IBM Resilient SOAR 플랫폼과 IBM QRadar® Security Intelligence

SIEM과 SOAR의 연계로 대응 시간 단축, 분석가의 워크로드 감축

주요 특징

- 의심이 되는 인시던트를 신속히 에스컬레이션하여 능률적인 조사 지원
- 인리치먼트(enrichment) 프로세스를 자동화하여 분석가의 워크로드에 우선 순위 지정
- QRadar와 Resilient 간에 모든 인시던트 데이터 동기화
- MITRE ATT&CK 전술/기법 활용
- 연속적인 피드백 루프로 탐지 정확성 향상

Gartner는 최근 발표한 마켓 가이드 리포트에서 "경보 분류의 품질 및 속도 향상"을 SOAR(Security Orchestration, Automation and Response) 툴을 도입하는 핵심 이유 중 하나로 꼽았습니다.[1] 현재 보안관제 팀은 조직을 위협하는, 숫자뿐만 아니라 복잡성과 파괴력까지 날로 증가하는 사이버 공격에 대처해야 합니다. 따라서 보안 인시던트를 더 빨리 차단하고 해결하기 위해 보안관제센터(SOC) 및 인시던트 대응(IR) 프로세스를 자동화할 방법을 모색하고 있습니다.

IBM Resilient SOAR(Security Orchestration, Automation and Response) 플랫폼을 IBM QRadar® Security Intelligence와 통합하면, 보안 팀은 다양한 사이버 활용 사례에서 위협 탐지, 조사, 해결을 지원하는 업계 최고의 위협 관리 솔루션을 구축할 수 있습니다. 이 두 솔루션 간의 기술 통합 덕분에 보안 분석 팀이 의심스러운 오펜스를 QRadar에서 Resilient에 신속하고 효율적으로 에스컬레이션한 다음, 추가로 자동화된 인리치먼트를 거쳐 본격적인 조사 프로세스를 시작하는 것이 가능해졌습니다. 인시던트가 진행되는 동안, QRadar와 Resilient 간에 모든 정보가 동기화되어 완전한 데이터 무결성을 보장합니다. Resilient에서 찾아내는 모든 새로운 정보는 다시 QRadar에 전달되어 탐지 프로세스를 개선합니다.

이미 구축된 QRadar가 Resilient SOAR 플랫폼과 만나 업계 최고의 보안 오케스트레이션/자동화/사례 관리 기능이 탄생합니다. 이로써 훨씬 더 효과적인 방법으로 사이버 공격에 대응할 수 있습니다. QRadar 고객은 IBM Security AppExchange에서 완벽하게 지원되는 여러 애플리케이션을 통해 Resilient와 연결할 수 있습니다. Resilient는 기존의 QRadar와 문제없이 연동하면서 SOC 기능을 확장합니다.

• 인텔리전스/인사이트와 자동화/통합의 연계

보안 분석 팀은 QRadar에서 제공하는 포괄적인 가시성을 바탕으로 위협 및 위험에 관한 최고의 인사이트를 얻을 수 있습니다. Resilient에서는 커스터마이즈 가능한 워크플로우 및 동적 플레이북를 통해 이러한 위협 인사이트를 가져와 신속히 조치를 취하여 위협을 제거합니다. 분석 팀은 반복적이고 시간 소모적인 작업에 자동화를 적용하여 전체 프로세스의 효율성을 높일 수 있습니다.

