Data Exchange Layer

Intégration simple des applications, de type « un-à-plusieurs », et communication instantanée

Les entreprises et les développeurs peuvent désormais communiquer, partager des données et orchestrer des tâches de sécurité entre les applications en toute facilité, au moyen d'une structure d'applications en temps réel. Un nouveau kit de développement logiciel (SDK) ouvert limite les tâches d'intégration, l'instabilité et les retards qui entravent souvent l'efficacité de la cybersécurité.

Vous payez probablement des frais d'intégration. Les intégrations 1-à-1, les scripts manuels et les processus planifiés sont les trois méthodes les plus souvent employées par les équipes de sécurité et leurs fournisseurs pour connecter des applications. Ces tactiques entravent souvent l'efficacité, la précision et la rapidité dont les équipes de cybersécurité ont besoin pour atteindre un niveau de performance optimal. Elles limitent votre capacité à partager la cyberveille, à enquêter sur les incidents et à orchestrer la réponse.

En quoi consistent exactement ces obstacles ? Jusqu'à présent, il manquait au secteur de la sécurité une méthode simple et sûre pour partager les données en continu et en temps réel.

- L'infrastructure informatique et de sécurité a été progressivement construite à partir de technologies et de fournisseurs disparates, ainsi que d'applications développées en interne.
- Les intégrations de produits point-à-point et pilotées par des API constituent des processus fastidieux et difficiles à développer et à gérer lorsque vous devez constamment mettre à niveau les produits et les formats de données.
- Pour que deux produits de sécurité puissent être intégrés, il faut que leurs fournisseurs respectifs négocient, s'entendent et implémentent cette intégration.
- Les modèles conventionnels d'interrogation et de publication planifiée de données rallongent le temps nécessaire à l'exécution de chaque transaction.

Une norme et un écosystème ouverts

Il existe heureusement une méthode plus efficace, en passe de devenir une norme sectorielle ouverte dans le cadre du projet Open Data Exchange Layer (OpenDXL). Le projet OpenDXL a notamment pour objectif d'accroître la souplesse, la simplicité et les

Laissez DXL révolutionner votre dynamique de sécurité

- **Raccourcissez les workflows du cycle de défense contre les menaces :** Le partage en temps quasi réel des informations et l'orchestration des tâches permettent de diminuer le temps nécessaire à la détection, au confinement et à la neutralisation des nouvelles menaces identifiées.
- **Limitez les délais, les tâches et la complexité de l'intégration entre plusieurs fournisseurs et produits de sécurité :** Notre plate-forme ouverte permet de connecter des produits de sécurité émanant de plusieurs fournisseurs avec vos propres applications et outils, sans aucun délai. Vous bénéficiez d'un véritable contrôle et choix en matière d'intégration.

opportunités d'intégration pour les développeurs, mais aussi d'améliorer les opérations de sécurité pour les entreprises qui le déploient. Le projet OpenDXL fournit aux nouveaux développeurs et participants un kit de développement logiciel pour étendre l'accès et l'utilisation de Data Exchange Layer (DXL), et augmenter ainsi la valeur d'une intégration ou d'un déploiement DXL de façon exponentielle.

Les développeurs utiliseront le kit de développement logiciel pour créer ou connecter des applications qui s'exécutent sur la structure de communication DXL. Celle-ci offre une méthode sûre pour orchestrer les données et les actions en temps réel entre des applications multiples provenant de différents fournisseurs et des applications développées en interne. Elle permet d'éviter les intégrations ponctuelles et à répétition entre deux produits.

Les applications n'ont qu'à publier et s'abonner à des fils de messages ou à passer des appels aux services DXL dans le cadre d'une invocation de type requête-réponse similaire aux API REST. La structure transmet immédiatement tous les messages et appels, connectant ainsi votre système de sécurité, votre environnement informatique et vos solutions internes au sein d'un système parfaitement opérationnel. OpenDXL inclut le client et le broker DXL à code source libre : OpenDXL Client et OpenDXL Broker. L'entreprise dispose ainsi d'un véritable modèle à code source libre pour la couche de communication entre les outils et les sources de cyberveille.

Depuis les débuts de DXL en 2014, les applications de plus de 30 éditeurs ont rejoint l'écosystème DXL avec quelque 100 intégrations. Les entreprises, les fournisseurs de services et les organismes publics l'utilisent déjà pour améliorer le processus décisionnel et réduire le délai d'application de mesures. En plus de diminuer les charges d'exploitation et de rationaliser la protection et la réponse aux incidents, la plate-forme permet à l'équipe de sécurité de se libérer des tâches manuelles et autres interventions tactiques urgentes.

Une seule intégration pour gouverner toutes les applications

À la différence des intégrations standard, chaque application est connectée à la structure de communication DXL universelle. Il n'existe qu'un seul processus d'intégration et non plusieurs. OpenDXL prend en charge un large éventail de langages afin de permettre aux développeurs de créer des intégrations dans leur environnement de développement de prédilection. Une application publie un message ou appelle un service, et une ou plusieurs applications consomment ensuite le message ou répondent à la demande de service. Comme c'est le cas pour n'importe quelle norme, l'interaction est indépendante de l'architecture propriétaire sous-jacente de chaque technologie à intégrer. Les intégrations sont beaucoup plus simples à réaliser grâce à l'abstraction des API et des exigences spécifiques aux fournisseurs.

