하이브리드 클라우드 보안 강화

필수적인 클라우드 네이티브 보안 고려 사항으로 비즈니스를 보호하세요

/오픈소스 솔루션을 활용하세요

Red Hat

작성자: Lucy Huh Kerner, Red Hat 보안 글로벌 전략 및 에반젤리즘 디렉터

목차

1장

보안 중심 하이브리드 클라우드 배포

클라우드 도입은 사용량과 인기 측면에서 계속 증가하고 있습니다. 오늘날 조직의 65%가 클라우드를 적극적으로 사용하고 있으며, 기업의 72%는 하이브리드 클라우드 전략을 채택하고 있습니다.[1]

하이브리드 클라우드는 베어 메탈, 가상화, 프라이빗 클라우드, 퍼블릭 클라우드 등을 포함하여, 서로 분리된 두 개 이상의 환경 전체에서 일정 수준의 워크로드 이식성, 오케스트레이션, 관리 기능을 통합하는 IT 아키텍처입니다. 하이브리드 클라우드 아키텍처를 사용하면, 연결된 환경 어디에서든 워크로드를 실행하고, 해당 환경에서 워크로드를 전환하고, 리소스를 상호 호환해 사용할 수 있습니다.

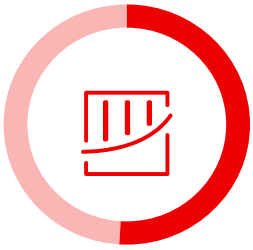
기업이 하이브리드 클라우드 환경을 도입하는 이유는 다음과 같습니다.

- 서로 다른 벤더의 인프라, 플랫폼, 애플리케이션 및 툴 연결
- 효율성과 확장성 증대
- 비용 절감
- 민첩성 향상
- 데이터 배치 최적화

[1] Flexera, "Flexera 2023 클라우드 현황 보고서(Flexera 2023 State of the Cloud Report)," 2023년 3월.

기업의 79%가 클라우드 보안을 과제로 꼽을 정도로 보안은 하이브리드 클라우드 여정의 모든 단계에서 주요 고려 사항입니다.[1] 하이브리드 클라우드 보안 취약성은 일반적으로 승인되지 않은 퍼블릭 클라우드 사용, 리소스에 대한 가시성 부족, 부적절한 변경 제어, 잘못된 구성 관리, 비효율적인 액세스 제어, 인적 오류 등을 비롯한 리소스 관리 및 제어의 실패에서 기인한 것이라 볼 수 있습니다. 이러한 보안 격차를 악용하여 인증되지 않은 사용자가 민감한 데이터와 내부 리소스에 액세스할 수 있으며, 이로 인해 상당한 비용이 발생할 수 있습니다.

전 세계에서 데이터 유출로 인한 평균 비용은 2023년에 **445만 달러**로 최고를 기록했으며, 이 비용에서 비즈니스 손실은 **29.2%**를 차지했습니다.[2]



51%

데이터 유출로 인해 보안 투자를 늘릴 계획이라고 답한 기업의 비율[2]

[1] Flexera, "Flexera 2023 클라우드 현황 보고서(Flexera 2023 State of the Cloud Report)," 2023년 3월.

[2] IBM Security, "2023년 데이터 침해로 인한 비용 보고서(Cost of a Data Breach Report 2023)," 2023년.

2023년에는 데이터 침해와 관련된 레코드당 평균 비용과 침해 해결에 필요한 시간이 모두 증가했습니다.[2] 온프레미스와 클라우드 아키텍처의 차이를 고려하여 전략을 조정하면 보안 중심의 하이브리드 클라우드를 배포하여 이러한 증가하는 문제를 극복하는 데 도움이 될 수 있습니다. 본 e-book은 하이브리드 클라우드 보안을 위해 고려해야 할 사항과 새로운 접근 방식에 대해 설명합니다.

277일

데이터 침해 식별 및 방지에 대한 평균 시간(2023년)[2]

미화 102만 달러

200일 이내 침해 식별 및 방지에 의한 절감 비용[2]

[2] IBM Security, "2023년 데이터 침해로 인한 비용 보고서(Cost of a Data Breach Report 2023)," 2023년.

