Rôle du renseignement dans la protection contre les risques numériques

Cyberint

RÔLE DU RENSEIGNEMENT DANS LA PROTECTION CONTRE LES RISQUES NUMÉRIQUES

Grâce à la plateforme de renseignement exclusive Argos™ et à la grande expérience de ses analystes en sécurité informatique, Cyberint propose une nouvelle approche en matière de protection contre les risques numériques et offre des solutions répondant aux défis suivants :

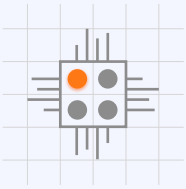
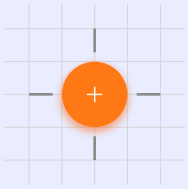
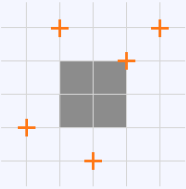
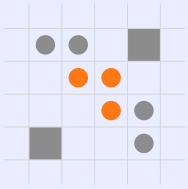
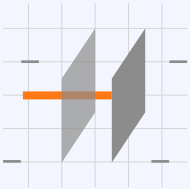
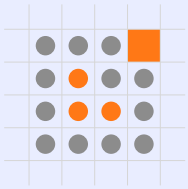
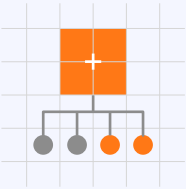
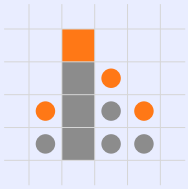
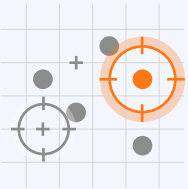
- **Déterminer quelles sont les menaces pertinentes** à considérer dans la conception d'un programme efficace de défense informatique
- **Illustrer le statut actuel du risque informatique** au conseil d'administration et à la direction en présentant un plan d'action clair
- **Obtenir des renseignements prédictifs** pour identifier les intentions, les techniques et les outils afin de réduire les menaces ciblées avant qu'elles ne se concrétisent
- **Surveiller constamment l'exposition aux risques numériques** pouvant être exploités par des cybercriminels
- **Détecter les failles lorsqu'elles se propagent** en dehors du périmètre de l'entreprise
- **Obtenir une meilleure visibilité sur les attaques** ciblant votre marque et vos clients, qui évoluent constamment en dehors de votre réseau

PROBLÈMES D'ENTREPRISE GÉRÉS PAR CYBERINT:

- PROTECTION DE LA MARQUE
- RISQUE INFORMATIQUE LIÉ AUX TIERS
- SURVEILLANCE DE SURFACE DES RISQUES NUMÉRIQUES
- FRAUDE
- DÉTECTION DES FUITES DE DONNÉES
- DÉTECTION DES ATTAQUES
- SURVEILLANCE DU DARK WEB
- RENSEIGNEMENT SUR LES MENACES

Cyberint Copyright © Tous droits réservés 2020

L'OFFRE DE CYBERINT

TECHNOLOGIE ARGOS™	SERVICE GÉRÉ
 RENSEIGNEMENT SUR LES MENACES	 SURVEILLANCE CIBLÉE
 SURVEILLANCE DU DARK WEB	 HUMINT VIRTUEL
 CARTOGRAPHIE DE SURFACE DES RISQUES	 ENQUÊTES APPROFONDIES
 CANEVAS D'ANALYSE FORENSIQUE	 ANALYSE DU PAYSAGE DES MENACES
 DÉTECTION ET ÉLIMINATION DU PHISHING	

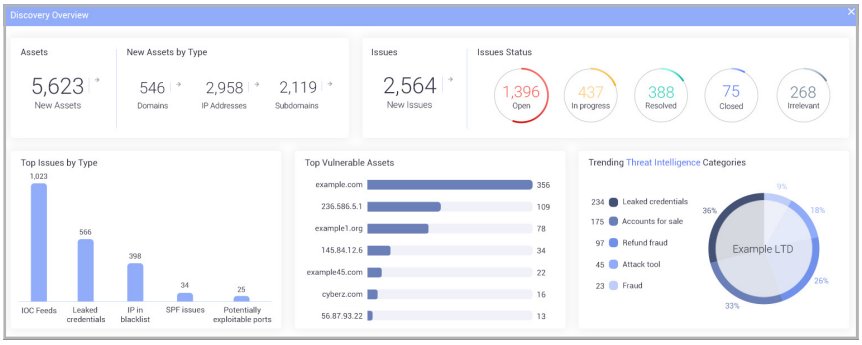
Cyberint Copyright © Tous droits réservés 2020

