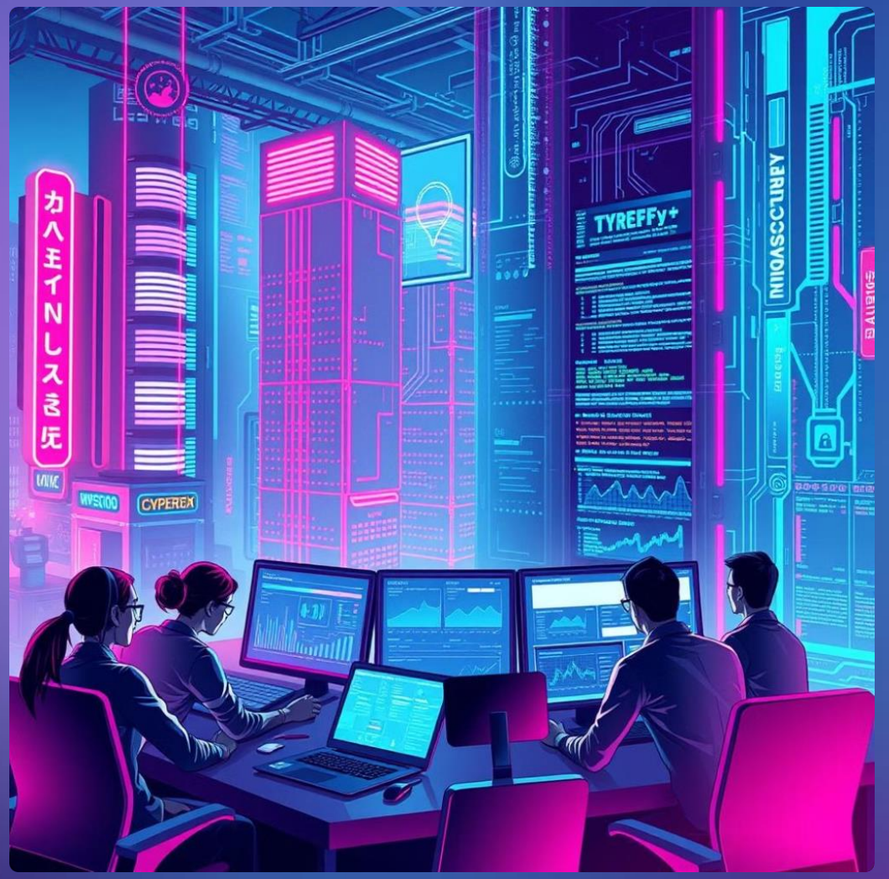
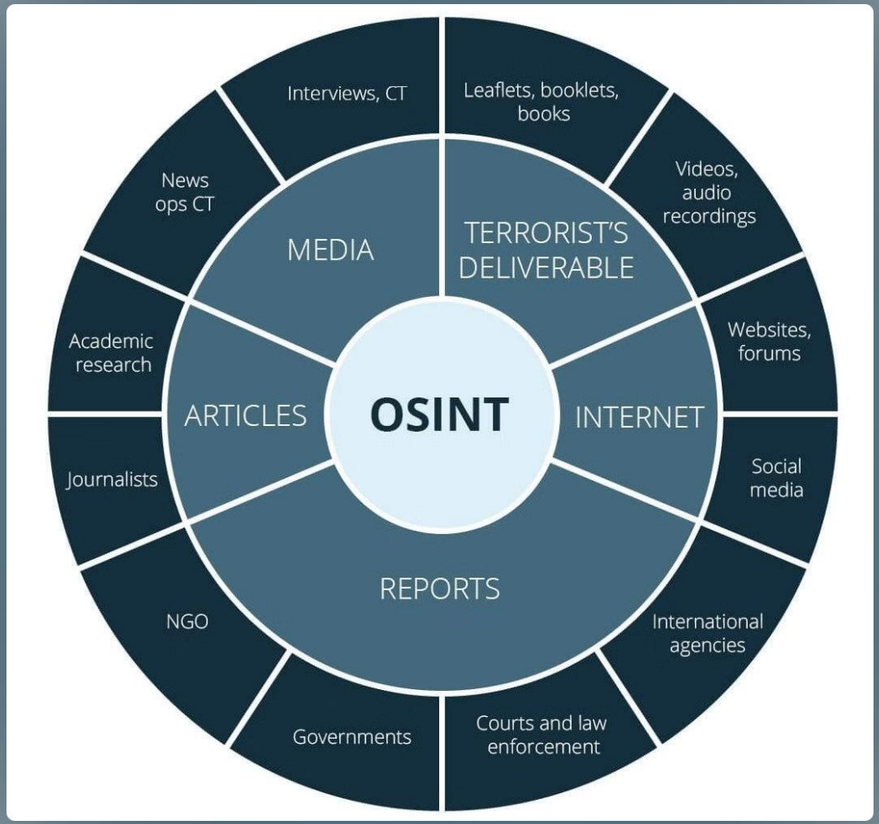
La découverte des actifs numériques grâce à l'OSINT

L'OSINT (Open Source Intelligence) peut être utilisée par les attaquants pour identifier des actifs et rassembler d'autres informations utiles avant le lancement d'une attaque. Cependant, une approche constructive de la découverte d'actifs permet aux entreprises de reconnaître les domaines à risque préalables. La découverte des actifs numériques est essentielle pour cartographier la surface d'attaque et réduire les interruptions.





Qu'est-ce que l'OSINT ?

1 Informations légitimes

L'OSINT se réfère à toute information légalement collectée sur Internet, qu'il s'agisse de données publiques ou de sources ouvertes.

2 Profiler une cible

En collectant des informations accessibles en ligne, un attaquant peut dresser le profil d'une cible potentielle afin de mieux comprendre ses capacités et trouver des vulnérabilités.

