

보안 운영 수준을 한 차원 높이는 FireEye Helix

머리말

사이버 보안은 그 어느 때보다 어려운 문제로 대두되었습니다. 매일 새로운 위협이 등장하고 취약점들이 노출됨에 따라 기업들은 제품을 추가로 구매하고 인재를 보강해야 한다는 압력을 받고 있습니다. 이 같은 사후 대응적 방식은 복잡성을 가중시키고, 이 같은 복잡성은 공격자들이 악용할 또 다른 취약점이 됩니다. 효율적인 보안 운영을 위해서는 종합적이고 근본적인 접근 방식이 필요합니다. FireEye Helix는 조직이 그러한 토대를 구축하는 데 도움을 줍니다.

FireEye Helix는 간단한 방식으로 모든 조직에 첨단 보안을 제공하는 보안 운영 플랫폼입니다. 이전에 볼 수 없었던 위협을 노출시키고 전문가가 인텔리전스를 활용해 결정을 내릴 수 있도록 함으로써, 방어 시스템에 대한 제어력을 다시 확보해 주고 보안 투자 효과를 극대화합니다. FireEye Helix는 모든 FireEye 솔루션과 함께 사용할 수 있으며, 타사 제품을 비롯하여 모든 보안 솔루션을 연결하고 개선할 수 있는 효율적이고 확장성이 뛰어난 토대가 됩니다. 보안 전문가에 의해, 보안 전문가를 위해 설계된 이 제품은 보안 팀이 경보 관리, 검색, 분석, 조사 및 보고와 같은 주요 업무를 효율적으로 수행하도록 지원합니다.

이점

가시성 개선

300여 개의 FireEye 및 타사 보안 툴을 통합하고 국가 등급의 위협 인텔리전스, 규칙, 분석을 오버레이하여 독보적인 상황 인식을 제공합니다.

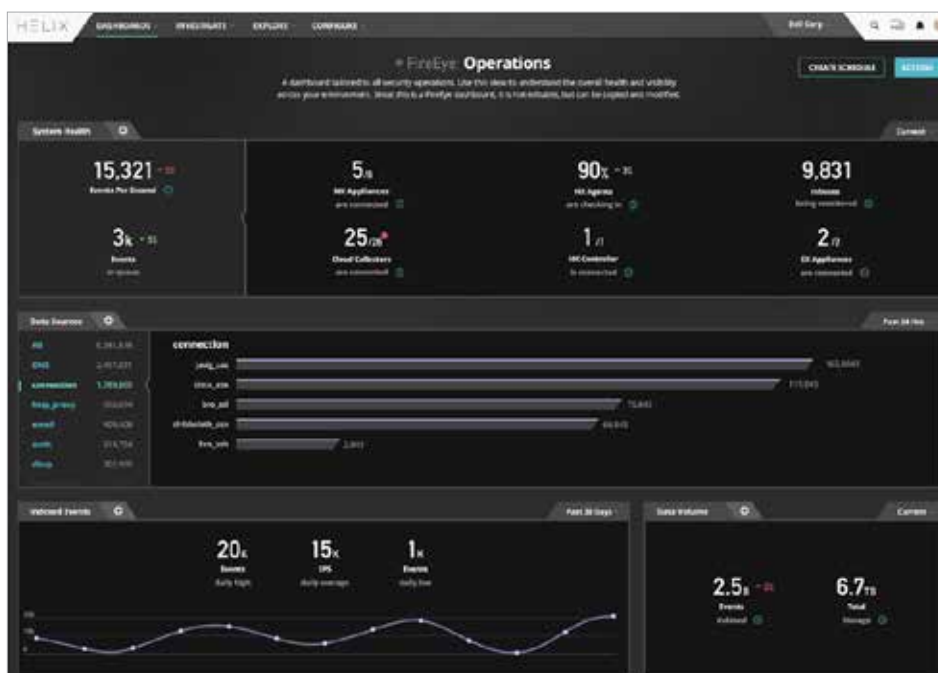
대응 시간 단축 및 침해 피해 최소화

최전선에서의 경험을 바탕으로 사전 제작된 플레이북을 활용하여, 주요 보안 기능을 집중화하고 워크플로우를 자동화합니다.

