비즈니스 과제

새로운 종합 보안 규제가 도입됨에 따라 해당 보험사는 단기간에 회사 전체에 보안 정보 및 이벤트 관리(SIEM)를 시행해야 했습니다.

변화

해당 손해보험•생명보험 회사는 뉴욕 주에서 새롭게 도입한 보안 규제를 기한 내에 시행하면서 신속하게 운영 정교화를 실현하고자 전사적 IBM® QRadar® SIEM 솔루션을 설계, 설치 및 원격 관리하는 작업을 IBM 비즈니스 파트너 Sirius에 의뢰했습니다.

결과

확장 가능 솔루션

EPS 최대 40,000건 및 기기 5,100여 개를 지원하는 확장 가능 솔루션

연중무휴

연중무휴 원격 모니터링 및 관리로 빈틈없는 운영 실현

신속한 구현

신속한 구현을 통해 뉴욕 주의 규제 준수 기한을 지킬 수 있었습니다.

손해보험•생명보험 회사

Sirius의 관리형 IBM QRadar SIEM 솔루션으로 새로운 보안 규제 의무에 대응

이 손해보험 · 생명보험 회사는 미국 남동부에 본사를 두고 있으며 미국 내 여러 주에서 정식으로 사업을 운영하고 있습니다.

"첫 번째 단계는 이 고객사의 현재 필요 사항을 충족하면서 미래에 대비한 전략적 플랫폼이 되어 줄 SIEM 도구를 선택하는 일이었습니다."

—Brian Reichart, Sirius 관리형 보안 및 인프라 전문가

SIRIUS

공유하기

단기간에 새로운 보안 규제에 대응해야 하는 상황 직면

뉴욕 주 금융 서비스국(NYDFS)이 뉴욕에서 사업을 운영하는 모든 금융기관에 적용되는 사이버 보안 규제인 23 뉴욕 코드 규칙 및 규제 500(23 NYCRR 500)을 발표하자, 대상 조직들은 촉박한 기한 내에 규제를 시행해야 하는 상황에 놓이게 되었습니다.

뉴욕 및 다른 여러 주에서 사업을 운영하는 해당 손해보험 · 생명보험 회사는 이 규제의 요건에 대응하는 일이 회사의 계획이 맞아떨어진다고 보았습니다. 회사는 보안 관리가 자사의 전략적 비즈니스 기능이라고 판단했습니다. 다만 문제는 규제를 준수해야 하는 기한이 촉박하다는 점이었습니다.

23 NYCRR 500의 시행 기한인 2018년 9월 전에 전사적 보안 정보 및 이벤트 관리(SIEM) 시스템을 마련하여 정상적으로 운영하는 것이 매우 중요했습니다. 회사의 인프라에는 이미 곳곳에 SIEM 도구가 배포되어 있었지만 기기와 법인에는 이러한 도구가 배포되지 않은 상황이었습니다. 게다가 이러한 간극이 존재하는 와중에도 도구에서 생성되는 이벤트가 현재 직원들이 효과적으로 처리하기에는 턱없이 방대했습니다. 회사 경영진은 회사 전체를 아우르는 상세한 관점을 확인할 수 없었습니다.

비즈니스 성장을 지원하는 전략적 플랫폼 선택

해당 보험사는 전사적 SIEM 솔루션을 선택하고 구현하는 작업을 직접 처리하는 대신 ITM 플래티넘 비즈니스 파트너 Sirius에 도움을 요청했습니다. 회사는 기존에 Sirius와 거래한 이력이 있었으며 Sirius는 해당 회사의 IT 환경에서 작업하는 데 필요한 승인을 이미 받은 상태였습니다. 이것이 바로 이 IT 솔루션 공급업체가 회사의 촉박한 규제 시행 작업 업체로 선정된 이유입니다.

"회사의 예상 연간 성장률인 10%~15%를 감안한 결과, 전용 온프레미스 QRadar 솔루션이 고객사에 적합하다고 보았습니다."

