데이터 시트

FireEye Managed Defense

FireEye의 모든 역량을 기반으로 한 관리형 탐지 및 대응(MDR) 서비스

요약

- **시장을 선도하는 위협 인텔리전스:** FireEye의 여러 그룹에서 일하는 보안 분석가들이 최신의 실시간 머신, 피해자 및 공격자 인텔리전스를 적용하여 고객의 보안 환경에서 보다 빠르게 위협을 찾아내고 세부적인 내용을 파악합니다.
- **포괄적인 추적:** 분석가들은 FireEye의 기술, 분석 전문 지식 및 인텔리전스를 활용하여 숨은 공격자와 위협 활동을 선제적으로 추적합니다.
- **조사 및 대응:** 분석가들이 중요 위협을 철저히 조사하여 효과적으로 대응하는 데 필요한 자세한 정보를 제공합니다.
- **경보 우선순위 지정:** 가장 중요한 경보를 식별하여 즉각적으로 대응해야 할 경보에 집중할 수 있도록 합니다.
- **Managed Defense 컨설턴트:** 보안 전문가는 고객의 주요 담당자 역할을 함으로써 악성코드 샘플 분석, 심층적인 포렌식 분석, 현장의 침해 사고 대응 등 추가적인 지원을 촉진합니다.
- **연중무휴로 방어 제공:** 미국(버지니아주), 아일랜드 및 싱가포르의 SOC에서 하루 24시간 연중무휴로 완벽한 방어를 제공합니다.

보안 위협이 계속 진화하고 있지만, 대부분의 조직은 여전히 가장 소중한 자산을 보호하는 데 사후 대응적인 기술 기반의 보안 솔루션에 의존하고 있습니다. 기술만으로는 거침없는 공격자를 완벽하게 방어할 수 없습니다. 그리고 보안 전문가와 특히, 은밀한 위협을 찾아 식별할 수 있는 전문가를 찾아 고용하고, 필요한 교육을 제공하며, 보유하는 데는 상당한 노력과 비용이 소모됩니다.

일선의 경험을 통해 구축한 최신 위협 인텔리전스를 활용하여 사전 대응적인 분석가 중심의 접근 방식을 통해 24시간 내내 네트워크를 모니터링하려면 신뢰할 수 있는 파트너가 필요합니다. 즉, FireEye Managed Defense가 필요합니다.

인텔리전스 중심의 탐지 및 대응

FireEye Managed Defense는 관리형 탐지 및 대응(MDR) 서비스로, 업계에서 인정받는 사이버 보안 전문성과 FireEye 기술, 공격자에 대한 독보적인 지식을 결합하여 보안 침해의 영향을 최소화하도록 지원합니다.

Managed Defense는 업계 최대 규모의 글로벌 사이버 위협 인텔리전스 제공 기능의 지속적인 지원을 받으며, 세계에서 가장 피해가 큰 사이버 공격과 관련하여 일선에서 확보한 머신, 캠페인, 공격자 및 피해자 인텔리전스를 활용합니다. 이 같은 일선의 인텔리전스와 전문 지식은 탐지율을 높이고 FireEye 분석가의 추적 및 조사 활동의 지침을 제시하여 가장 지능화된 공격자까지 포착할 수 있게 합니다. 보안 분석가가 공격자 활동에 대한 포괄적인 진단과 맞춤형 대응 권장 사항을 통해 위협을 파악하고, 위험을 진단하고, 완벽한 조치를 취하는 데 필요한 정황 정보를 제공합니다.

이용 방법

FireEye Managed Defense는 FireEye의 독점 기술 스택을 활용함으로써 ICS 및 클라우드 인프라를 비롯하여 기업 전반에 걸친 실시간 가시성을 제공합니다.

FireEye Managed Defense 분석가는 공격자, 피해자 및 시스템 기반 위협 인텔리전스를 사용하여 알려진 위협과 이전에 탐지되지 않던 위협을 탐지 및 조사하고 적극적으로 탐색합니다.

