



“ 사이버 보안의 올바른 방향을 제시합니다.”

# CCSPC 사용자 매뉴얼



# CONTENTS

“사이버 보안의 올바른 방향을 제시합니다.”

- 1. 소개
- 2. 시작하기
- 3. CSPC 구성
- 4. 실행 및 사용
- 5. 고급 기능

“NON-AGENT 방식의  
다중 플랫폼을 지원하는 최적의 거버닝 솔루션”

CSPC는 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 CSPC를 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.

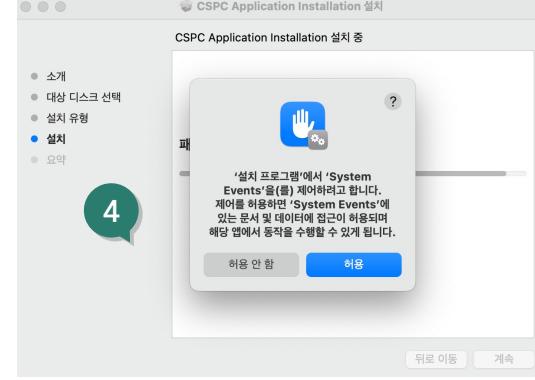
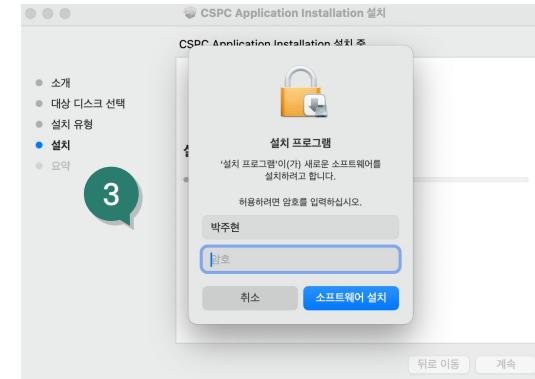
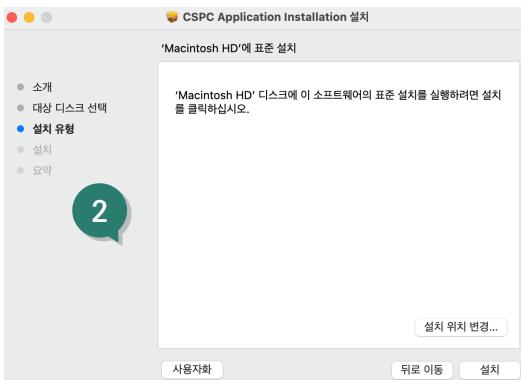
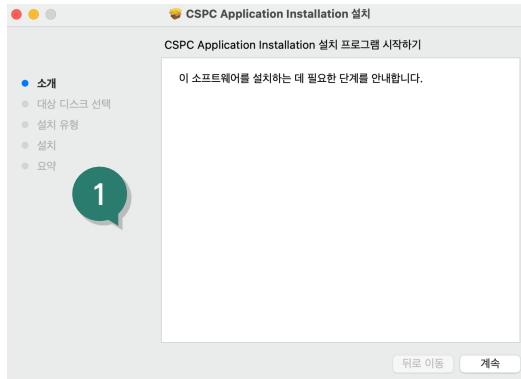
효과적인 Dashboard 지원

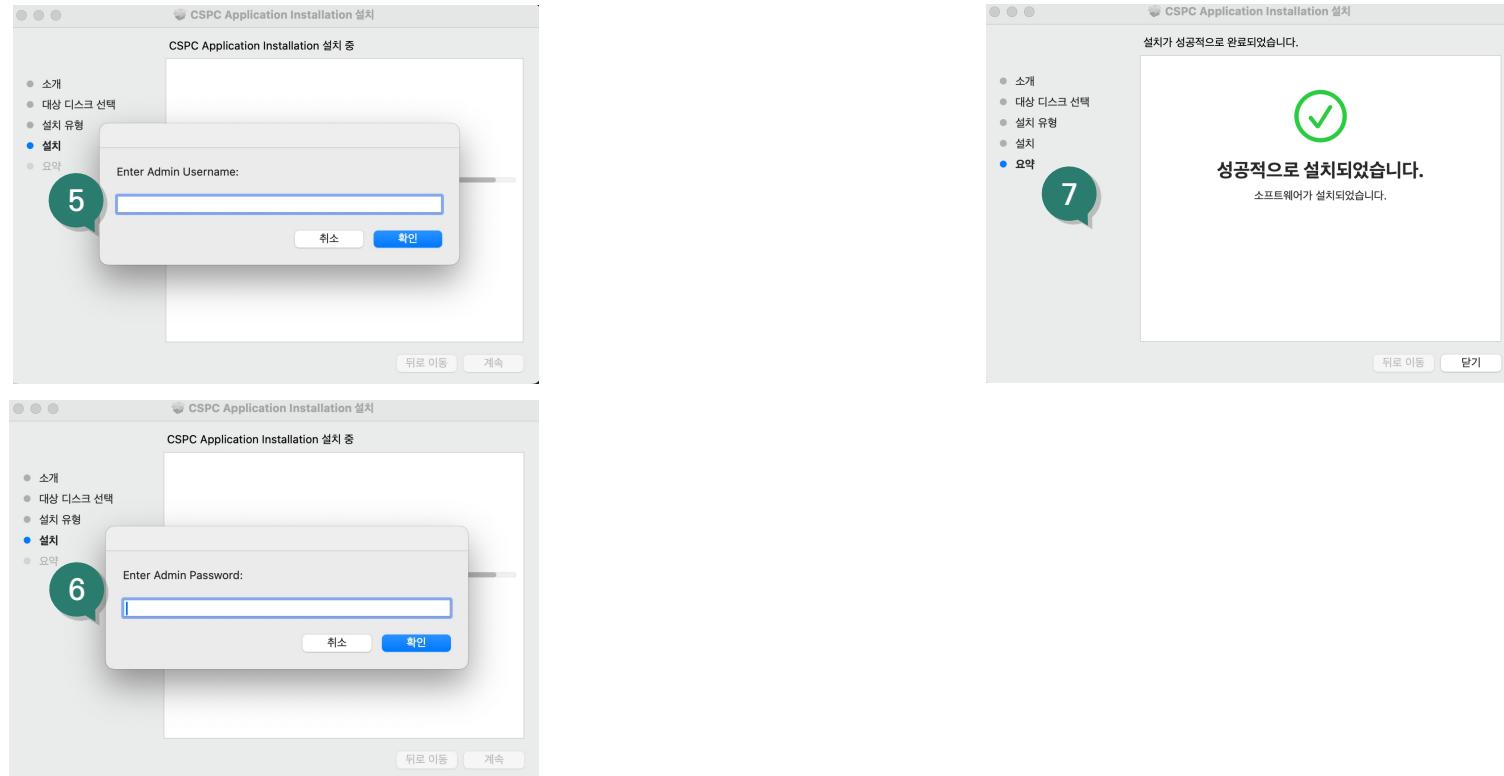
- 고급 사용자 인터페이스: 현대적인 디자인 원칙과 사용자 경험(UX) 최적화를 적용하여 사용자가 직관적으로 시스템을 이해하고 조작할 수 있게 합니다. 이는 사용자의 학습 곡선을 낮추고, 작업 효율성을 높입니다.
- 다양한 장치에서의 접근성: 반응형 웹 디자인을 통해 사용자가 데스크톱, 랩톱, 태블릿, 스마트폰 등 다양한 장치에서 동일한 사용성을 경험할 수 있습니다. 이는 현장에서의 실시간 데이터 접근과 수정을 가능하게 하여 업무의 유연성을 크게 향상시킵니다.