3 Sécuriser son entreprise

Les entreprises doivent connaître les informations publiquement disponibles pour les hackers afin de durcir leur sécurité et réduire leur surface d'attaque.

Découverte WHOIS

Identification des Propriétaires

Permet de trouver des informations sur le propriétaire d'un domaine, y compris son nom et ses coordonnées.

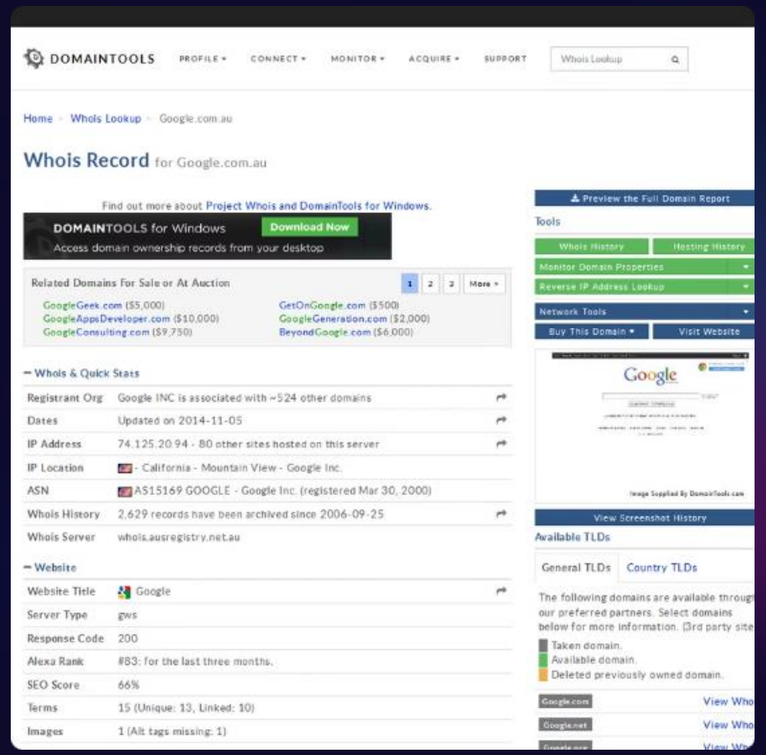
Analyse de Risques

Aide à détecter des activités suspectes en fournissant des données historiques sur l'enregistrement des domaines.

Point de Départ pour les Enquêtes

Sert de base pour approfondir les investigations sur des incidents de cybersécurité ou des fraudes en ligne.

Découverte WHOIS

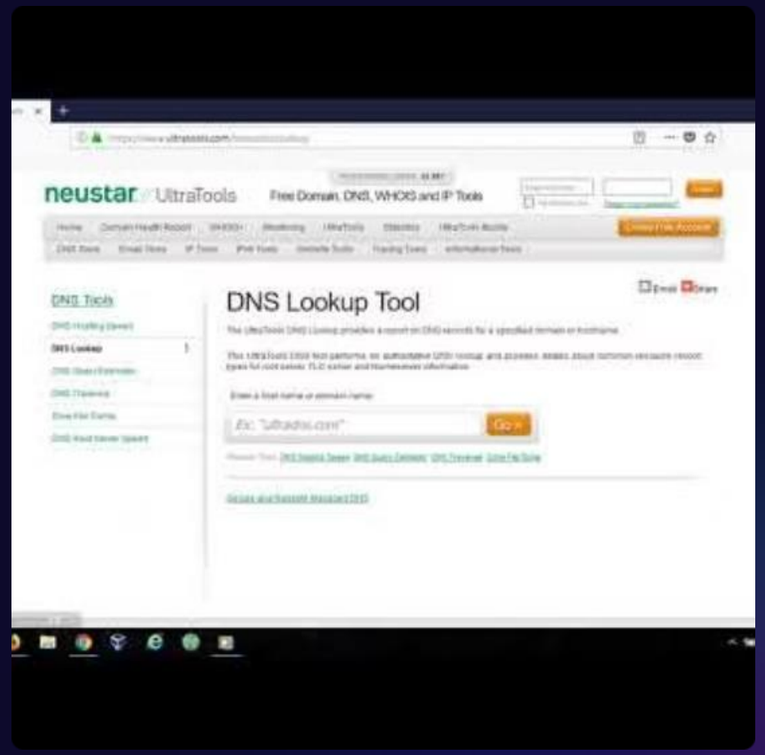


Domaintools – WHOIS

La recherche peut être effectuée facilement en entrant un nom de domaine ou une adresse IP. En outre, différentes options de recherche sont disponibles, telles que l'IP inversée, les domaines associés à ces IP, etc.

whois.com

Vous pouvez suivre la propriété et la détention du nom de domaine avec la recherche WHOIS.



Neustar UltraTools

Vous pouvez découvrir qui possède le domaine, où il a été enregistré, quand il expire, comment contacter le propriétaire du domaine, et plus encore.

Domaines associés

Identification de Relations

Permet de découvrir les domaines liés à un même propriétaire, facilitant la cartographie des réseaux d'entités.

Analyse de Comportement

Aide à détecter des modèles de comportement en examinant les connexions entre différents domaines, ce qui peut indiquer des activités malveillantes.

Évaluation de Risques

Fournit des insights sur des acteurs potentiellement dangereux en reliant plusieurs domaines associés à des incidents de cybersécurité ou à des fraudes.

Domaines associés

Whoxy

Whoxy est un moteur de recherche de domaines dont l'API vous permet de rechercher rapidement les données WHOIS d'un nom de domaine. Si vous avez accédé à des informations telles que le nom du propriétaire via le registre whois, vous pouvez également accéder à d'autres domaines acquis par ce propriétaire en entrant ces informations sur Whoxy. Dans ce cas, vous accéderez très probablement à d'autres domaines liés de l'institution.

