McAfee Investigator

분석가를 전문 조사자로

McAfee® Investigator는 분석가가 근본적인 원인을 파악했다는 확신을 갖고 더 많은 사례를 더욱 빨리 종결할 수 있도록 돕습니다. 경보 분류는 보조 데이터를 축적하고 증거를 해석하며 완벽하고 빠르게 위험을 입증하고 반응할 수 있도록 인사이트를 제공하는 전문가에 의한 취약점 탐색을 촉발합니다.

보안 운영 과제

막대한 이벤트 볼륨 및 데이터 보존 기간 문제로 인해 경보의 중요성과 범위를 정확히 평가하기가 어렵습니다. 분석가들은 대개 공식적인 사고로 취급해야 하는지 결정하기 위한 컨텍스트나 지식이 부족하기 때문에 경보를 무시하는 경향이 있습니다.

선별적 사고를 조사하는 경우 문제의 핵심을 조사하기 위해서는 위협 벡터 전반에 걸쳐 오랜 시간과 상당한 전문 기술이 필요할 수 있습니다. 이러한 경향에 따라 숙련된 보안 운영 분석가의 필요성이 커지는 반면 사용 가능한 인재 풀은 그렇지 못한 실정입니다.

새로운 조사 분석

이런 문제를 해결하기 위해 보안 운영팀은 경보 분류 및 조사를 간소화하고 빠르게 하여 기존 인력과 주니어 분석가들이 더 많은 일을 할 수 있도록 해야 합니다.

McAfee Investigator는 모든 보안 운영팀이 접근 할 수 있는 분류, 포괄적 데이터 수집 및 고급 분석을 포함한 안내식 조사를 제공합니다. SaaS 제공 항목인 전문가 시스템 및 엔드포인트 캡처 도구는 기존 데이터 소스 및 보안 관리 시스템과 통합되어 최소한의 노력으로 가치 달성 시간을 단축시킵니다.

이러한 대화형 분석은 지속적으로 업데이트되는 지침을 제공하여 사고 대응자가 보다 신속하고 정확하게 악성 프로그램, 네트워크 위협 및 IoC를 더 짧은 시간 안에 더욱 정확하게 조사할 수 있게 해줍니다.

기계 속도로 인사이트 검색

McAfee Investigator는 보안 운영에서 즉각적인 주의가 필요한 특정 상황에 대한 우선순위 분류를 자동화할 수 있게 함으로써 분류 능력을 즉각적으로 개선합니다. 이러한 경고는 물론 분석가가 알아보고자 하는 기타 경보에 대해 McAfee Investigator는 의심스러운 공격과 관련하여 수집된 경보, 활동, 증거 및 인텔리전스를 수집, 정리, 요약 및 시각화합니다.

주요 혜택

- **체류 시간 단축:** 사례 데이터를 철저히 탐색하면 증상을 해결하기보다는 근본 원인을 파악할 수 있습니다.
- **경보에서 사례로 이동:** 우선순위가 낮은 수동 조사 항목에 소비되는 시간을 줄입니다.
- **알 수 없는 사항에 집중:** 사용자의 해석과 결정이 요구되는 고유한 아티팩트와 인사이트에 집중하십시오.
- **분류 능력 향상:** 높은 성능으로 더 많은 사례를 보다 빠르고 정확하게 처리하십시오.
- **분석가의 피로 완화:** 한정된 시간, 에너지 및 인지 능력을 최대한 활용하십시오.
- **분석가 기술 개발:** 가이드북과 관련 인사이트는 분석가에게 워크플로 내에서 올바른 질문과 가설에 대해 알려줍니다.
- **현재 시스템의 가치 확대:** 집중도와 정확성을 높일 수 있도록 기존 데이터 소스 및 분석이 향상되었습니다.