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





### MAC 점검 PC 설정

#### MAC 점검 스크립트 설치

```
folks@IMAC Client_Scripts % sudo ./mac_pc_setup
Password:
Do you want to SETUP or REMOVE SSH and inspection account settings? [SETUP/REMOVE]
REMOVE
Disabling SSH service...
Do you really want to turn remote login off? If you do, you will lose this connection?
no? yes
Removing firewall rule for SSH...
Application at path ( /usr/sbin/sshd ) removed from firewall
Removing inspection account...
Removing home directory for inspectaccount...
SSH service and inspection account removal is completed.
folks@IMAC Client_Scripts % sudo ./mac_pc_setup
Do you want to SETUP or REMOVE SSH and inspection account settings? [SETUP/REMOVE]
SETUP
Enabling SSH service...
Checking and updating firewall for SSH port...
Application at path ( /usr/sbin/sshd ) added to firewall
Incoming connection to the application is permitted
Creating inspection account with UniqueID: 502...
Home directory for inspectaccount created successfully.
SSH service setup and inspection account setup is completed.
folks@IMAC Client_Scripts %
```

#### 스크립트 실행

이 스크립트는 macOS 시스템에서 SSH 서비스와 관련된 설정을 관리하고 검사용 계정을 설정하거나 제거하는 기능을 수행합니다. 스크립트는 사용자에게 'SETUP' 또는 'REMOVE' 옵션을 선택하도록 요청하며, 선택에 따라 아래 작업을 수행 합니다:

#### SETUP

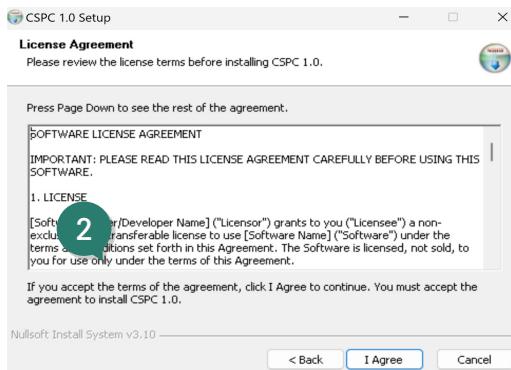
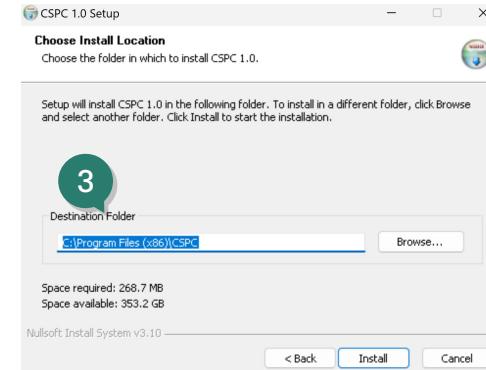
- SSH 서비스를 활성화합니다.
- 방화벽에서 SSH 포트(22번)가 열려 있는지 확인하고, 필요하다면 포트를 열어주는 규칙을 추가합니다.
- 'inspectaccount'라는 이름의 검사용 계정을 생성합니다. 이 계정은 관리자 권한을 가지고, 고유 사용자 ID, 훈 디렉토리, zsh 쉘 접근을 설정합니다.
- 검사용 계정의 훈 디렉토리를 생성합니다.

#### REMOVE

- SSH 서비스를 비활성화합니다.
- SSH에 대한 방화벽 규칙을 제거합니다.
- 'inspectaccount' 검사용 계정을 시스템에서 삭제합니다. 계정의 훈 디렉토리도 함께 제거합니다.

\* Mac 에 위와 같은 스크립트를 실행하여 점검 계정을 생성하는 것은 개인 PC의 id/pw 역시 개인정보에 해당되므로 점검을 위한 계정을 생성하는 것입니다.

### Windows Install



### Windows 점검 PC 설정

```
Windows 점검 스크립트 설치
▶ 관리자: Windows PowerShell
Select an operation:
1: Install and configure
2: Revert changes
Enter your choice (1 or 2):

--- Script Execution Start ---
Configuring WinRM service...
WinRM service configured successfully
Setting firewall rules...
Firewall rules set successfully
Checking if inspection account exists...
Creating inspection account...
Inspection account created successfully
Current network profile is not Public. No change needed.
Remote inspection setup completed
--- Script Execution End ---
```

#### 파워셸 스크립트 실행

이 PowerShell 스크립트는 Windows 시스템에서 원격 검사 설정을 설치하거나 제거하는 기능을 수행합니다. 사용자는 "Install and configure" 또는 "Revert changes" 중 하나를 선택할 수 있으며, 선택에 따라 다음 작업을 수행합니다::

#### Select 1 (설치 및 구성)

- WinRM 서비스 설정: Windows Remote Management (WinRM) 서비스를 자동 구성하고 활성화합니다.
- 방화벽 규칙 설정: WinRM 서비스에 대한 인바운드 TCP 트래픽을 허용하는 방화벽 규칙을 생성합니다.
- 검사용 계정 생성: 'InspectAccount'라는 이름의 사용자 계정을 생성하고, 해당 계정에 관리자 권한을 부여합니다. 계정의 비밀번호는 설정됩니다.
- 네트워크 프로파일 변경: 네트워크 프로파일이 공용으로 설정되어 있다면 사설로 변경합니다.

#### Select 2

- WinRM 서비스 비활성화: WinRM 서비스를 중지하고 비활성화합니다.
- 방화벽 규칙 제거: WinRM에 대한 방화벽 규칙을 제거합니다.
- 검사용 계정 삭제: 생성된 'InspectAccount' 사용자 계정을 삭제합니다.

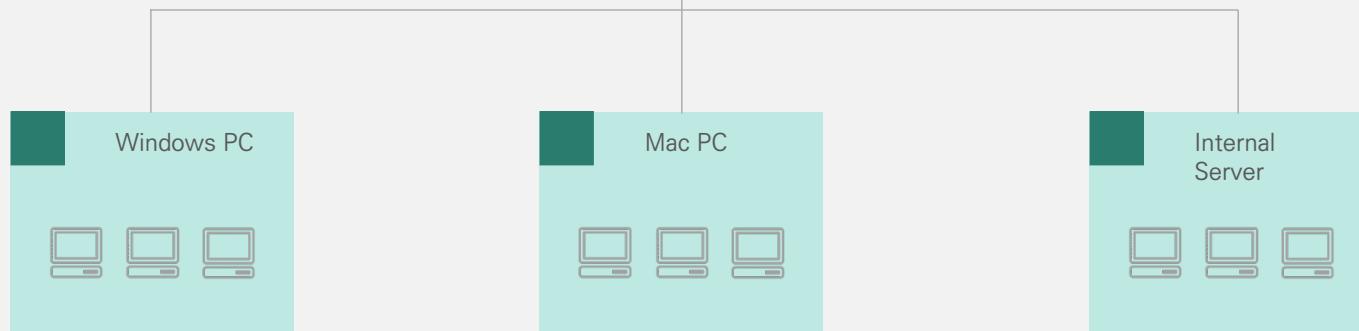
\* Windows PC 에 위와 같은 스크립트를 실행하여 점검 계정을 생성하는 것은 개인 PC의 id/pw 역시 개인정보에 해당되므로 점검을 위한 계정을 생성하는 것입니다.