2장

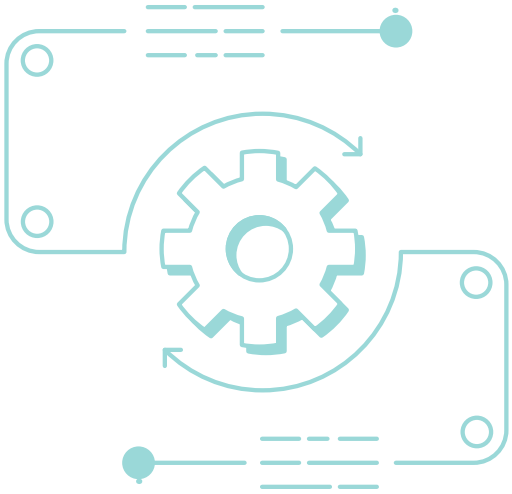
보안은 제품이 아닌 프로세스

효과적인 보안을 구축하려면 구성원, 프로세스, 기술을 통합하는 전체적인 접근 방식이 필요합니다. 단순히 보안 중심 제품과 툴을 배포하는 것만으로는 인프라, 클라우드, 비즈니스를 보호하기에 충분하지 않기 때문입니다. 또한 제품 기능을 극대화하고 위험을 완화하기 위한 보안 전략과 프로세스를 고려해야 합니다.

이러한 전략과 프로세스는 기술, 위협, 요구 사항의 진화에 맞춰 시간을 들여 점진적으로 도입해야 합니다. 하이브리드 클라우드 환경에서는 경계가 정의되어 있지 않아 기존의 보안 접근 방식은 효과적이지 않기 때문에 보안 접근 방식을 전환해야 합니다.

클라우드 중심 보안 접근 방식에서는 중앙화된 Identity 관리와 액세스 제어가 핵심입니다. 이는 사용자에게 필요한 액세스만 제공하는 최소 권한 원칙을 활용합니다. 이러한 접근 방식에는 사용자에 대한 현재 액세스 권한을 감사하고, 적절한 액세스 수준을 결정하기 위해 각 사용자를 재평가하는 과정이 필요합니다.

하이브리드 클라우드 보안은 운영 체제, 컨테이너 플랫폼, 자동화 툴 등의 기업 환경에서 각 계층의 기능을 사용하는 계층화되고 심도 있는 보안 전략을 요구합니다.



운영 체제

보안 컴플라이언스 요구 사항 준수, 물리적 보안 구현, 네트워크 보안 개선, 사용자 액세스 제어, 프로세스 격리 및 데이터 보안 강화를 지원하는 빌트인 툴을 제공할 수 있어야 합니다. 그 예로, OpenSCAP, USBGuard, Security-Enhanced Linux®(SELinux), Identity 관리, Network Bound Disk Encryption 등이 있습니다.

컨테이너 플랫폼

플랫폼과 쿠버네티스에서 빌트인 기능을 사용해 컨테이너 보안을 강화해야 합니다. pod 보안 정책, 네트워크 트래픽 제어, 클러스터 수신 및 발신(ingress and egress) 제어, 롤 기반 액세스 제어(Role-Based Access Control, RBAC), 통합 인증 관리, 네트워크 마이크로 세그멘테이션 등이 이러한 예에 속합니다.

자동화 툴

개발, IT 운영, 보안, 컴플라이언스 팀 등 조직 전반에서 누구나 쉽게 배우고 사용할 수 있는 자동화 언어 및 플랫폼을 선택해야 하며, 액세스 제어, 로깅, 감사 기능을 제공할 수 있어야 합니다.

또한 기존 보안 프로세스와 툴을 재검토하는 것도 중요합니다. 사용 가능한 모든 기능을 활용하고, 보안을 강화하기 위해 설정을 수정하거나 재설정해야 할 부분이 있는지, 또는 새로운 프로세스와 툴이 필요한지 확인해 보세요.

1. 기업의 현재 IT 자산과 툴의 인벤토리를 생성합니다.
2. 기존 보안 및 네트워크 아키텍처, 사이버 보안 정책, 작업 프로세스, 기술 및 인력의 격차 등을 문서화합니다.
3. 위협 모델을 구축하고 사이버 보안 침해에 대한 위험 허용 범위와 완화 전략을 결정합니다.
4. 아키텍처, 정책, 프로세스를 평가하여 변경이 필요한 부분을 식별합니다.
5. 현재 툴과 자산이 업데이트된 전략과 프로세스를 지원할 수 있는지 평가합니다. 보안 격차를 해결할 방법을 문서화하고 계획합니다.

다음 장에서는 하이브리드 클라우드 보안에 대한 주요 고려 사항과 보안을 개선하기 위한 팁을 제공합니다.

3장

보안 고려 사항 1

강력한 기반으로 시작

왜 중요할까요?

워크로드가 여러 환경에 분산되어 있거나 검증되지 않은 오픈소스 기술을 사용하는 환경에서는 취약점 위치를 식별하기 어려울 수 있습니다. 또한 강력한 보안 기반 없이는 다중 계층 보안으로 위험을 줄이기가 어렵습니다. 업스트림 커뮤니티에서 직접 다운로드한 오픈소스 소프트웨어를 사용하면 타사 서비스 및 소프트웨어의 약점을 악용하여 최종 타겟을 노리는 보안 위험과 공급망 공격에 노출될 수 있습니다. 이러한 공격은 소프트웨어 업데이트 해킹, 합법적인 소프트웨어에 악성 코드 삽입 등 다양한 형태로 이루어지며, 지난 3년간 소프트웨어 공급망 공격은 연평균 742% 증가했습니다.[3] 따라서 보안에 중점을 둔 통합된 안정적인 기반을 구축하는 것은 비즈니스 보호를 위해 매우 중요합니다.