SpyOnWeb

SpyOnWeb.com prend des informations provenant de sources publiques et les structure ensuite pour rechercher facilement et commodément les lieux susceptibles d'appartenir au même utilisateur. Les données suivantes sont extraites de leur robot d'exploration : Adresse IP, Identifiant Google Adsense, Identifiant Google Analytics.

Découverte d'enregistrements DNS

Extraction d'Informations Techniques

Permet d'obtenir des détails sur la configuration d'un domaine, tels que les enregistrements A, MX, et TXT, révélant des informations sur les serveurs et services associés.

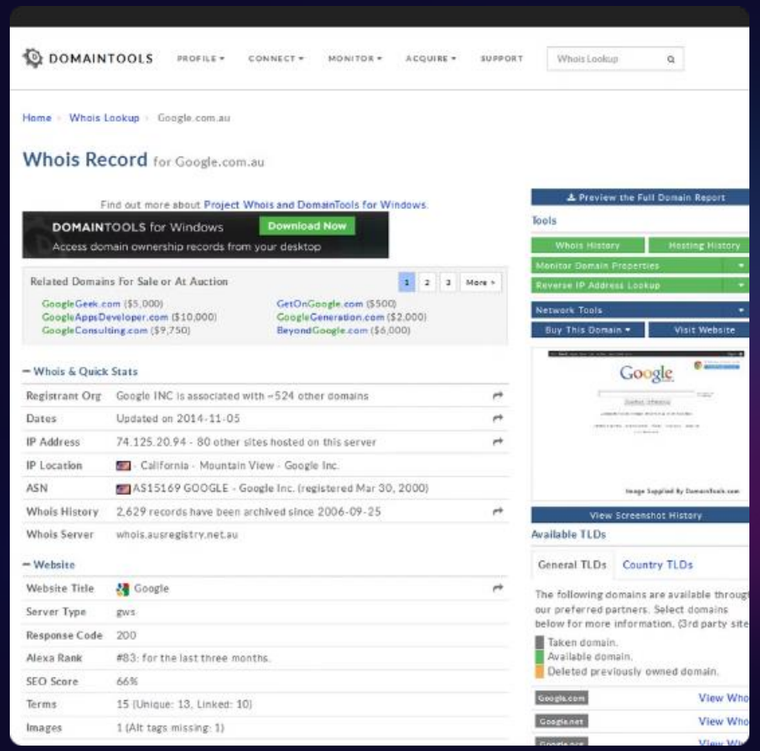
Analyse de la Sécurité

Aide à identifier des vulnérabilités potentielles en révélant des configurations incorrectes ou des enregistrements suspects liés à des activités malveillantes.

Suivi des Changements

Facilite la surveillance des modifications d'enregistrements DNS dans le temps, permettant de détecter des changements suspects ou inattendus dans la gestion d'un domaine.

Découverte d'enregistrements DNS



Pentest Tool

Pentest tool vous permet de lancer une recherche en entrant un domaine, et en fonction du nombre de domaines que vous trouverez, vous recevrez le rapport dans un court laps de temps.

Security Trails

Security Trails répertorie, avec les fournisseurs d'hébergement et de messagerie, tous les sous-domaines d'un domaine racine

Spyse

Spyse vous permet de rechercher les sous-domaines de n'importe quelle base de données.

Découverte de sous-domaines

Identification de Services Associés : Permet de révéler des sous-domaines liés à un domaine principal, fournissant des informations sur les services ou applications hébergés.

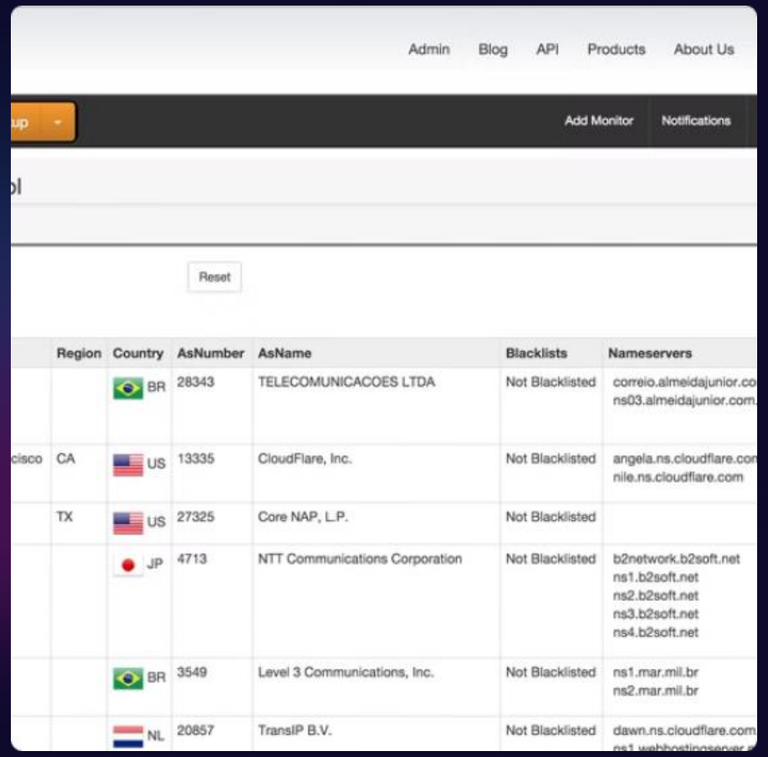
Analyse de Surface d'Attaque Aide à étendre la surface d'attaque potentielle en identifiant des sous-domaines vulnérables qui pourraient être exploités par des acteurs malveillants.

Cartographie de l'Infrastructure Facilite la compréhension de l'architecture d'un domaine, permettant de visualiser les relations entre le domaine principal et ses sous-domaines.

Découverte de sous-domaines

DNSdumpster

DNSdumpster est une plateforme d'analyse de domaine gratuite pour trouver des hôtes liés à un domaine. Les hôtes visibles sont des éléments essentiels dans le processus d'évaluation de la sécurité du point de vue des attaquants.



