Data Exchange Layer

Einfache Integration beliebiger Anwendungen und Echtzeitkommunikation

Unternehmen und Entwickler können jetzt mit einem Echtzeit-Anwendungs-Framework unkompliziert Anwendungen vernetzen, Daten austauschen und Sicherheitsaufgaben koordinieren. Ein neues, offenes Software Development Kit (SDK) senkt den Integrationsaufwand, die Fehleranfälligkeit sowie Zeitverzögerungen, die die Effizienz der Cyber-Sicherheit beeinträchtigen.

Sie bezahlen wahrscheinlich eine Art „Integrationssteuer". Die wichtigsten Methoden, mit denen Sicherheitsteams und ihre Anbieter Anwendungen vernetzen, sind 1-zu-1-Integrationen, manuelle Skripts und geplante Prozesse. Diese Ansätze stehen jedoch der Effizienz, Genauigkeit und Geschwindigkeit, die Cyber-Sicherheitsteams für maximale Leistung benötigen, im Weg. Sie schränken Ihre Möglichkeit ein, Bedrohungsdaten auszutauschen, Vorfälle zu untersuchen und Gegenmaßnahmen zu koordinieren.

Aber was genau steht dem im Weg? Die Sicherheitsbranche hatte bislang keine einfache und sichere Möglichkeit, Daten in Echtzeit kontinuierlich auszutauschen.

- Sicherheit und IT-Infrastruktur wurden jahrelang aus unterschiedlichen, getrennten Technologien, Anbietern und internen Anwendungen aufgebaut.
- Beim Aktualisieren Ihrer Produkte und Datenformate gestalten sich die Implementierung und Wartung API-gestützter Punkt-zu-Punkt-Produktintegrationen zeitintensiv und schwierig.
- Zur Integration zweier Sicherheitsprodukte müssen die beiden Anbieter Verhandlungen führen, Verträge abschließen und Implementierungsmaßnahmen durchführen.
- Herkömmliche Abfragen und geplante Datenveröffentlichungen verzögern jede Transaktion.

Offener Standard und offenes Ökosystem

Es gibt eine bessere Möglichkeit, und sie wird zu einem offenen Branchenstandard im Rahmen der Open Data Exchange Layer (OpenDXL)-Initiative. Die Ziele der OpenDXL-Initiative sind flexiblere und einfachere Integrationsprozesse, neue Möglichkeiten für Entwickler sowie die Verbesserung der Sicherheitsabläufe in den Unternehmen, die diesen Ansatz implementieren.

DXL verändert die Dynamik Ihrer Sicherheit

- **Straffung der Abläufe bei der Bedrohungsabwehr:** Die nahezu sofortige Weitergabe von Informationen und Koordinierung von Aufgaben kann die Zeit bis zur Erkennung, Eindämmung sowie Beseitigung neu erkannter Bedrohungen minimieren.
- **Verringerung von Verzögerungen, Aufwand und Komplexität bei der Integration von Sicherheitsprodukten sowie -anbietern:** Unsere offene Plattform ermöglicht die Vernetzung von Sicherheitsprodukten unterschiedlicher Anbieter mit Ihren eigenen Anwendungen und Tools ohne bürokratische Hindernisse. Sie haben die freie Wahl.
- **Steigerung des Mehrwerts Ihrer eingesetzten Anwendungen:** Anwendungen können die nützlichen Bedrohungsdaten, die sie generieren, jetzt austauschen und sofort Maßnahmen ergreifen oder ermöglichen.

Die OpenDXL-Initiative stellt neuen Entwicklern und Teilnehmern ein Software Development Kit (SDK) bereit, um die Nutzung des Data Exchange Layer (DXL) zu erhöhen. Dadurch steigt der Mehrwert einer DXL-Integration oder -Bereitstellung erheblich.

