Les prévisions 2023 de Vectra avertissent que la pénurie de compétences se transformera en guerre pour recruter des talents, et qu'une collaboration renforcée est nécessaire pour empêcher les attaques contre les chaînes d'approvisionnement

Face à l'augmentation de la surface d'attaque, de la pénurie de compétences et de la montée des menaces inconnues, il est essentiel de disposer d'informations fiables et rapides

Vectra AI, le leader de la détection et du traitement des menaces dans le Cloud hybride s'appuyant sur l'IA, a publié aujourd'hui ses prévisions pour 2023, révélant les tendances émergentes qui façonneront la cybersécurité l'année prochaine.

Christian Borst, directeur technique EMEA chez Vectra AI, a déclaré : « L'année prochaine, les entreprises seront confrontées à un plus grand nombre de cybermenaces inconnues ciblant les systèmes sur site, l'infrastructure dans le Cloud et les applications SaaS. La pénurie de compétences s'aggrave également, ce qui conduit au surchargement et à l'épuisement des analystes. Toutes les conditions sont réunies pour rendre les entreprises plus vulnérables à des failles de sécurité. Elles doivent adopter une stratégie de détection et de traitement efficace, capable de réduire la charge des analystes tout en accordant la priorité aux alertes associées aux plus grands risques. Cela signifie qu'il faut utiliser des outils capables d'identifier les comportements suspects d'un adversaire lors d'une attaque, en remontant ces informations afin que les entreprises puissent stopper une attaque avant qu'elle n'ouvre une brèche. »

Christian Borst et Brian Neuhaus, directeur technique Amériques chez Vectra AI, ont souligné une série de tendances qui, selon eux, auront un fort impact sur le secteur de la cybersécurité l'année prochaine.

Christian Borst, directeur technique EMEA chez Vectra AI :

- **Les attaques contre les chaînes d'approvisionnement vont se poursuivre, mais les pirates ne se limiteront pas aux cibles habituelles pour faire des ravages :** Ils continueront de perturber au maximum les chaînes d'approvisionnement, mais au lieu de viser des fournisseurs clés, ils s'en prendront à d'autres intervenants pour accéder aux réseaux. Il pourra s'agir par exemple de cabinets d'avocats ou de comptabilité. Une approche globale peut aider à renverser la situation : chaîne d'approvisionnement signifie partenariat, et partenariat signifie collaboration et soutien mutuel. Ce n'est qu'en tant que structure « maillée » et dotée d'une résilience constante que les entreprises peuvent prospérer dans l'économie numérique. Elles doivent notamment veiller à examiner les politiques de sécurité de tous les acteurs de cette chaîne interconnectée.

- **Les entreprises utiliseront l'automatisation pour se remettre des attaques de ransomwares :** Les procédures traditionnelles de restauration après une attaque de ransomware sont à la fois coûteuses et longues pour les entreprises. C'est pourquoi en 2023, nous les verrons se tourner vers l'automatisation, via l'infrastructure sous forme de code (IaC), afin de réduire les temps d'arrêt. Grâce à l'IaC, les entreprises peuvent développer des scripts qui permettent aux infrastructures clés de s'auto-réparer et de reprendre automatiquement leurs activités. En fin de compte, grâce à l'automatisation, le rétablissement d'une infrastructure brisée à partir de zéro est un processus beaucoup plus rapide que la restauration.

- **La lassitude et la résignation accrues des analystes feront que la protection du périmètre laissera sa place à la détection et au traitement :** Les attaquants continuent de percer les défenses, entraînant la lassitude et la résignation éventuelle des professionnels de la cybersécurité. Au lieu de s'efforcer d'éviter que ces attaques ne se produisent et d'empêcher l'épuisement des collaborateurs, nous allons assister à un changement nécessaire de focus, qui passera à la réduction de l'impact d'une attaque. Cela signifie qu'il faut renforcer la résilience au sein de l'entreprise, en couvrant les personnes, les processus et les technologies, et en se concentrant sur la détection précoce et le traitement approprié, plutôt que sur la protection et la prévention. Cela permettra d'identifier les activités suspectes et les types de comportements qu'un adversaire adoptera lors d'une attaque. L'essentiel est de pouvoir repérer les attaques en cours afin de les stopper avant qu'elles ne réussissent.

- **L'authentification multifacteur (MFA) restera une cible de choix pour les attaquants :** Les attaques contre les méthodes de vérification d'identité étant en hausse, elles continueront de profiter des méthodes de MFA vulnérables en 2023. À mesure que les entreprises déploient la MFA, les attaquants continueront d'en profiter, soit en inondant les utilisateurs finaux de demandes d'accès par force brute, soit en menant des campagnes de phishing habiles. Les utilisateurs finaux seront la cible directe des attaquants, ce qui signifie que non seulement les entreprises, mais également les consommateurs, devront être plus vigilants que jamais sur les risques qui pèsent sur leurs identités numériques. Parallèlement, les entreprises doivent s'assurer qu'elles disposent d'outils permettant de détecter les activités de connexion suspectes et les stopper net.

