VECTRA®

Cognito Detect, la solution la plus efficace pour détecter et bloquer les cyberpirates en temps réel

PRINCIPAUX ATOUTS

- Les modèles d'analyse comportementale à apprentissage continu s'appuient sur l'intelligence artificielle pour identifier les cyberpirates inconnus et furtifs, permettre l'application de mesures rapides et déterminantes, et fournir un point de départ clair pour la traque des menaces assistée par l'intelligence artificielle.
- La solution détecte les menaces connues en tirant parti de l'intelligence artificielle et en intégrant d'autres sources critiques de cyberveille.
- Elle analyse des métadonnées réseau enrichies, des journaux pertinents et des événements cloud pour offrir une visibilité haute fidélité sur les comportements des cyberpirates, que leurs cibles soient les centres de données, le cloud, les appareils IoT ou les terminaux des utilisateurs.
- Des données contextuelles uniques permettent d'accélérer la traque et la détection des menaces ainsi que l'application de mesures immédiates, en vous fournissant les informations les plus pertinentes de manière proactive.
- La solution fonctionne avec des EDR et des systèmes de contrôle d'accès réseau, des pare-feux et d'autres produits d'application de stratégies pour bloquer les nouvelles catégories de menaces.
- Elle fournit un point de départ clair pour des investigations plus poussées avec Cognito Recall, des SIEM et d'autres outils d'investigation.

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

Composant essentiel de Cognito™, la plate-forme de traque des menaces et de détection des cyberattaques de Vectra®, Cognito Detect™ offre une solution rapide et performante pour détecter et bloquer les cyberpirates dans les clouds publics, les centres de données privés et les environnements d'entreprise. La solution s'appuie sur l'intelligence artificielle pour offrir une visibilité en temps réel sur les attaques ainsi que des informations détaillées sur celles-ci.

En plus d'accélérer l'application de mesures déterminantes en réponse à des attaques en cours, Cognito Detect offre un point de départ clair aux spécialistes en traque des menaces qui utilisent Cognito Recall™ pour mener des investigations plus poussées.

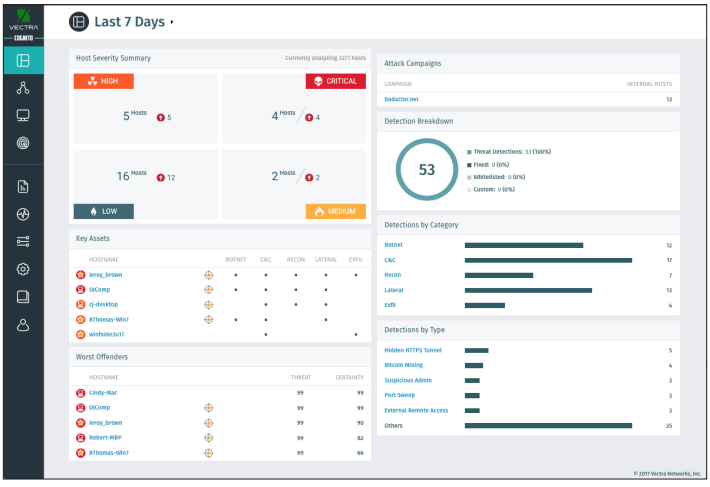
En associant des techniques d'apprentissage automatique (dont l'apprentissage profond et les réseaux neuronaux) à des modèles d'analyse comportementale à apprentissage continu, la solution détecte de façon rapide et efficace des cyberpirates inconnus et furtifs avant qu'ils ne causent des dommages.

Cognito Detect offre une visibilité complète sur les cyberattaques furtives grâce à l'analyse de tout le trafic réseau et tous les journaux des dispositifs de sécurité, des systèmes d'authentification et des applications SaaS. Une telle visibilité ne laisse aucune chance aux attaquants, que leurs cibles soient les centres de données, le cloud, les appareils IoT ou les terminaux des utilisateurs.