침해의 징후가 확인되면 즉시 사용자에게 알리므로 사용자가 안전한 포털을 통해 최신 분석 정보를 검토할 수 있으며, 그와 동시에 FireEye의 분석가들이 사고를 계속 분석합니다.

또한 고객은 효과적인 대책을 수립하고 공격자가 목적을 달성하는 것을 막을 수 있도록 위협에 대한 정황 정보와 해결 방법에 대한 권장 사항을 제공하는 자세한 요약 보고서도 받게 됩니다.

공격자 이해

점점 더 정교하고 표적화되는 오늘날의 사이버 공격을 예측하고 이에 대응하려면 공격자의 동기, 의도, 특성 및 수법을 이해해야 합니다. 이러한 이해는 최전선에서의 경험을 통해 확보한 지식에서 비롯됩니다.

Managed Defense 분석가는 독점적인 조사 기법을 활용하여 침입의 징후를 발견하고 공격자의 활동 방식을 파악하고 공격자의 역량을 심층적으로 평가합니다.

또한 경험이 풍부한 분석가가 중국 기반의 지속적인 지능형 위협에서 러시아 기반 공격자에 이르기까지 30개 이상의 국가 후원 그룹을 포함하여 약 16,000명의 위협 공격자에 대해 시장을 선도하는 위협 통찰력을 사용합니다.

분석가는 공격자의 활동 방식에 대한 이러한 행동적 통찰력을 통해 상황을 빠르게 평가하고 공격자의 활동 역량 정도를 면밀히 조사하며 공격자의 다음 행동을 예측하고 고객에게 효과적인 대응 계획을 제공할 수 있습니다.

그림 1. 인텔리전스 중심 탐지 .

포괄적인 추적 **조직적 대응** **중요 위협 식별 및 우선순위 지정**

포괄적인 추적

FireEye Managed Defense는 사전 대응적인 분석가 중심의 탐색 접근 방식을 활용합니다. 즉, 경험이 풍부한 분석가가 악의적인 활동의 징후를 검색할 때 공격자와 그들의 전술, 기법 및 절차(TTP)에 대한 지식 및 이해를 통합적으로 적용합니다. Managed Defense 분석가는 표적 환경에서 발판을 마련하려는 수법을 지속적으로 발전시키고 바꿔가면서 탐지를 회피하려고 시도하는 위협 공격자로부터 새로운 TTP 증거를 체계적으로 찾아냅니다.

FireEye 분석가가 창출하여 사용하는 독점적인 탐색 기법은 다른 Managed Defense 고객을 통해 확보한 인텔리전스, FireEye Mandiant와의 컨설팅 계약 및 FireEye 위협 인텔리전스 기능을 기반으로 지속적으로 업데이트 및 조정됩니다.

조직적 대응

Managed Defense 고객은 FireEye가 사이버 공격의 최전선에서 6,300개가 넘는 고객사를 보호함으로써 확보한 지식 및 경험을 활용하는 이점을 누릴 수 있습니다.

FireEye는 업계, 지역 또는 기술 프로파일을 기반으로 고객사와 유사한 조직에 시도된 공격을 관찰하거나 공격자 기법에 변경 사항이 있음을 알게 된 경우, 즉시 고객 네트워크에서 이러한 공격의 증거를 검색하기 시작합니다. 고객이 침해당하지는 않았지만, 표적이 될 수 있다는 증거가 있는 경우, FireEye는 예상되는 공격으로부터 고객을 방어하기 위한 권장 조치를 제공합니다.