MXToolbox

La recherche MX est effectuée directement contre le serveur de noms de domaine autoritaire, donc les enregistrements MX devraient être mis à jour instantanément.

Hackertarget

C'est un scanner de vulnérabilités en ligne pour cartographier la surface d'attaque et identifier les vulnérabilités.

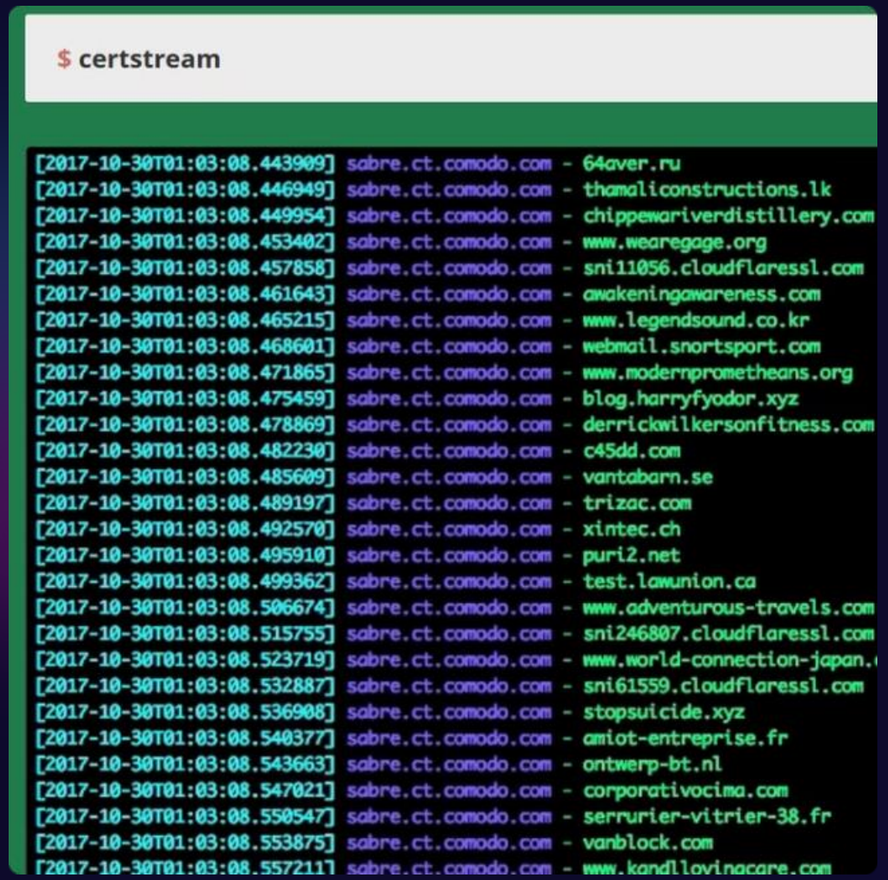
Découverte des certificats SSL

Vérification de l'Authenticité
Permet d'analyser les certificats SSL d'un domaine pour confirmer son identité et sa légitimité, ainsi que celle des entités associées.

Identification de Certificats Expirés ou Vulnérables
Aide à détecter des certificats SSL obsolètes ou mal configurés, ce qui peut exposer un domaine à des risques de sécurité.

Recherche de Liens entre Domaines
Facilite la découverte de domaines associés en analysant les certificats SSL partagés, révélant des connexions entre différentes entités ou infrastructures.

Découverte des certificats SSL



Certstream

CertStream est un flux de renseignemnt qui fournit des alertes en temps réel provenant du réseau Certificate Transparency Log, ce qui vous aide à créer des outils qui réagissent en temps réel aux nouveaux certificats qui sont publiés.

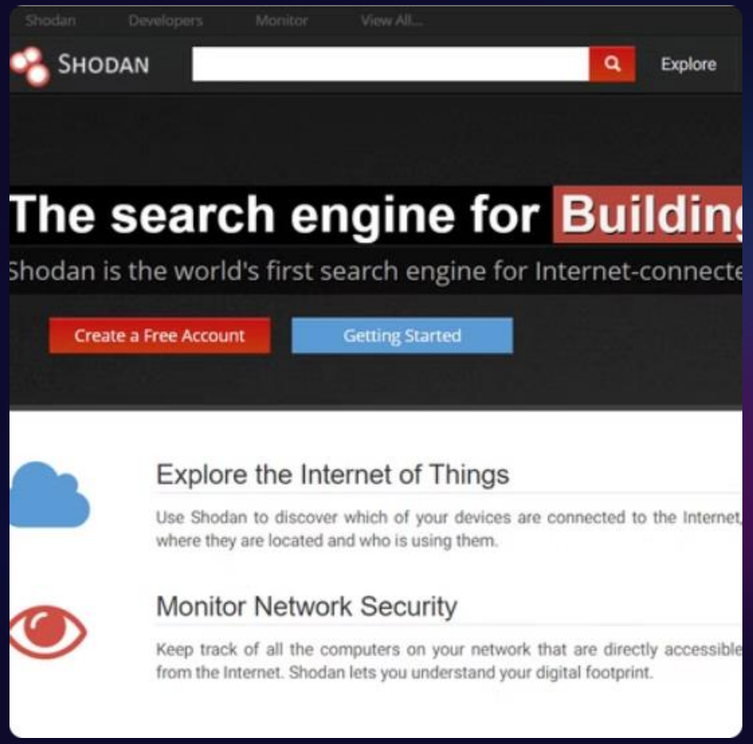
Infrastructure réseau et analyse passive

Cartographie de l'Infrastructure
Permet de visualiser l'architecture réseau d'une organisation en identifiant les adresses IP, les sous-réseaux et les équipements connectés.

