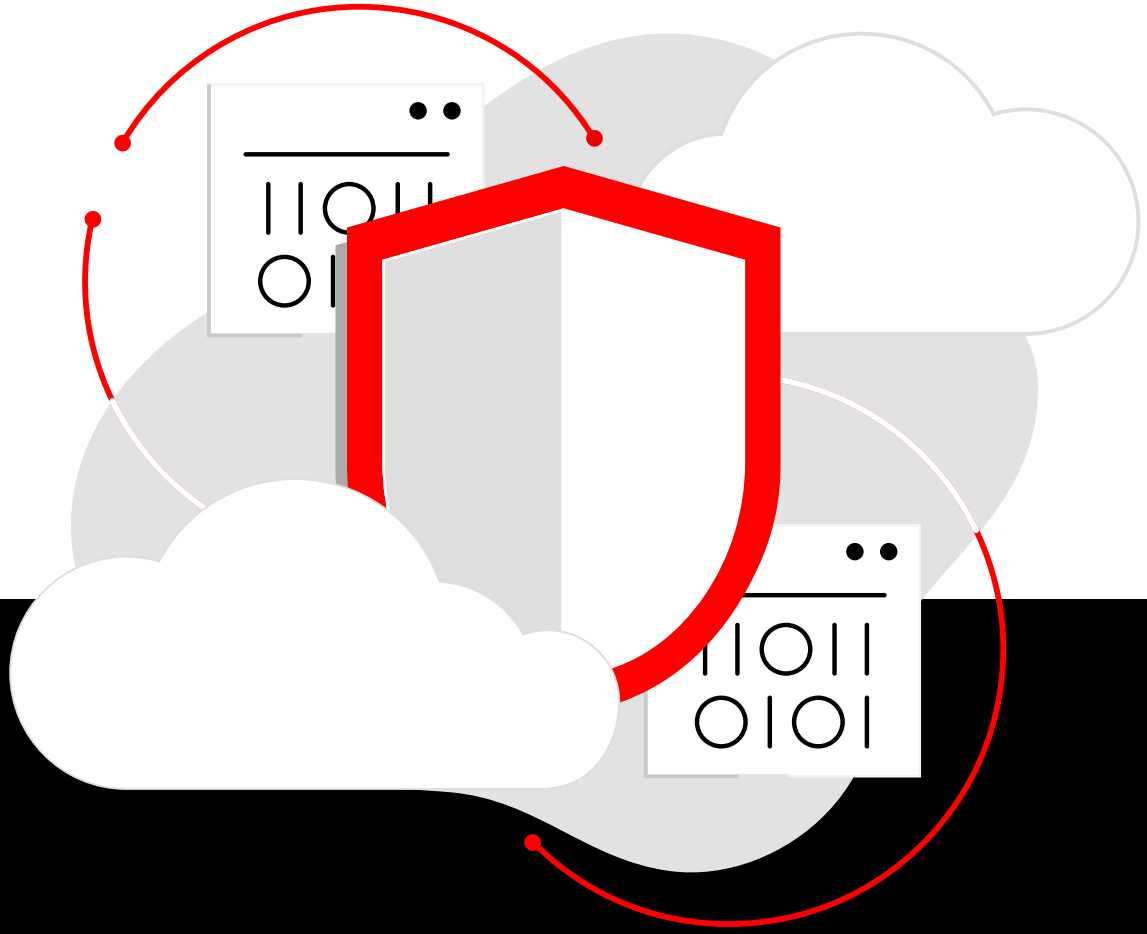
Red Hat



DevSecOps로 애플리케이션 라이프사이클을 현대화하고 보호하기

목차

소개

디지털 환경에서 매우 중요한 애플리케이션 보안

점점 더 많은 조직이 디지털 환경에서 경쟁하기 위해 클라우드, 컨테이너, 마이크로서비스 기술을 도입함에 따라 보안은 여전히 최우선 과제로 남아 있습니다. 실제로 기업의 고위 IT 리더 중 50%가 기술 이니셔티브를 위한 3대 주요과제로 사이버 보안을 꼽고 있습니다.[1] 이와 동시에 86%는 2021년에 조직의 디지털 트랜스포메이션 속도가 증가할 것으로 예상하고 있습니다.[1]

분산 환경에서 기존의 경계 기반 접근 방식은 효과적이지 않기 때문에 이러한 새로운 기술은 보안에 대한 다른 접근 방식을 취해야 합니다. 또한 DevOps와 클라우드 네이티브 방법론을 사용하면 개발 속도와 배포 유연성이 증가하므로 프로세스 초기에 보안을 고려하는 것이 중요합니다. 개발 주기 종료 시점에만 보안 조치를 적용하면 제공이 지연되고 보호 기능이 저하되는 경우가 많습니다.

DevSecOps 접근 방식과 사례를 도입하면 애플리케이션 환경과 비즈니스를 더 효과적으로 보호할 수 있습니다.

DevSecOps란?

DevSecOps는 DevOps의 협업 문화를 확장하여 애플리케이션 라이프사이클 전체에 걸쳐 보안을 통합합니다. 여기에는 분산된 환경에 더욱 광범위하게 보안을 적용할 수 있도록 하는 인력, 프로세스, 기술이 모두 포함됩니다.

