McAfee Threat Intelligence Exchange

여러 보안 솔루션에서 공유되는 위협 인텔리전스

McAfee® Threat Intelligence Exchange는 적응형 위협 탐지 및 대응을 지원하는 평판 브로커 역할을 합니다. 조직 전반에 걸친 보안 솔루션의 로컬 인텔리전스를 외부 글로벌 위협 데이터와 결합하고 이 집단 인텔리전스를 즉시 보안 에코시스템 전체에서 공유함으로써 솔루션이 공유 인텔리전스를 교환하고 그에 대처할 수 있도록 합니다.

협력적인 위협 인텔리전스 에코시스템 구축

평판 브로커인 McAfee Threat Intelligence Exchange는 McAfee Global Threat Intelligence (McAfee GTI) 및 타사 위협 정보(예: VirusTotal)와 같이 가져온 글로벌 소스의 위협 인텔리전스를 엔드포인트, 게이트웨이, 고급 분석 솔루션 등 로컬 소스의 인텔리전스와 결합합니다. 그런 다음 Data Exchange Layer (DXL)를 사용하여 이 집단 인텔리전스를 즉시 보안 에코시스템 전체에서 공유함으로써 여러 보안 솔루션이 하나로 작동하여 전사적으로 보호를 강화할 수 있게 해줍니다.

DXL에 의한 통합 간편성을 통해 다수의 직접 API (Application Programming Interface) 통합을 구현하고 운영하는 비용을 크게 절감하고, 탁월한 보안, 운영 효율성 및 효과를 실현할 수 있습니다. 개방형 프레임워크로 설계된 DXL은 타사 보안 제품을 비롯해 모든 보안 솔루션이 McAfee Threat Intelligence Exchange 에코시스템에 동적으로 참여할 수 있게 해줍니다.

위협에 적응 및 내성 증가

네트워크의 모든 위치에서 감지되는 공유 정보를 통해 표적 공격에 보다 효과적으로 대처할 수 있습니다. 이러한 위협은 본래부터 많은 주목을 받아온 공격이므로 조직은 경향을 알아내고 직면한 고유한 공격을 포착하기 위한 로컬 감시 시스템이 필요합니다. 인카운터에서 수집된 상황별 지역 데이터를 글로벌 위협 지능과 결합하여 처음 발견된 파일에 대해 보다 적절한 결정을 내릴 수 있으므로, 더 빠른 시간 내에 보호 및 탐지 효과를 얻을 수 있습니다.

주요 이점

- 위협 보호 기능은 문제 발생부터 진화한 타겟화된 공격 방지까지의 간격을 일, 주 및 월 단위에서 밀리초까지 줄여줍니다.
- 협력 가능한 위협 지능은 로컬 위협 지능 수집과 결합된 글로벌 지능 데이터 소스를 기반으로 구축됩니다.
- 관련 보안 지능이 엔드포인트, 게이트웨이, 네트워크 및 데이터 센터 보안 솔루션 간에 실시간으로 공유됩니다.
- 총체적 위협 지능과 결합된 엔드포인트 컨텍스트(파일, 프로세스 및 환경 속성)를 기준으로 처음 발견된 파일에 대해 보다 효과적인 결정을 내릴 수 있습니다.
- 통합이 DXL을 통해 간소화됩니다. McAfee 및 비 McAfee 보안 솔루션을 하나로 연결하여 위협 인텔리전스를 실시간으로 운영함으로써 구현 및 운영 비용이 줄어듭니다.

네트워크 어디에서든 알려지지 않은 파일이 발견될 경우 파일에 대한 평판이 있는지 판단하기 위해 McAfee Threat Intelligence Exchange에 연결됩니다. 조직적 확산 및 사용 기간과 같은 설명형 메타데이터도 유지 관리되고 집단 인텔리전스에 반영됩니다. 통합 보안 솔루션은 평판 요청 외에, 로컬 진단에 따라 McAfee Threat Intelligence Exchange에 대한 평판 업데이트를 제공할 수도 있습니다. 그러면 업데이트된 평판이 실시간으로 시스템 전체에 전파됩니다. 이러한 로컬 위협 지능은 이후 사례를 위해 저장되므로, 다른 장치 또는 서버에서 같은 문제가 발견되더라도, 더 이상 알려지지 않은 문제가 아니며, 즉시 감지됩니다.

