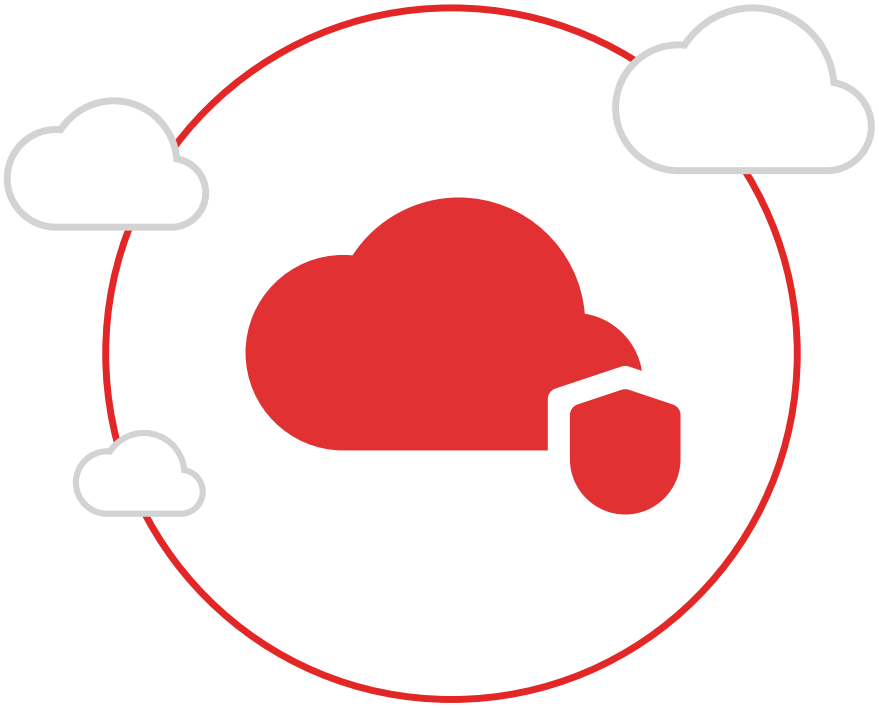
Red Hat



하이브리드 클라우드 보안 강화

클라우드 네이티브 보안 접근 방식으로 비즈니스 보호

Lucy Huh Kerner, Red Hat, 시니어 수석 보안 글로벌 기술 에반젤리스트 및 전략 담당자

목차

보안 중심 하이브리드 클라우드 배포

오늘날, 클라우드를 활용하는 조직은 94%에 달하며, 58%의 기업은 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, 환경과 환경 사이에서 워크로드를 전환할 수 있으며, 해당 환경으로부터 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

하이브리드 클라우드 여정의 어느 단계에 있든, 보안은 중요하게 고려해야 할 사항입니다. 실제로 81%의 기업이 클라우드 보안을 주요 과제로 꼽았습니다.[1] 하이브리드 클라우드 보안의 취약성은 일반적으로 승인되지 않은 퍼블릭 클라우드 사용, 리소스에 대한 가시성 부족, 부적합한 변경 제어, 잘못된 설정 관리, 비효율적인 액세스 제어를 비롯한 리소스 관리 및 제어의 실패에서 기인한 것이라 볼 수 있습니다. 이러한 보안 격차를 악용하여 인증되지 않은 사용자가 민감한 데이터와 내부 리소스에 액세스할 수 있습니다.

보안 침해는 막대한 비용 손실로 이어질 수 있습니다. 데이터 유출로 인한 평균 비용은 미화 392만 달러에 달하며, 이 중 36.2%가 비즈니스 손실에 대한 비용이었습니다.[2] 그리고 그 위협은 더욱 커지고 있습니다. 2년 이내에 보안 침해가 발생할 확률은 29.6%입니다.[2]보안 침해를 식별하고 해결하는 데 걸린 시간과 평균 데이터 레코드 수가 2019년에 모두 증가했습니다.[2]

온프레미스 및 클라우드 아키텍처 사이의 차이를 해결할 수 있는 방식을 채택하면, 보안 침해라는 도전 과제를 풀 수 있는 **보안 중심 하이브리드 클라우드**를 배포할 수 있습니다. 본 e-book은 하이브리드 클라우드에서 비즈니스를 보호하기 위해 고려해야 할 사항과 새로운 접근 방식에 대해 논의합니다.

