scan – 상세 결과



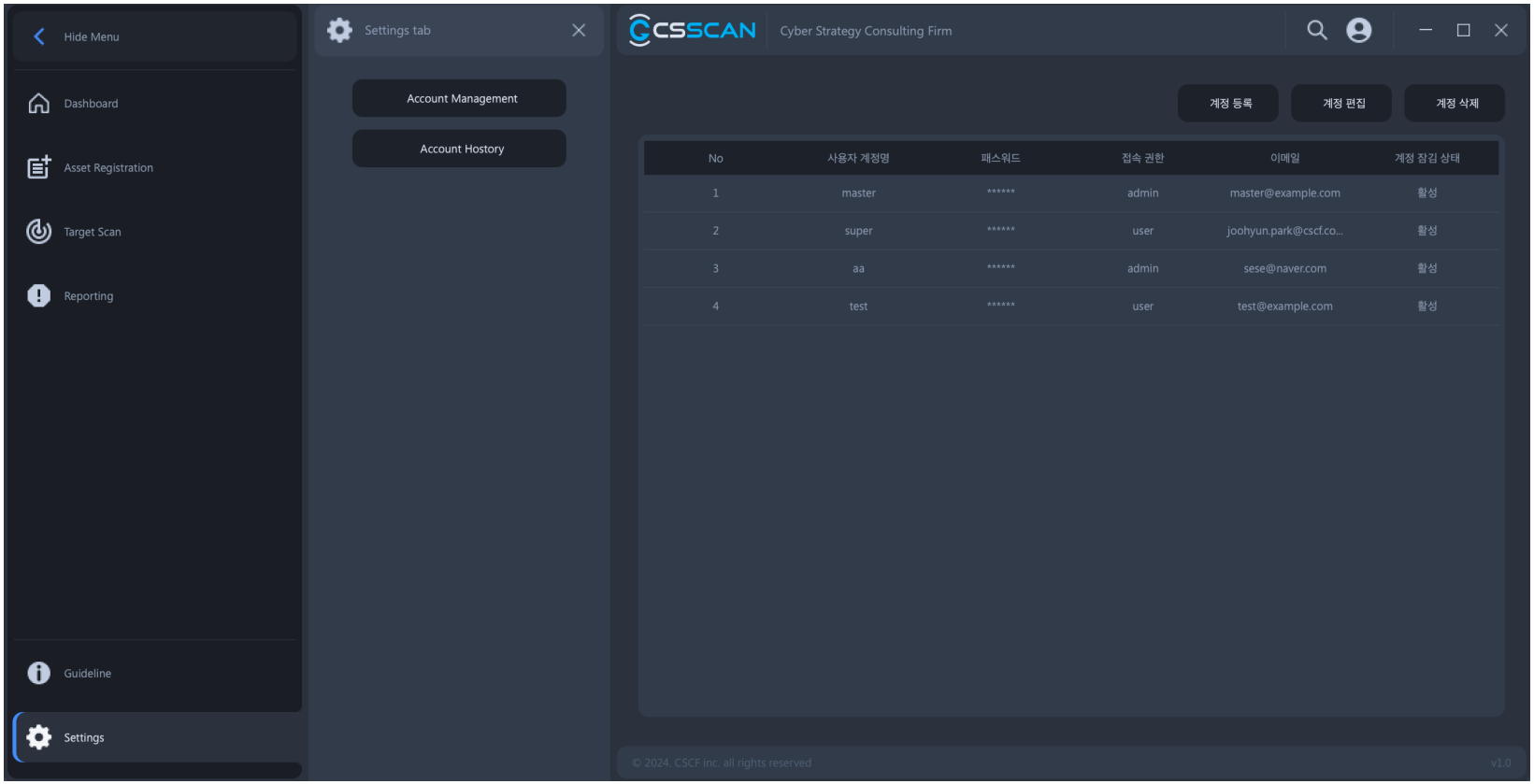
Reporting


Hide Menu
Dashboard
Asset Registration
Target Scan
Reporting
Guideline
Settings
Reporting
Excel Reporting
CSSCAN
Cyber Strategy Consulting Firm
New Report
Delete Report
리포트 템플릿
리포팅 대상
생성일시
STATUS
DOWNLOAD
linux_template.xlsx
linux
2024-03-31 08:51:45
Pending
Export
windows_template.xlsx
windows
2024-03-31 08:51:52
Pending
Export
database_template.xlsx
database
2024-03-31 08:51:56
Pending
Export
© 2024. CSCF inc. all rights reserved
v1.0

