IDG
STRATEGIC
MARKETING SERVICES

IBM Security

IDG Case Study

DGB데이터시스템

DGB금융그룹 전체의 보안을 고도화… 통합보안관제 센터 구축

IBM 큐레이더를 선택한
'3가지 이유'

DGB금융그룹 전체의
보안 역량 고도화

DGB금융그룹 전체의 보안을 고도화…

DGB데이터시스템 SoC 구축 사례

IDG Custom Contents

DGB금융그룹의 IT 시너지를 위해 2012년 4월 9일 설립된 DGB데이터시스템은 지난 2016년 총 8곳에 이르는 DGB금융그룹 계열사에 보안모니터링 서비스를 제공하기 위해 업계 선도적인 보안 위협 탐지 및 분석 플랫폼인 IBM 큐레이더(QRadar)를 도입했다. 외부 기업이 원격으로 진행하는 보안 관제로는 직접 대응에 어려움이 있었던 것은 물론, 필요한 정보를 적시에 받기조차 쉽지 않았기 때문이었다.

그러나 이는 쉽지 않은 결정이었다. 단순히 솔루션을 도입하는 수준의 문제가 아니었기 때문이다. 인프라를 구축하는 것은 물론 관제 노하우를 확보해야 하고, 관제 업무를 수행할 인력까지 훈련시켜야 했다. 오늘날 내로라하는 금융 그룹사 중 보안 관제를 직접 수행하고 있는 조직이 일부에 그치는 이유이기도 하다. DGB데이터시스템이 직접 IBM 큐레이더 기반의 SoC를 구축하고 운영해온 지난 5년 동안의 과정을 살펴본다.

"결국 책임은 우리가 진다, 역량 내재화 결정"

DGB금융그룹은 처음 계열사별로 보안 관련 업무를 대응을 하였으나 지능화, 첨단화되는 사이버테러 위험에 대해 계열사별 보안 수준 차이를 극복하고 금융당국의 규제 방식 변화, 금융 IT 패러다임의 변화 등 보안위험이 심화되는 상황을 보완하기 위하여 2015년 DGB금융그룹 통합보안관제센터 구축을 결정하게 되었고 DGB데이터시스템이 주관사로 선정되어 보안관제센터를 운영하게 되었다.

통합보안관제센터 설립 목표는 뚜렷하였다. 사이버테러에 대응 가능한 그룹 보안대응 체계를 구축하여 내,외부 보안위협으로부터 고객정보를 보호하고 그룹 업무 연속성 확보하는 것, 그리고 그룹 내 IT자회사 역할을 강화시키고 보안관제 업무 통합을 통해 계열사 보안 강화 및 효율성을 증대시키는 것이였다.

DGB데이터시스템은 2015년 어렵더라도 보안관제센터를 직접 구축하기로 결정하고 탐색에 나섰다. 시중의 보안관제 솔루션 도입을 물색하는 것은 물론, 도입 이후 역량 내재화와 고도화까지 염두에 뒀다. 금융전문 그룹으로서 '보안'을 간과할 수 없기에 내린 결정이었다. 김경화 본부장은 "결국 보안 문제가 생기면 책임은 우리가 져야 한다. 역량이 부족한 상태에서 보안 사고가 발생하면 심각한 상황이 될 수밖에 없다. 종합적인 보안 역량을 키워보자는 결정을 내렸다. 지역 인재를 채용하고 육성함으로써 지역 경제에 기여한다는 회사 차원의 판단도 있었다"라고 말했다.

IBM 큐레이더를 선택할 수밖에 없었던 '3가지 이유'

국내외 보안 전문 벤더를 대상으로 PoC를 진행한 결과 IBM 큐레이더가 단연 돋보였다. 일단 경쟁사의 경우 서드파티 솔루션의 조합으로 제안했던 데 반해, IBM은 자체 제품과 서비스를 함께 제안했다. 역량 내재화를 염두에 둔 DGB데이터시스템 입장에서는 적응 부담이 덜하고 UI가 우수한 단일 기업의 토탈 솔루션을 선택할 이유가 뚜렷했다.

