VECTRA®

Cognito Recall, la méthode la plus efficace pour la traque des menaces

PRINCIPAUX ATOUTS

- Visibilité haute fidélité sur toute l'entreprise grâce à la collecte et au stockage de métadonnées réseau riches, de journaux pertinents et d'événements cloud en temps réel
- Traque des menaces rétrospective à l'aide de métadonnées réseau enrichies
- Exploration des incidents déclenchés par les outils de sécurité pour identifier d'autres systèmes, comptes et acteurs externes impliqués dans un incident
- Stockage et recherche de métadonnées sur la période de votre choix avec montée en charge grâce au cloud

Cognito Recall™ de Vectra® est une pierre angulaire de Cognito™, la plate-forme de détection des cyberattaques et de traque des menaces. Cette solution ultraperformante s'appuie sur l'intelligence artificielle pour traquer les menaces ciblant le cloud, les centres de données, les appareils IoT ou les terminaux des utilisateurs.

Source complète de métadonnées réseau enrichies, Cognito Recall permet également aux analystes en sécurité chevronnés et aux spécialistes en traque des menaces de mener des investigations concluantes sur les incidents.

Dans Cognito Recall, les métadonnées sont organisées par nom de système, et pas simplement par adresse IP. Il n'est donc plus nécessaire d'éplucher les journaux DHCP pour identifier le système qui utilisait l'adresse IP concernée au moment de l'incident, pour ensuite répertorier tous les changements d'adresse IP au cours de l'investigation. La recherche par système représente un gain de temps précieux lorsque chaque minute compte.

Cognito Recall permet aux équipes de résolution des incidents de suivre la chaîne des événements depuis la première manifestation de la menace — qu'elle provienne de Cognito Detect™, d'un autre événement de sécurité ou de la cyberveille. Il exploite pour cela des métadonnées réseau enrichies sur lesquelles il est possible d'exécuter des recherches par nom de système.

Cognito Recall ressemble à bien des égards à un registre transactionnel de toutes les conversations au sein de l'entreprise. En revanche, comme il collecte et stocke des métadonnées historiques et non les charges actives des paquets, la confidentialité des données est garantie, de même que le respect de réglementations telles que le RGPD.

En outre, comme Cognito Recall est fourni sous la forme d'un service cloud, les clients n'ont pas besoin d'acheter, d'installer et de gérer une grosse infrastructure de données. Un simple clic permet de transférer les métadonnées vers le cloud Vectra.

Résumé des fonctionnalités

- **Cognito Recall offre aux spécialistes en traque des menaces** des fonctions de collecte et de stockage en temps réel de métadonnées réseau enrichies, journaux pertinents et événements cloud, ce qui leur permet d'exploiter au mieux de leurs connaissances pointues sur les cyberattaques avancées.
- **La solution permet une analyse intelligente des activités liées aux équipements** en associant des éléments tels que les équipements, les charges de travail et les noms des systèmes, indépendamment des changements d'adresse IP.
- **Elle offre une visibilité complète à l'échelle de l'entreprise** sur toutes les charges de travail des centres de données ou du cloud, mais aussi sur les actions liées aux appareils IoT et aux terminaux des utilisateurs.
- **Elle assure une montée en charge illimitée grâce au cloud** qui permet de stocker et lancer des recherches sur les métadonnées aussi longtemps que nécessaire tandis que Vectra se charge de la gestion de l'infrastructure.

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

Cognito Detect et Cognito Recall, l'alliance idéale

Cognito Recall permet aux analystes en sécurité de mener des investigations approfondies en s'appuyant sur les incidents précis et directement exploitables que Cognito Detect a identifiés. Cognito Detect, quant à lui, automatise la détection et l'intervention pilotées par intelligence artificielle en cas de cyberattaque.

Dans un contexte de traque des menaces, Cognito Recall permet aux analystes chevronnés d'employer les alertes déclenchées par des solutions de sécurité tierces et une cyberveille de qualité pour un examen rétrospectif.

	DÉTECTION DES CYBERATTAQUES	INVESTIGATION, TRAQUE OPTIMISÉE PAR L'INTELLIGENCE ARTIFICIELLE
Produit	Cognito Detect	Cognito Recall
Objectif	Identification des systèmes compromis comme point de départ de l'investigation	Investigation manuelle, recherche de menaces non détectées
Portée	Détection initiale → Validation de la détection	Clôture de l'investigation
Besoins	Temps réel, signal fiable et automatisation	Vue à 360° des métadonnées historiques, recherche efficace

