Red Hat

# Security Spotlight:
# 인적 오류로 인한 비용과 자동화의 장점

정부 기관에서 보안 관리에 대한 수동적 접근 방식을 재고하는 이유와 지능형 자동화를 통해 많은 비용을 초래하는 보안 격차의 잠재적 위협을 방지하는 방법

다음

# 이 e-book에서 다루는 내용:

01 소개: 증가하는 사이버 범죄 위협

02 모든 인력이 참여하는 효과적인 보안 전략

03 리스크 관리의 공통 과제

04 자동화로 보안 태세 강화

05 사이버 보안 접근 방식에서 Red Hat의 역할

# 01 소개: 증가하는 사이버 범죄 위협

사이버 범죄가 증가하고 있습니다. 지난 회계연도에 호주 사이버 보안 센터(Australian Cyber Security Centre, ACSC)에는 전년 동기 대비 13% 증가한 총 67,500건의 사이버 범죄 신고가 보고되었으며 자체 보고된 손실액은 총 330억 달러가 넘습니다.[3] 이러한 인시던트 중 약 4분의 1이 호주의 중요 인프라와 관련된 기관에 영향을 미쳤습니다.

정부 기관이 새로운 기술을 수용하고 하이브리드 업무 모델에 적응함에 따라 사이버 공격자들도 공격 형태를 변화시키고 있습니다. 인력과 컴퓨팅 리소스는 더욱 분산되고 있으며, 빠르게 진화하는 IT 인프라 환경은 악의적인 사용자들에게 보안 격차와 취약점을 악용할 수 있는 새로운 기회를 제공합니다. 이로 인해 데이터 침해가 조직에 초래하는 비용이 늘고 있습니다. 강력한 보안 태세를 개발한 조직조차도 이러한 환경에서 점차 더 많은 리스크에 직면하고 있습니다.

## 사이버 범죄에 대응하는 사전 예방적 보안

사이버 범죄자들이 보호되는 시스템과 데이터를 침해하는 새로운 방법을 끊임없이 고안함에 따라 조직은 사이버 공격을 막기 위해 더욱 전략적이고 사전 예방적인 보호 기능을 개발해야 한다는 내외부적인 압박을 받고 있습니다. 실제로 데이터 보안과 개인정보 보호 조치는 반드시 더욱 포괄적인 규칙과 규정을 준수해야만 합니다.

예를 들어, 뉴사우스웨일스주(NSW) 사이버 보안 정책은 현재 ACSC Essential Eight 리스크 완화 전략에 대한 성숙도 평가를 시행하고 프로비저닝하도록 의무화하고 있습니다.[1] 또한 호주의 중요 인프라 법안의 보안법 개정안은 중요 인프라를 관리하거나 운영하는 정부 조직에 규제 부담을 잠재적으로 높입니다.[2]

## 방어 체계 강화

사이버 보안을 개선하고자 하는 조직은 기존의 취약점을 먼저 식별해야 합니다. 이미 포괄적인 전략이 마련되어 있는데도 인적 오류와 부적절한 교육으로 인해 보안이 저해될 수 있는 경우가 매우 많습니다. 사소한 실수라도 제대로 점검하지 않으면 시스템에 위험을 초래하고 이미 복잡한 문제를 악화시킬 수 있습니다. 따라서 많은 조직이 보안 전략에서 신뢰성을 높이고 리스크를 줄이기 위해 자동화를 도입하고 있습니다.

이 e-book에서는 인적 오류로 인한 리스크가 사이버 범죄와의 전쟁에 어떤 영향을 미치는지 살펴봅니다. 또한 주요 사이버 보안 리스크 완화 전략을 자동화하여 보안을 강화하는 동시에 시간이 많이 소요되는 태스크로 인한 IT 팀의 부담을 줄일 수 있는 방법에 대해 설명합니다.

### 호주의 사이버 범죄로 인한 비용

67,500

사이버 공격 신고 건수[3]

330억 달러

자체 보고된 손실액[3]

13%

전년 대비 공격 건수 증가율[3]

1. 뉴사우스웨일스주 정부. "DCS-2021-02 NSW 사이버 보안 정책." 2021년 2월.
2. 호주 의회. "보안법 개정안(중요 인프라) 법안 2021." 2021년.
3. "ACSC 연간 사이버 위협 리포트 2020-21(Annual Cyber Threat Report 2020-21)." 호주 사이버 보안 센터, 2021년 9월.

