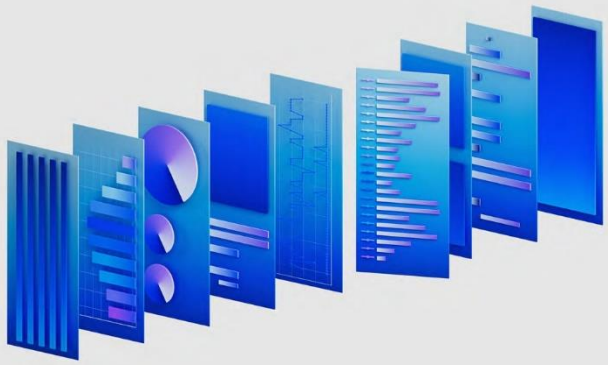
IBM Security QRadar Suite

분석가를 위한 최고의 솔루션

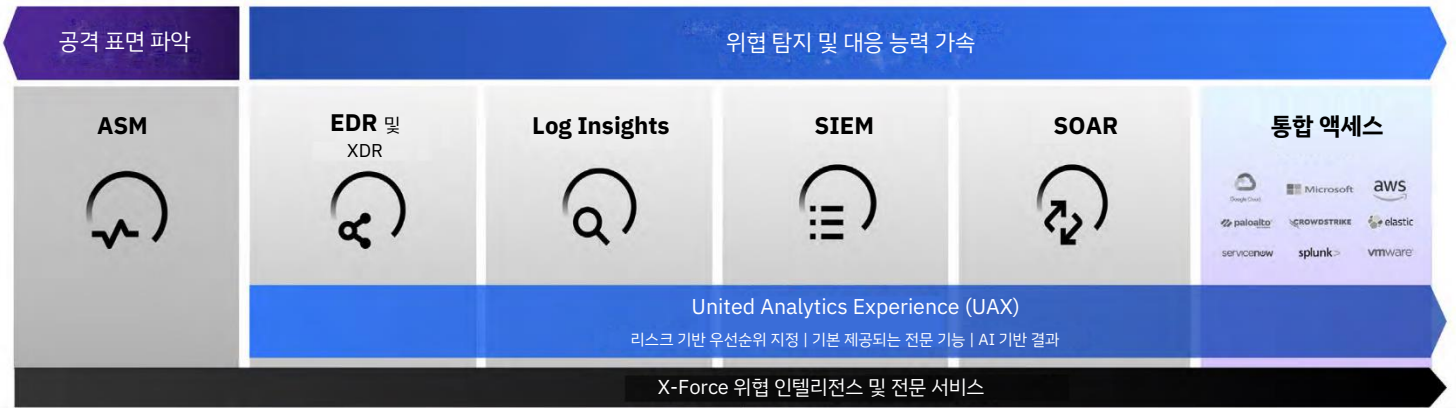


인프라가 확대되고 툴이 늘어나고 알림이 많아지면 분석가의 부담도 커집니다. 기업의 디지털 거점이 하이브리드 클라우드 환경으로 확장됨에 따라 복잡성이 증가하여 보안 팀은 당면한 위협을 찾아내고 대응하기가 더욱 어려워졌습니다. SOC 전문가들은 정규 근무 시간에 미처 확인하지 못하는 알림이 51%에 달한다고 말합니다. 이들이 속도를 내지 못하는 가장 큰 이유는 바로 수작업 위주의 조사 프로세스 때문입니다.[1] 보안 분석가가 오늘날의 공격에 지속적으로 대응하기 위해서는 더 높은 효율성이 필요합니다. 그러기 위해서는 더 간소화된 사용자 환경에서 다양한 인사이트를 자동으로 통합하고, 우선순위에 따라 리스크를 관리하며, 실제 공격 상황에서 중대한 피해와 손실이 발생하기 전에 더 정밀하고 신속하게 대응할 수 있도록 지원해야 합니다.

