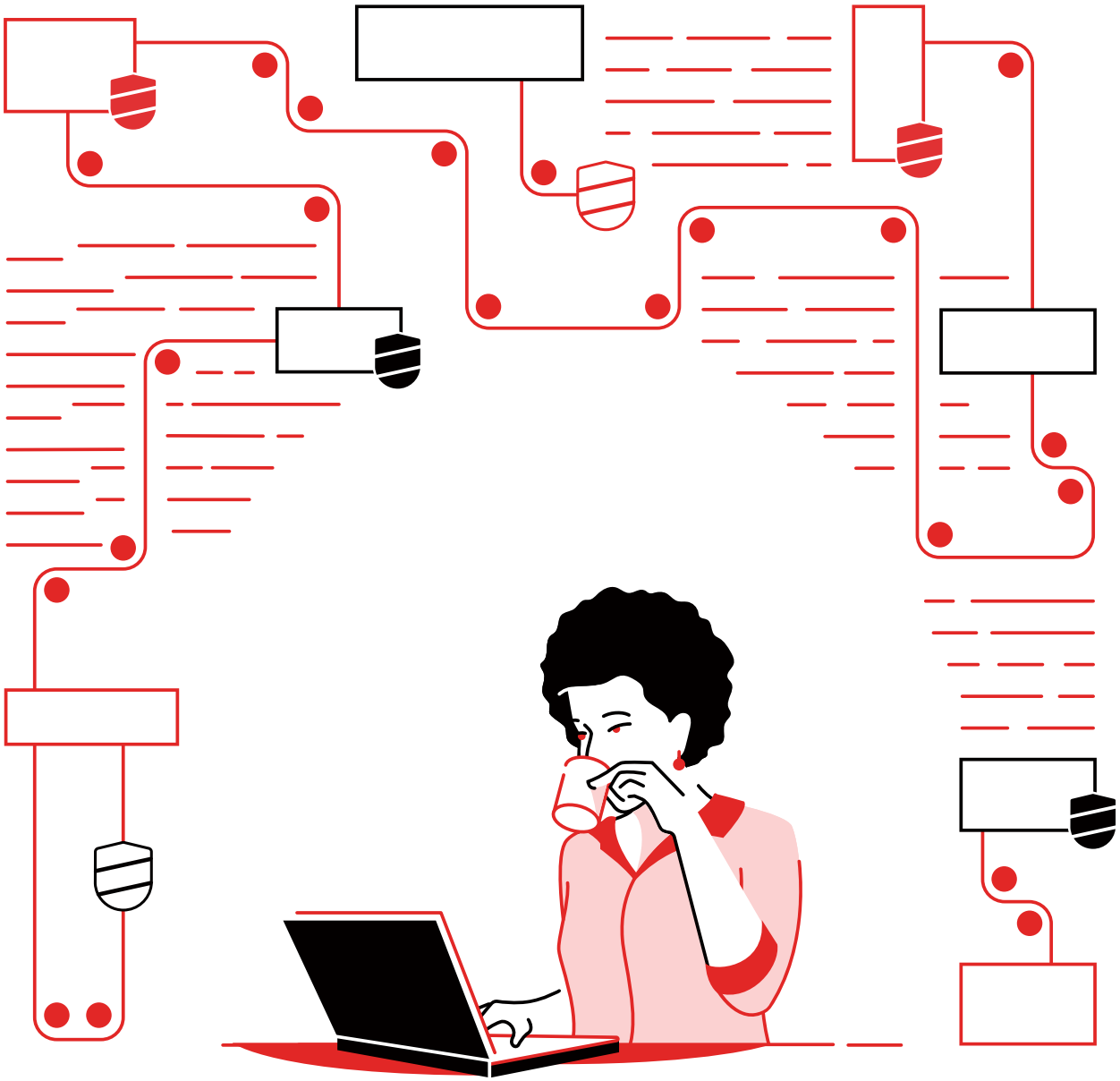
보안 운영 센터의 간소화

통합 자동화 플랫폼으로 속도, 시간, 보안 향상



Red Hat

목차

IT 보안은 왜 최우선 과제가 되었을까요?