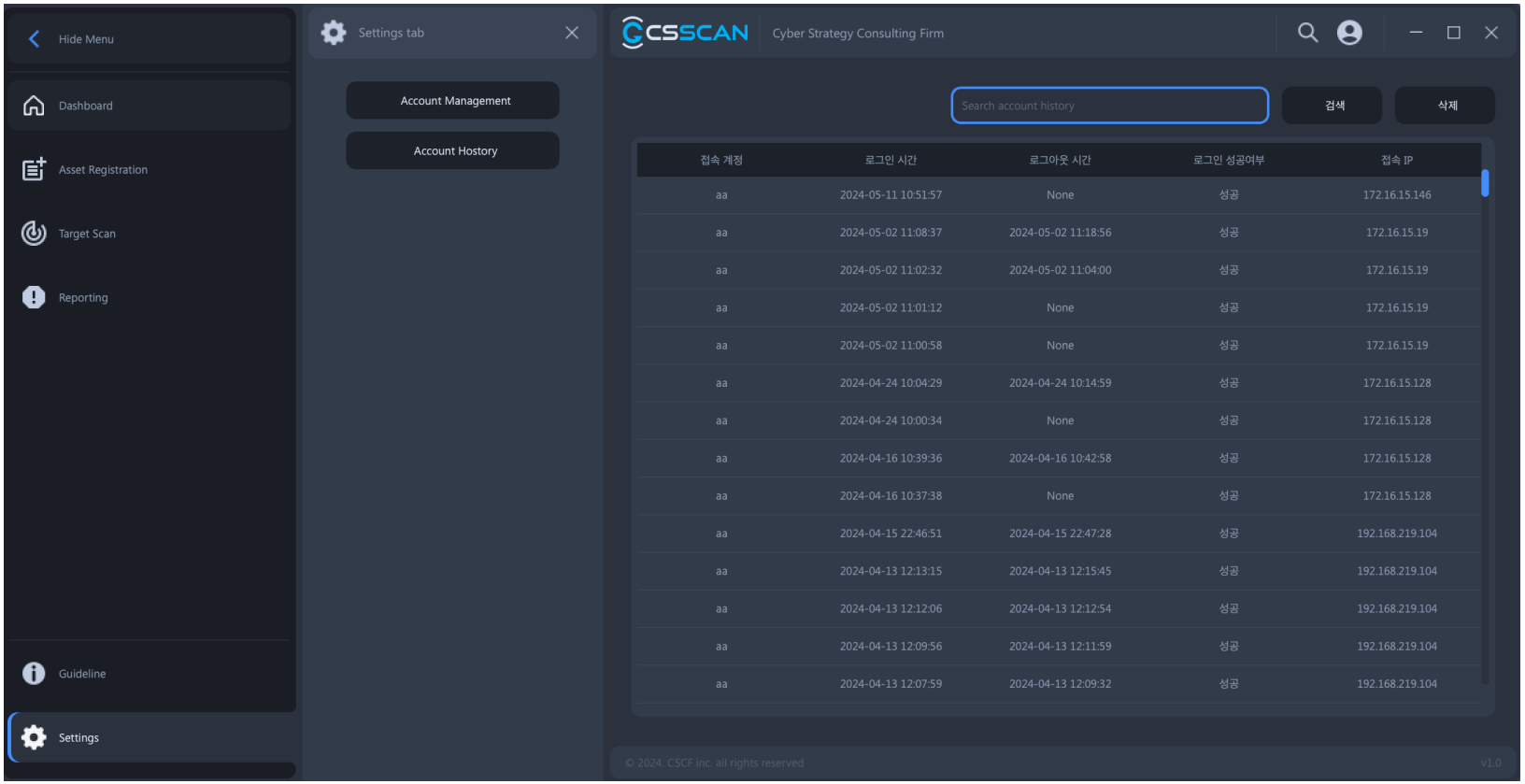
Guideline


Hide Menu
Dashboard
Asset Registration
Target Scan
Reporting
Guideline
Settings
Vul Guideline
Linux Guide
Windows Guide
Database Guide
CSSCAN
Cyber Strategy Consulting Firm
Export
NO 카테고리 점검항목 심각도 가이드
1_1 계정관리 root 계정 원격 접속 제한 상 원격 접속 시 root 계정으로 바로 접속 할 수 없도록 설정파...
1_2 계정관리 패스워드 복잡성 설정 상 계정과 유사하지 않은 8자 이상의 영문, 숫자, 특수문자의 ...
1_3 계정관리 계정 잠금 임계값 설정 상 계정 잠금 임계값을 10회 이하로 설정
1_4 계정관리 패스워드 파일 보호 상 패스워드 암호화 저장•관리 설정 적용
1_5 계정관리 root 이외의 UID가 '0'금지 중 UID가 0인 계정 존재 시 변경할 UID를 확인 후 다른 UID로 변...
1_6 계정관리 root 계정 su 제한 하 일반 사용자의 su 명령 사용 제한
1_7 계정관리 패스워드 최소 길이 설정 중 패스워드 정책 설정파일을 수정하여 패스워드 최소 길이...
1_8 계정관리 패스워드 최대 사용기간 설정 중 패스워드 정책 설정파일을 수정하여 패스워드 최대 ···
1_9 계정관리 패스워드 최소 사용기간 설정 중 패스워드 정책 설정파일을 수정하여 패스워드 최소 ···
1_10 계정관리 불필요한 계정 제거 하 현재 등록된 계정 현황 확인 후 불필요한 계정 삭제
1_11 계정관리 관리자 그룹에 최소한의 계정 포함 하 현재 관리자 그룹에 등록된 계정 현황 확인 후 불필요한 계정 삭제
1_12 계정관리 계정이 존재하지 않는 GID 금지 하 불필요한 그룹이 있을 경우 관리자와 검토하여 제거
1_13 계정관리 동일한 UID 금지 중 동일한 UID로 설정된 사용자 계정의 UID를 서로 다른 값으...
1_14 계정관리 사용자 shell 점검 하 로그인이 필요하지 않은 계정에 대해 /bin/false(/sbin/...
© 2024. CSCF inc. all rights reserved
v1.0