# 02 모든 인력이 참여하는 효과적인 보안 전략

### 사람은 실수를 합니다

IT 팀 내에서도 시스템의 취약점과 그로 인한 보안 리스크를 과소평가하거나 오해하는 경우가 많습니다. 리스크를 정확하게 평가하지 못하면 조직에 상당한 비용을 초래할 수 있습니다.

예를 들어, 기술 직원이 수동으로 방화벽을 업데이트한다고 가정해봅시다. 작은 실수를 저지르지만 이를 문제로 인식하지 않아 취약점이 해결되지 않은 채로 방치됩니다. 여기서 이들이 깨닫지 못한 점은 이처럼 사소한 오류 하나가 조직의 IT 시스템 전체에 중요 취약점을 유발하고, 사이버 범죄자들은 이를 빠르게 악용할 수 있다는 것입니다.

이 시나리오에서 기술 직원의 작은 실수는 데이터 손상, 산업과 정부의 데이터 보안 규제 위반, 서비스 중단, 시스템 다운타임 등 다양한 부정적인 결과를 야기할 수 있으며, 모두 조직에 큰 비용을 초래합니다.

애플리케이션에 패치를 적용하고 방화벽을 업데이트하는 것에서 관리 권한을 설정하고 강제 적용하는 데 이르기까지, 너무 많은 보안 퍼즐의 요소들을 수동으로 처리하는 과정에서 문제가 발생할 수 있습니다. 그리고 사이버 범죄자들이 이러한 취약점을 찾아내는 데 더욱 능숙해지면서 이러한 태스크 처리를 운영 팀에만 의존하면 해롭거나 회복 불가능한 결과를 가져올 수 있습니다.

### 인재 부족으로 인한 보안 격차 심화

사이버 보안 기술은 부족한 상황이기 때문에 수동 작업 중에 인적 오류가 발생할 가능성이 높아집니다. 그야말로 보안 리스크를 평가하고 해결할 수 있는 기술을 갖추고 교육을 받은 인력 자체가 부족합니다. (ISC)[2]의 사이버 보안 인력 연구에 따르면, 호주는 사이버 보안 격차를 해소하기 위해 25,000명의 IT 보안 인력이 더 필요합니다.[4]

이와 같은 사이버 보안 전문가의 만성적인 부족으로 인해 정부 기관들은 리스크를 적절하게 관리하기가 더 어려워집니다. IT 팀은 이미 한계에 도달하여 애초에 보안 프로세스를 구축하는 것은 고사하고 조직 전반에서 이를 시행할 시간조차 없습니다.

### 보안 팀에 자동화 지원

수동 보안 프로세스와 기술 부족으로 인해 조직의 위험이 증가하는 문제를 해결하는 것은 사이버 범죄와의 전쟁에서 빼놓을 수 없는 부분이 되었으며, 자동화 솔루션은 이에 대한 유망한 솔루션을 제시합니다. 앞으로 자세히 살펴보겠지만, 보안 프로세스를 자동화하면 조직 전체에서 매우 필요한 일관성, 정확성, 확장성을 제공할 수 있습니다.

### 수동 보안 조치의 위험성

"보안 자동화를 갖추지 않은 조직은 2021년에 보안 침해로 평균 671만 달러의 비용이 발생한 반면, 보안 자동화를 완전히 배포한 조직은 평균 290만 달러의 비용이 발생했습니다."[5]

4. "회복탄력성을 갖춘 사이버 보안 전문가가 제시하는 미래를 위한 경로(A Resilient Cybersecurity Profession Charts the Path Forward)" (ISC)[2] 사이버 보안 인력 연구(Cybersecurity Workforce Study), 2021년.
5. "2021년 데이터 침해로 인한 비용 보고서(Cost of a Data Breach Report 2021)." IBM, 2021년.

# 03 리스크 관리의 공통 과제

## 정부 기관의 리스크 관리 개선 필요

공식 정보의 기밀성, 무결성, 가능성을 보장하기 위해 정부 기관은 정확하고 효율적으로 리스크를 식별하고 관리할 수 있어야 합니다. 보안 위협은 끊임없이 진화하기 때문에 조직의 리스크 프로파일과 보안 태세는 계속해서 변화에 적응할 수 있어야 합니다. 이러한 변화에 빠르게 대응할 수 있으려면 운영을 자동화하는 것이 중요합니다.

