McAfee Active Response

포괄적인 엔드포인트 탐지 및 대응

보안 문제로 고심하는 오늘날의 기관은 매우 빠른 속도로 변화하는 위협 환경에 직면해 있습니다. 공격이 그 어느 때보다 더 빠른 속도로 생성되어 전파되고 있습니다. '디자이너' 공격은 중점 지식을 사용하여 개별 조직을 겨냥하므로 효과를 높이고 탐지를 최소화합니다. 공격자는 예방 기술을 빈번하게 침투합니다. 따라서 미래 지향적인 조직은 공격자를 효율적으로 탐지한 다음 조사하여 처리할 수 있는 간편하고 통합된 도구를 요구합니다. 최고의 탐지 및 대응 솔루션은 아무리 많은 시스템에서 아무리 많은 정보를 캡처하더라도 향상된 보안 효율성을 제공합니다. 즉시 사용 가능한 탁월한 기능을 제공하고 기존 보안 관리 솔루션과 자동으로 통합하며, 사용자 정의 가능한 McAfee® Active Response는 공격자가 사용자의 컴퓨팅 자산과 회사 브랜드에 피해를 줄 수 있는 기회를 획기적으로 줄여줍니다.

주요 이점

- **자동화됨:** IoA 등에서 컨텍스트 및 시스템 상태 변경을 캡처하여 모니터링하고 숨겨져 있는 공격 구성요소를 찾은 다음 분석, 운영 및 포렌식 팀에게 정보를 보낼 수 있습니다.
- **적응 가능:** 경고가 표시되면 공격 방법의 변화에 따라 대응 방법을 조정하고, 해당 개체에 대한 데이터 수집, 경고 및 대응을 자동화하고, 고객 워크플로에 맞게 구성을 사용자 정의할 수 있습니다.
- **연속:** 영구 수집기는 공격 이벤트가 감지되면 트리거를 활성화하여 사용자와 시스템에 감지된 공격 활동에 대해 경고합니다.

진화하는 위협 환경

기업은 언제든지 공격자가 침입할 수 있으므로 공격 또는 지속적인 활동을 조기에 탐지하고 공격 지표(IoA)를 감지하여 이러한 위반을 효율적으로 처리할 수 있도록 대비해야 함을 깨닫게 되었습니다. 이러한 인식과 함께 현재의 가시성, 검색, 탐지 및 대응 격차를 해소하기 위해 새로운 기술을 필요하다는 것을 이해하게 되었습니다.

현재 사고 대응 방법의 한계

조직 전반에서 의심스럽거나 알려진 사고를 조사하라는 요청이 있을 경우 사고 대응자와 보안 관리자는 시간과 규모라는 두 가지 주요 요소에 의해 제약됩니다. 기존 시스템이나 도구를 통해 많은 정보가 수집되지만 해당 정보를 수집하고 분석하는 데 매우 오래 걸립니다. 데이터 수집의 핵심 요건은 속도이므로 데이터를 수집하는 시스템이 많을수록 수집되는 데이터의 특성이 심각하게 훼손됩니다. 또한 주요 정보를 식별하기 위해 변환되어야 하는 수집된 정보의 순수한 규모가 커질수록 처리하기가 더 어려워집니다.

가장 일반적으로 사용되는 사고 대응 도구는 대응자가 직접 작성한 스크립트입니다. 이러한 도구는 광범위한 분석에서 데이터 수집의 기반으로 사용됩니다. 이러한 정보는 관련 도구와 함께 많은 개선이 이루어졌지만, 대규모로 신속하게 활용하는 데에는 제한이 있습니다. 조직 전반에서 특정 IoA에 대한 실시간 조사가 불가능하여 대응자가 검색 및 대응 노력을 근시안적으로 평가하게 되는 경우가 있습니다. 일반적으로 시간 요구 사항을 충족하기 위해 이러한 노력은 인위적으로 제한되며, 이로 인해 사고 대응 프로세스에 심각한 결함이 발생할 수 있습니다. 이는 대응자에게 심각한 장애로 작용하고, 현재 도구의 제약으로 인해 노력이 인위적으로 제한됩니다.

시스템 사양

최소 하드웨어 요구 사항

필요한 경우 가상 머신에 서버를 설치할 수 있습니다. McAfee Active Response 서버에 대한 최소 권장 하드웨어 요구 사항은 다음과 같습니다.