Fonctionnement de Cognito Recall

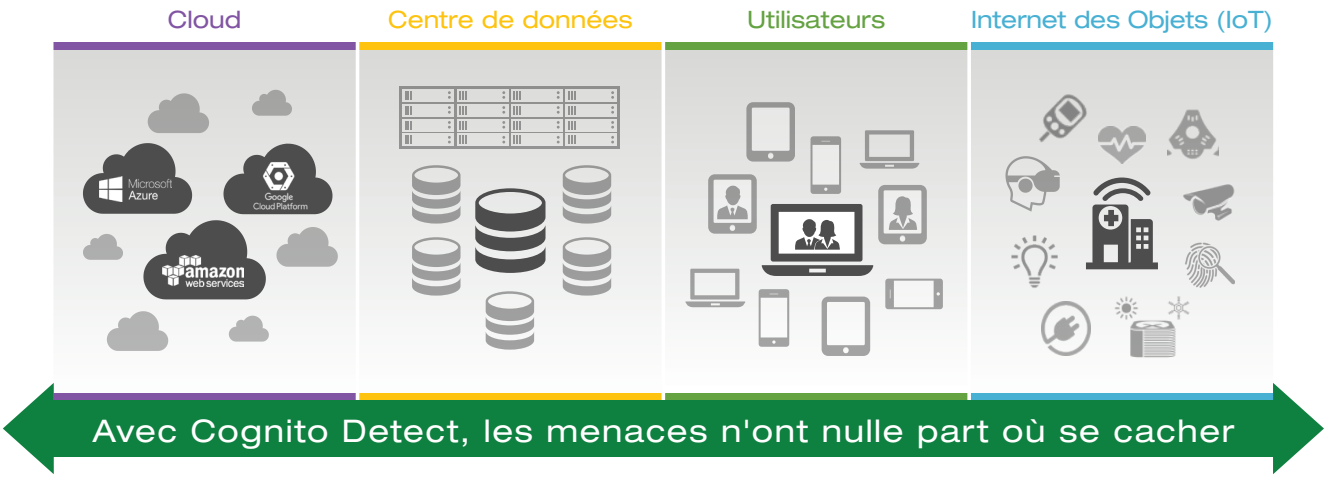
Visibilité haute fidélité dans toute l'entreprise

Cognito Recall offre une visibilité complète sur le trafic réseau en extrayant les métadonnées de tous les paquets et en les stockant dans le cloud à des fins de recherche et d'analyse. Il identifie et suit chaque équipement IP connecté et les données collectées peuvent être stockées pour la durée de votre choix.

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.

Cette visibilité s'étend aux ordinateurs portables, serveurs, imprimantes, équipements personnels et appareils IoT, ainsi qu'aux systèmes d'exploitation et applications. Elle comprend en outre le trafic entre les charges de travail virtuelles des centres de données, du cloud et même des applications SaaS.

Les journaux système, SaaS et d'authentification fournissent des données contextuelles riches à l'analyse des métadonnées réseau, afin de permettre une identification précise des systèmes et des utilisateurs.



Cognito Recall collecte les métadonnées réseau dans toute l'entreprise.

Traque des menaces

La traque des menaces optimisée par l'intelligence artificielle de Cognito Recall peut être déclenchée par les détections d'attaques de Cognito Detect, par des indicateurs de compromission existants et par des anomalies au niveau des données identifiées par les analystes.

Traque axée sur les indicateurs de compromission

Grâce à des fonctionnalités de recherche sur les métadonnées et à un stockage des données illimité, Cognito Recall permet aux analystes en sécurité de déterminer si des indicateurs de compromission sont présents dans les métadonnées, y compris les agents utilisateur, les adresses IP et les domaines.

Cognito Recall propose également des informations détaillées pour optimiser la traque des menaces, notamment les commandes PowerShell envoyées par une machine distante à un serveur, ou un type particulier de connexion provenant d'un site distant.

Cognito Recall propose des fonctionnalités de recherche de métadonnées et un stockage illimité des données.

Traque des comportements anormaux

Cognito Recall offre aux spécialistes en traque des menaces la possibilité d'identifier les comportements anormaux affichés par le biais de graphiques. Parmi les comportements anormaux mis en évidence par Cognito Recall, citons les suivants :

- Utilisation inhabituelle des applications et des ports TCP et UDP
- Taux de connexion anormalement élevés
- Indicateurs heuristiques
- Nouvelles activités de balisage
- Seuils volumétriques des connexions, des échecs de connexion et transferts excessifs de données internes et externes

Dans certains cas, les anomalies peuvent combiner plusieurs des comportements précités, comme un volume anormal de données envoyées à une adresse IP inhabituelle.

Cognito Recall offre aux spécialistes en traque des menaces la possibilité d'identifier les comportements anormaux.

Investigations concluantes sur les incidents

Cognito Recall permet aux analystes en sécurité de mener des investigations des incidents plus approfondies et concluantes avec une efficacité remarquable.