Entwickler können mithilfe dieses SDK Anwendungen erstellen oder vernetzen, die auf der DXL-Kommunikationsstruktur aufsetzen und abgesichert sowie in Echtzeit Daten und Aktionen unterschiedlicher Anwendungen von verschiedenen Anbietern sowie intern entwickelter Anwendungen koordinieren. Dadurch vermeiden wir Integrationsprozesse, die jeweils nur für eine bestimmte Produktkombination anwendbar sind.

Anwendungen veröffentlichen bzw. abonnieren lediglich Meldungsthemen oder kontaktieren DXL-Services per Anfrage/Antwort, so wie das auch bei RESTful-APIs der Fall ist. Die Struktur übermittelt die Meldungen und Aufrufe ohne Zeitverlust und vernetzt Ihre Sicherheits-, IT- und internen Lösungen zu einem gut funktionierenden System. OpenDXL umfasst den Open-Source-Client sowie den Broker für DXL: OpenDXL Client und OpenDXL Broker. Dadurch wird sichergestellt, dass das Unternehmen ein wirklich offenes Open-Source-Modell als Kommunikationsebene zwischen Tools und intelligenten Quellen nutzt.

Nachdem DXL im Jahr 2014 eingeführt wurde, umfasst das DXL-Ökosystem nun Anwendungen von mehr als 30 Anbietern mit mehr als 100 Integrationen.

Unternehmen, Dienstanbieter und Behörden nutzen diesen Ansatz bereits, um bessere Entscheidungen treffen und schneller Maßnahmen ergreifen zu können. Dadurch können Betriebskosten gesenkt, Schutz- und Reaktionsmaßnahmen optimiert sowie das Sicherheitsteam von manuellen Aufgaben und taktischen Notfallmaßnahmen entbunden werden.

Eine Integration – volle Kontrolle

Im Gegensatz zu typischen Integrationen verbindet sich jede Anwendung mit der universellen DXL-Kommunikationsstruktur. Daher gibt es statt vieler Abläufe lediglich einen einzigen Integrationsprozess. OpenDXL unterstützt zahlreiche Sprachen, sodass Entwickler die Integrationen in ihrer bevorzugten Umgebung implementieren können. Eine Anwendung gibt eine Meldung aus oder ruft einen Service auf, anschließend verarbeiten eine oder mehrere Anwendungen die Meldung oder reagieren auf die Service-Anfrage. Wie bei jedem Standard ist auch hier das Ziel, dass die Interaktion unabhängig von der zugrunde liegenden proprietären Architektur oder integrierten Technologie erfolgt. Aufgrund dieser Abstraktion von anbieterspezifischen APIs und Anforderungen lassen sich Integrationen erheblich einfacher realisieren.

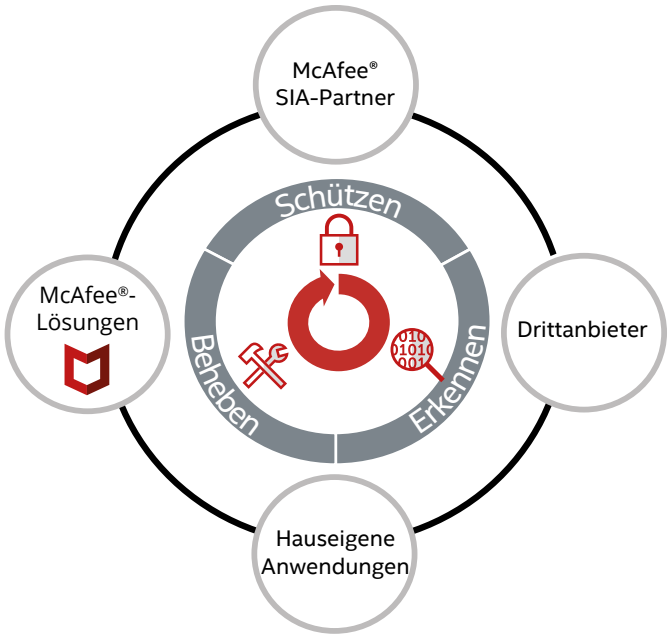

Abbildung 1. DXL bietet ein Modell zur schnellen Integration sowie eine Struktur zur Echtzeitkommunikation.

