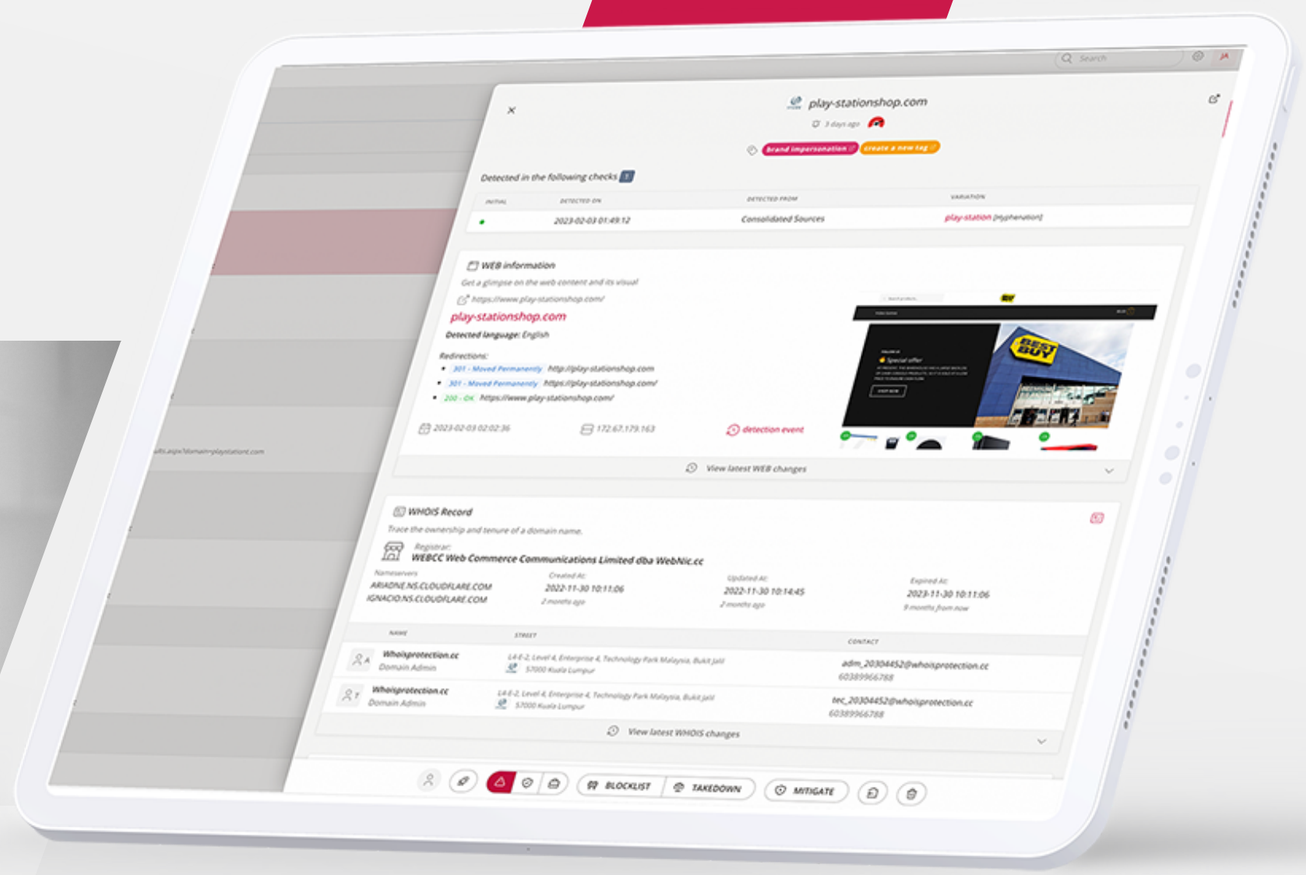
Fiche d'information sur la solution

Découvrir, contrer et prévenir les menaces numériques pesant sur votre organisation

PROTECTION CONTRE LES RISQUES NUMERIQUES



01

Faits et tendances

L'augmentation rapide de la cybercriminalité et des attaques numériques contre les organisations nécessite une protection holistique et continue des actifs numériques et des employés d'une organisation. Pour rester à l'abri des risques graves de cybersécurité, des fuites de données et des risques de conformité, les stratégies de sécurité des entreprises doivent adopter une approche de bout en bout qui identifie les menaces de manière proactive, fournit des renseignements exploitables qualifiés grâce à l'IA, prend des mesures rapides et ciblées, et fournit des conseils pour prévenir les attaques futures. En outre, une technologie de pointe doit être associée à des conseils professionnels d'experts pour rester en tête dans la course à la menace numérique.