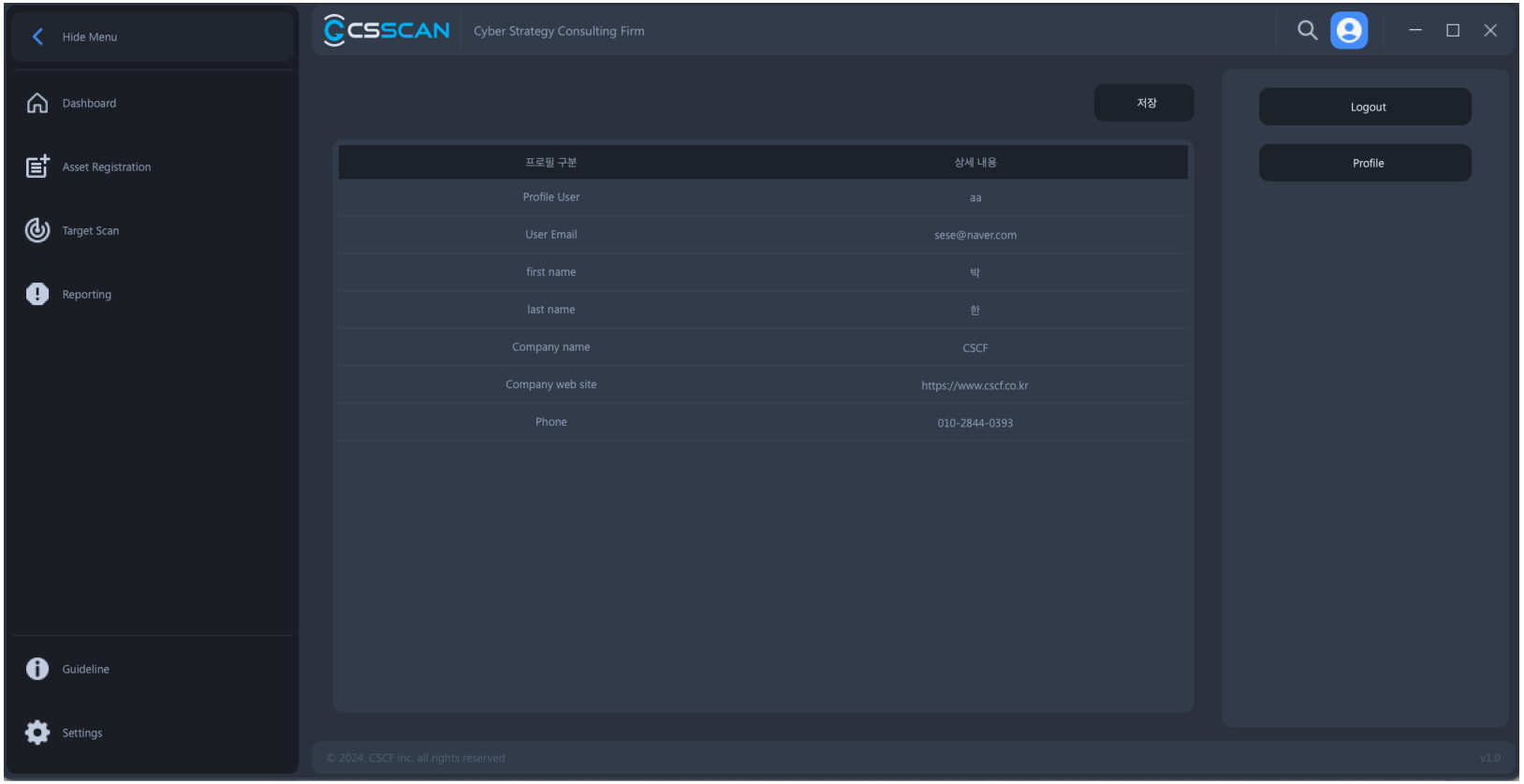
설정 – 계정관리


Hide Menu
Dashboard
Asset Registration
Target Scan
Reporting
Guideline
Settings
Settings tab
Account Management
Account Hostory
CSSCAN
Cyber Strategy Consulting Firm
계정 등록
계정 편집
계정 삭제
No
사용자 계정명
패스워드
접속 권한
이메일
계정 잠김 상태
1 master ****** admin master@example.com 활성
2 super ****** user joohyun.park@cscf.co... 활성
3 aa ****** admin sese@naver.com 활성
4 test ****** user test@example.com 활성
© 2024. CSCF inc. all rights reserved
v1.0

