McAfee MVISION Insights

고객의 보안 태세를 동적으로 강화하여 공격자보다 앞서게 할 수 있는 최초의 엔드포인트 보안 기능.

사이버 위협의 진화와 속도는 조직에 지속적인 위협이자 스트레스 요소입니다. 기업은 보안 전문 지식이 부족한 상태로 보안 예산을 늘려 사이버 위협에 대응했지만 여전히 도구, 전술, 기술 등의 무기를 지속적으로 업데이트하고 있는 첨단 공격자를 따라잡지 못하고 있습니다. 현재 조직에서 선택한 옵션은 인적 개입 및 수동 개입이 필요한 분리 인텔리전스입니다. 이 방법으로 즉각적인 위협은 해결할 수도 있지만 사이버 공격의 수와 유형이 증가함에 따라 보안 팀은 거의 지속적인 대응 태세로 공격에 시달리고 있습니다. 위협 인텔리전스 플랫폼(TIP)은 대량의 위협 데이터 레이크를 제공할 수 있지만 수동 통합 및 분석 주기가 필요해 실행 가능성과 해결 능력이 제한됩니다. 취약성 관리는 기존의 취약성 및 그 심각도에 대한 조언을 제공할 수 있지만 보안 태세가 실질적으로 현재의 위협을 방어할 수 있는지에 관해 제한적인 위협 통찰력을 제공합니다.

솔루션은 예방적 조치를 강화하는 실시간 인텔리전스인 McAfee® MVISION Insights입니다. 인공 지능과 인간을 통해 정제되고 분석된 종합 인텔리전스는 어떤 위협과 캠페인이 본인의 조직을 표적으로 삼을 가능성이 가장 높은지에 대한 우선순위를 제공합니다. MVISION Insights는 위협이 전체 보안에 어떤 영향을 미칠지 정확히 예측하고 보안 태세를 최적화하기 위해 취해야 할 조치를 정확히 처방합니다.

주요 이점:

- **10억 개의 센서에서 수집된 위협 인텔리전스:** 신뢰할 수 있는 소스에서 경계 외부의 위협 프로젝트를 예방적으로 식별합니다. 산업 분야, 지리, 기업 엔드포인트 보안 태세에 따라 위협 프로젝트의 우선순위를 지정합니다.
- **공격 전에 위협 캠페인을 식별하고 단일 콘솔에서 위험 수준의 우선순위를 지정합니다.** 해결 권장 사항을 비롯해 위협과 엔드포인트 보안 태세가 이러한 위협에 대응하기에 얼마나 적절한지에 관해 실행 가능한 인텔리전스를 확보합니다.
- **탐지부터 해결까지의 평균 시간 단축:** 워크플로를 간소화해 추가적인 보호 조치를 더 빠르게 시행합니다. 실행 가능한 필수 변경 사항으로 현재의 엔드포인트 보안 태세를 평가하고 대응 시간을 몇 개월에서 몇 시간으로 단축합니다.

McAfee에 문의

더 예방적으로 대처하기 위한 보안 혁신

MVISION Insights는 McAfee® 관리 플랫폼 환경에 내장된 새로운 기능을 제공해 위험 및 위협 대응을 조직에 맞게 조정 및 간소화하여 더 적은 리소스를 사용하면서 방어를 위한 대응 조치를 선제적으로 개선하고 대응 시간을 단축할 수 있도록 지원합니다. 10억 개의 센서에서 수집된 위험 인텔리전스가 방어의 우선순위를 지정하는 데 필요한 통찰력으로 기업의 역량을 강화합니다. 단 하나의 콘솔에서 탐지, 해결, 선제 대응 시간 단축, 현저한 위험 감소를 실현할 수 있습니다.

사후 사이버 방어 전략은 사이버 방어 구성 요소의 핵심이지만 공격을 포착해 진압하는 데는 효과적이지 않습니다. 공격자는 차세대 도구를 사용해 기존의 방어책을 공격하도록 설계된 캠페인을 고안함으로써 사후 대응 보안 제품을 테스트해 어떤 기술이 공격을 뚫을 수 있는지 파악하고 있습니다. 조직은 공격 발생 전후의 전체 공격 수명 주기를 파악해야 합니다.

공격 수명 주기

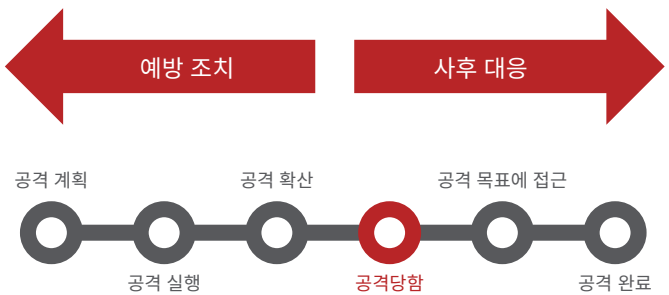

그림 1. 일반적인 공격 수명 주기

결국 인텔리전스와 실행 가능한 통찰력이 가장 발생 가능성이 큰 위협에 대해 가능한 한 최상의 사이버 보안 태세와 확신할 수 있는 방어력을 제공합니다. 다음은 McAfee MVISION Insights에서 이를 어떻게 달성하고 있는지 설명합니다.