보안은 대부분의 기업에서 중요한 문제입니다. 실제로 CEO의 33%는 사이버 위협을 매우 우려하는 것으로 나타났습니다.[1] 이러한 불안에는 근거가 있습니다. 32%의 기업이 지난 20년간 심각한 사이버 공격을 경험한 적이 있기 때문입니다.[2]

기업의 보안 문제에 대한 해결은 쉽지 않으며, 매우 중요한 과제입니다. 보안 팀은 경쟁 관계에 있는 다수의 벤더가 제공하는 각종 툴과 서비스를 사용해 복잡한 환경을 결합하고 유지, 관리 및 조정해야 합니다. 매년 제품과 서비스의 수량이 늘어나면서 보안 팀은 보안 환경 변화에 따라 새로운 제품을 지속적으로 연구, 평가 및 통합해야 하는 상황입니다.

또한 보안 침해의 빈도와 심각도 및 비용도 계속 증가하고 있습니다. 2년 이내에 보안 침해가 발생할 확률은 2014년 22.6%에서 29.6%로 높아졌습니다.[3] 각 데이터 침해에 관련된 평균 확률은 2018년부터 2019년까지 3.9% 증가했습니다.[3] 또한 데이터 침해로 인한 비용은 2019년에 평균 392만 달러로 증가했습니다.[3]

대부분의 기업은 보안 운영 작업을 수동으로 처리합니다. 인력이 보안 관련 작업을 수행하는 경우 시간이 많이 소요될 수 있고 반복적이며, 오류가 발생하기 쉽습니다. 그 결과 보안 팀은 과중한 업무 부담을 떠안게 되며, 많은 툴을 사용하게 되고 위협 알림 수신도 증가하게 됩니다. 실제로 보안 팀의 60%는 하루에 5,000개 이상의 알림을 받으며 16%는 매일 10만 개 이상을 받습니다.[4]

뿐만 아니라 인프라 규모와 복잡성이 증가하면서 취약점을 식별해 보안 침해를 확인하기가 점점 어려워지고 있습니다. 대다수의 보안 툴은 서로 통합되지 않으므로 보안 팀의 수동 작업이 늘어나게 됩니다. 그에 따라 인시던트 조사와 대응 시간도 길어질 수 밖에 없습니다. 2019년에 데이터 침해를 식별하고 방지하는 데 걸리는 평균 시간은 279일로 나타났는데, 이는 2018년에 비해 4.9% 늘어난 수치입니다.[3] 그리고, 팀을 확장하고 변화에 대응하기 위해 필요한 신규 인력을 확보하기도 어렵습니다. 2019년에 조직의 39%는 사이버 보안 기술 역량이 부족하다고 밝혔습니다.[2] 마지막으로, 사이버 보안 활동 예산도 한정되어 있습니다. 높은 수준의 사이버 복원력을 확보하는 데 충분한 예산을 갖추고 있다고 답한 조직은 33%에 불과했습니다.[5]

그 결과, 일반적인 보안 팀은 수신 알림의 48%만 검토해 이에 대응하며, 실제 위협의 50%만 해결됩니다.[4] 그로 인해 많은 기업이 공격에 취약한 상태에 놓여 있습니다.

77% 의 기업이 자동화 비중을 높여 간소화를 실현하고 자사의 보안 에코시스템 내 대응 시간을 단축할 계획을 갖고 있습니다.[4]

비효율적인 보안의 영향

보안 침해의 빈도와 심각도 및 비용이 늘어나고 있습니다.

392만 달러(US$)
데이터 침해로 인한 평균 비용(2019년)[3]

279일
데이터 침해 식별 및 방지에 대한 평균 시간(2019년)[3]

122만 달러(US$)
침해 식별 및 방지에 의한 절감 비용

200일
이내에 침해 식별 및 차단된 경우[3]

29.6%
2년 이내에 보안 침해를 경험할 확률[3]

50%
실제 위협 중 해결된 위협의 비율[4]

1 *PWC, "23회 연례 글로벌 CEO 설문조사: 높아지는 불확실성의 파도를 헤쳐가는 법(23rd Annual Global CEO Survey: Navigating the rising tide of uncertainty)," 2020년.* pwc.com/ceosurvey.