### 회사망 점검 구성

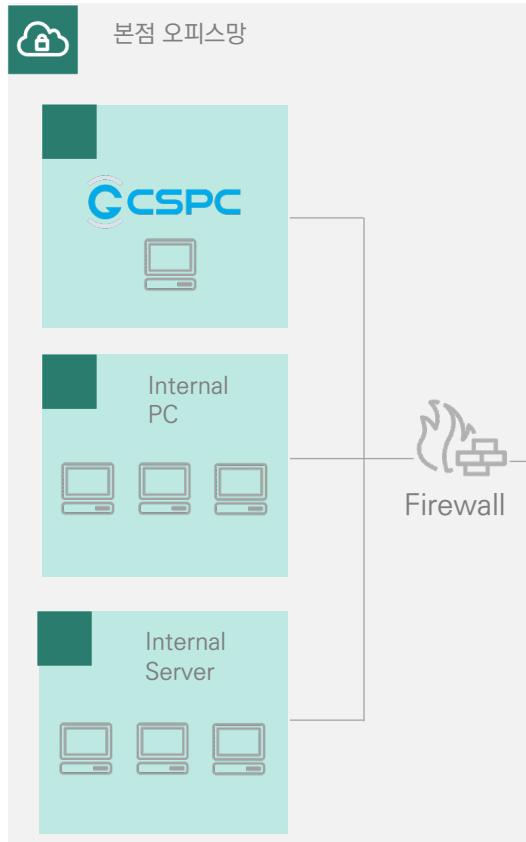


회사 네트워크(Broadcast network)

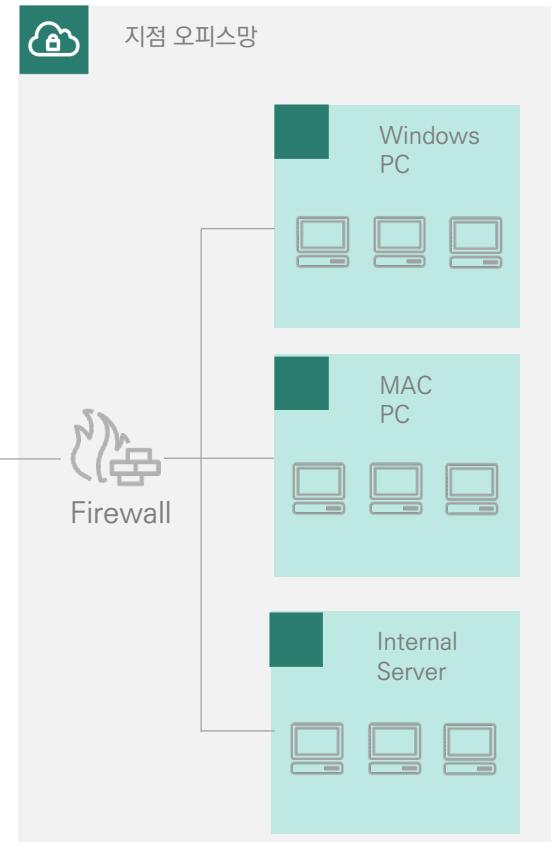
- ① 원도우/ 맥 PC에 setup 스크립트를 실행한다.
- ② 방화벽에서 CSPC 점검 PC → 원도우 PC로 TCP 5985 포트를 오픈한다.
- ③ 방화벽에서 CSPC 점검 PC → 맥 PC로 TCP 22 포트를 오픈한다



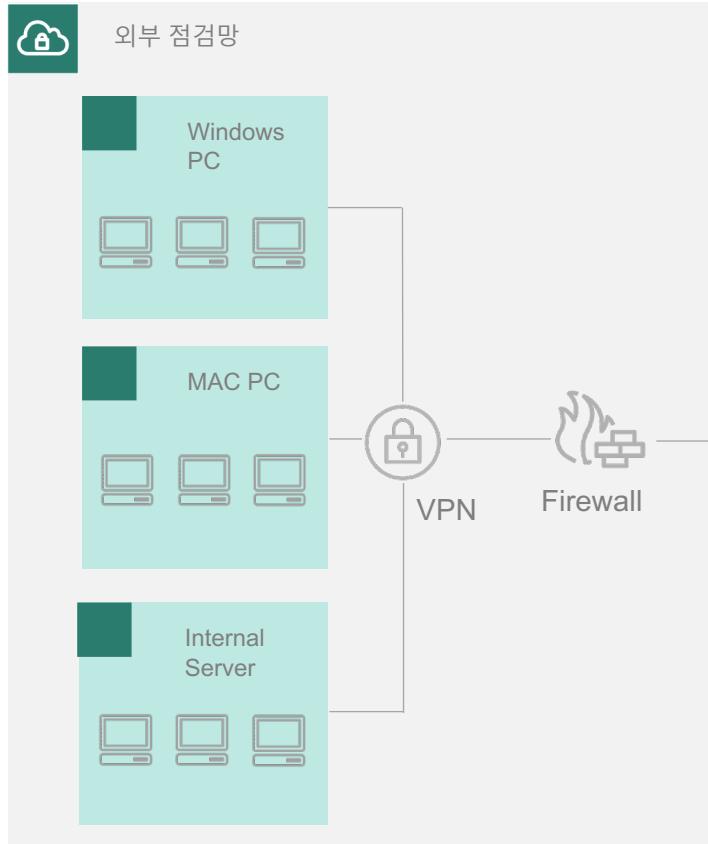
## 본점 – 지점 점검 구성



- ① 점검 원도우/ 맥 PC에 setup 스크립트를 실행한다.
- ② 본점 및 지점 방화벽에서 CSPC 점검 PC → 원도우 PC로 TCP 5985 포트를 오픈한다.
- ③ 본점 및 지점 방화벽에서 CSPC 점검 PC → 맥 PC로 TCP 22 포트를 오픈한다



### 외부 환경 점검 구성



- ① CSPC 점검 랩탑에서 외부 점검망으로 VPN 으로 접속한다.
- ② 외부 점검 원도우/ 맥 PC에 setup 스크립트를 실행한다.
- ③ 외부 점검망 방화벽에서 CSPC 점검 PC → 원도우 PC 로 TCP 5985 포트를 오픈한다.
- ④ 외부 점검망 방화벽에 CSPC 점검 PC → 맥 PC 로 TCP 22 포트를 오픈한다

### Dashboard 화면

The screenshot displays the CSCF Dashboard interface. At the top, there is a navigation bar with a 'Hide Menu' button, the CSCF logo, and a URL 'https://www.cscf.co.kr'. Below the navigation bar, there is a sidebar with icons for 'Home', 'Target', 'PC Scan', and 'Report'. The main content area features two large circular progress bars: one for 'Windows Security Level' (58.0% in red) and one for 'Mac Security Level' (48.0% in yellow). Below these bars are two tables showing audit results:

원도우 요약	상세 결과
점검 대수	1
취약 건수	8
HIGH 건수	6
MEDIUM 건수	1
LOW 건수	1

맥 요약	상세 결과
점검 대수	1
취약 건수	10
HIGH 건수	7
MEDIUM 건수	2
LOW 건수	1

At the bottom of the dashboard, there are 'Guideline' and 'Settings' buttons, and a copyright notice '© 2024. CSCF inc. all rights reserved'.

