통합적인 DevSecOps 솔루션 배포 방법

Red Hat DevSecOps 프레임워크는 고도의 확장성을 갖춘 엔드 투 엔드 DevSecOps 솔루션을 위한 확고한 기반을 제공합니다.

DevOps 보안 유지의 복잡성 해결

DevOps 툴이 빠르게 성장하고 변화하는 환경에서 DevOps의 보안을 유지하기란 쉬운 일이 아닙니다. 여기에 컨테이너와 쿠버네티스가 더해지면서 복잡성은 더욱 커지고, 새로운 공격 벡터와 보안 리스크가 발생합니다. 개발 및 운영팀에서 전체 애플리케이션 라이프사이클 전반에 보안을 필수 요소로 적용해야 중요 IT 인프라와 기밀 데이터를 보호하고 변화에 빠르게 대응할 수 있습니다.

Red Hat과 보안 에코시스템 파트너들은 더 효율적으로 배포하고 확장할 수 있는 DevSecOps 솔루션을 구현하기 위해 확고한 기반과 청사진을 제공하는 프레임워크를 만들었습니다. Red Hat® DevSecOps 프레임워크는 포괄적인 심층 방어 보안 전략에 포함된 DevOps 라이프사이클을 통해 핵심 보안 요구 사항을 해결합니다. Red Hat과 보안 파트너들은 리스크를 줄일 수 있도록 DevOps 보안을 간소화하고 DevSecOps 도입을 가속화합니다.

Anchore, Aqua, CyberArk, Lacework, NeuVector, Palo Alto Networks, Portshift, Snyk, StackRox, Synopsys, Sysdig, Thales, Tigera, Trend Micro, Tufin 등 보안 파트너는 보안 상태를 개선하고 기존 Red Hat 제품을 최대한 활용하는 엔드 투 엔드 DevOps 솔루션을 제공하여 Red Hat의 기본 보안 기능을 강화합니다.

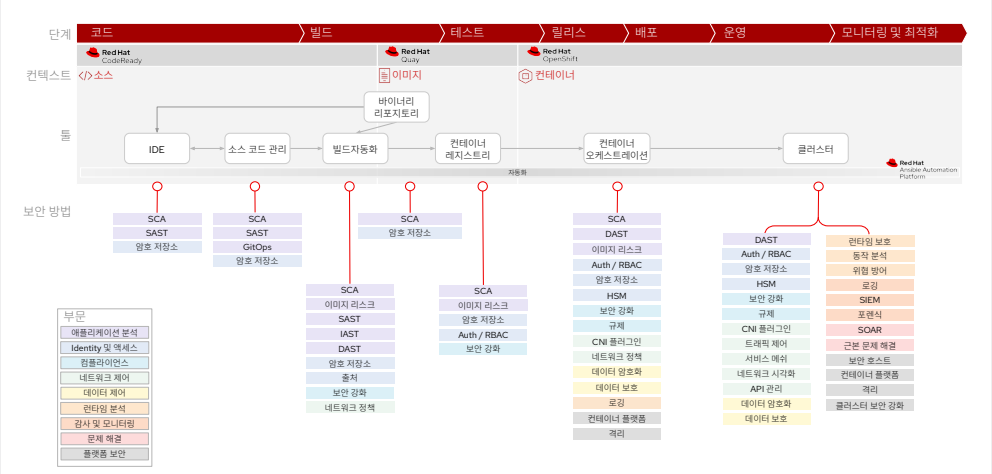

그림 1. DevSecOps 프레임워크

www.facebook.com/redhatkorea

다양한 보안 방식을 지원하는 완전한 프레임워크

Red Hat DevSecOps 프레임워크는 전체 애플리케이션 라이프사이클을 처리하는 9개 보안 범주와 32가지 방식 및 기술을 식별합니다. 이러한 프레임워크는 Red Hat 빌트인 기능, DevOps 툴체인, 보안 파트너 솔루션을 파이프라인의 핵심 통합 지점에 배치합니다. 사용자는 DevOps 환경의 범위와 고유한 요건에 따른 범주 내에서 방법과 기술의 일부 또는 전체를 구현하면 됩니다.

플랫폼 보안

쿠버네티스 플랫폼 보안은 필수적이지만 안전하고, 안정적이며, 확장 가능한 방식으로 비즈니스 크리티컬 애플리케이션을 지원할 쿠버네티스 플랫폼을 구축하는 작업은 어려울 수 있습니다. 사실, 쿠버네티스 배포와 관리는 기업의 지속적인 2대 과제입니다.[1] 엔터프라이즈 레디 쿠버네티스 컨테이너 플랫폼인 Red Hat OpenShift®는 복잡성과 도입 장벽을 제거하고 다양한 빌트인 플랫폼 보안 기능을 포함하고 있습니다.