Le Internet Crime Complaint Center du FBI 2021: augmentation de 7 % des cas par rapport à 2020, avec des pertes potentielles dépassant 6,9 milliards de dollars.

Le rapport d'INTERPOL sur les tendances mondiales en matière de criminalité classe le phishing et les escroqueries en ligne au premier rang des menaces de criminalité pour l'Europe.

Augmentation significative des cas d'hameçonnage et d'attaques de logiciels malveillants comme première étape de la cybercriminalité, entraînant des pertes de données, des atteintes à la réputation et un ralentissement, voire un arrêt de la production.

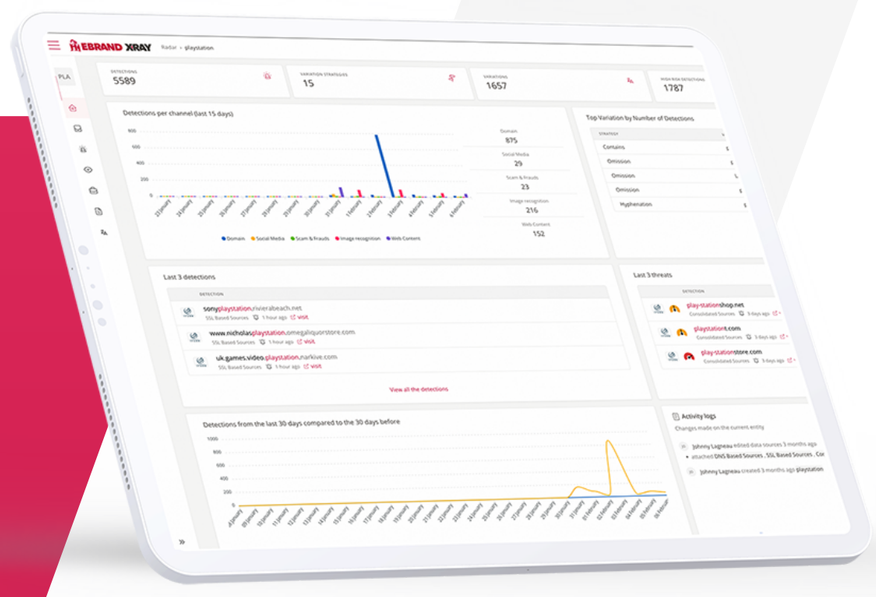
Le coût moyen mondial d'une violation de données en 2022/23 est de 4,35 millions de dollars.

Défis communs aux organisations

02

- Protégez vos clients, partenaires et fournisseurs contre les attaques de phishing.
- Détectez les sites Web frauduleux qui nuisent à votre marque et volent votre trafic, notamment les escroqueries suivantes : emploi, avance de fonds ou achat en ligne, investissement, crypto-monnaie, abonnement, programme d'affiliation.
- Lutter contre le hameçonnage des données grâce à de faux jeux et tombolas.
- Évitez les tentatives d'usurpation d'identité de vos employés sur les réseaux sociaux (spear phishing) ou de leur mail (Business Email).
- Protégez vos employés contre la prise de contrôle de leur compte par le biais d'identifiants d'utilisateurs piratés.
- Protégez vos clients en trouvant les données des clients violées sur le dark web.
- Protégez votre marque et vos leaders contre les usurpations d'identité sur les médias sociaux.
- Contrer les applications illégitimes ou fausses sur les app stores, mettant en danger vos clients.
- Effectuez des contrôles de conformité et de risque numérique et surveillez votre surface de menace externe.

Solution



La protection EBRAND contre les risques numériques utilise notre plateforme technologique avancée X-RAY pour découvrir en permanence et éliminer plus tôt les menaces externes , mettre fin à l'utilisation abusive de votre organisation et protéger vos employés contre la prise de contrôle de leur compte. Trouvez les domaines, les applications mobiles, les comptes de médias sociaux ou les contenus sur le web qui usurpent l'identité de votre marque et supprimez ce qui met en danger vos clients, vos employés et votre organisation. Voyez quels sites et comptes d'utilisateurs sont attaqués, quelles techniques ont été utilisées et si les informations d'identification ont été compromises. La solution EBRAND "Protection contre les risques numériques" est axée sur la protection des actifs, des clients, des employés et de la propriété intellectuelle (PI).

