AhnLab

Case Study

골프존 랜섬웨어 사례로 본 AhnLab XDR 활용 전략

산업

- 스포츠 시뮬레이션 소프트웨어

혜택

- SaaS 형태의 신속한 AhnLab XDR 구축
- 보안 솔루션별 이벤트 가시성 확보 및 선제적 대응
- AhnLab MDR 연계를 통한 보안관제 전문가 중심의 이벤트 분석, 보고서 발행
- 보안 담당자 업무 생산성 향상
- 탐지 정확도 향상으로 전반적인 사내 리스크 감소
- 안랩과 구축한 기술적 및 운영적 네트워크 100% 활용 가능

솔루션

- AhnLab V3
- AhnLab EDR
- AhnLab EPP
- AhnLab MDR
- AhnLab XDR

개요

골프존(Golfzon)은 골프와 자사 핵심 정보기술(IT)을 결합한 골프 시뮬레이터(Golf Simulator, GS) 전문 기업이다. 이 시스템을 중심으로 혁신적이고 몰입감 있는 다양한 통합 골프 서비스를 제공한다.

골프존은 안랩의 보안 솔루션을 도입하여 조직의 보안을 강화하고, 고객들에게 안전하고 신뢰할 수 있는 서비스를 제공하기 위해 노력하고 있다. 안랩의 엔드포인트 및 통합 보안 솔루션을 채택함으로써 위협 리스크를 줄이고, 서비스 안정성을 확보했다.

2023년 랜섬웨어 사고를 겪은 이후, 골프존은 자사 인터넷망과 IDC, AWS, 전자금융망 등에 안랩의 EDR과 EPP를 설치했다. 이와 더불어, 관리형 탐지 및 대응 서비스인 AhnLab MDR을 함께 도입하여 안랩의 위협 전문가가 탐지된 위협을 능동적으로 분석하고, 대응 방안을 제시하는 서비스도 제공받았다. 이후, AhnLab EDR과 더불어 좀 더 효율적인 보안 리스크 관리를 위해 AhnLab XDR을 추가로 설치했다. 기존에 AhnLab V3를 비롯해 AhnLab EDR, AhnLab EPP가 설치돼 있어, AhnLab XDR을 수월하게 구축할 수 있었다. 골프존은 이들 솔루션을 중심으로 실시간 위협 탐지와 대응, 랜섬웨어 사고 복구와 서비스 재개를 지원하고 있다.

골프존은 보안이 강화된 골프 상품과 서비스를 지속적으로 출시하고 운영함으로써 고객에게 최고의 골프 경험을 선사할 예정이다.

> 골프존은 안랩의 지원을 받아 랜섬웨어 피해를 신속하게 복구하고, 내부에 잠재된 공격자를 식별하여 처리할 수 있었습니다. 또한, 기존의 보안관제 서비스를 제공받는 과정에서 안랩과 함께 구축한 기술적·운영적 네트워크를 적극 활용할 수 있었던 점도 큰 도움이 됐습니다. 앞으로도 안랩과의 긴밀한 협업을 통해 안전성이 보장된 다양한 골프 서비스와 상품을 개발할 것입니다.
>
> - 골프존 정보보안팀 김정훈 프로

도전 과제

- 블랙 수트 조직에 의한 랜섬웨어 사고 발생
- 다수 이벤트 관리 및 대응 체계 미흡
- AhnLab EDR의 효과적인 운영 필요
- 이벤트 우선순위/중요도 판단을 위한 접근법 도입 필요성 대두

도전과제

2023년 11월 23일, 골프존은 랜섬웨어 조직 '블랙 수트(BlackSuit)'의 공격을 받아 서비스 장애가 발생했고, 탈취된 정보는 다크웹(DarkWeb)에 공개됐다.

골프존은 해당 침해 사고를 분석하는 과정에서 인가된 사용자의 권한을 도용해 다양한 악성 행위를 벌이는 것을 확인했다. 또한, 공격자는 랜섬웨어 공격 이후에도 골프존의 내부 정보를 이용해 지속적으로 공격을 시도한 것으로 나타났다. 골프존은 사태의 심각성을 인지하고, 엔드포인트 단의 모든 행위를 분석하고 공격 활동을 차단하고자 AhnLab EDR을 도입했다. 추가로, 안랩의 지원을 받아 골프존 내 서버와 엔드포인트에 엔드포인트 보호 플랫폼 'AhnLab EPP'를 설치했다.

이와 더불어, 골프존은 20여 종의 보안 솔루션을 운영해 옴에 따라 다양한 보안 솔루션에서 발생하는 단일 이벤트를 일일이 대응하고 처리하는 데 애로사항이 있었다. 각각의 얼럿(Alert)이 단순한 실수인지, 해커의 공격인지, 유의미한지 무의미한지 알기 어려웠다. 이들 이벤트를 꼼꼼히 검토할 수 있는 리소스와 인력, 툴 등의 체계가 부족했던 탓이다.