DevSecOps를 통해 보안은 한 팀이 소유하고 개발과 배포 프로세스 종료 시에 적용되는 일련의 태스크가 아니라 여러 팀 전반에 공유되는 책임이 됩니다. 따라서 보안, 개발, 운영 팀의 인력이 협력하여 정보, 피드백, 지식, 인사이트를 공유합니다. 이러한 접근 방식을 통해 애플리케이션 개발과 인프라 배포 시작 시점부터 보안을 통합하여 보호 성능을 강화하고 리스크를 줄일 수 있습니다.

DevSecOps의 장점

보안을 강화하고 위험 완화

프로덕션이 아닌 개발 단계에서 보안 문제를 해결하여 애플리케이션 보호를 강화하고 실패한 정책 점검으로 인해 지연되거나 중단되는 배포의 수를 줄입니다.

보안 문제를 더 빠르게 해결

협업을 장려하고 자동화를 통합하여 릴리스 주기를 가속화하고, 프로덕션 환경에서 보안 문제를 해결하는 데 필요한 시간을 줄이고, 시간과 비용을 절약하는 현대적인 보안 사례와 툴을 적용합니다.

컴플라이언스와 가시성 향상

수작업에 따른 오류의 위험을 줄이고 예측 가능성과 반복 가능성을 높이는 자동화된 프로세스와 툴을 도입하여 컴플라이언스를 개선하고 감사 프로세스를 간소화합니다.

1 *Flexera. "2021년 기술 지출 현황 Flexera 보고서(2021 Flexera State of Tech Spend Report)," 2021년 1월.*

DevSecOps 구현에 따르는 과제

DevSecOps 접근 방식은 여러 가지 장점을 제공하지만 몇 가지 요인으로 인해 DevSecOps 구현이 어려워질 수 있습니다.

- **보안 환경 진화.** 비즈니스, 기술, 지리적 요구 사항을 비롯한 보안 위협과 규제는 빠른 속도로 변화하고 있어 항상 최신 상태를 유지하기가 어렵습니다.
- **복잡한 애플리케이션 환경.** 컨테이너, 마이크로서비스, 클라우드 서비스 등 대규모의 복잡한 애플리케이션 환경을 구성하는 다양한 모든 기술의 연결과 보안이 미치는 영향을 이해하기 어려울 수 있습니다.
- **비효율적인 기존 툴과 프로세스.** 많은 팀이 기존 툴과 프로세스를 DevSecOps 이니셔티브에 적용하는 것으로 시작하지만 시간이 지남에 따라 이 접근 방식이 목표를 지원하지 않는다는 것을 알게 됩니다.
- **여러 가지 보안 툴.** 조직에 적합한 보안 툴을 선택, 테스트, 통합, 유지 관리하려면 시간, 연구, 그리고 지속적인 노력이 필요합니다.

문화, 프로세스, 기술에 따라 좌우되는 DevSecOps의 성공 여부

DevSecOps로 애플리케이션 라이프사이클의 보안을 유지하려면 문화, 프로세스, 기술의 세 가지 영역에서 변경과 조정이 필요합니다.

문화

개발, 운영, 보안 팀 전반에서 협업과 공유 목표를 촉진합니다. 각 팀이 애플리케이션 라이프사이클에 보안을 구축해야 하는 이유와 방법을 이해할 수 있도록 지원합니다.

프로세스

프로세스와 워크플로우를 표준화, 문서화, 자동화하여 애플리케이션 라이프사이클 전반에서 효율성을 높이고 보안을 강화합니다.

기술

애플리케이션 개발, 배포, 운영 플랫폼, 툴, 프로세스를 통합된 단일 시스템으로 결합합니다.