김경화 본부장은 또 IBM이 제공하는 글로벌 유즈케이스(Use Case)가 월등히 풍부했으며, 관제를 위한 TI(Threat Intelligence)가 차별화돼 있었다고 전했다. 타사의 경우 오픈소스 TI 정보를 직접 찾아서 넣어야 했던 반면, IBM은 X-Force 관제 서비스의 정교한 TI 콘텐츠를 제공하는 점이 매력적이었다는 설명이다. 그는 "제공되는 유즈케이스 수의 단위 자체가 달랐다"라고 말했다.

무엇보다도 DGB데이터시스템에게 절실했던 부분에 대해 IBM은 매력적인 제안을 제시했다. 막막하기만 한 보안관제 구축과 관련해, 관제실 구성에서부터 내부 배치, 운영 프로세스, 인력 추천은 물론, 관제 인력에 대한 교육 서비스까지 제시한 것이다. 대구에 소재한 현장에 1년에 수 차례 이상 방문 서비스한다는 구체적인 약속이 뒤따랐다.

IBM이 이렇듯 파격적인 제안을 할 수 있었던 데에는 이유가 있다. 지금은 'IBM 시큐리티'라는 단일 조직이지만 당시만 해도 서비스 부문과 솔루션 부문으로 나뉘어 있었다. IBM 담당자들은 '원 팀'을 구성해 비즈니스 사례를 만들어볼 수 있는 좋은 기회라고 판단해 과감한 투자를 결정했다는 후문이다.

DGB금융그룹 전체의 보안 역량 고도화

IBM 큐레이더 SIEM 관제 솔루션을 도입한 지 5년여가 지난 현재, DGB데이터시스템은 어떤 평가를 내리고 있을까? 김경화 본부장은 수많은 긍정적인 효과가 직간접적으로 도출됐다며 이야기를 시작했다. 초기 구축 및 인력 확보 과정이 결코 쉽지는 않았던 것이 사실이지만, 이들을 극복해낸 것이 오히려 전화위복이 되었다는 설명이다.

그는 "보안 이슈가 발생했을 때 대응하는 속도가 빨라진 것은 물론, 원인에 대해 제대로 파악할 수 있는 구조가 마련됐다. 아울러 특히 까다로운 은행 수준의 보안 역량을 그룹 전체에 확보할 수 있게 됨으로써 계열사 전체가 높은 보안 수준을 유지할 수 있게 됐다"라고 말했다.

직접적인 투입 비용 대비 효과에서도 확인할 수 있다고 김경화 본부장은 설명을 이어갔다. 그는 "5년 동안의 절감한 외주 비용이 이미 투자 비용을 넘어섰다"라며, 그간 DGB금융그룹 계열사의 보안을 안정적으로 유지할 수 있었던 점은 더욱 큰 가치라고 강조했다. 실제로 IBM이 매년 발간한 보안 보고서에 따르면 데이터 유출에 따른 대가는 국내 기업의 경우 평균 32억 원에 달한다. 금융 분야에서는 좀더 혹독하다.

글로벌 기업 기준 평균 60억 원을 데이터 유출에 따른 비용으로 지출하는 것으로 조사된 바 있다.

DGB데이터시스템의 보안 역량은 DGB데이터시스템의 IBM 큐레이더 활용상에서도 드러난다. 초기에는 큐레이더에 내재된 유즈케이스나 이를 기반으로 커스터마이징된 유즈케이스가 주로 활용됐지만, 이제는 DGB데이터시스템이 독자적으로 개발한 유즈케이스가 더 많이 활용될 정도다. 일례로 IBM 나병준 실장은 DGB데이터시스템의 큐레이더 활용 수준이 업계 최정상급이라고 표현했다. 그는 "솔루션 운영 노하우 측면에서 DGB데이터시스템의 수준은 최소 상위 10%에 든다. IBM 큐레이더를 이용해 관제를 어느 정도 수준까지 할 수 있는지 보여주는 사례"라고 평했다.

