목차

OpenSCAP 3
Openscap Profiles 3
ANSSI-BP-028 (enhanced) 3
ANSSI-BP-028 (high) 3
ANSSI-BP-028 (intermediarly) 3
ANSSI-BP-028 (minimal) 4
CIS Red Hat Enterprise Linux 8 벤치마크 Level 2 - 서버 4
CIS Red Hat Enterprise Linux 8 벤치마크 Level 1 - 서버 4
CIS Red Hat Enterprise Linux 8 벤치마크 Level 1 - 워크스테이션 4
CIS Red Hat Enterprise Linux 8 벤치마크 Level 2 - 워크스테이션 4
비연방 정보 시스템 및 조직의 비분류 정보(NIST 800-171) 4
호주 사이버 보안 센터(ACSC) Essential Eight 5
건강보험정보시스템 (HIPAA) 5
호주 사이버 보안 센터(ACSC) ISM 공식 5
범용 운영체제 보호 프로파일 5
PCI-DSS v4.0 Red Hat Enterprise Linux 8에 대한 제어 기준 5
DISA STIG for Red Hat Enterprise Linux 8 6
DISA STIG with GUI for Red Hat Enterprise Linux 8 6

OpenSCAP

- OpenSCAP 개요
- OpenSCAP 매뉴얼 v1.2
- XCCDF
- OVAL
    - 2016-11-18 OpenSCAP Workshop Coursebook
- SCAP rule repository
- https://www.redhat.com/en/blog/center-internet-security-cis-compliance-red-hat-enterprise-linux-using-openscap

Openscap Profiles

ANSSI-BP-028 (enhanced)

이 프로파일은 ANSSI-BP-028 v2.0의 강화 하드닝 수준에 맞춰 구성된 설정을 포함합니다. ANSSI는 프랑스 국가 정보 보안 기관으로, “Agence nationale de la sécurité des systèmes d'information”을 의미합니다. ANSSI-BP-028은 GNU/Linux 시스템을 위한 설정 권장사항입니다. ANSSI-BP-028의 사본은 ANSSI 웹사이트에서 찾을 수 있습니다: https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-a-un-systeme-gnulinux/. 영어 버전도 ANSSI 웹사이트에서 찾을 수 있습니다: https://cyber.gouv.fr/publications/configuration-recommendations-gnulinux-system.

ANSSI-BP-028 (high)

이 프로파일은 ANSSI-BP-028 v2.0의 높은 하드닝 수준에 맞춰 구성된 설정을 포함합니다. ANSSI는 프랑스 국가 정보 보안 기관으로, “Agence nationale de la sécurité des systèmes d'information”을 의미합니다. ANSSI-BP-028은 GNU/Linux 시스템을 위한 설정 권장사항입니다. ANSSI-BP-028의 사본은 ANSSI 웹사이트에서 찾을 수 있습니다: https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-a-un-systeme-gnulinux/. 영어 버전도 ANSSI 웹사이트에서 찾을 수 있습니다: https://cyber.gouv.fr/publications/configuration-recommendations-gnulinux-system.

ANSSI-BP-028 (intermediarly)

이 프로파일은 ANSSI-BP-028 v2.0의 중간 하드닝 수준에 맞춰 구성된 설정을 포함합니다. ANSSI는 프랑스 국가 정보 보안 기관으로, “Agence nationale de la sécurité des systèmes d'information”을 의미합니다. ANSSI-BP-028은 GNU/Linux 시스템을 위한 설정 권장사항입니다. ANSSI-BP-028의 사본은 ANSSI 웹사이트에서 찾을 수 있습니다: [https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-a-un-systeme-g

nulinux/](https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-a-un-systeme-gnulinux/). 영어 버전도 ANSSI 웹사이트에서 찾을 수 있습니다: https://cyber.gouv.fr/publications/configuration-recommendations-gnulinux-system.