권장 사항 및 모범 사례

Red Hat처럼 소프트웨어의 전체 라이프사이클 동안 엔터프라이즈 지원을 제공하는 신뢰할 수 있는 엔터프라이즈 오픈소스 공급업체의 오픈소스 소프트웨어를 사용하여 소프트웨어 공급망 보안 위험을 줄이세요. 엔터프라이즈 오픈소스 벤더는 고객을 대신하여 오픈소스 소프트웨어를 선별하는 등 강력한 소프트웨어 공급망 보안 프로세스를 통해 소프트웨어를 개발합니다. 이를 통해 오픈소스 소프트웨어의 신뢰성, 복원력, 안전성을 보장합니다.

또한 중요한 애플리케이션은 보안 기능이 내장된 플랫폼에서 실행하는 것이 중요합니다. 기본 보안 기능을 확보하면 중요한 애플리케이션을 안정적으로 실행하고, 위험을 줄이기 위한 다중 계층 보안 기능을 포함하며, 보안 및 컴플라이언스 자동화를 구현할 수 있습니다.

Red Hat® Enterprise Linux® 같이 안정성과 보안이 강화되고 복원력을 갖춘 신뢰할 수 있는 운영 체제를 채택하여 애플리케이션 및 프로세스에 대한 보안 중심 기반을 우선적으로 구축하세요. 이러한 안정적인 보인 기반 덕분에 베어메탈, 가상, 컨테이너 및 모든 유형의 클라우드 환경 전반에서 중요 애플리케이션을 안정적으로 확장하고, 보안 컴플라이언스를 유지하며, 이머징 기술을 지속적으로 출시할 수 있습니다.

[3] Sonatype. "제9차 소프트웨어 공급망 현황 연례 보고서(9th Annual State of the Software Supply Chain)," 2023년.

Red Hat Enterprise Linux는 Red Hat 포트폴리오 대부분의 기반이며, 빌트인 보안 기능 덕분에 많은 기업이 신뢰하는 운영 체제입니다.

Red Hat Enterprise Linux를 사용하면 다음을 실현할 수 있습니다.

실시간 커널 패치 적용과 같은 빌트인 보안 기능으로 데이터 또는 시스템 노출 위험을 완화할 수 있습니다. 따라서 재부팅하거나 런타임을 중단하지 않고도 보안 패치를 적용할 수 있습니다. 이 외에도 특정 사용자가 시스템에서 실행할 수 있는 승인된 애플리케이션 또는 실행 파일의 인덱스를 지정하는 애플리케이션 허용 목록, 그리고 파일, 프로세스, 사용자, 애플리케이션 등을 정교하게 제어하는 SELinux 등의 보안 기능이 기본으로 제공됩니다.

암호화된 시스템의 잠금 해제 자동화를 지원하는 네트워크 바운드 디스크 암호화(Network Bound Disk Encryption, NBDE) 같은 빌트인 보안 기능을 활용해 암호화 키를 관리하지 않고도 데이터 보호를 규모에 맞게 자동화하고 시의 적절하게 유지 관리할 수 있습니다. 또한 시스템 전반에 암호화 정책을 적용해 데이터를 안전하게 보호하는 데 집중할 수 있으며, 시스템 전반에서 일관되고 사용자 정의 가능한 암호화 설정으로 컴플라이언스를 유지하여 사이트별 정책 요건 등을 충족할 수 있습니다.

컴플라이언스 요구 사항을 충족하고 감사를 간소화할 수 있습니다. Red Hat Enterprise Linux에는 OpenSCAP을 통한 컴플라이언스 검사 및 문제 해결 기능이 내장되어 있어 로컬 시스템에서 구성 및 취약성을 검사하여 다양한 업계 보안 표준에 대한 컴플라이언스를 검증할 수 있습니다.

Red Hat Enterprise Linux가 제공하는 기본 보안 접근 방식을 기반으로 계층화되어 실행되는 **Red Hat OpenShift** 같은 제품은 컨테이너와 쿠버네티스에 대한 심층적인 방어 기능을 제공합니다. Red Hat은 보안 기능을 쿠버네티스 구성 요소로 확장합니다. 마찬가지로, 내장된 보안 기능을 갖춘 **Red Hat Ansible Automation Platform**을 활용하면 기업은 규모에 맞춰 보안 및 컴플라이언스 자동화를 구현할 수 있습니다.

