McAfee Data Exchange Layer

간편한 일대다 앱 통합과 즉각적인 통신

기업과 개발자는 실시간 응용프로그램 프레임워크를 사용하여 응용프로그램 전체에서 쉽게 연결하고 데이터를 공유하며 보안 작업을 조정할 수 있습니다. 새로운 개방형 SDK(소프트웨어 개발 키트)를 사용하여 통합 노력, 취약성 및 사이버 보안 효율성을 저해하는 시간 지연을 줄일 수 있습니다.

McAfee DXL을 통한 보안 역학 변화

위협 방어 수명 주기의 워크플로 단축
거의 즉각적인 정보 공유 및 작업 조정으로 새로 식별된 위협을 탐지, 억제 및 수정하는 시간을 줄일 수 있습니다.

보안 제품 및 공급업체 전체에서 통합 지연, 노력 및 복잡성 완화
McAfee 개방형 플랫폼을 사용하면 여러 공급업체의 보안 제품을 고유한 응용프로그램 및 도구와 연결할 수 있으며 공급업체가 협상할 때까지 기다릴 필요가 없습니다. 사용자가 직접 원하는 대로 선택할 수 있습니다.

배포하는 응용프로그램의 가치 확대
응용프로그램은 자신이 생성한 유용한 위협 데이터를 공유하고 즉시 조치를 유도하거나 수행할 수 있습니다.

통합 비용을 지불하고 있을 수 있습니다. 일대일 통합, 수동 스크립트 및 예정된 프로세스는 보안 팀 및 해당 공급업체가 응용프로그램을 연결하는 데 사용하는 가장 일반적인 방법입니다. 이러한 전술은 사이버 보안 팀이 최고의 성능을 얻는 데 필요한 효율성, 정확성 및 속도에 방해가 됩니다. 이로 인해 위협 인텔리전스를 공유하고, 인시던트를 조사하며 대응 기술을 조정할 수 있는 기능이 제한됩니다.

방해가 되는 요소는 무엇입니까? 보안 업계는 실시간 데이터를 지속적으로 공유할 수 있는 안전하고 간단한 방법을 보유하고 있지 않습니다.

- 보안 및 IT 인프라는 다년간에 걸쳐 개별 기술, 공급업체 및 사내 응용프로그램을 바탕으로 구축되었습니다.
- P2P, API 중심의 제품 통합의 경우 제품 및 데이터 형식이 업그레이드됨에 따라 구축하는 데 시간이 많이 소요되고, 유지 관리하기가 까다롭습니다.
- 보안 제품 2개를 통합하려면 두 공급업체가 협상, 합의하고 구현해야 합니다.
- 기존의 폴링 모델 및 예정된 데이터 게시 모델은 트랜잭션마다 시간이 추가로 소요됩니다.

단일 개방형 표준 및 에코시스템

더 좋은 방법이 있습니다. 바로 OpenDXL(Open Data Exchange Layer) 이니셔티브의 일부로 개방형 업계 표준을 따르는 것입니다. OpenDXL 이니셔티브의 목표는 통합 유연성, 단순성 및 개발자를 위한 기회를 확대하고, 배포하는 조직의 보안 작업을 개선하는 것입니다. OpenDXL 이니셔티브의 첫 번째 단계에서는 새로운 개발자 및 참가자로 McAfee® DXL(Data Exchange Layer)의 액세스 및 사용을 확대하는 SDK를 제공하여 DXL 통합 또는 배포의 가치를 기하급수적으로 높입니다.

개발자는 서로 다른 공급업체의 여러 응용프로그램은 물론 내부에서 개발된 응용프로그램 전반에 걸쳐 데이터 및 조치를 실시간으로 조정할 수 있는 안전한 방법으로 이 SDK를 사용하여 DXL 통신 패브릭을 통해 실행되는 응용프로그램을 생성하거나 연결합니다. McAfee에서는 반복적인 일회성 제품 간 통합을 지양합니다.

앱은 단순히 메시지 항목을 게시 및 구독하거나, 요청/응답 호출에서 RESTful API와 유사한 DXL 서비스를 호출합니다. 패브릭은 메시지 및 호출을 즉시 전달하며 보안, IT 및 사내 솔루션을 적절히 작동하는 시스템에 연결합니다.

intel Security

그림 1. DXL은 신속한 통합 모델 및 실시간 통신 패브릭을 제공합니다.

