FIREEYE™

솔루션 요약

위협 인텔리전스 사용 사례 시리즈

침해사고 대응자

침해사고 대응팀이 직면한 문제

침해사고 대응자들은 사이버 공격을 최일선에서 방어합니다. 보안 침해가 의심되는 사례를 조사하고, 지능형 공격을 포착하여 리버스 엔지니어링하며, 포렌식을 수행하고, 피해를 복구하는 역할을 맡습니다. 일반적으로 침해사고 대응(IR) 팀원은 숙련된 보안 분석가들이며, 레벨 2 및/또는 레벨 3 SOC 분석가로서 보안 운영 센터(SOC) 그룹의 일원으로 활동할 수 있습니다.

침해사고 대응자가 직면한 문제:

- 실제 위협이 될 만한 침해사고를 검증하고 위험 수준에 따라 침해사고의 우선순위를 정하는 요구 사항을 시급하게 해결해야 합니다.
- 침해사고와 특정 공격자 및 공격 캠페인과의 상관관계를 밝히기가 어렵습니다.
- 지능형 공격과 위협 범죄자들의 TTP에 대한 세부 정보를 알아내기 위해 위협 데이터베이스와 기술 자료를 검색하는 번거로운 작업을 수행해야 합니다.
- 경영진이 이해하고 조치를 취할 수 있도록 보안 문제를 비즈니스 용어로 바꾸는 것이 쉽지 않습니다.

한 설문조사에서 기업들은 잘못된 경보에 대응하는 데 연평균 127만 달러를 지출한다고 밝혔습니다.

침해사고 대응자가 사이버 위협 인텔리전스를 이용하는 방법

침해사고 대응자들은 사이버 위협 인텔리전스를 이용하여 심각한 위협의 탐지를 개선하고, 누가, 언제, 무엇을, 어떻게, 왜 공격하는지를 파악하며, 대응과 복구 속도를 높이고, 회사 네트워크에 숨어 있는 지능형 공격의 증거를 찾아냅니다.

표 1. 사용 사례—IR팀

사용 사례	주요 목표	필요한 인텔리전스
침해사고 검증 및 우선순위 지정	• 어떤 침해사고가 기업에 위험을 줄 수 있는지 파악하고 비즈니스에 부정적인 영향을 미칠 가능성이 가장 높은 사건의 우선순위 지정	• 요약 위협 데이터에 연결된 위협 지표
침해사고 분석	• 공격자, 대상, 이유, 시기 및 방법에 대한 질문에 답변 • 공격이 여전히 진행 중인지 확인하고 영향 파악	• 캠페인, 위협 범죄자 및 표적에 대한 정황 정보에 연결된 위협 지표 • 공격 기록 및 기법에 대한 자세한 정보를 제공하는 인텔리전스 지식 기반
억제 및 복구	• 공격자 커뮤니케이션 차단 • 악성코드 제거 및 변경 사항 되돌리기 • 취약점 제거	• 공격 기록 및 기법에 대한 자세한 정보를 제공하는 인텔리전스 지식 기반
추적 미션	• 현재의 침해사건이나 기업의 산업, 지리적 위치, 애플리케이션 등을 표적으로 하는 위협과 관련하여 이전에 발견되지 않은 공격 차단	• 캠페인, 위협 범죄자 및 표적에 대한 정황 정보에 연결된 위협 지표 • 공격 기록 및 기법에 대한 자세한 정보를 제공하는 인텔리전스 지식 기반

침해사고 검증 및 우선순위 지정: 잠재적 비즈니스 영향 평가

SOC 레벨 1 분석가가 침해사고를 IR팀으로 에스컬레이션하면 침해사고 대응자가 침해사고의 우선순위를 정하고 세부적인 조사가 필요한 사안을 결정해야 합니다. 사이버 위협 인텔리전스는 조직을 표적으로 삼는 공격자와 연관되었을 가능성이 높은 침해사고를 파악하고 비즈니스에 악영향을 미칠 가능성이 가장 높은 공격을 평가하는 데 도움을 줄 수 있습니다.

사이버 위협 인텔리전스는 공격 지표를 위협 범죄자, 동기(금전, 경쟁 및 이념), 표적 및 이전 공격의 피해와 같은 정황 정보와 연결하는 위협 데이터를 제공하여 프로세스를 가속화할 수 있습니다. 이 요약 위협 데이터는 침해사고 대응자가 다른 유형의 기업(또는 소비자)을 대상으로 하는 침해사고를 우선순위에 두지 않고, 중요한 비즈니스 프로세스나 귀중한 정보 자산을 실제로 위협하는 공격을 위해 부족한 침해사고 분석 리소스를 남겨 둘 수 있도록 지원합니다.

침해사고 분석: 리버스 엔지니어 공격

침해사고 대응자는 초기 사건에서 관심을 돌려 공격이 여전히 진행 중인지 확인하고, 시스템 및 애플리케이션의 변경 사항을 정확히 파악하고, 도난 데이터 및 운영 중단 측면에서 발생할 수 있는 손상을 식별해야 합니다. 사이버 위협 인텔리전스는 공격을 완벽하게 파악할 수 있는 질문(누가, 언제, 무엇을, 어떻게, 왜)에 답변하는 데 도움이 됩니다.