비효율적인 보안의 영향

보안 침해로 인한 비용 손실과 위협은 계속 확대되고 있습니다.

392만 달러(US$)
데이터 침해로 인한 평균 비용(2019년)[2]

279일
데이터 침해를 식별하고 중지하는 데 걸린 평균 시간(2019년)[2]

122만 달러(US$)
비용 절감

200일
이내 침해를 식별하고 차단했을 경우[2]

29.6%
2년 이내에 보안 침해를 경험할 확률[2]

1 *Flexera, "RightScale 2019년 클라우드 현황 Flexera 보고서(RightScale 2019 State of the Cloud Report from Flexera)," 2019년 2월.* info.flexerasoftware.com/SLO-WP-State-of-the-Cloud-2019.

2 *IBM Security, "2019년 데이터 유출로 인한 비용 보고서(2019 Cost of a Data Breach Report)," 2019년.* ibm.com/security/data-breach

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 제품의 기능을 사용해 효과적으로 보안 리스크를 완화할 수 있도록 보안 전략과 프로세스를 구현해야 하는 것은 물론, 기술, 위협, 요구 사항의 진화에 맞춰 시간을 들여 점진적으로 도입해야 합니다.

하이브리드 클라우드 환경은 기업이 보안에 대한 접근 방식을 변경할 것을 요구합니다. 왜냐하면 특정한 경계가 없기 때문에 전통적인 경계 기반의 보안 접근 방식은 더 이상 효과적이지 않기 때문입니다. 클라우드 중심 보안 접근 방식에서는 중앙화된 Identity 관리와 액세스 제어가 핵심입니다. 효과적으로 중앙화된 Identity 관리와 액세스 제어는 사용자에게 실제로 필요한 액세스만 제공하는 최소 권한 원칙을 활용합니다. 이러한 접근 방식에는 각 사용자에 대한 현재 액세스 권한을 감사하고, 올바른 액세스 수준을 결정하기 위해 각 사용자를 재평가하는 과정이 필요합니다.

하이브리드 클라우드 보안은 운영 체제, 컨테이너 플랫폼, 자동화 툴, 서비스로서의 소프트웨어(Software-as-a-Service, SaaS) 자산, 클라우드 서비스 등의 기업 환경에서 각 계층의 기능을 사용하는 계층화되고 심도있는 보안 전략을 요구합니다.

운영 체제

보안 컴플라이언스 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, 방화벽, 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, 운영, 보안, 컴플라이언스 팀 등 조직 전반에서 누구나 쉽게 배우고 사용할 수 있는 자동화 언어를 선택해야 하며, 액세스 제어, 로깅, 감사 기능을 제공할 수 있어야 합니다. 자동화는 **4장**에서 자세히 살펴볼 수 있습니다.

마지막으로, 기존 보안 프로세스와 툴을 다시 검토해야 합니다. 사용 가능한 모든 기능을 활용하고, 보안을 강화하기 위해 설정을 수정하거나 재설정해야 할 부분이 있는지, 또는 새로운 프로세스와 툴이 필요한지 확인해 보십시오.

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 범위과 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.

보안 고려 사항

협업

왜 중요할까요?

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 초반에 보안의 중요성이 커지고 있습니다. 개발 주기의 마지막에서 효과적인 보안을 적용하려면 꽤 많은 시간이 소요되고, 이로 인해 제공이 지연되어 팀에서는 보안에 소홀해질 우려가 있습니다.

권장 사항 및 모범 사례

DevSecOps 접근 방식으로 조직 전반의 보안을 통합하세요. DevSecOps는 처음부터 끝까지 보안을 통합하는 방식으로 책임을 공유하는 협업 방식의 프레임워크입니다. 분리된 단일 팀이 단독으로 보안 정책 설정을 담당하는 것이 아니라, 여러 팀 전반으로 보안을 확장하는 방식입니다. 보안, 개발, 운영 팀의 인력이 협력하여 가시성, 피드백, 지식, 인사이트를 공유합니다. 이러한 접근 방식을 통해 애플리케이션 개발과 인프라 배포 시작 시점부터 보안을 구축하여 보호 성능을 점차 강화할 수 있습니다.