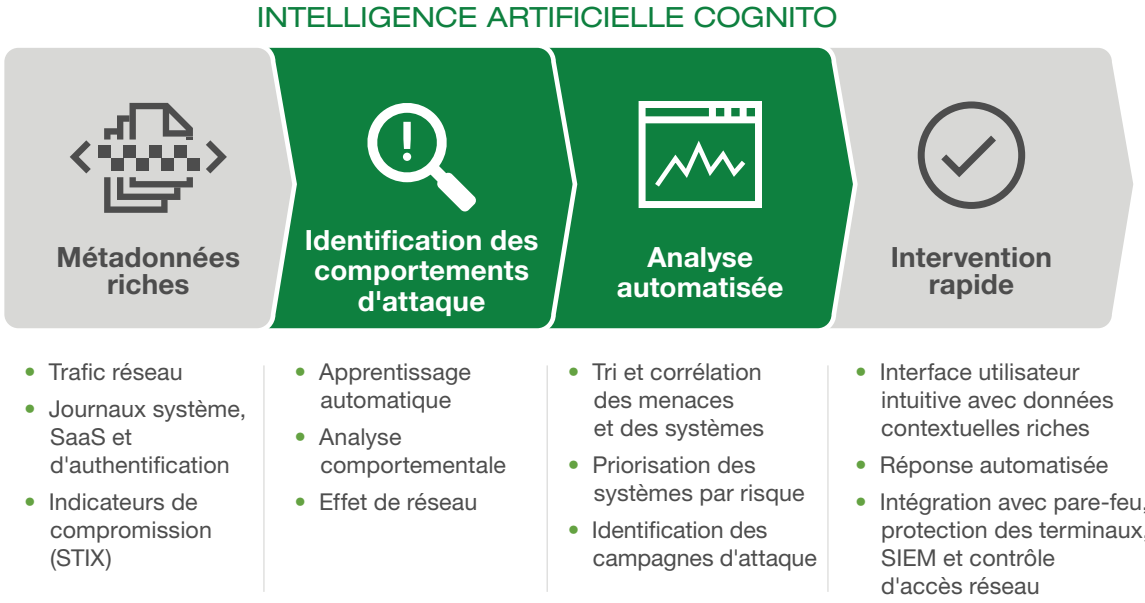
Comprises dans l'abonnement Cognito Detect, les mises à jour logicielles diffusent régulièrement des algorithmes de détection destinés à contrer les nouvelles menaces, afin de garantir une protection continue contre les dernières attaques avancées.

Un analyste en sécurité logiciel

Cognito Detect automatise la traque des cyberpirates, révèle où ceux-ci se cachent et rend compte de leurs actions. Les menaces les plus dangereuses sont instantanément triées, mises en corrélation avec les systèmes et priorisées pour permettre aux équipes de sécurité d'intervenir plus rapidement afin de bloquer les attaques en cours et de prévenir la perte de données.



Les détections des attaques sont instantanément priorisées, évaluées et mises en corrélation avec les systèmes compromis.



En automatisant l'analyse manuelle chronophage des événements de sécurité, Cognito Detect condense plusieurs semaines ou mois de travail en quelques minutes, réduisant considérablement la charge de travail des analystes en sécurité.

Les équipes responsables des opérations de sécurité, même en sous-effectif, peuvent ainsi garder une longueur d'avance sur les cyberpirates et contrer rapidement les menaces dissimulées.

Fonctionnement de Cognito Detect

Métadonnées riches

Cognito Detect assure une visibilité en temps réel sur le trafic réseau en exécutant l'extraction des métadonnées des paquets plutôt qu'une inspection approfondie, ce qui permet de garantir la protection sans violer la confidentialité des informations.

L'analyse des métadonnées est appliquée à tout le trafic interne (est-ouest) et Internet (nord-sud), à l'infrastructure virtuelle et à l'environnement de cloud. Cognito Detect identifie, suit et évalue chaque équipement IP connecté au réseau.