따라서 하루에 수백만 건씩 발생하는 얼럿 중 유의미한 위협을 찾아내어 사전에 조치할 수 있는 접근법을 도입하고, 기존 AhnLab EDR을 보다 효율적으로 운영하기 위해 안랩과 협력하여 AhnLab XDR을 구축했다.

솔루션

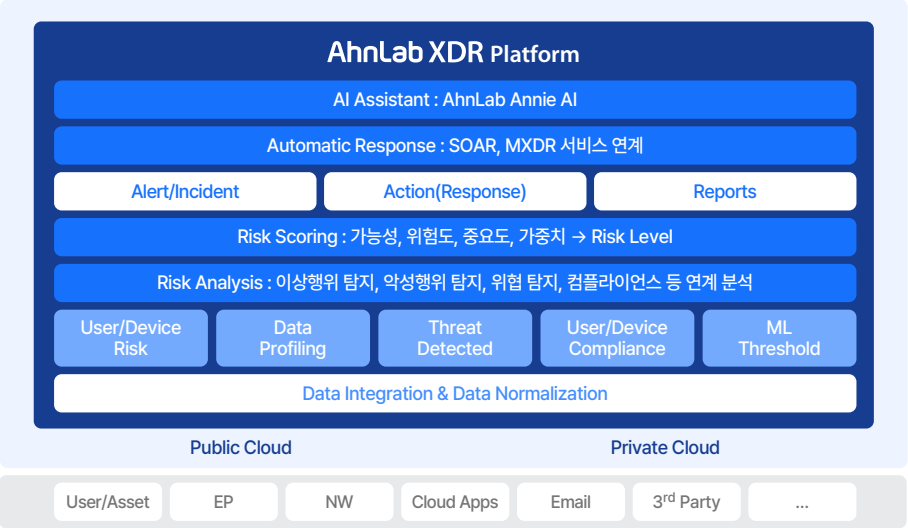
골프존에는 AhnLab EDR과 AhnLab EPP가 이미 구축돼 있었고, AhnLab MDR 서비스를 동시에 지원받아 엔드포인트에서 발생하는 다양한 위협을 효과적으로 관리하고 있다. 랜섬웨어 사건 발생 이후, 안랩의 위협 정보 분석 전문 팀 'A-FIRST'가 골프존의 침해사고를 정밀하게 분석하여 문제점을 진단하고, 해결을 위한 솔루션을 제공했다.

골프존은 각 보안 솔루션에서 발생하는 단일 이벤트에 일일이 대응하기 어려운 문제를 해소하고자 AhnLab XDR을 구축했다. AhnLab XDR은 SaaS 방식으로 구축돼 데이터로 인한 하드웨어 확장이나 성능 문제와 같은 고민을 해소하고, 신속하게 구축할 수 있었다. 또한, 서버나 엔드포인트 가용성을 해치지 않는 범위에서 원활한 운영이 가능했다.

골프존은 1,500여 대의 PC 자산과 700대 이상의 서버의 자산 정보를 AhnLab XDR과 연동하고, 보안 시스템과 주요 운영 솔루션의 로그를 결합하여 탐지 시나리오에 따라 이메일, 텔레그램(Telegram) 등으로 위협 알림을 발송하도록 설정했다. 이를 통해 보안 솔루션의 개별 관리를 넘어, 전사적 리스크 관리 및 대응 영역으로 AhnLab XDR의 기능을 확장하고자 했다.

솔루션

- AhnLab EDR, EPP 구축 및 MDR 지원을 통한 침해 사고 정밀 분석
- SaaS 형태의 AhnLab XDR 구축으로 하드웨어 확장 및 성능 문제 해결
- AhnLab XDR 도입 및 주요 자산 정보와의 연동



[그림 1] AhnLab XDR 플랫폼 구조도

도입효과

안랩의 EDR/MDR, EPP에 이어 AhnLab XDR을 도입한 후, 골프존의 보안 수준은 전반적으로 향상됐다. 골프존은 AhnLab XDR을 중심으로 다양한 보안 솔루션 로그에 대한 상관관계 분석을 통해 직관적이고 유의미한 분석과 처리를 수행하고 있다.

골프존은 보안 시스템에서 발생하는 방대한 양의 이벤트에 대한 오탐, 중요도가 낮은 위협에 대한 리소스 낭비를 줄이고, 담당자가 탐지하거나 대응하지 못한 이력들을 찾아내는 효과적인 보안 체계를 구축했다. 이를 통해 악성 의심 IP 접근, VPN 이상 로그인, 브루트 포스(Brute Force) 공격 방어, 관리되지 않은 방화벽 정책 고도화 등을 실현하며 전체 보안 이벤트 수가 크게 감소했다.