Analyse Passive des Flux de Données
Facilite l'examen des données sans interaction directe, permettant de recueillir des informations sur le trafic réseau, les protocoles utilisés et les communications entre systèmes.

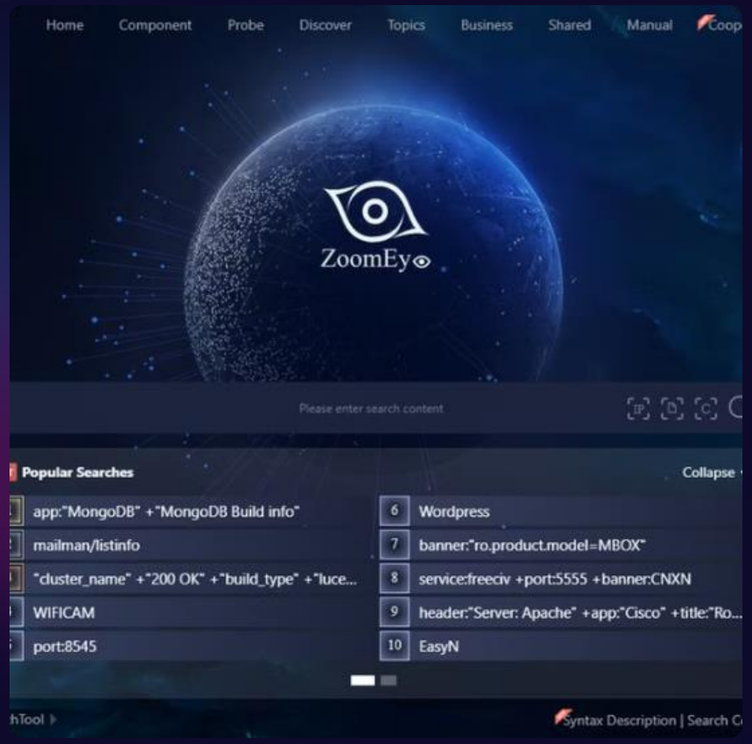
Détection d'Anomalies
Aide à identifier des comportements atypiques ou suspects au sein de l'infrastructure, contribuant à la prévention des attaques et à la sécurisation des réseaux.

Infrastructure réseau et analyse passive



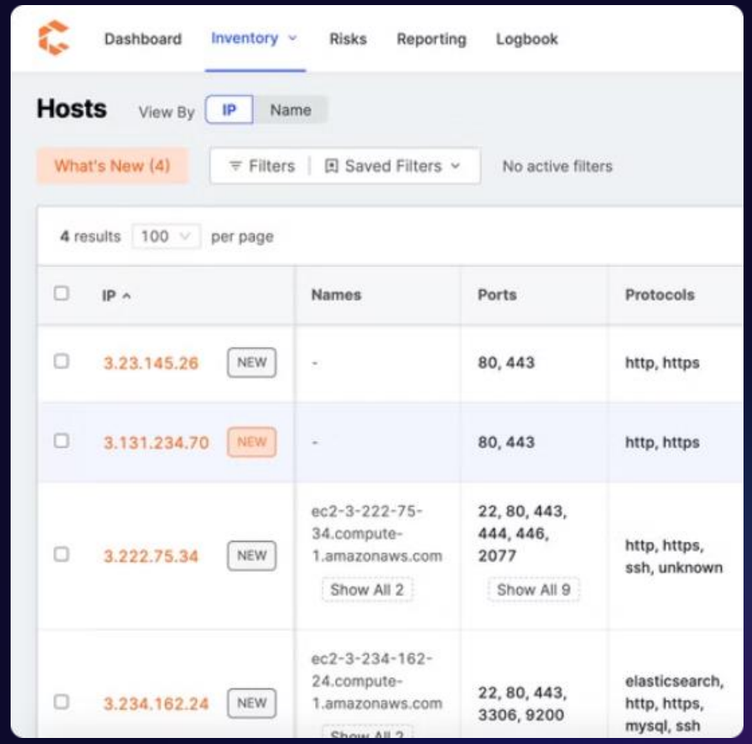
Shodan

Shodan est un moteur de recherche spécialisé dans les appareils connectés à Internet, permettant d'identifier les services, versions et ports ouverts.



ZoomEye

ZoomEye est un moteur de recherche de l'espace cybernétique qui recense les informations sur les appareils, sites web, services et composants.



Censys

Censys aide à découvrir, gérer et remédier aux risques dans l'environnement numérique d'une organisation.

Découverte des domaines de phishing

Identification de Domaines Malveillants

Permet de détecter des domaines similaires à ceux d'organisations légitimes, souvent utilisés pour du phishing, en analysant les variations dans les noms de domaine.

Surveillance des Signaux de Compromission

Facilite la détection d'activités suspectes en surveillant les nouveaux enregistrements de domaines, ce qui peut indiquer des tentatives de phishing en cours.

Analyse des Modèles de Phishing

Aide à comprendre les techniques utilisées par les cybercriminels, en examinant les domaines associés à des campagnes de phishing précédentes pour anticiper de futures menaces.

Découverte des domaines de phishing

DNSlytics

Cet outil affiche tous les domaines avec une différence d'un caractère par rapport au nom de domaine donné.

NormShield

Translate La détection des domaines de phishing de NormShield génère des combinaisons de mots à partir de votre nom de domaine avec des algorithmes spécifiques et recherche ces noms générés dans toutes les bases de données de noms de domaine. Avec ce service, vous pouvez identifier les noms de domaine de phishing possibles enregistrés pour des cyberattaques.