DevSecOps의 기본 사항에 대해 자세히 알아보기

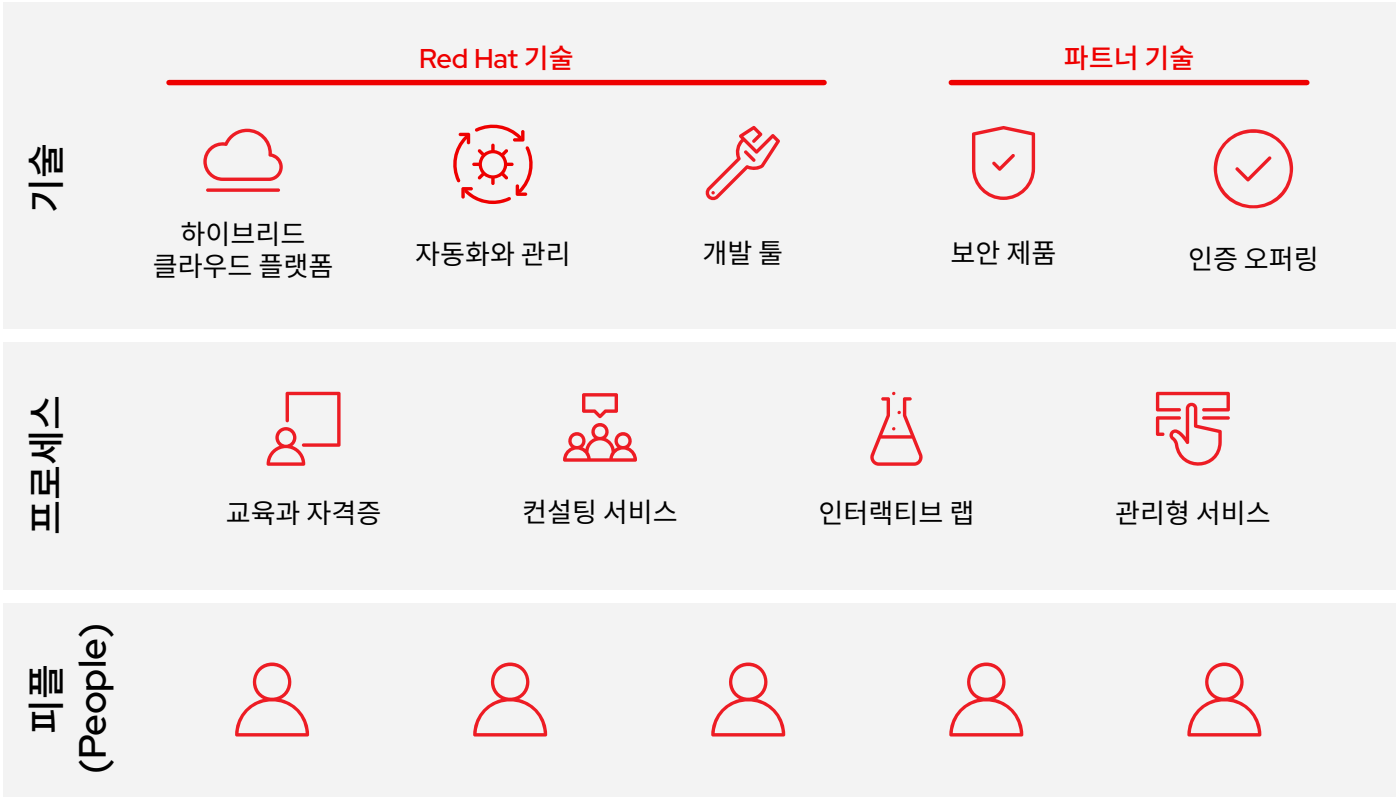
귀사의 DevSecOps 사례가 부족한 이유 블로그 포스트를 읽고 DevSecOps를 성공적으로 구현하는 데 필요한 변경 사항에 대해 자세히 알아보세요. **하이브리드 클라우드 보안 강화 e-book**을 읽고 클라우드 네이티브 보안 접근 방식으로 비즈니스를 보호하는 방법에 대해 알아보세요.

Red Hat DevSecOps 전략

Red Hat은 인증된 파트너 에코시스템, 광범위한 전문성, 혁신적인 플랫폼을 통해 하이브리드 클라우드 환경 전반의 애플리케이션을 빌드, 보호, 배포합니다. 이 조합을 통해 통합적인 DevSecOps 솔루션을 구현하여 애플리케이션 보안을 강화하고, 위험을 줄이고, 성능을 향상하고, 투자 가치를 극대화할 수 있습니다.

신뢰할 수 있는 콘텐츠 공급망, 전담 보안 팀의 지원, 주요 보안 기능 백포트를 통해 Red Hat® 플랫폼은 DevSecOps 솔루션에 이상적인 기반을 제공합니다. Red Hat 파트너는 애플리케이션 라이프사이클 전반에서 보안과 자동화를 적용하기 위한 혁신적인 통합 제품으로 이 기반을 확장하고 향상합니다. 끝으로 Red Hat은 **교육 및 자격증 과정**, **인터랙티브 랩**, **컨설팅 서비스**, **관리형 제품**을 제공하여 DevSecOps를 성공적으로 구현할 수 있도록 지원합니다.

Red Hat은 협력을 통해 DevSecOps 여정의 모든 단계에서 조직을 지원합니다. Red Hat의 확장 가능한 모듈식 솔루션과 전문 서비스를 통해 지금 바로 필요한 솔루션을 배포하고 향후 변화에 맞춰 조정할 수 있으며, 효율적이고 효과적인 DevSecOps 도입에 필요한 다양한 방법과 접근 방식을 익힐 수 있습니다.



Red Hat 제품으로 개방형 DevSecOps 기반 구축

Red Hat OpenShift

Red Hat OpenShift®는 엔터프라이즈 수준의 보안 중심 하이브리드 클라우드 플랫폼으로서, 기본적으로 지원되는 빌트인 DevOps 툴과 보안 기능이 포함되어 있습니다. 이 플랫폼은 파트너와 타사의 보안 툴, 기술과 연동되어 보안을 강화하고 강력한 DevSecOps를 구현합니다. **Red Hat OpenShift 보안 가이드**를 읽고 기술 스택 전반에서 보안을 시행하는 방법을 알아보세요.

주요 보안 기능

- SELinux(Security-Enhanced Linux)
- 보안 컨텍스트 제한 조건(SCC)
- Identity 및 액세스 관리
- 데이터 암호화
- 연방 정보 처리 표준(FIPS) 모드

무료 체험하기

Red Hat Ansible Automation Platform

Red Hat Ansible® Automation Platform은 보안 솔루션을 자동화하고 통합할 수 있는 유연하고 강력한 플랫폼으로서, 여러 보안 툴에서 사용할 수 있는 공통 언어를 제공합니다. **자동화 활용 사례**에 대해 알아보세요.