Managed Defense를 선택해야 이유

경험

가장 영향력이 높은 침해에 대응해온 연간 100,000시간 이상의 Mandiant 사고 대응팀 경험을 활용

더 빠른 탐지

Managed Defense를 통해 조사하고 대응하는 데 소요되는 평균 시간은 67분

경제적인 솔루션

내부 역량을 개발하고 유지하는 데에는 많은 시간, 예산 및 리소스가 소요될 수 있음

인텔리전스

150명 이상의 인텔리전스 분석가가 지원하는 국가 수준의 인텔리전스 컬렉션에 대한 액세스

강력한 방어

FireEye 기술 및 인텔리전스를 적용한 독점 기술 스택

- FireEye 제품 탐지 건수 1억 5,000만 건
- 수집된 Managed Defense 경보 2,200만 건
- 분석가 조사 건수 17만 건
- 우선순위가 높은 위협의 91%를 신속 대응 없이 해결
- 신속 대응 사고의 98%를 전체 사고 대응 서비스를 이용하지 않고도 해결

그림 2. 경험 기반 대응.

중요 위협 식별 및 우선순위 지정
FireEye Managed Defense 분석가는 가장 영향력이 큰 위협에 집중합니다. 즉, 다른 제품에서 보내는 대개 관련성이 없는 여러 경보 노이즈를 가려내 고객팀이 시간과 노력을 절약할 수 있도록 합니다. 고객은 FireEye 분석가 및 사고 대응자의 축적된 지식을 활용하여 기존의 보안 제어를 피했던 위협을 비롯하여 잠재적으로 영향력이 가장 높은 위협을 파악하는 이점을 누릴 수 있습니다.

면밀한 사고 조사
Managed Defense 분석가는 조사를 진행하는 동안 모든 FireEye 인텔리전스를 활용하여 모든 경보 아티팩트를 검토하고, 네트워크 트래픽 또는 엔드포인트를 검사하여 침해 정도를 파악하며, 해당하는 모든 이벤트를 통합하여 킬 체인 전체에 걸쳐 타임라인을 확인합니다. 분석가는 100,000시간이 넘는 사고 대응 서비스로부터 얻은 독점적 기법 및 인텔리전스를 활용하여 사고를 자세히 조사합니다.

신속한 대응
보다 심각한 공격의 경우 Managed Defense 분석가는 잠재적으로 FireEye 악성코드, 인텔리전스 및 사고 대응 팀의 추가적인 전문가 리소스를 참여시켜, 분류된 이벤트에 대한 심층 분석을 제공하고 고객 에코시스템 전반을 검색하여 전체 침해 범위를 파악할 수 있습니다.

복구 권장 사항
FireEye에서 조사하고 평가를 제공하면 Managed Defense 분석가가 복구 권장 사항을 제공하여 고객이 더 빠르게 사고에 대응할 수 있도록 합니다.

위협으로 확인된 경우, Managed Defense를 선호하는 요율로 FireEye Mandiant의 완벽한 사고 대응 서비스로 손쉽게 전환할 수 있습니다.

지침 및 통찰력
Managed Defense 고객은 보안 포털에 액세스할 수 있습니다. 보안 포털은 고객 커뮤니케이션 및 협업을 위한 통로뿐만 아니라 보고 및 인텔리전스에 대한 액세스도 제공합니다. 또한 일상적인 담당자 역할을 하는 Managed Defense 컨설턴트(MDC)를 배정해 드립니다. MDC는 사고 대응 및 포렌식에 대한 전문 지식과 풍부한 경험을 갖춘 전문가로, 전략적 권장 사항을 제공하여 고객이 보안 환경을 개선하도록 지원합니다.

FireEye에 대한 자세한 정보: **www.FireEye.com**

FireEye Korea
서울 특별시 강남구 테헤란로 534 글라스타워 20층
02.2092.6580
korea.info@fireeye.com

FireEye, Inc. 소개
FireEye는 인텔리전스 기반의 보안 회사입니다. FireEye는 혁신적인 보안 기술, 국가 수준의 위협 인텔리전스 및 세계적으로 유명한 Mandiant® 컨설팅을 결합한 단일 플랫폼을 제공하여 고객 보안 운영의 완벽한 확장을 지원합니다. 이를 통해 FireEye는 사이버 공격에 대비하고 이를 방어 및 대응하고자 노력하는 조직의 사이버 보안 부담을 줄이고 간소화합니다.

FIREEYE™