Data Exchange Layer

Facile integrazione fra numerose app e comunicazioni istantanee

Imprese e sviluppatori possono ora connettersi facilmente, condividere i dati e orchestrare le attività di sicurezza fra le varie applicazioni usando un framework applicativo in tempo reale. Un nuovo kit di sviluppo software (SDK) aperto riduce gli sforzi di integrazione, le fragilità e i ritardi che abbassano l'efficienza della sicurezza informatica.

Probabilmente stai pagando una tassa occulta per l'integrazione. Le integrazioni fra singole app, gli script manuali e i processi pianificati sono le tre modalità più comuni con le quali i team della sicurezza e i loro fornitori collegano le applicazioni. Questi metodi sono degli ostacoli per l'efficienza, l'accuratezza e la velocità di cui necessitano i team di sicurezza informatica per raggiungere le massime prestazioni. Limitano quindi la tua capacità di condividere le informazioni sulle minacce, di indagare gli eventi e di orchestrare la risposta.

Qual è il problema? L'industria della sicurezza non possedeva un modo semplice e sicuro per condividere i dati continuamente e in tempo reale.

- Per molti anni la sicurezza e l'infrastruttura informatica sono state realizzate a partire dalle tecnologie, dai fornitori e dalle applicazioni interne più disparati.
- Le integrazioni di prodotto da punto a punto, basate sulle API, sono lunghe da realizzare e difficili da mantenere, perché bisogna effettuare l'upgrade di svariati prodotti e formati di dati.
- Perché due prodotti di sicurezza possano integrarsi, i due rispettivi fornitori devono negoziare, trovare un accordo e implementarlo.
- I tradizionali modelli di pubblicazione dati, su richiesta e pianificata, allungano i tempi di ogni transazione.

Uno standard e un ecosistema aperti

C'è un modo migliore, che sta diventando uno standard aperto del settore, per mezzo dell'iniziativa Open Data Exchange Layer (OpenDXL). Gli obiettivi dell'iniziativa OpenDXL sono quelli di incrementare la flessibilità dell'integrazione, la semplicità e le opportunità per gli sviluppatori, oltre che di migliorare le operazioni di sicurezza per le aziende che la adottano. La prima fase dell'iniziativa OpenDXL fornisce un SDK per espandere l'accesso e l'utilizzo di Data Exchange Layer (DXL) da parte di nuovi sviluppatori e partecipanti, aumentando così esponenzialmente il valore di un'integrazione o distribuzione di DXL.

DXL cambia le dinamiche della tua sicurezza

Abbrevia i flussi di lavoro del ciclo di vita delle difese contro le minacce
La condivisione delle informazioni e il coordinamento delle attività in modo pressoché istantaneo riduce le tempistiche necessarie per rilevare, contenere e correggere le minacce appena identificate.

Riduce i ritardi, gli sforzi e la complessità dell'integrazione dei diversi prodotti e fornitori di sicurezza
La nostra piattaforma aperta ti permette di connettere i prodotti di sicurezza di più fornitori con le tue applicazioni e i tuoi strumenti, senza dover negoziare con i fornitori stessi. La scelta è nelle tue mani.

Aumenta il valore delle applicazioni che utilizzi
Le applicazioni possono ora condividere gli utili dati sulle minacce da esse generati e guidare o eseguire immediatamente le azioni.

Gli sviluppatori useranno questo SDK per creare o connettere le applicazioni che vengono eseguite nel tessuto di comunicazioni DXL, come modo sicuro e in tempo reale per orchestrare dati e azioni su molteplici applicazioni di diversi fornitori, oltre che su quelle sviluppate internamente. Evitiamo la ripetizione delle singole integrazioni da prodotto a prodotto.

Le app semplicemente pubblicano e si abbonano agli argomenti dei messaggi oppure fanno delle chiamate ai servizi DXL in un richiamo di tipo richiesta/risposta simile alle API RESTful. Il tessuto invia messaggi e chiamate immediatamente, connettendo sicurezza, infrastruttura informatica e soluzioni sviluppate internamente in un sistema dal funzionamento ottimale.

A partire dal debutto di DXL nel 2014, nell'ecosistema DXL sono entrate le applicazioni di decine di fornitori. Grandi imprese, fornitori di servizi e organizzazioni governative già lo usano per migliorare le decisioni e agire in meno tempo. Questo abbassa i costi operativi, semplifica la protezione e la risposta, liberando le preziose risorse del team di sicurezza dalle attività manuali e dalle esercitazioni di emergenza tattiche.

Una sola integrazione per tutto

A differenza delle tipiche integrazioni, ogni applicazione si connette al tessuto di comunicazioni DXL universale. Anziché tanti sforzi c'è un solo processo di integrazione. OpenDXL supporta un'ampia gamma di linguaggi, così gli sviluppatori possono creare le integrazioni usando l'ambiente di sviluppo che preferiscono. Un'app pubblica un messaggio oppure richiama un servizio; una o più app consumano il messaggio oppure rispondono alla richiesta di servizio. Come ogni standard che si rispetti, l'interazione è indipendente dall'architettura brevettata alla base di ciascuna tecnologia di integrazione.
Le integrazioni sono molto più semplici grazie a questa astrazione dalle API e dai requisiti specifici di un fornitore.

