데이터 시트

위협 인텔리전스 포트폴리오

위협 인텔리전스의 가치와 영향력 극대화를 위한 방안

주요 기능

- 보안 업무에 맞춤 설계된 실행 가능한 위협 인텔리전스 서비스 제공
- 글로벌 위협에 대한 상황 정보와 우선 순위를 적용하여 일반적인 공격 라이프사이클을 넘어선 가시성을 제공
- 보다 정확한 정보를 기반으로 한 경영 위험 관리를 위해 자산 보호 개선
- 발생 가능성이 가장 높은 위협 및 공격자에 대비하여 보안 프로그램 및 리소스를 조정
- 위협 인텔리전스를 잘 활용할 수 있게 최적화 설계 및 구축
- 보안 의사 결정권자 및 일선의 네트워크 보안 담당자를 위한 맞춤형 인텔리전스 및 분석 제공

사이버 공격자들은 대부분의 보안 조직보다 잘 훈련되고 풍부한 자금력과 보다 나은 조직력을 확보하고 있습니다. 그리고 사이버 공격은 점점 더 복잡해지고 더 심각한 피해를 줍니다.

이런 이유로 외부 위협 인텔리전스 서비스를 활용해 위험을 줄이고 보안을 강화하려는 조직이 늘어나고 있습니다. 하지만 어디서 시작해야 할지 모르는 조직이 많고, 어떤 위협 인텔리전스가 필요한지, 아니면 어떻게 사용해야 할지를 이해하지 못한 채 무작정 뛰어드는 조직도 있습니다. 그 결과는 비효율적이고 비용만 많이 들게 됩니다.

FireEye iSIGHT 위협 인텔리전스가 해답을 드립니다.

FireEye 위협 인텔리전스는 위협 인텔리전스 요구사항의 모든 측면을 해결하도록 설계된 구독 모델 및 서비스 포트폴리오입니다. 위협 인텔리전스 여정을 막 시작한 조직이나 전용 인텔리전스 팀을 보유한 조직 모두에게 이 솔루션은 조직의 자산 보호를 개선하고 보안 프로그램의 효율성을 향상시키며 비즈니스 위험 프로세스에 대한 정보를 제공하는 통찰력을 제공합니다. 제공하는 혜택은 다음과 같습니다.

- **인텔리전스 구독:** 전략 및 운영을 위한 인텔리전스, 사이버 범죄 및 사이버 스파이 위협, 정보 운영, 산업 제어 시스템 위협 및 취약성 인텔리전스에 관한 인텔리전스 보고서를 제공합니다.
- **인텔리전스 구현:** 지정된 위협 인텔리전스 분석가 및 관리자는 신뢰할 수 있는 조언자로서 기업 및 조직의 담당자와 정기적으로 협력하여 해당 인텔리전스 서비스에 대한 투자를 최대한 활용할 수 있도록 합니다. 여기에는 온보딩 및 프로비저닝, 기존 보안 시스템과의 API 통합, 보안 분석 정보, 맞춤형 위협 보고 및 전략 워크샵이 포함됩니다.
- **인텔리전스 역량 개발:** 해당 컨설팅 및 평가 서비스는 인텔리전스 기반의 보안 프로그램에 접근하여 평가 및 구축을 하고 성숙하게 하여 사이버 위협 인텔리전스에서 얻은 가치를 실현하고 유지하는 데 도움이 됩니다. 그리고 ICD 서비스에는 기존 위협 인텔리전스 프로그램 기능 및 위협 노출 평가, 프로그램 개선을 위한 전략적 계획 수립 및 조직의 위협 인텔리전스 프로그램 운영 프레임워크 개발이 포함됩니다.
- **디지털 위협 모니터링:** 브랜드, VIP 및 통합 파트너 커뮤니티에 대한 맞춤형, 선제적 모니터링 및 위협 분석을 제공합니다.
- **고급 인텔리전스 제공:** 해당 기능은 FireEye의 전방위적 가시성, 인사이트 및 인텔리전스를 직접 확인할 수 있습니다. 또한 전담 분석가를 통해 관련 조직에 특정 니즈에 맞는 리서치와 분석이 진행됩니다.