Red Hat DevSecOps 플랫폼은 기본 컨테이너 호스트(Red Hat Enterprise Linux®, Red Hat CoreOS)와 컨테이너 플랫폼을 보호하는 기반 기능을 제공합니다. 대부분의 Red Hat 보안 기능은 배포를 간소화하고 리스크를 최소화할 수 있도록 기본적으로 지원됩니다. 이 기능을 통해 고객은 컨테이너 경계에서 보안을 유지하고 호스트의 컨테이너 탈출(Container escape)과 같은 보안 이슈를 막을 수 있습니다.

플랫폼 보안 방식

- 호스트 보안: SELinux 기능이 설정된 필수 액세스 제어(MAC), 보안 컴퓨팅 모드(seccomp)로 시스템 호출을 제어하는 커널 기능, Cgroup으로 CPU와 메모리 및 기타 리소스를 격리하는 커널 기능 제공
- 컨테이너 플랫폼 보안: 경량 컨테이너 런타임에 CRI-O, 보안 컨테이너 이미지 레지스트리에 Quay 제공
- Linux 네임스페이스: 팀, 그룹, 부서 전체에서 애플리케이션 격리
- 쿠버네티스 및 컨테이너 강화: NIST 800-190 및 CIS Benchmark와 같은 표준 적용

애플리케이션 분석

애플리케이션 분석 기능을 활용하면 라이프사이클 초기에 애플리케이션 취약점과 기타 보안 문제를 식별할 수 있습니다. DevOps 라이프사이클에서 남아있는 보안 정책을 변경해 초기에 취약점을 식별하고 해결하여, 나중에 작업이 반복되지 않도록 할 수 있습니다.

애플리케이션 분석 방식

- 정적 애플리케이션 보안 테스트(SAST): 개발 중인 코드를 분석해 취약점과 품질 문제 해결
- 소프트웨어 구성 분석(SCA): 애플리케이션에 포함된 종속 패키지를 검사해 알려지지 않은 취약점과 라이센스 문제 탐색
- 양방향 애플리케이션 보안 테스트(IAST) 툴 및 동적 애플리케이션 보안 테스트(DAST) 툴: 실행 중인 애플리케이션 분석을 통해 실행 취약점 탐색

애플리케이션 분석에는 멀웨어, 내장된 암호 및 구성 오류 탐지 기능과 같은 컨테이너 이미지 리스크 관리 기능 및 GitOps 구성 관리 보안 방식이 포함됩니다.

---

1 *Vizard, Mike. "쿠버네티스 엔터프라이즈 도입의 이점에 관한 설문조사(Survey Sees Kubernetes Enterprise Adoption Gains)." Container Journal, 2020년 3월.*

Identity 및 액세스 관리

Identity 및 액세스 관리(IAM) 방식은 온프레미스 및 클라우드 자산, 애플리케이션, 사용자나 애플리케이션 Identity 및 관리를 위해 정의된 정책 기반 데이터에 대한 액세스를 제어합니다. 이런 방식은 DevOps 라이프사이클의 전체 단계에 적용되며 무단 시스템 액세스 및 내부 이동을 차단할 수 있도록 지원합니다.

IAM 방식

- 인증 및 권한 부여 제어: 사용자 및 애플리케이션의 Identity를 확인하고 이들에게 특정 리소스 및 기능에 대한 액세스 권한 부여
- 롤(role) 기반 액세스 제어 (RBAC): 사용자 컬렉션에 직무 기반 리소스 또는 기능에 대한 액세스 권한을 부여하고 관리 및 온보딩을 간소화하며 권한 확대 축소
- Identity 제공업체, 암호 저장소, 하드웨어 보안 모듈(HSM): 유휴 상태 및 전송 중인 보안 자격 증명, 키, 인증서 및 암호 관리

추가 IAM 방식으로는 컨테이너 이미지의 신뢰성을 검증하고 신뢰를 구축하기 위한 컨테이너 이미지 출처 및 이미지 서명 기능이 있습니다.

컴플라이언스

컴플라이언스 방식 및 기술은 산업 및 정부 규제와 기업 정책을 준수하도록 지원합니다. 이는 DevOps 파이프라인 전체에서 컴플라이언스 확인 및 보고를 자동화하므로 감사를 간소화하고 많은 비용을 초래하는 규제 벌금과 소송을 방지할 수 있습니다.

이러한 방식은 다음과 같은 다양한 개인정보 보호 및 정보 보안 규정을 통해 컴플라이언스를 강화합니다.

- 결제 카드 산업 데이터 보안 표준(PCI-DSS)
- ISO 27001 정보 보안 관리 표준
- 미국 건강보험 정보의 이전 및 그 책임에 관한 법률(HIPAA)
- EU 일반 데이터 보호 규정(GDPR)

네트워크 제어 및 세그멘테이션

네트워크 제어 및 세그멘테이션 방식은 쿠버네티스 트래픽을 제어, 분리, 시각화합니다. 이는 테넌트를 격리하고 컨테이너화된 애플리케이션과 마이크로서비스 간 통신 흐름의 보안을 유지할 수 있도록 해줍니다.

