MANDIANT®

Security Validation

운영 중인 사이버 보안의 효과성 검증

CISO는 보안 효과성을 항상 입증해야 합니다.
사이버 리스크에 대한 대비를 갖춰야 하는 최근 비즈니스 환경으로 인해, CISO와 보안 담당자들은 기업 자산에 대한 보안 유지와 재무 상태뿐 아니라 기업 평판을 보호하는 데 과거 대비 훨씬 큰 압박을 받고 있습니다. 이들은 사이버 보안 투자의 가치와 기업의 주요 시스템을 향한 공격을 차단함으로써 임원진에게 운영 중인 보안 프로그램의 효과성을 증명해야만 합니다.

하지만 보안의 효과성을 검증하고, 리스크를 정량화된 상태로 확인하거나, 전반적인 보안 시스템의 역량을 검증해서 보여줄 수 있는 확실한 방법이 부재하여 취약성 스캐너, 침투 테스트, 레드팀 또는 침해 및 공격 시뮬레이션에 의존하고 있습니다. 이러한 접근 방식은 충분히 검증해 내는 데 한계가 있어 효과성을 충분히 평가하지 못하며 조직을 표적으로 한 우선순위가 높은 특정 보안 위협에 대해 충분한 인사이트를 제공하지도 못합니다.

이는 Mandiant만의 기술로 만들어진 성능 측정 모듈을 포함한 지속적이면서도 자동화된 인텔리전스 기반 포트폴리오인 Mandiant Security Validation과 Mandiant Security Instrumentation Platform으로 해결할 수 있습니다.[1]

보안 효과성을 확인하고 운영 중인 사이버 보안 프로그램을 정량화된 정보를 기반으로 검증할 수 있어야 합니다.
보안성 검증을 효과적으로 하기 위해서 진행 테스트들의 우선순위를 결정하고 해당 조직이나 관련 산업을 표적할 수 있는 공격자와 공격 기술에 대한 정보를 기반으로 방어 체계를 최적화하는 방안에 대한 인사이트를 도출하기 위해 5단계로 구성된 방법론으로 진행됩니다.

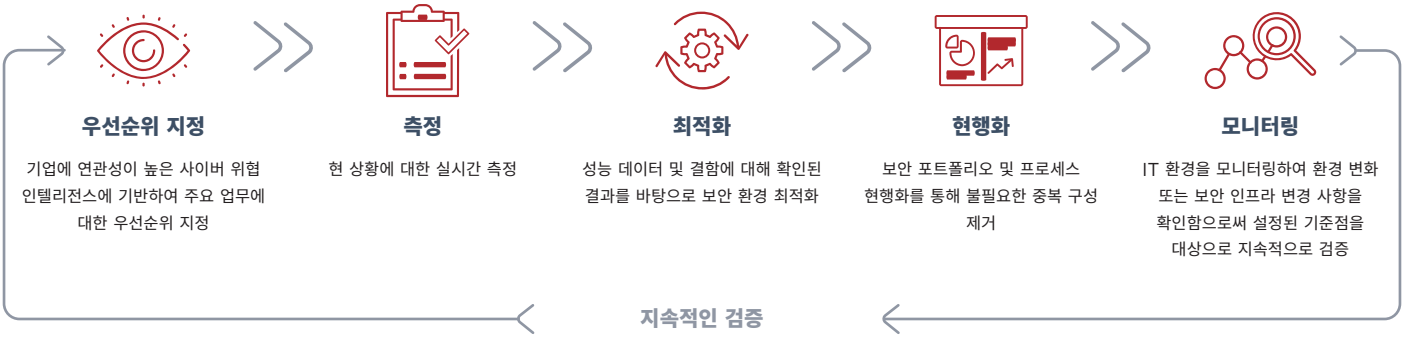

그림 1. Mandiant의 인텔리전스 기반 5단계 검증 방법론

1 이전 Verodin Security Instrumentation Platform

이 방법을 사용하려면 실시간으로 위협 데이터를 활용할 수 있어야 합니다. Mandiant Security Validation은 Mandiant 위협 인텔리전스와 침해 사고 대응 데이터를 사용하여 공격자들의 현재 활동 전반에 대한 가시성을 제공합니다. 인텔리전스 기반의 보안성 검증은 높은 우선순위의 위협을 확인할 수 있고, 조직에 위협이 되는 공격자와 공격 기술에 대한 정보를 기반으로 보안성 검증 계획을 수립할 수 있습니다. 보안 담당자들은 Mandiant를 통해 기술, 프로세스 및 인력 전반에 걸쳐 보안 컨트롤에 대해 완벽하면서도 지속적인 검증을 수행할 수 있습니다.

Mandiant Security Validation은 자체 보안 성능 검증 기술인 Security Instrumentation Platform을 사용하여 보안 컨트롤을 대상으로 실제 공격을 실행함으로써 보안 프로그램의 효과성을 파악하고 고도화된 공격에 대한 방어 능력을 신속하게 정량화하고 증명할 수 있게 합니다.

Mandiant Security Instrumentation Platform의 기본 기능은 다음과 같습니다.

- 주요 위협과 공격 방어 업무에 대한 우선순위 지정
- 실제 공격에 대한 보안 컨트롤의 성능 측정
- Mandiant 위협 인텔리전스 및 침해 사고 대응 데이터를 기반으로 검증을 위해 기업에 위협이 되는 공격을 안전하게 실행
- 조직의 보안 인프라에서 탐지되지 않은 결함 확인
- 최적화 구성을 위해 개선 요소 파악
- 시간 경과에 따라 개선되는 방어 시스템을 정량 데이터로 확인
- 정량화된 정보로 임원진에게 보안 투자에 대한 가치 증명

Mandiant Security Implementation Platform의 고급 기능은 다음과 같습니다.

