보안 및 컴플라이언스 개선을 위한 8가지 기술 팁

Red Hat® Enterprise Linux® 보안 및 컴플라이언스 기능을 활용하여 위험을 완화하고, 보안 구성과 정책을 시행하고, 조직의 컴플라이언스를 유지하세요.

1 표준 기반 컴플라이언스 설정 관리

시스템 전반의 암호화 정책은 인프라에 대한 표준 기반 컴플라이언스 설정을 일관성 있게 구현하고 유지 관리할 수 있는 방법을 제공합니다.

하나의 간소화된 명령으로 내장된 암호화 정책을 선택하여 시스템의 여러 애플리케이션 전반에 일관되게 적용할 수 있습니다. 또한 전문적인 규제 컴플라이언스 요구 사항이 있는 경우 조직의 목표를 충족하기 위해 사용자 정의 정책을 생성할 수 있습니다.

컴플라이언스 관리에 대해 자세히 알아보기

2 시스템 롤을 통한 보안 구성 자동화

Red Hat Ansible® Automation Platform으로 지원되는 Red Hat Enterprise Linux 시스템 롤을 통해 관리자는 자동화를 사용해 더 짧은 시간 내에 규모에 맞춰 보안 설정을 설치하고 관리할 수 있습니다.

시스템 롤은 다양한 풋프린트 전반에서 여러 개의 Red Hat Enterprise Linux 릴리스로 작업하도록 작성되므로 관리자는 Red Hat 솔루션을 위한 모범 사례를 사용할 수 있습니다. 하나의 명령 또는 워크플로우를 통해 새로운 보안 설정을 구성하여 모든 시스템에서 유지 관리할 수 있습니다.

보안 자동화에 대해 자세히 알아보기

3 인증 및 권한 부여 중앙화

Red Hat Enterprise Linux는 전체 데이터센터에 걸쳐 확장 가능한 단일 인터페이스를 사용하여 사용자를 인증하고 역할 기반 액세스 제어(RBAC)를 구현할 수 있는 중앙집중식 Identity 관리(IdM) 기능을 포함합니다. Red Hat Enterprise Linux의 Identity 관리는 표준 애플리케이션 프로그래밍 인터페이스(API)를 통해 Microsoft Active Directory, LDAP(Lightweight Directory Access Protocol), 그 밖의 타사 Identity 및 액세스 관리 솔루션과 통합됩니다.

또한 인증서 기반 인증 및 권한 부여 기술을 사용하여 중앙에서 서비스 인증과 권한 부여를 관리할 수 있습니다.

Identity 관리에 대해 자세히 알아보기

4 정책 사용자 정의

SELinux(Security-Enhanced Linux)는 Linux 커널에서 필수 액세스 제어(Mandatory Access Control, MAC)를 구현한 것입니다. Red Hat Enterprise Linux 컨테이너는 기본적으로 SELinux와 함께 실행됩니다. SELinux는 운영 체제(OS) 내에 추가 보안 계층을 포함하며 컨테이너가 시스템에서 벗어나 기본 호스트 OS 또는 다른 컨테이너를 덮어쓰는 것을 방지합니다. Udica를 통해 시스템 관리자와 컨테이너 개발자는 실행 중인 컨테이너를 분석하고 컨테이너별 SELinux 룰이 포함된 정책을 자동으로 생성할 수 있습니다. 따라서 정책 작성 절차가 간소화되고 슈퍼 사용자(superuser) 권한으로 컨테이너를 실행할 필요가 없어 위험이 줄어듭니다.

정책 잠금에 대해 실험하고 자세히 알아보기

5 시스템에 패치 적용 시 다운타임 최소화

Red Hat은 EUS(Extended Update Support) 릴리스에 대해 '매우 중요' 또는 '중요' 등급을 받은 일반적인 취약점 및 노출도(CVE)에 커널 실시간 패치를 추가 비용 없이 제공합니다. 커널 실시간 패치 적용(Kernel Live Patching, KLP)을 활용하면 실행 중인 커널에 패치를 적용하여 시스템을 재부팅하지 않고도 취약점을 즉시 해결함으로써 보안을 저해하지 않고 다운타임을 최소화할 수 있습니다.

KLP에 대해 실험하고 자세히 알아보기

6 규모에 따른 보안 및 컴플라이언스 관리

Red Hat Enterprise Linux 서브스크립션에 추가 비용 없이 포함되는 Red Hat Insights는 서비스로서의 소프트웨어(SaaS) 오퍼링이며, 배포를 위해 실행 가능한 보안 데이터를 제공합니다. 운영과 취약점에 관련된 위험을 찾아내 해결하고, 시스템을 더 빠르게 스캔하여 패치가 누락된 시스템을 식별하고, 가장 먼저 적용해야 할 중요 패치에 우선순위를 지정합니다. 단일 웹 인터페이스에서 모든 Red Hat Enterprise Linux 시스템에 걸쳐 보안 구성 정책을 생성, 수정, 구현, 유지 관리할 수 있습니다. 또한 Red Hat Smart Management 서브스크립션을 이용해 Red Hat Insights에서 문제 해결 계획을 실행, 확장, 자동화할 수 있습니다.

컴플라이언스에 대해 자세히 알아보기

7 시스템 활동을 기록하여 컴플라이언스 목표 달성 지원

Red Hat Enterprise Linux에는 세션 기록이 포함되어 있으며, 여기에서 제공되는 감사 및 로깅 기능을 활용하여 보안 관리자는 시스템에서 특정 사용자 그룹의 키보드 입력과 활동을 캡처할 수 있습니다. 이 데이터는 다른 모든 활동과 마찬가지로 시스템 저널 또는 로그 파일에 기록되며 재생 툴에 포함된 재생 및 일시 정지 기능을 사용해 분석하고 상관 관계를 파악할 수 있습니다.

세션 기록 실험하기

8 무단 애플리케이션 실행 방지

애플리케이션 허용 목록을 작성하면 잠재적 공격 벡터를 줄이고 악성 애플리케이션이 시스템에서 실행되지 않도록 방지할 수 있습니다. 파일 액세스 정책 데몬(fapolicyd)은 사용자가 승인된 실행 파일만 시스템에서 실행하도록 허용하는 내장형 애플리케이션 허용 목록 작성 기능을 제공합니다. 시스템 관리자는 기본 정책으로 fapolicyd를 구성하거나, 수정된 애플리케이션 또는 무단 애플리케이션이 실행되지 않도록 직접 빌드할 수 있습니다.

애플리케이션 허용 목록 작성 기능에 대해 자세히 알아보기

한국레드햇 홈페이지 https://www.redhat.com/ko

Red Hat 소개

Red Hat은 권위 있는 어워드를 수상한 지원, 교육, 컨설팅 서비스로 고객이 여러 환경에서 표준화를 진행하고, 클라우드 네이티브 애플리케이션을 개발하고, 복잡한 환경을 통합, 자동화, 보안, 관리할 수 있도록 지원합니다.

www.facebook.com/redhatkorea
구매문의 02-6105-4390
buy-kr@redhat.com

www.redhat.com/ko
O-F31208