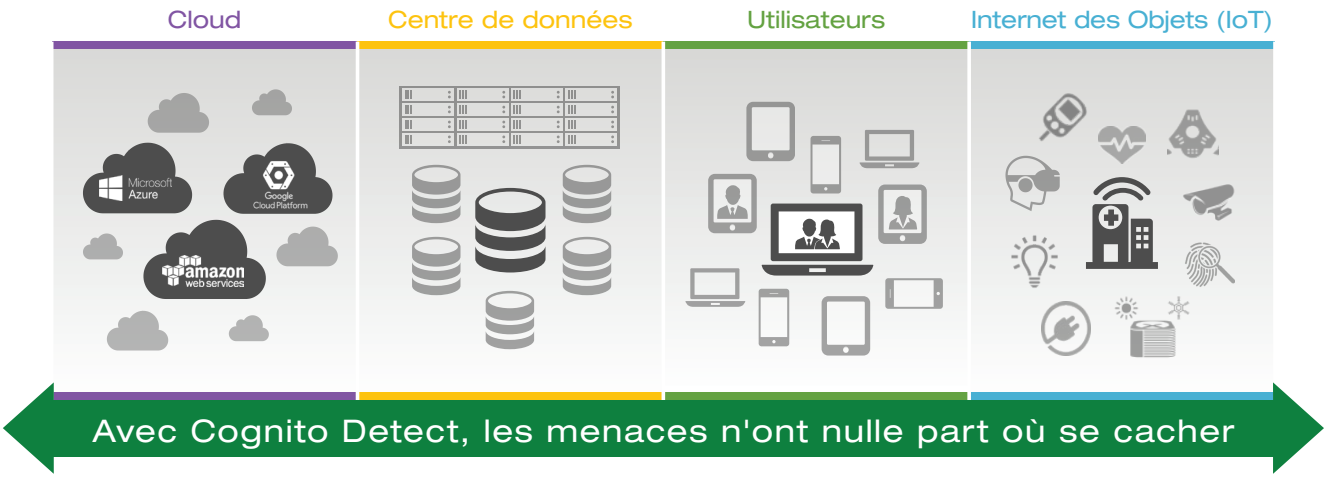
Cette visibilité s'étend aux ordinateurs portables, serveurs, imprimantes, équipements personnels et appareils IoT, ainsi qu'aux systèmes d'exploitation et applications. Elle comprend en outre le trafic entre les charges de travail virtuelles des centres de données, du cloud et même des applications 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 Detect s'appuie sur les informations de cyberveille STIX pour détecter les menaces sur la base des indicateurs de compromission connus. Ceux-ci sont mis en corrélation avec les autres comportements d'attaque pour évaluer avec une grande précision les scores de risque et de certitude d'un système et ainsi prioriser les risques.

Identification des comportements d'attaque

Les métadonnées collectées sont analysées à l'aide d'algorithmes de détection comportementale qui identifient les menaces dissimulées et inconnues. Cette analyse expose les comportements



Cognito Detect assure la détection des menaces à l'échelle de l'entreprise.

d'attaque de base identifiés dans le trafic réseau, tels que les outils d'accès distant, les tunnels dissimulés, les portes dérobées (backdoors), l'utilisation abusive des identifiants, les opérations de reconnaissance internes et les déplacements latéraux.

Cognito Detect examine en permanence votre environnement local et suit tous les systèmes physiques et virtuels afin de déceler des signes de compromission d'équipements et de menaces internes. La solution détecte automatiquement un large éventail de cybermenaces à chaque phase du cycle d'attaque, telles que :

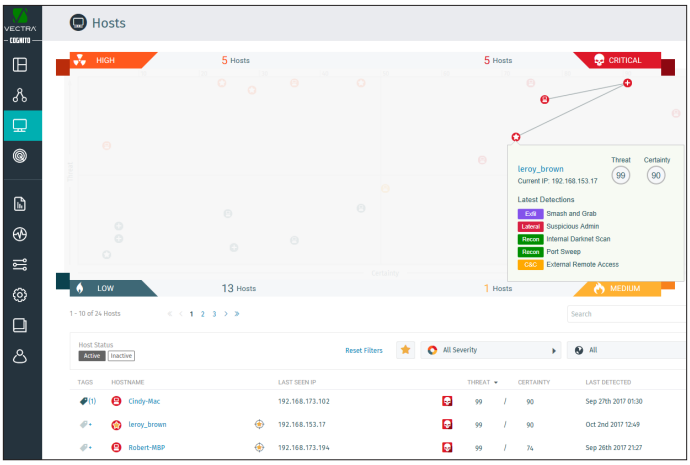
- Communications C&C (Command & Control) et autres communications dissimulées
- Reconnaissance interne
- Déplacement latéral
- Utilisation abusive des identifiants de compte
- Exfiltration de données
- Indicateurs précoces d'activités liées aux ransomwares
- Monétisation des botnets
- Campagnes d'attaque, notamment la mise en correspondance de tous les systèmes et des indicateurs d'attaque associés

Cognito Detect surveille et détecte également les accès suspects aux ressources critiques par des employés autorisés, ainsi que les violations de stratégies liées à l'utilisation du stockage dans le cloud, du stockage USB et d'autres modes de transfert des données hors du réseau.