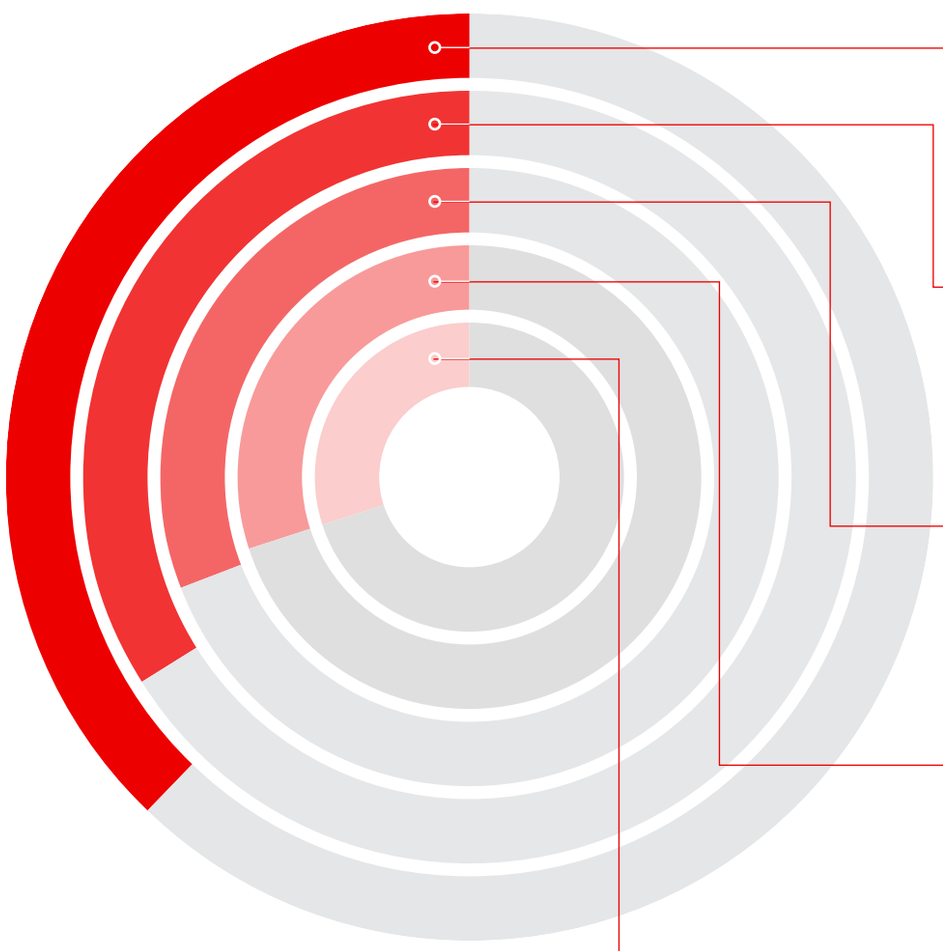
## 변화하는 보안 사례의 장애물

보안을 강화하고자 하는 정부 기관은 특히 변화 관리와 관련된 몇 가지 문제에 직면합니다. 일반적인 질문은 다음과 같습니다.

- 새로운 사이버 보안 이니셔티브를 구현하기 위해 팀을 어떻게 확장해야 할까요?
- 새로운 보안 프로토콜을 준수하기 위해 조직의 다양한 부분을 어떻게 지원해야 할까요?
- 조직이 필요로 하는 최신 보안 전략을 채택하면서 중요 서비스를 제공하는 기존 시스템의 보안을 향상하려면 어떻게 해야 할까요?
- 기존 아키텍처에 제로 트러스트와 같은 전략을 구현할 수 있을까요?

그러나 정부 기관은 이러한 고려 사항을 부담으로 여기는 대신, 변화하는 보안 환경을 보안 사례를 재평가하고 더욱 견고한 프로토콜을 구현할 수 있는 하나의 기회로 생각할 수 있습니다.

### 사이버 보안과 관련한 공통 과제



38%

빠르게 변화하는 위협에 대응[6]

34%

리스크와 행동에 관한 교육[6]

31%

내부 사이버 보안 태세 강화[6]

30%

사이버 보안 교육의 필요성[6]

30%

데이터 침해로 인한 법적/재정적 영향[6]

6. "2021 채널 현황(State of the Channel 2021)." CompTIA, 2021년 8월.