- 4 Intel® Xeon® CPU X5675, 3.07GHz
- 8 GB RAM
- 120 GB 반도체 디스크

필수 서비스 인프라

- McAfee® ePolicy Orchestrator®(McAfee ePO™) 5.1.1 이상
- McAfee Agent 5.0 확장 이상
- McAfee Data Exchange Layer 2.0.0.405 브로커 이상

지원되는 웹 브라우저

- Microsoft Internet Explorer 9 이상
- Google Chrome 17 이상
- Mozilla Firefox 10.0 이상

필수 클라이언트 인프라

- Linux용 McAfee Agent 5.0.0.2710 이상 엔드포인트
- Microsoft Windows용 McAfee Agent 5.0.0.2610 이상 엔드포인트
- 모든 관리되는 엔드포인트에서 McAfee Data Exchange Layer 2.0.0.405 클라이언트 이상

포괄적인 엔드포인트 탐색 및 대응

McAfee Active Response는 진화하는 보안 위협을 지속적으로 탐지하고 대응하여 보안 관련자가 미래 지향적인 검색, 세부 분석, 포렌식 조사, 포괄적인 보고, 우선순위에 따른 경고와 조치 등을 통해 보안 상태를 모니터링하고, 위협 감지를 향상하고, 사고 대응 기능을 확장할 수 있도록 지원합니다. 엄격한 엔드포인트 탐지 및 대응(EDR) 기준을 충족하도록 최적화된 McAfee Active Response는 미리 정의되고 사용자 정의 가능한 수집기를 통해 모든 시스템을 세부적으로 검색하여 실행 중인 프로세스를 통해 실제하거나 숨겨져 있는 IoA뿐만 아니라 삭제된 IoA도 찾아낼 수 있습니다. 또한 McAfee Active Response를 사용하면 현재의 IoA를 검색할 수 있을 뿐만 아니라 향후에 IoA가 발생할 경우에 대한 지침을 제공하는 트리거를 통해 보안 목적에 따라 경고하고 조치할 수도 있습니다.

McAfee Active Response는 Intel Security 통합 보안 아키텍처의 효율성을 입증하며, 점점 더 복잡해지는 환경에서 더 적은 수의 리소스로 더 많은 위협을 빠르게 해결하도록 설계되었습니다. McAfee Active Response는 위반 사항을 더 빠르게 식별할 수 있도록 엔드포인트를 지속적으로 모니터링하여 강력한 통찰력을 제공합니다. 또한 비즈니스에 가장 적합한 방식으로 더 빠르게 문제를 해결하는 데 필요한 도구를 제공합니다. 이러한 모든 기능은 McAfee Data Exchange Layer를 활용하는 McAfee® ePolicy Orchestrator®(McAfee ePO™) 소프트웨어를 통해 관리됩니다. 따라서 제품 관리를 위해 직원을 충원하지 않고도 통합된 확장성을 제공합니다.

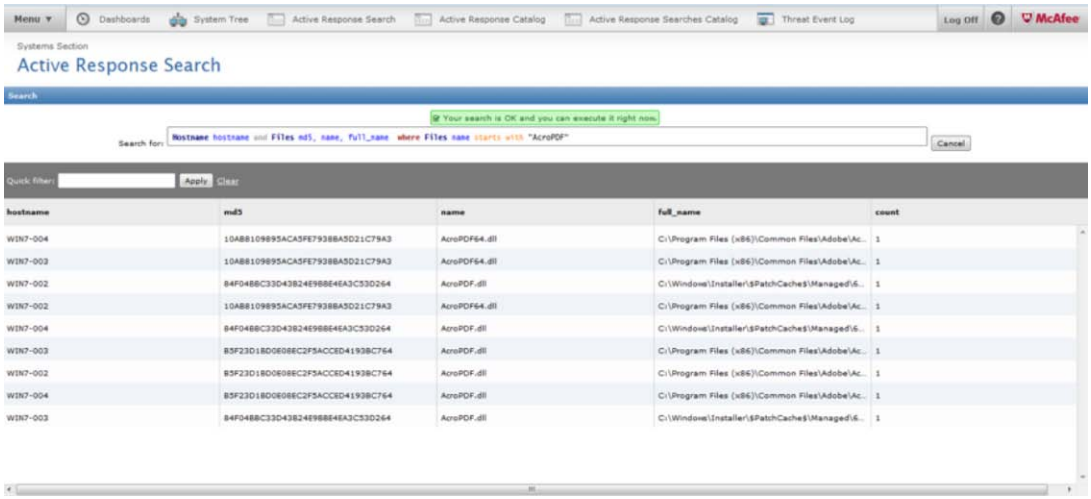

그림 1. McAfee Active Response 검색 사용자 인터페이스

지원되는 클라이언트 운영 체제

- Microsoft Windows
  - Windows 8.0, Base, 32비트 및 64비트
  - Windows 8.1, Base, U1, 32비트 및 64비트
  - Windows Server 2012, Base, R2, U1, 64비트
  - Windows Server 2008 R2 Enterprise, SP1, 64 비트
  - Windows Server 2008 R2 Standard, SP1, 64 비트
  - Windows 7 Enterprise, 최대 SP1, 32비트 및 64비트
  - Windows 7 Professional, 최대 SP1, 32비트 및 64비트
- CentOS 6.5, 32비트
- RedHat 6.5, 32비트