실제로 2024년 5월 기준 3,046건이었던 보안 리스크가 2024년 8월 1,691건으로 줄어 3개월 만에 56% 감소했다. 이 중에서도 엔드포인트 영역에서 확인된 리스크는 1,840건에서 264건으로, 총 86% 감소했다.

이 외에도, 정탐율이 향상되고 보안 담당자의 생산성이 높아졌으며, 데이터 허브(Data Hub)를 통해 보안성 강화와 데이터 수집 및 연동 효율화를 달성했다.

[그림 2] AhnLab XDR 도입 후 골프존 사내 리스크 감소 현황

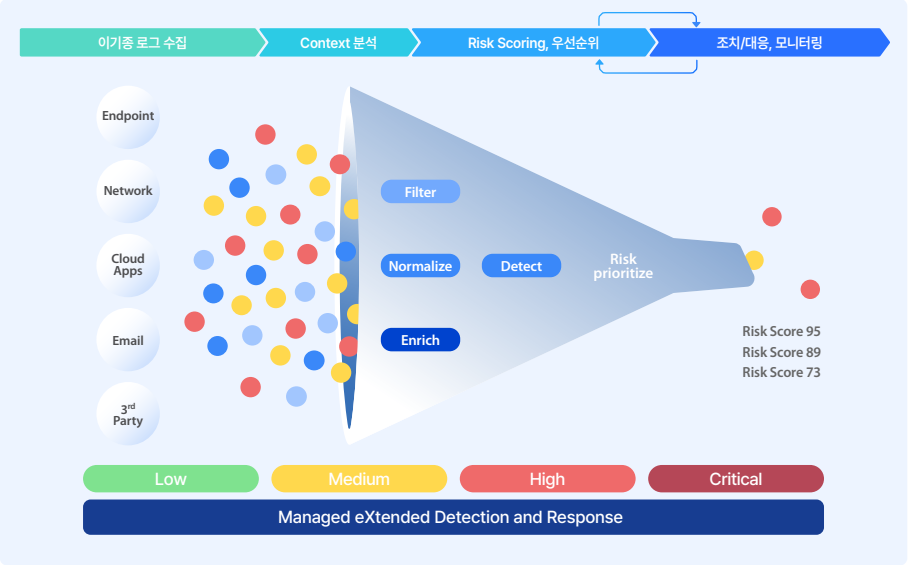
결과

- 로그 상관관계 분석을 통한 직관적 보안 관리
- 전체 보안 이벤트 수 감소
- 정탐율 향상 및 보안 담당자 생산성 증대
- 데이터 수집 및 연동 효율성 극대화

향후 계획

골프존은 보안 강화를 위한 지속적인 투자와 노력의 일환으로, 안랩의 보안 솔루션을 적극적으로 활용할 계획이다. 특히, AhnLab XDR을 기반으로 점차 복잡해지는 위협 환경에 선제적으로 대응하기 위해 더욱 견고한 보안 체계를 구축할 예정이다. AhnLab XDR을 활용해 다양한 보안 솔루션에서 발생하는 이벤트 간의 상관관계를 정교하게 분석하고, 이를 바탕으로 전사적 리스크 관리와 대응 기능을 강화하며, 실시간 위협 모니터링 및 탐지, 분석 역량을 향상시킬 것이다.

최근에는 안랩의 MXDR 서비스 도입을 검토하고 있다. AhnLab MXDR은 원격 보안 관제와는 별개의 서비스로, 안랩의 보안 전문가가 내부의 위협 요소를 식별하고, 상세 분석 후 제거하며, 실시간으로 경고를 전송하는 XDR 전용 관리 서비스이다. 현재도 안랩은 자사 MDR 서비스를 통해 골프존의 리스크 탐지 내역과 특이사항, 악성코드 탐지 관련 권장 사항을 이메일로 전송하는 등 실시간으로 골프존 보안성 강화를 위해 노력하고 있다.



[그림 3] AhnLab MXDR 위협 탐지/대응 프로세스

향후에도 안랩과의 협업을 통해 엔드포인트 외에도 클라우드 환경과 외부 시스템에 대한 보안 점검 및 모니터링을 강화해 공격자가 골프존의 인프라를 타겟으로 삼지 않도록 철저히 대비할 것이다. 이를 통해, 고객에게 안정적인 서비스를 제공하며 업계 리더로서의 입지를 더욱 확고히 할 계획이다.

AhnLab

경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901