OpenDXL Ontology : une langue commune pour les logiciels de sécurité

En octobre 2019, une quinzaine de fournisseurs de solutions de sécurité fondaient, sous la houlette d'IBM et de McAfee, l'Open Cybersecurity Alliance.

Celle-ci vient de communiquer sur le premier fruit de ses travaux : Ontology.

Le projet se fonde sur le bus de données DXL (Data Exchange Layer), que McAfee avait lancé en 2014 pour favoriser l'intégration d'applications de sécurité.

L'initiative OpenDXL, amorcée en 2016, vise à faire de cette structure de communication une norme sectorielle ouverte.
Objectif : permettre aux applications de publier et de s'abonner à des fils de messages. Ou de passer des appels aux services DXL dans le cadre de requêtes-réponses sur le modèle des API REST.

Ontology se greffe à OpenDXL pour offrir un langage commun facilitant l'échange d'informations et d'actions entre applications. Il englobe pour cela plusieurs standards ouverts, dont OpenC2.

Les « actions » d'Ontology s'apparentent aux « commandes » d'OpenC2. Mais elles tirent parti d'OpenDXL. Ce en permettant en particulier de transmettre une action qui agit sur plusieurs services. Exemple : une mise en quarantaine à laquelle réagiraient à la fois un pare-feu et un système de tickets.

Au-delà des « actions », Ontology prend en charge les « notifications », types d'alertes qui n'ont pas d'équivalent sur OpenC2.

Un tel langage commun évite entre autres d'avoir à mettre les intégrations OpenDXL à jour lorsque des produits de sécurité évoluent.

L'Open Cybersecurity Alliance approche de la trentaine de membres. Elle développe en parallèle STIX Shifter.
Cette bibliothèque Python s'appuie le le langage sérialisé STIX (Structured Threat Information eXpression). Elle permet aux applications de sécurité de se connecter à des bases de données pour y effectuer des recherches.