Digital Threat Monitoring

Points forts

- Plus de 200 marketplaces, réseaux sociaux, forums de carding et sites de ransomwares surveillés
- Mots-clés personnalisables pour une solution sur mesure
- Nombre illimité d'utilisateurs
- Proposée sous forme de services managés ou autogérés

Open, deep, dark : une visibilité inégalée sur toutes les strates du web

Le rayon d'action des attaquants couvre aussi bien le web dit « de surface » que le deep et le dark web. Mais pour les repérer, encore faut-il savoir où chercher et parvenir à infiltrer leur milieu pour mieux écouter – et décoder – leurs conversations. En filtrant le brouhaha ambiant qui entoure leurs échanges, vous pourrez entendre tout ce qu'ils ont à dire sur vous, votre entreprise et vos partenaires. L'objectif ? Anticiper la menace qu'ils représentent et être averti d'une éventuelle compromission dont vous seriez déjà victime.

- **Open web :** aussi appelée « web de surface », cette strate regroupe les données indexées par les moteurs de recherche et donc facilement accessibles. Ces dernières ne représentent toutefois que 10 % des informations disponibles sur le web.
- **Deep web :** cette strate renferme la grande majorité des informations en ligne. Ici, les données ne sont pas indexées par les moteurs de recherche. On y retrouve, entre autres, les réseaux universitaires et toutes les informations payantes ou accessibles sur abonnement.
- **Dark web :** cette strate du net nécessite un logiciel (tel que TOR) et des configurations spécifiques pour y accéder. Elle renferme la plupart des forums et marketplaces de nature crapuleuse (également appelé l'Internet « clandestin »).

La solution Mandiant Advantage Digital Threat Monitoring surveille toutes les strates du web (open, deep et dark) pour vous aider à détecter et neutraliser les menaces externes potentielles. Grâce à sa CTI de pointe, Digital Threat Monitoring sait exactement où débusquer les attaquants. Non seulement elle localise et écoute leurs conversations, mais elle vous aide également à infiltrer les canaux chiffrés les plus privés afin de mieux analyser et décoder le jargon employé par les cybercriminels. Digital Threat Monitoring utilise des filtres, la reconnaissance d'entités nommées et le traitement du langage par machine learning dans le but d'éliminer le bruit et les faux positifs. Quelques minutes par jour suffisent pour détecter les éventuelles fuites de données ou d'identifiants, ou savoir si une attaque se trame contre votre entreprise, vos collaborateurs clés ou vos fournisseurs.

Protéger l'essentiel

Marketplaces clandestines, blogs, pastebins… Digital Threat Monitoring scrute les moindres recoins du web pour vous aider à anticiper les menaces et à détecter les fuites jusque-là passées inaperçues. Grâce aux mots-clés uniques et personnalisables, vous pouvez surveiller les éléments vitaux de votre entreprise :

Marque
Prévenez la perte de clients, de chiffre d'affaires et toute atteinte à votre image et votre cote de confiance

Dirigeants
Neutralisez les attaques ciblées et luttez plus efficacement contre le hacktivisme

Ressources techniques
Réduisez les risques d'extorsion et de perte de données

Relations de confiance
Enrayez tout vecteur de compromission ou perturbation de la supply chain

Option managée à valeur ajoutée

La surveillance des menaces potentielles, des campagnes d'attaque et des compromissions est essentielle, mais elle requiert des ressources, du temps et des compétences que toutes les entreprises n'ont pas. C'est pourquoi Mandiant propose Digital Threat Monitoring sous forme de services managés. Avec cette option, les analystes Mandiant se chargent de trier les alertes et de signaler les cas à traiter en priorité.

Autre avantage : vous n'avez plus besoin de gérer vos mots-clés ou de perdre du temps à configurer vos consoles. Un analyste dédié le fait pour vous. Ce dernier vous transmet également les dernières tendances d'activité et réaligne ses interventions et conseils sur vos besoins dans le cadre de rapports mensuels et de réunions de suivi régulières. Il vous accompagne dans la surveillance et la détection des menaces externes sur Internet – jusque sur le deep et le dark web – pour vous aider à prendre les bonnes décisions. Sa mission couvre le tri des alertes, la priorisation des interventions et les analyses contextuelles visant à limiter l'impact des compromissions de données, des ransomwares et de toutes autres menaces cyber.

	Digital Threat Monitoring	Managed Digital Threat Monitoring
Onboarding	Oui	Oui
Nombre illimité d'utilisateurs	Oui	Ne s'applique pas
Accès au portail de Threat Intelligence	Oui (gratuit)	Oui (gratuit)
Notifications d'alertes	Oui	Oui
Catégories de mots-clés	Toutes	Toutes
Gestion des mots-clés	Autogérée	Mandiant
Suivi/tri des alertes	Autogérée	Mandiant
Investigations CTI	Disponibles dans le cadre du service Expertise On-Demand	Mandiant
Rapports de synthèse	Non inclus	Tous les mois
Réunions de suivi	Non incluses	Tous les mois
Notifications d'actions urgentes	Non incluses	Incluses
Démantèlements et contre-offensives	Disponibles prochainement	Incluses

Digital Threat Monitoring est une composante essentielle de la solution Mandiant Digital Risk Protection. Rien ne lui échappe : vecteurs à haut risque, orchestrations malveillantes sur le deep et le dark web, campagnes d'attaques lancées sur le web de surface, etc. Digital Risk Protection vous apporte des informations contextualisées sur les acteurs cyber et leurs modes opératoires. Vous disposez ainsi de tous les éléments pour dresser un profil complet de la menace, garant de la protection de vos ressources digitales, de votre supply chain et de votre marque.

Digital Risk Protection

Service Cyber Threat Profile

Google Cloud

Pour plus d'informations, rendez-vous sur cloud.google.com

A-EXT-DS-FR-FR-000211-07