2 *Harvey Nash 및 KPMG, "2019 CIO 설문조사: 관점의 변화(CIO Survey 2019: A Changing Perspective)," 2019년.* home.kpmg/xx/en/home/insights/2019/06/harvey-nash-kpmg-cio-survey-2019.html.

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

4 *Cisco, "Cisco 벤치마크 설문조사: 혁신 기업의 현재와 미래(Cisco Benchmark Study: Securing What's Now and What's Next)," 2020년 2월.* cisco.com/c/en/us/products/security/ciso-benchmark-report-2020.html.

5 *Ponemon Institute(IBM Security 후원), "사이버 복원력을 갖춘 기업(The Cyber Resilient Organization)," 2019년 4월.* ibm.com/account/reg/us-en/signup?formid=urx-37792.

보안 자동화란 무엇일까요?

보안 자동화란 기업의 보안 상태 유지와 관련된 수동 태스크를 자동화하는 것을 말합니다. 여기에는 다양한 사례가 포함되며 대체로 4개 카테고리로 나눌 수 있습니다.

대응 및 문제 해결
보안 애널리스트 참여, 지침 등을 포함한 이벤트 기반 활동

보안 운영
기술 팀이 보안 인프라에서 수행하는 일상적인 프로세스 및 정책 기반 활동

보안 컴플라이언스
인프라가 보안 정책 및 규정을 준수하도록 보장하는 활동

보안 강화
타겟 의도와 목표에 따라 맞춤화된 보안 정책을 인프라에 적용하는 활동

보안 컴플라이언스 및 보안 강화에 대해 자세히 알아보기

자동화를 통해 보안 컴플라이언스 및 강화를 어떻게 해결할 수 있는지 다음 자료에서 확인해 보세요.

- **E-book: 하이브리드 클라우드 보안 강화**
- **개요: 보안 및 컴플라이언스를 자동화해야 하는 이유**
- **데이터시트: Red Hat Services - 보안 및 안정성 워크플로우 자동화**

본 e-book은 대응 및 문제 해결 활동과 보안 운영 작업의 자동화를 중점적으로 다룹니다.

보안 운영 작업, 대응 및 문제 해결 활동을 지원하는 자동화의 이점

속도 및 효율성 증대

자동화는 태스크를 간소화하고 수동 작업의 필요성을 최소화하므로 보안 운영 작업 속도를 높여 직원들이 높은 가치를 창출하는 이니셔티브에 다시 집중할 수 있습니다. 또한 IT 인프라의 복잡성도 줄여줍니다. 고도로 자동화된 기업의 40%는 적정 수의 보안 솔루션과 기술을 갖추고 있다고 답했습니다.[6]

스케일에 따른 보안 강화

보안 인프라 전반에 자동화를 적용하면 일관성이 향상되어 보다 포괄적인 보안을 구현할 수 있습니다. 각 직원들은 더 많은 툴과 기기 및 시스템을 관리할 수 있으므로 스케일에 따라 운영할 수 있습니다. 자동화를 사용하면 인적 오류가 발생할 위험도 줄일 수 있어 정확성이 개선됩니다.

보안 침해 리스크 및 비용 감소

대규모 자동화를 추진하는 기업들은 보안 사고와 비즈니스 운영 중단을 더 잘 방지할 수 있는 것으로 나타났습니다.[6] 보안 자동화를 완전히 배포하면 평균 보안 침해 비용을 95%까지 줄일 수 있습니다.[7] 그 결과로, 기업의 52%는 보안 자동화를 어느 정도 구축했으며 36%는 향후 24개월 내에 자동화 비율을 높일 계획이라고 밝혔습니다.[7]

6 *Ponemon Institute(IBM Security 후원), "사이버 복원력을 갖춘 기업(The Cyber Resilient Organization)," 2019년 4월.* ibm.com/account/reg/us-en/signup?formid=urx-37792.

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

자동화로 보안 툴, 시스템 및 프로세스 통합

인력, 프로세스 및 툴을 유연하고 일관된 플랫폼과 통합

자동화 플랫폼은 보안 팀과 툴, 프로세스 사이의 통합 계층 역할을 할 수 있습니다. 유연하고 상호 운용 가능한 플랫폼은 다음 작업을 지원합니다.

