

Vectra est le leader mondial

de la détection et neutralisation en temps réel des cyberattaques avancées grâce à l'intelligence artificielle

Vectra®, leader de la détection réseau et de l'aide à la résolution des incidents, révolutionne la sécurité réseau grâce à la plateforme Cognito®. Elle remplace avantageusement les anciennes technologies qui peinent à relever les défis actuels en matière de détection et d'aide à la résolution des incidents — du cloud jusqu'aux centres de données, aux appareils connectés ou aux terminaux des utilisateurs.

La plate-forme Cognito

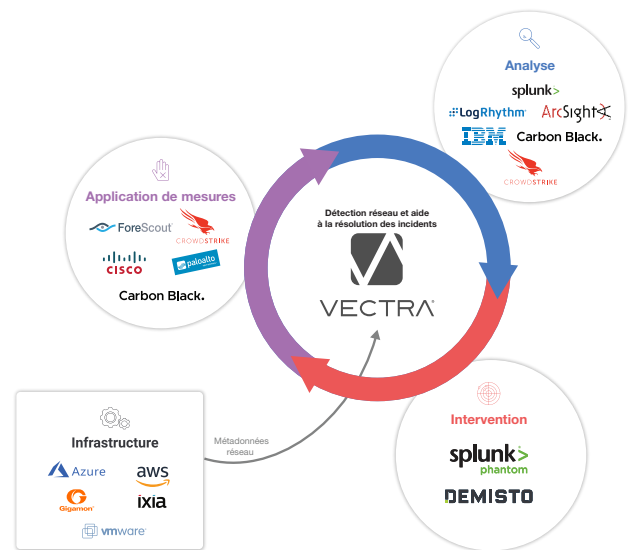
La plate-forme Cognito accélère la détection et l'analyse des menaces grâce à une technologie d'intelligence artificielle sophistiquée permettant de collecter, stocker et enrichir des métadonnées réseau avec des données contextuelles pertinentes. Objectif : détecter, traquer et analyser les menaces connues et inconnues en temps réel.

La plate-forme Cognito est capable de gérer efficacement les plus grands réseaux d'entreprise avec architecture distribuée prenant en charge un large éventail de capteurs physiques, virtuels et cloud, afin d'offrir une vue à 360° sur le cloud, les centres de données, les appareils connectés et les terminaux des utilisateurs.

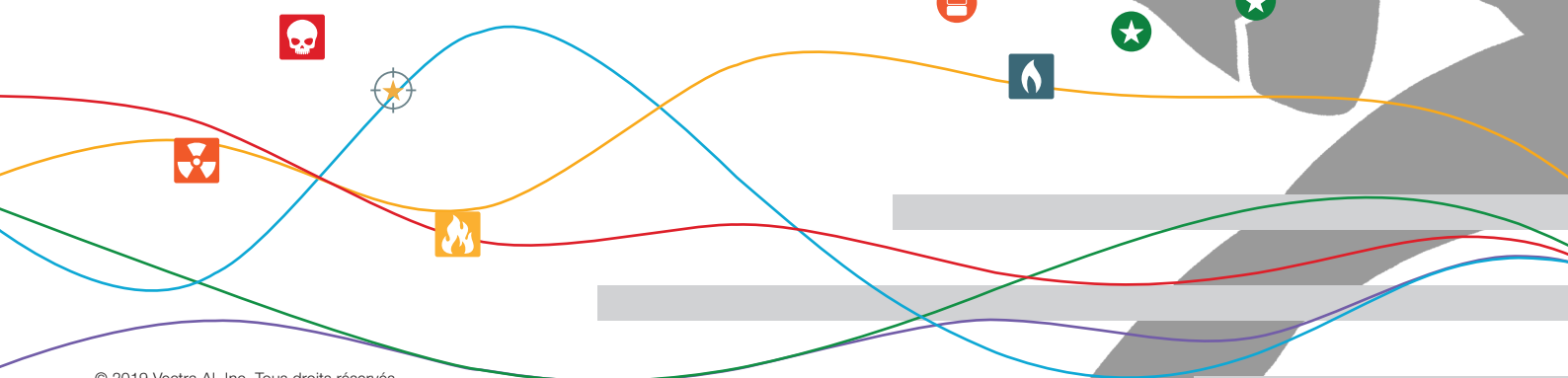
Sur la plate-forme Cognito, Vectra propose trois applications qui permettent de résoudre les cas d'utilisation à priorité élevée. Cognito Stream™ envoie des métadonnées enrichies par des informations de sécurité aux lacs de données et aux solutions SIEM. Cognito Recall™ est une application cloud permettant de stocker des métadonnées enrichies et d'analyser les menaces. Cognito Detect™ s'appuie sur l'intelligence artificielle pour identifier rapidement les cyberpirates inconnus et furtifs et gérer le problème selon une échelle de priorités appropriée.

