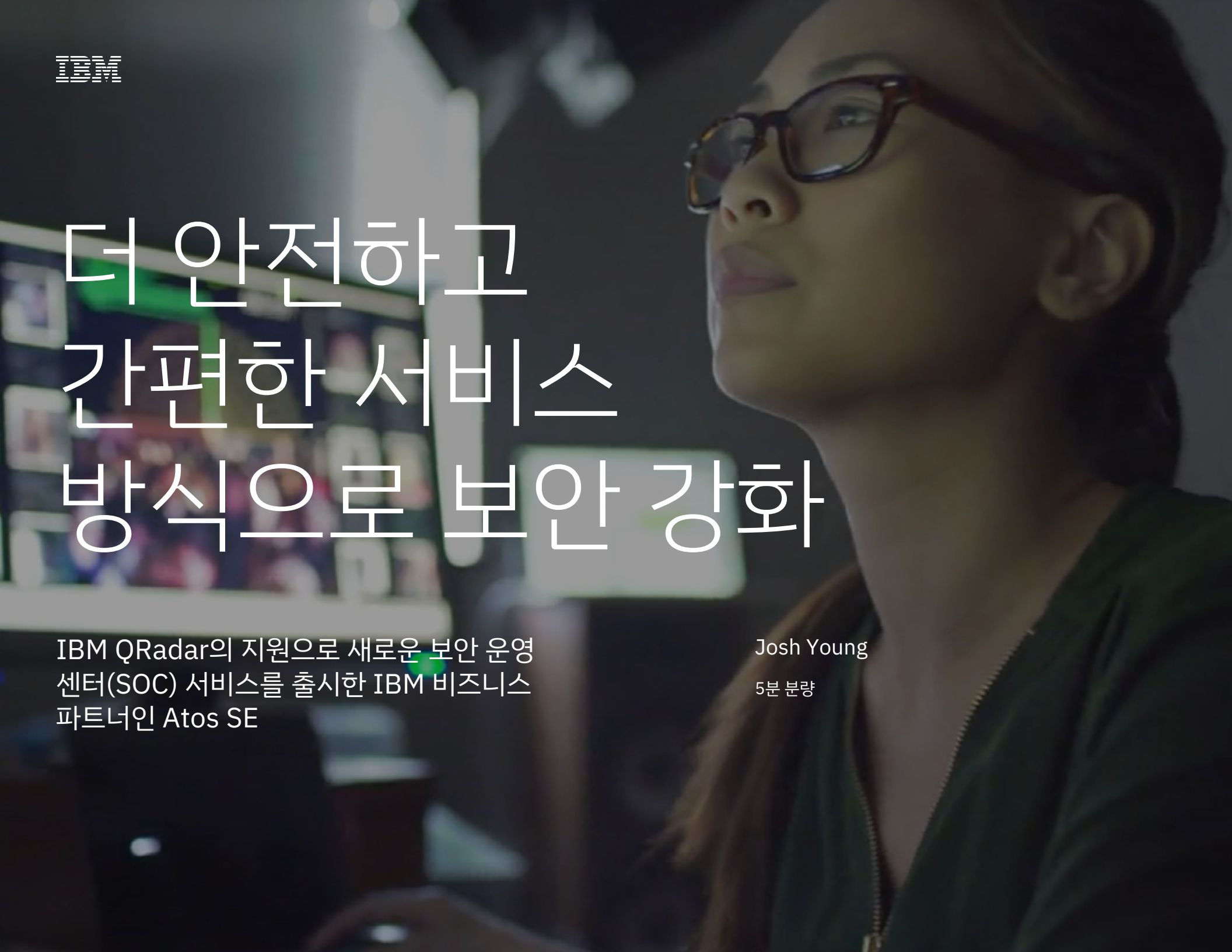


더 안전하고 간편한 서비스 방식으로 보안 강화

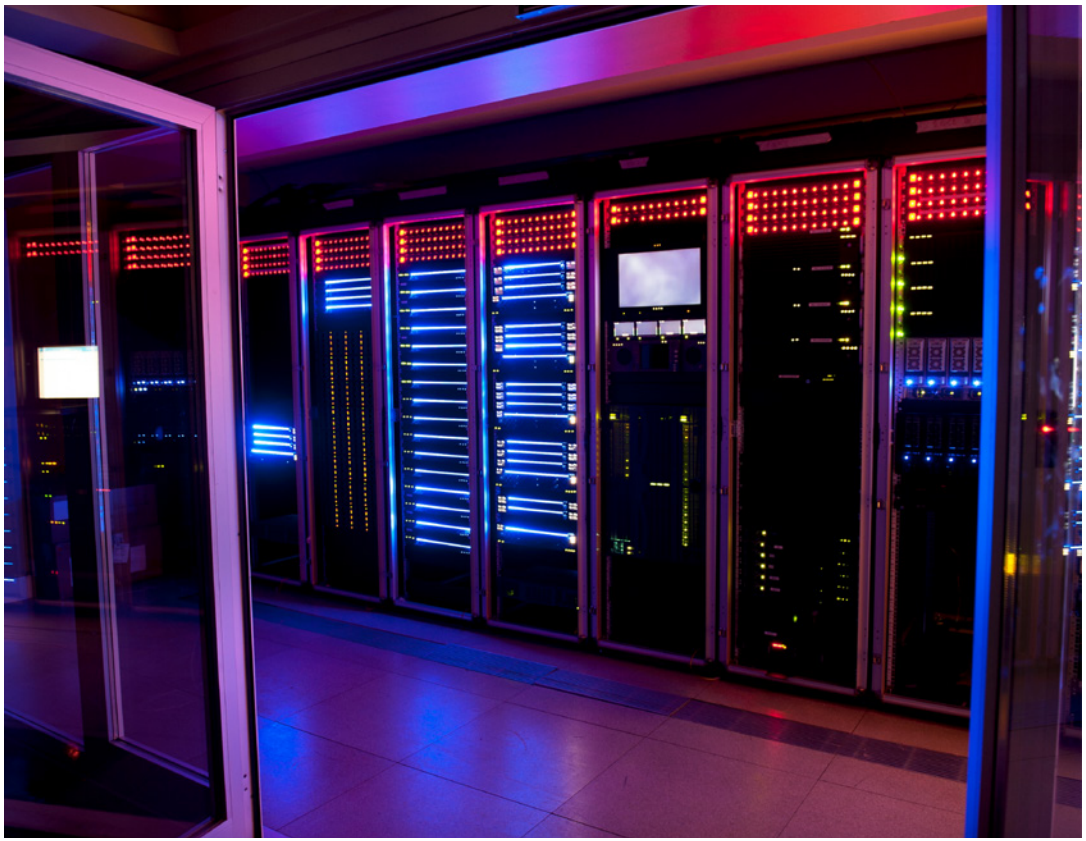
IBM QRadar의 지원으로 새로운 보안 운영 센터(SOC) 서비스를 출시한 IBM 비즈니스 파트너인 Atos SE

Josh Young

5분 분량

사이버 범죄자들이 단 하루도 쉬지 않는 만큼, IT 보안 팀은 언제든지 사이버 공격을 감지하고 차단할 준비가 되어 있어야 합니다. 그러나 대부분의 기업은 연중 무휴 상주하는 보안 팀을 고용하는 것이 단지 실용적이지 않다고 결론을 내렸거나 그럴 여유 자금이 없습니다.

Atos China의 빅 데이터 및 보안 책임자인 Cheng Cai He는 “지난 20년 동안 보안 및 데이터 유출에 대한 위협은 꾸준히 증가해 왔습니다. 그리고 바이러스와 같은 공격 유형이 중국 지역에서 매우 빠르게 진화하고 있습니다.”라고 말합니다.