Red Hat Enterprise Linux CoreOS

Red Hat Enterprise Linux® CoreOS는 변경 불가능한 경량화 컨테이너 최적화 운영 체제로서, Red Hat Enterprise Linux의 보안 중심 기반에 바탕을 두고 있으며 Red Hat OpenShift 내에서 사용됩니다.

Red Hat Quay

Red Hat Quay는 컨테이너를 빌드, 분산, 배포할 수 있도록 지원하는 분산된 고가용성 컨테이너 이미지 레지스트리입니다.

Red Hat CodeReady Workspaces

Red Hat CodeReady Workspaces는 개발자가 Red Hat OpenShift에서 실행되는 컨테이너에서 코딩, 빌드, 테스트할 수 있도록 지원하는 툴입니다.

Red Hat Advanced Cluster Security for Kubernetes

Red Hat Advanced Cluster Security for Kubernetes는 빌드 단계에서 런타임까지 애플리케이션을 보호하는 컨테이너 보안을 위해 클라우드 네이티브 아키텍처를 제공합니다.

Red Hat Advanced Cluster Management for Kubernetes

Red Hat Advanced Cluster Management for Kubernetes는 빌트인 된 보안 정책을 갖춘 단일 콘솔에서 클러스터와 애플리케이션을 제어합니다.

인증된 보안 파트너 에코시스템으로 유연성과 신뢰성 확보

어떤 단일 벤더도 효율적인 DevSecOps를 완전히 구현하는 데 필요한 모든 기능을 제공하지는 않습니다. 또한 각 조직은 서로 다르며 조직의 요구 사항을 충족하려면 여러 제품과 기술을 고유한 방식으로 조합해야 합니다.

Red Hat은 **업계를 선도하는 혁신적인 보안 파트너**와 협업하여 인증된 통합, 컨테이너 이미지, **Red Hat OpenShift 오퍼레이터**에 기반을 둔 완벽한 솔루션을 제공합니다. 항상 귀사의 요구 사항에 가장 적합한 파트너, 제품, 기술을 선택할 수 있으며, 이러한 요소가 안정적이고 일관된 방식으로 함께 작동할 것이라는 확신을 가질 수 있습니다. 또한 이러한 솔루션은 전문가 서비스, 지원, 교육을 통해 지원되어 DevSecOps 문화, 프로세스, 툴을 성공적으로 구현하는 데 도움이 됩니다.

Red Hat 보안 파트너 에코시스템의 장점

선택

항상 조직의 요구 사항을 가장 잘 충족하는 제품과 벤더를 선택할 수 있습니다.

인증

모든 구성 요소가 서로 안정적으로 연동된다는 인증을 받았으므로 안심하고 솔루션을 구축할 수 있습니다.

전문성

Red Hat과 파트너의 통합 DevSecOps 전문성과 경험을 활용할 수 있습니다.

서비스

조직 내에서 DevSecOps 문화, 프로세스, 툴을 구현하기 위한 지원을 받을 수 있습니다.

교육

모범 사례에 대해 알아보고 DevSecOps 접근 방식을 도입하는 데 필요한 기술을 획득할 수 있습니다.

Red Hat Vulnerability Scanner Certification

Red Hat Vulnerability Scanner Certification은 취약점 스캐너 결과 사이의 불일치를 최소화합니다. Red Hat은 인증된 보안 파트너와 협력하여 Red Hat이 게시한 이미지와 패키지에 대해 더 정확하고 신뢰할 수 있는 컨테이너 취약점 스캐닝 결과를 제공합니다.