DXL은 2014년에 처음 소개되었으므로 수십 여 공급업체의 응용프로그램이 DXL 에코시스템에 참여했습니다. 기업, 서비스 공급자 및 정부 조직은 이미 DXL을 사용하여 결정 능력을 개선하고 보다 빠르게 조치를 수행하고 있습니다. 이를 통해 운영 비용을 낮추고, 보호 및 대응 능력을 효율화하며, 수동 작업 및 전술적인 보안 훈련으로부터 소중한 보안 팀 리소스를 해방시킬 수 있습니다.

단일 통합으로 모두 관리

기존의 통합과 달리 각 응용프로그램은 일반 DXL 통신 패브릭에 연결됩니다. 여러 작업이 필요하지 않은 하나의 통합 프로세스가 있을 뿐입니다. OpenDXL은 광범위한 언어를 지원하므로 개발자는 자신이 즐겨 사용하는 개발 환경에서 통합을 구축할 수 있습니다. 한 앱이 메시지를 게시하거나 서비스를 호출하면 하나 이상의 앱이 메시지를 사용하거나 서비스 요청에 응답합니다. 이는 모든 표준에서 목표로 하는 내용이므로 각 통합 기술의 기본적인 독점 아키텍처와는 독립적으로 상호 작용이 이루어집니다. 공급업체별 API 및 요구사항을 바탕으로 한 이와 같은 개념을 통해 통합 과정이 훨씬 간단해집니다.

기본 DXL 통합을 구축하는 것 외에, 개발자는 상용 제품 API와 상호 작용 및 래핑하도록 서비스를 포함시켜 데이터를 DXL에 게시할 수 있습니다. 기타 서비스는 DXL 메시지 및 호출을 수신하여 기능을 최신 데이터로 보강하거나 적절한 조치를 수행합니다. 조정을 반영하는 보다 정교한 앱의 경우 이러한 종류의 조치를 함께 스크립팅하여 일련의 또는 동시에 설정된 조치를 유발할 수 있습니다.

기업은 각 호스트의 소규모 DXL 클라이언트와 메시지 교환을 관리할 DXL 브로커를 사용하여 기존 네트워크에 표준화된 통합 및 통신 계층을 배포합니다. 모든 DXL 트래픽은 데이터 정보 보호 및 운영 제어를 제공하는 기업 네트워크에 포함됩니다. 방화벽 친화적인 모델에서는 DXL을 통해 전달되는 최신 정보에 지속적으로 액세스할 수 있도록 클라이언트와 서버 간에 연결을 유지합니다. 게시 또는 수신 응용프로그램 자체에 변경 사항이 있는 경우 DXL 추상화 계층에서 배포의 나머지 부분이 변경되지 않도록 보호하므로 위험과 통합 유지 관리 비용을 줄일 수 있습니다.

향상된 사이버 보안 엔진

이전에는 사용할 수 없었던 최신 데이터 유형에 액세스할 수 있는 기능은 보안 업계의 판도를 바꾸어 놓았습니다. 분석가, 응답자 및 운영 팀은 데이터를 최대한 빠르게 확보, 분석하고 그에 대한 조치를 수행해야 합니다. 공급업체 및 개발자는 도움이 되기를 바라지만, 기술 복잡성 또는 공급업체의 비즈니스 파트너십에 대한 종속성으로 인해 통합이 어려워질 수 있습니다.

이제 주도권을 잡아 선택할 수 있으므로 이러한 장애 요소가 사라졌습니다.

보안 작업에서는 이제 다음 데이터로부터 즉각적인 이점을 얻을 수 있습니다.

- 속임수 위협 이벤트
- 파일 및 응용프로그램 평판 변경
- 검색된 모바일 장치 및 자산
- 네트워크 및 사용자 동작 변경
- 충실도가 높은 경보
- 취약성 및 손상 지표 (IoC) 데이터

소프트웨어 및 솔루션 공급업체는 DXL을 소프트웨어 및 고객의 조직에서 보안 및 IT 활동 시간을 단축하고 새로운 기능을 지원할 수 있는 강력한 프레임워크로 간주해야 합니다. 새로운 데이터 유형은 분석의 복잡성을 가중시킬 수 있습니다. 결론에 따라 즉각적인 에스컬레이션, 억제, 교정 또는 개입이 발생할 수 있습니다. 데이터의 실시간 공유 및 매끄러운 프로세스 통합을 통해 새로운 기회를 포착할 수 있습니다.

www.mcafee.com/kr/solutions/data-exchange-layer.aspx에서 시작해 보십시오.

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