독자적 보안관제포탈 '프리즘' 개발로 이어지다

DGB데이터시스템의 보안 역량을 보여주는 대표적인 사례가 있다. IBM 큐레이더 SIEM은 보안 위협을 정확하게 탐지하고, 위협이 발견되었을 때 우선 순위에 따라 빠르게 대응할 수 있도록 하여 영향을 최소화할 수 있도록 하는 지능형 보안 분석 플랫폼이다. IBM 큐레이더 SIEM은 일반적인 통합 보안 로그 모니터링 시스템과는 달리, 업데이트되는 위협 정보까지 학습해 적용하는 인공지능 보안 기술인 '왓슨 포 사이버 시큐리티(Watson for Cyber Security)' 머신러닝 기법도 사용한다. 이를 통해 내부사용자 이상행위 탐지(UBA) 기술, IBM의 방대한 보안 위협 정보(Threat intelligence), 네트워크 패킷 분석 등 첨단 보안 기술을 단일 시스템에서 제공할 수 있다.

DGB데이터시스템은 3년 동안 축적한 경험과 역량을 바탕으로 이러한 IBM 큐레이더의 활용 가치를 높이는 새로운 무기를 직접 개발하기로 결정했다. IBM 큐레이더 SIEM으로부터 수집된 정보를 일목요연하게 확인할 수 있게 해주는 보안관제포탈까지 직접 개발하기로 한 것. 강력한 보안 컴플라이언스 의무를 가지고 있으며, 각종 금융 공공 기관에게 제출해야 할 보안 데이터가 적지 않은 그룹 내 금융 기업들에게 꼭 필요하다는 판단에서였다.

그 주인공이 2019년 탄생한 통합 보안관제포털인 '프리즘'(PRISM)이다. 대구 팔공로에 위치한 DGB 데이터시스템은 물론, DGB금융그룹 산하의 여러 계열사 곳곳에서 24/365로 동작하며, IBM 큐레이더가 제공하는 각종 보안 정보를 실시간으로 한눈에 보여주는 시스템이다. 직관적인 정보 확인을 위한 3D 그래픽 UI 기술도 적용됐다. 이를테면 전세계 각 지역에서 유입되는 트래픽 및 공격 현황이 3D로 표현된 지구본에 가시적으로 표현된다.

DGB데이터시스템 김형식 대표는 "시중의 보안관제포털 솔루션과 비교해 확실히 차별화된 강점을 갖추고 있다. 빠른 속도 외에도 일괄 처리 기능, 3D 그래픽을 이용한 우수한 가시성의 대시보드, 2팩터 인증, 보고서 자동 생성, 다양한 알림 기능, SEIM API 연계, 금융보안원 전문 연계(16종), 보안 관련 소명 프로세스를 활용한 내부 보안 기능 등이 그것"이라고 설명했다.

김형식 대표는 "앞으로 대외 서비스 사업을 검토하고 있다. 보안관제센터를 운영하는 중견 규모 이상의 기업, 금융 기업에게 차별화된 경쟁력을 가질 것으로 자부한다. 국내외 다수의 고객사를 확보한 IBM이기에 '윈윈'하는 사업 기회가 될 것으로 기대한다. 상품성 검증 과정도 함께 진행했다"라며, "이제 새로운 비즈니스 모델을 창출하는 단계에 이르렀으니 보안관제

솔루션 도입 프로젝트가 기대 이상의 성과로 이어진 셈"이라고 웃으며 말했다.

보안관제, 솔루션 이상의 가치제안이 중요하다

김형식 대표는 그러나 지난 5년 동안 과정이 결코 쉽지만은 않았다고 토로했다. 무엇보다 인력 문제가 쉽지 않았다는 이야기였다. 그는 "관제 인력을 대구 경북 지역에 채용하는 것 자체가 힘들었다. 또 초급 인력을 육성시키는 기간 역시 현실적인 비즈니스 문제였다. 솔루션의 기능이 아무리 좋아도 운영에 녹이는 것은 순전히 우리 몫이라는 점을 체감했다"라고 말했다.

이와 관련해 IBM의 적극적인 협력이 주효했다고 그는 덧붙였다. 6개월에서 1년에 걸린 체득화 기간 동안 IBM과 긴밀이 협업함으로써 현실적인 문제들을 해결해나갈 수 있었다고 그는 전했다. 김형식 대표는 "솔루션의 성능과는 또다른 문제다. 벤더에서 얼마나 지원을 잘 해주느냐, 전문 인력을 얼마나 보유하고 있느냐, 실제 보안 운영에 대한 전반적인 경험을 가지고 종합적인 가이드나 조언을 해줄 수 있느냐를 꼭 살펴봐야 한다"라고 조언했다.