Analyse automatisée

L'outil Vectra Threat Certainty Index™ de Cognito Detect met en corrélation des milliers d'événements et le contexte historique pour identifier les systèmes qui posent le plus gros risque.

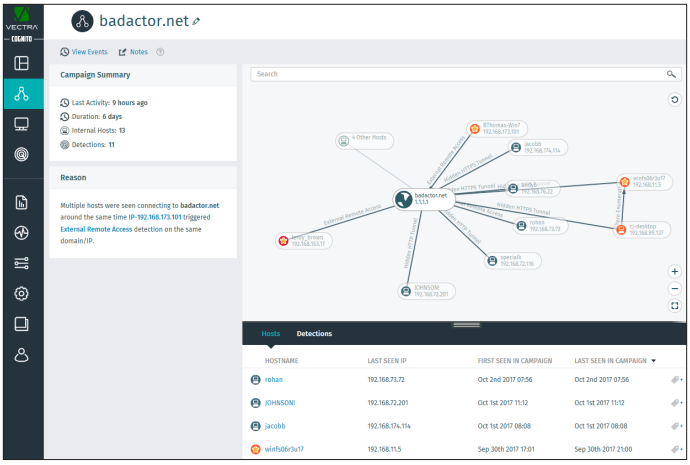
Au lieu de générer davantage d'événements à analyser, Cognito Detect dissèque d'énormes volumes de données pour en extraire les informations pertinentes. Les scores de risque et de certitude déclenchent l'envoi de notifications à votre personnel ou une action de la part des autres solutions d'application des stratégies, systèmes SIEM et outils d'investigation numérique.



Threat Certainty Index dans Cognito Detect.

La fonctionnalité Campagnes d'attaque automatise les détections de sécurité : elle fait le lien entre des comportements d'attaque liés et met en évidence les relations entre systèmes au niveau des détections internes, des détections de comportements C&C externes avancés et des communications avec des infrastructures C&C courantes.

À mesure que les cyberpirates mènent des opérations de reconnaissance et se déplacent d'un système à l'autre du réseau, Cognito Detect met en corrélation leurs comportements sur tous les systèmes et détections concernés, puis présente une vue synthétique de toute la campagne d'attaque.



Cognito Detect présente une vue synthétique de toute une campagne d'attaque.