정규 교육 프로그램을 활용하면 모든 사람들이 보안의 중요성과 조직을 보호할 수 있는 방법을 배울 수 있습니다. 이 프로그램은 다음과 같은 주제를 다룹니다.

- 보안 정책 및 규제를 통해 애플리케이션 및 리소스 컴플라이언스 유지 관리
- 전통적인 환경, 컨테이너화된 환경, 하이브리드 클라우드 환경에 대해 각기 다른 보안 방식 구축
- 신규 및 기존 보안 취약성의 최신 정보를 파악할 수 있는 패치 전략 수립

경영진의 공식적인 지원 역시 중요한 요소입니다. 경영진은 협업을 권장하고 열린 태도로 조직 전반의 다양한 팀에서 피드백을 수렴해야 합니다.

전략적 단계

조직 내 협업을 강화하기 위한 다음 단계를 살펴 보십시오.

작게 시작하여 확장

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

명확한, 합의된 목표 및 타임라인 설정

DevSecOps의 핵심은 바로 투명성입니다. 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 워크그룹 생성

보안 활용 사례와 전략을 정의할 다양한 분야의 통합된 팀을 구축합니다.

사례를 통한 학습

미국의 **국세청**이나 **국토안보부** 등의 다양한 사례 결과를 활용합니다.

보안 고려 사항

자동화

왜 중요할까요?

설정 오류와 부적절한 변경 제어는 보안에 가장 큰 위협 요소이며,[3] 설정 오류로 인해 시스템이 공격에 취약해질 수 있습니다. 변경 제어는 설정을 누가 언제 수정했는지, 시스템 라이프사이클 전반에서 무엇이 변경되었는지 파악하기 위해 필수적입니다. 자동화는 일상 업무를 간소화하고 처음부터 보안을 프로세스와 애플리케이션 및 인프라에 통합할 수 있도록 지원합니다. 실제로 완전한 배포 보안 자동화를 구현하면 보안 유출로 인한 평균 비용을 95% 절감할 수 있지만, 이를 구현한 조직은 16%에 불과합니다.[4]

권장 사항 및 모범 사례

통합된 자동화 전략을 구현하면 조직 전체에서 잘못된 설정이나 수동 작업으로 인한 오류가 발생할 위험이 줄어듭니다. 자동화는 인프라 관리, 애플리케이션 배포, 보안 운영을 간소화하고 일관성을 강화하여 보안, 컴플라이언스, 변경 제어를 개선합니다.

- 사전 승인된 정책에 따라 리소스를 일관적으로 설정하고, 라이프사이클이 진행되는 동안 반복 가능한 방식으로 사전 예방적으로 유지 관리합니다.
- 패치 또는 재설정이 필요한 시스템을 신속하게 식별합니다.
- 정의된 기준에 따라 다수의 시스템에 일관적인 방식으로 보다 손쉽게 패치를 적용하고 시스템 설정을 변경합니다.
- 자동으로 기록된 작업 로그를 사용하여 감사와 문제 해결이 쉬워집니다.

자동화 플랫폼과 프로세스에 대한 Identity 관리 및 액세스 제어를 구현하면 인증된 직원만 자동화 태스크를 실행하도록 할 수 있습니다.

조직의 모든 사람이 이용할 수 있는 자동화 플랫폼을 선택할 수 있습니다. 배우기 쉬운 공통된 자동화 언어를 구현한 플랫폼을 활용하면 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.

전략적 단계

다음 작업에 따라 보안 자동화를 시작해 보세요.

단일 프로젝트로 시작

한 번에 모든 것을 자동화할 수는 없습니다. 단일 프로젝트 또는 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.

확장 계획

모든 자동화를 검증, 감사 및 공유 가능하도록 구현하여 조직 내 다른 사람들이 이점을 활용할 수 있도록 합니다.