점검 Target 등록

Hide Menu

CSFC https://www.cscf.co.kr

Enter PC IP MAC

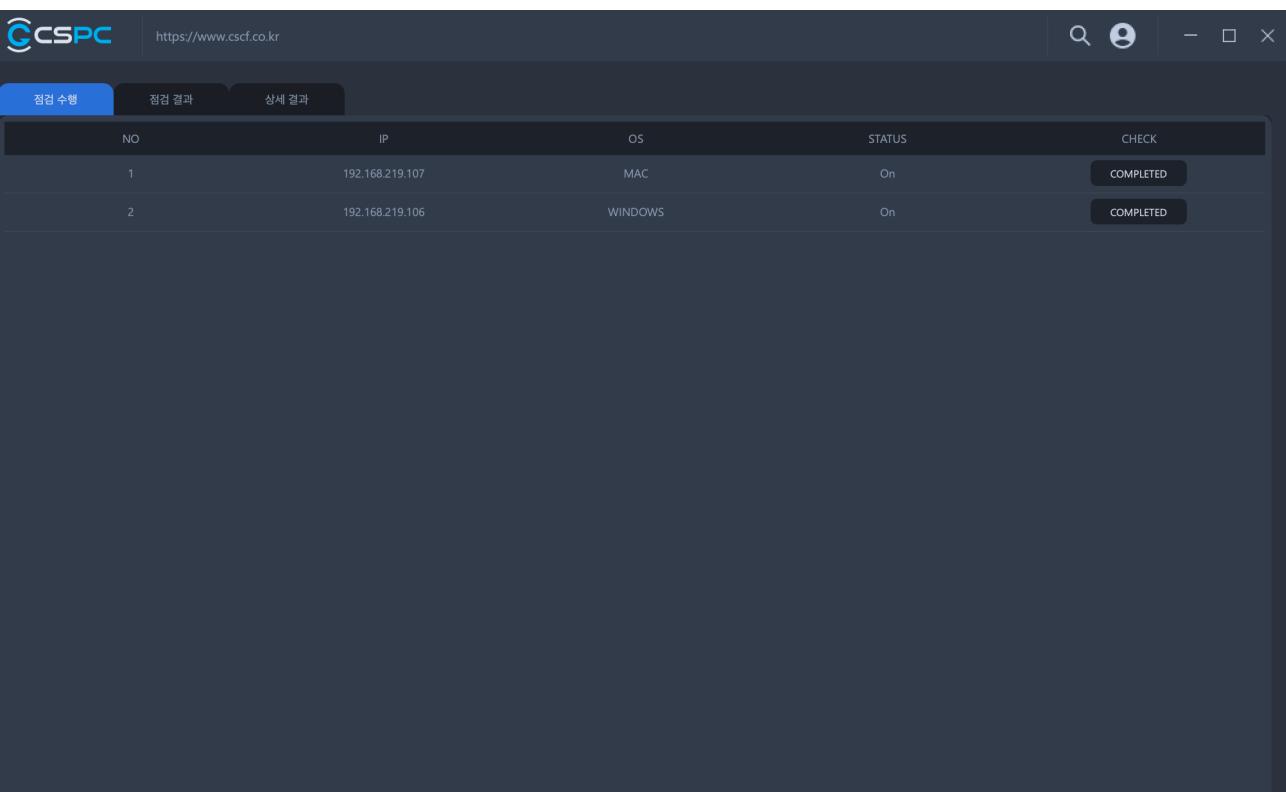
등록 삭제 업로드

NO	IP	OS	STATUS
1	192.168.219.107	MAC	On
2	192.168.219.106	WINDOWS	On

Home Target PC Scan Report Guideline Settings

© 2024, CSCF inc. all rights reserved v1.0

### PC Scan – 점검 수행



NO	IP	OS	STATUS	CHECK
1	192.168.219.107	MAC	On	COMPLETED
2	192.168.219.106	WINDOWS	On	COMPLETED

© 2024, CSFC Inc. all rights reserved v1.0

Hide Menu

CSFC https://www.csfc.co.kr

Home Target PC Scan Report Guideline Settings

### PC Scan – 점검 결과

NO	IP	OS	점검일	상세보기	내보내기
1	192.168.219.107	MAC	2024-03-06 14:46:32	<a href="#">Detail View</a>	<a href="#">Export</a>
2	192.168.219.106	WINDOWS	2024-03-06 14:45:39	<a href="#">Detail View</a>	<a href="#">Export</a>

© 2024. CSCF inc. all rights reserved v1.0

# 사용자 인터페이스 소개

## 4. 실행 및 사용

### PC Scan – 상세 결과

NO	카테고리	첨감항목	심각도	상세결과	첨감결과
1_1	계정관리	패스워드의 주기적 변경	상	최대 암호 사용기간 설정: 설정 안됨	취약
1_2	계정관리	패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정	상	패스워드 복장도 설정: 미적용	취약
1_3	계정관리	복구 편슬에서 자동 로그온을 금지하도록 설정	하	자동 로그온 설정: 비활성화됨	양호
2_1	서비스 관리	공유 폴더 제거	상	공유 폴더 설정: 취약한 설정이 발견됨 공유 폴더: /Users/watangca/Public ...	취약
2_2	서비스 관리	불필요한 서비스 제거	상	불필요한 서비스 확인: 불필요한 서비스 발견되지 않음	양호
2_3	서비스 관리	Windows Messenger(MSN, .NET 메신저 등)와 같은 상용 메신저의 사용 ...	상	사용중인 메신저: KakaoTalk.app	취약
2_4	서비스 관리	윈도우 일 경우 파일 시스템이 NTFS 포맷으로 설정 됨...	중	파일시스템 탐색: APFS, 암호화 여부: None	취약
2_5	서비스 관리	대상 시스템이 Windows/mac을 제외한 다른 OS로 멀티 부팅이 가능하지 않도...	중	Boot Camp: 사용 안함, Parallels Desktop: 사용 안함	양호
2_6	서비스 관리	브라우저 종료 시 임시 인터넷 파일 폴더의 내용을 삭제 하도록 설정	하	사파리 캐시 설정: 기본값 또는 설정되지 않음	취약
3_1	폐지 관리	HOT FIX 등 최신 보안패치 적용	상	적용할 최신 패치가 발견됨: Software Update found the following new ...	취약
3_2	폐지 관리	최신 서비스팩 적용	상	최신 패치가 발견됨: Software Update found the following new or ...	취약
3_3	폐지 관리	MS-Office, 한글, 어도비 아크로벳 등의 음악 프로그램에 대한 최신 보안패치 ...	상	MS 오피스 설치 여부: 설치됨, 설치할 패치가 있음	양호
4_1	보안 관리	비바이러스 백신 프로그램 설치 및 주기적 업데이트	상	설치된 백신: XProtect, 정보: XProtectPlistConfigData:\n ...	양호
4_2	보안 관리	비바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화	상	XProtect의 실시간 감시 기능은 macOS 시스템에서 자동으로 활성화되며, 알려...	양호
4_3	보안 관리	OS에서 제공하는 침입차단 기능 활성화	상	방화벽 기능 활성화 여부: Firewall is disabled (State=0)	취약
4_4	보안 관리	화면보호기 대기 시간 설정 및 제시작 시 암호 보호 설정	상	화면 보호기 대기 시간: 300초	양호
4_5	보안 관리	CD, DVD, USB 메모리 등과 같은 미디어의 자동실행 방지로 이동식	상	macOS는 기본적으로 이동식 미디어(USB 드라이브)의 자동 실행을	양호

© 2024, CSFC Inc. all rights reserved.