- **파악할 수 없는 부분을 줄이고 상황 인식을 향상하도록 지원:** 위협이 발생하기 전에 방어가 얼마나 적절한지 정확히 파악합니다. MVISION Insights는 기업을 공격하리라 예측되는 국소적 및 전역적 위협을 예방적으로 추적해 우선순위를 지정합니다.
- **머신 러닝 분석:** 이 기능은 사용자가 특정 보안 태세의 방식을 결정하도록 지원하고 공격을 차단하기 위해 빠르고 쉽게 구현할 수 있는 선제 보호 조치를 처방합니다.
- **알지 못했던 전역적 위협을 자동으로 식별:** MVISION Insights는 10억 개가 넘는 센서로부터 방대하게 축적된 보안 인텔리전스를 활용합니다.

엔드포인트 위험 관련 질문에 답을 제공하는 MVISION Insights

- 위험에 노출되어 있습니까? 노출 수준은 어떻습니까?
- 조직을 상대로 발생할 수 있는 공격의 우선순위를 지정하는 방법은 무엇입니까? 이에 대해 어떻게 학습하고 있습니까? 조사 프로세스는 무엇입니까?
- 아직 조직에 발생하지 않았지만 발생 가능성이 있는 위협을 어떻게 파악하고 있습니까?
- TIP가 있다고 해도, TIP 데이터베이스에 속한 모든 공격의 우선순위를 어떻게 정하고 있습니까?
- 동료를 공격했던 위협을 어떻게 알고 있습니까?
- 속한 산업 및 영역에 얼마나 만연해 있습니까?
- 현재 보안 태세는 이 위협을 어떻게 견디고 있습니까?
- 전체 위협 환경에 어떤 확신이 있으며 그 이유는 무엇입니까?