PLATEFORME ARGOS™ DE RENSEIGNEMENTS DE PROTECTION CONTRE LES RISQUES NUMÉRIQUES

Argos™ est une plateforme SaaS multi-comptes offrant différents modules:

CARTOGRAPHIE DE SURFACE DES ATTAQUES

La cartographie de surface des attaques d'Argos™ identifie l'empreinte numérique de l'entreprise et surveille en continu ses actifs au-delà du périmètre, garantissant la visibilité sur ceux-ci avec une hiérarchisation des problèmes à régler en fonction de leur gravité, et mettant en valeur les menaces, vulnérabilités et faiblesses associées.

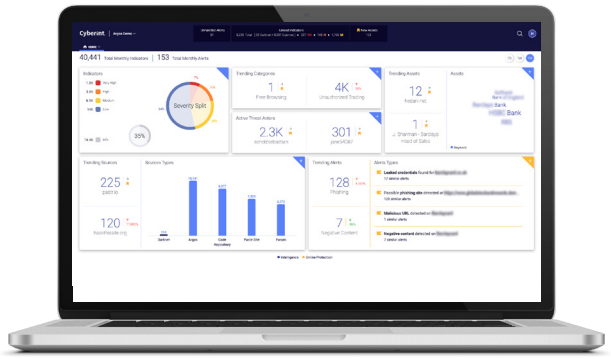


Plateforme Argos™ de protection contre les risques numériques, surveillance de surface des attaques

COLLECTE ET ANALYSE DE RENSEIGNEMENTS SUR LES MENACES

Le suivi en temps réel de milliers de sources de menace sur le dark web permet à Cyberint de recueillir des millions d'éléments de renseignement par jour dans la base de donnés interne d'Argos™.

Ces éléments d'information bruts sont automatiquement agrégés aux actifs de l'entreprise (IP, domaines, marques, direction, etc.) et classés en fonction d'un cas d'utilisation spécifique : phishing, campagnes de logiciels malveillants, credential stuffing, fuites de données, activités frauduleuses et autres. Grâce à l'algorithme d'apprentissage automatique exclusif de Cyberint, ces renseignements bruts sont hiérarchisés selon le risque et l'impact potentiels, permettant ainsi une analyse intelligente et économique.