네트워크 제어 및 세그멘테이션 방식

- 쿠버네티스 네트워크 보안 정책: IP 주소 또는 포트 수준에서 트래픽 흐름을 제어하고 클러스터 수신 및 발신(ingress and egress) 트래픽 제어, 로깅 및 네트워크 시각화를 통해 개선 가능
- 소프트웨어 정의 네트워킹(SDN): 실시간으로 동적 보안 요구 사항과 변화하는 비즈니스 요구 사항을 지원하는 프로그래밍 가능한 적응형 네트워크 패브릭 제공
- 서비스 메쉬(Service mesh): 네트워크 세그멘테이션, 네트워크 시각화, 인증 및 권한 부여를 통해 컨테이너화된 애플리케이션과 마이크로서비스 지원

데이터 제어

데이터 제어 방식 및 기술은 데이터 무결성을 보호하고 무단 데이터 공개를 방지하도록 지원합니다. 이는 유휴 상태 및 전송 중인 데이터를 보호하여 지적 재산 및 고객의 비밀 정보를 보호하도록 해줍니다.

데이터 제어 방식

- 데이터 암호화: 데이터 암호화, 토큰화, 데이터 마스킹 및 핵심 관리 기능을 제공하여 데이터베이스, 파일, 컨테이너에 있는 데이터의 무단 공개를 차단하도록 지원
- 데이터 보호: 데이터 검색 및 분류, 활동 모니터링 및 감사를 통해 민감한 데이터를 보호하고 컴플라이언스를 강화하도록 지원

런타임 분석 및 보호

프로덕션 런타임 방식은 의심스럽고 악의적인 활동을 실시간으로 식별하고 완화하여 클러스터를 안전하게 유지하도록 해줍니다.

런타임 분석 및 보호 방식

- 권한 컨트롤러: 쿠버네티스 게이트키퍼처럼 기능하여 클러스터에서 실행할 수 있는 항목을 제어하고 실행
- 런타임 애플리케이션 행동 분석: 실시간으로 시스템 활동을 조사하고 의심스러운 행위 또는 악성 행위를 지능적으로 감지
- 런타임 애플리케이션 자체 보호(RASP): 실시간으로 사이버 공격 감지 및 차단
- API 관리: API 액세스 제어 및 API 트래픽 보안 유지

감사 및 모니터링

감사 및 모니터링 방식은 프로덕션 환경에서 보안 인시던트 정보를 제공합니다. 이는 이벤트 발생 시기를 설명하고 가능한 원인 및 영향에 대한 정보를 제공하므로 가시성을 개선하고 인시던트 대응을 가속화할 수 있습니다.

감사 및 모니터링 방식에 포함된 사항:

- 보안 정보 및 이벤트 관리(SIEM): 분산된 기기, 엔드포인트 및 애플리케이션의 로그 및 네트워크 흐름 데이터를 통합해 이벤트 보고 중앙화
- 포렌식: 보안 침해에 대한 가시성 제공, 컴플라이언스 감사를 뒷받침하는 증거 제공, 복구 활동 가속화

문제 해결

문제 해결 방식은 프로덕션 환경에서 보안 인시던트 발생 시 자동으로 수정 조치를 수행하며, 업타임을 개선하고 데이터 손실을 방지할 수 있도록 해줍니다.

문제 해결 방식

- 보안 오케스트레이션, 자동화 및 대응(SOAR) 플랫폼: 작업을 자동화하고 다른 보안 툴과 통합하여 보안 인시던드에 대응
- 근본적인 문제 해결: 쿠버네티스 구성 오류 및 정책 위반 관련 문제를 자동으로 해결

결론

Red Hat DevSecOps 프레임워크는 확장 가능한 안정적 기반을 마련하여 DevOps 보안을 확대하고 리스크를 줄일 수 있도록 지원합니다. Red Hat과 보안 파트너들은 DevSecOps 구현을 간소화하고 가속화하는 데 필요한 기술을 지원합니다. 자세한 내용은 Red Hat에 문의해주시기 바랍니다.

한국레드햇 홈페이지 https://www.redhat.com/ko

RED HAT 정보

Red Hat은 세계적인 엔터프라이즈 오픈소스 솔루션 공급업체로서 커뮤니티 기반 접근 방식을 통해 신뢰도 높은 고성능 Linux, 하이브리드 클라우드, 컨테이너, 쿠버네티스 기술을 제공합니다. 또한 고객으로 하여금 신규 및 기존 IT 애플리케이션을 통합하고, 클라우드 네이티브 애플리케이션을 개발하며, 업계를 선도하는 Red Hat의 운영 체제를 기반으로 표준화하는 동시에 복잡한 환경의 자동화, 보안 및 관리를 실현할 수 있도록 지원합니다. Red Hat은 전세계 고객에게 높은 수준의 지원과 교육 및 컨설팅 서비스를 제공하여 권위있는 어워드를 다수 수상한 바 있으며, Fortune 선정 500대 기업의 신뢰를 받는 어드바이저로 인정받고 있습니다. 또한 기업, 파트너, 오픈소스 커뮤니티의 전략적인 파트너로서 고객들이 디지털 미래에 대비할 수 있도록 지원하고 있습니다.

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