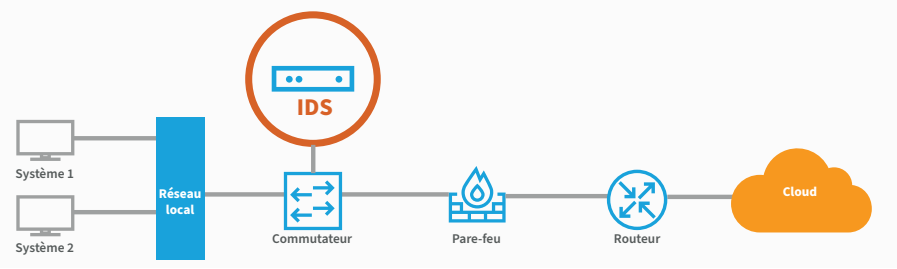
VECTRA
SECURITY THAT THINKS®

ANALYSE CONCURRENTIELLE

Les IDS de nouvelle génération cacheraient-ils un problème bien connu ?

Les systèmes de détection des intrusions (IDS), comme Cisco Firepower (anciennement Sourcefire), Trend Micro Deep Discovery ou encore McAfee Network Threat Behavior Analysis, tirent tous parti de technologies conventionnelles qui s'appuient fortement sur des mécanismes de détection et de protection basés sur les signatures.

Ces solutions ne peuvent être considérées comme de réels concurrents de la plate-forme Cognito® de détection et aide à la résolution des incidents de Vectra®, même si depuis peu, elles sont présentées comme telles dans les campagnes marketing. Ce document explique brièvement pourquoi les technologies IPS sont encore loin de rivaliser avec Cognito.



Aucune détection comportementale

Les systèmes de détection par simple analyse heuristique ou basés sur les signatures sont uniquement capables d'identifier des caractéristiques récurrentes des attaques spécifiques et connues. La plupart des attaques actuelles, y compris les attaques opportunistes, sont au moins modifiées superficiellement pour répondre aux besoins des cyberpirates et être les plus efficaces possibles. Nous vous renvoyons pour plus de détails à notre Spotlight Report on Ransomware.

L'époque où les cyberpirates envoyaient en masse des milliers de messages dans l'espoir de piéger une poignée de victimes est révolue. Ils privilégient aujourd'hui les attaques ciblées, lesquelles offrent une rentabilité bien supérieure. Confier la protection de votre réseau à un IDS revient à exécuter une version d'essai gratuite de Kaspersky Antivirus datant du début des années 2000. Qui pourrait alors s'étonner d'être infecté en 2020 ?

97 %

La plate-forme Cognito de détection et aide à la résolution des incidents réseau (NDR) prend en charge plus de 97 % du cadre MITRE ATT&CK.

Conçu pour les modèles de sécurité d'ancienne génération

Alors qu'un nombre croissant d'entreprises adoptent le modèle Zero Trust, les systèmes archaïques qui se limitent à protéger leur périmètre physique extérieur sont devenus obsolètes. Dans ce contexte, le seul trafic examiné par les IDS est celui qui transite par le pare-feu.

Or, si les attaquants parviennent à compromettre le réseau interne, ils sont alors libres d'agir en toute impunité, sans même que les IDS s'en aperçoivent. La seule différence visible pour les IDS sera en réalité la baisse importante des performances qu'affichent les pare-feux lors de l'exécution d'analyses heuristiques sur les paquets qui transitent par eux.

Les entreprises modernes peuvent par ailleurs générer autant de trafic dans le cloud que sur leurs réseaux physiques. Dans la mesure où les IDS se concentrent sur le trafic entrant du réseau, les cyberpirates qui s'infiltrent par le biais d'un compte de service cloud compromis passent complètement inaperçus.

La plate-forme Cognito peut être déployée sur tous les composants du réseau, y compris les environnements multiclouds, afin d'offrir aux analystes en sécurité une visibilité complète sur l'ensemble des ressources, où qu'elles résident.

La plate-forme Cognito renforce en outre les initiatives Zero Trust par le biais de sa technologie Privileged Access Analytics (PAA). Les fonctions PAA permettent d'analyser l'utilisation des comptes sur votre réseau et de détecter les auteurs de menaces en interne qui utilisent des identifiants compromis pour étendre la portée de leurs attaques.

Préparez-vous à une avalanche d'alertes pour anomalie

En tant que système de détection basé sur les anomalies, un IDS est incapable d'identifier les menaces les plus dangereuses et submergera votre équipe de sécurité par un flux d'alertes incessant. Ces dernières doivent être triées manuellement et individuellement, ce qui augmente sensiblement la charge de travail liée aux opérations de sécurité. Déjà surchargées, les équipes de sécurité se passeront bien d'avoir à endosser une telle responsabilité.

