VECTRA®

Cognito Stream : des métadonnées réseau enrichies d'informations pertinentes

PRINCIPAUX ATOUTS

- Transfert des métadonnées pouvant faire l'objet de recherches au format Zeek vers le magasin de données de votre choix, avec prise en charge de Kafka, syslog et Elastic
- Métadonnées enrichies par des informations de sécurité pour simplifier les investigations
- Création d'outils et modèles personnalisés afin de détecter, analyser et traquer les menaces
- Exploitation de tous les outils Zeek existants
- Corrélation des métadonnées réseau et cloud et des données des systèmes et équipements de votre lac de données (p. ex. journaux d'applications, processus, mémoire)
- Simplicité du déploiement : aucune optimisation des performances ni maintenance continue nécessaire
- Performances plus de 5 fois supérieures à celles du capteur unique Zeek

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

Cognito Stream™ de Vectra® fournit des métadonnées évolutives, enrichies par des informations de sécurités et issues du cloud natif, du cloud hybride et du trafic d'entreprise. Objectif : permettre aux analystes en sécurité et aux spécialistes en traque des menaces de mener des investigations concluantes sur les incidents.

Aujourd'hui, les données de sécurité sont morcelées. NetFlow est incomplet, tandis que les captures de paquets exigent une puissance de traitement et un espace de stockage importants. Les entreprises qui décident de déployer et gérer l'infrastructure d'analyse open source Zeek doivent consacrer beaucoup de temps et de ressources à l'assemblage et à la configuration du matériel, à la configuration des logiciels et à l'intégration dans les outils existants. Pour les responsables de la sécurité, une telle situation est intenable.

Grâce à Cognito Stream, les équipes de sécurité ont toutes les données contextuelles réseau riches nécessaires pour créer des outils personnalisés et alimenter les modèles de détection, d'investigation et de traque. Fournies au format Zeek open source, les informations de sécurité sont intégrées en toute transparence dans les lacs de données et les SIEM sans la charge administrative et les limitations d'échelle généralement associées au format Zeek open source.

Les métadonnées de Cognito Stream intègrent en outre l'identité du système, ce qui permet de mener des investigations basées sur les noms des équipements et pas uniquement les adresses IP. Il n'est donc plus nécessaire d'examiner en parallèle les journaux DHCP pour identifier le système qui utilisait l'adresse IP concernée à des moments spécifiques. De même, il ne faut plus surveiller les changements d'adresse IP pendant la période visée par l'investigation. La recherche par nom de système représente un gain de temps précieux lorsque chaque minute compte. Les informations de sécurité incorporées dans les métadonnées offrent aux spécialistes en traque des menaces la cyberveille dont ils ont besoin pour les investigations et la traque des menaces.

Traque des menaces et investigation d'incidents plus performantes

- **Données réseau exploitables au format Zeek.** Cognito Stream extrait des centaines d'attributs de métadonnées collectés dans le cloud et l'ensemble de l'entreprise, et les présente dans un format Zeek compact et facile à comprendre, qui tire parti des outils existants. À l'inverse de NetFlow, Cognito Stream fournit aux analystes tous les détails dont ils ont besoin, sans la complexité de stockage associée à la capture de paquets complets.
- **Informations de sécurité intégrées.** Les informations de sécurité générées par l'apprentissage automatique sont incorporées aux métadonnées (p. ex. activités de balisage, prévalence des domaines) en vue de fournir des éléments utiles 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 sur les adresses IP.** Cognito Stream associe automatiquement les métadonnées réseau à 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 parmi les groupes de systèmes.

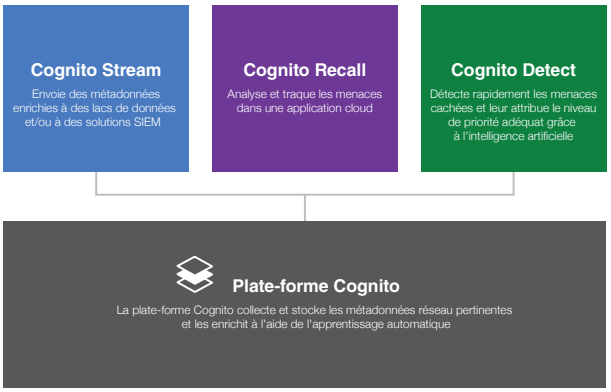
- **Simplicité d'emploi grâce à une configuration unique.** Cognito Stream est configuré en moins de 30 minutes, n'exige aucune optimisation des performances ni maintenance continue et affiche des performances plus de cinq fois supérieures à celles du capteur unique de Zeek. Libérées de la charge de gestion de l'infrastructure Zeek open source, les équipes de sécurité peuvent ainsi se concentrer sur les investigations.