MVISION Insights 대시보드

그림 2. MVISION Insights 대시보드의 예

위험 평가

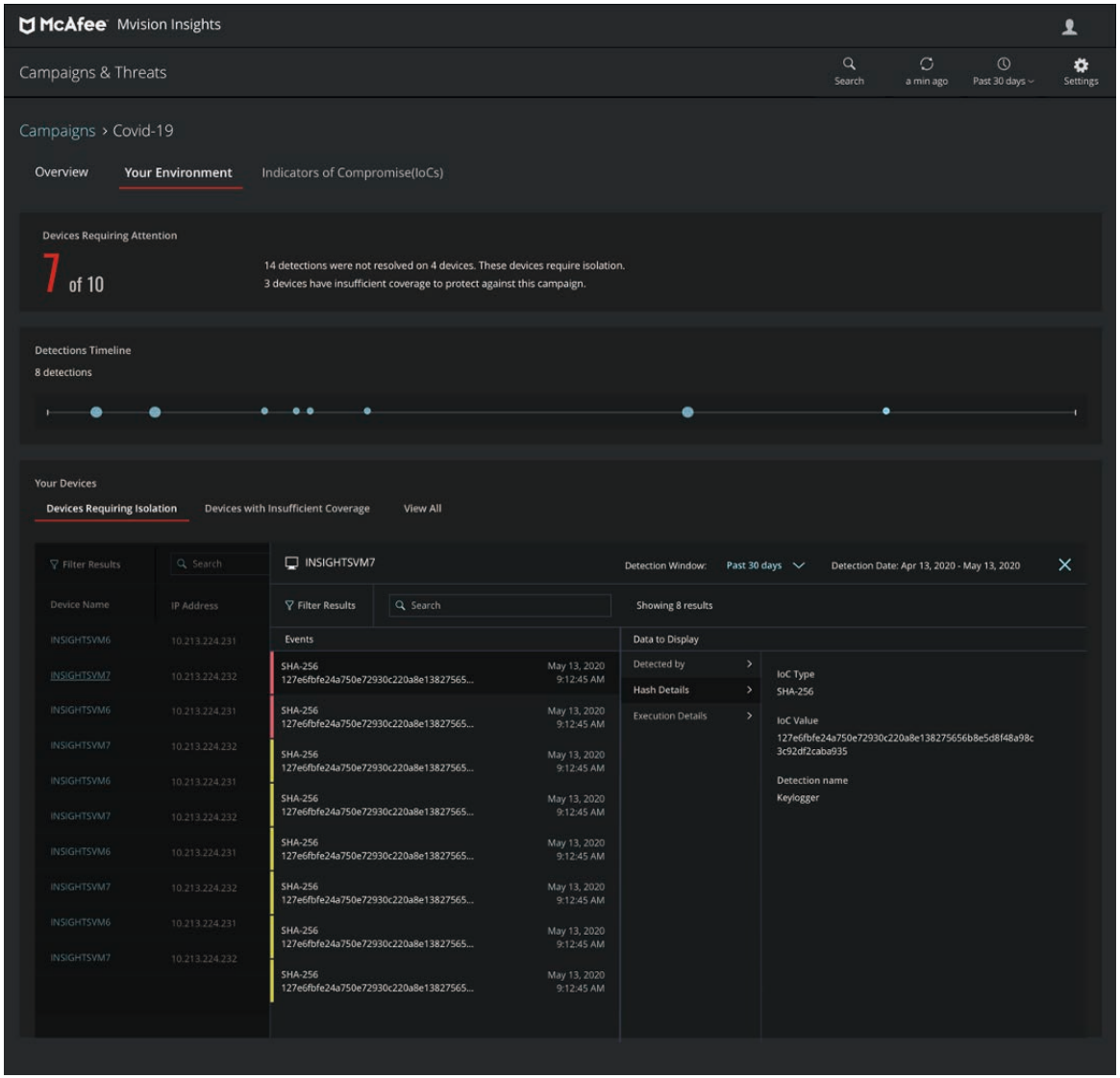

그림 3. 위협에 예방적으로 대응할 수 있도록 사용자 환경에서 주의가 필요한 부분을 파악합니다.

탐지 및 대응 시간을 대폭 단축

MVISION Insights는 기업이 사용자의 고유한 환경을 변경 및 개선하기 처방된 지침과 자동화된 조치를 통해 핵심적인 다음 예방적 단계를 취하도록 지원합니다. 자동화는 외부 공격에 대항하는 효과를 높이며 외부 위협을 자동으로 분석 및 비교하고 공격이 발생하기 전에 예방적으로 방어하게 합니다.

- **탐지 및 해결에 소요되는 평균 시간이 몇 개월에서 몇 분으로 단축:** 인간과 기계의 협업(딥러닝 및 머신 러닝) 및 고급 분석 기능은 확장되어 방대한 데이터를 살피고 실행 가능한 인텔리전스를 제시합니다. 확장된 탐지 기능은 대응 시간을 선제적으로 단축하고 위험을 대폭 감소합니다.
- **위협 지표의 신호 대 노이즈 비율 향상:** 고급 분석은 탐지 범위를 확대하고 경보를 더 잘 파악합니다. MVISION Insights 위협 분석은 손쉽게 McAfee® MVISION EDR로 전환해 손상 지표(IoC)와 같은 추가 컨텍스트를 검색하고 조사 주기를 단축할 수 있습니다.
- **사용자에게 위협을 이해할 수 있고, 우선순위가 있으며, 조치를 취할 수 있는 상태로 제시:** 분석되고 우선순위가 지정된 인텔리전스와 통찰력을 기반으로 한 대응 방법이 안내되어 초보 분석가라도 문제없이 작업할 수 있습니다. 통합 콘솔에서 구성을 변경하거나 감염된 장치를 격리하거나 정책을 업데이트하거나 엔드포인트 탐지 및 대응(EDR)으로 전환해 빠르고 손쉽게 대응하십시오.

SOC 리소스 강화

사용자 환경을 보호하기 위해 면밀한 조사가 필요한 인텔리전스의 양은 보안팀을 압도할 만큼 방대합니다. 한정된 리소스와 시간으로 인해 위협 및 방어 분석이 제한됩니다. 인간과 기계의 협업을 활용하는 분석 기능은 분석가의 기술 수준과 상관없이 확장되어 막대한 데이터양을 크롤링하고 실행 가능한 인텔리전스로 제시합니다. MVISION Insights를 이용하여 기업은 기술 격차를 해결하고 SOC 기능을 강화할 수 있습니다. 보안팀은 다양한 정보를 접하므로 더 나은 결정을 내릴 수 있습니다.

- 제공된 데이터 인텔리전스를 이용해 확보한 인간의 통찰력으로 보안팀은 인력을 늘리거나 더 높은 수준의 전문 지식을 갖출 필요 없이 최적의 상태로 보호하도록 기업 방어력을 사용자 지정하고 극대화할 수 있습니다. MVISION Insights는 MVISION EDR에 더 유용한 통찰력을 제공하여 조사 주기를 단축하고 조사에 필요한 전문 지식과 리소스를 제공합니다. 분석가는 빠르고 효율적으로 사고의 위험과 근본 이유를 확인할 수 있습니다.