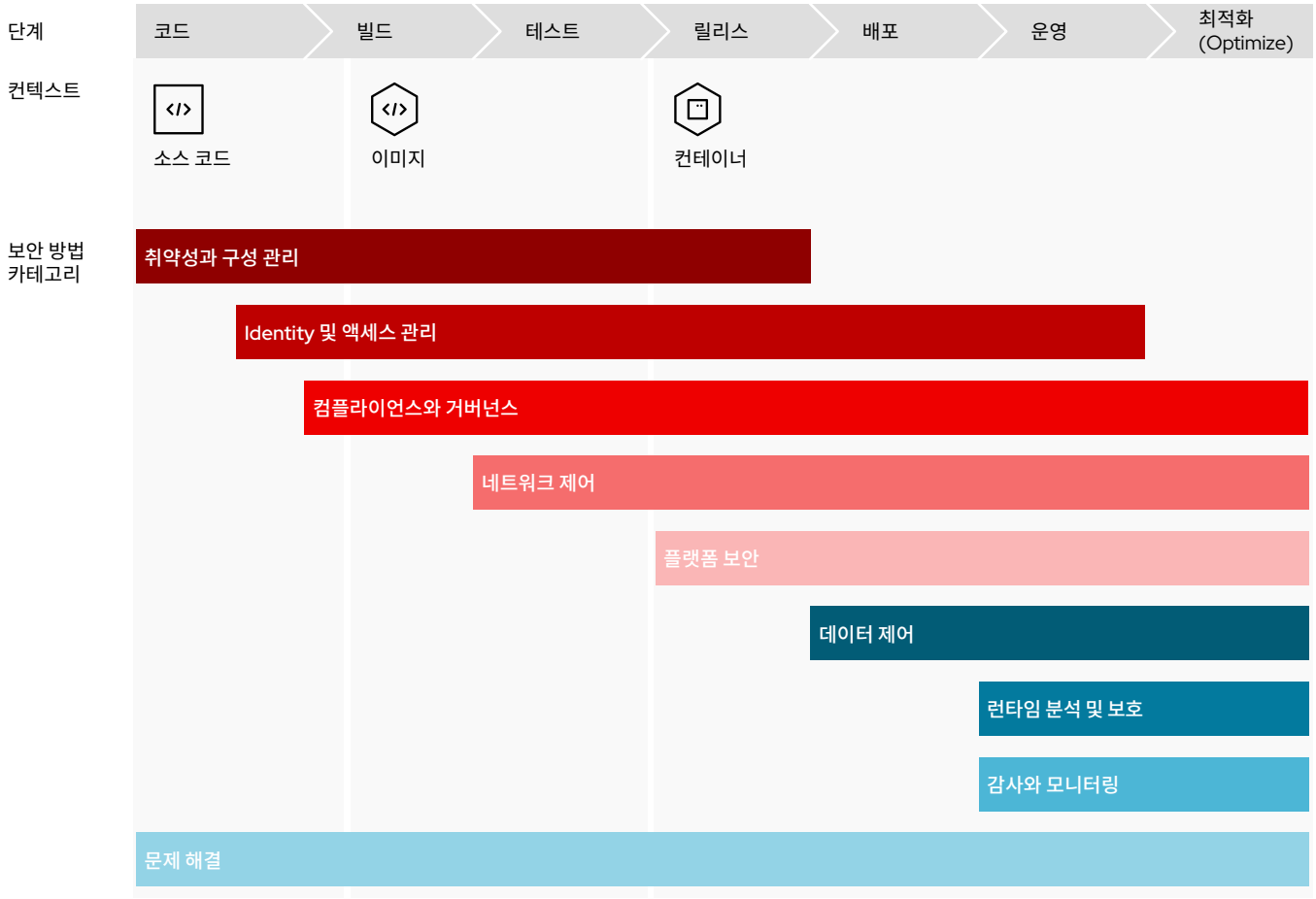
- 오탐과 기타 불일치를 최소화합니다.
- 전략적 프로젝트와 이니셔티브에 더 많은 시간과 예산을 할애할 수 있습니다.
- 더 높은 수준의 보증을 확보합니다.
- Red Hat이 게시한 이미지에 대한 중앙화된 데이터로 정확성을 향상합니다.
- 취약점 관리를 간소화합니다.

인증 제품 찾기

완벽한 DevSecOps 솔루션 생성

Red Hat은 애플리케이션 라이프사이클 전체에서 보안 요구 사항을 해결하는 고가용성의 통합 DevSecOps 솔루션을 구축할 수 있는 프레임워크를 제공합니다. Red Hat의 보안 파트너와 함께 생성한 이 프레임워크를 통해 현재는 물론 예상되는 요구 사항에 따라 조직 내에서 DevSecOps를 구현할 수 있습니다.

Red Hat DevSecOps는 기능에 따라 범주화된 일련의 통합 보안 툴과 방법을 애플리케이션 개발 라이프사이클로 매핑합니다.



개요 읽기

요구 사항에 적합한 보안 방법과 제품 선택

Red Hat DevSecOps 프레임워크는 34개의 기본 보안 방법을 9개의 범주로 체계화합니다. Red Hat과 인증 파트너 기술은 이러한 방법을 한 개 이상 연계하여 조직의 요구 사항을 충족하고 향후 변화에 적응하는 완벽한 DevSecOps 솔루션을 구축할 수 있도록 지원합니다.

취약성과 구성 관리

- 정적 애플리케이션 보안 테스트(SAST)
- 정적 코드 분석(SCA)
- 양방향 애플리케이션 보안 테스트(IAST)
- 동적 애플리케이션 보안 테스트(DAST)
- 구성 관리
- 이미지 리스크

Identity 및 액세스 관리

- 인증
- 권한 부여
- 암호 저장소
- 하드웨어 보안 모듈(HSM)
- 출처

컴플라이언스와 거버넌스

- 규제 컴플라이언스 감사
- 컴플라이언스 제어와 문제 해결

네트워크 제어

- 컨테이너 네트워크 인터페이스(CNI) 플러그인
- 네트워크 정책
- 트래픽 제어
- 서비스 메쉬
- 시각화
- 패키지 분석
- 애플리케이션 프로그래밍 인터페이스(API) 관리

플랫폼 보안

- 보안 호스트
- 컨테이너 플랫폼
- 네임스페이스
- 격리
- 쿠버네티스와 컨테이너 강화

데이터 제어

- 데이터 보호와 암호화

런타임 분석 및 보호

- 권한 컨트롤러
- 애플리케이션 동작 분석
- 위협 방어

감사와 모니터링

- 클러스터 모니터링
- 보안 정보와 이벤트 관리(SIEM)
- 포렌식

문제 해결

- 보안 오케스트레이션, 자동화 및 대응(SOAR) 플랫폼
- 자동 해결

인증 파트너 찾기

주요 파트너

Sysdig

Sysdig는 조직이 보안 중심 DevOps 기술을 이용해 클라우드에서 워크로드를 안심하고 실행할 수 있도록 지원합니다. 애플리케이션, 워크로드, 컨테이너를 모니터링하고 보호하기 위한 Sysdig의 제품을 활용하여 수백 개의 기업이 클라우드 네이티브 애플리케이션을 더 빠르게 배송할 수 있습니다.