IR팀은 사이버 위협 인텔리전스를 통해 경보 및 지표를 관련 이벤트 및 아티팩트와 연결할 수 있습니다. 예를 들어 악성코드 샘플이 탐지된 경우 해당 샘플에 연결된 것으로 알려진 IP 주소가 없는지 파악합니다. 위협 인텔리전스는 악성코드가 실제로 사이버 범죄 조직이 명령 및 제어 서버로 사용하는 IP 주소에 연결되었음을 보여줄 수 있습니다. 그런 다음 침해사고 대응자는 네트워크 로그를 확인하여 이 서버와 통신하여 침해될 가능성이 있는 다른 기업 시스템을 찾을 수 있습니다.

보안 위협 인텔리전스의 저장소가 지식 기반에 유지되는 경우, 침해사고 대응자는 해당 지식 기반을 사용하여 공격자의 ID와 기법, 대상, TTP 및 표적 기업에 미치는 영향에 대한 자세한 정보를 찾을 수 있습니다. 그 정보는 IR팀에게 누가 공격을 하고 있는지, 무엇을 했는지, 어떻게 했는지, 그리고 공격이 아직 진행 중인지에 대한 증거를 어디서 찾아야 하는지 알려줍니다.

억제 및 복구: 피해 차단 및 취약점 제거

침해사고 대응자는 다른 IT 그룹이 공격을 억제하고 피해를 복구할 수 있도록 이들에게 정보를 제공해야 합니다.

위협 인텔리전스 지식 기반은 침해사고와 관련된 공격자의 동기, 기법 및 인프라에 대한 정보를 제공합니다. 이렇게 하면 외부 명령 및 제어 서버와의 통신을 중단하거나 피싱 공격으로 침해된 인증 정보를 사용하지 않도록 설정하여 진행 중인 공격을 차단할 수 있습니다.

특정 공격자가 시스템을 대상으로 하는 방법과 사용하는 악성코드의 동작에 대한 정보를 통해 IT 그룹은 감염된 시스템을 식별하고, 악성코드를 제거하고, 레지스트리 및 파일에 대한 변경 사항을 역순으로 적용하며, 취약점을 제거하여 공격이 반복되지 않도록 할 수 있습니다.

추적 미션: 숨겨진 공격을 사전에 포착

오늘날 대부분의 기업은 일부 공격이 보호 및 탐지 시스템에 침투하여 네트워크에 인식되지 않고 상주할 것으로 가정합니다. 추적 미션은 이러한 공격을 사전에 밝혀내기 위한 노력입니다.

사후 대응적 추전 미션은 사이버 위협 인텔리전스를 사용하여 현재 침해사고와 관련된 발견되지 않은 공격을 찾아냅니다. 예를 들어, 최근 발생한 침해사고에 피싱 캠페인이 포함된 경우, 위협 인텔리전스에서 이 캠페인이 다른 피싱 캠페인 및 '워터링 홀' 공격의 일종을 사용하는 특정 공격자에 의해서도 사용된다는 것을 보여줄 수 있습니다. 두 종류 이상의 공격을 사용할 가능성이 큰 만큼, 추적팀은 다른 피싱 캠페인과 공격자의 '워터링홀' 웹사이트를 방문한 직원들의 증거를 추적할 수 있습니다.

사전 예방적 추적 미션은 특정 산업 또는 특정 시스템의 일부 조직을 대상으로 하는 것으로 알려진 공격자들이 동일한 산업 또는 동일한 시스템으로 다른 조직도 표적으로 할 가능성이 높다는 전제에서 시작됩니다. 위협 인텔리전스, 특히 포괄적인 인텔리전스 리포지토리는 가장 위협적인 범죄자들에 대한 정확하고 상세한 정보 출처와 기업 네트워크에서 이들의 존재에 대한 증거를 찾을 수 있는 장소를 추적팀에 제공합니다.

FireEye 위협 인텔리전스가 침해사고 대응자에게 유용한 이유

- 포괄적인 인텔리전스를 시장에서 사용할 수 있습니다. 고도로 검증된 인텔리전스 및 관련 지표
  - 공격자, 캠페인, TTP에 대한 풍부한 정황 정보
  - 범죄에서 스파이, 해킹에 이르기까지 광범위한 공격자 파악 범위
  - 글로벌 소싱 및 분석
  - 8년간의 기록 데이터베이스
- 고객의 툴 및 프로세스의 통합을 지원하는 강력한 API
- 주요 침해사고 대응 툴과의 파트너 통합
  - 분석: Splunk, BAE, Palantir, Maltego
  - 엔드포인트: Tripwire, Ziften
  - TIP: ThreatConnect, Anomali, ThreatQuotient
  - IR: Resilient Systems 등

이점

FireEye의 신뢰할 수 있고 실행 가능하며 컨텍스트가 풍부한 인텔리전스를 통해 침해사고 대응자는 다음을 이행하기 위해 신속하고 정보에 입각한 의사결정을 내릴 수 있습니다.

- 즉시 조사해야 하는 이벤트를 식별합니다.
- 공격 원인과 대상을 신속하게 파악하기 위해 격리된 지표를 위협 범죄자 및 캠페인과 연결합니다.
- 보다 정확하고 완벽하게 심층 조사를 수행하고 공격자, 대상, 이유, 시기 및 방법에 대한 질문에 답변합니다.
- 더욱 빨리 공격을 차단하여 비즈니스에 미치는 영향을 줄입니다.
- 나중에 동일한 유형의 사건이 반복되지 않도록 방지합니다.
- 네트워크에서 탐지되지 않은 공격을 검색하기 위해 추적 미션을 수행합니다.

FireEye에 대한 자세한 정보: **www.FireEye.com**

FireEye Korea
서울특별시 강남구 테헤란로 534 글라스타워 20층
02.2092.6580/
korea.info@fireeye.com/
www.fireeye.kr

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™