—Brian Reichart, Sirius 관리형 서비스 솔루션 영업 전문가

"첫 번째 단계는 이 고객사의 현재 필요 사항을 충족하면서 미래에 대비한 전략적 플랫폼이 되어 줄 SIEM 도구를 선정하는 일이었습니다." 이번 작업을 담당한 Sirius 관리형 서비스 솔루션 영업 전문가 Brian Reichart의 말입니다. Sirius는 회사에서 이미 사용 중인 도구인 IBM® QRadar® SIEM을 추천했습니다.

"새롭게 임명된 CISO(정보 보호 최고 책임자)는 매우 까다로운 조건을 내세웠고, 그래서 QRadar가 알맞은 제품이라고 판단했습니다. 또한 우리는 온프레미스 배포와 클라우드 각각의 가치에 대해 오랜 시간 논의했습니다. 회사의 보안 관련 전략적 의무를 분석하는 동시에 회사의 예상 연간 성장률인 10%~15%를 감안한 결과, 전용 온프레미스 QRadar 솔루션이 고객사에 적합하다고 보았습니다."

고려 대상이 된 여러 SIEM 플랫폼 중 QRadar를 선택하게 된 차별화 요소로는 기본 포함된 다양한 표준 보고서, 그리고 보고의 유연성이 있습니다. 이는 보안 소프트웨어를 설치하는 데 맞춤 작업이 거의 필요 없다는 의미입니다. 로그 관리자 플랫폼을 이용하면 운영 검토용 데이터에 빠르게 액세스하고 환경 하위 세트의 활동을 분석할 수 있습니다.

해당 보험사의 CISO는 또한 IBM Security App Exchange를 통해 기능을 추가할 수 있다는 점을 높이 평가했습니다. IBM Security App Exchange는 QRadar 및 기타 보안 솔루션용 앱 및 애드온을 받을 수 있는 개발자 에코시스템입니다.

회사의 "시행" 목표 날짜까지 6개월이 조금 넘게 남은 시점에서, Sirius는 확장 가능 QRadar 솔루션을 설계하고 회사의 주요 데이터 센터 3곳과 여러 원격 지점에 수집기 및 콘솔을 설치하는 작업에 착수했습니다. 해당 Sirius 솔루션에는 가양성(false positive)을 필터링해 주며 SIEM 솔루션의 효율에 매우 중요한 역할을 하는 상관 관계 규칙이 포함되어 있다고 Reichart는 말합니다. "Sirius는 IBM에서 추천한 상관 관계 규칙과 별도로 추가할 상관 관계 집합을 자체 개발했습니다. 이러한 튜닝은 시스템에서 발생하는 알림의 수를 대폭 줄이는 데 도움이 됩니다."

관리형 서비스로 빈틈없는 운영 실현

현재 해당 보험 회사에 설치된 QRadar SIEM 시스템에서는 기기 5,100여 개를 관리하며, 비즈니스가 성장함에 따라 새로운 로그 소스가 지속적으로 추가되고 있습니다. 이 솔루션은 회사의 현재 워크로드 24,000EPS(events per second)를 지원하며 최대 40,000EPS까지 확장 가능합니다.

모니터링 및 상시 관리 기능은 비즈니스 파트너 Sirius의 SOC를 통해 구현됩니다. 덕분에 해당 보험사는 자체 운영 센터를 구축하고 센터 인력을 충원할 필요 없이 촉박한 기한 내에 운영 정교화를 실현했습니다. 그 결과 회사는 23 NYCRR 500 위반으로 인한 벌금 및 처벌을 피하는 동시에 향후 자체 SOC에 인력 및 장비를 공급하는 데 필요한 시간을 확보할 수 있었습니다.

"현재 우리는 QRadar를 상시 지원하고 있습니다."

—Brian Reichart, Sirius 관리형 서비스 솔루션 영업 전문가

"현재 우리는 QRadar를 상시 지원하고 있습니다." Reichart의 말입니다. 새로운 상관 관계 규칙을 추가하여 시스템을 정교하게 튜닝하는 것, 고객사 측과 매주 회의를 하는 것, 회사가 IT 환경에 새로운 리소스를 추가함에 따라 새로운 로그 소스를 구현하는 것 등이 상시 지원에 포함됩니다.