기능	이점	고객 이점	차별화
수집기	수집기를 사용하여 시스템에서 데이터를 검색 및 시각화할 수 있습니다.	수집기는 시스템을 세부적으로 조사할 수 있는 검색 기능을 제공합니다. 또한 수집기는 중요 위반 또는 잠재적 공격을 모니터링하고 이러한 시스템으로부터 데이터를 수집하여 시각화합니다. 사용자는 다양한 일반 스크립팅 언어를 사용하여 수집기와 대응을 쉽게 사용자 정의하여 최적의 구성과 적응성을 제공할 수 있습니다.	McAfee Active Response는 실행 가능하거나 실행 중인 파일에서 숨겨져 있는 코드뿐만 아니라 공격자의 트랙을 포함하려는 시도에서 삭제된 코드도 찾아낼 수 있습니다. McAfee Active Response는 파일, 네트워크 흐름, 레지스트리 및 프로세스 매핑을 검색할 수 있습니다.
트리거	보안 관련자는 트리거를 사용하여 단일의 지침에 따라 현재와 미래의 중요 이벤트 또는 상태 변경을 지속적으로 모니터링할 수 있습니다.	이벤트가 생성되거나 대응을 실행하기 전에 트리거 집합에 의해 조치가 시작됩니다. McAfee Active Response는 정적 '피크'를 초과하여 지속적인 응답 모드로 전환할 수 있습니다.	McAfee Active Response는 현재의 위협을 확인하고 미래에 발생할 수 있는 위협에 대한 조치를 트리거할 수 있습니다.
대응	대응은 트리거 조건이 충족될 경우 위협을 찾아서 차단할 수 있도록 미리 구성된 사용자 정의 조치를 제공합니다.	대응을 통해 조치를 수행할 수 있습니다. 예를 들어, 파일 해시(MD5 및 SHA1)에 의해 시스템에서 삭제된 파일을 검색하거나, 호스트가 IP 주소에 현재 연결되어 있거나 과거에 IP 주소에 연결된 적이 있는지를 확인하거나, 시스템에서 액세스되거나 발생되지 않은 PE 기반이 아닌 악의적인 파일을 검색(파일 시스템에 복사되었지만 열리지 않은 시스템에서 악의적인 PDF 검색)할 수 있습니다.	McAfee Active Response는 검색 결과에 대해 조치하고 사용자가 특정 사용자 정의 요구사항을 충족하기 위해 규정한 사용자 정의 조치를 수용하도록 미리 구성되어 있습니다.
McAfee ePO 소프트웨어를 통한 중앙 집중식 관리	단일 콘솔 환경에서 포괄적인 관리 및 자동화 기능을 제공합니다.	관리자는 McAfee ePO 소프트웨어를 Intel Security의 통합 보안 아키텍처의 일부로 활용하여 트리거 및 검색에 자동으로 응답하고 위협에 대응하여 완화할 수 있습니다. 단일 창 관리 효율성은 추가적인 관리 부담 없이 향상된 보안 가시성을 제공합니다. 운영 측면을 간소화하고 관리 직원의 시간 투자를 축소합니다.	단일 콘솔을 통한 관리와 조치는 명확한 차별화 요소입니다. 단일 콘솔에서 McAfee Active Response를 비롯한 강력한 보안 제어를 통해 다양한 플랫폼을 고유하게 보호할 수 있습니다.
통합 보안 아키텍처	Intel Security의 일부로 Data Exchange Layer를 활용하여 McAfee의 다른 제품과의 통신을 간소화합니다.	McAfee Active Response는 Intel Security 통합 보안 아키텍처의 일부로 이 플랫폼의 혁신적 개념, 최적화된 프로세스, 실용적 권장 사항을 통해 위험 및 대응 시간을 단축하고 간접 비용 및 운영 직원 비용을 절감합니다.	

McAfee Active Response의 이점에 대한 자세한 내용은 **http://www.mcafee.com/kr/about/active-response-technology-preview.aspx**를 참조하십시오.

McAfee. Part of Intel Security.
서울특별시 강남구 역삼동 737
강남파이낸스센터 5층 135-984
+82.2.3458.9800
www.intelsecurity.com