이에 대응하여 많은 Atos의 고객들은 새로운 보안 장비 및 보안 제품에 상당한 투자를 하기 시작했습니다. 그러나 이러한 장비 및 제품이 제대로 통합되지 않아 사용자를 보호하는 기능이 제한되는 경우가 빈번합니다.

Cheng Cai는 “보안 기능이 효과적으로 작동하지 않았죠. 제조 산업을 시작으로 많은 기업들이 이 모든 제품이 함께 작동하도록 하는 방법에 대해 이야기하기 시작했습니다. 이에 클라우드 기반 보안 운영 센터(SOC) 서비스를 구축하는 방법을 모색하기 시작했습니다.”라고 덧붙입니다

오늘날 보안 운영 센터(SOC)는 중국 시장에서 더욱 보편화되었습니다. 그리고 Atos는 SOC 서비스를 통해 고객의 보안 데이터를 더욱 효율적으로 중앙 집중화하여 전반적인 네트워크의 상태 및 안정성을 전방위적으로 파악할 수 있었습니다.

Cheng Cai는 “이전에는 우리가 알고 있던 모든 SOC는 회사 내부에서 직접 구축되었습니다.”라고 말하며 “이러한 SOC는 비용이 많이 들어가는 큰 투자이기 때문에 흔치 않았습니다. 모든 유형의 보안 디바이스를 구입해야 하고, 연중 무휴 보호 기능을 제공하려면 전담 지원 팀을 구성해야 하고 자금을 투자해야 합니다.”라고 덧붙입니다.