전략적 단계

다음 작업에 따라 하이브리드 클라우드 보안을 시작해 보세요.

상용 버전으로 전환

업스트림 오픈소스 프로젝트에서 바로 가져온 오픈소스 소프트웨어 대신, 신뢰할 수 있는 상용 버전으로 마이그레이션합니다. 상용 버전은 버그와 보안 취약성의 위험을 최소화하기 위해 테스트와 검증 과정을 거쳤습니다. 또한 보안 패치를 신속하게 제공하고 소프트웨어를 안전하게 설정할 수 있도록 안내하는 엔터프라이즈급 지원을 포함합니다. 신뢰할 수 있는 엔터프라이즈 오픈소스 벤더의 오픈소스 소프트웨어를 채택하면 강력한 소프트웨어 공급망 보안 프로세스를 통해 소프트웨어를 개발하고 소프트웨어의 전체 라이프사이클 동안 엔터프라이즈 지원을 보장할 수 있습니다. 이 모든 조치를 통해 기업은 보안 위험을 최소화하면서 오픈소스 소프트웨어를 사용할 수 있습니다.

보안 기능이 내장된 플랫폼 선택

보안 기능이 내장된 플랫폼(예: OS, 컨테이너 애플리케이션 플랫폼, 자동화 플랫폼)을 선택하는 것이 중요합니다. 기본 보안 기능을 확보하면 중요한 애플리케이션을 안정적으로 실행하고, 위험을 줄이기 위한 다중 계층 보안 기능을 포함하며, 보안 및 컴플라이언스 자동화를 규모에 맞게 구현할 수 있습니다.

기술 스택 전반에서 보안 구현

기본적인 보안 기반을 구축한 후에는, 그 기반에서 실행되는 계층화된 기술이 보안 혜택을 상속하고 다중 계층 보안을 위해 함께 작동하도록 보장합니다.

4장

보안 고려 사항 2

DevSecOps로 신뢰할 수 있는 소프트웨어 공급망 구현

왜 중요할까요?

2023년 데이터 침해의 12%가 소프트웨어 공급망 공격에서 비롯되었습니다.[2] 업스트림 커뮤니티에서 직접 다운로드한 확인되지 않은 오픈소스 소프트웨어를 사용하는 경우, 타사 서비스 및 소프트웨어의 약점을 악용하여 최종 타겟을 노리는 보안 취약점 및 공급망 공격에 노출될 수 있습니다. 이러한 공격은 소프트웨어 업데이트의 해킹 및 합법 소프트웨어에 악성 코드를 주입하는 등 다양한 형태를 취합니다.

구획화된 보안 접근 방식은 애플리케이션 개발과 인프라 배포 과정에서 추후에 보안을 추가하기 때문에 종종 보안 격차를 불러와 중복 작업을 초래합니다. 개발의 속도와 배포의 유연성이 증가함에 따라, 프로세스 전체에서 보안의 중요성이 커지고 있습니다.

권장 사항 및 모범 사례

소프트웨어 공급망에 보안 중심 접근 방식을 도입하기 위한 초기 단계는 DevSecOps 관점을 개발하는 것입니다. DevSecOps 관점에서는 애플리케이션 개발자, IT 운영 및 보안 팀이 모두 협업하여 소프트웨어 개발 라이프사이클(SDLC) 및 인프라 라이프사이클 전반에서 소프트웨어 공급망 보안을 구현하며, 이는 하이브리드 클라우드 전반에서 엔터프라이즈급으로 강화된 오픈소스 기반으로 구축됩니다.

[2] IBM Security, "2023년 데이터 침해로 인한 비용 보고서(Cost of a Data Breach Report 2023)," 2023년.

DevSecOps는 초기 설계부터 통합, 테스트, 배포 및 소프트웨어 제공에 이르는 소프트웨어 개발 라이프사이클의 모든 단계에서 보안 통합을 자동화합니다.

DevSecOps 프로세스 도입의 장점:

- IT 팀과 보안 팀이 인력, 프로세스, 기술 전반의 문제를 해결하는 데 도움이 됩니다.
- 효율성, 일관성, 반복 가능성 및 협업을 개선할 수 있습니다.
- 인적 오류를 줄여 궁극적으로 위험을 줄일 수 있습니다.

DevSecOps를 도입하면 보안은 처음부터 끝까지 통합된 공동 책임이 됩니다. 단절된 단일 팀이 보안 정책 수립을 전담하는 것이 아니라 보안, 개발, 운영 팀의 인력이 협력하여 가시성, 피드백, 지식, 인사이트를 공유합니다. 이러한 접근 방식을 통해 애플리케이션 개발과 인프라 배포 시작 시점부터 보안 프로세스를 구축하여 보호 성능을 점차 강화할 수 있습니다.