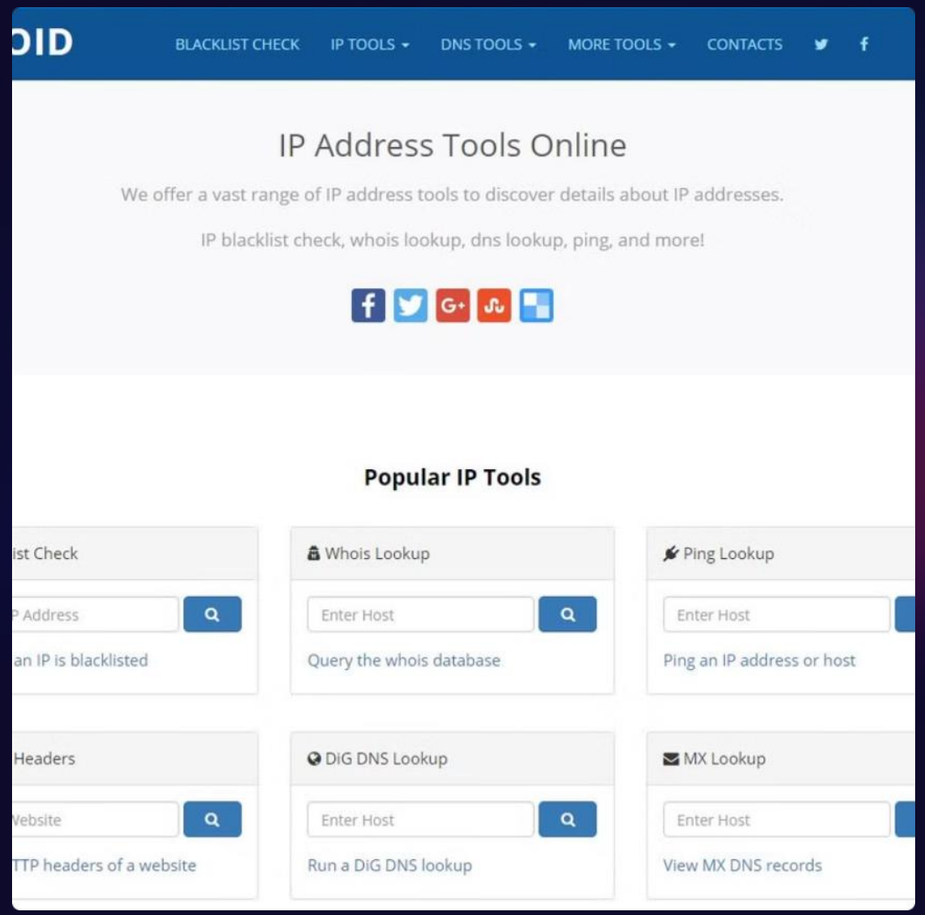
Découverte des adresses IP bloquées

Identification des Adresses IP Malveillantes
Permet de détecter des adresses IP figurant sur des listes noires, souvent utilisées pour des activités frauduleuses ou malveillantes, comme le spam ou les attaques par déni de service (DDoS).

Analyse des Comportements Anormaux
Facilite l'examen des historiques d'activité des adresses IP pour identifier des comportements suspects ou des connexions à des réseaux compromis.

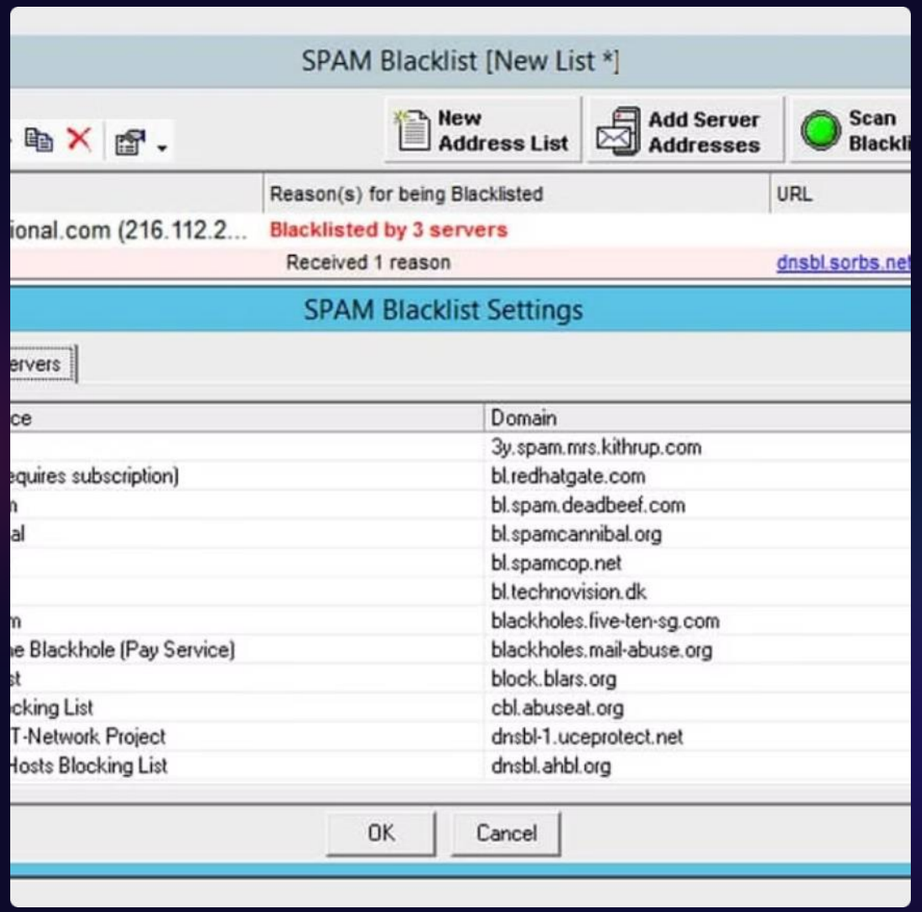
Surveillance de la Sécurité Réseau
Aide à renforcer la sécurité des systèmes en fournissant des informations sur les adresses IP bloquées, permettant de prévenir d'éventuelles intrusions ou attaques.