The screenshot displays the CSFC Reporting interface. The top navigation bar is teal with the word "Reporting". The main content area shows a table of reports with the following columns: 리포트 템플릿 (Report Template), 리포팅 대상 (Reporting Target), 생성일시 (Creation Date), STATUS, and DOWNLOAD. The first report listed is "pc\_template.xlsx" for target "pc" on "2024-03-04 11:50:08" with a status of "Pending". There are "Export" and "Download" buttons for this row. The sidebar on the left contains a "Hide Menu" button and links for Home, Target, PC Scan, Report (which is highlighted with a blue box), Guideline, and Settings. The bottom of the page includes a copyright notice "© 2024 CSFC inc. all rights reserved." and a version number "v1.0".

리포트 템플릿	리포팅 대상	생성일시	STATUS	DOWNLOAD
pc_template.xlsx	pc	2024-03-04 11:50:08	Pending	<button>Export</button> <button>Download</button>

### Guideline

Guideline

https://www.cscf.co.kr

Export

Report

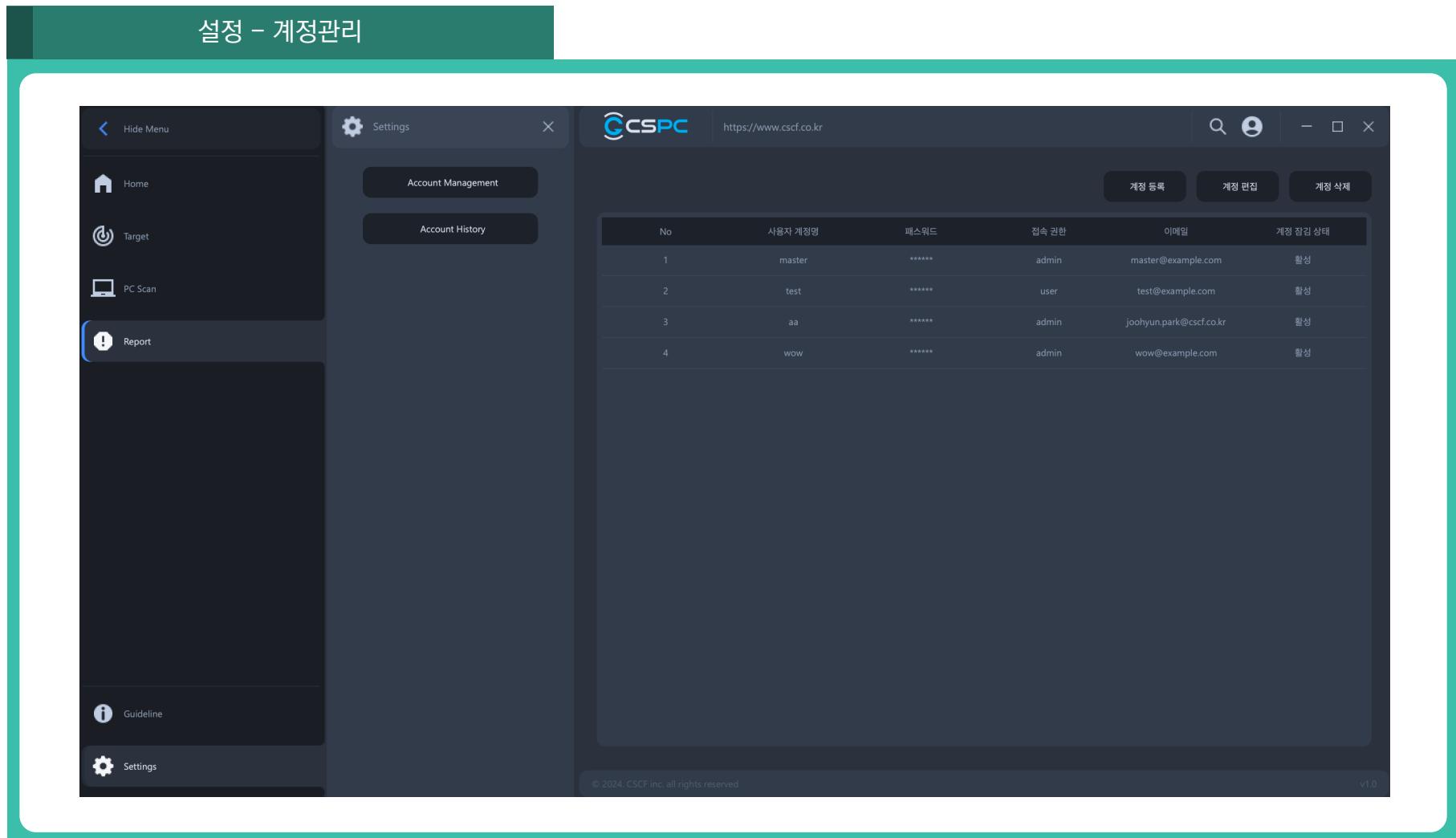
© 2024, CSCF Inc. all rights reserved

v1.0

NO	카테고리	점검항목	상각도	기아드라인
1_1	계정관리	패스워드의 주기적 변경	상	최대 암호 사용 기간 “90일” 설정 최소 암호 사용 기간 “1일” 설정...
1_2	계정관리	패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정	상	패스워드 복잡도 규정 적용 영문, 숫자, 특수문자를 조합하여 ...
1_3	계정관리	복구 퀸슬에서 자동 로그온을 금지하도록 설정	하	자동 로그온 허용 “사용 안 함”으로 설정 ...
2_1	서비스 관리	공유 폴더 제거	상	< 공유 폴더 설정 기준 > 1. C\$, D\$, Admin\$ 등의 기본 공...
2_2	서비스 관리	불필요한 서비스 제거	상	불필요한 서비스 중지 Alerter, Clipbook, Computer ...
2_3	서비스 관리	Windows Messenger(MSN,.NET 메신저 등)와 같은 상용 메신저의 ...	상	“Windows Messenger”를 실행하지 않음” 설정 및 상용 메신...
2_4	서비스 관리	원도우 파일 시스템이 NTFS 포맷으로 설정 됨...	중	모든 디스크 볼륨에 대해 파일 시스템 NTFS로 변경
2_5	서비스 관리	대상 시스템이 Windows/mac을 제외한 다른 OS로 멀티 부팅이 ...	중	하나의 OS만 설치하여 운영함
2_6	서비스 관리	브라우저 종료 시 임시 인터넷 파일 폴더 비우기”를 “사용”으로 ...	하	브라우저를 닫을 때 임시 인터넷 파일 폴더 비우기”를 “사용”으로 ...
3_1	폐치 관리	HOT FIX 등 최신 보안폐치 적용	상	Windows Update 사이트에 접속하여 최신 폐치 설치 여부 확인...
3_2	폐치 관리	최신 서비스팩 적용	상	Windows Update 사이트에 접속하여 최신 서비스팩 여부 확인...
3_3	폐치 관리	MS-Office, 한글, 어도비 아크로뱃 등의 응용 프로그램에 대한 최신 ...	상	설치된 MS-Office, 한글, 어도비 아크로뱃의 최신 보안 폐치 적용
4_1	보안 관리	바이러스 백신 프로그램 설치 및 주기적 업데이트	상	바이러스 백신 설치 및 최신 업데이트 적용
4_2	보안 관리	바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화	상	백신을 설치하고 실시간 감시 기능을 활성화함
4_3	보안 관리	OS에서 제공하는 침입차단 기능 활성화	상	Windows 방화벽 “사용”으로 설정 또는 유무료 기타 방화벽을 사용
4_4	보안 관리	화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정	상	화면보호기(10분) 설정 및 암호화 보호 설정

18

**CSCF** CYBER STRATEGY  
CONSULTING FIRM



The screenshot shows the 'Account Management' section of the CSCF user interface. The left sidebar has a 'Report' item selected. The main content area displays a table of account information with the following data:

No	사용자 계정명	패스워드	접속 권한	이메일	계정 잠김 상태
1	master	*****	admin	master@example.com	활성
2	test	*****	user	test@example.com	활성
3	aa	*****	admin	joohyun.park@cscf.co.kr	활성
4	wow	*****	admin	wow@example.com	활성

The interface includes a top navigation bar with 'Settings' and a search bar. The CSCF logo and URL 'https://www.cscf.co.kr' are visible in the header.

