데이터 시트

침해 대응 준비 평가

지능형 사이버 공격을 탐지, 대응, 억제하는 능력 평가

FireEye Mandiant 를 선택해야 하는 이유

FireEye Mandiant 는 2004 년부터 사이버 보안 및 사이버 위협 인텔리전스를 선도해 왔습니다 . Mandiant 의 사고 대응 팀은 전 세계에서 가장 복잡한 침해 사건을 일선에서 처리하고 있습니다 . 기존의 위협 공격자와 새로 등장하는 위협 공격자를 상세히 파악하는 동시에 이들이 사용하는 빠르게 변화하는 전술 , 기술 및 절차 (tools, tactics and procedures, TTP) 를 심층적으로 파악하고 있습니다 .

개요

고객이 처음부터 새로운 침해 사고 대응 기능을 구축하거나 , 기존의 프로세스를 강화하거나 , 또는 기술 지원을 위해 투자해야 하는지 여부에 상관없이 , Mandiant 는 지속적이고 지능화된 실제 공격에 대한 방어 태세를 강화하도록 지원할 수 있습니다 . FireEye Mandiant Response Readiness Assessment 는 일반적으로 조직의 보안 운영 센터 (security operations center, SOC) 및 침해 사고 대응 (incident response, IR) 능력을 포함하여 조직의 사이버 방어 역량을 평가합니다 . 이 평가는 다양한 지역과 산업 분야에서 침입에 대응하면서 얻은 모범 사례와 최일선의 경험을 활용하여 Mandiant 컨설턴트가 주도합니다 . 평가 후 Mandiant 컨설턴트는 자세한 로드맵과 우선 순위가 지정된 개선 권고 사항이 수록된 보고서를 제공합니다 .

사이버 방어에 막대한 예산을 투자한 조직을 비롯한 대부분의 조직은 표적 위협을 적절히 식별하고 정확하게 평가하며 대응하는 능력에 대한 불확실성이 어느 정도 있을 수 있습니다 . Mandiant 컨설턴트는 일반적인 악성코드 , 랜섬웨어 , 사이버 범죄 및 국가 차원의 APT 공격과 같은 다양한 위협에 대응하면서 얻은 교훈을 활용하여 고유한 위협을 관리하는 조직의 능력을 평가하고 실질적이고 의미 있는 개선을 실현하는 데 필요한 지침을 제공합니다 .

접근 방식

Mandiant 컨설턴트는 문서 검토 , 로깅 구성 분석 , 심층 분석 워크샵 , 모의 연습 및 시뮬레이션을 통한 위협 탐지 제어 테스트를 조합하여 Mandiant 의 6 가지 핵심 대응 준비 역량을 기준으로 조직의 사이버 방어 역량을 엄격하게 검토하고 검증합니다 .

- **거버넌스 .** 전반적인 비즈니스 임무를 지원하는 효과적인 사이버 방어 역량의 토대
- **커뮤니케이션 .** 침해 사고 발생 전 , 발생 중 , 발생 후의 내부 및 외부 이해관계자와 관련된 커뮤니케이션 프로세스
- **가시성 .** 조직의 인프라 전반에 걸쳐 위협을 탐지하는 사람 , 프로세스 및 기술
- **위협 인텔리전스 .** 탐지 및 대응 작업을 지원하기 위해 위협 공격자 툴 , 전술 및 절차 (TTP) 를 파악하고 식별하는 데 사용되는 공격자 인텔리전스
- **대응 .** 조직이 사고를 확인 및 분류하고 심각도를 평가하며 적절한 대응 조치를 결정하는 방법
- **지표 .** 장기적으로 사이버 방어 역량을 관리하고 개선하는 데 필요한 평가 및 개발 전략

평가 후 Mandiant 컨설턴트는 사이버 방어 역량 강화를 위한 우선 순위가 지정된 권고 사항이 수록된 자세한 보고서를 제공합니다 .

계층형 모델 : 조직마다 규모 , 성숙도 및 최종 목표가 다릅니다 . 침해 대응 준비 평가는 조직의 요구 사항에 따라 맞춤화됩니다 . 다양한 지원 활동을 통해 핵심 역량을 검토하고 강화합니다 .

표 1. 침해 대응 준비 평가 단계

단계 및 평가 구성 요소	1단계 평가	2단계 연습 평가	3단계 연습 평가를 기술적으로 검증
일반적인 기간(주)	4	5	6
문서 검토	X	X	X
6가지 핵심 대응 준비 역량 워크샵	X	X	X
로깅 구성 검토	X	X	X
자세한 침해 대응 준비 평가 보고서	X	X	X
기술 브리핑(보고서 검토)	X	X	X
임원 브리핑(맞춤형 PowerPoint)		X	X
침해 사고 대응팀 기술 매트릭스 연습		X	X
조직의 침해 대응 준비 능력 및 산업 비교		X	X
침해 대응 준비 상태 개선 로드맵		X	X
산업별 위협 통찰력		X	X
기술 모의 연습		X	X
임원 모의 연습			X
시뮬레이션을 통한 위협 탐지 제어 테스트 (FireEye Verodin 기반)			X

평가 일정

단계에 따라 , 평가는 4~6 단계로 구성되며 보통 완료하는 데 4~6 주 정도가 소요됩니다 .

문서 검토 (1 주)

사고 대응 계획 , 플레이북 , 커뮤니케이션 계획 및 위기 관리 계획과 같은 관련 사이버 방어 문서의 오프사이트 검토

현장 워크숍 및 기술 매트릭스 연습 (1 주)

이해관계자와 협력하여 각각의 핵심 대응 준비 역량을 다루는 현장 워크샵 및 침해 사고 대응팀과 함께 진행하는 기술 매트릭스 연습 (최대 7 개의 워크샵)

로깅 구성 검토 (0.5 주)

중요 로그 샘플을 검토하여 효과적인 위협 탐지 및 대응을 위한 구성 검증

모의 연습 (0.5 주)

전반적인 침해 사고 대응 프로세스를 평가하기 위해 기술 및 경영진 이해관계자와 함께 진행하는 토론 중심의 모의 연습 (최대 2 회 연습)

시뮬레이션을 통한 위협 탐지 제어 테스트 (1 주)

위협 탐지 제어의 효과를 평가하기 위해 안전하고 통제된 방식으로 네트워크에서 실행하는 시뮬레이션된 공격

보고 및 설명 (2 주)

조직의 사이버 방어 역량을 개선하기 위한 우선 순위가 지정된 전술적 권고 사항 및 전략적 권고 사항 , 실행 가능한 로드맵을 자세히 설명하는 보고서

제공되는 결과물

평가 후 Mandiant 컨설턴트는 다음과 같은 보고서를 제공합니다.

- 조직의 현재 사이버 방어 역량 평가
- 사이버 방어 역량을 확보하거나 강화할 때 고려해야 할 자세한 권고 사항
- 기술 브리핑
- 개선을 위한 실행 가능한 권장 이니셔티브 로드맵(2단계 및 3단계)
- 임원 브리핑(2단계 및 3단계)

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.