"회사는 성장에 전혀 타격을 입지 않았습니다." Reichart의 말입니다. "회사에서는 새로운 도구, 새로운 하드웨어 및 새로운 서버를 환경에 지속적으로 배포하고 있습니다. 모두 우리가 상시 구현하고 있는 새로운 로그 소스입니다."

솔루션 구성 요소

- IBM® QRadar® SIEM

다음 단계

이 사례에서 사용된 IBM 솔루션에 대한 자세한 내용은 IBM 담당자 또는 IBM 비즈니스 파트너에게 문의하십시오.

Sirius 소개

IBM 플래티넘 비즈니스 파트너인 Sirius는 데이터 센터, 영업 부문 등 기업 전반을 아우르는 미국의 기술 기반 비즈니스 솔루션 통합업체입니다. Sirius는 1980년 창립 이래 북미 최대 규모의 IT 솔루션 통합업체 중 한 곳으로 성장했습니다. 현재 Sirius는 500명 미만 소기업, 직원 수천 명과 지점 수백 곳을 둔 대기업 등 규모에 관계없이 모든 조직을 대상으로 통합형 다중 업체 기술 솔루션을 제공하고 있습니다. Sirius에 대한 자세한 내용은 다음을 참조하십시오. www.siriuscom.com

© Copyright IBM Corporation 2019, IBM Security, 75 Binney Street, Cambridge, MA 02142. Produced in the United States of America, 2019년 1월. IBM, IBM 로고, ibm.com 및 QRadar는 전 세계에 등록된 International Business Machines Corp.의 상표입니다. 기타 제품 및 서비스 이름은 IBM 또는 타사의 상표입니다. 최신 IBM 상표 목록은 "저작권 및 상표 정보"(ibm.com/legal/copytrade.shtml) 웹 사이트에 있습니다. 이 문서는 처음 발행될 당시의 날짜를 기준으로 업데이트되었으며 IBM은 언제든지 문서 내용을 변경할 수 있습니다. IBM 지사가 있는 국가라도 일부 오퍼는 제공되지 않을 수 있습니다. 이 문서에서 인용하는 성능 데이터 및 고객 예시는 이해를 돕기 위한 목적으로만 사용됩니다. 실제 성능 결과는 특정 구성 및 운영 조건에 따라 다를 수 있습니다. 이 문서의 정보는 상품성에 대한 보증, 특정 목적의 적합성 여부 및 저작권을 침해하지 않는다는 보증 또는 조건을 포함해 명시적 또는 암묵적 보증 없이 "있는 그대로" 제공됩니다. IBM 제품은 제공된 약정에 명시된 조항 및 조건에 따라 보증됩니다. 고객은 관련 법령과 규제를 반드시 지켜야 할 책임이 있습니다. IBM은 고객이 법령 또는 규제를 준수한다고 해서 당사의 서비스 또는 제품이 보증하는 법적 상담을 제공하거나 보증을 대신하지 않습니다. 보안 무결성 관련 고지: IT 시스템 보안은 기업 내부 및 외부에 걸쳐 승인되지 않은 부적절한 액세스를 방지, 감지 및 응대함으로써 시스템 및 정보 보호에 관여합니다. 승인되지 않은 부적절한 액세스는 결국 정보 변경, 폐기, 손실 또는 오용으로 이어질 수 있으며 타 시스템 공격은 물론 시스템 손상 또는 오용까지 포함합니다. 그 어떤 IT 시스템 또는 제품으로도 보안이 완벽하다고 볼 수 없는데다 하나의 제품, 서비스 또는 보안만으로 승인되지 않은 부적절한 사용 또는 액세스 방지에 대한 효과가 완전하다고 볼 수 없습니다. IBM 시스템, 제품 및 서비스는 추가 운영 절차에 관여하고 타 시스템, 제품 또는 서비스 효과를 극대화시킬 수 있는 합법적, 포괄적 보안 접근 방식의 일부로 적용할 수 있게 고안되었습니다. IBM은 시스템, 제품 또는 서비스가 악의적 또는 불법적인 행위로부터 완벽히 안전하거나 그러한 행위로부터 회사를 완벽히 보호할 수 있음을 보증하지 않습니다.

86022886-KRKO-00