관련 데이터는 백그라운드에서 수집되며 결정을 트리거하는 특정 위협 조사에 중요한 인사이트만 포함합니다. 보안 정보 및 이벤트 관리(SIEM) 솔루션의 데이터는 각 노드에 엔드포인트 탐지 및 대응(EDR) 에이전트가 없어도 엔드포인트의 데이터로 보강될 수 있습니다. 이 모델은 IoC, 전술, 기술, 절차 및 관계에 대한 컨텍스트 가시성으로 사일로를 대체합니다.

데이터 분석 및 기계 학습 엔진은 증거 데이터를 알려진 기준 및 위협 인텔리전스 소스와 비교합니다. 아티팩트를 처리하고 의심스러운 주요 인사이트를 승격시킵니다.

McAfee Investigator는 적절한 데이터를 자동으로 수집하고 우선순위를 지정함으로써 분석가가 사고의 위험과 긴급성을 판단할 수 있는 노력을 최소화하고 속도를 높입니다. 분석가는 보다 빠르게 분류 결정을 내리고 보다 심각한 위협에 집중할 수 있습니다.

조직 수준에서는 이점이 배가됩니다. 경보 검토부터 상황별 사례에 이르는 분류의 수준을 높임으로써 각 분석가의 효율성을 향상할 수 있으며 계층 1 분석가가 더 많은 사례를 처리할 수 있습니다. 그뿐 아니라 분석가는 더 가치 있는 활동에 시간을 할애할 수 있습니다.

전문 지식을 통해 조사 안내

자세한 조사를 위해 사고를 선택하면 분석가는 대화형 가이드북을 활용하여 범위를 정하고 평가하는 과정에서 중요한 사안에 집중할 수 있습니다. 조사 가이드북은 스크립트를 기반으로 하는 정적 지침서가 아닙니다. 시스템은 인간의 두뇌를 모방하며 속도와 정확도를 극대화하기 위해 여러 가정을 동시에 살펴봅니다.

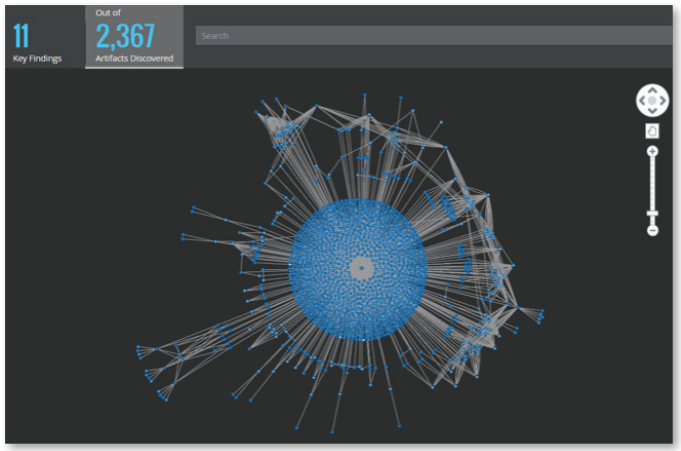

그림 1. McAfee Investigator는 수천 가지의 증거를 수집합니다.

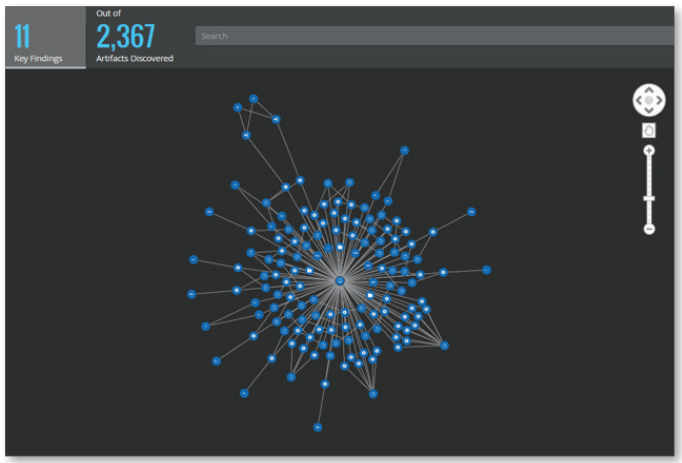

그림 2. 그런 다음 McAfee Investigator는 전문가 분석 및 지침을 적용하여 중요한 발견 결과를 제시합니다.