Des données pertinentes pour la détection des menaces et l'aide à la résolution des incidents

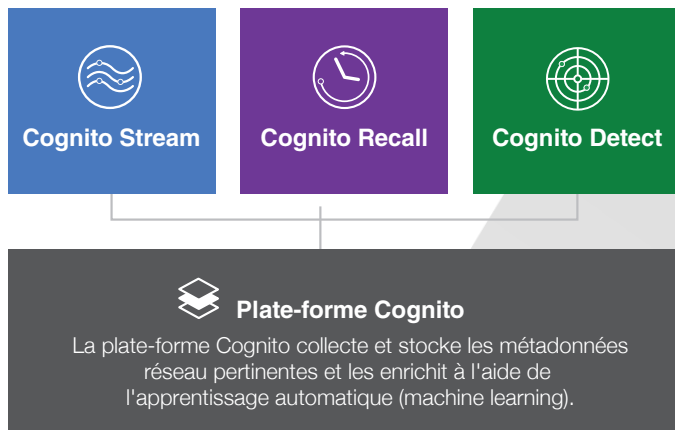
Cognito s'appuie sur la seule source d'informations fiables lors d'une cyberattaque : le trafic réseau. Seul ce trafic — qu'il transite dans des clouds publics, des centres de données privés ou des environnements d'entreprise — fournit des indications totalement fiables et objectives. Les cyberpirates peuvent supprimer des journaux, mais sont incapables d'effacer leur empreinte sur le réseau.



Je suis l'intelligence artificielle.
Je suis le moteur de la lutte contre les cyberpirates.
Je suis Cognito.



Cognito est une plate-forme de détection des menaces et d'aide à la résolution des incidents



Cognito Stream : des métadonnées réseau enrichies

Envoie des métadonnées enrichies à un lac de données ou à une solution SIEM

Données réseau exploitables

Cognito Stream extrait des centaines d'attributs de métadonnées à partir du trafic réseau brut et les présente dans un format Zeek compact et facile à comprendre, qui tire parti des outils logiciels existants.

Informations de sécurité intégrées

Les informations de sécurité générées par l'apprentissage automatique sont incorporées aux métadonnées en vue de fournir des composants puissants aux spécialistes en traque des menaces, qui peuvent alors les exploiter grâce à leurs compétences particulières pour obtenir rapidement des résultats.

Analyses basées sur les systèmes, et pas uniquement sur les adresses IP

Cognito Stream associe automatiquement les métadonnées réseau avec d'autres attributs afin de créer une identité de système unique. Cela permet aux analystes en sécurité d'investiguer efficacement les systèmes indépendamment des changements d'adresses IP, mais aussi d'explorer les relations entre les groupes de systèmes.



E-mail : Info_France@vectranetworks.com / info_DACH@vectranetworks.com Téléphone : +41 43 810 47 52 / +33 (0)6 29 12 41 19 vectra.ai

© 2019 Vectra AI, Inc. Tous droits réservés. Vectra, le logo Vectra AI, le slogan « Security that thinks » et Cognito sont des marques commerciales déposées ; Cognito Detect, Cognito Recall, Vectra Threat Labs et Threat Certainty Index sont des marques commerciales de Vectra AI. Les autres noms de marque, de produit ou de service sont des marques commerciales, des marques commerciales déposées ou des marques de service de leurs propriétaires respectifs.

J'offre une vue à 360° sur votre cloud, vos appareils connectés et vos réseaux d'entreprise, ce qui ne laisse aucune chance aux cyberpirates.

Cognito Recall : conçu pour l'analyse et la traque des menaces

Application cloud destinée à stocker et à analyser des métadonnées enrichies

Des spécialistes en traque des menaces mieux armés

La collecte et le stockage en temps réel de métadonnées réseau enrichies, de journaux pertinents et d'événements cloud permettent aux spécialistes en traque des menaces de tirer parti de connaissances approfondies sur les cyberpirates chevronnés.

Analyse intelligente des activités des équipements

Cognito Recall associe les métadonnées réseau à des équipements, et pas uniquement à des adresses IP. Il offre une visibilité instantanée sur les activités des équipements au fil du temps, indépendamment des changements d'adresses IP.

Couverture illimitée, optimisée par le cloud

Les spécialistes en traque des menaces peuvent s'appuyer sur des métadonnées réseau enrichies qui sont stockées et consultables aussi longtemps que nécessaire, pendant que Vectra gère l'infrastructure.

Cognito Detect : l'intelligence artificielle au service de la détection des menaces et d'une gestion raisonnée des incidents

Identification rapide des cyberpirates inconnus et furtifs grâce à l'intelligence artificielle

Détection des menaces optimisée par l'intelligence artificielle

Les modèles d'analyse comportementale à apprentissage continu s'appuient sur l'intelligence artificielle pour identifier efficacement les cyberpirates inconnus et furtifs, afin de permettre l'application de mesures rapides et déterminantes et de fournir un point de départ clair pour l'analyse des incidents.

Données contextuelles pertinentes en temps réel

Cognito Detect accélère la traque et la détection des cyberattaques avancées. La solution permet en outre l'application de mesures immédiates en fournissant aux analystes en sécurité les données contextuelles les plus pertinentes de manière proactive.

Multiplicateur de force pour les investissements de sécurité existants

Cognito Detect vient compléter la détection des menaces et l'aide à la résolution des incidents, le contrôle de l'accès au réseau, les pare-feux et les autres points d'application de stratégies. Il permet ainsi de bloquer de nouvelles catégories de menaces et de fournir un point de départ pour l'analyse des incidents au sein de Cognito Recall, des lacs de données et des solutions SIEM.