Découverte des adresses IP bloquées



IPVOID

IPVOID permet de découvrir les détails d'une adresse IP, notamment si elle est présente dans des blacklists.



Spam Check

Spam Check vérifie si les adresses IP d'expédition de courriers indésirables sont bloquées par des serveurs DNS.

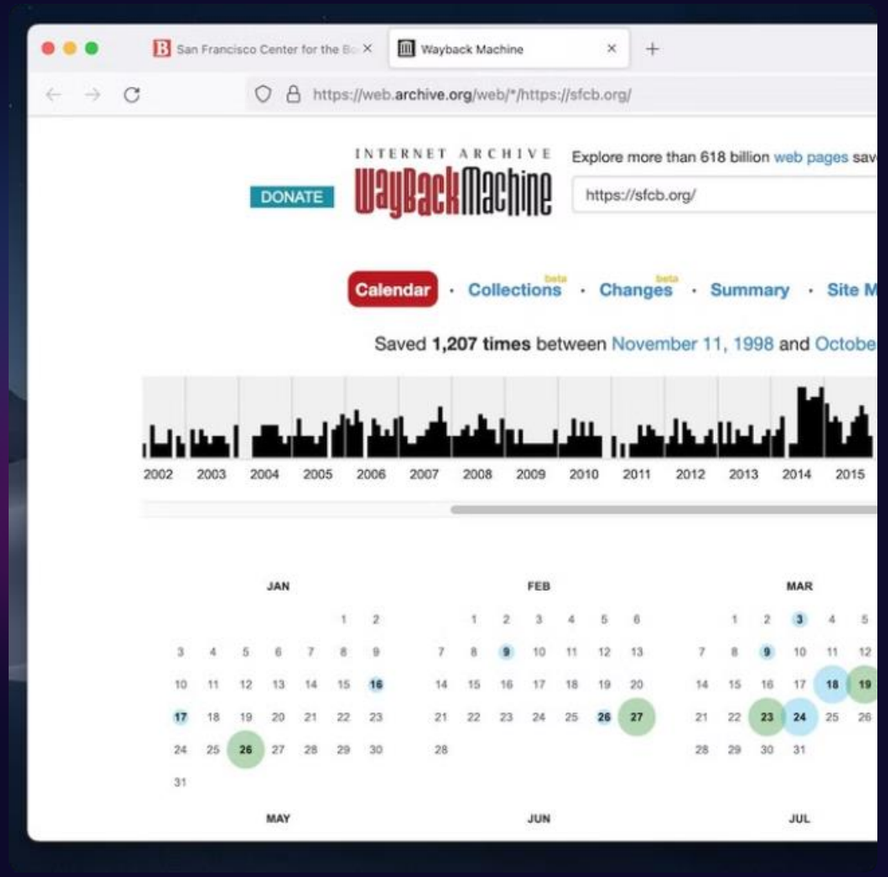
Anciennes versions des sites web

Accès à l'Historique des Changements
Permet d'explorer les versions précédentes d'un site web, fournissant un aperçu des modifications de contenu, de design et de structure au fil du temps.

Analyse des Pratiques et Contenus Anciens
Aide à identifier les pratiques commerciales, les offres de produits ou les informations qui peuvent avoir été supprimées ou modifiées, révélant des tendances ou des stratégies passées.

Recherche de Preuves
Facilite la collecte de preuves pour des enquêtes juridiques ou de sécurité, en permettant de documenter des informations qui ne sont plus accessibles sur le site actuel.

Anciennes versions des sites web



Wayback Machine

Avec Wayback Machine, les versions précédentes de n'importe quelle page web peuvent être consultées. Il est possible de recueillir des informations s'il y avait une vulnérabilité de sécurité dans l'ancienne version.

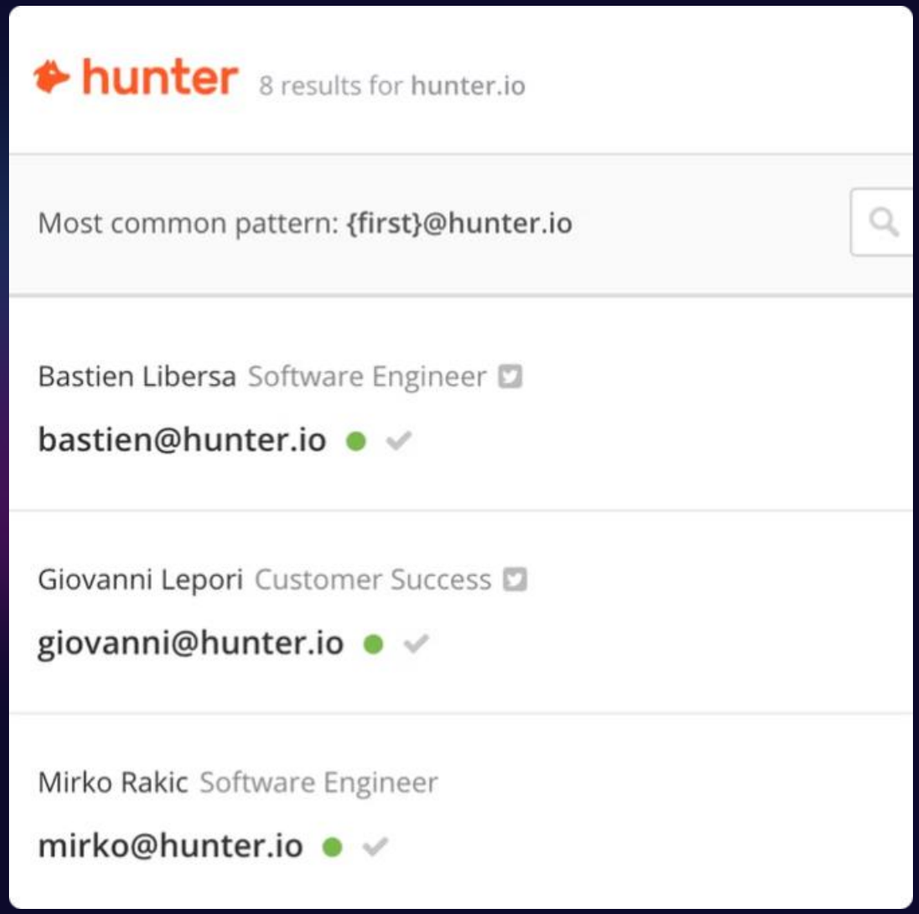
Emails d'entreprise

Identification des Contacts Clés
Permet de découvrir des adresses email associées à des employés ou des départements d'une entreprise, facilitant le ciblage pour des communications ou des enquêtes.