주요 기능

- 정확한 주문형 데이터 수집
- 일시적인 엔드포인트 수집 에이전트
- 전문가 지침 및 인공지능을 바탕으로 수집된 데이터 해석
- 대화식 시각화
- 가능성 있는 데이터를 탐색하기 위한 멀티 벡터 가설
- 제도적 인텔리전스에 대한 기준
- 사례 관리를 통해 인력을 관리할 수 있으며 조사 내내 정보 공유를 할 수 있습니다

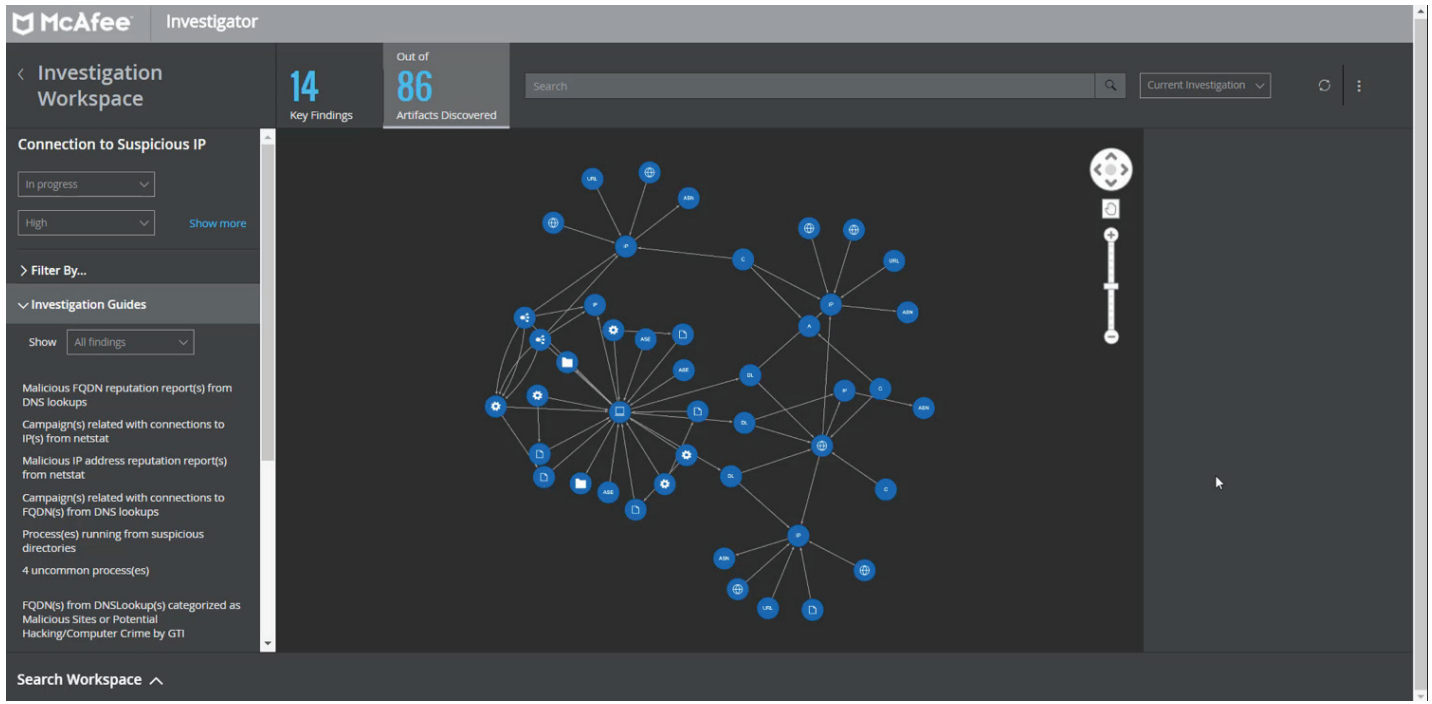

그림 3. 작업 공간을 통해 주요 발견 결과를 분명하고 쉽게 탐색할 수 있습니다.