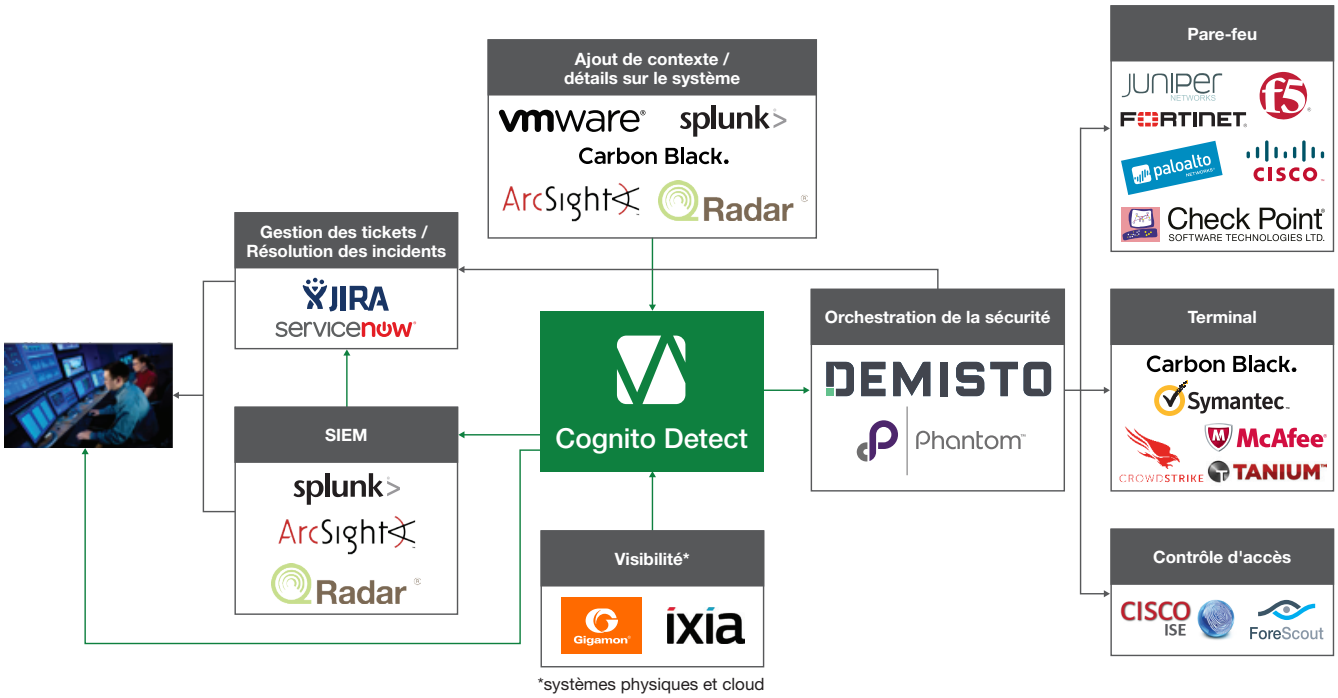
Cognito Detect peut basculer vers d'autres vues pour montrer des systèmes ou des détections de campagnes liées, et analyser l'historique des événements couvrant tout le cycle de vie de la campagne pour mieux comprendre les activités et l'ampleur de l'attaque.

Intervention rapide

Intervenez rapidement et de façon décisive sur les menaces en accédant facilement au contexte et aux informations les plus pertinentes. Contrairement aux produits d'analyse de la sécurité, Cognito Detect élimine les investigations manuelles en définissant automatiquement le niveau de risque et en corrélant les menaces avec les systèmes compromis et les ressources critiques ciblées par une attaque.

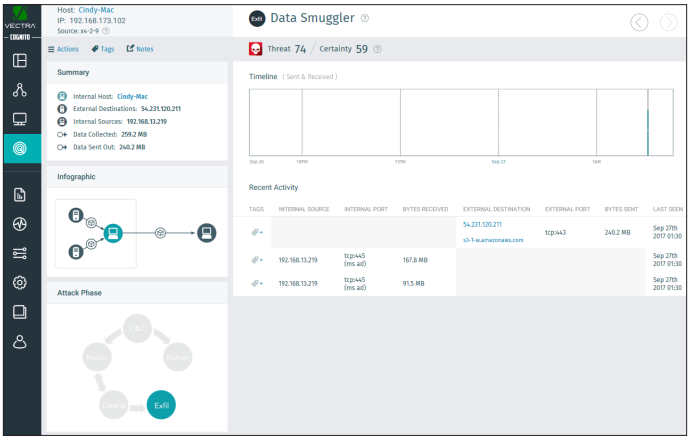
Cognito Detect met à votre disposition de nombreux détails concernant la détection, dont le contexte du système, les captures de paquets, ainsi que les scores de risque et de certitude.

Par ailleurs, la solution travaille de concert avec vos pare-feux de nouvelle génération, vos outils de protection des terminaux, vos systèmes de contrôle d'accès réseau et d'autres solutions d'application de stratégies pour bloquer automatiquement les cyberattaques inconnues et personnalisées. Cognito Detect fournit également un point de départ clair pour les investigations sur les menaces, ce qui renforce l'efficacité des outils SIEM et d'investigation.



Cognito Detect travaille de concert avec les solutions d'application de stratégies de sécurité, les systèmes SIEM et les outils d'investigation numérique les plus courants.

Security that thinks®, ou l'intelligence au service de la sécurité



Détection en temps réel d'une exfiltration de données en cours.