# 04 자동화로 보안 태세 강화

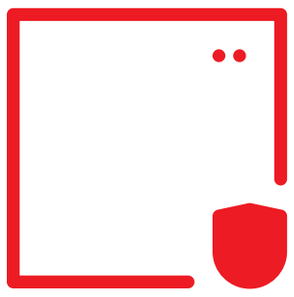
### 사이버 보안 전략의 주요 요소 자동화

리스크를 줄이고 사이버 범죄와의 전쟁에서 승리하기 위해 정부 기관은 사이버 보안 자동화로 전환하고 있습니다. 정기적이고 반복적인 업무를 자동화하면 사이버 보안 팀이 더욱 중요하고 전략적인 업무에 집중할 수 있습니다. 또한 자동화는 IT 팀이 인적 오류가 발생하기 쉽고 보안 리스크를 높이는 태스크와 작업 부하로 인해 과도한 부담에 시달리는 것을 방지할 수 있습니다.

ACSC Essential Eight는 자동화를 사용하여 사이버 보안 전략을 강화하는 방법을 설명합니다. Essential Eight를 구현할 때 많은 조직은 특히 현재의 리소스 제약과 기술 격차로 인해 인적 오류를 지속적으로 줄이거나 제거할 수 있는 방법이 없다는 사실에 어려움을 겪습니다.

이러한 문제점에 대응하기 위해 IT 리더들은 보안 프레임워크의 일부 요소를 자동화하는 것이 가능할 뿐만 아니라 필수적이라는 점을 깨닫고 있습니다. 다음 예시는 조직 내에서 자동화를 채택하기에 적합한 방법과 영역을 설명합니다.

### ACSC Essential Eight 자동화

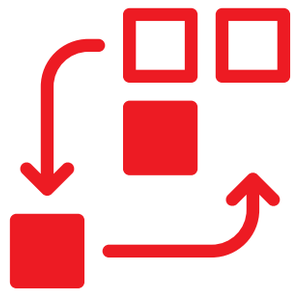


애플리케이션 제어

하이브리드 클라우드 전반에서 애플리케이션 제어 상태에 대한 변경 자동화

애플리케이션과 운영 체제에 대한 패치 적용

실행 전 검사, 콘텐츠 프로모션, 사후 업데이트 검증/테스트 자동화



백업과 복원

백업, 복원, 검증 테스트 자동화

## 패치 적용 프로세스 개선

공격을 방지하기 위해 Essential Eight는 조직이 악성 보안 문제로부터 보호하도록 정기적으로 애플리케이션에 패치를 적용하고 업데이트를 적용할 것을 권고합니다. 업데이트를 사용할 수 있게 되는 즉시 애플리케이션을 패치를 적용하는 것은 모범 사례일 뿐만 아니라 많은 경우 규제 요구 사항이기도 합니다. 그렇지만 수동 패치 적용은 항상 인적 오류에 취약하고, 특히 대규모 조직에서는 시간이 많이 소요될 수 있습니다.

패치 적용은 자동화된 워크플로우의 탁월한 활용 사례입니다. 조직은 테스트 수행, 실행 전 검사 설정, 패치 실행 등을 IT 직원에게만 의존하는 대신 검증과 테스트를 자동화할 수 있습니다. 그렇게 하면 적절한 보안 조치를 구현한 상태에서 이러한 모든 단계를 원활하고 효율적으로 진행할 수 있습니다.

## 관리 권한 관리

Essential Eight는 공격의 범위를 제한하기 위해 조직이 관리 권한을 제한할 것을 권고합니다. 권한 있는 액세스를 제어하면 인프라와 애플리케이션에 보안을 제공하고, 비즈니스 프로세스를 효율적으로 운영하며, 민감한 데이터와 중요 인프라의 기밀성을 유지할 수 있습니다.

조직 내에서 글로벌 제어 권한을 가지는 사용자는 소수 인원으로 한정되어야 합니다. 누가 권한을 가져야 하는지 결정하는 것은 어려운 일일 수 있습니다. 보안 인시던트의 영향 범위를 추정하고, 잠재적인 이벤트의 총 영향을 평가하는 것도 어려울 수 있지만, 이 방법을 통해 누군가 자격 증명을 오용하는 경우 발생할 문제를 예측할 수 있습니다. 그러면 IT 팀은 이러한 인시던트가 조직 전체에 영향을 미치지 못하도록 보안 조치를 구현할 수 있습니다.

권한 있는 액세스 관리 워크플로우를 자동화하고 액세스 자격 증명을 중앙에 저장하면 유출 위험성이 있는 애플리케이션에 이러한 자격 증명을 주입하지 않고도 전체 프로세스를 더욱 쉽게 관리하고 신뢰할 수 있습니다.