McAfee Threat Intelligence Exchange는 관리자가 위협 인텔리전스를 쉽게 조정하는 데 도움이 됩니다. 보안 관리자는 포괄적인 인텔리전스 정보를 취합, 재정의, 보강 및 조정하여 사용자 환경 및 조직에 맞게 보호를 맞춤 설정할 수 있습니다. 이러한 로컬 우선 및 조정된 위협 정보를 통해 어떠한 미래 위협에 대해서도 즉각적으로 대처할 수 있습니다.

보호를 향상하는 시행 지점

엔드포인트부터 네트워크 주변부에 이르는 네트워크 전반의 통합 솔루션은 사용 가능한 평판, 메타데이터 또는 데이터 포인트의 조합을 바탕으로 정책을 적용합니다. 긴밀히 통합된 단일 솔루션인 McAfee Endpoint Security는 결합된 로컬 인텔리전스(조직적 확산, 사용 기간 등의 파일 메타데이터와 기타 보안 구성 요소에서 제공되는 로컬 평판)와 현재 사용 가능한 글로벌 위협 인텔리전스를 활용하여 정확한 결정을 내립니다. 예를 들어 글로벌 평판은 없지만 조직적 확산성이 높은 사용자 지정 응용프로그램은 악의적인 복합 평판을 생성하지 않으며 실행이 허용될 가능성이 높습니다. 반면, 이전에 조직에서 본 적이 없으며 글로벌 또는 로컬 평판이 없고 의심스럽게 압축된 파일은 낮은 신뢰 수준을 생성하여 차단을 시작하거나 자세한 조사가 요구될 가능성이 높습니다. 이때 추가 McAfee Endpoint Security 엔진이 사용되거나 McAfee Advanced Threat Defense 또는 McAfee Cloud Threat Detection을 통한 모래상자 처리가 사용됩니다.

McAfee Endpoint Security의 시스템 학습 기능인 Real Protect와 동적 응용프로그램 억제는 엔드포인트 탐지 및 보호 기능을 더욱 강화합니다. Real Protect는 사전 및 사후 분석을 통해 최신 위협 인텔리전스에 대한 클라우드 조회를 수행하는 반면, 동적 응용프로그램 억제는 엔드포인트에 대한 악의적인 활동을 차단함으로써 신규 위협에 노출된 첫 번째 시스템을 보호하는 동시에 추가적인 분석을 수행합니다.

진화한 표적 공격은 현실적인 과제

탐지를 방해하고 조직 내에서 지속적으로 발판을 마련하도록 설계된 지능형 표적 공격은 조직에 계속 해를 입히고 가치가 높은 데이터를 유출합니다. Verizon 2015 Data Breach and Investigations Report (Verizon 2015 데이터 유출 조사 보고서)에서 최근 발표된 데이터에 따르면 악성 프로그램 샘플 중 70%~90%가 단일 조직에서만 고유하게 발생하여, 고유 위협 지표가 오늘날 가장 큰 문제임을 보여줍니다.[1]

자세한 내용은 **www.mcafee.com/kr/products/threat-intelligence-exchange.aspx**를 참조하십시오.

공동 작업의 혜택

향상된 위협 분석

파일에 추가 정보가 필요한 경우 McAfee Threat Intelligence Exchange에서 McAfee 고급 분석 솔루션(예: McAfee Advanced Threat Defense 또는 McAfee Cloud Threat Detection)으로 해당 정보를 자동 전송하여 잠재적인 신규 위협에 대한 추가적인 통찰력을 즉시 확보하고 해당 파일의 평판을 확인할 수 있습니다. 이러한 모든 기능은 전체 보안 에코시스템 보호를 위해 DXL을 통해 자동화 및 문서화되며 종합적으로 공유됩니다.

보안 이벤트 관리

McAfee Enterprise Security Manager는 McAfee Threat Intelligence Exchange로 확인된 손상 지표(IoC)를 조사할 때 보다 심도 있는 조사가 가능하게 해줍니다. 이전 보안 정보에 액세스할 수 있고 자동화된 감시 목록을 생성할 수 있으므로 조직의 보안 효율성이 증가됩니다.

1. http://www.verizonenterprise.com/DBIR/2015/

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