IBM Security® QRadar® Suite는 개방형 모듈식 위협 탐지/대응 솔루션으로, 보안 분석가를 위한 통합 환경에서 전체 인시던트 라이프사이클 및 관련 툴 전반의 속도와 효율성을 높여 줍니다. 엔터프라이즈 환경에 최적화된 AI 및 자동화를 통해 분석가의 생산성이 획기적으로 향상되어 인력난에 시달리는 보안 팀은 핵심 기술을 활용하여 더욱 효과적으로 일할 수 있습니다. 이 포트폴리오는 엔드포인트 보안(EDR, XDR, MDR), 로그 관리, SIEM 및 SOAR 제품을 통합하여 단일 공통 UI, 공유 인사이트, 상호 연결된 워크플로우와 함께 제공됩니다. 광범위한 파트너 에코시스템과 통합 기능을 갖춘 플랫폼을 기반으로 구축하여 AWS에서 aaS(as-a-service)로 제공됩니다.

주요 이점

- **분석가를 위한 통합 경험:** 분석가는 통합형 단일 공통 UI를 사용하여 다양한 툴과 데이터 소스 전반의 인사이트를 공유하고 작업을 자동화함으로써 조사 및 대응 프로세스를 더 빠르고 효율적으로 수행할 수 있습니다. 이와 같이 프로세스를 능률화하면 사고 대응 시간을 85% 단축할 수 있는 것으로 나타났습니다.[2]
- **클라우드 기반, 속도, 규모:** AWS에서 aaS(as-a-service)로 제공되는 QRadar Suite 제품은 여러 클라우드 환경에 간편하게 배포하고, 퍼블릭 클라우드 및 SaaS 로그 데이터와도 통합할 수 있습니다. 또한, 새로운 클라우드 네이티브 보안 관측 및 로그 관리 기능도 포함하여 대규모 데이터 수집, 초고속(sub-second) 검색, 신속한 분석을 지원하도록 최적화되었습니다.
- **개방형 플랫폼 및 사전 통합 기능:** QRadar Suite는 효과적인 SOC에 필요한 핵심 툴을 통합하여 제공합니다. 광범위한 파트너 에코시스템을 토대로 IBM 제품뿐만 아니라 타사 제품을 지원하는 900여 종의 사전 구성된 통합 기능을 통해 유연성과 선택권을 제공합니다. 뿐만 아니라 위협 인텔리전스, 로그 관리, EDR, SIEM, SOAR을 위한 기능도 사전 통합되어 있습니다.



개방형 플랫폼. 개방형 통합. 개방형 위협 인텔리전스.

주요 구성 요소와 사용 사례

- **United Analytics Experience(UAX):** 자동으로 조사하고 대응 방안을 추천합니다. 통합 검색 및 위협 추적 기능이 Log Insights, SIEM, SOAR 기능과 함께 제공됩니다.
- **QRadar EDR & XDR:** 알려졌거나 알려지지 않은 엔드포인트 위협을 거의 실시간으로 제거합니다. 이를 위해 지능형 자동화 및 AI, 공격 시각화 스토리보드, 자동 알림 관리 기능을 활용합니다. 위협 탐지 및 대응의 범위를 엔드포인트뿐만 아니라 클라우드, 이메일, 네트워크, 사용자 및 데이터로 확장하여 단일 뷰를 통해 한 눈에 파악함으로써 더 신속하게 위협을 찾아내고 차단합니다.
- **QRadar Log Insights:** 클라우드 스케일의 로그 수집, 빠른 검색, 강력한 시각화 및 통합 위협 추적/협업 기능으로 완전한 가시성을 제공합니다.
- **QRadar SIEM:** 기본 제공되는 가시성 및 보안 분석 기능을 활용하면서 클라우드와 온프레미스에서 비즈니스를 운영하여 지능적인 위협에 대비하고 분석가의 사고 조사 시간을 90% 이상 단축합니다.[3]
- **QRadar SOAR:** 업계 최고의 개방성과 상호 운용성을 자랑하는 SOAR 플랫폼에서 사고 대응을 자동화하고 지능화하여 더 능률적인 SOC로 업그레이드합니다.

"UAX가 정규 근무 인력 5명의 역할을 합니다. 사람을 더 투입하기보다 AI를 접목한 툴을 활용함으로써 더 우수한 데이터를 더 수월하게 얻을 수 있었습니다. 덕분에 직원들은 더 빨리, 더 효과적으로 업무를 수행했습니다."[4]

IBM QRadar Suite를 사용해야 하는 이유

이 특별하고 목표 지향적이며 보안 분석가 중심의 접근 방식은 위협 조사 및 대응을 위해 수행할 단계와 확인할 화면의 수를 획기적으로 줄여 줍니다.