- 보안 시스템, 툴, 팀을 연결
- 시스템 정보를 수집해 이를 사전 정의된 시스템과 위치로 수동 작업 없이 신속하게 이동
- 중앙화된 인터페이스에서 신속히 설정 변경 및 전파
- 사용자의 보안 툴 및 프로세스와 관련된 사용자 정의 자동화 콘텐츠 생성, 유지관리 및 액세스
- 위협이 감지되는 경우 다양한 보안 툴 전체에 자동화된 작업 트리거

조직 전체에 일관된 자동화 플랫폼과 언어를 사용하면 커뮤니케이션과 협업 개선 효과도 누릴 수 있습니다. 보안 포트폴리오에 포함된 모든 솔루션이 동일한 언어를 통해 자동화되는 경우, 애널리스트와 운영자가 모두 단시간에 제품 전체의 작업을 수행할 수 있으므로 보안 팀의 전반적인 효율성이 극대화됩니다. 또한 보안 및 IT 팀은 공통 프레임워크와 언어를 통해 내부적으로뿐만 아니라 조직 전체에서 설계, 프로세스 및 아이디어를 보다 손쉽게 공유할 수 있습니다.

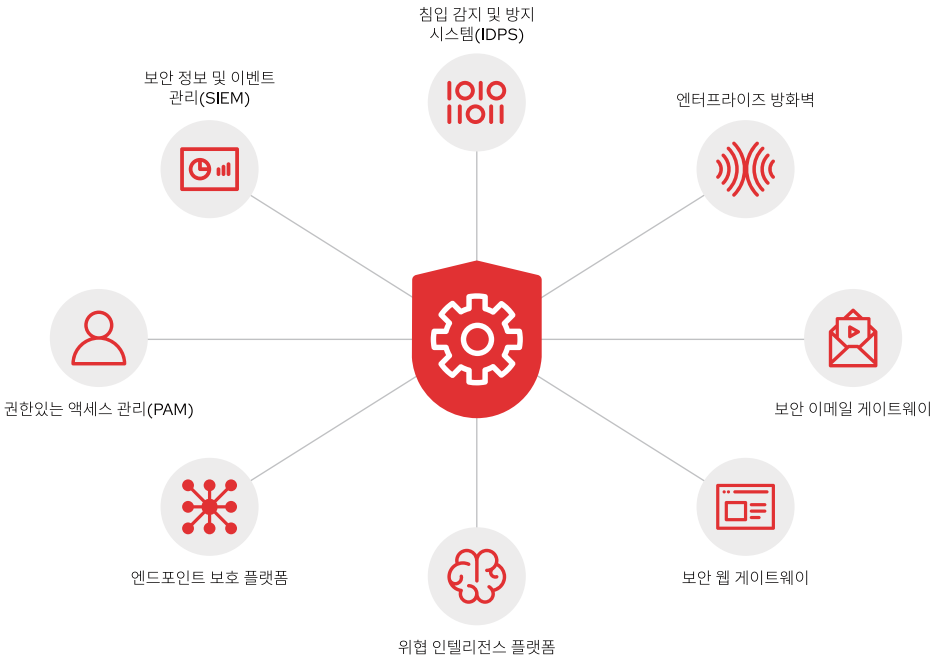


그림 1. 자동화 플랫폼은 보안 시스템, 툴, 팀을 연결합니다.

자동화 성공 =
구성원 + 프로세스 + 플랫폼

자동화의 가치를 극대화하려면 툴 이상의 요소, 즉 구성원, 프로세스, 플랫폼이 모두 필요합니다.

- **구성원**은 모든 비즈니스 이니셔티브의 핵심입니다. 팀 내에서는 물론 여러 팀 간의 활발한 참여를 통해 직원들은 아이디어를 공유하고 보다 효율적으로 협업할 수 있습니다.
- **프로세스**는 조직 내에서 처음부터 끝까지 프로젝트를 진행시킵니다. 명확히 문서화된 프로세스는 효과적인 자동화의 필수 요소입니다.
- 자동화 **플랫폼**은 자동화 자산 구축, 실행 및 관리 기능을 제공합니다. 단순한 자동화 툴과 달리 자동화 플랫폼은 기업의 스케일에 따라 일관된 자동화 콘텐츠 및 정보를 구축, 배포, 공유하기 위한 통합 기반을 제공합니다.