# 05 사이버 보안 접근 방식에서 Red Hat의 역할

## 미래에 대비한 사이버 보안 사례 구축

Red Hat® 솔루션은 기존 수동 프로세스를 자동화하여 조직 내 IT 팀의 인력 부족과 과도한 업무로 인해 인적 오류가 발생할 위험을 줄여줍니다. Red Hat의 오픈소스 제품은 클라우드 환경과 아키텍처 전반에 유연성과 확장성을 제공하여 조직이 현재와 미래 환경에 배포할 수 있도록 지원합니다.

어떤 사이버 보안 성숙도 모델 기반에서도 자동화를 사용하면 모든 조직이 실질적인 단계를 수행하여 자동화 계층을 빠르고 반복적으로 추가하여 수동 프로세스를 대체할 수 있습니다. 또한 Red Hat 솔루션은 리스크 완화와 대응을 모두 지원할 수 있습니다.

### Red Hat Ansible Automation Platform

Red Hat Ansible® Automation Platform은 사람이 읽을 수 있는 자동화 언어인 Ansible로 구축되어 복잡한 수동 프로세스를 자동화된 워크플로우로 전환합니다. Ansible Automation Platform을 사용하면 IT 팀이 다양한 보안 프로토콜을 엔터프라이즈 전반에서 자동화하고 통합할 수 있습니다. 이 플랫폼을 통해 조직은 엄선된 플레이북, 모듈, 롤 컬렉션을 통해 상호 조율되고 통합된 방식으로 위협에 대응할 수 있습니다.

Red Hat Ansible Automation Platform을 통해 조직은 다음을 자동화할 수 있습니다.

- CVE(Common Vulnerabilities and Exposures) 패치 적용
- 애플리케이션 제어 롤아웃
- 백업, 복원 또는 검증 프로세스

Ansible Automation Platform은 하이브리드 클라우드에서 엣지 환경에 이르기까지 규모에 따라 IT 자동화를 구축하고 운영하기 위한 보안 중심의 안정적인 엔터프라이즈 프레임워크를 제공합니다. 이 자동화 솔루션으로 개발자와 운영 팀에서 보안 팀, 네트워크 팀에 이르기까지 조직 전체의 사용자들이 Ansible Playbook을 생성, 공유, 관리할 수 있습니다. IT 관리자는 개별 팀에 자동화가 적용되는 방식에 대한 지침을 제공하는 한편, 오토메이션 크리에이터는 기존 지식을 활용하여 태스크를 작성할 수 있습니다.

또한 Ansible Automation Platform은 보안 기술의 관리와 통합을 자동화하는 데 사용할 수 있는 CyberArk, IBM, Splunk와 같은 인증 파트너가 제공하는 콘텐츠를 포함하고 있기 때문에 보안 솔루션의 통합 지점 역할을 할 수 있습니다.

**Ansible Automation Platform에 대해 자세히 알아보기 >**

### Red Hat Enterprise Linux

Red Hat Enterprise Linux®는 일관된 보안을 유지하면서 베어 메탈, 가상 환경, 클라우드, 엣지 풋프린트 전반에서 기존 애플리케이션을 확장하고 이머징 기술을 출시할 수 있는 기반을 제공합니다.

Red Hat Enterprise Linux는 보안 과제를 해결하기 위해 실용적인 세 가지 접근 방식을 취합니다.

- 위험 감소: 데이터, 시스템 또는 평판이 위험에 노출되기 전에 보안을 관리하여 침해를 줄입니다.
- 보안: 스케일에 따라 최소한의 다운타임으로 보안 제어를 자동화하고 지속적으로 유지 관리합니다.
- 컴플라이언스: 규제가 엄격한 환경의 조직에 대해 컴플라이언스 표준을 간소화합니다.

또한 Red Hat Enterprise Linux는 정보 보안 매뉴얼(ISM), Essential Eight와 같은 ACSC 지침에 따른 빌트인 보안 정책을 갖추고 있어 정부 기관이 새로운 디지털 서비스에 대한 보안 제어 롤아웃을 간편하고 일관되게 자동화하여 리스크를 더욱 효과적으로 관리할 수 있도록 지원합니다.

**Red Hat Enterprise Linux에 대해 자세히 알아보기 >**

Red Hat

이전

# Red Hat과 함께 보안을 강화하세요

**Red Hat이 귀사의 디지털 서비스 보안을 개선하도록 도와 드립니다.**

Red Hat은 ACSC의 지침을 자동화하고 보안 통합 자동화를 통해 리스크를 더욱 효과적으로 관리할 수 있도록 지원합니다.

**자세히 알아보려면 지금 문의하세요 ›**