개발자를 위한 DevSecOps 모범 사례

1 애플리케이션 종속성 위험 완화

관리해야 하는 애플리케이션을 빌드하는 데 사용되는 소프트웨어 구성 요소에는 취약점이 있을 수 있습니다. 특히 오픈소스 소프트웨어 구성 요소를 사용할 때 소프트웨어 구성 분석(SCA) 툴을 사용해 소프트웨어 공급망 위험을 완화할 수 있습니다. 다음 요건을 충족하는 SCA 툴을 찾아보세요.

- 애플리케이션 종속성을 검사하여 알려진 취약점이 없는지 확인할 수 있는 툴
- 구성 요소와 그 라이센스를 식별하여 호환되지 않을 수 있는 라이센스에 플래그를 지정함으로써 소프트웨어 라이센싱 컴플라이언스를 자동화할 수 있도록 지원할 수 있는 툴
- 애플리케이션 종속성이 있는지, 그리고 여전히 활성화되어 있고 업데이트를 산출하는 커뮤니티에서 종속성이 비롯된 것인지 확인할 수 있는 툴
- 애플리케이션 빌드 프로세스의 자동화된 일부일뿐 아니라 개발 환경의 일부인 툴 이 요건을 충족하는 경우 개발자는 통합 전에 문제를 해결할 수 있는 기회를 얻을 수 있고, 이로써 애플리케이션 빌드 실패 횟수를 줄일 수 있습니다.

2 코드와 구성 관리 통합

쿠버네티스와 컨테이너화된 환경에서 널리 사용되는 GitOps 패러다임에는 다음과 같이 개발 단계에서부터 보안 태세를 크게 개선할 수 있는 사례가 포함되어 있습니다.

- 소스 코드 관리(SCM)를 위한 개발 모범 사례를 구성에 적용 체크인, 병합, 승인에 대해 동일한 제어 기능을 사용하면 인프라 구성 변경 사항을 특정 개인 및 시간까지 추적할 수 있습니다.
- 개발자는 Ops에 의존하기보다는 프로세스 초기에 구성을 고려하고 애플리케이션이 의도하는 프로덕션 환경에 대한 비전을 확립해야 합니다. 개발, 테스트 및 프로덕션에 대해 동일한 유형의 환경과 보안 제어 기능을 사용하면 라이프사이클 전반에서 구성을 더 손쉽게 관리할 수 있습니다.
- 자동화된 빌드 파이프라인을 사용하여 지속적 통합/지속적 제공(CI/CD)을 위한 컨테이너 이미지 및 바이너리 아티팩트를 구성하세요. 이러한 이미지를 프로덕션으로 배포할 때 임시 변경이 필요해서는 안 됩니다.
- SCM 시스템에 민감한 데이터를 저장하지 마세요. 툴을 사용해 구성 및 컨테이너 이미지를 스캔하여 임베딩된 암호가 포함되어 있지 않은지 확인하세요.

3 애플리케이션 암호 보호

애플리케이션 라이프사이클 전반에서 비밀번호, 토큰, 키와 같은 Identity 및 암호를 관리하는 것이 중요합니다. SCM 시스템, 컨테이너 레지스트리, 바이너리 리포지토리에 대한 액세스 권한을 제어해야 합니다. 애플리케이션이 데이터베이스와 서비스에 액세스하기 위해 사용하는 자격 증명과 자동화된 빌드 및 테스트 프로세스에 필요한 자격 증명도 보호해야 합니다. SCM 시스템이나 구성 파일에 저장된 암호는 사고로 인해 유출될 수 있습니다. 애플리케이션 암호를 보호하는 방법은 다음과 같습니다.

- Identity 관리 및 액세스 제어 인프라를 라이프사이클 초기에 확립합니다.
- 암호 저장소 또는 하드웨어 보안 모듈(HSM)을 사용해 유휴 상태 및 전송 중인 암호를 관리하고 보호하는 방법을 고려합니다. 암호 저장소는 일반적으로 소프트웨어 솔루션인 반면, HSM은 향상된 보호 수준을 제공하기 위한 특수 하드웨어를 사용합니다. 둘 중 어느 것이든 Identity 관리 인프라에 통합되어야 합니다.