대략적인 SOC 서비스 제공 가격대

< 풀타임 직원 (FTE) 1.5명 급여

사내 보안 팀을 구축하려면 7~8명의 풀타임 직원(FTE) 필요

중소기업 규모의 고객 대상

24 x 7

보안 모니터링 및 보호 서비스 제공

반면에 Atos는 서비스 기반 접근 방식을 선택함으로써 SOC의 장점을 주요 IT 프로젝트에 재정을 투자할 여력이 없는 중소기업에게까지 확대하여 보안 서비스를 제공할 수 있었습니다. 또한 Atos는 이러한 서비스를 다양한 최종 사용자 환경에 손쉽게 제공하기 위해 클라우드 기반 제공 모델에 의존해야 했습니다.

Cheng Cai는 다음과 같이 덧붙입니다. "중국에서 클라우드 산업은 지난 5년 동안 많은 발전을 이루었습니다. 그리고 많은 고객들이 IT 자산을 은프레미스에서 클라우드로 이전하고 있습니다. 하지만 클라우드로의 전환 과정은 다소 복잡합니다. 중요한 정보와 고객의 개인 데이터를 국외로 전송할 수 없다는 데이터 보호법을 준수해야 하기 때문이죠. 따라서 새로운 서비스를 제공하기 위해 클라우드 솔루션을 중국 내에서 호스팅해야 했었습니다."

"지난 20년 동안 보안 및 데이터 유출에 대한 위협은 꾸준히 증가해 왔습니다. 그리고 바이러스와 같은 공격 유형이 중국 지역에서 매우 빠르게 진화하고 있습니다." 라고 말합니다.

Cheng Cai He, IBM 비즈니스 파트너 Atos China의 빅 데이터 및 보안 책임자

새로운 기술. 새로운 구현 방식. 새로운 기능.

Atos는 이 계획된 SOC 서비스를 제공하는 방법을 고려하기 시작하면서 광범위한 마케팅 분석, 고객 요구 사항 및 기대치 평가에 직접 참여하였습니다. 동시에 Atos는 새로운 SOC를 구축하는 데 신뢰하고 사용할 수 있는 잠재적인 보안 제품과 도구를 고려하기 시작했습니다.

IBM 비즈니스 파트너인 Atos는 IBM 기술, 특히 IBM Security® QRadar® XDR 제품군에 집중했습니다. 그리고 플랫폼을 통한 성공적인 개념 증명(POC) 후 Atos는 새로운 SOC 서비스의 SIEM(보안 정보 및 이벤트 관리) 요구 사항을 감독하기 위해 IBM Security QRadar SIEM을 선택했습니다. 한편 Microsoft Azure는 Shanghai Blue Cloud Technology Co., Ltd.(“21Vianet”)

를 통해 중국에서 필요한 클라우드 환경을 제공하고 있습니다.

반면 QRadar 기술은 AI 기반 위협 탐지 및 로그 분석과 함께 모니터링하는 고객 네트워크에 대한 전반적인 뷰를 제공합니다. “QRadar 덕분에 모든 것을 볼 수 있습니다.”라고 Cheng Cai는 덧붙입니다. “고객의 상황을 정확히 파악하고, 우선 순위가 높은 항목과 큰

문제가 되지 않는 부분을 파악할 수 있어서 매우 유용합니다."

고객 온보딩 이후 QRadar의 배치를 간소화하기 위해 Atos는 IBM® Embedded Solution Agreement(ESA)에 서명했습니다. Cheng Cai는 당시를 회상하며 다음과 같이 말했습니다. "지난 4월에 ESA에 서명했습니다. QRadar 제품을 Atos의 제품에 통합하면서 라이센싱이 더 쉬워졌어요. 그리고 이 계약은 Atos와 IBM의 파트너십을 공식화하고, 두 기업이 얼마나 긴밀하게 협력하고 있는지 보여주었습니다."

새로운 서비스는 2022년 8월에 완성되었으며, 처음에는 기존 Atos 고객 세 곳과 함께 파일럿 단계를 진행했습니다. 그리고 다음 달에 Atos SOC 서비스가 일반 대중을 대상으로 공식 출시되었습니다.

Cheng Cai는 "그리고 베이징에 소재한 IBM Innovation Center에서 두 개의 워크샵을 개최하여 SOC 서비스 데모를 선보였습니다. 그리고 워크샵에서 이루어진 논의를 기반으로 Atos의 제품 카탈로그를 더욱 확장하고 있습니다."라고 말합니다.