ANSSI-BP-028 (minimal)

이 프로파일은 ANSSI-BP-028 v2.0의 최소 하드닝 수준에 맞춰 구성된 설정을 포함합니다. ANSSI는 프랑스 국가 정보 보안 기관으로, “Agence nationale de la sécurité des systèmes d'information”을 의미합니다. ANSSI-BP-028은 GNU/Linux 시스템을 위한 설정 권장사항입니다. ANSSI-BP-028의 사본은 ANSSI 웹사이트에서 찾을 수 있습니다: https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-a-un-systeme-gnulinux/. 영어 버전도 ANSSI 웹사이트에서 찾을 수 있습니다: https://cyber.gouv.fr/publications/configuration-recommendations-gnulinux-system.

CIS Red Hat Enterprise Linux 8 벤치마크 Level 2 - 서버

이 프로파일은 Center for Internet Security®의 Red Hat Enterprise Linux 8 벤치마크™(v3.0.0, 2023-10-30 발표)에서 정의된 “Level 2 - Server” 구성과 일치하는 기준을 정의합니다. 이 프로파일은 CIS Red Hat Enterprise Linux 8 벤치마크™ 콘텐츠를 포함합니다.

CIS Red Hat Enterprise Linux 8 벤치마크 Level 1 - 서버

이 프로파일은 Center for Internet Security®의 Red Hat Enterprise Linux 8 벤치마크™(v3.0.0, 2023-10-30 발표)에서 정의된 “Level 1 - Server” 구성과 일치하는 기준을 정의합니다. 이 프로파일은 CIS Red Hat Enterprise Linux 8 벤치마크™ 콘텐츠를 포함합니다.

CIS Red Hat Enterprise Linux 8 벤치마크 Level 1 - 워크스테이션

이 프로파일은 Center for Internet Security®의 Red Hat Enterprise Linux 8 벤치마크™(v3.0.0, 2023-10-30 발표)에서 정의된 “Level 1 - Workstation” 구성과 일치하는 기준을 정의합니다. 이 프로파일은 CIS Red Hat Enterprise Linux 8 벤치마크™ 콘텐츠를 포함합니다.

CIS Red Hat Enterprise Linux 8 벤치마크 Level 2 - 워크스테이션

이 프로파일은 Center for Internet Security®의 Red Hat Enterprise Linux 8 벤치마크™(v3.0.0, 2023-10-30 발표)에서 정의된 “Level 2 - Workstation” 구성과 일치하는 기준을 정의합니다. 이 프로파일은 CIS Red Hat Enterprise Linux 8 벤치마크™ 콘텐츠를 포함합니다.

비연방 정보 시스템 및 조직의 비분류 정보(NIST 800-171)

NIST 800-171, Section 2.2에 따르면, 비연방 정보 시스템 및 조직에서 CUI(Controlled Unclassified Information)의 기밀성을 보호하기 위한 보안 요구사항은 다음과 같은 구조를 가집니다: (i) 기본 보안 요구사항 섹션, (ii) 파생된 보안 요구사항 섹션. 기본 보안 요구사항은 연방 정보 및 정보 시스템에 대한 고수준 및 기본 보안 요구사항을 제공하는 FIPS Publication 200에서 가져옵니다. 파생된 보안 요구사항은 NIST SP 800-53의 보안 통제에서 가져와 기본 보안 요구사항을 보완합니다. 이 프로파일은 Red Hat Enterprise Linux 8을 NIST SP 800-53에서 식별된 통제 기준에 맞춰 CUI를 보호합니다.

호주 사이버 보안 센터(ACSC) Essential Eight

이 프로파일은 Red Hat Enterprise Linux 8이 호주 사이버 보안 센터(ACSC) Essential Eight에 맞도록 설정 검사 내용을 포함합니다. Linux 환경에서의 Essential Eight 가이드는 ACSC 웹사이트에서 찾을 수 있습니다:
https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-linux-workstations-and-servers.

건강보험정보시스템 (HIPAA)

HIPAA 보안 규칙은 전자 건강 정보의 기밀성, 무결성 및 보안을 보호하기 위해 미국의 국가 표준을 정합니다. 보안 규칙은 전자적으로 보호된 건강 정보의 기밀성과 무결성을 보장하기 위한 적절한 관리적, 물리적 및 기술적 보호조치를 요구합니다. 이 프로파일은 전자적으로 보호된 건강 정보를 보호하기 위해 Red Hat Enterprise Linux 8을 HIPAA 보안 규칙에 맞춰 설정합니다. 이 프로파일을 사용한다고 해서 법적 HIPAA 보안 규칙 준수를 보장하거나 이에 대해 주장하지 않습니다.