Des données contextuelles sur la sécurité qui font gagner du temps

Cognito Detect est un outil précieux pour les équipes responsables des opérations de sécurité, souvent en sous-effectif, dont il allège la charge de travail. En effet, il automatise l'analyse manuelle chronophage des événements de sécurité et évite au personnel de devoir traquer constamment les menaces furtives.

Chaque détection est expliquée en détail, de même que l'événement sous-jacent et le contexte historique ayant conduit à la détection. Les analystes en sécurité peuvent voir instantanément une carte des connexions de chaque système pour identifier les autres équipements avec lesquels il communique et leur mode de communication.

Cognito Detect offre également un accès à la demande à des métadonnées enrichies, issues des paquets capturés, à des fins d'investigation numérique. Les équipes de sécurité ont ainsi les preuves et la précision dont elles ont besoin pour appliquer immédiatement des mesures déterminantes.

Renforcement de l'infrastructure de sécurité existante

Cognito Detect vous permet de tirer pleinement parti des technologies de sécurité existantes, qu'il s'agisse de fournir la cyberveille nécessaire pour bloquer une nouvelle catégorie de menaces avec des pare-feux, des outils de protection des terminaux, des systèmes de contrôle d'accès réseau ou des solutions d'application de stratégies, ou encore d'offrir un point de départ clair pour mener des recherches plus poussées avec des solutions SIEM et d'autres outils d'investigation numérique.

Cognito Detect s'intègre avec des solutions de protection de terminaux de pointe pour apporter automatiquement des données contextuelles enrichies aux investigations et permettre aux équipes responsables des opérations de sécurité d'isoler les systèmes compromis.

Une API robuste permet d'automatiser l'intervention sur incidents et l'application de stratégies avec la plupart des solutions de sécurité. Cognito Detect génère également des messages syslog et des journaux CEF pour toutes les détections, ainsi que des scores de risque priorisés pour les systèmes. Bien plus qu'une simple source de données journalisées, Cognito Detect est le point de départ idéal aux investigations et workflows de votre solution SIEM.

Détection du cycle de vie complet d'un ransomware

Cognito Detect identifie les campagnes de ransomware ciblant les entreprises et d'autres organisations pendant toutes les phases de l'attaque. Grâce à la surveillance de l'ensemble du trafic réseau interne, Cognito Detect identifie en quelques secondes les comportements caractéristiques d'une attaque de ransomware qui tente de prendre en otage des ressources critiques.

En plus de détecter directement le ransomware, Cognito Detect décèle les signes précurseurs d'une attaque, notamment le trafic C&C, les analyses réseau et le comportement de propagation adopté par un ransomware pour localiser et chiffrer les ressources critiques.

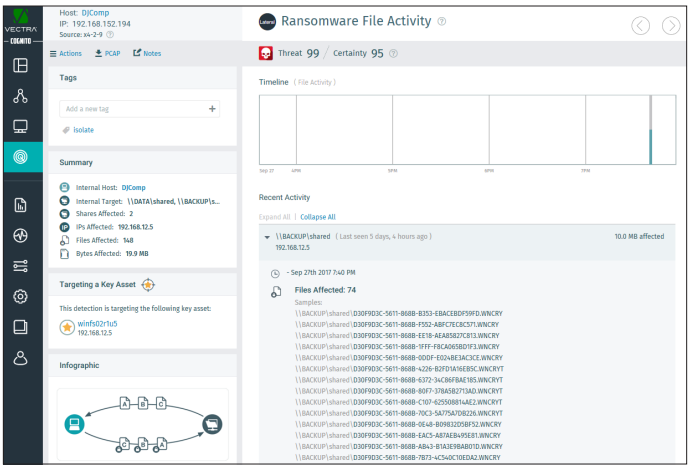
Surveillance des surveillants

Si les cyberpirates commencent souvent par compromettre l'appareil d'un utilisateur, leur but ultime est de prendre le contrôle des identifiants système ou des administrateurs. Cognito Detect va plus loin que la simple surveillance des comportements des utilisateurs pour repérer les signes de compromission de comptes d'administrateur.

