SÉCURITÉ DOMAINE

Protection contre la Fraude Domaine et le Phishing

Détection de domaines similaires,
surveillance et takedown automatisé

DMARC EXPERT KFT

Votre partenaire de confiance en sécurité et délivrabilité email

contact@dmarc.fr | www.dmarc-expert.com

La menace des domaines similaires

Même avec DMARC en p=reject, les cybercriminels s'adaptent. Plutôt que d'usurper directement votre domaine, ils créent des **domaines similaires (typosquatting)** pour tromper vos clients, partenaires et collaborateurs. Ces domaines peuvent être utilisés pour des emails de phishing ciblés, de faux sites web ou des attaques de spear phishing sophistiquées.

< 24h	24/7	3 couches
Détection des nouveaux domaines	Surveillance automatique	Méthodologie de protection complète

Les 3 couches de protection DMARC EXPERT

1

Authentification Email — SPF + DKIM + DMARC

Première ligne de défense : s'assurer que seuls les systèmes autorisés envoient des emails depuis vos domaines officiels. Cette étape neutralise les attaques massives d'usurpation directe.

2

Surveillance des Domaines Similaires — DETECT

Surveillance permanente des nouveaux domaines similaires au vôtre : typosquatting, homoglyphes, variations orthographiques. Détection sous 24 heures sur l'ensemble des registrars mondiaux.

3

Blocage & Takedown Automatisé — DETECT PLUS / TAKEDOWN

Neutralisation active des domaines frauduleux identifiés : blocage immédiat dans les solutions de sécurité (Defender, Cisco, Symantec…) et lancement de procédures de takedown auprès des registrars et hébergeurs.

DETECT PLUS — Surveillance Étendue

DETECT PLUS offre une visibilité étendue : surveillance des certificats SSL (Certificate Transparency), monitoring des réseaux sociaux, détection de faux comptes et de pages usurpant votre marque. Les alertes sont accessibles via une **URL discrète dédiée**, sans installation requise.

Cas d'usage par secteur

Services Financiers	Faux portails bancaires, fraude au virement	ENTERPRISE + DETECT+ + TAKEDOWN
Énergie / Industrie	Spear phishing fournisseurs, fraude au président	ENTERPRISE + DETECT+
Distribution / Retail	Phishing clients, faux bons de réduction	PREMIUM + DETECT

Administration / Santé	Usurpation institutionnelle, ransomware	ENTERPRISE + DETECT+ + TAKEDOWN

Intégration SIEM : Les IOCs identifiés par DMARC EXPERT sont transmissibles directement à vos solutions SIEM, EDR et antispam (Microsoft Defender, Cisco IronPort, Symantec, Proofpoint) pour un blocage immédiat et automatisé.