설정 – History 관리

접속 계정	로그인 시간	로그아웃 시간	로그인 성공여부	접속 IP
wow	2024-05-10 13:21:31	None	성공	192.168.219.105
aa	2024-05-06 05:03:19	2024-05-06 14:03:31	성공	192.168.219.105
aa	2024-05-05 15:56:18	2024-05-06 00:56:59	성공	192.168.219.103
aa	2024-05-05 15:54:27	2024-05-06 00:54:58	성공	192.168.219.103
aa	2024-05-05 15:54:02	2024-05-06 00:54:09	성공	192.168.219.103
aa	2024-05-05 15:53:42	2024-05-06 00:53:54	성공	192.168.219.103
aa	2024-05-05 10:11:37	2024-05-05 19:11:45	성공	192.168.219.103
aa	2024-04-13 03:27:27	2024-04-13 12:29:42	성공	192.168.219.104
aa	2024-04-13 03:20:18	2024-04-13 12:27:21	성공	192.168.219.104
aa	2024-04-13 02:39:06	2024-04-13 11:57:48	성공	192.168.219.104
aa	2024-04-13 02:04:19	2024-04-13 11:04:41	성공	192.168.219.104
aa	2024-04-12 06:33:17	None	성공	192.168.219.104
aa	2024-03-31 01:28:56	2024-03-31 10:54:20	성공	192.168.219.102
aa	2024-03-31 01:24:17	None	성공	192.168.219.102
aa	2024-03-21 15:17:33	2024-03-22 00:17:40	성공	192.168.219.101
aa	2024-03-21 03:46:28	2024-03-21 12:51:05	성공	192.168.219.103

© 2024. CSF inc. all rights reserved v1.0

### 로그아웃 및 프로필 설정

NO	카테고리	점검항목	심각도	가이드라인
1_1	계정관리	패스워드의 주기적 변경	상	최대 일자 사용 기간 '90일' 설정 최소 일자 사용 기간 '1일' 설정...
1_2	계정관리	패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정	상	패스워드 복잡도 규정 적용 sudo pwpolicy -u /Local/Defa...
1_3	계정관리	복구 콜드에서 자동 로그온을 금지하도록 설정	하	1. GUI 명령 -Apple 메뉴에서 '시스템 ...' 1. 공유폴더 check: sudo sharing -l ...
2_1	서비스 관리	공유 폴더 제거	상	1. 명령어로 다음의 보안에 취약한 서비스 점검 ...
2_2	서비스 관리	불필요한 서비스 제거	상	1. 키보드 및 페이스북 메신저 발견시 프로그램 삭제
2_3	서비스 관리	Windows Messenger(MSN, .NET 메신저 등)와 같은 상용 메신저의 ...	상	1. GUI
2_4	서비스 관리	원도우 일 경우 파일 시스템이 NTFS 포맷으로 설정 점검...	중	-시스템 환경설정 열기: Apple 메...
2_5	서비스 관리	대상 시스템이 Windows/mac을 제외한 다른 OS로 멀티 부팅이 ...	중	1. Boot Camp 파티션 제거 방법 -Boot Camp 지원 소프트웨어 ...
2_6	서비스 관리	브라우저 종료 시 임시 인터넷 파일 폴더의 내용을 삭제 하도록 설정	하	1. Safari에서 설정 변경하기 -개인정보 보호 모드 사용하기: ... * macOS에서 보안 패치, 서비스 팩, 시스템 업데이트 등은 주로 통합되...
3_1	패치 관리	HOT FIX 등 최신 보안패치 적용	상	* macOS에서 보안 패치, 서비스 팩, 시스템 업데이트 등은 주로 통합되...
3_2	패치 관리	최신 서비스팩 적용	상	설치된 MS-Office, 한글, 어도비 아크로뱃 등의 유통 프로그램에 대한 최신 ... * macOS에서는 기본적으로 바이러스 및 멀웨어로부터 보호하기 위한 여...
3_3	패치 관리	MS-Office, 한글, 어도비 아크로뱃 등의 유통 프로그램에 대한 최신 ...	상	macOS에서는 기본적으로 바이러스 및 멀웨어로부터 보호하기 위한 여...
4_1	보안 관리	바이러스 백신 프로그램 설치 및 주기적 업데이트	상	XProtect의 실시간 감시 기능은 macOS 시스템에서 자동으로 ...
4_2	보안 관리	바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화	상	1. 방화벽 상태 확인 sudo /usr/libexec/...
4_3	보안 관리	OS에서 제공하는 침입차단 기능 활성화	상	1. 현재 화면보호기 시작 시간 확인 defaults -currentHost read ...
4_4	보안 관리	화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정	상	

### 취약점 점검 수행

The screenshot shows the CSFC web interface with a dark theme. The main content area displays a table of scan results for two targets. The first target (IP: 192.168.219.107) is marked as 'On' and has a 'COMPLETED' status. The second target (IP: 192.168.219.106) is also marked as 'On' and has a 'COMPLETED' status. A modal dialog titled '사용자 정보 입력' (User Information Input) is overlaid on the page, prompting for 'ID' and 'PW' with a '확인' (Confirm) button. The left sidebar contains navigation links: Home, Target, PC Scan (selected), Report, Guideline, and Settings. The top right corner shows the CSFC logo and the URL https://www.cscf.co.kr. The bottom right corner indicates the version v1.0.