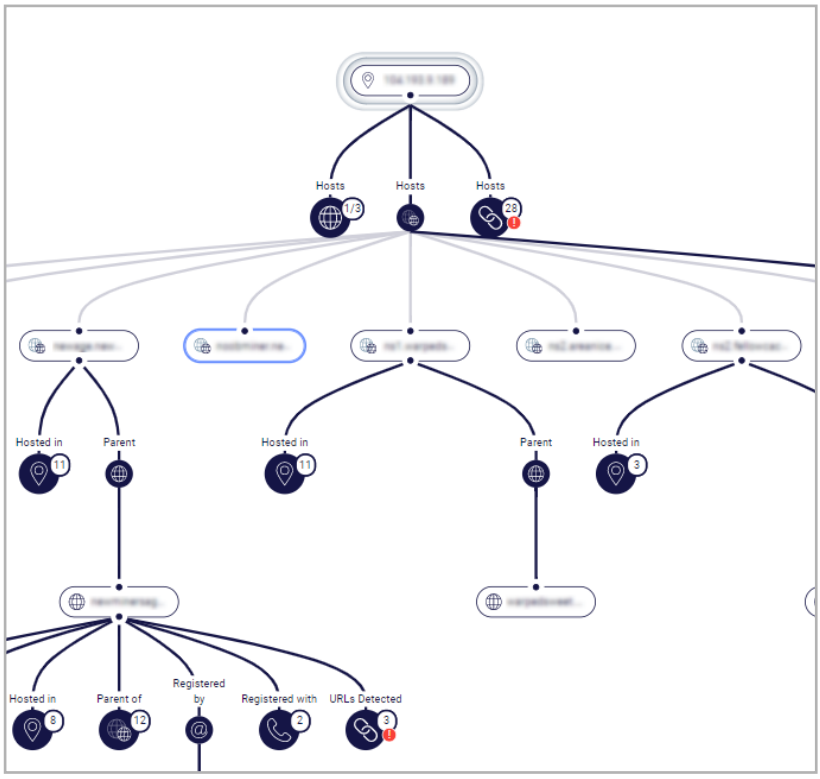


Plateforme Argos™ de protection contre les risques numériques

Les moteurs d'analyse automatique et semi-automatique génèrent des alertes exploitables qui sont ensuite diffusées aux équipes de sécurité avec une étude approfondie, un contexte enrichi, un profilage des vecteurs de menace et plus encore, permettant à l'entreprise de prendre des mesures efficaces.

Cyberint Copyright © Tous droits réservés 2020

CANEVAS D'ANALYSE FORENSIQUE



Plateforme Argos™ de protection contre les risques numériques, canevas d'analyse forensique

Le module de canevas forensique de Cyberint permet l'identification et le profilage des vecteurs de menace, ainsi qu'une enquête approfondie sur les outils, tactiques et procédures utilisés.

Le canevas forensique sert à enrichir le contexte d'inversions de contrôle spécifiques ou multiples, en intégrant divers services à travers une plateforme d'analyse unifiée prenant en charge différents types de connexion, notamment Argos™ Threat Intelligence, les services WHOIS, le DNS passif, le balayage de la présence sur les réseaux sociaux, la détection de code malveillant, etc.

TECHNOLOGIE DE DÉTECTION ET D'ÉLIMINATION PROACTIVE DU PHISHING

Le phishing reste l'un des principaux risques pour les entreprises numériques, entraînant la prise de contrôle de comptes, la perte de clients et affectant la réputation de la marque. Pour faire face à ce défi, Cyberint a développé le Phishing Beacon, un module exclusif offrant une visibilité en temps réel sur les nouveaux sites de phishing clonés à partir du contenu du site Web de l'entreprise, une technique efficace utilisée par les vecteurs de menace. La détection rapide effectuée par Cyberint nous permet de désactiver les sites de phishing au nom de l'entreprise pour éliminer rapidement le risque.

AVANTAGES POUR VOTRE ENTREPRISE

- **RÉDUIRE LES RISQUES DE SÉCURITÉ INFORMATIQUE INVISIBLES**
- **GAGNER DE LA VISIBILITÉ SUR VOTRE EXPOSITION AUX ATTAQUES**
- **RÉDUIRE LE TEMPS DE RÉPONSE À UNE MENACE**
- **AUGMENTER LES CAPACITÉS DE VOTRE ÉQUIPE**
- **RÉDUIRE LE COÛT DE LA CYBERSÉCURITÉ**

Cyberint Copyright © Tous droits réservés 2020

SERVICE GÉRÉ

Des services de renseignement informatique sur mesure qui répondent à vos besoins

AUGMENTATION DE L'ÉQUIPE DE RENSEIGNEMENT SUR LES MENACES

Cyberint offre un service géré de protection contre le risque numérique vous donnant accès à notre plateforme Argos™ et à une équipe d'analystes en sécurité informatique, complétant n'importe quel programme de CTI pour fournir un meilleur niveau de qualité et de performance.

Le partenariat avec l'équipe d'analystes de Cyberint inclut une interaction quotidienne avec un professionel dédié qui est intégré à votre équipe interne. Les analystes sont affectés en fonction de leur connaissance des secteurs et de leur compréhension profonde des besoins de l'entreprise.

Tous les éléments de renseignement bruts mis en lumière par Argos™ sont vérifiés soigneusement, contextualisés et associés à des risques réels grâce à une énorme quantité de données recueillies sur le dark web.

