IBM 보안
솔루션 요약

IBM 보안:
조정 사고 대응

하이라이트

공격 전
공격 중
공격 후

보안 오케스트레이션 및 자동화로 사이버 위협을 예방할수 있는 6가지 단계입니다.

다음을 통해 사이버 공격에 신속하게 대응하세요.

모범 사례 및 조직의 표준 운영 절차를 기반으로 사고 대응 프로세스를 사전 예방하세요.

SIEM(Security Information and Event Management), 티켓팅, 엔드포인트 탐지 및 대응, 위협 인텔리전스를 포함하는 **보안 도구를 통합합니다.**

반복적이고 시간이 많이 소요되는 작업을 자동화하여 SOC(Security Operations Center) 직원은 보다 전략적인 우선 순위에 집중합니다.

인적 및 사이버 인텔리전스를 활용하여 위협을 보다 효과적으로 조사하고 대응 프로세스를 안내하며 오탐지를 방지합니다.

탄력적인 사고 대응 프로세스 및 절차를 지속적으로 측정, 평가 및 조정합니다.

공격 전

점점 정교해지는 보안 사고에 대비

사이버 범죄자는 점점 더 복잡한 공격을 계속 진화시키고 있습니다. SOC는 직면한 수많은 경고 또는 끊임없이 변화하는 규제 환경에 간신히 대응하고 있습니다. 분석가와 관리자는 위협에 대해 보호하고 해결하는 대신 경영진 보고서를 준비하는 데 시간을 할애합니다.

사고 대응 프로세스를 정의하고, 보안 도구를 통합하며, 시간이 많이 소요되는 작업을 자동화하여 방어를 준비하세요. 오케스트레이션은 공격 초기에 위협 및 이상 징후를 파악하고, 사고 대응을 간소화하고, 보안 팀이 보다 전략 및 비즈니스 우선 순위에 있는 업무에 집중할 수 있도록 해줍니다.

IBM® Resilient 인적 및 머신 인텔리전스를 오케스트레이션 및 자동화 기능과 결합하여 사이버 공격에 대한 조직의 대응 능력을 향상시킵니다. 사용자 지정이 가능하고 자동화된 워크플로우를 통해 다이나믹 플레이북을 구축하고 에스컬레이션, 조사 및 해결 작업을 조정하여 대응 시간을 단축하세요.

→ **자세히 알아보기**

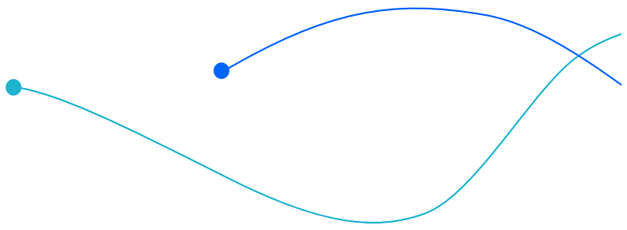
IBM QRadar Security Intelligence Platform 애플리케이션을 비롯한 클라우드 자산을 보호하는 데 필요한 기준 가시성을 보안 팀에 제공합니다. 본의 아니게 데이터가 노출될 수 있는 잘못된 부분을 감지하고 승인받지 않은 도구를 식별하세요.

→ **자세히 알아보기**

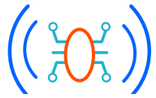
IBM X-Force IRIS(Incident Response Intelligence Services) 온디멘드 사고 대응 전문가가 풍부한 기술, 전문 지식 및 정보를 제공하여 팀의 보안 역량을 강화합니다. 이 팀은 다양한 보안 위협에 대비하고 대응할 수 있도록 지원하는 고도로 숙련된 업계 전문가로 구성되어 있습니다. 이러한 숙련된 전문가들은 불가피한 상황이 발생하면 바로 투입되어 보안 사고 관리 프로세스와 전략적 보안 솔루션의 개발을 지원합니다.

→ **자세히 알아보기**

지능형 오케스트레이션 알아보기



공격 중



지능형 조정을 통해 위협을 신속하게 탐지, 분석 및 대응

사이버 보안 사고와 침해가 발생할 것이라는 점은 공공연한 사실입니다. 귀사는 이러한 가상의 사이버 공격에 어떻게 대응할 것입니까? 위협 인텔리전스, 운영 교육 및 사고 관리 프로세스를 준비하면 피할 수 없는 상황에 대비할 수 있습니다.