NO	IP	OS	STATUS	CHECK
1	192.168.219.107	MAC	On	COMPLETED
2	192.168.219.106	WINDOWS	On	COMPLETED

사용자 정보 입력

ID

PW

확인

© 2024, CSCF inc. all rights reserved. v1.0

### 취약점 검색

Hide Menu

CCSPC https://www.cscf.co.kr

Mac IP 입력 No 입력 상 양호 암호 검색

시스템 유형	IP 주소	번호	카테고리	점검 항목	점검 상세	결과	점검 상세
mac	192.168.219.107	2_2	서비스 관리	불필요한 서비스 제거	상	양호	불필요한 서비스 확인: 불필요한 서비스 발견되지 ...
mac	192.168.219.107	3_3	패치 관리	MS-Office, 한글, 어도비 아크로벳 등의 응용 ...	상	양호	MS 오피스 설치 여부: 설치됨, 설치할 패치가 없음
mac	192.168.219.107	4_1	보안 관리	바이러스 백신 프로그램 설치 및 주기적 업데이트	상	양호	설치된 백신: XProtect, 정보: XProtectPlistConfigData...
mac	192.168.219.107	4_2	보안 관리	바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 ...	상	양호	XProtect의 실시간 감시 기능은 macOS 시스템에서...
mac	192.168.219.107	4_4	보안 관리	화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정	상	양호	화면 보호기 대기 시간: 300초
mac	192.168.219.107	4_5	보안 관리	CD, DVD, USB 메모리 등과 같은 미디어의 자동실행 방 ...	상	양호	macOS는 기본적으로 자동실행 방지로 설정됨
mac	192.168.219.107	4_6	보안 관리	Windows PC 내부의 미사용(3개월) ActiveX 제...	상	양호	발견된 확장프로그램이 없음
mac	192.168.219.106	1_1	계정관리	패스워드의 주기적 변경	상	양호	최대 암호 사용 기간 설정값: 42일
mac	192.168.219.106	3_1	패치 관리	HOT FIX 등 최신 보안패치 적용	상	양호	보안패치 적용여부: 설치함 보안 업데이트가 없음 ...
mac	192.168.219.106	3_2	패치 관리	최신 서비스팩 적용	상	양호	시스템 패치여부: 설치함 시스템 업데이트가 없음 ...
mac	192.168.219.106	3_3	패치 관리	MS-Office, 한글, 어도비 아크로벳 등의 응용 ...	상	양호	MS 오피스 설치 여부: 설치됨, 설치할 패치가 없음
mac	192.168.219.106	4_2	보안 관리	바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 ...	상	양호	실시간 보호 상태: Real-time protection is enabled.
mac	192.168.219.106	4_3	보안 관리	OS에서 제공하는 침입차단 기능 활성화	상	양호	윈도우 방화벽 활성화 여부: 모든 프로필에서 방화벽이 ...
mac	192.168.219.106	4_4	보안 관리	화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정	상	양호	화면보호기 설정 여부 확인: 대기 시간: 600초, 암호로 ...
mac	192.168.219.106	4_6	보안 관리	Windows PC 내부의 미사용(3개월) ActiveX 제...	상	양호	3개월 동안 사용되지 않은 ActiveX 발견되지 않음.

© 2024. CSCF inc. all rights reserved v1.0

## 상세 보고서

192.168.219.107

NO	CATEGORY	CHECKLIST	SEVERITY	CHECK DETAIL	RESULT
1_1	계정관리	패스워드의 주기적 변경	상	최대 암호 사용기간 설정: 설정 안됨	취약
1_2	계정관리	패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정	상	패스워드 복잡도 설정: 미적용	취약
1_3	계정관리	복구 콘솔에서 자동 로그온을 금지하도록 설정	하	자동 로그온 설정: 비활성화됨	양호
2_1	서비스 관리	공유 폴더 제거	상	공유 폴더 설정: 취약한 설정이 발견된 공유 폴더: /Users/watangca/Public (공유 활성화, 계스트	취약
2_2	서비스 관리	형목의 불필요한 서비스 제거	상	불필요한 서비스 확인: 불필요한 서비스 발견되지 않음	양호
2_3	서비스 관리	Windows Messenger(MSN, .NET 메신저 등)와 같은 상용 메신저의 사용 금지	상	사용중인 메신저: KakaoTalk.app	취약
2_4	서비스 관리	파일 시스템이 NTFS 포맷으로 설정	중	파일시스템 타입: APFS, 암호화 여부: None	취약
2_5	서비스 관리	대상 시스템이 Windows 서비스를 제외한 다른 OS로 멀티 부팅이 가능하지 않도록 설정	중	Boot Camp: 사용 안함, Parallels Desktop: 사용안함	양호
2_6	서비스 관리	브라우저 종료 시 임시 인터넷 파일 폴더의 내용을 삭제 하도록 설정	하	사파리 캐시 설정: 기본값 또는 설정되지 않음	취약
3_1	패치 관리	HOT FIX 등 최신 보안패치 적용	상	적용할 최신 패치가 발견됨: Software Update found the following new or updated software:	취약
3_2	패치 관리	최신 서비스팩 적용	상	최신 패치가 발견됨: Software Update found the following new or updated software: * Lab	취약
3_3	패치 관리	MS-Office, 한글, 어도비 아크로뱃 등의 응용 프로그램에 대한 최신 보안패치 및 벤더 권고사항 적용	상	MS 오피스 설치 여부: 설치됨, 설치할 패치가 없음	양호
4_1	보안 관리	바이러스 백신 프로그램 설치 및 주기적 업데이트	상	설치된 백신: XProtect, 정보: XProtectPlistConfigData:\n\n Version: 2144\n Source: macOS	양호
4_2	보안 관리	바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화	상	XProtect의 실시간 감시 기능은 macOS 시스템에서 자동으로 활성화되며, 일려진 악성 코드로부터	양호
4_3	보안 관리	OS에서 제공하는 침입차단 기능 활성화	상	방화벽 기능 활성화 여부: Firewall is disabled (State=0)	취약
4_4	보안 관리	화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정	상	화면 보호기 대기 시간: 300초	양호
4_5	보안 관리	CD, DVD, USB 메모리 등과 같은 미디어의 자동실행 방지등 이동식 미디어에 대한 보안대책 수립	상	macOS는 기본적으로 이동식 미디어(.iso, USB 등)의 자동 실행을 차단함	양호
4_6	보안 관리	PC 내부의 미사용(3개월) ActiveX 제거	상	발견된 확장프로그램이 없음	양호
4_7	보안 관리	원격 지원을 금지하도록 정책이 설정	중	원격연결 사용 여부: 원격연결 사용함, 보안 점검을 위한 원격접속 OPEN 반드시 점검 후 계정 삭제	취약

## 상세 보고서

고객사(주)

## PC 취약점진단 보고서

Version 1.0  
2024-05-10

ORY	CHECKLIST	SEVERITY	192.168.219.107	192.168.219.106
2_1	파스워드의 주기적 변경	상	취약	양호
2_2	파스워드 정책이 해당 기관의 보안 정책에 적합하게 설정	상	취약	취약
2_3	복구 콘솔에서 자동 로그온을 금지하도록 설정	하	양호	양호
2_4	공유 폴더 제거	상	취약	취약
2_5	항목의 불필요한 서비스 제거	상	양호	취약
2_6	Windows Messenger(MSN, .NET 메신저 등)와 같은 상용 메신저의 사용 금지	상	취약	취약
2_7	파일 시스템이 NTFS 포맷으로 설정	중	취약	양호
2_8	대상 시스템이 Windows Server를 제외한 다른 OS로 멀티 부팅이 가능하지 않도록 설정	중	양호	양호
2_9	파일 시스템이 FAT32로 설정되어 있는 경우, 파일의 내용을 삭제 하도록 설정	하	취약	취약
3_1	브라우저 종료 시 일시 인터넷 파일 폴더의 내용을 삭제 하도록 설정	상	취약	양호
3_2	HOT FIX 등 최신 보안패치 적용	상	취약	양호
3_3	최신 서비스팩 적용	상	취약	양호
3_4	MS-Office, 한글, 어도비 아크로뱃 등의 응용 프로그램에 대한 최신 보안패치 적용	상	양호	양호
4_1	파일 시스템이 FAT32로 설정되어 있는 경우, 파일의 내용을 삭제 하도록 설정	상	양호	취약
4_2	파일 시스템이 NTFS 포맷으로 설정되어 있는 경우, 파일의 내용을 삭제 하도록 설정	상	양호	양호
4_3	파일 시스템이 FAT32로 설정되어 있는 경우, 파일의 내용을 삭제 하도록 설정	상	양호	양호
4_4	파일 시스템이 NTFS 포맷으로 설정되어 있는 경우, 파일의 내용을 삭제 하도록 설정	상	양호	양호
4_5	파일 시스템이 FAT32로 설정되어 있는 경우, 파일의 내용을 삭제 하도록 설정	상	양호	취약
4_6	파일 시스템이 NTFS 포맷으로 설정되어 있는 경우, 파일의 내용을 삭제 하도록 설정	상	양호	양호
4_7	파일 시스템이 FAT32로 설정되어 있는 경우, 파일의 내용을 삭제 하도록 설정	중	취약	취약
SECURITY LEVEL			48	58