조직을 위해 새로운 소프트웨어 기능을 구축하는 엔터프라이즈 애플리케이션 개발자는 보안 상태를 크게 강화하는 동시에 인지 부하를 줄여야 합니다. 보안은 SDLC 전체에서 구현되어야 합니다. 코드 타임에서 통합 애플리케이션 보안 검사를 통해 초기에 문제를 파악하여 오래 지속되는 다운타임을 줄이고, 빌드 타임에서 보안 중심의 지속적 통합/지속적 제공(CI/CD) 워크플로우를 사용해 빌드 시스템을 보호하며, 배포 타임과 런타임에서 최적의 경로 템플릿과 취약성 분석, 아티팩트 서명, 증명, 출처, 정책 시행 지점 및 SBOM(Software Bill of Materials)을 통해 보안을 유지해야 합니다.

또한 팀이 신뢰할 수 있는 출처에서 가져온 오픈소스 기술을 사용하도록 하고, 자동화된 방식으로 지속적으로 패치를 적용하며, 보안을 중심에 두고 구성하는 전략을 수립해야 합니다. 전체 라이프사이클 전반에 걸쳐 기업에 적합한 지원을 제공하는 엔터프라이즈급 오픈소스 제품을 사용하도록 권장해야 합니다.

Red Hat 제품과 같은 엔터프라이즈급 오픈소스 제품을 사용하면 30년 이상의 경험을 통해 축적된 Red Hat의 전문성을 활용해 제품의 오픈소스 소프트웨어 공급망을 보호할 수 있습니다. 또한 기업은 쿠버네티스 클러스터를 배포, 관리, 보호하는 데 도움이 되는 솔루션과 애플리케이션을 규모에 따라 안전하게 구축, 현대화 및 배포할 통합된 방법이 필요합니다.

Red Hat OpenShift Platform Plus는 Red Hat OpenShift, Red Hat Advanced Cluster Security for Kubernetes, Red Hat Advanced Cluster Management for Kubernetes, Red Hat Quay, Red Hat OpenShift Data Foundation을 포함하는 통합 플랫폼으로, 기업이 컨테이너화된 애플리케이션을 쿠버네티스에서 안전하고 규모에 맞게 구축, 현대화 및 배포할 수 있도록 지원합니다. 멀티클러스터 보안, 컴플라이언스, 애플리케이션 및 데이터 관리 기능이 제공되어 소프트웨어 공급망 전반에서 일관성을 유지할 수 있습니다.

전략적 단계

다음 작업에 따라 DevSecOps 및 소프트웨어 공급망 보안 개선을 구현해 보세요.

소규모로 시작하여 확장
단일 프로젝트를 선택하여 시작합니다. 여러 가지 실험적인 작업을 수행하고 반복적이고 지속적인 개선을 통해 프로세스를 미세 조정하고 최적화합니다. 성공하는 경우 이를 축하하고 조직 내 다른 사람들과 공유하여 입증된 가치를 소개합니다.

명확한, 합의된 목표 및 타임라인 설정
투명성이 핵심입니다. 관련된 모두가 프로젝트의 목표와 타임라인을 파악하고 동의하는지 확인합니다.

직원들을 위한 교차 교육

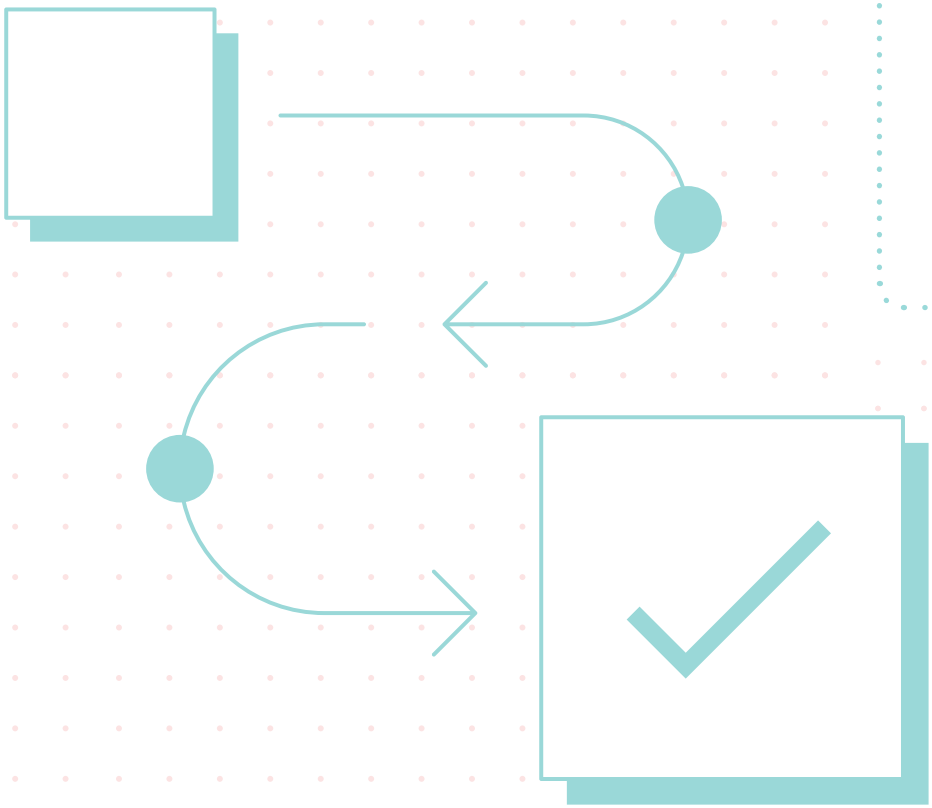
보안, 인프라, 개발에 대한 학습 경로를 구축하여 정기적으로 업데이트되며 모든 팀원에게 제공되도록 합니다.