<u>Brian Neuhaus, directeur technique Amériques chez Vectra AI :</u>

- **Les attaquants commenceront à voler des données chiffrées pour les conserver et les déchiffrer dans un monde post-quantique :** Il est facile de connaître le motif d'une cyberattaque, par exemple dans le cas des ransomwares, mais qu'en est-il des incidents que nous ne pouvons détecter ou qui impliquent des données que nous pensions être à l'abri du déchiffrement ? Les progrès de l'informatique quantique obligeront les responsables de la sécurité en 2023 à commencer à réfléchir à ces données sensibles chiffrées dans un monde post-quantique. Cette approche attirera également l'attention des attaquants. Au lieu d'ignorer les données chiffrées qui étaient précédemment protégées, ils tenteront de s'en emparer et de les conserver pour les vendre ou pour les déchiffrer ultérieurement. Les défenseurs ne doivent pas se reposer sur les lauriers du

chiffrement et commencer à prendre note cette année de ce que fait le NIST en matière de chiffrement post-quantique pour agir dans les années à venir.

- **À mesure que la lutte s'intensifie pour attirer les talents, les entreprises de sécurité devront développer des moyens créatifs de recruter et fidéliser leurs salariés :** Dans un marché du travail de plus en plus mondialisé où les travailleurs cherchent de plus en plus de nouvelles opportunités, les entreprises de cybersécurité risquent de perdre des talents au profit des entreprises technologiques traditionnelles. Les entreprises de cybersécurité, qui ne sont pas étrangères à l'épuisement professionnel et au stress, devront s'assurer qu'elles peuvent être vues comme des employeurs attrayants. Il s'agit de faire face à la concurrence des entreprises technologiques qui offrent souvent des salaires plus lucratifs, et un meilleur équilibre entre vie professionnelle et vie privée. Pour y parvenir, les entreprises de cybersécurité doivent adopter une approche plus avant-gardiste, qui pourrait inclure la mise en place de modalités de travail flexibles, d'incitations à la performance, et de politiques de santé et de bien-être.

- **Les secteurs privé et public vont renforcer leurs défenses contre les cyberattaques sponsorisées par des États :** La cyberguerre demeurera une menace réelle en 2023, qu'il s'agisse d'une utilisation plus étendue des TTP connues ou d'un nombre inconnu de menaces zero day qui n'attendent que le moment stratégiquement opportun pour être déployées contre leurs ennemis. Les menaces zero day ont un poids économique. Le développement de certaines d'entre-elles ont coûté plusieurs millions d'euros, et elles causent des pertes tout aussi dévastatrices lorsqu'elles sont déployées pour la première fois. Les dirigeants des organisations des secteurs privé et public commenceront à y prêter réellement attention, investissant davantage dans le traitement des incidents et la remédiation rapide des vulnérabilités au cours de l'année à venir, afin de limiter le rayon d'action d'une telle cyber-arme. Ainsi, les responsables de la sécurité commenceront à accepter que la compréhension de la posture est essentielle pour s'accommoder du risque d'une vulnérabilité non corrigée ou potentielle de type zero day. La posture, la détection et l'intervention rapides seront primordiales l'année prochaine.

- **L'étiquetage des logiciels et des appareils de l'IoT devient une réalité :** Après une série d'incidents de cybersécurité très médiatisés qui ont ciblé les chaînes d'approvisionnement des logiciels cette année, les décrets américains qui en ont immédiatement résulté amèneront la plupart des entreprises à réagir en 2023. L'un de ces décrets (14028) demandait au NIST d'instaurer des programmes d'étiquetage de tous les logiciels et appareils, qu'il s'agisse de logiciels pour entreprises ou bien de serrures de portes. Plus précisément, la section 4 du décret 14028 vise le même objectif que l'étiquetage nutritionnel des aliments aujourd'hui. Les étiquettes doivent clairement indiquer les paramètres de confidentialité et de sécurité de l'information pour le produit et l'entreprise. L'une des principales informations figurant sur les étiquettes devrait être la durée de l'assistance technique proposée par l'entreprise pour ses logiciels, car la durée de vie d'un appareil physique peut dépasser la durée de son assistance technique. Ceci est particulièrement important en termes de gestion des vulnérabilités. En dehors des États-Unis, les gouvernements du monde entier prennent des mesures similaires. Pourquoi voudrions-nous que les gouvernements agissent autrement ? Si nous considérons que ces étiquettes sont suffisamment bonnes pour notre propre santé, alors

pourquoi ne pas les utiliser pour quelque chose de tout aussi important, à savoir nos informations personnelles. Je prédis qu'il ne s'agira plus de simples directives, mais d'une réalité cette année, tant au niveau des produits de consommation qu'au niveau des offres pour entreprises.

À propos de Vectra

Vectra® est un leader dans le domaine de la détection et de la réponse aux menaces pour les entreprises hybrides et multi-cloud. La plateforme Vectra utilise l'Intelligence Artificielle (IA) pour détecter rapidement les menaces dans le cloud public, les identités, les applications SaaS et les centres de données. Seule Vectra optimise l'IA pour détecter les méthodes des attaquants – grâce aux TTP au cœur de toutes les attaques - plutôt que d'alerter de manière simpliste sur une « particularité ». Les entreprises du monde entier font confiance à Vectra pour leur capacité de résilience face aux dangereuses cybermenaces et pour empêcher les ransomwares, la compromission de la supply chain, les usurpations d'identité et autres cyberattaques d'avoir un impact sur leurs activités. Pour plus d'informations, visitez https://www.vectra-ai.com/ .