- **Apportez une valeur ajoutée aux applications que vous déployez :** Les applications peuvent désormais partager toutes les informations utiles qu'elles collectent et génèrent sur les menaces mais aussi fournir des recommandations et appliquer des mesures sans délai.

En plus de créer des intégrations DXL natives, les développeurs peuvent également intégrer leurs services afin qu'ils interagissent entre eux ou encapsuler l'API d'un produit commercial pour publier des données sur la plate-forme DXL. D'autres services peuvent écouter les messages et appels DXL pour enrichir leurs fonctionnalités avec les données les plus récentes ou appliquer les mesures appropriées. Dans le cas d'une application plus sophistiquée, par exemple un outil d'orchestration, il est possible d'écrire un script pour enchaîner une série d'actions.

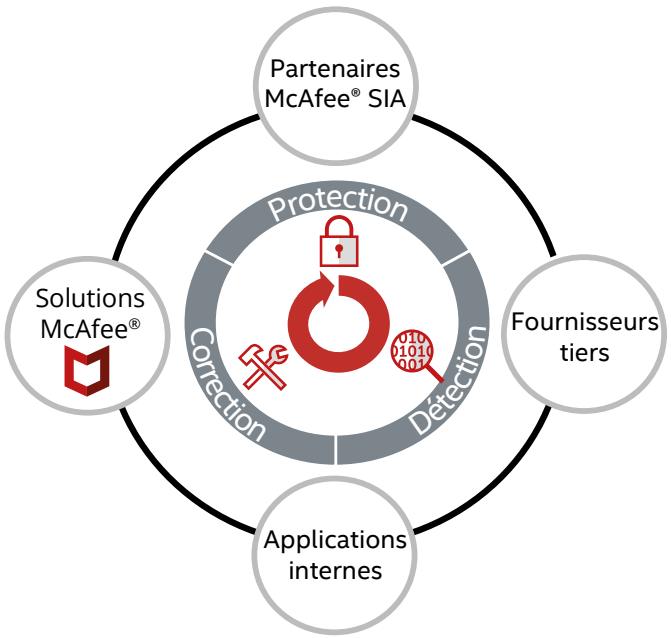

Figure 1. DXL fournit un modèle d'intégration rapide et une structure de communication en temps réel.

Les entreprises déploient une couche de communication et d'intégration standardisée sur leur réseau existant, avec un client DXL léger sur chaque hôte et un service de courtage DXL qui gère les échanges de messages. Tout le trafic DXL reste dans le réseau de l'entreprise afin de garantir la confidentialité des données et de garder le contrôle des opérations. Un modèle compatible avec les pare-feux maintient une connexion entre le client et le serveur pour garantir un accès continu aux dernières informations acheminées vers la plate-forme DXL. En cas de modification de l'application qui publie ou reçoit le message, la couche d'abstraction DXL isole le reste du déploiement de la modification, ce qui réduit les risques et les coûts de gestion des intégrations.

Moteur de cybersécurité optimisé

L'accès à des types jusque-là non disponibles de données toujours à jour va révolutionner le secteur de la sécurité. Les analystes et les équipes opérationnelles et d'intervention cherchent constamment à réduire les délais nécessaires pour obtenir et analyser les données et appliquer des mesures de correction. Les fournisseurs et les développeurs aimeraient leur faciliter la tâche mais l'intégration est parfois bloquée par des complexités techniques ou des dépendances liées aux partenariats du fournisseur.

En éliminant ces obstacles, DXL vous permet de retrouver le contrôle de vos opérations de sécurité.

Celles-ci peuvent désormais exploiter directement les données, par exemple :

- Événements liés à des menaces de fraude
- Modification du score de réputation des fichiers et des applications
- Découverte des terminaux mobiles et des ressources
- Modification du comportement des utilisateurs et du réseau
- Alertes de haute fidélité
- Données sur les vulnérabilités et les indicateurs de compromission

Les éditeurs de solutions et de logiciels doivent considérer DXL comme une structure de communication performante, capable d'accélérer les activités informatiques et de sécurité et de favoriser la mise en œuvre de nouvelles fonctionnalités dans leurs logiciels et les entreprises de leurs clients. Les nouveaux types de données peuvent servir à alimenter des analyses plus complexes. Les conclusions de ces analyses peuvent immédiatement se traduire par une remontée d'incident, un confinement, une intervention ou l'application de mesures correctives. Le partage en temps réel des données et l'intégration fluide des processus permettent d'envisager une myriade de nouvelles opportunités.

En savoir plus

Pour vous lancer, consultez la page **www.mcafee.com/fr/solutions/data-exchange-layer.aspx**.

McAfee
Together is power.

11-13 Cours Valmy - La Défense 7
92800 Puteaux, France
+33 1 4762 5600
www.mcafee.com/fr