À l'inverse, confrontés à des attaquants humains plutôt qu'à des attaques simulées, les modèles algorithmiques Cognito surpassent de loin les systèmes de détection par analyse heuristique ou basés sur les signatures. En fait, la plate-forme Cognito de détection et aide à la résolution des incidents réseau prend en charge plus de 97 % du cadre MITRE ATT&CK.

La supériorité de ses capacités de détection devient vite évidente dans le cadre d'une preuve de concept (PoC).

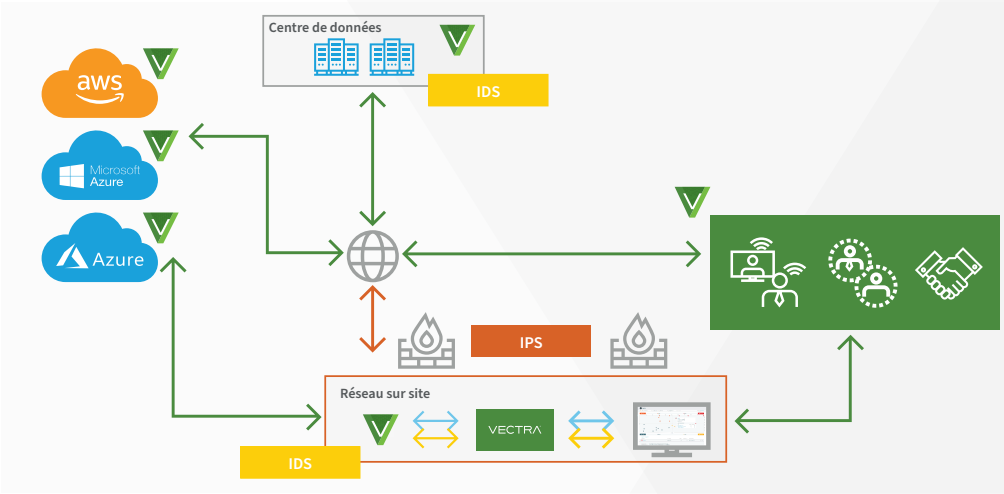
Cognito permet même une réduction par 38 de la charge de travail liée aux opérations de sécurité. La plate-forme trie automatiquement les alertes en fonction des incidents, classe les systèmes par niveau de risque et extrait des métadonnées enrichies à partir de l'ensemble du trafic réseau afin de faciliter les enquêtes et les investigations numériques.

La dépendance vis-à-vis d'un fournisseur unique freine l'adoption de technologies de pointe

Les IDS sont généralement intégrés à une plate-forme plus large et ne permettent donc pas une protection efficace à eux seuls. Un investissement complémentaire est alors nécessaire en pare-feux, filtrages d'URL, outils de visibilité des applications, détection avancée des attaques, etc. Autrement dit, pour bénéficier d'une expérience intégrée, vous devez acheter l'ensemble des composants auprès du même fournisseur.

La plate-forme Cognito, quant à elle, s'intègre facilement avec votre dispositif de sécurité existant, et ce, par le biais d'API. Notre écosystème de partenaires technologiques est constitué de leaders des secteurs de l'EDR, des pare-feux de nouvelle génération, des solutions SIEM, de l'orchestration de la sécurité et du contrôle d'accès réseau. Les intégrations Cognito prennent en charge les stratégies les plus en pointe et offrent une valeur ajoutée continue en protégeant vos investissements existants.

E-mail : info_france@vectra.ai / info_dach@vectra.ai vectra.ai/fr



Les IDS de l'avenir

La plate-forme Cognito de Vectra offre une foule d'avantages par rapport aux IDS de nouvelle génération, tels que :

- **Détection des attaques modernes et réelles** appuyée par des algorithmes d'apprentissage automatique supervisés et non supervisés.
- **Visibilité complète** sur l'ensemble du réseau, de l'entreprise jusqu'au cloud, et pas uniquement des données qui transitent par votre pare-feu.
- **Réduction de la charge de travail liée aux opérations de sécurité** par un facteur de 38. Cognito trie les résultats de la détection des attaques en fonction des incidents pour une résolution rapide et efficace.
- **Performances visibles de la plate-forme** par l'intégration avec d'autres solutions dans votre dispositif de sécurité.

Pour plus d'informations, veuillez contacter l'un de nos représentants à l'adresse sales-inquiries@vectra.ai.