FIREEYE™

데이터 시트

Mandiant 컨설팅 및 MDR 서비스

심각한 침해 대응 및 조직의 자산 보호 능력 강화를 위한 서비스

보안 프레임워크의 필요성

"Mandiant는 조직이 보안 침해에 대비하는 방법을 재고하도록 하는 중요한 위치에 있습니다."

Michael Chertoff
전임 국토안보부 장관

Mandiant Difference

FireEye Mandiant는 2004년부터 사이버 보안 및 사이버 위협 인텔리전스를 선도해 왔습니다. Mandiant의 사고 대응 팀은 세계에서 가장 복잡한 침해 사건을 일선에서 처리해 왔습니다. 기존의 위협 공격자와 새로 등장하는 공격자를 상세히 파악하는 동시에 급변하는 공격 툴, 전술 및 절차를 심층적으로 파악하고 있습니다.

당사는 업계 최고의 사이버 침해 사고 대응 및 인텔리전스 기반의 위험 기반 보안 서비스를 제공하여 침해 사고 전후와 발생 당시에 조직이 공격자를 저지하는 데 도움을 줍니다.

공격자 행동, 탁월한 위협 인텔리전스, 맞춤형 기술, Mandiant 보안 평가, 혁신, 교육 및 관리형 탐지 및 대응(managed detection and response, MDR) 서비스에 대한 심층적인 이해를 통해, 비즈니스 위험을 줄이기 위해 기능적 복원력을 구축하고 보안 격차를 좁힐 수 있습니다.

전문성: 가장 심각한 침해에 대응해 온 15년 이상의 실무 경험을 갖추고 있습니다. Mandiant는 공격자의 행동, 방법, 사용한 툴 및 기술과 공격 대상을 식별합니다. Mandiant는 이렇게 식별된 정보를 바탕으로 공격자의 진화하는 행동 및 동기를 독자적인 방법으로 파악하고 전체적인 그림을 봅니다.

인텔리전스: Mandiant의 인텔리전스 기반 서비스 접근 방식은 수천 명 이상의 FireEye iSight 인텔리전스 전문가, 수천 건의 Mandiant 조사, FireEye 제품 및 Managed Defense 서비스로부터 얻은 업계 최고의 사이버 위협 인텔리전스를 바탕으로 빠른 속도로 변화하는 전 세계 위협 환경을 파악합니다.

기술: Mandiant 전문가는 Windows, Linux 또는 macOS를 실행하는 고객의 요구 사항에 따라 클라우드 또는 온프레미스에서 구동되는 FireEye 엔드포인트 기술, 네트워크 센서 및 분석 플랫폼을 활용합니다. 이러한 기술은 더 큰 규모의 환경에서 최소한의 비용으로 신속하게 대응할 수 있도록 합니다.

엄선된 Mandiant 서비스 요약

보안 기능	보안 요구 사항	서비스	개요	혜택
대응	**침해 대응**	**사고 대응 서비스**	심각한 보안 사고의 조사, 억제 및 복구에 필요한 속도, 확장성 및 효율성을 제공합니다.	심각한 보안 사고를 해결하고, 장기적 솔루션을 설정합니다.
		침해 사고 대응 자문 서비스	침해 사고 대응 서비스에 대해 설정된 조건	사고 대응 시간이 크게 단축되고 침해의 전체적인 영향이 축소됩니다.
평가	**공격자의 존재 여부 확인**	**침해 진단 서비스**	환경에서 발생한 과거 또는 현재의 침해를 식별하고, 보안 관리 상태를 기반으로 향후 침해 위험을 진단하고, 대응 능력을 개선합니다.	조직에서 현재 또는 이전에 침해가 발생했는지 여부를 확인합니다.
	대응 준비	**레드팀, 퍼플팀 평가**	침해 사고 대응 분야의 일선에서 볼 수 있는 최신 공격자 툴, 전술 및 절차(tools, tactics and procedures, TTP)에 대한 보안 태세를 테스트합니다.	이전에 탐지되지 않은 약점을 공격자보다 먼저 식별합니다.
		침해 대응 준비 평가	보안 모니터링 및 대응 기능에 대한 독립적인 성숙도 진단 서비스로, 사고 대응의 실무 경험에서 얻은 정보를 바탕으로 진단을 수행합니다.	정보 보안 프로그램의 효과를 평가하여 조직의 보안 태세를 개선하고 비즈니스 위험을 축소합니다.
		모의 연습	시나리오 게임플레이를 사용하여 조직의 사이버 침해 사고 대응 계획을 테스트합니다.	문서화된 프로세스와 실제 대응 간의 차이를 신속하고 효율적으로 파악
	보안 제어 및 보안 태세 평가	**보안 프로그램 평가**	정보 보안 프로그램의 10개 주요 보안 영역을 심층 평가합니다. 각 보안 영역은 규정 준수, 보안 및 산업 프레임워크에 연결됩니다.	정보 보안 프로그램의 효과를 평가하여 조직의 보안 태세를 개선하고 비즈니스 위험을 축소합니다.
		ICS 건전성 점검	최소 침습 진단 방식으로 산업 시설의 전반적인 사이버 보안 태세를 진단하여 IT 보안과 OT 보안을 연결합니다.	ICS의 노출된 취약성을 파악하고 시스템의 사이버 보안 위험을 축소하는 계획을 설정합니다.
		Active Directory 보안 평가	Active Directory의 잘못된 구성, 프로세스 취약점 및 악용 방법 완화	일반적인 공격 경로를 강화하여 보안 사고의 위험과 영향 최소화
		클라우드 인프라 평가	더 나은 클라우드 아키텍처와 구성을 통해 사이버 방어 강화	일반적인 악용 기법으로부터 클라우드 공격 경로를 줄여 위험 완화
혁신	**성숙한 보안 태세**	**사이버 방어 센터 신설**	지능형 위협 공격자들을 방어하기 위해 보안 운영 프로그램을 설계하고 강화합니다.	방어 태세를 개선하여 보안 사고의 영향 최소화, 보안 개선 및 리소스 우선 순위 설정에 대한 합의 도출
교육	**팀 교육**	**제품, 인텔리전스 및 전문 지식 교육**	보안 팀을 대상으로 최신 위협 지식에 대한 교육을 제공하고 변화하는 사이버 위협 환경에 효과적으로 대응하는 데 필요한 운영 기술을 개선합니다.	이론적 시나리오가 아닌 실제 조사에 기반을 둔 학습 및 교육 환경을 제공할 수 있습니다.
방어	**관리형 탐지 및 대응**	**Managed Defense**	업계 최고의 기술과 인텔리전스를 결합한 전문가 중심의 24x7 서비스	침해의 영향을 최소화할 수 있도록 조기에 위협을 식별합니다.
		엔드포인트를 위한 Managed Defense	FireEye Endpoint Security를 사용하여 엔드포인트에서 위협을 신속하게 탐지, 조사 및 억제하는 전문가 중심의 24x7 서비스	네트워크에 대한 가시성 개선 및 대응 가속화
		OT를 위한 Managed Defense	산업 제어 시스템(industrial control systems, ICS) 및 운영 기술(operational technology, OT)에 대한 위협을 파악하고 대응을 가속화하는 전문 지식을 활용한 24x7 서비스	ICS/OT 환경의 방어 태세를 개선하고 보안 이벤트의 영향 최소화

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

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 고객 보안 운영의 완벽한 확장을 지원합니다. 이를 통해 FireEye는 사이버 공격에 대비하고 이를 방어 및 대응하고자 노력하는 조직의 사이버 보안 부담을 줄이고 간소화합니다.

FIREEYE™