4 신뢰할 수 있는 기본 이미지 사용

컨테이너 기본 이미지는 고도로 최소화된 Linux® 배포판입니다. 수백 개의 패키지는 미리 설치할 수 있고 잠재적인 취약점을 포함할 수 있습니다. 컨테이너 이미지 위험을 완화하는 방법은 다음과 같습니다.

- 신뢰할 수 있고, 정기적이며, 충실한 테스트를 거친 업데이트가 포함된 신뢰할 수 있는 이미지를 선택합니다. 이미지 소스와 사용 가능한 지원 옵션을 조사합니다.
- 이미지 툴을 사용해 알려진 취약점이 있는지 확인합니다. 이미지도 스캔하여 구성이 보호되고 있는지, 임베딩된 암호는 없는지 확인해야 합니다.
- 익스플로잇 중에 사용될 수 있는 불필요한 바이너리(운영 체제(OS) 툴 포함)를 제거하여 공격 벡터를 줄입니다.

5 컴플라이언스 및 감사 관련 고려 사항을 조기에 해결

프로덕션 단계로 이동할 때 지연을 줄이려면 개발 단계 초기에 필요한 컴플라이언스 프레임워크와 기술 제어에 대해 이해하는 것이 중요합니다. 컴플라이언스 및 보안 요구 사항 이행을 위한 자동 점검을 빌드 파이프라인에 삽입할 수 있습니다.

절차 및 정책에 대한 도큐멘테이션이 감사의 50% 이상을 차지할 수 있으므로 적극적으로 문서화를 시작하세요. 정책 도큐멘테이션에는 액세스 제어, 변경 제어, 백업, 데이터 보존이 포함되어야 합니다. 절차를 문서화할 때 애플리케이션 보안 테스트 및 SCA와 같은 보안 점검이 포함되어야 합니다.

6 강력한 플랫폼 및 에코시스템으로 시작

보안 위협이 지속적으로 증가함에 따라 지원되는 통합 솔루션을 제공하는 통합 보안 에코시스템이 포함된 플랫폼을 사용하는 것이 필수적입니다. Red Hat® OpenShift®는 개발뿐 아니라 운영도 지원하는 광범위한 기능이 포함된 엔터프라이즈급 쿠버네티스 플랫폼입니다. Red Hat OpenShift의 강력한 빌드 및 배포 파이프라인은 자동화된 보안 점검 및 제어를 구현할 수 있는 이상적인 장소를 제공합니다. 보안 점검은 이미지로 소스 코드를 빌드하는 단계에서 프로덕션 배포 단계에 이르기까지 프로세스의 모든 단계에 삽입할 수 있습니다.

Red Hat은 Red Hat OpenShift에서 보안 기능을 강화하고 확장하는 보안 파트너 에코시스템을 보유하고 있습니다. 이들 파트너는 Red Hat과 협력하여 Red Hat OpenShift과 통합되는 지원되는 솔루션을 제공합니다. 다양한 솔루션 중에서 특정 보안 및 조직 요구 사항에 부합하는 것을 선택하실 수 있습니다.

Red Hat CodeReady Workspaces는 컨테이너 기반 애플리케이션 개발을 가속화하기 위해 Red Hat OpenShift에서 실행되는 쿠버네티스 네이티브 개발 환경입니다. Red Hat Universal Base Images와 Red Hat Runtimes는 신뢰할 수 있는 소스로 구축된 강력한 기반을 애플리케이션에 제공합니다.

Red Hat DevSecOps 프레임워크

보안 라이프사이클에 대한 전체 뷰를 확보하고 개발 보안 기능과 Red Hat DevSecOps 프레임워크이 서로 얼마나 잘 부합하는지 확인하세요. red.ht/DevSecOps를 방문하세요.

개발 보안 솔루션 찾기

Red Hat과 Red Hat 보안 파트너가 제공하는 웨비나를 시청하여 애플리케이션 라이프사이클 전반에서 보안을 구현하는 방법을 알아보세요.

한국레드햇 홈페이지 https://www.redhat.com/ko

Red Hat 소개

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

www.facebook.com/redhatkorea
구매문의 080 708 0880
buy-kr@redhat.com

www.redhat.com/ko
#F29682_0921