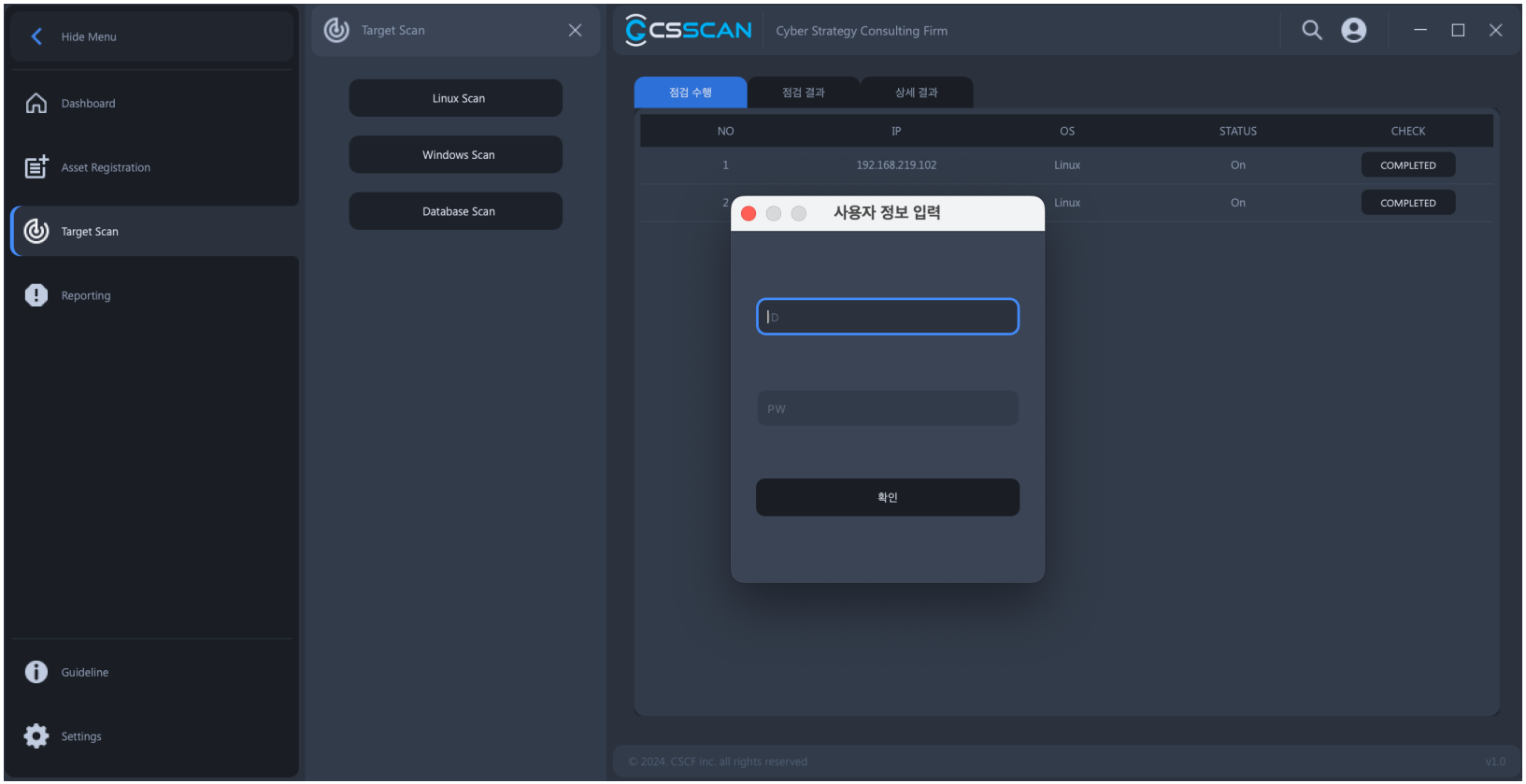
설정 – History 관리



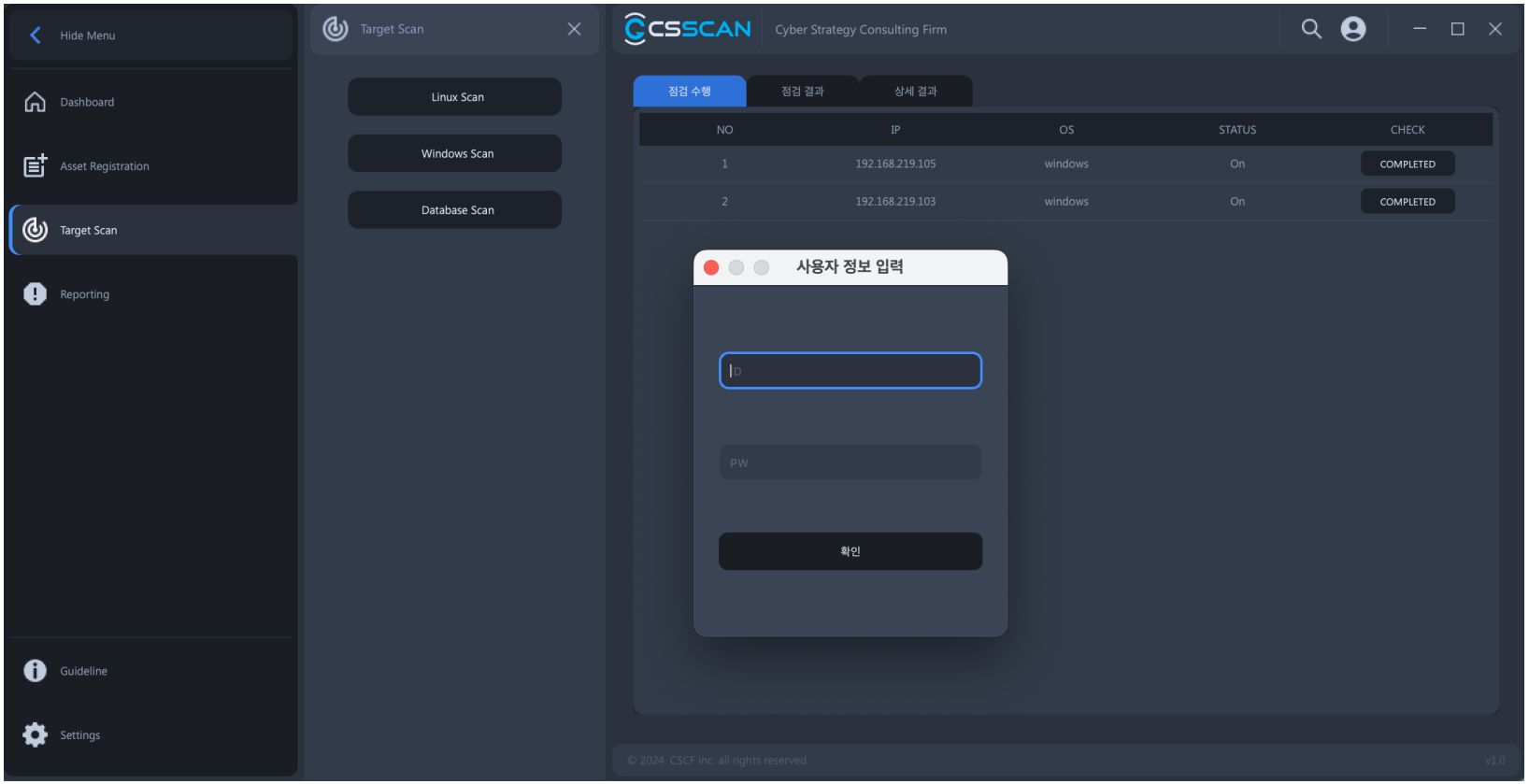
로그아웃 및 프로필 설정


Hide Menu
Dashboard
Asset Registration
Target Scan
Reporting
Guideline
Settings
CSSCAN
Cyber Strategy Consulting Firm
저장
Logout
Profile
프로필 구분
상세 내용
Profile User
aa
User Email
sese@naver.com
first name
박
last name
한
Company name
CSCF
Company web site
https://www.cscf.co.kr
Phone
010-2844-0393
© 2024. CSCF inc. all rights reserved
v1.0