e-book 읽기

보안 자동화 여정

조직의 어떤 측면에서든 자동화는 즉시 실현할 수 있는 것이 아니며, 양자택일의 문제도 아닙니다. 보안 자동화는 하나의 여정입니다. 각 기업은 요구 사항에 따라 출발점과 도착점이 다릅니다. 그러한 요구 사항에 따라 각 기업의 자동화 여정도 달라집니다. 하지만 여정의 어느 단계에 있든지 소규모의 보안 자동화 노력만으로도 이점을 실현할 수 있습니다.

보안 자동화 성숙도 평가

기업의 보안 자동화 성숙도는 대부분 주요 3단계 중 하나에 해당됩니다. 기업의 현재 단계를 판단하면 적합한 때에 적합한 툴과 프로세스를 도입하는 데 도움이 되므로 자동화 여정을 성공적으로 수행할 수 있습니다.

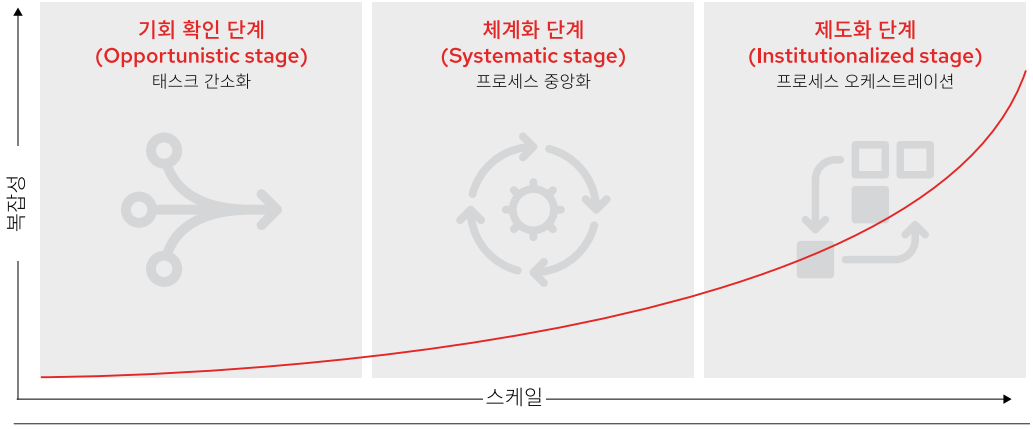


그림 2. 보안 자동화 성숙도 단계

1단계: 기회 확인

이 단계에서는 보안 운영 작업을 자동화하여 시간을 절약하는데 집중합니다. 공통 목표로는 유사한 기기 및 기술 전반에서 보안 작업을 표준화하고 다양한 벤더 제품 전체에서 수행되는 수동 태스크를 간소화하는 것 등이 있습니다.

2단계: 체계화

이 단계에서는 통합적인 보안 운영 툴과 서비스를 도입하여 프로세스와 효율성을 개선하는 데 집중합니다. 공통 목표로는 보안 프로세스를 상위 수준의 워크플로우에 통합하고 보안 대응 프로세스를 중앙화하는 것 등이 있습니다.

3단계: 제도화

이 단계에서는 조직 전체에서 협업을 강화하고 보안을 통합하는 데 집중합니다. 공통 목표로는 보안의 모든 측면을 포괄하는 프로그래밍 방식의 자동화된 워크플로우 생성과 보안 및 IT 기술을 통합하는 것 등이 있습니다.

블로그 게시물 읽기

활용 사례 및 통합

보안 자동화 구현 단계

보안 자동화를 위한 공통적 활용 사례

이러한 각 활용 사례는 보안 자동화 여정의 출발점이 될 수 있습니다. 규모가 작고 간단한 사례에서 시작해 시간이 지남에 따라 확장하는 것이 핵심입니다.