Red Hat과 Sysdig는 협력을 통해 기업이 클라우드 네이티브 접근 방식을 신속하게 도입할 수 있도록 지원합니다. **Sysdig Secure DevOps Platform**, **Sysdig Secure**, **Sysdig Monitor**는 Red Hat OpenShift, **Red Hat Advanced Cluster Management for Kubernetes**와 연동해 프라이빗, 하이브리드, 멀티클라우드 환경에 대한 통합 보안, 컴플라이언스, 모니터링 기능을 제공합니다. 이러한 솔루션을 통해 빌드 파이프라인 보호, 위협 감지와 대응, 클라우드 태세와 컴플라이언스의 지속적 검증, 성능 모니터링 등의 작업을 수행할 수 있습니다. 오픈소스 스택 기반으로 구축된 Sysdig의 클라우드 네이티브 모니터링, 보안, 포렌식 기능은 더 적은 위험으로 클라우드를 이동할 때 필요한 인사이트와 제어 기능을 제공합니다.

Red Hat과 Sysdig 솔루션을 통해 다음과 같은 장점을 누릴 수 있습니다.

- 지속적 통합/지속적 배포(CI/CD) 파이프라인 내부의 이미지를 직접 스캔
- 클라우드 규모로 성능과 가용성 모니터링
- 지속적인 컴플라이언스와 런타임 보안 구현
- Red Hat OpenShift 인프라 구성 검증
- 더 손쉽게 문제를 트러블슈팅하고 대응

2020

공공 부문 올해의 Red Hat 라이징 스타(Rising Star) 파트너[2]

보안 위험 관리

파이프라인 전체에서 취약점을 식별하고 해결합니다. 자동화된 정책과 제어로 런타임 시 위협을 감지하고 차단합니다. 컨테이너가 사용 종료된 후에도 인시던트에 대응하고 조사합니다.

성능과 가용성 증진

수백만 개의 메트릭을 조사하고 유지합니다. 환경 전반에서 상태와 성능을 모니터링하여 문제를 사전 예방적으로 찾아 해결합니다. 클러스터, 포드, 컨테이너 내부의 문제를 더 쉽게 트러블슈팅합니다.

클라우드 컴플라이언스 검증

공통 표준으로 Red Hat OpenShift 환경 컴플라이언스를 검증합니다. 상세 활동 리포트를 통해 클러스터, 노드, 컨테이너를 감사합니다. 컨테이너 라이프사이클 전반에서 파일 무결성 모니터링을 구현합니다.

통합에 액세스

2 Red Hat 블로그. "**Red Hat, 오픈소스 혁신에 공헌한 북미 파트너에게 어워드 수여(Red Hat awards North American partners for commitment to open source innovation)**," 2020년 4월 23일.

주요 파트너

Synopsys

Synopsys는 보안 소프트웨어를 신속하게 빌드할 수 있도록 정적 소프트웨어 구성과 다이나믹 분석 솔루션을 제공합니다. Synopsys는 업계를 선도하는 툴, 서비스, 전문성을 조합하여 조직이 DevSecOps를 적용해 소프트웨어 개발 라이프사이클 전체에서 보안과 품질을 최적화할 수 있도록 지원합니다.

Red Hat과 Synopsys를 통해 고품질의 보안 중심 코드를 생성하여 리스크를 최소화하고 속도와 생산성을 극대화할 수 있습니다. **Synopsys Black Duck 소프트웨어 구성 분석(SCA)**은 Red Hat OpenShift와 통합되어 컨테이너 내부의 오픈소스 코드에서 보안 취약점과 정책 위반에 대한 가시성과 제어 능력을 향상합니다. **Black Duck for OpenShift**는 Red Hat OpenShift 클러스터에서 모든 컨테이너 이미지를 자동으로 검색, 스캔, 모니터링, 검사하여 컨테이너 구성의 모든 단계에서 오픈소스 보안과 컴플라이언스 관련 리스크를 식별합니다. 또한 이 소프트웨어를 통해 취약한 컨테이너가 프로덕션으로 푸시되지 않도록 하고 실행 중인 컨테이너에 영향을 미치는 새로운 취약점에 신속히 대응할 수 있습니다.

Black Duck for OpenShift 솔루션의 장점은 다음과 같습니다.

- 각 컨테이너 이미지에서 모든 타사 오픈소스 코드의 전체 목록을 제공하고취약점과 정책 메타데이터로 포드에 주석을 추가할 수 있습니다.
- 컨테이너에 영향을 미치는 새로운 취약점에 대해 즉시 알리고 영향을 받는 이미지와 컨테이너를 식별할 수 있습니다.
- 오픈소스 포크와 백포트를 이해하고 적절한 경우 취약점을 '패치됨'으로 표시하여 조사가 필요한 취약점의 수를 줄일 수 있습니다.
- Red Hat Advanced Cluster Management for Kubernetes와 **통합**되어 모든 클러스터에서 일관된 배포를 보장할 수 있습니다.