Évaluation de la Structure d'Email
Aide à analyser le format des adresses email utilisées par une entreprise, permettant d'estimer d'autres adresses potentielles en fonction de la structure identifiée (ex. : prénom.nom@entreprise.com).

Surveillance des Fuites de Données
Facilite la détection d'adresses email compromises en les recherchant dans des bases de données de violations de données, contribuant à la sécurité de l'entreprise et à la protection des informations sensibles.

Emails d'entreprise



Hunter.io

Les utilisateurs d'entreprise dont les adresses e-mail ont été divulguées et le format d'e-mail de l'institution peuvent être connus.

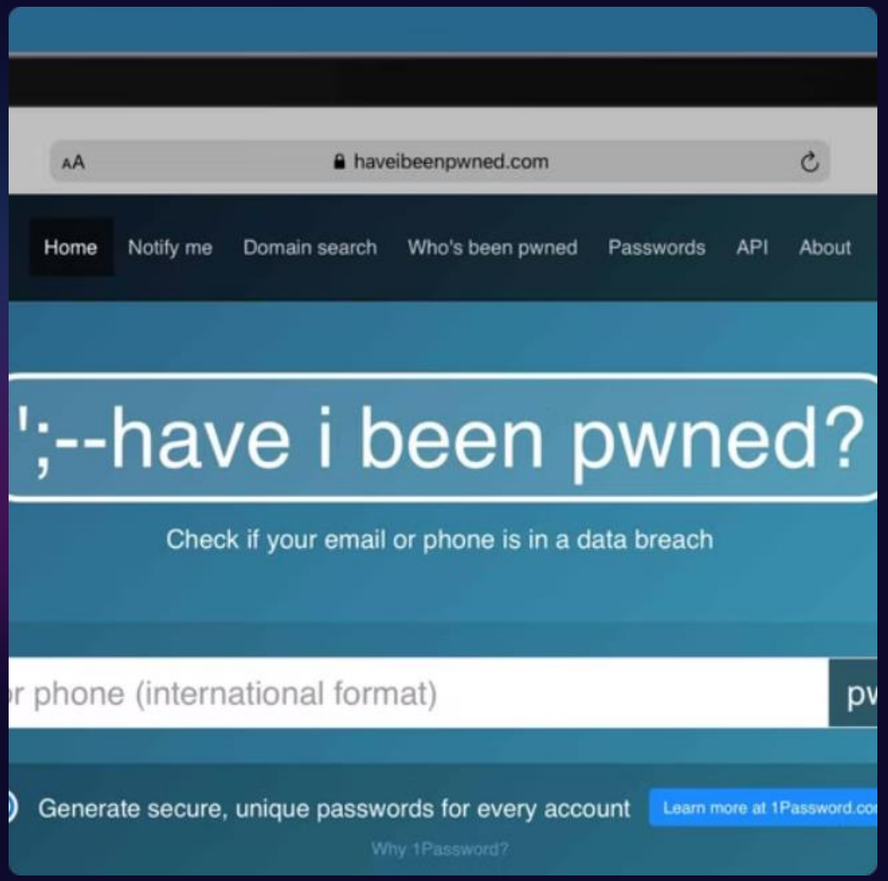
Mots de passe compromis

Vérification des Fuites de Données
Permet d'explorer des bases de données de violations pour identifier des mots de passe associés à des comptes d'utilisateurs compromis, renforçant ainsi la sécurité.

Analyse des Pratiques de Sécurité
Aide à évaluer la robustesse des mots de passe utilisés par une organisation, mettant en lumière des mots de passe faibles ou courants qui pourraient être facilement exploités.

Sensibilisation des Utilisateurs
Facilite la sensibilisation à la sécurité en alertant les utilisateurs sur les mots de passe compromis, encourageant l'adoption de meilleures pratiques de création et de gestion des mots de passe.

Mots de passe compromis



Have I Been Pwned

CertStream est un flux de renseignemnt qui fournit des alertes en temps réel provenant du réseau Certificate Transparency Log, ce qui vous aide à créer des outils qui réagissent en temps réel aux nouveaux certificats qui sont publiés.

Avantages de la découverte d'actifs numériques

Détection des fuites de données

L'OSINT permet d'identifier rapidement les fuites de données confidentielles publiées en ligne, afin de les sécuriser.

Analyse des failles de sécurité

La découverte d'actifs est essentielle pour cartographier la surface d'attaque et identifier les vulnérabilités à corriger.

Cartographie de la surface d'attaque

En répertoriant tous les éléments exposés, la découverte d'actifs permet de mieux protéger l'entreprise contre les cybermenaces.

Conclusion : la clé d'une cybersécurité renforcée

La découverte proactive des actifs numériques à l'aide de l'OSINT est un outil essentiel pour les entreprises soucieuses de leur sécurité. En identifiant les informations publiquement accessibles, les organisations peuvent mieux cartographier leur surface d'attaque, détecter les failles et fuites de données, et se prémunir contre les cybermenaces. Une approche globale de la découverte d'actifs est la clé d'une cybersécurité renforcée et durable.