MANDIANT®
A FireEye® Company

사고 대응 서비스

심각한 보안 사고의 조사, 억제 및 복구에 필요한 속도, 확장성 및 효율성 제공

사례 연구:
MANDIANT IR 작업 사례

전 세계에 수만 대의 컴퓨터가 배포되어 있는 다국적 전문 서비스 기업이 중요한 고객 데이터의 잠재적 데이터 침해에 대응하기 위해 Mandiant와 계약했습니다.

제1일 - Mandiant는 통보를 받고 4시간 내에 18,000대의 시스템에 클라우드 기반 엔드포인트 기술을 배포하기 시작했습니다.

- 같은 날, 조사도 시작되었습니다.
- 조사를 시작하고 4시간 만에 침해의 확실한 증거가 식별되었습니다.

제6일 - 대부분의 조사 작업이 완료되었습니다. 18,000대 이상의 엔드포인트를 분석했고 80개의 시스템에 심층 라이브 대응 분석을 수행했습니다.

제7일 - 비즈니스 중단 없이 억제 활동을 수행했습니다. Mandiant는 네트워크를 지속적으로 모니터링하여 위협 공격자의 침해 시도가 재발하지 않는지 확인했습니다.

제11일 - 고객의 비즈니스는 정상적인 상태로 다시 운영되었습니다.
모든 작업은 원격으로 수행되었습니다.

Mandiant는 2004년부터 사이버 보안 및 사이버 위협 인텔리전스를 선도해 왔습니다. Mandiant의 사고 대응 팀은 가장 복잡한 침해 사건을 일선에서 처리해 왔습니다. 기존의 위협 공격자와 새로 등장하는 위협 공격자를 상세히 파악하는 동시에 이들이 사용하는 빠르게 변화하는 전술, 기술 및 절차를 심층적으로 파악하고 있습니다.

Mandiant는 수천 건의 사고에 대응하면서 얻은 조사 및 복구 전문 지식을 FireEye의 업계 최고 위협 인텔리전스 및 최첨단 네트워크/엔드포인트 기술에 접목시켰습니다.

Mandiant는 가장 크고 가장 유명한 사고에 대응할 수 있는 자질을 갖추고 있습니다. 따라서 기술적 대응부터 위기 관리에 이르는 모든 측면의 사고 대응에서 고객이 필요로 하는 지원을 제공할 수 있습니다.

Mandiant는 더 빠르고 더 효율적으로 조사 및 복구를 완료하여 가장 중요한 비즈니스 운영을 신속히 재개할 수 있도록 합니다.

개요
클라우드 솔루션과 온프레미스 솔루션을 사용하므로 조사를 즉시 시작하는 동시에 고객 데이터의 개인정보보호와 관련된 문제를 관리할 수 있습니다. Mandiant는 단 몇 시간 안에 수천 대 엔드포인트의 네트워크 트래픽 및 정보를 분석할 수 있습니다. Mandiant의 사고 대응 팀은 일선의 공격 연구 및 기타 인텔리전스 소스에 기반을 둔 광범위한 위협 인텔리전스에 액세스하여 최신 공격자 전술 기술 및 절차를 파악합니다.

Mandiant는 기술적 조사, 억제 및 복구를 넘어서는 종합적인 사고 및 침해 대응 서비스를 제공합니다. 뿐만 아니라 법률, 규정 및 홍보 측면에서 경영진의 커뮤니케이션 및 위기 관리를 지원합니다. 회사의 명성이 손상되는 상황과 법적 책임을 방지하려면 위기 관리가 중요합니다.

표 1. Mandiant가 일반적으로 관리하는 사고 유형:

지적 재산 유출	영업 비밀 또는 기타 중요한 정보의 유출.
금융 범죄	결제 카드 데이터 유출, 불법 ACH/EFT 현금 이체, 갈취 및 랜섬웨어.
PII(개인 식별 정보)	개인을 고유하게 식별하는 데 사용되는 정보의 노출.
PHI(보호 건강 정보)	보호되는 의료 정보의 노출.
내부자 위협	직원, 벤더 및 기타 내부자의 부적절하거나 불법적인 활동.
파괴적인 공격	정보 또는 시스템을 복구할 수 없게 만들어 피해 조직에 위기를 발생시키려는 의도의 공격.