1 **Hiérarchisation automatisée** des détections à l'aide de la technologie X-RAY et de l'apprentissage automatique/IA avancé. Utilisation de sources de données complètes et d'un moteur de permutation avancé.

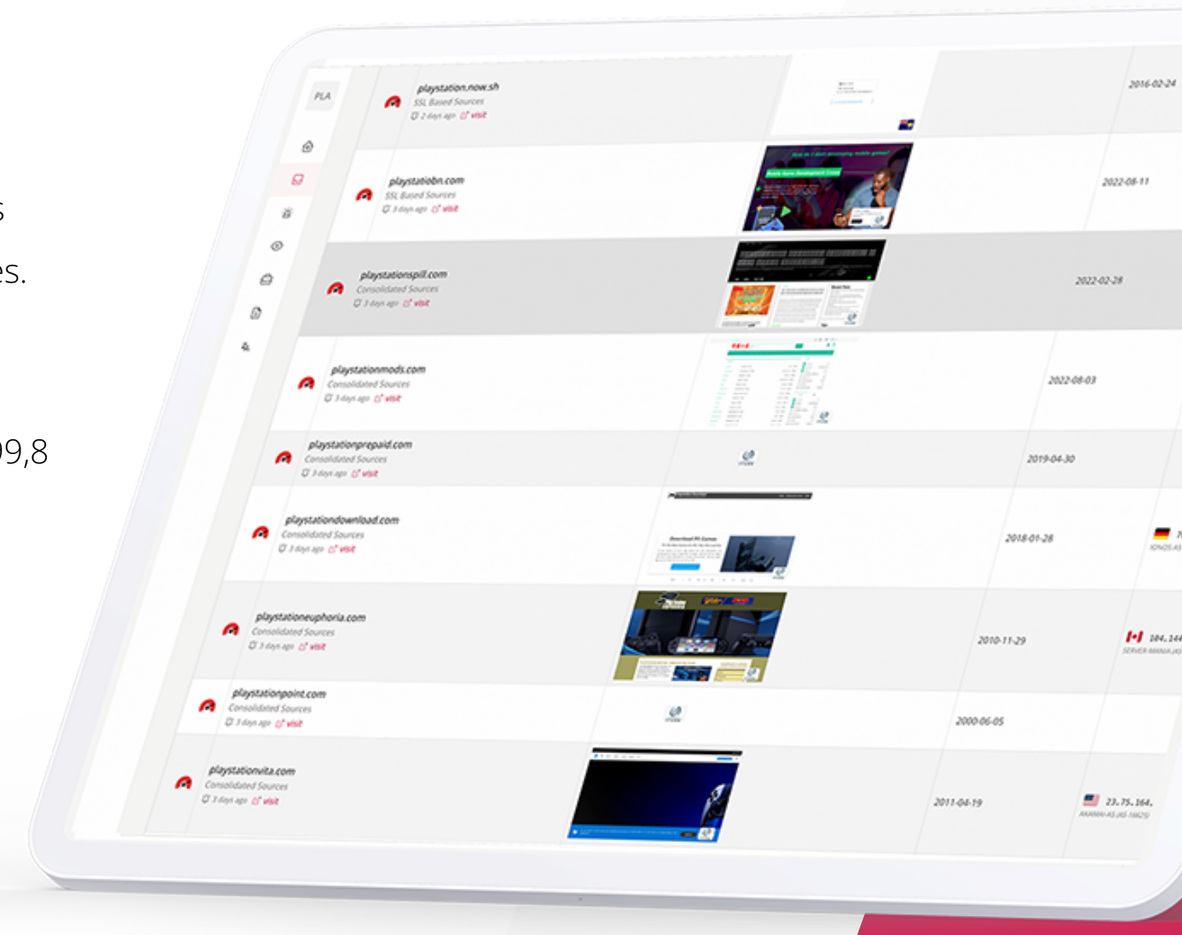
2 **Alerte en temps réel** - Détection rapide et précoce grâce à une surveillance holistique continue.

3 **Flux de travail collaboratifs** pour les interactions entre équipes.

4 **Rapports automatisés** aux listes de blocage mondiales, y compris les navigateurs, les logiciels de sécurité et les vastes réseaux de partenaires.

5 **Automatisation du déréférencement** avec un taux de réussite de 99,8 % et blocage en quelques minutes.

6 **Enregistrement de domaines de protection** - obtenez des informations sur les domaines que vous devriez posséder à titre préventif, sur la base du rapport entre le coût et la probabilité d'une attaque.