La plate-forme Cognito

Données pertinentes et contextualisées

Vectra, leader de la détection réseau et de l'aide à la résolution des incidents, révolutionne la sécurité réseau grâce à la plate-forme Cognito®. Celle-ci 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 IoT ou aux terminaux des utilisateurs.

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 IoT et les terminaux des utilisateurs.

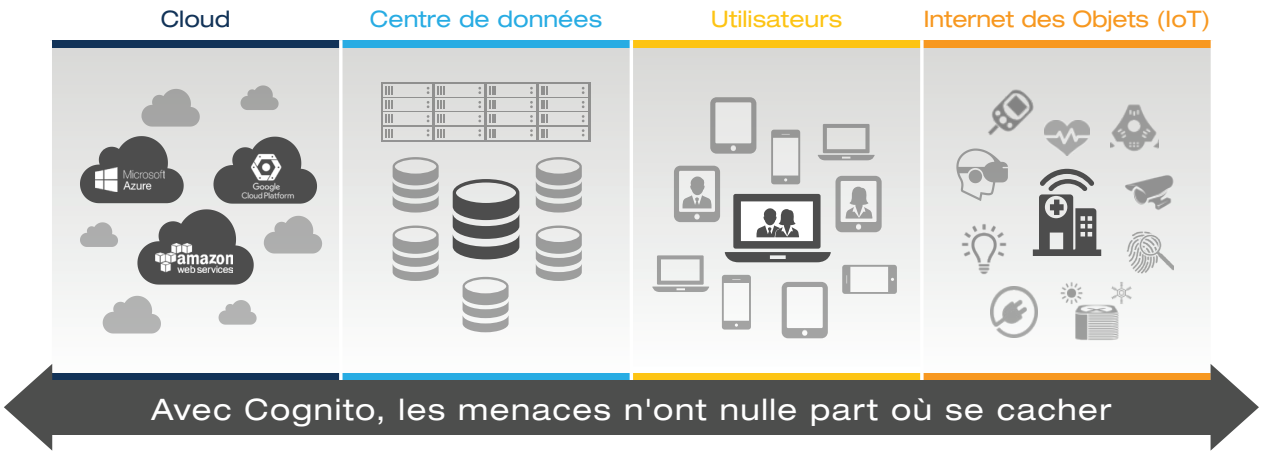
Sur la plate-forme Cognito, Vectra propose trois applications qui permettent de résoudre les cas d'utilisation à priorité élevée. Cognito Stream envoie des métadonnées enrichies par des informations de sécurité aux lacs de données et aux solutions SIEM. Cognito Recall™ est une application cloud destinée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

Fonctionnement de Cognito Stream

Transfert de métadonnées enrichies aux lacs de données

Cognito Stream offre une visibilité complète sur le trafic réseau en extrayant les métadonnées de tous les paquets et en les stockant dans votre lac de données ou solution SIEM à des fins de corrélation, recherche et analyse. Il identifie et suit chaque équipement IP connecté au réseau.

Cette visibilité s'étend aux serveurs, ordinateurs portables, imprimantes, équipements personnels et appareils IoT, ainsi qu'aux systèmes d'exploitation et applications, et comprend le trafic entre les charges de travail virtuelles des centres de données et du cloud. Les métadonnées incluent les connexions et les détails relatifs aux protocoles, indispensables pour la traque des menaces et l'investigation des incidents.



Les métadonnées capturées incluent tout le trafic interne (est-ouest) et Internet (nord-sud), ainsi que celui de l'infrastructure virtuelle et des environnements cloud. Cognito Stream transfère les métadonnées indexées aux lacs de données avec prise en charge de Kafka, syslog et Elastic.