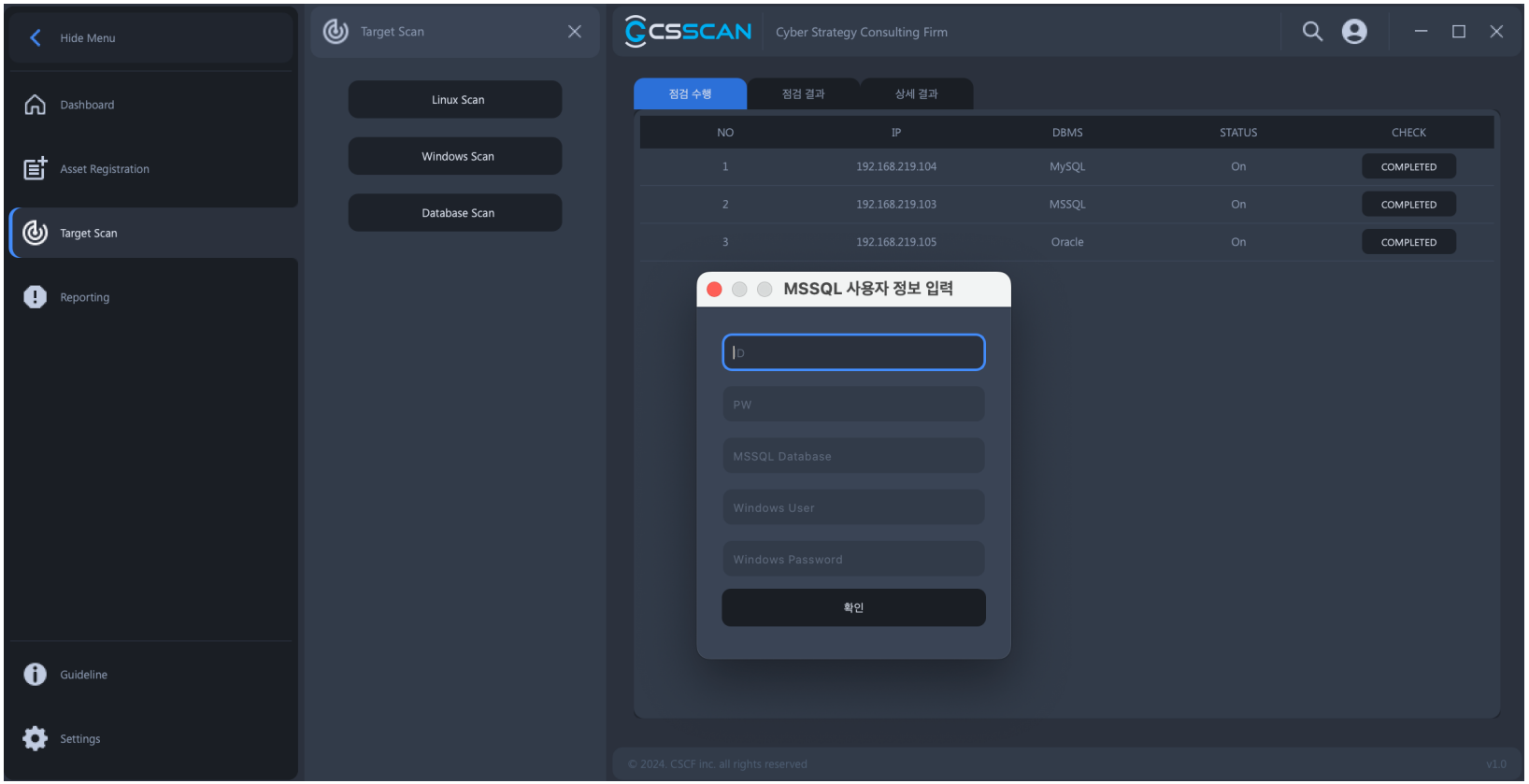
취약점 점검 수행 – Linux



취약점 점검 수행 – Windows

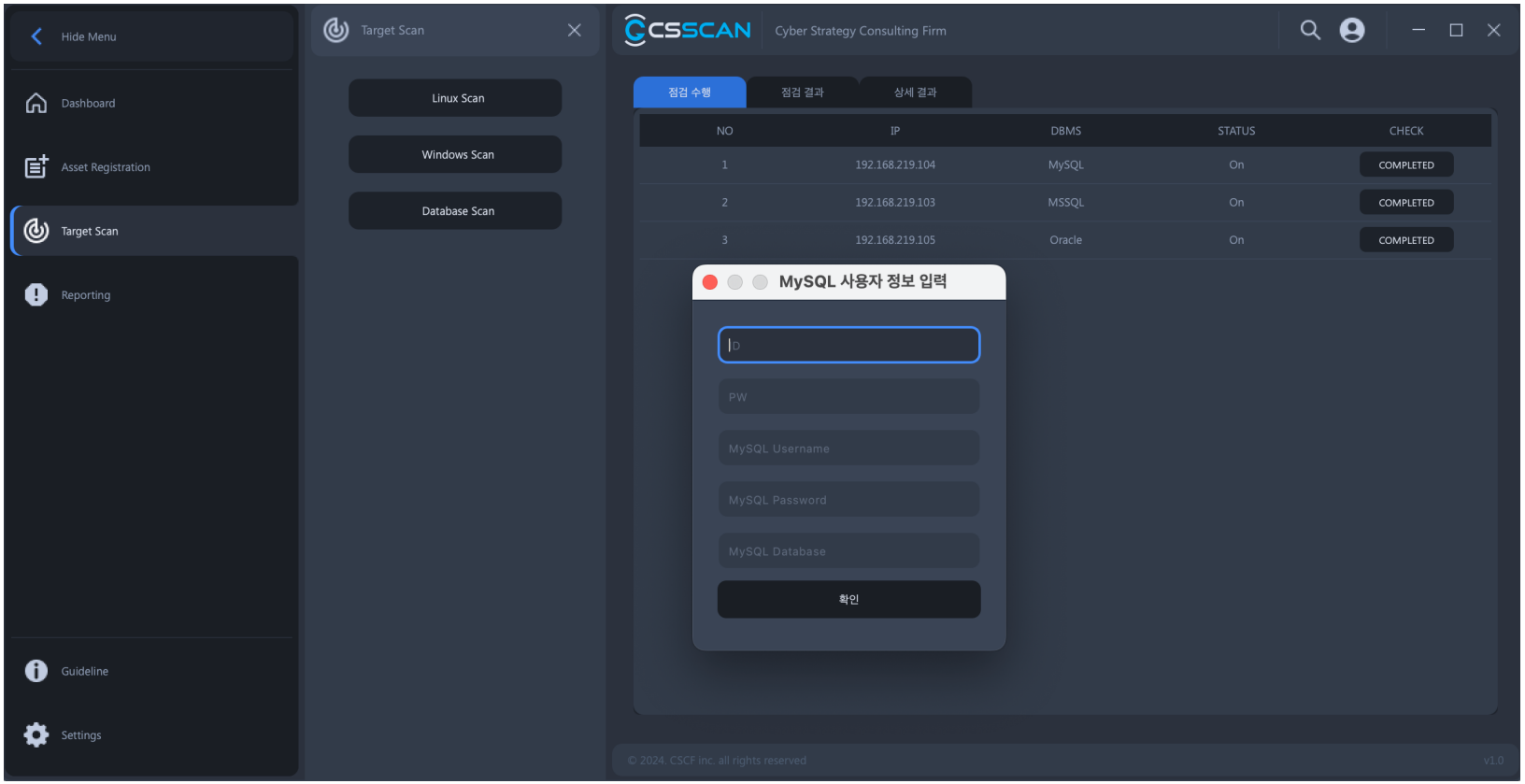


취약점 점검 수행 – MSSQL



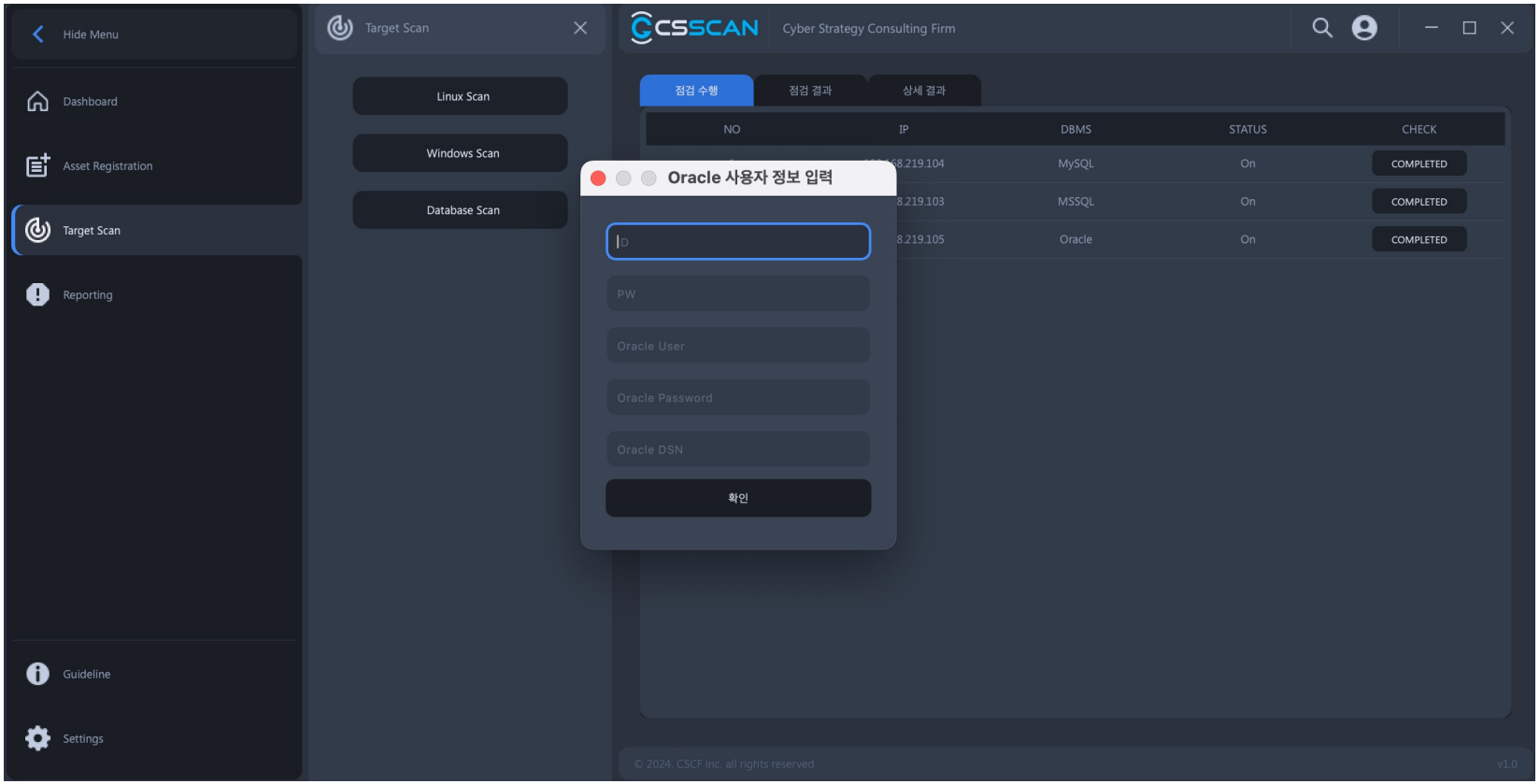
* MSSQL Database 에는 일반적으로 “master” 를 입력하거나 점검하고자 하는 DB를 입력한다.

