GoSecure lance la détection et réponse face aux menaces internes

Annonce d'une toute nouvelle approche pour détecter et prévenir les attaques internes

GoSecure, l'un des principaux fournisseurs de services de détection et de réponse gérées (MDR) et d'une plateforme prédictive de détection et réponse pour les points de terminaison (EDR), a annoncé aujourd'hui l'ajout à son portefeuille de la détection et réponse face aux menaces internes.

Les incidents causés par des malveillants internes ou dont l'objectif est le vol d'informations d'identifications représentent 32% des incidents*. Avec les 68% restants, étant le résultat d'une négligence dans l'utilisation finale, le défi consiste de plus en plus à connaître le bon comportement du mauvais. Alors que de nombreuses solutions de lutte contre les menaces internes se concentrent sur les données, la solution de détection et réponse face aux menaces internes (ITDR) de GoSecure se concentre sur les utilisateurs, les actions et les comportements.

« La menace interne est un problème croissant pour la plupart des organisations, au point où 34% des organisations ont connu un incident interne de nature malveillante », a déclaré Neil Creighton, directeur général de GoSecure. « Notre approche est unique en ce sens que nous permettons aux équipes de sécurité de définir les comportements et les acteurs suspects plutôt que de simplement définir les données à protéger. La détection et réponse aux menaces internes de GoSecure est basée sur les évènements et non sur les données ».

Avec plus de 50 types d'évènements uniques liés aux menaces internes, le service ITDR de GoSecure fournit une visibilité accrue et une flexibilité quasiment illimitée pour la création des règles de protection face aux menaces internes pour toute organisation. En combinant le personnel et les actions, la ITDR de GoSecure peut détecter le comportement des utilisateurs et réagir immédiatement avec une variété d'actions potentielles.

La ITDR de GoSecure a également adopté une approche unique afin de répondre aux activités suspectes. La manipulation propriétaire 3D d'adversaire permet au détecteur de points de terminaison de GoSecure d'empêcher ou de manipuler un évènement avant le traitement par le système d'exploitation. La manipulation 3D d'adversaire de GoSecure offre trois capacités distinctes :

- Dénier: Bloquer complètement l'accès à un fichier, un registre, un hôte distant, etc.
- Ralentir: Lorsque les critères d'évaluation de la condition sont remplis, le détecteur se met en mode « veille » pendant la durée de temps spécifiée avant de transmettre l'opération au système d'exploitation. Plutôt que de compresser un fichier en quelques secondes, par exemple, le processus peut être retardé de quelques minutes. Cela donne à l'équipe de sécurité un avertissement préalable, mais également le temps de répondre.
- Dégrader: Lorsque les critères d'évaluation de la règle d'interception sont remplis, le détecteur va dégrader les opérations en corrompant les données ou en les remplaçant par un contenu alternatif. Cela peut donner l'apparence d'une opération réussie, cependant les données ont été remplacées.

Sur la base de critères définis par le client, la détection et réponse des menaces internes de GoSecure peut également enregistrer l'activité de l'utilisateur via l'enregistrement de la frappe ou la capture vidéo.

Selon Creighton, « le cadre de gestion de la maturité du National Insider Threat Task Force (NITTF) établit la surveillance des activités des utilisateurs comme une capacité clé pour les agences fédérales américaines. Lors de conversations avec certains de nos plus gros clients, le secteur privé a défini des exigences très similaires ».

La surveillance du trafic Web avant que le navigateur ne le chiffre, est le dernier élément clé de la détection et sécurité aux menaces internes de GoSecure. Plutôt que de déchiffrer le trafic SSL en utilisant l'approche classique de l'homme du milieu (MITM), la ITDR de GoSecure utilise une introspection SSL. L'introspection SSL est effectuée par le détecteur GoSecure afin d'examiner la requête Web et les données avant qu'elles ne soient envoyées au navigateur. Cela permet à la ITDR de GoSecure d'appliquer une politique sans avoir à dépendre du déchiffrement du trafic Web.

La détection et réponse face aux menaces internes de GoSecure offre une vue sans précédent sur les activités suspectes des utilisateurs d'une organisation. Grâce à des options de surveillance et de réponse flexibles, la ITDR de GoSecure donne aux équipes de sécurité non seulement le temps de réagir et de répondre, mais également les informations nécessaires pour évaluer précisément le risque.

GoSecure offre une gamme complète de solutions en matière de cybersécurité, allant des services d'architecture, qui comprennent l'évaluation des menaces de cybersécurité et les tests d'intrusion, aux technologies de sécurité complètes et aux services de sécurité gérés. Cette gamme est alimentée par la plateforme CounterTack qui traite de la détection et réponse, des menaces internes et de l'analyse « forentics » qui atténue les vecteurs d'attaque émergents comme les rançongiciels et les logiciels malveillants sans fichiers.

À propos de GoSecure
GoSecure est reconnu comme un leader et un innovateur en matière de solutions de la cybersécurité. La société est la première et la seule à intégrer une plateforme de détection des menaces pour les points de terminaison et les réseaux, des services de détection et de réponses et une prestation de services de type Cloud et SLAs. La plateforme CounterTack offre une détection, une prévention et une réponse prédictive multisectorielle appliquant une combinaison unique d'analyse comportementale, de mémoire « forensics », d'apprentissage automatique et de techniques de réputation afin de contrer les menaces les plus avancées. Nos services MDR sont régis par des SLAs agressifs pour obtenir une réponse rapide et des services d'atténuation actifs qui touchent directement le réseau et les points de terminaison des clients. Ensemble, ses capacités constituent la réponse la plus efficace à la sophistication croissante des logiciels malveillants en constante évolution et des malveillants internes qui ciblent les personnes, les processus et les systèmes. Avec un accent placé sur la qualité, l'intégrité et le respect de l'innovation, GoSecure est devenu le fournisseur de confiance en matière de produits et de services de cybersécurité pour les organisations de toutes tailles et dans tous les secteurs d'activité à l'échelle mondiale. Pour en savoir plus, veuillez visiter le site Internet de GoSecure : https://fr.gosecure.net/.

*Rapport sur les menaces internes de Crown Research Partners en 2018

Contact de GoSecure:
Brian Fisher
bfisher@gosecure.net