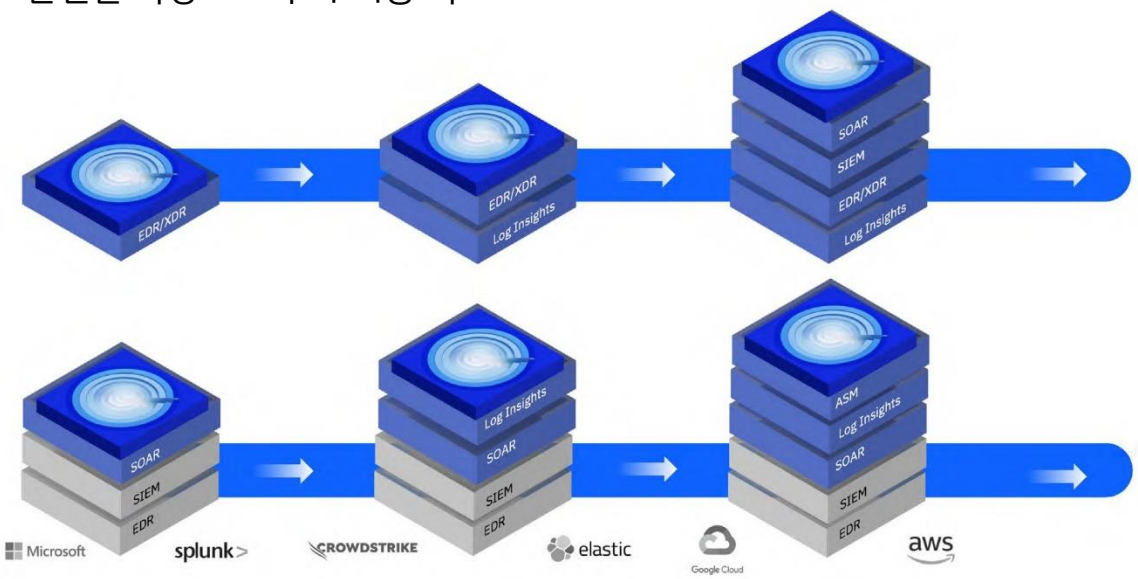
- **AI 기반 알림 분류:** 과거의 분석가 대응 패턴을 학습한 AI 모델을 사용하는 AI 기반 리스크 분석, IBM X-Force®에서 제공하는 외부 위협 인텔리전스, 그리고 각종 탐지 툴 세트에서 제공하는 더 폭넓은 컨텍스트 기반 인사이트를 바탕으로 자동으로 알림의 우선순위를 지정하거나 알림을 종료합니다. 분석에 의하면, 이 솔루션 구현 후 5년 이내에 평균적으로 알림 종결 처리의 70% 이상을 자동화하고 알림 분류 타임라인을 55% 단축할 수 있습니다.[5]
- **위협 조사 자동화:** 반드시 조사해야 할 우선순위가 높은 사고를 식별하고 자동으로 조사를 시작합니다. 이를 위해 관련 아티팩트를 전달하고, 환경 전반에 대한 데이터 마이닝을 수행하여 증거를 수집합니다. 이 시스템에서는 그 결과를 참고하여 MITRE ATT&CK 프레임워크에 따라 해당 사고의 타임라인 및 공격 그래프를 작성한 다음 신속하게 대응 방안을 제안합니다.
- **더 빠른 위협 추적:** 오픈소스 위협 추적 언어와 통합 검색(federated search) 기능을 사용하여 기존 소스에서 데이터를 이동하지 않고도 위협 추적 팀에서 모든 환경을 대상으로 잠복 상태의 공격 및 침해 지표를 찾아낼 수 있습니다.

필요한 단계에서 시작 – 간편한 확장으로 추가 기능 확보

예

필요한 단계에서 시작하고,
손쉽게 추가 기능 확장

기존 환경에
필요한 기능 추가



출처

1. 2023 IBM 글로벌 보안 운영 센터 연구
2. 새로운 사이버 위협에는 새로운 접근 방식 필요, ibm.com
3. 2023 Forrester TEI - QRadar SIEM
4. 북미 지역의 주정부 산하 기관
5. 고객 400여 곳을 대상으로 한 관리형 서비스 분석, IBM 비즈니스 가치 연구소 보고서, "사이버 보안을 위한 AI와 자동화", 2022.

IBM Corporation New Orchard Road, Armonk, NY 10504
Produced in the United States of America, April 2023