• 공격 발생 시 더 빨리 대응

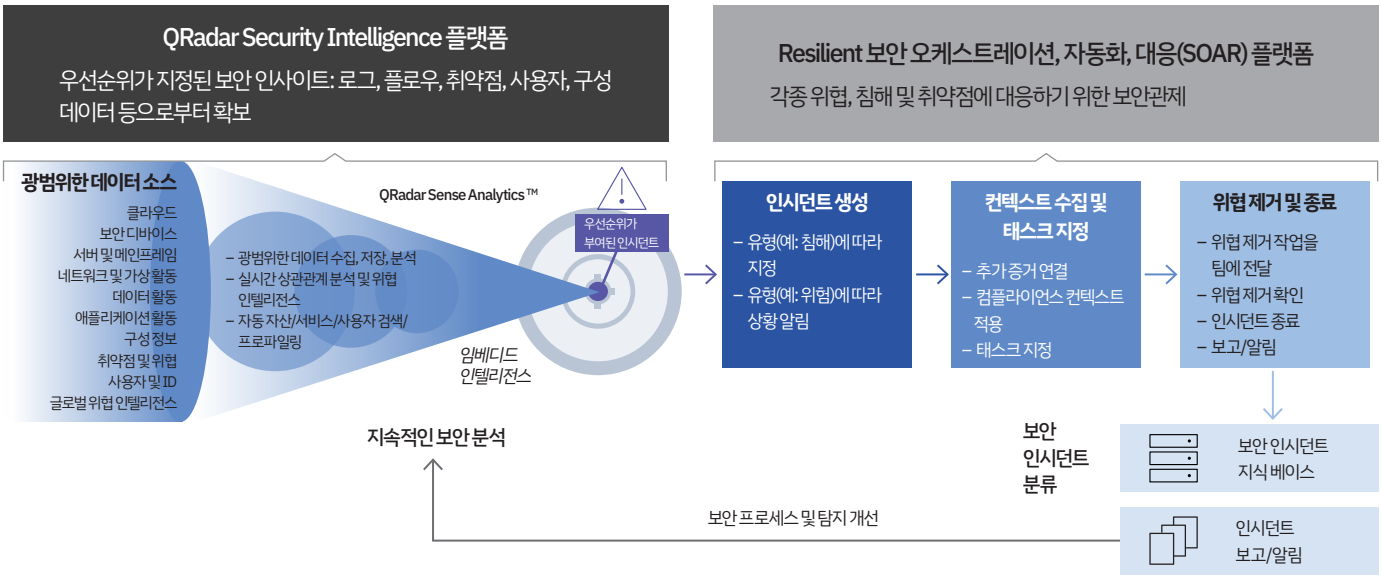
QRadar가 사이클 초기에 위협을 발견하면, Resilient에서 대응 프로세스를 활용하여 더 빨리 위협을 제거할 수 있습니다. 분석 팀은 가이드 대응(Guided Response)을 통해 철저한 검증과 테스트를 거친 IR 계획에 따라 인시던트 조사부터 해결까지 단계적으로 진행하면 됩니다. 이제는 QRadar Advisor with Watson에서 MITRE ATT&CK™을 지원하기 때문에 Resilient에서 인리치먼트 프로세스를 통해 인시던트 정보를 보강한 다음 MITRE 전술, 기법, 절차(TTP) 기반 인사이트에 따라 대응 프로세스를 결정할 수 있습니다.

• 공격 전후 프로세스 개선

QRadar와 Resilient는 공격 발생 전후의 보안 프로세스를 한층 더 발전시키는 데 도움이 됩니다. QRadar가 공격 사이클의 초기에 이상을 발견하면, 분석 팀은 위협 정보 및 학습 경험을 토대로 탐지 메커니즘을 계속 조정할 수 있습니다. SOC는 Resilient를 활용하여 사람, 프로세스 및 기술의 오케스트레이션을 위한 강력한 자동 IR 워크플로우를 준비합니다. 이 플랫폼은 공격 이후 단계에 계속 프로세스를 평가하고 개선할 수 있는 툴도 제공합니다. 양방향 통합을 통해 이 학습 결과를 QRadar에 보내 탐지 규칙을 개선하고 QRadar 레퍼런스 세트에 새 아티팩트를 추가할 수 있습니다.

QRadar와 Resilient의 조합으로 End to End 위협 관리 솔루션이 완성됩니다. 정확한 위협 탐지, 사례 관리, 오케스트레이션 및 자동화, 인공지능과 인간 지능의 시너지 효과를 통해 더 빠르고 정확한 IR 프로세스를 제공할 수 있습니다. 분석 팀에서 빠르고 효율적으로 QRadar 오펜스 조사를 실행할 수 있으므로 인시던트 해결 시간이 단축됩니다.

분석 팀은 QRadar에서 습득한 인사이트를 곧바로 Resilient에 보내 가장 시급한 위협에 대처할 수 있습니다. Resilient에서는 사례 관리는 물론이고 커스터마이즈 가능한 자동 워크플로우를 갖춘 동적 플레이북, 강력한 서드파티 통합 에코시스템까지 제공합니다. 분석 팀은 이러한 툴을 통해 QRadar로부터 가져온 정보를 활용하면서 빠르고 효율적으로 인시던트에 대응할 수 있습니다.



IR 라이프사이클

QRadar를 위한 Resilient 통합

QRadar 사용자는 IBM Security App Exchange에서 제공하는 4가지 통합 모델을 통해 Resilient의 이점을 빠르고 손쉽게 누릴 수 있습니다.

Resilient + QRadar 통합

QRadar 오펜스를 자동 또는 수동 프로세스를 통해 Resilient SOAR 플랫폼에 에스컬레이션하여 조사하고 해결합니다. 이 통합 덕분에 기존 또는 신규 인시던트 데이터에 IP 주소 및 기타 아티팩트를 추가하는 것이 가능합니다. 오펜스가 변경되면, 자동으로 기존 인시던트 데이터에 전달됩니다. 그리고 Resilient와 QRadar 간의 양방향 노트 동기화로 데이터 무결성을 보장합니다. 이 통합에서는 여러 QRadar 도메인을 Resilient 하위 조직과 연결하여 MSSP 활용 사례를 다루는 것도 지원합니다.

