FIREEYE™

데이터시트

ThreatSpace

실제 피해 없이 실제 위협에 대응하는 방법 연습

이점

- **결점 및 개선 기회 식별:** 실제의 복잡한 사고를 조사하여 교육, 프로세스, 절차 및 커뮤니케이션 계획의 결점을 식별합니다.
- **침해 사고 대응 전문가의 코칭:** 풍부한 경험과 수년 간의 인텔리전스 기반 조사 전문 지식을 갖춘 Mandiant 침해 사고 대응 담당자가 긴밀하게 연계하여 실시간 피드백 및 코칭을 제공합니다.
- **중요 보안 사고 조사:** 조직의 대응 및 인텔리전스 팀이 Mandiant의 지능형 지속 공격(Advanced Persistent Threat, APT) 조사에서 조직과 관련된 최신 공격 시나리오 및 공격자 TTP를 배우고 이러한 내용을 숙지할 수 있도록 합니다.
- **다양한 공격 시나리오 및 위협 공격자를 통한 경험 습득:** 침해 사고 대응 및 인텔리전스 팀이 다양한 공격 시나리오와 공격자에 대응하는 과정에서 팀의 능력을 평가하고 개선합니다.
- **식별된 위협 조사 및 분석:** 공격자의 TTP를 조사하는 방법과 호스트 기반 및 네트워크 기반 아티팩트에서 침해 지표를 식별하는 방법을 학습합니다.

ThreatSpace는 기술에 기반을 둔 서비스로, 조직의 보안 팀은 이 서비스를 사용하여 피해 없는 환경에서 실제 위협에 대응하는 팀의 능력을 평가하고 개발할 수 있습니다. 조직의 보안 팀은 일반적인 IT 인프라(예: 네트워크 세그먼트, 워크스테이션, 서버 및 애플리케이션)를 시뮬레이션하는 가상 환경에서 ThreatSpace를 사용하여 시뮬레이션 공격 시나리오를 조사하면서 팀의 기술적 기능, 프로세스 및 절차를 평가하게 됩니다.

Mandiant가 수천 건의 침해에 대응하면서 쌓은 폭넓은 침해 사고 대응 경험을 기반으로 만든 이러한 공격 시나리오는 공격자의 최신 전술, 기술 및 절차(Tactics, Techniques and Procedures, TTP)를 포함하며 표적 공격에 대한 조직의 탐지, 범위 파악 및 복구 능력을 테스트하는 데 사용됩니다. 프로세스를 진행하는 동안 Mandiant 침해 사고 대응 전문가가 보안 팀의 사이버 공격 대응 능력을 개선하는 데 필요한 실시간 피드백 및 코칭을 제공합니다.

Mandiant는 기술에 관계없이 분석 결과에 기반을 둔 테스트 접근 방식을 사용하며, 시스템 및 포렌식 아티팩트를 식별하고 그 우선 순위를 결정하는 보안 팀의 능력을 테스트하는 과정에서 다음과 같은 항목을 분석합니다.

영향을 받은 시스템, 네트워크, 사용자 계정 및 애플리케이션

악성 소프트웨어 및 악용된 취약성

액세스된 정보 및/또는 유출된 정보

ThreatSpace 시나리오는 표적 공격 수명주기의 모든 단계를 포함합니다.

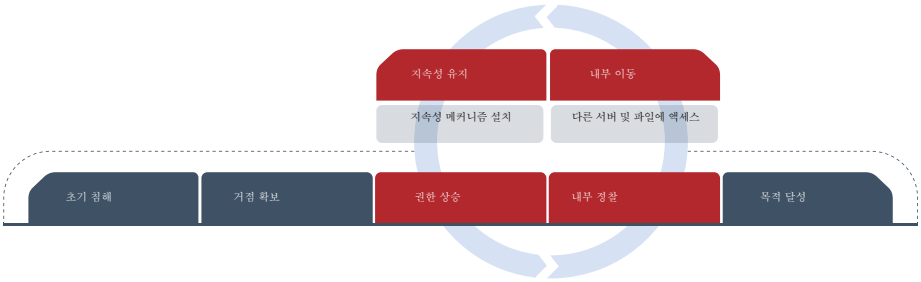

그림 1. 공격 라이프사이클

서비스 제공
원격 준비

시나리오 **식별**

목표, 예상 및 실행 계획 **검토**

침해 사고 대응 프로세스 및 절차 **논의**

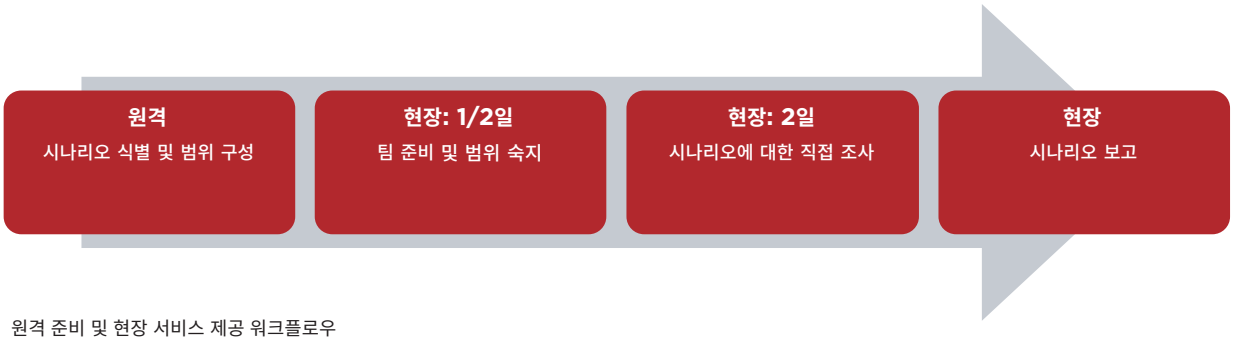

그림 2. 원격 준비 및 현장 서비스 제공 워크플로우

현장 시나리오

- 반일간 교육을 받고 범위를 숙지합니다.
- 공격 수명주기의 단계를 거쳐 진행되는 시뮬레이션 공격을 2일간 직접 조사합니다. 시나리오를 진행하는 동안 Mandiant 사고 대응 담당자가 조직의 사고 대응 담당자 및 사이버 위협 분석가에게 실시간 피드백 및 코칭을 제공합니다.
- 팀의 성과 및 강점과 교육, 프로세스 및 절차의 측면에서 팀의 결점을 검토하고 개선을 위한 권장 사항을 함께 보고합니다.

제공되는 결과물

작업이 완료된 후에는 조직의 침해 사고 대응 능력에 대해 관찰된 강점과 개선점이 표시된 보고서를 받게 됩니다.

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 솔루션을 제공합니다. FireEye는 혁신적인 보안 기술, 최고의 Threat Intelligence 및 세계적으로 인정받는 Mandiant® 컨설팅을 결합한 단일 플랫폼을 제공하여 고객 보안 운영 플랫폼을 완벽하게 확장하여 보안을 강화시킵니다. 이를 통해 FireEye는 사이버 위협에 대비하고 공격 방어 및 대응하는 조직의 사이버 보안 부담을 줄이고 보안 운영의 복잡성을 간소화합니다.

M-EXT-DS-US-EN-000007-03