보안 실무 그룹 구축

보안 활용 사례와 전략을 정의할 다양한 분야의 통합된 팀을 구축합니다. 다양한 사례를 통해 학습하고, 다른 조직에서 얻은 결과를 활용합니다.

통합 애플리케이션 플랫폼으로 SDLC 전반에 보안 구현

보안은 SDLC 전체에서 구현되어야 합니다. 코드 타임에서 통합 애플리케이션 보안 검사를 통해 초기에 문제를 파악하여 오래 지속되는 다운타임을 줄이고, 빌드 타임에서 보안 중심의 지속적 통합/지속적 제공(CI/CD) 워크플로우를 사용해 빌드 시스템을 보호하며, 배포 타임과 런타임에서 최적의 경로 템플릿과 취약성 분석, 아티팩트 서명, 증명, 출처, 정책 시행 지점 및 SBOM(Software Bill of Materials)을 통해 보안을 유지해야 합니다.



5장

보안 고려 사항 3

자동화 및 관리를 사용하여 하이브리드 클라우드 보호

왜 중요할까요?

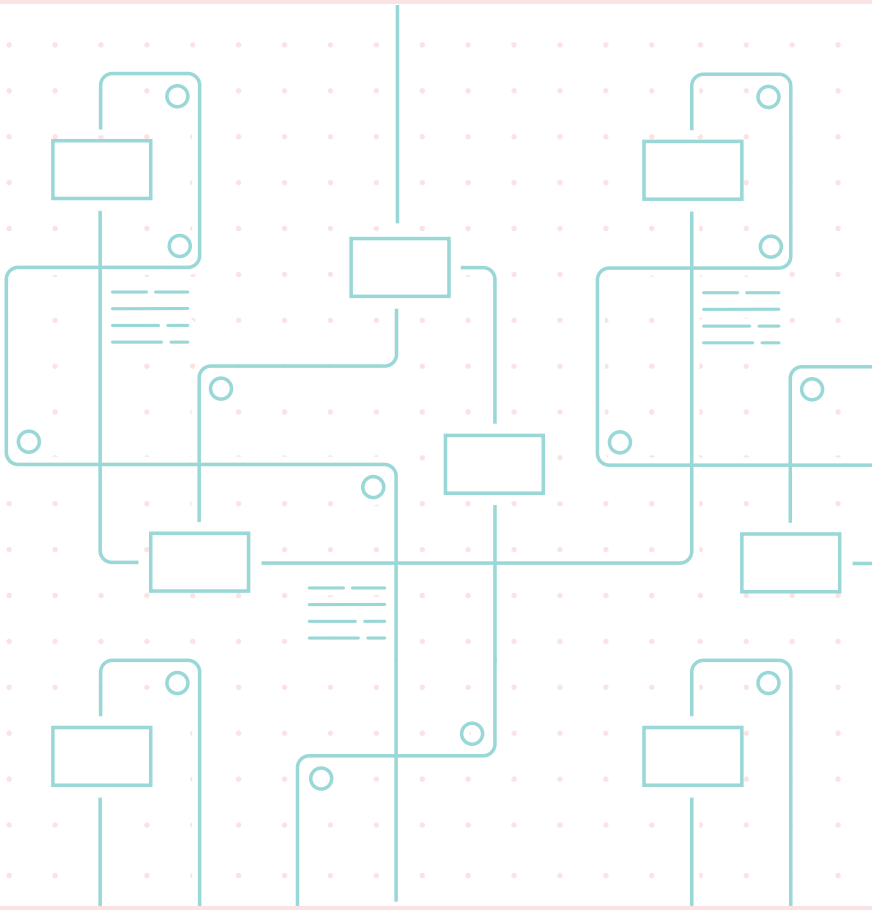
구성 오류와 부적절한 변경 제어는 보안에 가장 큰 위협 요소이며, 구성 오류로 인해 시스템이 공격에 취약해질 수 있습니다. 변경 제어는 구성을 누가 언제 수정했는지, 시스템 라이프사이클 전반에서 무엇이 변경되었는지 파악하기 위해 필수적입니다.