총 운영 비용 절감

SIEM, 위협 인텔리전스 및 보안 오케스트레이션을 비롯한 기존의 지출 분야를 통합 합니다.

그림 1. 즉각적인 상황 인식을 위한 운영 인터페이스



IT의 역할



실제 적을 탐지하고 행동 파악



상황별 위협 인텔리전스를 이용하여 정보에 근거한 결정을 내릴 수 있게 함



기존 보안 투자의 효용성 개선

그림 2. FireEye Helix의 기능

 <p>분석 데이터에서 숨겨진 패턴 및 비정상적인 상태를 찾아 탐지 기능을 더욱 강화하고, 조사 프로세스에 상황 정보를 제공합니다.</p>	 <p>API 타사 제품과 통합하고 고객 환경에 원활하게 통합할 수 있는 유연한 개방형 API를 지원합니다.</p>	 <p>상황(컨텍스트) 인텔리전스, 경보, 호스트 및 사용자 데이터 전체에서의 상황 정보를 비롯한 관련 데이터가 자동으로 통합되므로 빠르게 의사 결정을 내릴 수 있습니다.</p>
 <p>컴플라이언스 미리 정의되거나 사용자 지정된 대시보드 및 위젯을 통해 컴플라이언스 요구 사항을 충족하는 동시에 사용자에게 가장 중요한 정보를 시각적으로 취합하고 표시하고 탐색합니다.</p>	 <p>탐지 기존 데이터에 FireEye 전문 규칙과 FireEye iSIGHT 인텔리전스를 적용하여 다른 톨로는 감지할 수 없는 위협을 확인합니다.</p>	 <p>디바이스 및 정책 관리 환경 전체의 구성, 정책 및 상태를 관리합니다.</p>
 <p>역할 기반 접근 제어 역할 기반 그룹을 만들어 콘솔에 액세스할 수 있는 세분화된 권한을 할당할 수 있습니다.</p>	 <p>인텔리전스 FireEye의 최신 인텔리전스 위협을 국가 및 산업별로 분류하여 탐지, 강화, 탐색 및 학습합니다.</p>	 <p>오케스트레이션 제품 통합 및 특정 경보에 대해 정의된 작업을 통해 조사 및 대응 프로세스를 자동화하고 시간을 단축합니다.</p>
 <p>조사 워크벤치 유연한 보안작업의 전환과 신속한 탐지를 지원하기 위해 인프라 전체에 있는 모든 소스의 경보 및 이벤트 데이터에 대해 완벽한 인덱싱, 보관, 검색 및 악성코드 분석을 수행합니다.</p>	 <p>워크플로우 관리 자동화된 워크플로우 및 수동 워크플로우를 통해 조사 프로세스 전체의 단계를 체계화, 할당, 협력 및 실행합니다.</p>	

FireEye에 대한 더 자세한 정보를 원하시면
다음의 웹사이트를 방문하십시오.

www.FireEye.kr

FireEye 소개

FireEye®는 인텔리전스 기반 SaaS(Security-as-a-Service)의 리더입니다. FireEye는 고객 보안 운영의 완벽한 확장을 위해 혁신적인 보안 기술, 국가 수준의 위협 인텔리전스 및 세계적으로 유명한 엔드포인트 컨설팅을 결합한 단일 플랫폼을 제공합니다. 이를 통해 FireEye는 사이버 공격에 대비, 방어 및 대응하고자 노력하는 조직의 사이버 보안 부담을 감소시킵니다. FireEye는 포브스 글로벌 2000 기업 중 940개 이상의 기업을 포함해 67개국의 5,000여 기업을 고객으로 보유하고 있습니다.

파이어아이 코리아(유)

서울특별시 강남구 테헤란로 534.
글라스타워 20층
전화: 02.2092.6580
korea.info@fireeye.com
www.fireeye.kr

www.FireEye.kr