Déploiement simplifié à l'aide de la plate-forme Cognito

Les entreprises peuvent déployer la plate-forme Cognito en 30 minutes ou moins et commencer directement à traquer les menaces ou investiguer les incidents sans les frais induits par la gestion de l'infrastructure de capteurs :

- Les capteurs physiques et virtuels collectent les métadonnées en différents points du réseau, par exemple le campus, le centre de données et le cloud.

Les capteurs se connectent à une entité centrale (« centre névralgique ») qui déduplique les flux et exécute les algorithmes d'identification des systèmes et d'enrichissement. Cognito Stream est déployé comme une machine virtuelle sur site. La machine virtuelle normalise les métadonnées au format Zeek et les transfère vers une solution SIEM ou un lac de données hébergé sur site ou dans le cloud.

Traque des menaces

Il existe plusieurs sources possibles d'indicateurs de compromission : ils peuvent être repérés par l'analyste dans le cadre de son travail quotidien ou provenir d'une cyberveille partagée ou de recherches internes. La recherche d'indicateurs de compromission dans les métadonnées réseau enrichies permet à un analyste d'identifier rétrospectivement les adresses IP, les domaines, les URL, les hachages et les certificats SSL utilisés au cours d'une cyberattaque. Grâce à une conservation des métadonnées à long terme, la recherche des indicateurs de compromission critiques est très efficace.

Corrélation des données des systèmes et du réseau

Pour que la traque des menaces soit efficace, il faut une visibilité totale sur les ressources informatiques, les risques et les flux au sein du réseau d'entreprise. Les données indispensables pour bénéficier d'une telle visibilité se répartissent en trois catégories :

- Les métadonnées réseau offrent une visibilité sur toutes les communications entre les systèmes, en décrivant les interactions des entités, notamment les utilisateurs, les équipements, les charges de travail, les adresses IP et les domaines d'un réseau. Les spécialistes en traque des menaces se basent sur ces interactions pour identifier les activités d'un cyberpirate dans le réseau.
- Les données des systèmes offrent une visibilité sur les événements survenus sur les systèmes de l'environnement, y compris les activités des comptes d'utilisateur et les processus système.
- Les ensembles de données d'applications sont des événements consignés par les programmes exécutés dans l'environnement.

Les métadonnées réseau offrent à l'analyste une vue globale des comportements et des événements observés dans tout un réseau. Les données des systèmes et des applications (combinées en données d'équipements) offrent des informations granulaires sur les comportements au niveau du système, dont les processus système et les accès mémoire.

Ensemble, ces trois catégories de données offrent une carte complète de l'entreprise, avec une vue multiniveau des événements et des activités. Elles permettent ainsi aux spécialistes en traque des menaces de détecter les menaces avancées.

Création d'outils et modèles personnalisés afin de détecter, analyser et traquer les menaces

Grâce aux détections personnalisées, un analyste peut surveiller des événements afin d'identifier divers types de comportements, par exemple des menaces suspectes ou émergentes, des violations de conformité, des abus internes ou des vecteurs d'attaque spécifiques au secteur. Les informations de sécurité de Cognito Stream offrent des composants d'apprentissage automatique intégrés aux métadonnées qui peuvent être combinés avec d'autres attributs pour créer des modèles personnalisés puissants mis en corrélation avec un système ou un compte d'utilisateur spécifique.

Investigations concluantes sur les incidents

Extrêmement efficace, Cognito Stream permet aux analystes en sécurité de mener des investigations des incidents plus approfondies et concluantes dans une solution SIEM ou un lac de données existant.

En tirant parti des métadonnées réseau enrichies, ces derniers peuvent suivre facilement l'enchaînement d'événements liés dans les détections effectuées par Cognito Detect, les produits de sécurité tiers et une cyberveille fiable et indexée des métadonnées réseau historiques.

Lorsque des incidents sont signalés par Cognito Detect ou d'autres produits de sécurité tiers, Cognito Stream les organise de façon à proposer une vue à 360° de toutes les activités des équipements et des charges de travail.

Avec Cognito Stream, les analystes peuvent investiguer les incidents avec une efficacité sans précédent, en s'appuyant sur des données contextuelles complètes sur les transactions du réseau, ainsi que des détails pertinents sur les équipements, comptes et communications réseau associés.

Pour demander une démonstration, consultez la page vectra.ai/demo

E-mail : info_france@vectra.ai / info_dach@vectra.ai **Téléphone :** +33 62 912 4119 / +41 44 551 0143

vectra.ai