자동화, 관리, AI를 활용하면 일상 업무를 간소화하고 처음부터 보안을 프로세스와 애플리케이션 및 인프라에 통합할 수 있습니다. 조직 전반에서 자동화 및 관리 전략을 수립하면 인적 오류를 줄이고 속도, 일관성, 반복 가능성, 검증 및 감사 기능을 제공할 수 있습니다. 또한 중앙집중식 자동화 및 관리 전략은 기업이 처음부터 애플리케이션 개발 및 IT 운영에 보안을 통합하고 라이프사이클 전체에서 보안 및 컴플라이언스를 개선하는 데 도움이 됩니다. 이를 통해 DevSecOps를 성공적으로 구현할 수 있습니다. 실제로, 광범위한 자동화, 관리, AI를 보안 프로세스에 통합하면 침해로 인한 비용을 평균 39.3%까지 줄일 수 있지만, 이를 수행한 조직은 28%에 불과합니다.[2]

[2] IBM Security, "2023년 데이터 침해로 인한 비용 보고서(Cost of a Data Breach Report 2023)," 2023년.
[4] Cloud Security Alliance, "클라우드 컴퓨팅의 가장 큰 위협: 팬데믹 11 심층 분석(Top Threats to Cloud Computing: Pandemic 11 Deep Dive)," 2023년 10월.

권장 사항 및 모범 사례

전사적인 자동화 및 관리 전략을 구현하여 동적 보안, 위험 및 컴플라이언스 요구 사항에 발맞춰야 합니다. 하이브리드 클라우드에 일관된 자동화 및 관리 전략을 채택하면 민첩성, 반복 가능성, 일관성을 강화하고 감사를 간소화할 수 있습니다.



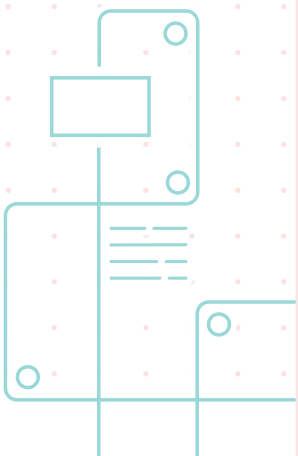
통합된 자동화 및 관리 전략은 조직 전체에서 잘못된 구성과 수작업 오류로 인한 위험이 줄어듭니다. 자동화 및 관리는 인프라 관리, 애플리케이션 배포, 보안 운영을 간소화하고 일관성을 강화하여 보안, 컴플라이언스, 변경 제어를 개선합니다. 이를 통해 다음을 수행할 수 있습니다.

사전 승인된 정책에 따라 리소스를 일관적으로 구성하고, 라이프사이클이 진행되는 동안 반복 가능한 방식으로 사전 예방적으로 유지 관리합니다.

패치 또는 재설정이 필요한 시스템을 신속하게 식별합니다.

정의된 기준에 따라 다수의 시스템에 일관된 방식으로 패치 적용을 간소화하거나 시스템 설정을 변경할 수 있습니다.

자동으로 기록된 작업 로그를 사용하여 감사와 문제 해결이 쉬워집니다.



자동화 플랫폼과 프로세스에 대한 Identity 관리 및 액세스 제어를 구현하면 권한이 있는 직원만 자동화 태스크를 실행하도록 할 수 있습니다. 조직의 모든 사람이 이용할 수 있는 자동화 플랫폼을 선택하세요. 배우기 쉬운 공통된 자동화 언어를 구현한 플랫폼을 선택하면 다음과 같은 부분을 개선할 수 있습니다.

가시성: 어떤 자동화 태스크가 진행되고 있는지 모두가 파악할 수 있습니다.

반복 가능성: 액세스 가능한 플랫폼과 언어를 사용하여 인증된 모든 직원이 효과적이고 효율적으로 자동화를 활용할 수 있습니다.

협업: 자동화 태스크를 조직 전반에서 공유할 수 있으므로, 다른 팀에서 완료한 작업을 활용하고 중복 작업을 방지할 수 있습니다.

감사: 여러 명의 인력이 자동화 태스크를 검증하고 감사를 위한 로그를 볼 수 있습니다.