So können Entwickler native DXL-Integrationen erstellen, ihre Services mit DXL zusammenarbeiten lassen oder der API eines kommerziellen Produkts die Weitergabe von Daten an DXL ermöglichen. Andere Services können DXL-Meldungen und Abrufe empfangen, um ihre Funktionen mit den neuesten Daten zu versorgen oder angemessene Maßnahmen zu ergreifen. Bei einer hochentwickelten Anwendung, die bessere Koordination ermöglicht, können diese Aktionen zur parallelen Ausführung geskriptet werden, um eine Kaskade oder einen Strom gleichzeitig ausgeführter Aktionen zu gewährleisten.

Unternehmen stellen eine standardisierte Integrations- und Kommunikationsebene in ihrem vorhandenen Netzwerk bereit, bei der ein kleiner DXL-Client auf jedem Host installiert wird und ein DXL-Broker die Verwaltung des Meldungsaustauschs übernimmt. Der gesamte DXL-Datenverkehr ist auf das Unternehmensnetzwerk beschränkt, sodass Datenschutz und Kontrolle über die Abläufe gewährleistet bleiben. Das Modell wird von der Firewall unterstützt und hält die Verbindung zwischen Client sowie Server aufrecht, damit über den DXL auf die neuesten Informationen zugegriffen werden kann. Bei Veränderungen in der veröffentlichenden oder empfangenden Anwendung isoliert die DXL-Abstraktionsebene den Rest der Bereitstellung von der Veränderung, was das Risiko und die Kosten der Integrationsverwaltung senkt.

Bessere Cyber-Sicherheit

Der Zugriff auf bisher nicht verfügbare minutengenaue Daten ist eine bahnbrechende Neuerung im Sicherheitsbereich. Ihre Analysten, Sicherheitsverantwortlichen und Prozessteams sind darauf angewiesen, Daten innerhalb kürzest möglicher Zeit zu erhalten, zu analysieren und geeignete Maßnahmen zu ergreifen. Ihre Anbieter und Entwickler würden das gern unterstützen, doch die Integration wird häufig durch technische Komplexität oder Abhängigkeiten von den geschäftlichen Partnerschaften Ihres Anbieters behindert.

Diesen Hindernissen wird nun ein Ende bereitet, sodass die Kontrolle und Wahl wieder in Ihren Händen liegt.

Ihre Sicherheitsprozesse können sofort von Daten wie den folgenden profitieren:

- Bedrohung durch Täuschungsereignisse
- Veränderung der Datei- und Anwendungsreputation
- Erkennung von Mobilgeräten und Ressourcen
- Veränderungen beim Netzwerk- und Nutzerverhalten
- Präzise Warnungen
- Daten zu Schwachstellen und Kompromittierungsindikatoren

Für Software- und Lösungsanbieter ist DXL ein leistungsfähiges Framework, das Sicherheits- und IT-Maßnahmen unterstützt sowie die Einführung neuer Funktionen in ihrer Software und in den Unternehmen ihrer Kunden erlaubt. Neue Datentypen können komplexere Analysen ermöglichen. Die daraus gewonnenen Schlussfolgerungen führen unverzüglich zu Eskalationen, Eindämmungen, Behebungen oder Eingriffen. Der Echtzeit-Austausch von Daten und die nahezu reibungslose Prozessintegration ergeben gänzlich neue Möglichkeiten.

Weitere Informationen

Starten Sie noch heute durch – unter **www.mcafee.com/de/solutions/data-exchange-layer.aspx**.

McAfee
Together is power.

Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 3707 0
www.mcafee.com/de

McAfee und das McAfee-Logo sind Marken oder eingetragene Marken von McAfee, LLC oder seinen Tochterunternehmen in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer. Copyright © 2018, McAfee, LLC. 4131_1018 OKTOBER 2018