3 *Cloud Security Alliance, "클라우드 컴퓨팅의 가장 큰 위협 11가지(Top Threats to Cloud Computing: The Egregious 11)", 2019년 8월* cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven

4 *IBM Security, "2019년 데이터 유출로 인한 비용 보고서(2019 Cost of a Data Breach Report)," 2019년* ibm.com/security/data-breach

보안 고려 사항

업데이트 및 패치

왜 중요할까요?

패치가 적용되지 않았거나 오래된 시스템은 컴플라이언스 문제 및 보안 취약성의 원인이 될 수 있습니다. 실제로 악용되는 대부분의 취약점은 침해가 발생했을 때 이미 보안 및 IT 팀에 알려진 취약점인 경우가 많습니다.

권장 사항 및 모범 사례

패치를 자주 적용하고 해당 패치가 올바르게 적용되었는지 확인하고, 패치가 필요한 컴플라이언스 문제와 보안 취약점이 있는지 시스템을 매일 스캔합니다. 위험, 성능, 시간 고려 사항은 물론 위협 모델에 따라서, 발견된 항목을 수정하는 작업의 우선순위를 지정합니다. 해당하는 모든 시스템에 정기적으로 패치를 적용하여 중요한 문제를 적시에 해결합니다. 중요한 문제 및 알려진 취약점에 대한 패치를 가능한 한 빨리 적용합니다. 프로덕션에 다시 적용하기 전에 패치된 시스템의 기능을 테스트합니다.

베이스 이미지에서 배포되는 클라우드 및 컨테이너 리소스에 대한 패치 전략도 업데이트해야 합니다. 베이스 이미지는 조직의 보안 기준을 준수해야 합니다. 물리 또는 가상화 시스템의 경우 베이스 이미지를 정기적으로 스캔하고 패치합니다. 베이스 이미지를 패치하는 경우, 해당 이미지를 기반으로 하는 모든 컨테이너 및 클라우드 리소스를 다시 빌드하고 재배포합니다.

마지막으로, 자동화를 적용하여 패치 작업을 간소화합니다. 패치 자동화 워크플로우를 생성하여 작업을 가속화하고, 오류 발생 위험을 줄이며, 시스템 전반의 일관성을 높입니다. 예를 들어, 애플리케이션 및 인프라 모두에 Jenkins 기반의 지속적인 통합/지속적인 배포(CI/CD) 파이프라인을 사용하여 패치와 같은 라이프사이클 프로세스를 자동화할 수 있습니다.

전략적 단계

다음 단계를 따라 강력한 패치 및 업데이트 전략을 세우세요.

1. 패치가 필요한 시스템을 식별합니다.
2. 위협 모델, 예상 위험, 성능 영향, 가능한 패치 기간에 따라 작업의 우선순위를 정합니다.
3. 패치 적용을 자동화하여 전통적인 인프라 및 하이브리드 클라우드 인프라 모두에 대한 일관성과 반복 가능성을 개선합니다.
4. 패치 전략을 주기적으로 재평가하고 조정하며 진화하는 기능, 기술 및 위협에 대응합니다.

보안 고려 사항

오픈소스 기술

왜 중요할까요?

오픈소스 기술은 클라우드와 컨테이너 운영에 필수적인 요소이지만, 조직에서 무서명(unsigned) 소프트웨어를 사용하거나 기술을 보안이 되지 않은 방식으로 배포하는 경우 보안 취약점을 야기하는 원인이 될 수 있습니다. 업스트림 커뮤니티에서 직접 다운로드한 확인되지 않은 오픈소스 소프트웨어를 사용하는 경우, 제3사의 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. 2018년에 공급망 공격은 78% 증가했습니다.[5]

권장 사항 및 모범 사례

현재 사용하는 오픈소스 기술을 누가 배포한 것인지 파악하고 안전한 방식으로 활용해야 합니다. 우선, 조직에서 사용 중인 오픈소스 기술 목록을 작성하고, 널리 알려지고 신뢰할 수 있는 출처에서 취득한 오픈소스 기술이 아니라면 사용을 중지해야 합니다. 프로세스와 정책을 정의하여 나머지 기술을 IT와 보안 팀이 제어할 수 있도록 합니다.