취약점 점검 수행 – Mysql



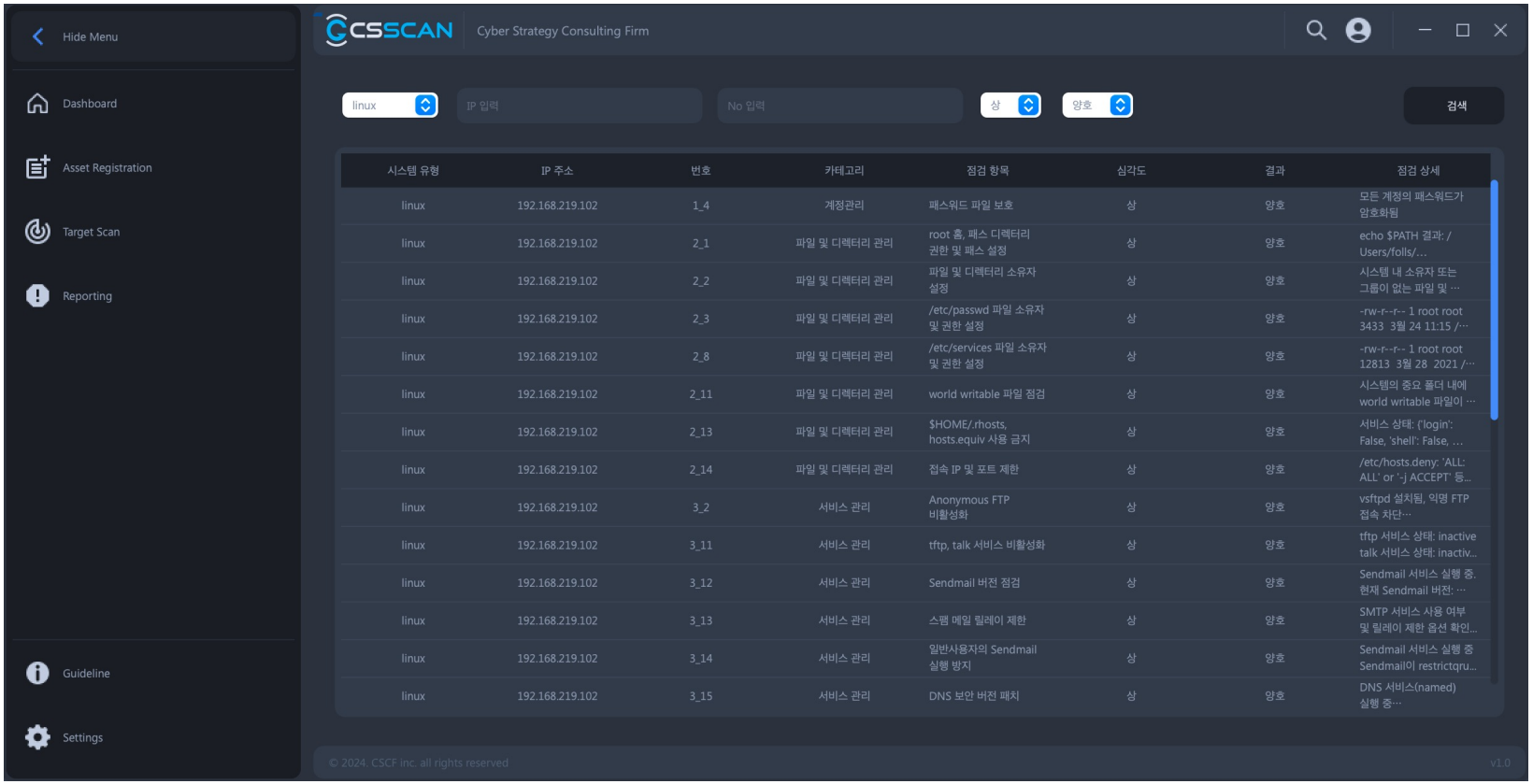
* Mysql Database 에는 일반적으로 “mysql” 를 입력하거나 점검하고자 하는 DB를 입력한다.

취약점 점검 수행 – Oracle



* Oracle Database 에는 “IP:1521/instance name” 를 입력하거나 점검하고자 하는 DB를 입력한다. 예) Oracle DSN = 192.168.219.107:1521/XE

취약점 검색


Hide Menu
Dashboard
Asset Registration
Target Scan
Reporting
Guideline
Settings
CSSCAN
Cyber Strategy Consulting Firm
linux
IP 입력
No 입력
상
양호
검색
시스템 유형 | IP 주소 | 번호 | 카테고리 | 점검 항목 | 심각도 | 결과 | 점검 상세
linux | 192.168.219.102 | 1_4 | 계정관리 | 패스워드 파일 보호 | 상 | 양호 | 모든 계정의 패스워드가 암호화됨
linux | 192.168.219.102 | 2_1 | 파일 및 디렉터리 관리 | root 홈, 패스 디렉터리 권한 및 패스 설정 | 상 | 양호 | echo $PATH 결과: /Users/folls/…
linux | 192.168.219.102 | 2_2 | 파일 및 디렉터리 관리 | 파일 및 디렉터리 소유자 설정 | 상 | 양호 | 시스템 내 소유자 또는 그룹이 없는 파일 및 …
linux | 192.168.219.102 | 2_3 | 파일 및 디렉터리 관리 | /etc/passwd 파일 소유자 및 권한 설정 | 상 | 양호 | -rw-r--r-- 1 root root 3433 3월 24 11:15 /…
linux | 192.168.219.102 | 2_8 | 파일 및 디렉터리 관리 | /etc/services 파일 소유자 및 권한 설정 | 상 | 양호 | -rw-r--r-- 1 root root 12813 3월 28 2021 /…
linux | 192.168.219.102 | 2_11 | 파일 및 디렉터리 관리 | world writable 파일 점검 | 상 | 양호 | 시스템의 중요 폴더 내에 world writable 파일이 …
linux | 192.168.219.102 | 2_13 | 파일 및 디렉터리 관리 | $HOME/.rhosts, hosts.equiv 사용 금지 | 상 | 양호 | 서비스 상태: {'login': False, 'shell': False, …
linux | 192.168.219.102 | 2_14 | 파일 및 디렉터리 관리 | 접속 IP 및 포트 제한 | 상 | 양호 | /etc/hosts.deny: 'ALL: ALL' or '-j ACCEPT' 등…
linux | 192.168.219.102 | 3_2 | 서비스 관리 | Anonymous FTP 비활성화 | 상 | 양호 | vsftpd 설치됨, 익명 FTP 접속 차단…
linux | 192.168.219.102 | 3_11 | 서비스 관리 | tftp, talk 서비스 비활성화 | 상 | 양호 | tftp 서비스 상태: inactive talk 서비스 상태: inactiv…
linux | 192.168.219.102 | 3_12 | 서비스 관리 | Sendmail 버전 점검 | 상 | 양호 | Sendmail 서비스 실행 중. 현재 Sendmail 버전: …
linux | 192.168.219.102 | 3_13 | 서비스 관리 | 스팸 메일 릴레이 제한 | 상 | 양호 | SMTP 서비스 사용 여부 및 릴레이 제한 옵션 확인…
linux | 192.168.219.102 | 3_14 | 서비스 관리 | 일반사용자의 Sendmail 실행 방지 | 상 | 양호 | Sendmail 서비스 실행 중 Sendmail이 restrictqru…
linux | 192.168.219.102 | 3_15 | 서비스 관리 | DNS 보안 버전 패치 | 상 | 양호 | DNS 서비스(named) 실행 중…
© 2024. CSCF inc. all rights reserved
v1.0