- 보안 분석가가 단순 작업에서 해방되고 일반 사원이 더욱 효과적으로 업무를 진행하게 되므로 최고 보안 책임자(CSO)가 직원과 제품을 가장 효율적으로 활용할 수 있습니다. 조직은 보안 관리와 관련된 시간을 단축할 수 있습니다. 워크플로가 간소화되어 추가적인 보호 조치를 더 빠르게 시행할 수 있습니다.
- 단일 콘솔에서 우선순위가 지정된 위협의 탐지, 대응 및 방어를 선제적으로 자동화하여 분석가가 여러 작업을 병행해야 하는 부담을 줄여줍니다. MVISION Insights는 한 장소에서 관련 데이터 요소를 축적 및 분석하고 실행 가능한 지침을 제공하므로 필요할 때 분석가가 바로 활용할 수 있습니다.

더 깊이 있는 통찰력

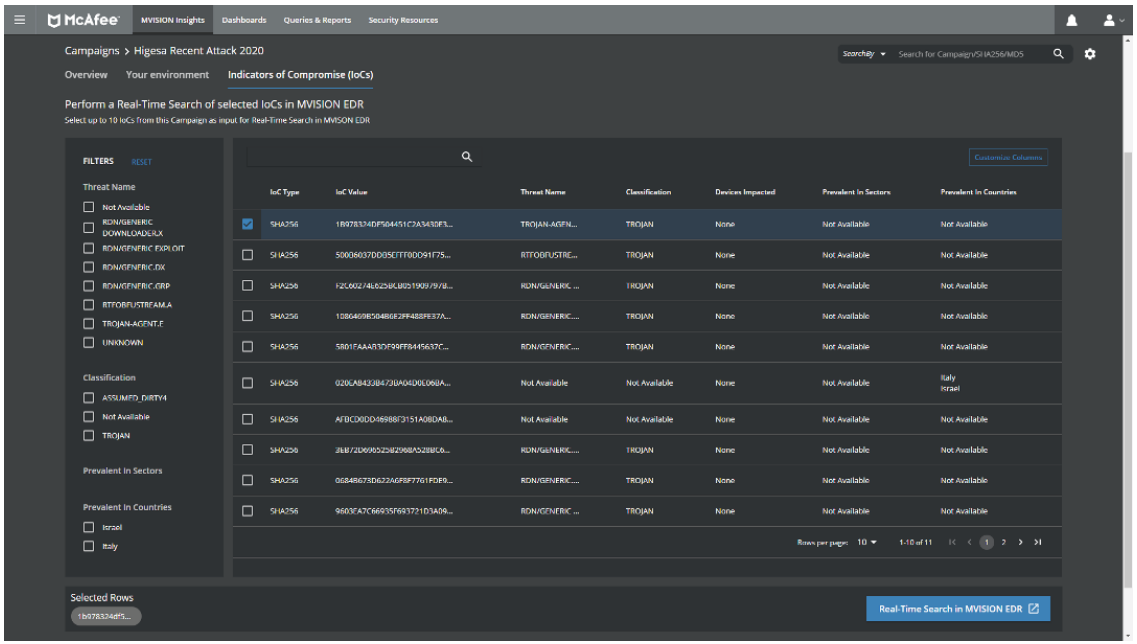

그림 4. 위협 이벤트를 이해하고 조직 방어 능력을 파악하기 위해 더 심도 있게 살펴봅니다.

MVISION Insights 요구 사항

MVISION Insights는 McAfee® ePolicy Orchestrator®(McAfee® ePO™) 소프트웨어 5.10(사내 및 IaaS) 및 McAfee® MVISION ePO™(SaaS)에서 관리됩니다. 최신 엔드포인트 보호 기술인 McAfee® Endpoint Security 및 McAfee® Agent와 함께 사용할 수 있도록 최적화되었습니다. MVISION Insights가 효율적으로 작동하려면 McAfee Endpoint Security 원격 측정 옵트인이 필요합니다.

샘플 사용 사례

문제	해결 방법	결과
표적 대상입니까? **새로운 캠페인 유형입니까?**	▪ 알려진 캠페인 위협 평가 ▪ 일부 소급 공격 분석 ▪ 비교 보호 효과 보고 ▪ 사용자 IoC 소급 공격 분석	질문에 답하기: 위험에 처해 있습니까?
현재 보호 구성이 보호할 수 있습니까?	▪ 국소적 보호 태세 확인	현재 보안 태세 평가
보호하기 위해 특히 변경해야 할 사항은 무엇입니까?	▪ 국소적 보호 태세 확인	취해야 할 조치의 처방적 지침
다른 보안 기능을 분리할 수 있습니까?	▪ 다른 보안 기능을 격리 또는 포함할 수 있도록 게시	다른 보안 기능에 포함되는 조치를 보내 위험 더욱 완화 (DXL 이용)

자세히 알아보기

자세한 내용은 www.mcafee.com 에서 확인하십시오.

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