- **Threat Actor Assurance Module:** 실행 가능한 위협 인텔리전스로 조직을 표적으로 삼을 가능성이 가장 높은 실제 공격자들에 대해 보안 성능에 대한 테스트 진행 TAAM은 업계 최고의 외부 인텔리전스 피드와 연동
- **Advanced Environmental Drift Analysis:** IT 인프라를 지속적으로 모니터링하여 환경 변화(environmental drift)를 제거하고 보안 시스템의 회귀(defensive regression)에 대한 지속적인 검증을 시행하여 조직의 보안 인프라에 대한 안정성을 보장
- **Protected Theater:** 멀웨어, 랜섬웨어 및 기타 파괴적인 공격을 안전하게 실행함으로써 최신 위협에 대해 선제적으로 방어하면서 엔드포인트의 제어 효과를 검증
- **Email Theater:** 이메일 보안 플랫폼에서 제공되는 보안 성능 테스트 진행

Mandiant Security Validation 포트폴리오에는 다음과 같은 여러 설치 옵션이 포함됩니다.

- **자체 관리형:** 클라우드 기반 서비스형(SaaS) 보안 또는 온프레미스에 가상 어플라이언스 형태로 배포
- **완전 관리형 및 공동 관리형 모델:** 비즈니스 요구사항에 따라, Mandiant 팀은 특정 케이스에 맞춰 검증 프로그램을 구축하여, 지속적으로 조직의 이해관계자에게 세부 보고서 제공
- **주문형 검증:** 하나의 케이스만 구매하여 일회성으로 사전 정의된 공격을 차단하는 성능을 평가하여 방어 체계를 강화하고 위험 노출도를 줄이기 위해 추가적인 조사가 이루어져야 할 부분에 대한 권고사항 제시

그림 2.

현재 운영 중인 보안 플랫폼이 기업의 주요 자산을 안전하게 보호하고 있다는 검증 결과를 시각화해서 볼 수 있게 합니다.

보안성 검증의 이점

보안 효과성을 측정하고 보안 투자에 대한 ROI를 높일 수 있습니다.
우선순위가 지정된 공격 유형에 대한 보안성을 높이고 전반적인 리스크 요소들을 정량 데이터화해서 확인함으로써 투자가 필요한 부분을 정확히 판단하여 결정할 수 있습니다. 또한 보안 담당자들은 이러한 데이터를 사용하여 임원진과 이사진들을 대상으로 보안 투자의 가치를 설득할 수 있습니다.

인수 합병
인수 합병을 진행하고 있는 기업들은 보안 기능들이 중복 구성되어 있거나 결함이 있는 부분을 파악해 볼 수 있습니다. 지출 구조를 합리화함으로써 통합 가능한 비용과 합병 이후의 리스크 범위를 산정할 수 있습니다.

보안 인재 채용 및 교육
보안 전문가의 경력과 학습 잠재력, 그리고 이들이 보유하고 있는 업무 경력의 유형을 포함해 이들의 기술이 실제 시나리오에서 조직 구성에 얼마나 적절하게 배치되어 있는지를 평가할 수 있습니다. IT 리더들은 실제 조직의 환경 전반에 공격 시나리오를 안전하게 실행하여 채용 지원자들이 답변하고 대응하는 방식을 모니터링할 수 있습니다. 또한 IT리더들도 가장 최신의 공격 시나리오를 통한 보안팀의 공격 대응 활동 확인 및 수용 가능한 수준의 대응 시간, 기술적 보완 사항 등에 대한 정기적인 평가를 수행할 수 있습니다.

기업 평판 보호
보안 효과성을 선제적이고 지속적으로 측정하여 침해 및 공격의 리스크를 줄이고 기업 평판과 고객 충성도를 유지할 수 있습니다.

데이터 프라이버시 및 보호
고객 데이터를 보호하고 기업과 외부 기관에서 규제하는 컴플라이언스 준수를 보장합니다.

Mandiant Threat Intelligence에서 얻은 정보를 통한 보안 검증

Mandiant는 15년 이상 침해 조사, 사고 컨설팅을 진행하고 전 세계 레드팀 활동을 통해 확인되는 새로운 정보 및 전문 인력 확보와 고유의 분석 기술로 지속적으로 업데이트되는 위협 인텔리전스 포트폴리오 관리하고 있습니다. Mandiant는 다음 사항들을 통해 현재 사이버 위협 인텔리전스 분야를 주도하고 있습니다.

- **Mandiant 컨설팅 침해 사고 대응 활동을 통해** 수집된 침해 인텔리전스
- **Mandiant 연구원들이** 확보한 공격자 인텔리전스
- **FireEye 보안 제품을 통한** 머신 인텔리전스
- **Mandiant Managed Defense 서비스에서** 추출된 운영 인텔리전스

Mandiant 솔루션에 대한 자세한 내용은 **www.FireEye.com/validation**를 참조하십시오.

FireEye Korea
서울특별시 강남구 테헤란로 507 WeWork 빌딩
12층 112호
02-6959-4017
korea.info@fireeye.com

Mandiant 솔루션 소개
Mandiant 솔루션은 세계 최고의 Threat Intelligence와 최일선에서 수집된 전문 지식을 지속적인 보안 검증 기능과 통합하여, 조직이 보안 효과성을 높이고 비즈니스 위험을 줄이는 데 필요한 툴을 제공합니다.