조사 강화

보안 경고 및 인시던트를 조사하려면 다양한 보안 시스템 정보를 수집해 실제 이벤트가 발생했는지 판단해야 합니다. 정보는 일반적으로 일련의 사용자 인터페이스, 이메일 및 전화 통화를 통해 수집됩니다. 이처럼 비효율적인 프로세스는 위협 대응을 지연시켜, 비즈니스를 취약하게 만들고 보안 침해와 관련된 잠재적 비용을 증가시킬 수 있습니다. 자동화를 통해 보안 시스템 전체에서 프로그램에 따라 정보를 종합할 수 있으므로 보안 정보 및 이벤트 관리(Security Information and Event Management, SIEM) 시스템을 통해 수행되는 분류 활동을 온디맨드로 강화할 수 있습니다. 그에 따라 경고 및 인시던트를 보다 신속히 평가하고 대응할 수 있습니다.

위협 헌팅(Threat hunting)

위협 헌팅은 사전 예방적으로 잠재적인 보안 위협을 식별해 조사하는 활동입니다. 인시던트 조사와 마찬가지로 직원은 여러 시스템 간 정보를 수동으로 수집하고 전송합니다. 자동화를 사용하면 경고, 상관관계 검색 및 서명 조작을 맞춤화하고 간소화하여 잠재적 위협을 더욱 신속히 검사할 수 있습니다. 또한 SIEM 상관관계 쿼리 및 침입 감지 시스템(Intrusion Detection System, IDS) 룰을 자동으로 생성하고 업데이트하여 감지를 개선할 수 있습니다. 따라서 조직의 보안 방어 체계를 더 자주 업데이트하고 비즈니스를 더욱 효율적으로 보호할 수 있게 됩니다.

인시던트 대응

인시던트 대응은 보안 침해가 지속되지 못하도록 대응하는 활동입니다. 보안 침해가 발견되면 보안 팀은 스케일에 따라 신속히 대응하여 이를 중지시킵니다. 그러나 대응 작업에는 다양한 수동 태스크가 포함되므로 문제 해결이 지연되어 조직이 더 오래 취약한 상태로 남아있게 됩니다. 자동화를 사용하면 작업을 반복 가능한 사전 승인 플레이북으로 코드화하여 보다 빨리 대응할 수 있습니다. IP 주소 또는 도메인 공격을 차단하는 등의 태스크를 빠르게 수행할 수 있으므로, 위협적이지 않은 트래픽을 허용하고, 손상된 자격 증명을 비활성화하며, 의심스러운 워크로드를 격리해 추가 조사를 수행하여 해당 인시던트와 관련된 피해를 최소화할 수 있습니다.

통합의 중요성

통합 자동화 방식에는 자동화 플랫폼과 보안 기술 간 통합이 필요합니다. 기본적인 통합 기능은 다음과 같습니다.

- **방화벽**: 네트워크 간 트래픽 흐름을 제어하여 인터넷에 노출된 애플리케이션을 보호합니다. 자동화는 정책 및 로그 설정 변경을 빠르게 처리할 수 있습니다.
- **침입 감지 및 방지 시스템(IDPS)**: 네트워크 트래픽을 모니터링하여 의심스러운 활동을 감지하고 위협 알림을 생성하고 공격을 차단합니다. 자동화는 룰 및 로그 관리를 간소화할 수 있습니다.
- **보안 정보 및 이벤트 관리 시스템**: 보안 이벤트를 수집하고 분석하여 위협을 탐지하고 이에 대응하도록 지원합니다. 자동화는 프로그램에 따라 데이터 소스에 액세스할 수 있도록 해줍니다.
- **권한있는 액세스 관리(PAM) 툴**: 권한있는 계정 및 액세스를 모니터링하고 관리합니다. 자동화는 자격 증명 관리를 간소화합니다.
- **엔드포인트 보호 시스템**: 기기를 모니터링하고 관리하여 보안을 강화합니다. 자동화는 공통 엔드포인트 관리 태스크를 간소화할 수 있습니다.

자세히 알아보기

Red Hat Ansible Automation Platform으로 보안 운영 센터 간소화

사용할 수 있는 자동화 솔루션은 많지만, 효과적인 보안 자동화에 필요한 모든 기능이 포함된 솔루션은 많지 않습니다. 자동화 플랫폼은 다음을 제공할 수 있어야 합니다.