Notre équipe d'analystes est polyglotte et peut comprendre les vecteurs de menaces dans leurs langues respectives. De plus, la maîtrise du jargon et de la culture des cybercriminels par nos analystes nous permet d'identifier, de vérifier et de réduire les menaces qui ont le plus de chances de se concrétiser sous forme d'attaques.

Cyberint fournit un composant humain précieux en matière de recherche, d'enquête et d'opérations de renseignement sur les menaces. L'HUMINT virtuel, c'est-à-dire l'interaction en direct avec les vecteurs de menace, permet une meilleure mise en contexte nécessaire à une protection efficace.

RECHERCHE CYBERINT

L'équipe de recherche informatique de Cyberint explore les limites du paysage des cybermenaces pour conserver une visibilité stratégique sur les menaces courantes. Elle analyse d'énormes quantités de données pour créer des rapports stratégiques de renseignement sur les menaces, permettant aux preneurs de décisions d'identifier les tendances significatives et d'acquérir une perspective plus large et plus approfondie des risques numériques pouvant affecter leur entreprise. Le rapport inclut une analyse régulière des risques actuels posés au secteur, des principaux vecteurs de menace, une analyse des outils, tactiques et procédures, etc.

DERNIERS RAPPORTS CYBERINT

Secteur financier des Philippines
Rapport sur le paysage des menaces

TÉLÉCHARGER

REvil - Vol, chiffrement et vente aux enchères
Rapport de recherche

TÉLÉCHARGER

Attaques ciblées de ransomwares à Taiwan
Rapport de recherche

TÉLÉCHARGER

Cyberint Copyright © Tous droits réservés 2020

AVANTAGES DU PARTENARIAT AVEC LES SERVICES GÉRÉS DE RENSEIGNEMENT SUR LES MENACES DE CYBERINT

DÉTECTION DES MENACES

Détecter les menaces grâce à l'intelligence prédictive

ÉVALUER LA GRAVITÉ

Évaluer la gravité des menaces et comprendre la vue d'ensemble

CAPACITÉS HUMINT VIRTUELLES

Communiquer directement avec les vecteurs de menaces, associer leur activité à des campagnes particulières et acquérir plus de contexte et de renseignements.

IDENTIFIER LES FRAUDES

Identifier et fournir des informations exploitables pour réagir et protéger l'entreprise

DÉTECTION EN TEMPS RÉEL DU PHISHING

Opérations de détection et de déconnexion en temps réel des sites Web de phishing

ENQUÊTES SUR LES MENACES AUX VIP

Superviser la présence en ligne de la direction pour empêcher les vecteurs de menace d'obtenir des informations personnelles à des fins malveillantes.

CARTOGRAPHIE ET SUPERVISION

Cartographier et superviser la présence numérique de l'entreprise, y compris les fuites de codes d'accès, les vulnérabilités numériques et les fuites de documents sensibles.

Cyberint Copyright © Tous droits réservés 2020

Gartner peerinsights™ 4.8

FROM OUR CUSTOMERS

C'est le service géré qui offre une véritable valeur pour transformer des découvertes en informations pertinentes et en alertes adaptées à notre activité.

Grand détaillant basé aux États-Unis

Il est impossible de vraiment comprendre qui essaye d'attaquer votre entreprise avant d'utiliser Cyberint.

Grand détaillant de commerce en ligne basé aux États-Unis

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

ÉTATS-UNIS
214 W 29th St.
New York, 10001
Tél: +1-646-568-7813

ISRAËL
17 Ha-Mefalsim St.
4951447 Petah Tikva
Tél: +972-3-7286-777

ROYAUME-UNI
14 Grays Inn Rd., Holborn
WC1X 8HN, Londres
Tél: +44-203-514-1515

SINGAPOUR
135 Cecil St. #10-01 MYP
PLAZA 069536
Tél: +65-3163-5760

LATAM
Panama City
Tél: +1-929-399-8495

FRANCE
67 Avenue de Wagram
75008 Paris
Tél: +33-1-77-50-5891

Cyberint Copyright © Tous droits réservés 2020