호주 사이버 보안 센터(ACSC) ISM 공식

이 프로파일은 Red Hat Enterprise Linux 8이 호주 사이버 보안 센터(ACSC)의 정보 보안 매뉴얼(ISM)의 “공식” 등급에 맞도록 설정 검사 내용을 포함합니다. ISM은 사이버 보안에 대한 리스크 기반 접근 방식을 사용합니다. 이 프로파일은 조직의 보안 태세와 리스크 프로파일에 맞는 보안 통제를 선택하는 가이드를 제공합니다. ISM의 사본은 ACSC 웹사이트에서 찾을 수 있습니다:
https://www.cyber.gov.au/ism.

범용 운영체제 보호 프로파일

이 프로파일은 NIAP 보호 프로파일 버전 4.2.1에 따른 필수 설정 통제를 반영합니다. 이 설정 프로파일은 CNSSI-1253과 일치하며, 미국 국가 보안 시스템이 특정 구성 매개변수를 준수하도록 요구합니다. 따라서, 이 구성 프로파일은 미국 국가 보안 시스템에 적합합니다.

PCI-DSS v4.0 Red Hat Enterprise Linux 8에 대한 제어 기준

신용카드/결제기관 데이터 보안 표준(PCI-DSS)은 지불 카드 데이터의 안전한 처리를 보장하기 위해 설계된 일련의 보안 표준으로, 데이터 유출을 방지하고 민감한 금융 정보를 보호하는 것을 목표로 합니다. 이 프로파일은 Red Hat Enterprise Linux 8이 PCI-DSS v4.0 요구 사항에 맞게 구성되었는지를 보장합니다.

DISA STIG for Red Hat Enterprise Linux 8

이 프로파일은 Red Hat Enterprise Linux 8 V1R13에 대한 DISA STIG(Security Technical Implementation Guide)에 맞춰 구성된 설정 검사를 포함합니다. Red Hat Enterprise Linux 8뿐만 아니라, 이 구성 기준은 Red Hat Enterprise Linux 8 기반의 Red Hat 기술 운영 체제 계층에도 적용 가능합니다:

1. Red Hat Enterprise Linux Server
2. Red Hat Enterprise Linux Workstation 및 Desktop
3. Red Hat Enterprise Linux for HPC
4. Red Hat Storage
5. Red Hat Containers with a Red Hat Enterprise Linux 8 image

DISA STIG with GUI for Red Hat Enterprise Linux 8

이 프로파일은 Red Hat Enterprise Linux 8 V1R13에 대한 GUI(그래픽 사용자 인터페이스)를 포함한 DISA STIG에 맞춰 구성된 설정 검사를 포함합니다. Red Hat Enterprise Linux 8뿐만 아니라, 이 구성 기준은 Red Hat Enterprise Linux 8 기반의 Red Hat 기술 운영 체제 계층에도 적용 가능합니다:

1. Red Hat Enterprise Linux Server
2. Red Hat Enterprise Linux Workstation 및 Desktop
3. Red Hat Enterprise Linux for HPC
4. Red Hat Storage
5. Red Hat Containers with a Red Hat Enterprise Linux 8 image

경고: 그래픽 사용자 인터페이스(GUI)를 설치하고 사용하는 것은 공격 벡터를 증가시키고 전체 보안 태세를 약화시킵니다. 정보 시스템 보안 담당자(ISSO)가 GUI에 대한 문서화된 운영 요구 사항이 없는 경우, 표준 DISA STIG for Red Hat Enterprise Linux 8 프로파일을 사용하는 것을 고려하십시오.

From:
https://atl.kr/dokuwiki/ - **AllThatLinux!**

Permanent link:
https://atl.kr/dokuwiki/doku.php/openscap

Last update: **2025/06/09 02:08**