FireEye®

MANDIANT의 차별화 요소

- **조사 경험:** Mandiant의 조사 담당자는 세계 최대 규모의 가장 복잡한 사고를 조사하면서 기술을 연마했습니다.
- **위협 인텔리전스:** 일선의 사고 대응, FireEye 기술을 통해 수집된 DTI(동적 위협 인텔리전스) 및 iSIGHT 인텔리전스 소스로부터 결집된 업계 최고의 인텔리전스를 제공합니다.
- **기술:** Mandiant는 FireEye의 최신 클라우드 및 온프레미스 기술을 사용하여 즉시 조사를 시작할 수 있습니다. 이러한 기술은 네트워크 트래픽과 Microsoft Windows, Linux 및 Mac OS X를 실행하는 엔드포인트에 대한 가시성을 제공하여 대규모의 신속한 대응을 가능하게 합니다. FireEye의 Network Security MVX 기술을 기반으로 구동되는 자동 악성코드 샌드박싱은 시그니처 기반 기술로는 탐지되지 않는 위협을 식별합니다.
- **위기 관리:** Mandiant의 사고 대응 담당자는 오랜 경험을 바탕으로 사고 관련 커뮤니케이션(예: 경영진 커뮤니케이션, 홍보 및 공개 요구 사항)에 대한 조언을 제공합니다.
- **악성코드 분석:** 업계 최고의 리버스 엔지니어 및 연구원이 조사 중에 검색된 악성코드를 분석하여 해당 악성코드의 기능을 파악합니다.

접근 방식

Mandiant의 조사에는 환경을 종합적이고 전체적으로 진단하기 위한 호스트 및 네트워크 기반 분석이 포함됩니다. Mandiant는 고객 환경에서 발생한 사고를 대응 및 복구하는 동시에 규제 요건 및 평판 손실을 방지하는 데 적절한 맞춤형 대응 조치를 제공합니다. Mandiant가 조사 중 식별하는 항목은 일반적으로 다음과 같습니다.

- 영향을 받은 애플리케이션, 네트워크, 시스템 및 사용자 계정
- 악성 소프트웨어 및 악용된 취약성
- 액세스된 정보 또는 유출된 정보

사고 분석

1. **기술 배포/초기 단서 조사:** 빠르고 종합적인 사고 대응에 가장 적합한 기술을 배포합니다. 동시에, 고객이 제공한 초기 단서를 조사하여 IOC(침해 지표)를 생성하기 시작합니다. 이러한 지표는 환경에서 악의적인 활동의 모든 지표를 찾는 동안 공격자 활동을 식별하는 데 사용됩니다.
2. **위기 관리 계획:** 임원진, 법무팀, 비즈니스 리더 및 수석 보안 담당자와 협력하여 위기 관리 계획을 개발합니다.
3. **사고 범위 파악:** 실시간으로 공격자의 활동을 모니터링하고 과거 공격자 활동의 포렌식 증거를 검색하여 사고의 범위를 파악합니다.
4. **심층 분석:** 공격자가 수행한 작업을 분석하여 초기 공격 경로를 파악하고, 활동 타임라인을 설정하고, 침해의 규모를 식별합니다. 여기에는 다음이 포함될 수 있습니다.
   - 라이브 대응 분석
   - 포렌식 분석
   - 네트워크 트래픽 분석
   - 로그 분석
   - 악성코드 분석
5. **피해 진단:** 영향을 받은 시스템, 시설, 애플리케이션 및 노출된 정보를 식별합니다.
6. **복구:** 공격자가 수행한 작업과 비즈니스 요구 사항을 고려하여 공격자의 액세스를 제거하고 환경의 보안 상태를 개선할 수 있는 맞춤형 억제 및 복구 전략을 개발하여 향후 공격을 방지하거나 피해를 제한합니다.

결과물

외부 감사를 받기에 적절한 간략한 조사 및 복구 보고서를 제공합니다.

- **주요 내용 요약:** 일정/조사 프로세스, 주요 결과 및 억제/근절 활동을 간략하게 설명하는 요약입니다.
- **조사 보고서:** 공격 타임라인 및 중요한 경로에 대한 세부 정보를 제공합니다(공격자가 환경에서 공격을 수행한 방법). 이 보고서에는 영향을 받은 컴퓨터, 위치, 사용자 계정 및 유출되거나 위험한 상태인 정보의 목록이 포함됩니다.
- **복구 보고서:** 전략적 권장 사항을 비롯하여 조직의 보안 상태를 향상하기 위해 수행된 억제/근절 조치를 상세히 보고합니다.

사고가 의심되십니까? **investigations@mandiant.com** 으로 이메일을 보내거나 **https://www.fireeye.com/company/incident-response.html**을 방문하십시오.

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. FireEye는 포브스 글로벌 2000 기업 중 45% 이상의 기업을 포함해 67개국의 6,600여 기업을 고객으로 보유하고 있습니다.

FireEye