기업은 계속해서 더 복잡해지는 운영 환경, 애플리케이션, 보안 운영, 하이브리드 클라우드 환경 전반에서 보안을 관리하기 위해 IT 자동화에 의존하고 있습니다. **Red Hat Ansible Automation Platform**은 규모에 맞게 IT 자동화를 구축하고 운영하기 위한 일관된 엔터프라이즈 프레임워크를 제공하는 동시에 모든 단계에서 보안을 최우선으로 고려하는 엔드 투 엔드 자동화 플랫폼입니다. 이 플랫폼은 효율성을 향상하고, 생산성을 높이며, 위험과 비용을 제어할 뿐만 아니라, 팀이 반복 가능한 방식으로 기업 전반의 보안 및 컴플라이언스 일관성을 자동화하도록 지원하고, Red Hat의 24시간 엔터프라이즈 지원을 통해 위협에 유기적으로 대응할 수 있도록 인증된 오토메이션 콘텐츠를 제공합니다.

Red Hat Ansible Automation Platform은 자동화된 구성 관리부터 자동화된 패치 적용 및 문제 해결이 이르는 모든 기능을 제공하여 조직이 자동화된 보안 프로세스 관리를 통해 악의적인 공격에 앞서 대응할 수 있도록 지원합니다. 또한 Red Hat Ansible Automation Platform은 CyberArk, IBM, Palo Alto Networks와 같은 인증 파트너 콘텐츠를 사용하여 보안 솔루션의 통합 지점 역할을 합니다. 이를 통해 사용자는 다양한 외부 보안 기술의 관리와 통합을 자동화할 수 있습니다.

전략적 단계

다음 작업에 따라 보안 자동화를 시작해 보세요.

단일 프로젝트로 시작
한 번에 모든 것을 자동화할 수는 없습니다. 제한된 태스크 세트를 선택하여 시작하세요.

반복적인 태스크 선택
설정 관리, 소프트웨어 패키지 및 패치 관리, 보안 취약성 식별 및 해결, 정책 실행 등 반복적으로 수행하는 태스크를 자동화합니다.

측정, 조정, 반복
자동화를 배포하고, 결과를 측정하며, 이에 따라 조정하는 작업을 반복 수행합니다.

엔드 투 엔드 엔터프라이즈 자동화 플랫폼을 사용하여 확장 계획
모든 자동화가 검증, 감사 및 공유 가능하도록 구현하여 조직 내 다른 사람들이 장점을 활용하고 엔드 투 엔드 엔터프라이즈 자동화 플랫폼을 사용하여 확장할 수 있도록 합니다.

6장

지금 시작해 보세요

하이브리드 클라우드 보안은 모든 조직의 공동 책임입니다. 하이브리드 클라우드 여정의 모든 단계에서 Red Hat은 고객이 보안 중심의 하이브리드 클라우드를 배포하도록 도와드립니다.

통합된 빌트인 보안 기능을 갖춘 Red Hat의 프로덕션급 오픈소스 소프트웨어 포트폴리오는 현재와 미래의 보안 및 컴플라이언스 문제를 해결할 수 있는 툴과 플랫폼을 제공합니다. 또한, Red Hat은 엔터프라이즈 수준의 지원, 핸즈온 교육 및 전문가 서비스를 제공하여 하이브리드 클라우드 환경을 더욱 효율적이고 안전하게 구축하고 운영할 수 있도록 도와드립니다.

Red Hat의 하이브리드 클라우드 보안 접근 방식 살펴보기

다음 리소스를 참고하여 하이브리드 클라우드 전반에서 Red Hat의 보안 및 컴플라이언스에 대한 접근 방식을 자세히 알아보세요.

- 하이브리드 클라우드 보안 개요
- 하이브리드 클라우드 보안 평가
- 하이브리드 클라우드 환경을 위한 보안 접근 방식
- 하이브리드 클라우드 보안 강화

한국레드햇 홈페이지 https://www.redhat.com/ko

Lucy Huh Kerner 소개(Red Hat 보안 글로벌 전략 및 에반젤리즘 디렉터)
Lucy Huh Kerner는 보안 사고 리더십과 전 세계 Red Hat 및 Red Hat의 전체 포트폴리오의 보안을 위한 기술 및 GTM(Go-To-Market) 전략을 이끌고 있으며, 글로벌 업계, 고객, 파트너, 애널리스트 및 언론에 보안 관련 기술 콘텐츠를 작성하여 지원하고 보안 컨퍼런스를 비롯한 수많은 글로벌 이벤트에서 주요 발표를 해왔습니다. 소프트웨어 및 하드웨어 개발 엔지니어, 솔루션 아키텍트 겸 글로벌 보안 전략가로서 보안의 다양한 측면을 다루며 20년 이상의 전문 경력을 보유하고 있습니다.

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

www.redhat.com/ko