- **보편적이고 접근 가능한 자동화 언어:** 쉽게 이해하고 쓸 수 있는 언어를 사용하면 서로 다른 도메인 전문성을 갖춘 보안 팀 구성원들 간 정보를 공유하고 문서화할 수 있습니다.
- **개방적이고 편향되지 않은 접근 방식:** 자동화 플랫폼이 효과적으로 작동하려면 전체 보안 인프라 및 벤더 에코시스템과 서로 호환되어야 합니다.
- **확장 가능한 모듈식 설계:** 모듈식 플랫폼을 사용하면 자동화를 단계별로 배포할 수 있으며, 확장성을 활용하여 필요에 따라 나중에 보안 툴을 추가할 수도 있습니다.

Red Hat 솔루션으로 보안 조직의 역량 확대

스케일에 따라 자동화 서비스를 구축하고 운영하기 위한 기반으로서, **Red Hat® Ansible® Automation Platform**은 보안 자동화를 구현하는 데 필요한 모든 툴과 기능을 제공합니다. 이는 읽기 쉽고 간소화된 자동화 언어에 신뢰할 수 있는 구성 가능한 실행 환경 및 보안 중심 공유 및 협업 기능을 결합합니다. 개방형 기반으로 보안 및 IT 인프라 내 거의 모든 요소를 연결해 자동화하여, 조직 전체에서 참여 및 공유를 위한 공통 플랫폼을 생성할 수 있습니다. Red Hat Ansible Automation Platform은 IT 및 네트워크 운영과 DevOps를 포함한 다른 영역에서도 기술력을 인정받았습니다.

모듈, 롤, 플레이북을 포함한 일련의 **보안 중심 Ansible 지원 컬렉션**이 이 플랫폼에 포함되어 있습니다. 이러한 자산은 사이버 위협과 보안 운영 작업에 보다 통합적으로 대응하기 위해 다양한 클래스의 보안 솔루션 활동을 조정합니다.

- 워크플로우 및 플레이북을 연결하여 모듈식 재사용성 지원
- 로그 통합 및 중앙화
- 로그 디렉터리 서비스 및 액세스 제어 지원
- RESTful 애플리케이션 프로그래밍 인터페이스(API)를 사용해 외부 애플리케이션 통합

Red Hat Ansible Automation Platform에는 또한 자동화를 최적화할 수 있는 툴과 기능이 포함되어 있습니다. **Automation Analytics**는 조직의 자동화 사용 방식을 파악합니다. **Automation Hub**는 팀 구성원이 중앙화된 리포지토리를 통해 인증된 자동화 콘텐츠에 액세스할 수 있도록 합니다. **Content Collection**은 자동화 자산의 관리, 분산 및 사용을 간소화합니다.

전문가의 지원

Red Hat은 기업의 자동화를 빠르고 성공적으로 배포할 수 있도록 지원합니다.

- **Red Hat Services Program: 자동화 채택(Automation Adoption)**은 전사적인 자동화 도입 여정을 관리하기 위한 프레임워크를 제공합니다.
- **Red Hat 교육 및 자격증**은 핸즈온 교육과 실용적인 자격증을 제공하여 자동화를 보다 효과적으로 활용하는 데 도움이 됩니다.
- **Red Hat 지원**은 기업의 IT 여정의 성공을 돕기 위해 기업과 협업합니다. 권위있는 어워드로 입증된 웹 지원[8]을 통해 모범 사례, 설명서, 업데이트 및 보안 경고와 패치를 이용할 수 있습니다. 또한, 지원 엔지니어 또는 테크니컬 어카운트 매니저(TAM)에 문의하여 문제를 해결하고 전문 가이드를 지원받을 수 있습니다.
- **인증된 파트너 콘텐츠 컬렉션**으로 다양한 벤더가 제공하는 하드웨어 및 소프트웨어를 손쉽게 자동화할 수 있습니다. 이처럼 신뢰할 수 있는 사전 구축 자동화 콘텐츠는 Automation Hub를 통해 사용할 수 있으며 파트너사와 Red Hat이 모두 지원합니다.