상세 보고서

192.168.219.102

NO	CATEGORY	CHECKLIST	SEVERITY	CHECK DETAIL	RESULT
1_1	계정관리	root 계정 원격 접속 제한	상	root 원격접속 제한:telnet 서비스 사용 안 함 PermitRootLogin 설정: yes	취약
1_2	계정관리	패스워드 복잡성 설정	상	/etc/security/pwquality.conf: minlen 설정값 없음 /etc/pam.d/common-password: passwordrequisitepam_pwquality.so retry=3 /etc/pam.d/system-auth: pam_pwquality.so 설정값 없음 /etc/pam.d/password-auth: pam_pwquality.so 설정값 없음	취약
1_3	계정관리	계정 잠금 임계값 설정	상	/etc/pam.d/system-auth: 설정이 발견되지 않음 /etc/pam.d/password-auth: 설정이 발견되지 않음 계정 잠금 설정이 발견되지 않음	취약
1_4	계정관리	패스워드 파일 보호	상	모든 계정의 패스워드가 암호화됨	양호
1_5	계정관리	root 이외의 UID가 '0'금지	중	UID 값이 0인 계정: root	양호
1_6	계정관리	root 계정 su 제한	하	su 명령어 제한 설정이 발견되지 않음	취약
1_7	계정관리	패스워드 최소 길이 설정	중	/etc/login.defs에 PASS_MIN_LEN 설정되지 않음 (기본값: 6)	취약
1_8	계정관리	패스워드 최대 사용기간 설정	중	/etc/login.defs: PASS_MAX_DAYS 99999	취약
1_9	계정관리	패스워드 최소 사용기간 설정	중	패스워드 최소 사용기간 설정값: 0일	취약
1_10	계정관리	불필요한 계정 제거	하	발견된 OS 기본 계정: lp, uucp	취약
1_11	계정관리	관리자 그룹에 최소한의 계정 포함	하	root 그룹에 root 계정 외 추가된 계정 없음	양호
1_12	계정관리	계정이 존재하지 않는 GID 금지	하	계정이 존재하지 않는 그룹명: staff, floppy, sambashare, shadow, systemd-journal, tty, cdrom, dip, src, netdev, lxd, ssl-cert, render, kvm, scanner, bluetooth, utmp, users, sudo, disk, sgx, fax, adm, tape, crontab, pulse-access, voice, sasl, dialout, kmem, video, input, operator, _ssh 계정이 존재하지 않는 그룹명 사용여부 판단 필요	취약
1_13	계정관리	동일한 UID 금지	중	동일한 UID로 설정된 사용자 계정이 존재하지 않음	양호
1_14	계정관리	사용자 shell 점검	하	로그인 쉘이 /bin/false 또는 /usr/sbin/nologin으로 설정되지 않은 계정: games 해당 계정에 대해 /bin/false 또는 /usr/sbin/nologin 설정 필요	취약
1_15	계정관리	Session Timeout 설정	하	Session Timeout 설정값이 없음	취약
2_1	파일 및 디렉터리 관리	root 홈, 패스 디렉터리 권한 및 패스 설정	상	echo $PATH 결과: /Users/folls/instantclient:/usr/local/bin:/Library/Frameworks/Python.framework/Versions/3.12/bin:/usr/local/bin:/System/Cryptexes/App/usr/bin:/usr/bin:/bin:/usr/sbin:/sbin:/var/run/com.apple.security.cryptexd/codex.system/bootstrap/usr/local/bin:/var/run/com.apple.security.cryptexd/codex.system/bootstrap/usr/bin:/var/run/com.apple.security.cryptexd/codex.system/bootstrap/usr/appleinternal/bin:/Library/Apple/usr/bin:/Applications/VMware Fusion.app/Contents/Public:/usr/local/go/bin:/Users/folls/instantclient:/Library/Frameworks/Python.framework/Versions/3.12/bin	양호

상세 보고서

고객사(주)

DATABASE 취약점진단 보고서

Version 1.0
2024-05-12

영역별 보안수준

NO	점검 영역	상 양호 점수	중 양호 점수	하 양호 점수	만점	N/A 점수	보안 수준
1	계정 관리	18	6	0	64	0	38%
2	접근 관리	3	6	0	68	15	17%
3	옵션 관리	6	2	0	48	18	27%
4	패치 관리	12	6	0	32	0	56%
5	로그 관리	0	0	2	4	1	67%

		CHECKLIST	SEVERITY	192.168.219.104	192.168.219.103	192.168.219.105
		, 권한 등을 변경하여 사용	상	양호	양호	양호
		요 계정을 제거하거나, 잠금설정 후 사용	상	양호	취약	취약
		및 복잡도를 기관 정책에 맞도록 설정	상	양호	취약	양호
		권한을 꼭 필요한 계정 및 그룹에 허용	상	취약	취약	취약
1_5	계정 관리	패스워드 재사용에 대한 제약 설정	중	취약	취약	취약
1_6	계정 관리	DB 사용자 계정을 개별적으로 부여하여 사용	중	양호	양호	양호
2_1	접근 관리	원격에서 DB 서버로의 접속 제한	상	취약	취약	양호
2_2	접근 관리	DBA 이외의 인가되지 않은 사용자 시스템 테이블에 접근할 수 없도록 설정	상	취약	취약	취약
2_3	접근 관리	오라클 데이터베이스의 경우 리스너의 패스워드를 설정하여 사용	상	n/a	n/a	취약
2_4	접근 관리	불필요한 ODBC/OLE-DB 데이터 소스와 드라이브를 제거하여 사용	중	n/a	양호	n/a
2_5	접근 관리	일정 횟수의 로그인 실패 시 이에 대한 잠금정책이 설정	중	취약	n/a	양호
2_6	접근 관리	데이터베이스의 주요 파일 보호 등을 위해 DB 계정의 umask를 022 이상으로 설정하여 사용	하	취약	n/a	취약
2_7	접근 관리	데이터베이스의 주요 설정파일, 패스워드 파일 등과 같은 주요 파일들의 접근 권한이 적절하게 설정	중	취약	양호	취약
2_8	접근 관리	관리자 이외의 사용자가 오라클 리스너의 접속을 통해 리스너 로그 및 trace 파일에 대한 변경 제한	하	n/a	n/a	취약
3_1	옵션 관리	응용프로그램 또는 DBA 계정의 Role 이 Public으로 설정되지 않도록 조정	상	n/a	양호	양호
3_2	옵션 관리	OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES를 FALSE로 설정	상	n/a	n/a	n/a
3_3	옵션 관리	패스워드 확인함수가 설정되어 적용	중	n/a	취약	취약
3_4	옵션 관리	인가되지 않은 Object Owner의 제한	하	n/a	n/a	취약
3_5	옵션 관리	인가되지 않은 GRANT OPTION 사용 제한	중	취약	양호	취약
3_6	옵션 관리	데이터베이스의 자원 제한 기능을 TRUE로 설정	하	n/a	n/a	취약
4_1	패치 관리	데이터베이스에 대해 최신 보안패치와 밴더 권고사항을 모두 적용	상	양호	양호	양호
4_2	패치 관리	데이터베이스의 접근, 변경, 삭제 등의 감사기록이 기관의 감사기록 정책에 적합하도록 설정	상	취약	취약	양호
4_3	패치 관리	보안에 취약하지 않은 버전의 데이터베이스를 사용	중	양호	양호	양호
5_1	로그 관리	Audit Table은 데이터베이스 관리자 계정에 접근하도록 제한	하	n/a	양호	양호
SECURITY LEVEL				43.2%	47.6%	51.0%