컨테이너 이미지를 자동으로 스캔

오픈소스 코드를 지속적으로 모니터링

보안 취약점 식별

"Synopsys와 Red Hat은 보안 애플리케이션 개발과 배포의 미래에 대해 유사한 비전을 공유하고 있으며, 함께 조직이 컨테이너화된 애플리케이션에 대한 신뢰를 구축하도록 도울 수 있기를 기대합니다."

Vatsal Sonecha
Synopsys 비즈니스 개발 부문 부사장

통합에 액세스

주요 파트너

Palo Alto Networks

Palo Alto Networks는 변화 속도가 빨라진다 해도 혁신을 제공하여 안전한 디지털 트랜스포메이션을 지원합니다. 이 회사는 전 세계 60,000명 이상의 고객이 비즈니스를 보호할 수 있도록 지원하는 보안 솔루션 포트폴리오를 제공합니다.

Red Hat과 Palo Alto Networks는 개발 라이프사이클 전체에 걸쳐 클라우드 네이티브 보안과 컴플라이언스를 통해 환경을 보호할 수 있도록 지원합니다. Palo Alto Networks의 Prisma Cloud는 Red Hat OpenShift와 연동해 배포를 위한 통합 클라우드 보안 태세 관리(CSPM)와 클라우드 워크로드 보호(CWP)를 제공합니다. 이 솔루션은 호스트, 컨테이너, 서버리스를 위한 완벽한 라이프사이클 보안을 제공하며 보안 태세에 대한 가시성과 거버넌스도 제공합니다.

Red Hat 파트너십 체결:

2017

주요 특징 및 장점

취약성 관리

애플리케이션 라이프사이클의 모든 단계에서 취약점 감지, 이해, 방지를 통해 개발에서 프로덕션 단계에 이르기까지 보안을 포함합니다.

컴플라이언스

CIS(Center for Internet Security) 벤치마크, 외부 컴플라이언스 체제, 사용자 정의 요구 사항에 대한 컴플라이언스를 손쉽게 구현하고 유지 관리합니다.

CI/CD 보안

프로덕션으로 배포되기 전에 지속적 통합(CI) 프로세스로 보안을 직접 통합하여 문제를 찾아 해결합니다.

런타임 방어

모든 애플리케이션 버전을 위한 최소 권한의 허용 목록 기반 런타임 모델을 자동으로 생성하는 머신 러닝으로 보안을 규모에 맞게 적용합니다.

웹 애플리케이션과 인터페이스 보안

퍼블릭, 프라이빗 클라우드 환경 전반에서 계층 7과 Open Web Application Security Project(OWASP) 상위 10개 위협에 맞서 보호합니다.

액세스 제어

워크로드와 애플리케이션에 대한 액세스 제어를 확립하고 모니터링하는 동시에 기존 Identity, 액세스, 암호 관리 툴과 통합합니다.

통합에 액세스

주요 파트너

CyberArk

CyberArk는 Identity 기반의 권한 있는 액세스 제어에 대해 고유한 보안 우선 접근 방식을 적용합니다. 이 회사는 엔터프라이즈, 클라우드, DevOps 환경 전반에서 사람, 애플리케이션, 스크립트, 머신이 사용하는 암호와 자격 증명을 보호할 수 있는 완벽한 솔루션을 제공합니다.

Red Hat과 CyberArk는 협력을 통해 컨테이너 환경과 자동화 스크립트의 보안을 강화하도록 지원합니다. 전사적인 권한이 있는 액세스 보안 정책은 가시성, 감사, 실행, 기밀 정보 관리를 제공하여 비즈니스 리스크를 완화합니다. **Conjur Secrets Manager**와 **Credential Providers**를 포함한 CyberArk DevSecOps 제품은 Red Hat OpenShift, Red Hat Ansible Automation Platform과 통합되며, 중앙집중식 플랫폼을 사용해 사람, 애플리케이션, 스크립트, 기타 비인간 Identity를 위한 권한 있는 자격 증명을 보호, 교체, 모니터링, 관리합니다. 조직 전반의 단일 제어 지점을 이용해 보안 관리를 통합하고, 보안 취약점을 줄이고, 공격 표면을 최소화하고, 운영을 간소화할 수 있습니다.

모듈식 아키텍처를 사용해 각 구성 요소를 독립적으로 배포하여 하이브리드 클라우드, 멀티클라우드, 컨테이너화, DevOps 환경 전반에서 보호를 사용자 정의할 수 있습니다. 강력한 런타임 인증과 역할 기반 액세스 제어는 승인된 포드와 컨테이너만 암호를 수신하도록 보장합니다. Red Hat Ansible Automation Platform과의 통합을 통해 플레이북은 관리되는 암호에 액세스하고, 수동으로 암호를 입력하고 교체할 필요성을 없앨 수 있습니다. 이러한 통합을 통해 감지된 보안 인시던트에 대응하여 문제 해결 태스크를 자동화할 수 있습니다.

보안 통합

정책에 따라 인프라 전반에서 암호와 권한 있는 액세스 자격 증명을 중앙에서 관리하고 보호합니다.

운영 간소화

개발자와 자동화 엔지니어가 정책에 근거하여 사용하는 암호와 자격 증명을 보호, 관리, 교체할 수 있습니다.

일관성 향상

관리 콘솔에 액세스하는 애플리케이션, 스크립트, 사람이 사용하는 암호와 자격 증명을 일관성 있게 보호합니다.