사람이 읽을 수 있는 이 가이드북은 Foundstone® 연구원의 전문 기술과 인공지능의 조합으로 제작되었습니다. 이것이 바로 McAfee Investigator가 사용자-시스템 팀을 실현하는 한 가지 방법입니다.

작업 공간에서는 분석가가 올바른 질문을 제기할 수 있도록 사례 인사이트 및 발견 결과를 구성합니다. 이와 같이 집중적인 멀티 벡터 탐색으로 분석가는 근본 원인을 파악했다는 확신을 갖고 정확하고 효율적으로 사례를 종결할 수 있습니다.

전문 지식 및 역량 확장

McAfee Investigator의 대화형 작업공간은 단일 인식 환경에서의 워크플로 및 데이터 탐색을 촉진합니다. 이 모델은 효율성을 높이고 다양한 경보 유형으로 생성되는 과도한 정보의 양을 줄이고 여러 화면을 확인해야 할 필요성을 없애줍니다.

작업 공간에서는 초보 및 중급 분석가가 고급 분석가의 사고 프로세스를 구현할 수 있도록 지도하므로 별도의 교육 없이 기술을 연마할 수 있습니다.

기존 도구 및 데이터 기반 구축

McAfee Investigator는 SIEM 및 McAfee® ePolicy Orchestrator® 소프트웨어와 연동되어 기존 데이터 소스, 기준, 상관관계 및 경보에 고급 분석을 추가합니다. 일시적인 에이전트는 미묘한 증거의 정확한 해석에 특히 중요한 새로운 엔드포인트 데이터를 수집합니다. McAfee Investigator와 McAfee Active Responsed의 통합을 통해 분석가는 실시간으로 엔드포인트에 위험이 끼치는 영향을 자세히 살필수 있습니다. 활동 피드는 타사 도구와 데이터를 공유해 현재 워크플로에 접속하여 절차를 간소화하고 협력을 향상시킵니다. 전문 서비스는 온보딩 및 성공적인 활성화를 신속하게 처리합니다.

자세한 내용

McAfee Investigator를 사용하면 의심스러운 부분이 있는 경우 데이터를 수집하느라 몇 시간을 낭비할 필요가 없으며 데이터를 해석하느라 시간을 소비할 필요도 없습니다. McAfee Investigator의 고급 분석 엔진은 컨텍스트 중심 인터페이스에서 위협 경보를 조사 및 분류하여 보안 운영을 확장합니다. McAfee Investigator는 SOC 조사에서 전문 지식의 사용을 자동화함으로써 분석가가 더욱 뛰어난 정확성으로 보다 빠르고 현명하게 작업할 수 있게 해줍니다.

이것이 바로 사용자-시스템 팀입니다.

자세히 알아보려면 **www.mcafee.com/kr/products/investigator.aspx**를 방문하십시오.

McAfee 기술의 특징과 이점은 시스템 구성에 따라 다르며 사용하는 하드웨어, 소프트웨어 또는 서비스 활성화를 필요로 할 수 있습니다. www.mcafee.com/kr에서자세히 알아보십시오. 완벽히 안전한 컴퓨터 시스템은 없습니다.

비용 및 시간 절약 시나리오는 특정 McAfee 제품이 특정 상황 및 설정에서 미래 가격에 미치는 영향과 절약되는 비용 및 시간을 나타내기 위한 예시입니다. 상황 및 결과는 변할수 있습니다. McAfee는 어떠한 가격 또는 할인도 보장하지 않습니다.

McAfee (Singapore) Pte Ltd
10 Kallang Avenue #08-10
Aperia Tower 2
Singapore 339510
www.mcafee.com/kr