IBM QRadar® Security Intelligence Platform 어디서나 데이터를 수신하여 위협을 정확하게 탐지하고 위협 조사를 개선하고 대응 프로세스를 안내하며 오탐지를 제거하는 고급 분석을 적용합니다. 위협 탐지 및 사건 대응 시간의 속도와 효율성을 향상시킵니다. 타사 앱과의 통합은 단일 시스템의 전체 환경에 대한 가시성을 통해 생산성을 높입니다.

→ **자세히 알아보기**

공격 발생 시, **IBM Resilient** 자동화된 사고 조사 및 해결 기능을 통해 보안 분석가에게 신속하고 완벽한 대응을 안내합니다. SOC 분석가부터 마케팅, HR 및 법률 전문가에 이르기까지 조직 전반의 인텔리전스를 공개하세요. IBM Resilient를 모든 사고 관리 활동에 대한 기록 시스템으로 사용하여 대응 프로세스를 가속화하세요. SIEM, 엔드포인트 감지 및 응답, 위협 인텔리전스 및 기타 도구와의 강력한 엔터프라이즈급 통합 기능을 통해 팀 및 도구의 효율성을 위한 메트릭스를 단순화합니다.

→ **자세히 알아보기**

IBM QRadar: 지능형 SIEM

인적 및 사이버 인텔리전스를 실시간으로 활용

과중한 업무 부담과 경험이 부족한 SOC 분석가들은 이미 자신들의 역할을 수행하는 것만으로도 벅찹니다. 공격이 발생하면 일련의 긴급 조치가 시작됩니다. 본안 사고를 제대로 통제 및 관리하려면 보안 전문가가 필요합니다.

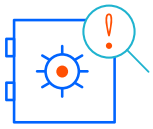
IBM QRadar Advisor with Watson 인공 지능을 이용하여 침해 지표를 빠르게 조사합니다. 인식 추론을 이용하여 보안 분석가가 매일 수신하는 수많은 사건 경고를 관리하는 데 도움이 되는 중요한 정보를 제공합니다. 분석가는 활용 가능한 정보를 활용하여 정보 기반의 문제 해결 및 결정을 내릴 수 있습니다.

→ **자세히 알아보기**

IBM Managed Detection and Response Services
X-Force Command Center의 글로벌 네트워크를 통해 보안사고의 근본 원인 및 킬 체인 가시성을 통해 위협을 감지하고 대응합니다. 당사의 보안 전문가는 공격 실행 시간을 줄이고 조사를 가속화하며 신속한 대응을 제공하며, 향후 유사한 피해가 발생하는 것을 방지합니다.

→ **자세히 알아보기**

공격 후



지속적인 측정, 평가 및 구체화를 통한 개선

사이버 공격으로 인한 피해를 줄이고 인사이트를 확보하세요. 실제 사고로부터 배우는 것과, 그 교훈을 정책과 절차에 반영하는 것은 별개입니다. 귀사 팀은 애플리케이션을 비롯한 클라우드 자산을 보호할 수 있습니까? 본의 아니게 데이터를 노출할 수 있는 잘못된 구성을 사전 감지하고 승인받지 않은 도구를 식별할 수 있습니까?

사고는 완전한 형태로 발생하지 않습니다. 가장 효과적인 사고 대응 플랫폼(IRP)을 통해 기존 보안 기술을 중앙에서 관리할 수 있습니다. 적절한 데이터 소스에서 인텔리전스를 추출하고, 분류, 조사 및 수정하는 동안 자동으로 플레이북을 조정합니다.

단일 대응 허브에서 사이버 공격을 더 똑똑하고, 빠르게 그리고 전략적으로 대응합니다. **IBM Resilient** 반복적이고 시간이 많이 소요되는 작업을 자동화하여 보안 도구를 확장합니다. 애자일 플레이북은 실시간으로 사건 세부 사항에 적용해 분석가들에게 올바른 도구를 사용하여 올바르게 대응하는 방법을 안내합니다. 글로벌 규제 및 대응 계획에 대한 참고 자료를 통해 개인 정보 대응 관리를 간소화하여 대응을 시기적절하고 효율적으로 진행합니다.

→ **자세히 알아보기**

불가피한 상황 발생 시, **IBM X-Force IRIS(Incident Response Intelligence Services)** 민첩한 사고 관리 프로세스를 개발하고 전략적 해결책 및 솔루션 구현을 수행할 수 있도록 도와줍니다.

→ **자세히 알아보기**

IBM X-Force IRIS: 사전 예방적이며 신속한 사고 대응

IBM 보안 솔루션이 어떻게 사고에 대응하며 오늘날의 복잡한 위협으로부터 보호하는지 확인해 보세요.

→ **자세히 알아보기**

IBM 보안
솔루션 요약

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
2018년 11월

700-21870-KRKO