또한, 오픈소스 기술을 안전하게 사용하기 위한 전략을 세워야 합니다. 신뢰할 수 있는 출처에서 가져온 오픈소스 기술을 사용하고, 자동화된 방식으로 지속적으로 패치를 적용하며, 보안을 중심에 두고 설정하는 조치가 이 전략에 포함되도록 합니다. 전체 라이프사이클 전반에 걸쳐 기업에 적합한 지원을 제공하는 엔터프라이즈급 오픈소스 제품을 사용하도록 권장해야 합니다.

78% 전년 대비 2018년 서플라이 체인(supply chain) 공격 증가율[5]

전략적 단계

다음과 같이 오픈소스 기술의 보안을 강화하십시오.

상용 버전으로 전환

업스트림 오픈소스 프로젝트에서 바로 가져온 오픈소스 소프트웨어 대신, 신뢰할 수 있는 **상용 버전**으로 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.

이 기사에서 오픈소스 기술에 보안을 적용하는 방식을 자세히 알아보세요.

템플릿에 기반한 오픈소스 소프트웨어 배포

관리 및 플랫폼 툴이 사전 정의되고 검증된 템플릿에 기반한 셀프서비스 프로비저닝을 제공하는지 확인합니다. 템플릿을 사용하면 신뢰할 수 있는 최신 오픈소스 기술만 배포할 수 있습니다. 또한, 신속하고 자동화된 배포를 통해 IT 및 보안 팀이 제어할 수 없는 리소스를 배포하는 대신에 인증된 IT 리소스를 사용하도록 권장합니다.

5 *Symantec, "인터넷 보안 위협 보고서, Volume 24(Internet Security Threat Report, Volume 24)", 2019년 2월.*

지금 시작해 보세요

하이브리드 클라우드 보안은 모든 조직에서 중요하게 고려해야 하는 사항입니다. 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 엔터프라이즈급 지원, 핸즈온 교육 및 전문가 서비스를 제공하여 하이브리드 클라우드 환경을 보다 효율적이고 안전하게 구축하고 운영할 수 있도록 도와드립니다.

다음 리소스를 읽고 Red Hat의 보안 및 컴플라이언스에 대한 접근 방식을 자세히 알아보세요.

- **하이브리드 클라우드 보안 개요**
- **지속적인 IT 보안을 위해 왜 Red Hat을 선택해야 할까요?**
- **보안 및 컴플라이언스를 자동화해야 하는 이유**
- **Red Hat® Services: 시스템 보안 및 컴플라이언스 자동화**

무료 디스커버리 세션을 예약해 보세요

redhat.com/ko/services/consulting

Lucy Huh Kerner 소개 (Red Hat, 시니어 수석 보안 글로벌 기술 에반젤리스트 및 전략 담당자)

Lucy Huh Kerner는 보안 관련 리더십 개발을 돕고, 전체 Red Hat 포트폴리오의 보안을 위한 글로벌 기술 및 GTM(Go-To-Market) 전략을 이끌고 있으며, 글로벌 업계, 고객, 파트너, 애널리스트 및 언론에 보안 관련 기술 콘텐츠를 작성하여 지원하고 수많은 글로벌 이벤트에서 주요 발표를 해왔습니다. Lucy Huh Kerner는 현 직책 이전에 Red Hat 북미 공공 부문 팀의 시니어 클라우드 솔루션 아키텍트로 근무했으며, 클라우드 기술에 대한 전문 지식을 활용하여 광범위한 북미 공공 부문 고객을 위한 Red Hat 클라우드 솔루션을 설계하고 제공하여 Red Hat 클라우드 영업을 지원했고, 소프트웨어 및 하드웨어 개발 엔지니어 겸 사전 영업 솔루션 아키텍트로서 사이버 보안의 다양한 측면을 다루며 15년 이상의 전문 경력을 보유하고 있습니다.

F18867_0220_KVM

Red Hat