UI 설정

다양한 UI 설정 지원

```
{
    "app_name": "https://www.cscf.co.kr",
    "version" : "v1.0",
    "copyright" : "© 2024. CSCF inc. all rights reserved",
    "year" : 2024,
    "theme_name" : "default",
    "custom_title_bar": true,
    "startup_size": [
        1300,
        700
    ],
    "minimum_size": [
        960,
        540
    ],
    "lef_menu_size" : {
        "minimum" : 50,
        "maximum" : 240
    },
    "left_menu_content_margins" : 0,
    "left_column_size" : {
        "minimum" : 0,
        "maximum" : 240
    },
    "right_column_size" : {
        "minimum" : 0,
        "maximum" : 240
    },
    "time_animation" : 500,
    "font" : {
        "family" : "Segoe UI",
        "title_size" : 10,
        "text_size" : 9
    }
}
```

- UI 텍스트 셋팅
- 테마 셋팅

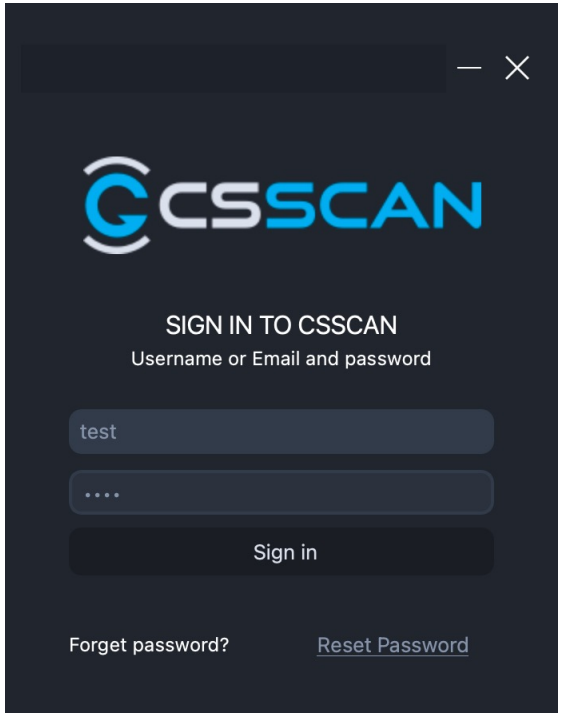
- 다양 UI 사이즈 셋팅
- 타임 애니메이션 값 설정

- UI 폰트 설정

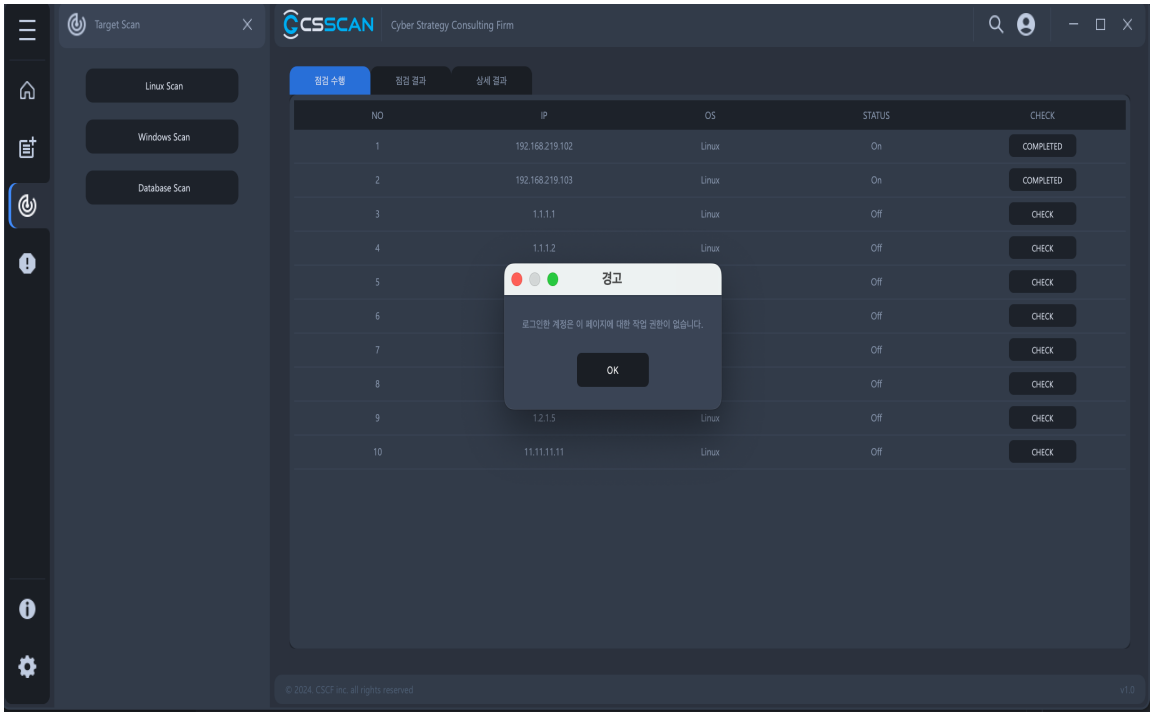
사용자 권한 분리

일반 사용자 권한 분리

일반 사용자 계정으로 로그인



일반 사용자 계정으로 로그인 시 Admin user 사용 기능을 제한됨



* 일반 사용자 계정으로도 상세 보고서는 export 기능을 사용할 수 있으며 이로 인해 해당 서버 담당자가 담당 서버의 취약점을 확인할 수 있도록 개발됨

감사합니다.

FOLLOW US ON:

https://www.cscf.co.kr

partner@cscf.co.kr

010-2844-0393

CSCF CYBER STRATEGY CONSULTING FIRM