## 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  
  ],  
  "left_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  
  }  
}
```

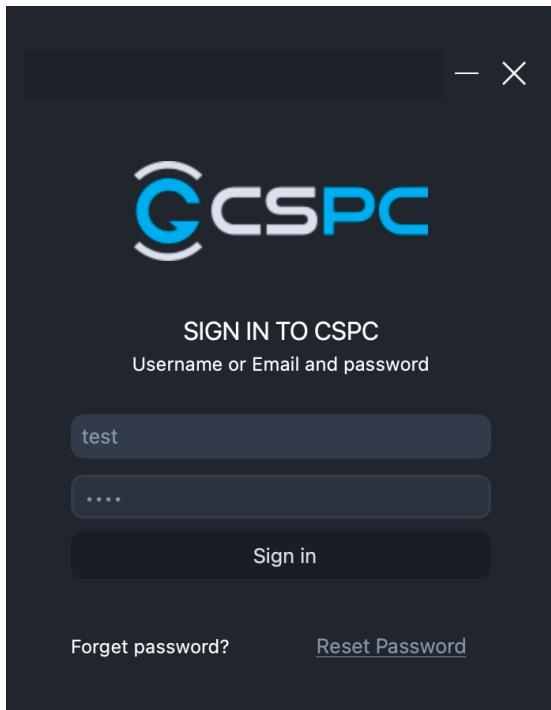
- UI 텍스트 설정
- 테마 설정

- 다양 UI 사이즈 설정
- 타임 애니메이션 값 설정

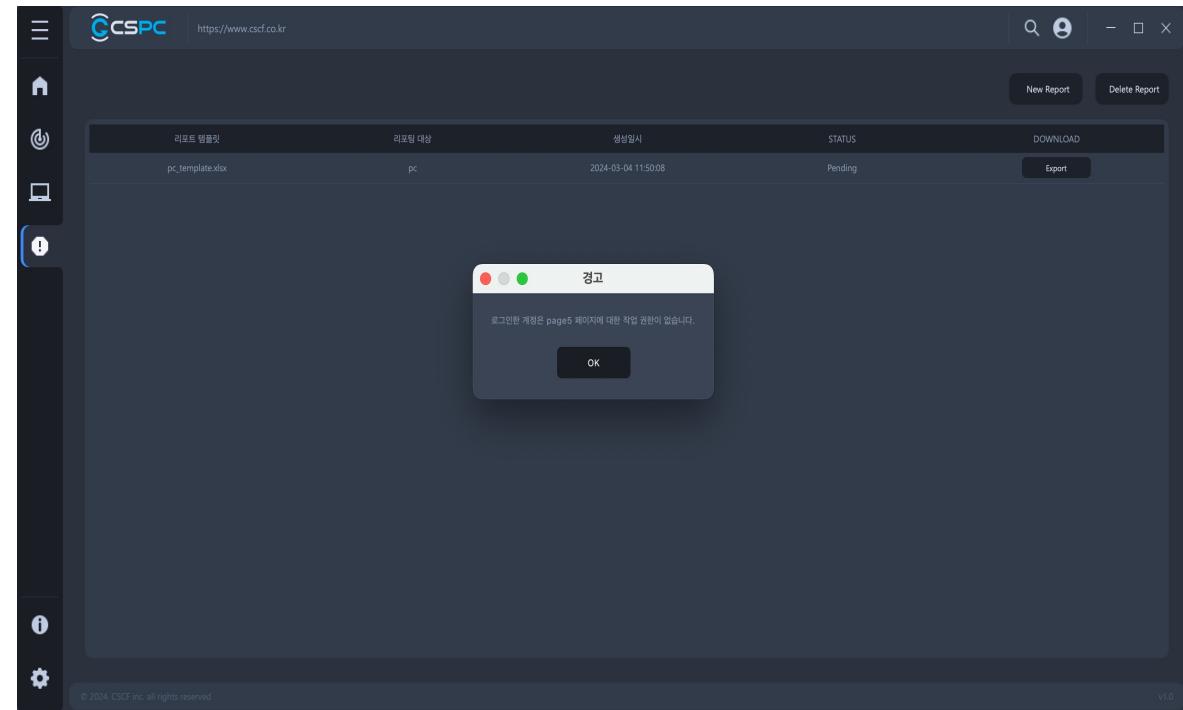
- UI 폰트 설정

### 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 PC 담당자가 본인 PC 취약점을 확인할 수 있도록 개발됨

# 감사합니다.

FOLLOW US ON:

-  <https://www.cscf.co.kr>
-  [partner@cscf.co.kr](mailto:partner@cscf.co.kr)
-  010-2844-0393

© Copyright CSCF Corporation 2023. All rights reserved. . 모든 권리 보유. 이 자료에 포함된 정보는 정보 제공의 목적으로만 제공되며 명시적이든 묵시적이든 어떠한 종류의 보증도 없이 있는 그대로 제공됩니다. CSCF는 이러한 자료의 사용으로 인해 또는 이와 관련하여 발생하는 모든 손해에 대해 책임을 지지 않습니다. 본 자료에 포함된 어떠한 내용도 CSCF, 공급자 또는 라이센스 제공자로부터 보증 또는 진술을 생성하거나 CSCF 소프트웨어 사용에 적용되는 해당 라이센스 계약의 조건을 변경하려는 의도가 없으며 그러한 효과를 가져서는 안됩니다. 본 자료에서 CSCF 제품, 프로그램 또는 서비스를 언급한다고 해서 운영되는 모든 국가에서 해당 제품, 프로그램 또는 서비스를 사용할 수 있다는 의미는 아닙니다. 본 자료에 언급된 제품 출시 날짜 및/또는 기능은 시장 기회 또는 기타 요인에 따라 CSCF의 단독 재량에 따라 언제든지 변경될 수 있으며 어떤 방식으로든 향후 제품 또는 기능 가용성에 대한 약속이 아닙니다.

모범 보안 관행 선언문: IT 시스템 보안에는 기업 내부 및 외부로부터의 부적절한 액세스에 대한 예방, 감지 및 대응을 통해 시스템과 정보를 보호하는 것이 포함됩니다. 부적절한 액세스로 인해 정보가 변경, 파괴, 오용 또는 오용될 수 있으며, 타인에 대한 공격에 사용하는 것을 포함하여 시스템이 손상되거나 오용될 수 있습니다. 어떠한 IT 시스템이나 제품도 완전히 안전하다고 간주되어서는 안 되며, 단일 제품, 서비스 또는 보안 조치도 부적절한 사용이나 액세스를 방지하는 데 완전히 효과적일 수 없습니다. CSCF 시스템, 제품 및 서비스는 합법적이고 포괄적인 보안 접근 방식의 일부로 설계되었으며, 여기에는 반드시 추가 운영 절차가 필요하며 가장 효과적이기 위해서는 다른 시스템, 제품 또는 서비스가 필요할 수 있습니다.

CSCF은 시스템, 제품 또는 서비스가 악의적이거나 불법적인 행위로부터 면제되거나 귀하의 기업이 면제될 것이라는 점을 보증하지 않습니다.