고객과 함께 성장하는 보안

기존 보안 프로그램 또는 위협 인텔리전스 요구사항에 관계없이 FireEye 위협 인텔리전스 포트폴리오는 고객의 조직을 위한 적합한 솔루션을 제공합니다. 처음 시작하게 되는 경우, 고객 조직과 함께 현재 상황을 진단 후 필요한 솔루션에 대해 파악할 수 있게 됩니다. 필요한 인텔리전스와 이해 관계자가 누구인지 알고 있다면 FireEye의 다양한 인텔리전스 구독 서비스를 통해 보안 결정에 도움을 받을 수 있습니다. 조직이 인텔리전스 관련 인력의 기술을 강화하거나 팀의 역량을 확장해야 하는 경우 FireEye 위협 인텔리전스가 필요한 솔루션을 제공합니다.

진단

위협 인텔리전스 관련 현재 조직의 현 수준을 진단하고 앞으로의 상황에 대비할 수 있는 가치를 최대한 활용할 수 있게 대비할 수 있습니다. FIreEye는 다음 질문에 대한 해답을 드립니다.

- 사이버 위협 노출이란 무엇입니까?
- 인텔리전스를 어떻게 활용할 수 있습니까?
- 현재 우리 조직의 인텔리전스 프로그램의 빈틈은 무엇입니까?

정보

포괄적이고 실행 가능한 인텔리전스를 활용하여 새로 부상하는 사이버 위협에 대한 더 나은 방어 기능을 지원합니다. 광범위한 주제와 활용 사례는 성숙되었거나 성장하는 조직의 보안 팀에게 공격자의 의도, 방법 및 활동에 대한 중요한 맥락을 제공합니다. FIreEye는 다음 질문에 대한 해답을 드립니다.

- 운영하는 사업, 관련 산업 군 또는 지역에 가장 높은 위협 사항은 무엇입니까?
- 다음 중 어떤 경보를 먼저 처리해야 하며 이러한 경보를 어떻게 더 잘 이해할 수 있습니까?
- 다음 중 기업 또는 조직의 현황에 기반하여 보완해야 하는 취약성은 어떤 것들이 있습니까?
- 기업 및 조직의 브랜드, VIP, 인프라 및 파트너 커뮤니티에 대한 위협에 대해 알 수 있는 방법은 무엇입니까?

향상

인텔리전스 작업의 효율성을 높이기 위해 모범 사례 및 업계 전문 지식을 축적합니다. 또한 최적화된 인텔리전스 조직을 설계하고 전담 분석가 지원을 포함한 FireEye 위협 인텔리전스에서 제공하는 서비스를 전부 활용할 수 있습니다. FIreEye는 다음 질문에 대한 해답을 드립니다.

- 인텔리전스 분석가의 역량을 개선할 수 있는 방법은 무엇입니까?
- 위협 탐지 능력을 개선할 수 있는 방법은 무엇입니까?
- 팀이 접근할 수 있는 인텔리전스 및 전문 지식 수준을 어떻게 보완할 수 있습니까?

FIREEYE INTELLIGENCE를 선택해야 하는 이유

FireEye는 그 누구보다도 사이버 위협과 이를 담당하는 사람에 대해 잘 알고 있습니다. 당사는 현재 사이버 활동에 대한 탁월한 접근성을 보유하고 있으며 이를 위협 인텔리전스 운영에 직접 활용합니다. FireEye는 공격자, 피해자 및 캠페인 정보를 제품 원격 측정 데이터와 결합하여 경쟁업체가 따라올 수 없는 실행 가능한 위협 인텔리전스를 생성합니다. 추가 이점은 다음과 같습니다.

- 인텔리전스 수집, 분석 및 컨설팅에서 12년 이상의 경험
- 23개국에 걸쳐 30여 가지 모국어 및 현지 언어를 사용하는 "현장" 연구 인력 180명
- "Forrester New Wave:™ 외부 위협 인텔리전스 서비스, 2018년 3분기" 유일한 리더로 선정
- 인텔리전스 역량 개발 서비스는 수년 간의 고객 프로젝트 참여 및 점진적인 FireEye 위협 인텔리전스 기능의 축적을 기반으로 합니다

자세한 내용은 **www.fireeye.com/solutions/cyber-threat-intelligence.html** 및 **Forrester 보고서** 를 참조하십시오.

FireEye Korea
서울특별시 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 고객의 보안 운영 플랫폼을 완벽하게 확장할 수 있습니다. 이를 통해 FireEye는 사이버 공격에 대비하고 이를 방어 및 대응하고자 노력하는 조직의 사이버 보안 부담을 줄이고 간소화합니다.