DGB데이터시스템 개발 개요

프로젝트 명	DGB금융그룹 통합보안관제 구축 및 통합보안관제 포탈 개발
기반 솔루션	IBM 큐레이더
도입 솔루션	자체 구축 개발

주요 특징

- 보안강화 : 2팩터 인증, 암호화 통신, 로그인IP 설정
- 시각화 : 기본대시보드 및 3D대시보드 제공
- 편의성 : 일괄처리 및 조회, 각종 알림 기능, 보고서 자동 생성
- 확장성 : SIEM API 연계, 금융보안원 전문 연계(16종) 가능

Interview

“한층 높은 수준의 보안관제 서비스 제공”

● DGB데이터시스템 **김형식** 대표

김형식 대표는 30년 이상 대구은행에 근무한 금융맨이다. 대구은행 지점장 및 부서장을 역임했으며, 2018년 공모를 거쳐 DGB데이터시스템 대표에 취임했다. 다음은 김형식 대표와의 일문일답이다.

직접 통합보안관제센터를 구축하고 관제포탈까지 개발하게 된 결정적 계기가 있다면?

그룹 내 고객사들의 만족시키기 위한 유일한 방법이라고 판단했다. 기성 솔루션을 도입하거나 외주 개발을 맡기면 명목상으로는 고객사의 요구대로 만든다. 그러나 현업 담당자는 IT를 잘 알기 어렵고 개발자는 현업의 니즈를 속속들이 알기 어렵다. 그래서 우선순위가 엇갈린 결과물이 나오기 쉽다. 꼭 필요한 기능을 제대로 정리하고 확장성과 유연성을 확보하기 위해서는 IT와 현업의 니즈를 모두 파악하고 있는 내부 인력의 역량이 요구됐다.

아울러 대표로서 내부 직원의 역량에 초점을 맞추고 있다. 금융그룹의 자회사로서 보안은 함께 가야만 하는 주제다. 내부 직원들의 경쟁력을 높일 수 있는 기회라고 판단했다.

IBM 큐레이더를 직접 활용한 입장에서 평가한다면?

2015년 도입 당시의 큐레이더와 2020년 현재의 큐레이더가 크게 달라졌다는 점을 언급하고 싶다. ‘고객이 귀찮을 정도로 업그레이드를 많이 요구’하는 측면도 있다. 전세계 선도 업체들의 요청을 반영하다보니 고객사에게 이를 앞서 ‘푸시’하는 것으로 풀이된다. 꾸준히 이에 대응하는 과정도 그리 녹록하지 않았지만 이렇듯 새로운 기능과 콘텐츠를 추가하는 것이 DGB데이터시스템의 보안 역량을 높이는데 큰 도움이 됐다.

프리즘의 상용화를 시도 중이다. 핵심 차별화 포인트를 간략히 설명한다면?

보안관제포털의 근본 목적에 충실하다. 기업에서 일어나는 각종 보안 현황을 한눈에, 알기 쉽게 보여준다. 아울러 보안관제와 관련해 기업에서 특히 관심있는 요소는 ‘소명’이라고 본다. 침해가 어디서 어떻게 발생했는지를 프리즘을 통해 간단히 확인할 수 있다. 즉 기본적인 위협을 충실하게 보여주는 한편, 소명 또한 이 시스템을 통해 명료하게 할 수 있다.

덧붙여 말하고 싶은 것이 있다면, 보안 부문과 현업 부문의 소통이다. 소수 전문가들이 암호 같은 로그 정보와 씨름하는 모니터링은 현업 부문과 괴리된 업무이기 쉽다. 비용은 비용대로 쓰면서 하는 일이 뭐냐는 소리를 듣게 되는 배경이다. 그런 의미에서 보안관제의 핵심은 ‘가시성’과 ‘즉시성’, ‘현업의 활용성’이며, 이러한 고민이 프리즘에 녹아 있다고 말하고 싶다.