웨비나 보기

주요 파트너

Tigera

Tigera는 기업의 쿠버네티스 네트워킹과 마이크로서비스 통신의 보안을 유지하고, 관찰하고, 트러블슈팅하는 방식을 혁신합니다.

Red Hat과 Tigera는 조직이 네트워크 트래픽을 모니터링, 분석, 관리하여 보안을 자체 쿠버네티스 환경에 구축할 수 있도록 지원합니다. Red Hat OpenShift 인증을 받은 Tigera Calico Enterprise는 클라우드 환경 전반에서 중요한 컨테이너화 애플리케이션을 성공적으로 운영, 최적화, 보호할 수 있도록 지원합니다. 쿠버네티스 네이티브 아키텍처는 이 솔루션을 애플리케이션 환경에 포함하여 네트워크와 마이크로서비스 계층 간에 세부적인 보안 제어와 향상된 가시성을 제공합니다. 또한 이 솔루션은 기존 보안 툴, 환경, 보안 운영 센터(SOC)와 통합되어 현대적인 워크로드에 추가 제어 능력과 기능을 제공합니다. 제로 트러스트 네트워킹, 이그레스 액세스 제어, 트래픽 가시성, 위협 보호와 방어, 자동 컴플라이언스 감사 리포트를 통해 개발, 테스트, 프로덕션 환경 전반에서 애플리케이션 보안을 강화할 수 있습니다.

보안 기능 확장

기존 방화벽, 최소 권한 보안, 포드 간 트래픽 암호화를 통해 애플리케이션을 보호합니다.

네트워크 가시성 확보

디버그 연결, 위협 헌팅에 이르는 네트워크 플로우에 액세스하고 컴플라이언스 보고를 자동화합니다.

컴플라이언스 보장

애플리케이션 컴플라이언스를 모니터링하고 규정을 준수하지 않는 워크로드에 대한 실시간 경고를 제공합니다.

오프레이터에 액세스

주요 파트너

Aqua Security

Aqua Security는 고객이 마찰을 최소화하면서 비즈니스를 혁신하고 운영하도록 지원합니다. 이 회사는 애플리케이션 라이프사이클 전반에서 위협 방지, 감지, 대응 자동화를 제공하여 환경의 모든 측면에서 보안을 강화합니다.

Red Hat과 Aqua Security는 온사이트, 하이브리드, 클라우드 인프라 전반에서 클라우드 네이티브 워크로드를 더 안전하게 관리하고 확장할 수 있도록 지원합니다. Aqua Cloud Native Security Platform은 Red Hat OpenShift와 통합되어 위험 기반 취약성 관리, 상세 런타임 보호, 통합 인프라 보증과 컴플라이언스를 제공합니다. 이 솔루션은 개발, 보안, 운영 팀이 애플리케이션을 더 안전하게 제공하고, 런타임 시 위협을 방지하고, 정책 확인에 근거하여 인프라 구성에 액세스하고 관련 문제를 해결할 수 있도록 지원합니다.

주요 특징 및 장점

DevSecOps 접근 방식 지원

- Red Hat OpenShift 레지스트리 이미지에 대한 코드, 구성, 권한을 규모에 맞게 분석합니다.
- 위험에 따라 취약점의 우선순위를 지정합니다.
- CI/CD 파이프라인과의 통합으로 빌드 프로세스를 자동화합니다.

런타임 시 애플리케이션 보호

- 무단 컨테이너 활동을 애플리케이션 중단 없이 감지하고 자동으로 완화합니다.
- 표준 이미지의 무단 변경을 식별하고 방지함으로써 컨테이너 불변성을 보장합니다.

소프트웨어 공급망 보안 강화

- 보호되는 사전 프로덕션 테스트 환경에서 이미지를 실행하고 검증합니다.
- 정적 스캐너가 배포 전에 감지할 수 없는 고급 맬웨어를 식별합니다.

인프라 컴플라이언스 유지 관리

- 모범 사례와 CIS(Center for Internet Security) 벤치마크 컴플라이언스를 위한 수백 가지의 구성과 제어 정책을 검사하고 검증합니다.
- OPA(Open Policy Agent) 기반의 선언적 보증 정책을 통해 역할 기반 액세스 제어(RBAC)를 시행합니다.

통합에 액세스

DevSecOps 여정을 시작할 준비가 되셨나요?

애플리케이션 보안은 디지털 비즈니스에 필수적인 요건입니다. DevSecOps 접근 방식을 도입하면 애플리케이션 환경과 비즈니스에 대한 보호를 강화할 수 있습니다.

Red Hat은 혁신적인 기술 기반을 통합 DevSecOps 에코시스템, 광범위한 전문성과 결합하여 조직 전반에서 DevSecOps를 성공적으로 구현할 수 있도록 지원합니다.

- 업계를 주도하는 다양한 인증 툴과 기술 중에서 선택하여 현재와 미래의 요구 사항을 충족할 수 있습니다.
- 전문가 교육 리소스를 통해 모범 사례를 학습하고 DevSecOps 기술을 습득할 수 있습니다.
- 전문 서비스와 컨설팅을 통해 배포 속도를 높일 수 있습니다.

redhat.com/ko/partners/devsecops에서 Red Hat과 함께 DevSecOps를 구현하는 방법에 대해 자세히 알아보세요.

F29623_0721_KVM

Red Hat