FIREEYE™

데이터 시트

RTO(레드팀 활동)

실제 표적 공격으로부터 가장 중요한 자산을 보호하는 역량 테스트

이점

- 중요한 데이터가 위험에 처해 있는지 여부와 악성 공격자가 그러한 데이터를 얼마나 쉽게 입수할 수 있는지 확인
- 현실적이고 "전면적인" 공격자에 대해 환경을 방어하는 보안 평가
- 현실적이고 통제된 환경에서 침해 사고를 방지 및 탐지하고 이에 대응하는 내부 보안 팀의 역량 테스트
- 복잡한 보안 취약점을 공격자가 악용하기 전에 식별 및 완화
- 사실 기반의 위험 분석 및 보안 환경 개선을 위한 권장 사항 확보

Mandiant를 선택하는 이유

FireEye의 계열사인 Mandiant는 2004년부터 사이버 보안 및 사이버 위협 인텔리전스의 최전선에 있었습니다. 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.

서비스 요약

레드팀 활동 참여는 고객의 환경에서 "모든 수단을 동원한" 현실적인 공격 시나리오로 구성됩니다. Mandiant 레드팀은 공격자의 행동을 시뮬레이션하는 동시에 고객과 공동으로 합의한 일련의 임무 목표를 달성하는 데 필요한 방법(운영 환경에 피해를 주지 않는)을 사용합니다. 레드팀은 최근의 실제 사고 대응 교전 시 나타난 TTP를 사용하여 실제 공격자의 적극적이고 은밀한 공격 방법을 거의 유사하게 모방합니다. 이를 통해 고객의 보안 팀이 적극적인 공격자 시나리오를 탐지하고 이에 대응할 수 있는지 평가합니다.

공격 목표 예시		
임원 또는 개발자의 이메일 유출	민감한 비즈니스 데이터가 들어있는 망분리 환경 침투	사물 인터넷(IoT) 장치, 의료 장치 또는 제조 장치와 같은 자동화된 장치 제어

방법론

레드팀 활동은 레드팀이 고객의 환경에 대해 어느 정도 알고 수행할지 또는 전혀 모르는 상태에서 수행할지를 공동으로 결정함으로써 시작됩니다. Mandiant는 업계의 경험을 살려 고객의 핵심 비즈니스 기능에 대한 주요 위험을 나타내는 목표를 파악합니다.

레드팀 활동 참여는 공격 라이프사이클의 단계를 따릅니다.

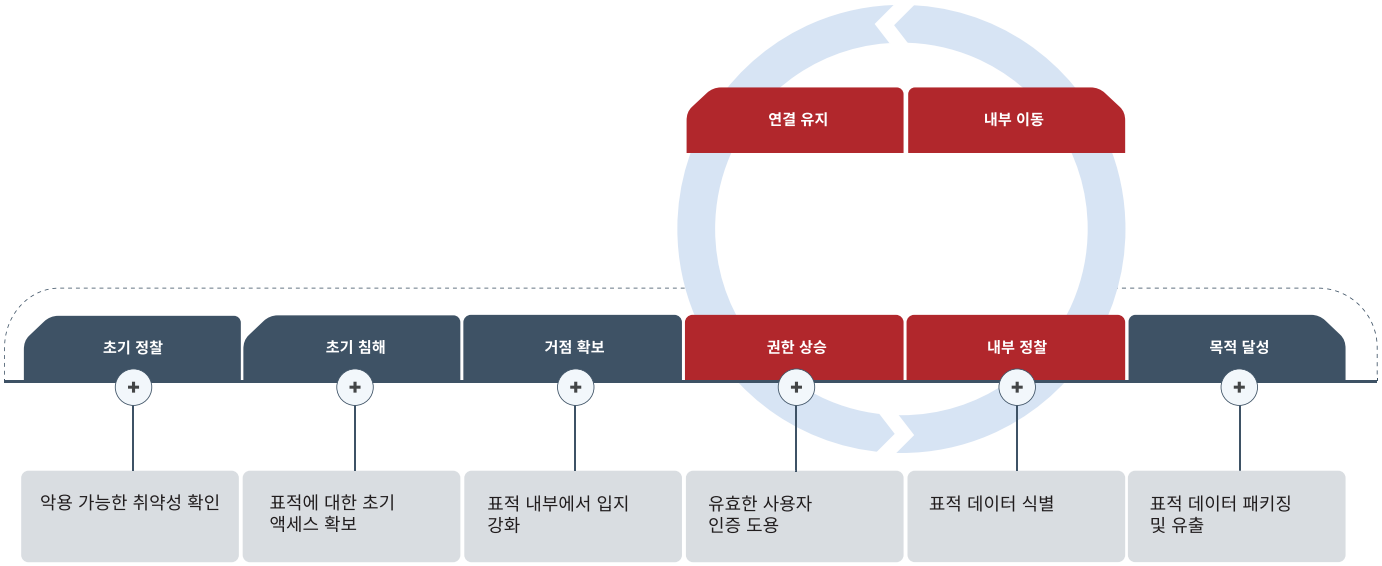

그림 1. 공격 라이프사이클.

목표가 설정되면 레드팀은 초기 정찰을 수행함으로써 활동을 시작합니다. Mandiant는 독점적 인텔리전스 리포지토리와 오픈 소스 인텔리전스(OSINT) 툴 및 기법의 조합을 활용하여 표적 환경에 대한 정찰을 수행합니다.

Mandiant는 취약성을 악용하거나 소셜 엔지니어링 공격을 수행하여 표적 환경에 대한 초기 액세스 확보를 시도합니다. Mandiant는 실제 공격자가 사용한 기법을 활용하여 이러한 시스템에 대한 액세스 권한을 확보합니다.

액세스 권한을 확보하면 레드팀은 공격자와 마찬가지로 명령 및 제어 인프라를 배포함으로써 환경 내에서 지속성을 설정 및 유지하기 위해 권한을 상승시키려고 시도합니다.

레드팀은 환경 내에 지속성을 설정하고 명령 및 제어 시스템을 구축한 후 비즈니스 중단이 초래되지 않는 한에서, 필요한 모든 수단을 통해 목표를 달성하려고 시도합니다.

레드팀 활동을 선택해야 하는 이유

레드팀 활동은 다음을 하려는 조직에 권장됩니다.

- *탐지 및 대응 역량 테스트*. 보안 팀은 실제 사고에 대비하고 있어야 합니다. 따라서 실질적 위험 없이 보안 팀이 제대로 대응할 수 있는지 확인해야 합니다.
- *인식 제고 및 영향력 확인*. Mandiant 레드팀은 실제 공격자처럼 행동하며, 인터넷에서 구할 수 있는 정보만 사용하여 인터넷에서 고객 환경을 침해하려고 합니다. 성공적인 레드팀 활동 참여를 통해 보안 예산 증가의 타당성을 증명하고 추가 투자가 필요한 격차를 확인할 수 있습니다.

고객이 받는 혜택

- 임원 및 고위 경영진을 위한 요약
- 조사 결과를 재현할 수 있도록 단계별 정보가 포함된 기술 세부 정보
- 사실 기반의 분석이므로, 중요한 조사 결과가 특정한 환경과 관련이 있다는 것을 인식
- 즉각적인 개선을 위한 전술적 권고 사항
- 장기적인 개선을 위한 전략적 권고 사항
- 실제 침해 사고에 준하는 시뮬레이션을 통해 사고에 대응해볼 수 있는 귀중한 경험

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™