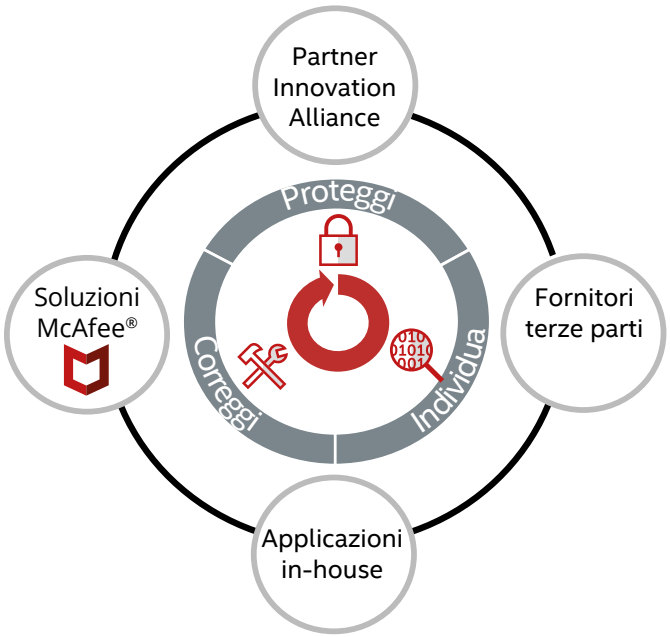

Figura 1. DXL offre un modello di integrazione rapida e un tessuto di comunicazioni in tempo reale.

In aggiunta alla creazione di integrazioni DXL native, gli sviluppatori possono anche eseguire il wrapping dei propri servizi, in modo che interagiscano o eseguano il wrapping dell'API di un prodotto in commercio, per pubblicare i dati in DXL. Altri servizi possono ascoltare i messaggi e le chiamate DXL per arricchire le proprie funzionalità con i dati più recenti o per prendere le

misure appropriate. Per un'app più sofisticata che rifletta l'orchestrazione, questo tipo di azioni può essere riunito in uno script per avviare una serie di azioni consecutive o simultanee.

Le grandi imprese impiegano un'integrazione standardizzata e un livello di comunicazione sulla loro rete esistente, con un piccolo client DXL su ogni host e un broker DXL che gestisce gli scambi di messaggi. Tutto il traffico DXL è contenuto nella rete dell'impresa, offrendo la riservatezza dei dati e il controllo delle operazioni. Un modello a misura di firewall mantiene la connessione fra client e server per l'accesso continuo alle ultime informazioni che scorrono nel DXL. Se qualcosa nell'applicazione di pubblicazione o ricezione cambia, il livello di astrazione DXL isola il resto della distribuzione da tale modifica, riducendo i rischi e i costi associati alla manutenzione dell'integrazione.

Un motore di sicurezza informatica migliore

L'accesso ai tipi di dati aggiornati al minuto, precedentemente non disponibili, cambia le prospettive per la sicurezza. I tuoi analisti, il personale di intervento e quello operativo sono già ansiosi di ottenere, analizzare e prendere delle misure in base ai dati nel minor tempo possibile. I tuoi fornitori e sviluppatori vorrebbero dare una mano, ma l'integrazione può impantanarsi in complessità tecniche oppure nella dipendenza dalle partnership aziendali dei fornitori stessi.

Questi ostacoli ora cadono, rimettendo il potere di scelta nelle tue mani.

Ora le tue operazioni di sicurezza possono avere vantaggi immediati dai dati come:

- inganno delle minacce;
- variazioni alla reputazione di file e applicazioni;
- scoperta di dispositivi mobili e risorse;
- variazioni della rete e dei comportamenti dell'utente;
- avvisi ad alta fedeltà;
- dati sulle vulnerabilità e indicatori di compromissione.

I fornitori di software e soluzioni dovrebbero guardare a DXL come a un framework potente per velocizzare le attività informatiche e di sicurezza e per attivare nuove capacità nei propri software e nelle organizzazioni dei rispettivi clienti. Nuovi tipi di dati alimentano analisi più complesse. Le conclusioni fanno scattare immediatamente l'inoltro del caso, il contenimento, la remediation o l'intervento. Quando si guarda tramite la lente della condivisione in tempo reale dei dati e di un processo di integrazione pressoché senza attriti, si intravedono delle nuove opportunità.

Ulteriori informazioni

Inizia da **www.mcafee.com/it/solutions/data-exchange-layer.aspx**.

McAfee
Together is power.

Via Fantoli, 7
20138 Milano
Italy
(+39) 02 554171
www.mcafee.com/it