Ils 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.

Lorsqu'il reçoit des alertes ou événements envoyés par Cognito Detect ou d'autres produits de sécurité, Cognito Recall les organise de façon à proposer une vue à 360° de toutes les activités des équipements et des charges de travail.

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

Investigations axées sur les systèmes

Cognito Recall permet d'identifier les activités des systèmes au moment de la détection d'une menace et de mettre en évidence les changements de comportement importants de ceux-ci.

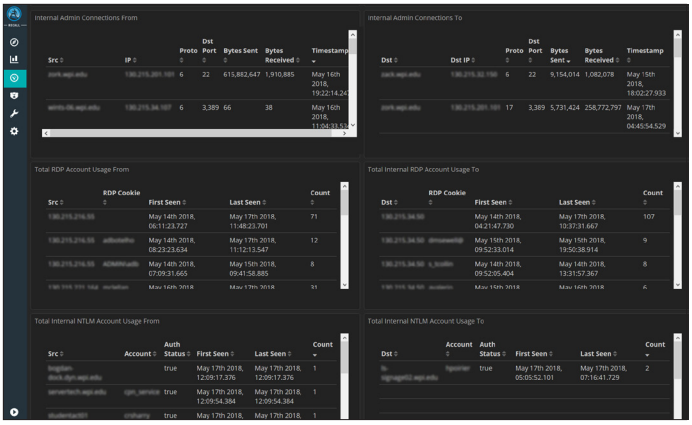
Au moyen de graphiques et de fonctionnalités de recherche, Cognito Recall décèle d'autres systèmes, comptes, domaines et adresses IP externes, ce qui permet d'évaluer l'ampleur de l'incident.

Les analystes en sécurité peuvent ainsi déceler facilement la séquence de comportements suspects et dégager un faisceau de preuves menant à d'autres systèmes, afin d'y rechercher des indicateurs de compromission.

Investigations axées sur les comptes

Cognito Recall améliore les investigations axées sur les comptes, car il fournit les détails nécessaires pour identifier toutes les utilisations et actions des comptes potentiellement compromis au cours des périodes concernées, sans oublier les actions menées contre les cibles.

En outre, Cognito Recall offre un tableau très complet d'une cyberattaque globale, un élément important lorsque les investigations doivent étudier d'autres systèmes dont certains comptes sont peut-être compromis.

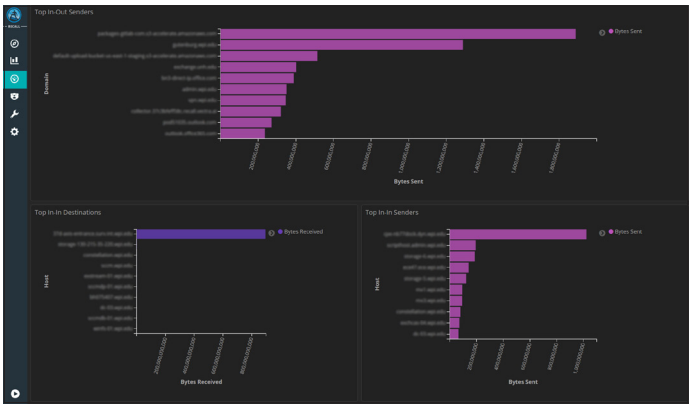


Cognito Recall affiche des détails utiles aux investigations menées sur les comptes.

Investigations sur les adresses IP et les domaines cibles

Une fois que le système compromis est identifié, il est essentiel que les analystes en sécurité puissent déterminer quels autres systèmes communiquent avec une adresse IP ou un domaine malveillant impliqué dans l'attaque.

Cognito Recall surveille toutes les communications entrantes et sortantes afin que vous puissiez identifier les systèmes ayant communiqué avec la même adresse IP ou le même domaine pendant une période donnée, ainsi que les actions intervenues pendant la communication.



Cognito Recall suit toutes les communications entrantes et sortantes des systèmes.

Données contextuelles plus riches sur les comportements d'attaque

Lors d'une analyse comportementale portant sur une cyberattaque détectée par Cognito Detect, il peut être utile de disposer d'informations détaillées sur toutes les activités réseau survenues au cours de l'incident.

En passant en un seul clic de Cognito Detect à Cognito Recall, les analystes en sécurité bénéficient de données contextuelles plus précises et pertinentes sur les communications réseau malveillantes.

Cognito Detect offre des informations sur les comportements d'attaque spécifiques et les systèmes compromis par le cyberpirate, tandis que Cognito Recall permet aux analystes en sécurité de rechercher dans les données stockées les communications réseau établies au cours de l'attaque.

VECTRA®
Security that thinks®

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