DomainTools

Transformer les données de domaines en intelligence contre les attaques

Phishing, Command & Control, usurpation, etc., les attaquants sont dépendants d'IP et de domaines malveillants pour concevoir et distribuer leurs attaques. Maîtriser les données des domaines, c'est voir venir les attaques.

DomainTools transforme les données de domaines en intelligence contre les cyberattaques. Par une analyse approfondie, DomainTools évalue les risques ou la réputation, profile les attaquants, guide les investigations, et cartographie la cyber activité malveillante. Les opérateurs de SOC, les analystes, les « *threat hunters* » ont à leur disposition une source unique d'informations exploitables automatiquement et instantanément par leurs outils (SOAR, SIEM, Threat Intel).

DETECT. INVESTIGATE. PREVENT.

DomainTools est une combinaison entre la base de données de domaines la plus riche du monde, issue de décennies de collectes, et une analyse prédictive, permettant une méthode unique de « **Risk-Scoring** » des domaines.

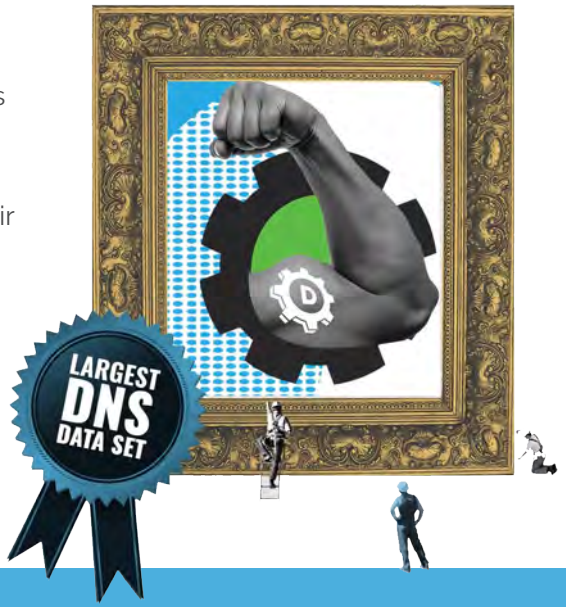
DETECTION
DomainTools utilise les indicateurs du réseau comme les IP et les domaines, puis les relie aux domaines actifs sur Internet.

INVESTIGATION
DomainTools créé une cartographie de l'activité malveillante liée aux domaines afin de trier les menaces et évaluer les risques.

INFORMATION ET CONTEXTUALISATION
DomainTools identifie potentiellement tout domaine malveillant avant son action, parfois avant même qu'il ne soit armé. Les faux positifs sont déclassés.

ENRICHISSEMENT
DomainTools accède à des dizaines d'attributs attachés aux domaines dans les SIEM, les solutions *Open Source* ou propriétaires pour enrichir à grande échelle les incidents

ORCHESTRATION
Forts de ces informations, les solutions d'orchestration comme les SOAR exploitent DomainTools pour trier les événements et agir de manière ciblée.

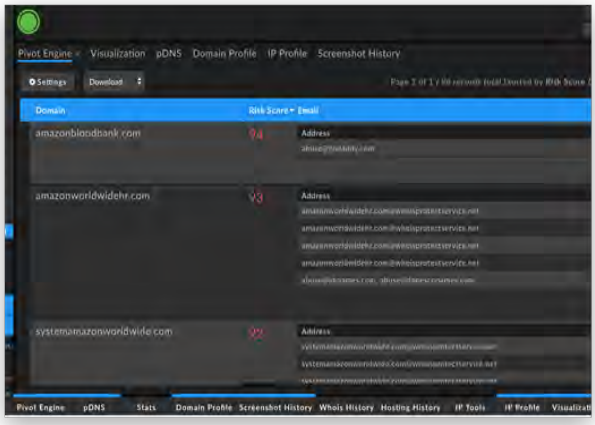


MIEL

Distribué en France par MIEL

01 60 19 34 52 - www.miel.fr/control-up

IRIS
La plateforme d'investigation



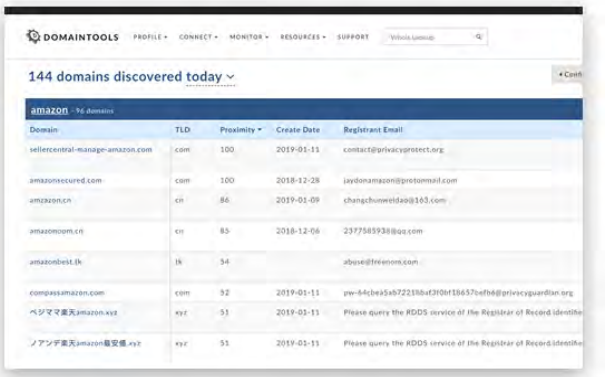
Iris est la plateforme d'investigation de DomainTools. Elle combine les techniques de « *risk-scoring* » avec les données DNS passives les plus riches de l'industrie.

- Evaluation rapide des risques
- Cartographie de l'infrastructure connectée
- Construction des profils
- Identification des tactiques d'attaques
- Monitoring des futurs changements

DOMAIN RISK SCORE
Prédiction des domaines malveillants

Domain Risk Score permet de mettre en place un processus efficace de détection et d'élimination de domaines malveillants avant même leur armement.

- Prédiction des domaines malveillants avant impact
- Information vers les process de «*threat hunting*» et réponse à incident
- Réduction drastique des risques venant de domaines inconnus ou nouveaux



PHISHEYE
Détection de noms de domaine usurpés

PhishEye permet de détecter les domaines dont le nom est usurpé ou vient d'être usurpé.

- Identification et alertes sur les noms de domaine usurpés à leur découverte/enregistrement
- Information et prédiction de risque sur les noms de domaine soumis à alerte

IRIS APIs
Enrichissement et orchestration

Les APIs permettent d'exploiter les informations de DomainTools dans les solutions SOAR, SIEM et de Threat Intelligence

- Interopérabilité native avec de nombreuses solutions
- Accès à la base Iris pour l'enrichissement contextuel et l'orchestration
- Exploitation de « Domain Risk-Score » pour l'investigation et la détection de menaces