EBRAND

ebrand.com

Fonctionnalités

03

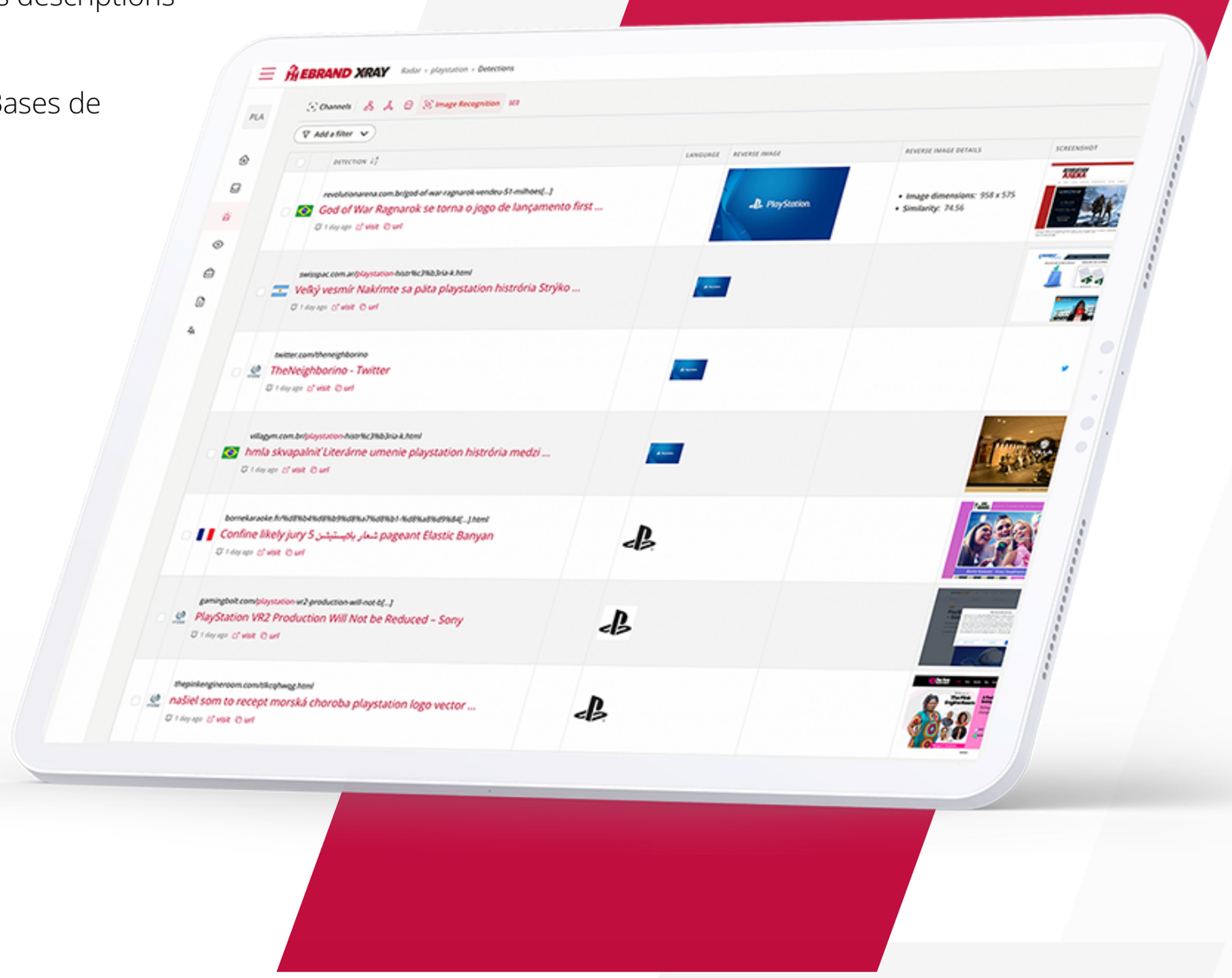
Technologie

RADAR – Protection numérique contre les risques

Détection précoce des signaux liés aux menaces externes visant les actifs du client et se faisant passer pour ou exploitant les canaux formels entrants et sortants du client, tels que les clients, partenaires, transporteurs, fournisseurs et prestataires.

Un large éventail de plus de 1 000 sources de données réparties sur différents canaux.

- Canal du domaine - DNS, SSL et autres sources.
- Canal de contenu Web - résultats de recherche ciblés, logo et recherche d'images.
- Canal des médias sociaux - Recherche dans les profils et les descriptions dans les réseaux sociaux pertinents.
- Dark Web Channel - Forums non publics, Dark/deep web, Bases de données des brèches, Canaux Telegram non publics.



