

Security Center Automation

자신 있게 보안 규칙을 자동화하세요

Security Center Automation은 시스템 동작 자동화에 필요한 환경 설정 횟수를 줄여줍니다. 이를 통해 여러 가지 트리거와 대응을 하나의 자동화에 결합할 수 있습니다. 또한 다양한 소스를 선택해 이벤트를 트리거할 수 있기에 자동화 작업이 보다 유연하고 강력해집니다.

잡은 환경 설정으로 업무에 지장을 겪고 있으신가요?

규칙 설정은 긴 시간이 걸리고 오류가 발생하기 쉽습니다. 복수의 시스템을 운영하고 있다면 더욱 그렇습니다. 이러한 복잡성으로 인해 경보를 효과적으로 관리하기가 어렵습니다. 관리자는 운영자들이 중요한 일에 집중할 수 있도록 오경보를 줄이고 경고를 세밀하게 조정하고 싶어합니다.

자동화되고 효율적인 규칙 생성

Security Center Automation을 통해 Security Center 온프레미스와 Security Center SaaS에서 자동화 규칙을 손쉽게 설정할 수 있습니다. 시스템 내 규칙을 정함으로써 복잡한 시나리오에 대응하고, 운영자의 부담을 경감시키며, 구축과 설정을 간소화하고, 시간과 리소스 여유를 증대할 수 있습니다.

애플리케이션:

Security Center 및 Security Center SaaS

범주:

인텔리전스, 보안

주요 장점

경고를 정밀하게 검증하여 오경보 또는 불필요한 경보 감소

다양한 트리거와 대응을 하나의 규칙으로 결합해 설정 작업 감소

반복적인 작업을 자동화하여 운영자 업무량 경감

여러 시스템에 걸쳐 구축, 설정, 유지보수 작업 간소화

고급 스케줄링 옵션을 활용해 자동화 실행 시점 정밀 제어

Security Center Automation을 선택해야 하는 이유



오경보 또는 불필요한 경보 감소

자동화를 통해 시간과 자원을 절약하고 중요한 작업에 집중할 수 있습니다. 보다 정밀하게 트리거 조건을 다듬고 경고를 검증함으로써 오경보 또는 불필요한 경보를 줄이고 전반적인 시스템 효율을 개선할 수 있습니다.



보다 정교한 시나리오 구현

자동화는 활용도가 높습니다. 여러 트리거 정의, 다양한 조치 설정, 복수의 소스 선택, 상황 맞춤형 대응 등을 통해 간단하거나 복잡한 자동화 작업을 구현할 수 있습니다.



구축 및 설정 간소화

한 번의 자동화로 여러 트리거와 대응을 선택할 수 있어 특히 복수의 시스템을 사용하는 경우 시스템 설정 작업이 원활해집니다. 더 이상 동일한 동작을 하는 이벤트마다 별도로 규칙을 생성하지 않아도 됩니다.

업무 방식에 맞춘 자동화

기존의 이벤트 투 액션 및 작업 예약이 자동화로 전환

처음부터 시작할 필요 없이 새로운 기능을 바로 활용하세요. 기존의 이벤트 투 액션과 작업 예약을 자동화 엔티티로 전환할 수 있습니다. 이 과정을 통해 기존 규칙은 자동으로 비활성화되고 새로운 자동화가 활성화됩니다.

여러 가지 트리거 및 대응 선택

한 번의 자동화로 여러 트리거와 대응을 결합하세요. "Or", "And", "Followed by" 트리거를 모든 이벤트에 원하는 순서나 시퀀스로 연결할 수 있습니다. 또한 지정 기간 내에 여러 번 발생하는 이벤트도 검색할 수 있습니다.

다양한 이벤트 트리거 소스

더 이상 한 가지 아니면 전체를 선택하는 대신, 특정 소스 또는 복수의 소스(일부 카메라나 도어 등)를 선택해 이벤트를 트리거할 수 있습니다.

소스 구성 요소에 대한 상황별 조치

이벤트의 소스나 위치에 기반하여 조치를 지정할 수 있다는 사실을 알고 계셨나요? 이를 통해 자동화 개수를 줄일 수 있으며, 정확히 필요한 순간에만 조치가 실행되도록 설정할 수 있습니다.

수동 자동화 트리거

Config Tool이나 Security Desk 또는 Web App을 통해 원할 때 자동화를 트리거하세요. 이를 통해 관리자와 운영자는 테스트 목적으로 맵이나 핫 액션 등에서 조치를 수동 트리거할 수 있습니다.

내보내기 및 가져오기 설정

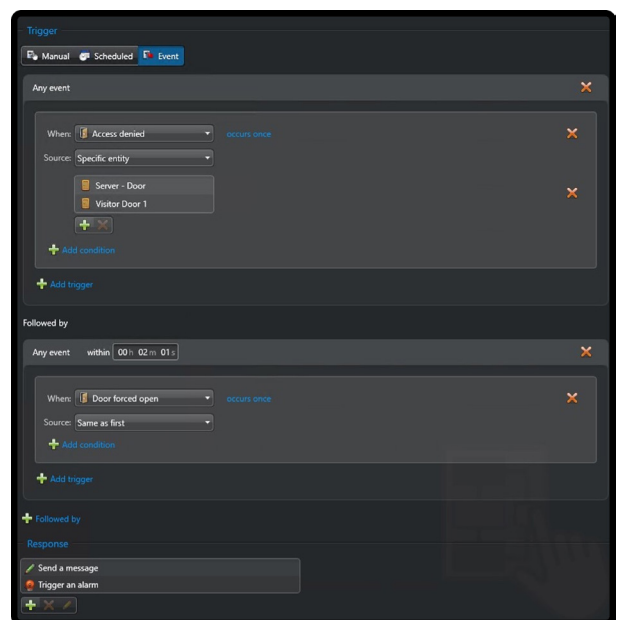
손쉽게 재사용 가능한 템플릿을 생성해 여러 시스템에서 공유할 수 있습니다. 여러 가지 자동화 설정을 하나의 파일로 추출하거나 원하는 내용을 선택적으로 가져올 수 있습니다. 추출된 파일에서 개인 식별 정보(PII)를 제거하여 보안성을 높일 수 있습니다.

스케줄링 옵션 개선

복수의 스케줄, 예외 스케줄, 실행일, 만료일 등의 옵션을 활용해 자동화 실행 시점을 안전하게 제어할 수 있습니다.

사용 사례

이벤트 기반 자동화는 두 가지 시퀀스 트리거 그룹을 이용합니다. 첫 번째 그룹은 서버와 방문자 도어에서 출입 거부 이벤트를 정의합니다. 두 번째 그룹은 도어 강제 개방 이벤트를 정의하는데, 이는 동일 도어에서 첫 번째 이벤트 발생 후 2분 이내로 발생해야 합니다. 해당 이벤트가 발생하면 시스템에서 메시지를 전송하고 경보를 트리거합니다.



자동화는 Security Center 5.13.1 및 Security Center SaaS에서 이용할 수 있습니다.