"[QRadar] 덕분에 모든 것을 볼 수 있습니다 고객의 상황을 정확히 파악하고, 우선 순위가 높은 항목과 큰 문제가 되지 않는 부분을 파악할 수 있어서 매우 유용합니다."

Cheng Cai He, IBM 비즈니스 파트너 Atos China의 빅 데이터 및 보안 책임자

IBM을 선택해야 하는 이유

Cheng Cai는 “QRadar가 Atos의 SIEM에 가장 적합했습니다”라고 말하면서 “QRadar에는 중국 정부가 요구하는 수많은 정책 및 규제 요건에 통합되어 있었으니까요. 그리고 고객사 중 한 곳에서 SOC 플랫폼을 배치한 첫째 날부터 사용할 수 있었습니다.”라고 덧붙입니다.

그리고 계속해서 이렇게 말합니다. “그리고 지난 10년 동안 QRadar와 IBM Security가 Gartner Magic Quadrant에 계속 포함되었다는 사실을 확인했습니다. 고객에게 동급 최고의 서비스를 제공하려면 동급 최강의 보안 제품이 필요하죠.”

Atos는 IBM 비즈니스 파트너로서, 지난 수년간 글로벌 비즈니스와 함께 형성해 온 두 기업의 지속적인 좋은 관계에 큰 가치를 두고 있습니다. Cheng Cai는 “Atos는 오랫동안 IBM과 파트너십을 유지해 왔습니다. 하지만 이 프로젝트는 중국 내 IBM과 협력한 두 번째 프로젝트에 불과합니다 우리는 외부

지원을 통해 새로운 솔루션을 제작할 경우 다른 기업의 협력과 신뢰가 전체적인 운영을 성공으로 이끄는 필수 요소라는 점을 알고 있었습니다. 그리고 IBM은 성공을 위한 열쇠를 제공했습니다.”

Cheng Cai는 이러한 신뢰 정신의 중요성에 대해 다음과 같이 설명합니다. “우리는 IT 서비스 기반의 회사이며, IBM China에는 보안 서비스 팀이 있습니다. 따라서 일부 사업 기회에서 사실 IBM과 경쟁 관계에 놓이기도 합니다. 하지만 IBM과 같은 글로벌 기업과의 기존 관계, 그리고 이 프로젝트의 직접적인 경험을 통해 IBM이 전적으로 신뢰할 수 있는 파트너라는 것을 확신했습니다”

간단한 구현, 복잡한 보호

Atos는 새로운 SOC 서비스를 통해 중국 중소기업을 위한 포괄적이고 강력한 보안 모니터링 및 관리 기능을 합리적인 가격에 제공할 수 있게 되었습니다.

Cheng Cai는 다음과 같이 설명합니다. "당사의 가격 정책을 기준으로 SOC 서비스를 구축하려면 약 1~1.5명의 풀타임 직원(FTE)의 임금이 필요합니다. 그러나 기업이 자체 SOC를 구축하려면 7~8명으로 구성된 전담 팀이 필요합니다. 따라서 모든 보안 제품을 확보하는 데 필요한 자본 지출을 제외하더라도, 연중무휴 24시간 지원을 제공하는 것만으로도 경쟁력이 있습니다."

그는 다음과 같이 계속해서 설명합니다. "한편 위협과 보안 기술은 매우 빠르게 진화하고 있기 때문에 정책 및 기술을 지속적으로 업데이트해야 합니다. SOC는 이러한 업데이트를 지속적으로 제공하며 이러한 유형의 서비스를 제공하는 것은 Atos가 시장 최초입니다."

QRadar 플랫폼은 내장된 AI 및 자동화 기능을 활용해 사이버범죄를 보다 신속하게 식별하고 해결할 수 있도록 지원합니다. Cheng Cai는 "사이버 공격에 대응하려면 속도가 가장 중요합니다."라며 "네트워크의 비정상적인 동작을 더 빨리 식별하고 격리할수록 침입으로 인해 발생할 수 있는 잠재적 손상이 줄어들기 때문입니다."라고 덧붙입니다.

Atos SE 소개

IBM 비즈니스 파트너 Atos(ibm.com 외부 링크)는 IT 컨설팅 서비스, 디지털 보안 솔루션 및 탈탄소화 제품을 제공하는 글로벌 공급업체입니다. 프랑스 파리에 본사를 두고 71개 국가에 사무소와 사이트를 운영하고 있으며, 전 세계적으로 112,000명 이상의 직원을 고용하고 있습니다.

솔루션 구성 요소

- IBM® Embedded Solution Agreement
- IBM Security® QRadar® XDR
- IBM Security QRadar SIEM