Analyse des menaces par l'IA

- Qualification visuelle avancée.
- Qualification intelligente du contenu.
- Analyse de la réputation.
- Analyse de la proximité des marques.

Automatisation de la plateforme

- Hiérarchisation automatisée des détections.
- Rapport automatisé aux listes de blocage mondiales.
- Processus automatisé de retrait légal.
- Alerte en temps réel 24/7.

Plateforme de bout en bout

- Collaborez en temps réel en attribuant, gérant et transmettant les menaces.

Contre-mesures

- Demandez à nos experts juridiques de retirer les menaces identifiées.
- Bloquez les découvertes malveillantes directement via la plateforme.

Open Intelligence

X-RAY peut s'intégrer à votre système d'information par API, web-hook, ou intégration personnalisée, pour pousser des détections ou bloquer des sites malveillants.

Tracker

- Surveillance et inventaire continus des menaces potentielles telles que les pages parking ou les domaines suspects.
- Recensement des points aveugles de votre infrastructure vus par les attaquants externes : chemins de prise de contrôle de domaines et sous-domaines, certificats expirés, expiration des enregistrements, etc.
- Surveillance et évaluation des risques de votre propre portefeuille de domaines.

Surveillance des menaces

Surveiller les sites Web de tiers pour recueillir des preuves de changements dans la configuration technique, le contenu ou la conception.
Être alerté dans l'heure qui suit de tout changement technique ou de contenu dans une ressource surveillée.

- Surveiller les activités suspectes sur le web, comme les pages parking et les domaines proches de votre marque, qui pourraient potentiellement vous nuire.
- Surveillez les atteintes potentielles à la propriété intellectuelle et l'utilisation non autorisée de votre marque et rassemblez automatiquement les preuves nécessaires à des actions en justice.

Surveillance des actifs

Surveillez vos propres actifs destinés au public pour évaluer les vulnérabilités et prévenir les violations en évitant:

- Chemins de reprise des domaines et sous-domaines.
- Mauvaise configuration publique.
- Vulnérabilités non corrigées.
- Certificats SSL expirés.
- Enregistrements de domaines expirant.

Services

Services gérés

Nos experts en sécurité gèrent votre programme et prennent en charge les tâches quotidiennes liées au suivi des résultats, des infractions ou des menaces. L'équipe couvrira les fonctions suivantes:

- Évaluation initiale du paysage des menaces et de vos priorités afin de créer une surveillance personnalisée.
- Priorité et traitement des flux de travail en fonction des exigences du client.
- Contrer les menaces en prenant des mesures pré-approuvées ou en signalant les cas via la plateforme.
- Examen continu des résultats des analyses et des menaces.
- Ajustement continu du programme pour optimiser les scans, les flux de travail et les résultats afin de maximiser l'impact du programme.
- Rapports personnalisés en fonction des besoins individuels.

Possibilité d'utiliser le portail X-RAY en libre-service pour:

- Recevoir des notifications claires et exploitables.
- Assigner des cas à un autre utilisateur.
- Commentaires sur les affaires.
- Étiquetage des éléments par des étiquettes et des groupes d'étiquettes personnalisés.
- Création de rapports personnalisés.
- Blocage de sites web et demande de services de retrait.

04

À propos de EBRAND

EBRAND aide les grandes entreprises à dynamiser et à protéger leurs activités à l'ère du numérique en préservant la réputation en ligne, en protégeant les consommateurs et en améliorant la présence de la marque. En tant que leader dans le domaine de la gestion des domaines d'entreprise (CDM), de la protection de la marque en ligne (OBP) et de la protection contre les risques numériques (DRP), la société déploie des technologies avancées alimentées par l'intelligence artificielle, soutenues par des services professionnels, et fournit la solution la plus complète pour couvrir les besoins uniques et divers et les risques auxquels tous les secteurs et types d'organisations sont confrontés à l'ère numérique. En tant que fournisseur certifié ISO 27001 basé en Europe et disposant de bureaux en Allemagne, en Angleterre, en Belgique, en Chine, au Danemark, en Espagne, en France, au Luxembourg, aux Pays-Bas et en Pologne, nous sommes fiers de notre histoire de plus de 15 ans de partenariat avec des centaines d'entreprises clientes et un réseau de partenaires industriels de premier plan.

EBRAND

Pour en savoir plus, consultez le site ebrand.com