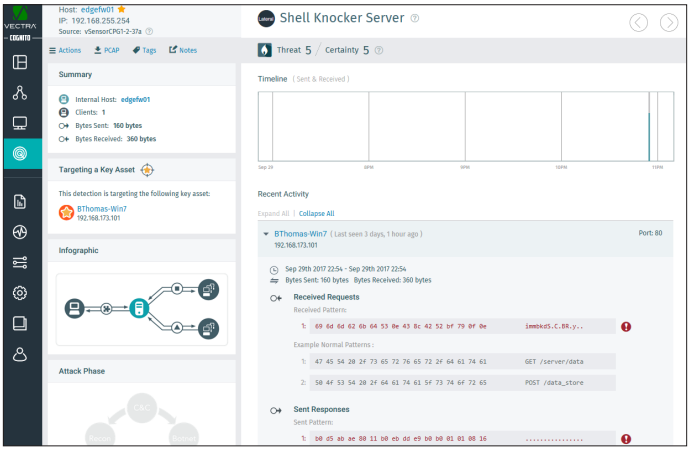
Cognito Detect surveille les protocoles d'administration et identifie les machines spécifiques ou systèmes d'accès utilisés pour gérer des systèmes, serveurs et charges de travail spécifiques. Grâce à cette surveillance rapprochée, la solution détecte rapidement les tentatives d'utilisation d'identifiants et de protocoles d'administration pour propager une attaque dans le réseau.

Sécurité native pour votre cloud privé

Le centre de données hébergé dans un cloud privé est devenu le cœur de nombreuses entreprises. Pourtant il reste souvent une zone d'ombre pour les équipes de sécurité. Cognito Detect surveille en permanence les applications critiques des centres de données, les données et l'infrastructure, et peut détecter les attaques les plus évoluées.



Détection de ransomware par Cognito Detect.



Détection de Shell Knocker par Cognito Detect.

Quelque 80 % du trafic du centre de données ne quitte jamais ce dernier et n'est donc pas surveillé par les solutions classiques de protection du périmètre. Les capteurs virtuels (vSensor) de Cognito Detect peuvent être connectés à n'importe quel commutateur virtuel (vSwitch) VMware dans le centre de données pour offrir une visibilité sur l'ensemble du trafic et détecter des menaces qui se déplacent entre les charges de travail de l'environnement virtuel.

Cognito Detect s'intègre également avec VMware vCenter pour offrir une vue de référence, constamment actualisée, de votre environnement virtuel. En fait, Cognito Detect est la première solution à allier à la fois la visibilité, le contexte et la cyberveille nécessaires à la détection d'attaques avancées au sein du centre de données.

Protection de toute l'infrastructure, du matériel aux charges de travail

La sécurité du centre de données dépasse le simple cadre de la virtualisation pour inclure également les serveurs physiques et les outils de bas niveau utilisés pour sa gestion. Cognito Detect garantit une détection inégalée des menaces qui s'étend de la couche applicative au matériel sous-jacent.

Par exemple, la fonction de détection « Port Knocking » de Cognito Detect permet d'identifier les serveurs compromis par un rootkit, lequel peut résider sous le système d'exploitation physique lui-même. En outre, Cognito Detect surveille et détecte toute utilisation incorrecte des protocoles de gestion de bas niveau, comme IPMI et iDRAC.

Normalement utilisés par les administrateurs pour la gestion en service réduit du matériel serveur, ces protocoles sont de plus en plus souvent pris pour cible par les cyberpirates car ils offrent un backdoor sur l'environnement virtuel sans être consignés dans les journaux ni surveillés par les solutions de sécurité.

Unification des opérations de centre de données

Les centres de données modernes exigent une coordination constante entre les équipes d'administration réseau, de développement d'applications, de virtualisation et bien sûr l'équipe de sécurité. Cognito Detect permet à tous ces groupes de rester synchrones et de conserver une parfaite visibilité sur l'environnement virtuel, même lorsque les charges de travail sont constamment déplacées.

La solution affiche une représentation visuelle des connexions entre toutes les charges de travail ainsi que le type de trafic circulant entre elles. Grâce à l'intégration étroite à VMware vCenter, Cognito Detect propose une vue toujours à jour de l'environnement et des alertes concernant toutes les ressources non surveillées par un outil de détection des menaces.

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