8 Red Hat 고객 포털 수상 이력 및 인지도, https://access.redhat.com/ko/recognition.

자동화 실현

Red Hat Ansible Automation Platform으로 검증된 비즈니스 가치 제공

Red Hat Ansible Automation Platform은 보다 효율적이고 간소화된 방식으로 보안 운영 센터를 자동화합니다. 애널리스트 연구에 따르면 Red Hat Ansible Automation Platform을 사용하는 조직은 측정 가능한 비즈니스 가치를 보여줍니다. 실제로 IDC는 Red Hat Ansible Automation Platform 사용 경험이 있는 다양한 의사 결정자들을 인터뷰한 결과, 각 조직이 자동화를 통해 생산성과 민첩성을 대폭 향상하고 운영상 이점을 실현했음을 파악했습니다.

더 효율적이고 생산적인 IT 보안 팀[9]

더 효율적인 보안 인시던트 완화[9]

더 효율적인 보안 패치[9]

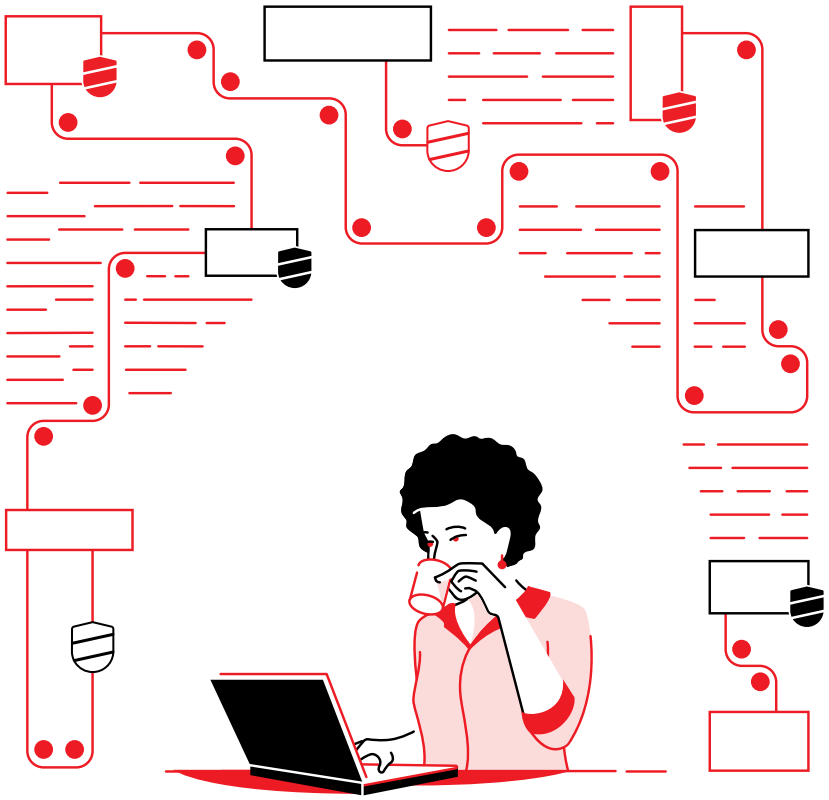
"Red Hat Ansible Automation Platform은 우리 IT 팀이 효율적으로 협업할 수 있도록 도와주는 최적의 솔루션입니다. 서버, 보안, 네트워크, 데이터베이스 팀들이 모두 별도의 티어에서 작업하고 Red Hat Ansible Automation을 사용해 자체 플레이북을 만들 수 있습니다."[9]

애널리스트 리포트 읽기

9 *IDC 백서, Red Hat 후원. "Red Hat Ansible Automation의 IT 민첩성 및 시장 출시 속도 개선(Red Hat Ansible Automation Improves IT Agility and Time to Market)," 2019년 6월.* redhat.com/ko/resources/business-value-red-hat-ansible-automation-analyst-paper.

보안 운영 센터를 간소화할 준비가 되셨나요?

자동화를 통해 점점 늘어나는 보안 위협을 스케일에 따라 더욱 신속하게 식별하고 이에 대응할 수 있습니다. Red Hat은 일관된 협업 자동화 플랫폼으로 보안 팀, 툴, 프로세스를 연결하여 비즈니스를 보호하도록 지원합니다.



Red Hat Ansible Automation Platform으로 보안을 자동화하는 방법을 알아보세요. **red.ht/automate-security**

F24343_0720_KVM

Red Hat