Resilient + QRadar 기능

이 패키지형 통합에 포함된 검색 기능으로 레퍼런스 세트 항목에 대해 작업을 수행하고 인시던트 아티팩트를 업데이트하면서 워크플로우를 발전시킬 수 있습니다. 사용자는 이 검색 기능으로 QRadar에서 사용자 이름, IP 주소 또는 오펜스 ID에 대한 수동 또는 자동 검색을 실행한 다음 Resilient에서 사용자 정의 데이터 테이블의 형태로 검색 결과를 생성할 수 있습니다. QRadar 레퍼런스 세트 항목을 관리하고 Resilient 인시던트 아티팩트와 연결하는 기능도 있는데, 그러면 각 아티팩트에는 업데이트된 노트의 "증거 자료(paper-trail)"가 생성됩니다. 이 패키지는 Resilient의 4가지 기능, 5가지 워크플로우 및 5가지 규칙을 포함하며, QRadar의 인시던트 피드백을 토대로 워크플로우를 실행합니다.

Resilient + QRadar Advisor with Watson

이 통합으로 QRadar Advisor with Watson 고객은 Watson의 IoC(Indicator of Compromise) 조사 결과를 토대로 위협 인사이트를 보강하고, 위협의 전 범위를 맵핑한 다음 위협 데이터와 영향을 받은 시스템을 패키지화하고 Resilient에 보내 위협을 제거할 수 있습니다.

사실상 IR 프로세스의 기능과 효율성을 확장합니다. Watson은 보안 분석가가 아티팩트를 심층 분석하고 그에 관한 컨텍스트를 제공하여 위협 제거 프로세스의 속도와 정확도를 높이는 데 큰 역할을 합니다. 이 통합으로 QRadar 오펜스로부터 MITRE ATT&CK 전술 정보를 추가할 수도 있습니다.

QRadar-MITRE 콘텐츠 패키지

QRadar Advisor with Watson과 연동하는 이 앱에는 QRadar Advisor로부터 분석 및 인사이트(ATT&CK 전술과 기법 포함)를 가져오는 워크플로우가 있습니다. MITRE ATT&CK 지식 베이스를 통해 이러한 정보를 보강한 다음, 인시던트 태스크로 변환하여 후속 조치에 활용합니다. 이 새로운 정보를 토대로 인시던트의 우선순위를 바꾸거나, 대응 프로세스를 변경합니다.

"Resilient, QRadar, 그리고 전체 IBM 에코시스템 덕분에 우리의 역량이 획기적으로 향상되었습니다. 보안 인시던트 대응을 위한 포괄적이고 동적인 프로그램을 보유한 어엿한 조직으로 발전했습니다."

– Brian Herr, Secure-24 최고보안/개인정보보호책임자

Resilient SOAR 플랫폼을 IBM QRadar에 통합함으로써 보안 팀이 강력한 통합형 솔루션을 탐지 및 대응 프로세스에 십분 활용하면서 복잡한 사이버 공격도 더 빨리 탐지하고 차단하는 것이 가능합니다.

Resilient의 보안 자동화/오케스트레이션/사례 관리를 QRadar의 탐지/상관관계 분석 기능과 연계하면, 보안 분석 팀이 중요 인시던트에 우선적으로 집중하고, 수작업 중심의 인시던트 조사 워크로드를 줄이며, 더 빠르고 효율적인 보안관제 프로세스를 마련할 수 있습니다.

[1] Gartner, Market Guide for Security Orchestration, Automation and Response Solutions, Claudio Neiva, Craig Lawson, Toby Bussa, Gorka Sadowski, 2019년 6월 27일

왜 IBM인가?

IBM Security는 가장 발전되고 통합된 엔터프라이즈 보안 제품 및 서비스 포트폴리오를 제공합니다. 세계적 명성의 IBM X-Force® 연구소가 뒷받침하는 이 포트폴리오는 기업이 효과적으로 위협을 차단하고 컴플라이언스를 입증하며 안전하게 성장하는 데 필요한 보안 솔루션을 제공합니다.

IBM은 가장 광범위하면서 수준 높은 보안 연구, 개발, 서비스 조직을 운영하면서 130여 개국에서 월 2조 건 이상의 이벤트를 모니터링하고 있으며 3,000개 이상의 보안 특허를 보유하고 있습니다. 자세한 내용은 ibm.com/security를 참고하시기 바랍니다.

자세한 정보

IBM Resilient SOAR Platform에 대한 자세한 내용은 IBM 영업대표 또는 IBM 비즈니스파트너에게 문의하거나 https://www.ibm.com/security/intelligent-orchestration/resilient 웹 사이트에서 확인하세요.