# Lumière sur les cyber-risques qui pèsent sur votre entreprise

Points forts

- Leader dans le classement Forrester Wave™ : External Threat Intelligence Services (1er trimestre 2021)
- > 200 000 heures par an consacrées à la réponse aux incidents
- Détection et footprinting de toutes les ressources digitales
- Offre de services destinée à dresser un tableau composite des cybermenaces les plus sérieuses pour votre entreprise et des modes d'attaque potentiels
- Surveillance de plus de 200 sites de carding, forums, marketplaces et sites de ransomware présents sur l'open web (ou « web de surface »), le deep web et le darknet à l'aide de mots-clés
- > 285 contrôles disponibles pour confirmer les vulnérabilités, les erreurs de configuration et les expositions

## Élargissez votre champ de vision avec Digital Risk Protection

Au fil de la préparation de leurs attaques, les cybercriminels laissent des traces partout sur Internet. Pour peu que vous sachiez où regarder et comment y accéder, ces indices peuvent vous alerter suffisamment tôt pour vous permettre de dresser des remparts face à ces attaques.

Digital Risk Protection vous offre une visibilité sur l'intégralité de votre surface d'attaque et les activités du dark web. Vous avez ainsi toutes les cartes en main pour neutraliser les campagnes d'attaque avant même qu'elles n'impactent votre entreprise : image de marque écornée, perte de la confiance des clients, exposition de données sur l'ensemble de l'infrastructure, etc. Digital Risk Protection permet aux professionnels de la sécurité d'identifier un large éventail de menaces :

- Vecteurs d'attaque à haut risque
- Orchestration malveillante depuis le deep web et le darknet
- Campagnes d'attaque lancées sur l'open web
- Groupes de cybercriminels et leurs modes opératoires actuels

Ainsi munies de ces informations, les entreprises peuvent préparer leur défense, exploiter leurs ressources plus efficacement et réduire le temps de réponse.

## Visibilité sur les risques et menaces externes

Si la visibilité est une bonne chose, savoir où et quand regarder peut véritablement changer la donne. C'est pourquoi Digital Risk Protection puise dans la Threat Intelligence les éléments qui permettront de repérer ce qui se trame contre vous sur l'open, le deep et le dark web.

## Analyse des menaces et identification des risques

Avant toute chose, commencez par vous poser ces trois questions :

De qui êtes-vous la cible ?

Quels sont leurs objectifs ?

Comment comptent-ils vous compromettre ?

Pour y répondre, vous devez passer au crible tout Internet, jusqu'aux confins du deep et du dark web, pour mieux comprendre les plans des acteurs cyber et leurs points d'entrées potentiels dans votre organisation. C'est pourquoi Digital Risk Protection vous aide à identifier les risques les plus sérieux pour votre entreprise. Connaître l'adversaire et ses techniques, c'est adapter ses systèmes de défense pour mieux lui faire échec.

## La CTI au service d'une priorisation efficace

L'étape suivante consiste à rassembler des données CTI de confiance. Là encore, Digital Risk Protection s'appuie sur la Threat Intelligence pour vous aider à cerner les méthodes des acteurs cyber et les armes qu'ils comptent employer contre vous. Ces éclairages précieux vous permettent d'agir par ordre de priorité et d'adapter vos défenses en connaissance de cause.

## Mandiant Digital Risk Protection : mode d'emploi

Pour vous aider à renforcer votre protection contre les risques du numérique, Mandiant décline son offre sous la forme de produits et services adaptés à vos besoins. Côté produits, Digital Risk Protection inclut Mandiant Advantage Threat Intelligence, Mandiant Advantage Digital Threat Monitoring et Mandiant Advantage Attack Surface Management. Côté services, Managed Digital Threat Monitoring et Cyber Threat Profile sont proposés. Quel que soit votre choix, tous ont comme socle commun la CTI d'excellence de Mandiant, digne des services de cyber-renseignement des États.

Concrètement, Digital Threat Monitoring et Attack Surface Management fournissent la visibilité nécessaire pour anticiper les attaques. Notre Threat Intelligence pointe Digital Threat Monitoring dans la bonne direction sur l'open, le deep et le dark web. Forums, pastebins, réseaux sociaux, marketplaces… Digital Threat Monitoring est aux aguets. Conjugué à Attack Surface Management, ce tandem élargit votre champ de vision à vos ressources vulnérables connectées à Internet ou dans votre écosystème cloud. Car si ces produits sont individuellement très puissants, ensemble, ils augmentent votre champ de vision et vous permettent de prendre les devants face aux attaques.

Exemple, si Attack Surface Management détecte une vulnérabilité sur un appareil hébergé par un tiers, Digital Threat Monitoring peut ratisser le deep web et le darknet pour repérer les discussions sur l'exploitation de cette faille de manière entièrement automatique. Le Mandiant Indicator Confidence Score entre ensuite en action pour attribuer les conversations à tel ou tel groupe cyber. Vous pouvez alors étudier ses modes opératoires pour renforcer vos défenses et limiter le plus possible l'impact de l'attaque en gestation.

Autre scénario possible : Digital Threat Monitoring détecte des activités suspectes à l'encontre de l'un de vos dirigeants. Les informations recueillies vous aident à remonter jusqu'aux acteurs en cause et à identifier leurs autres modes opératoires de prédilection. Ainsi alerté de la forte éventualité d'une attaque et des vecteurs potentiels, vous pouvez scanner votre surface d'attaque externe à la recherche de vulnérabilités à corriger ou d'ajustements à opérer.


## Validation des ajustements

Un des atouts majeurs de l'offre de produits et services Digital Risk Protection réside dans cette capacité à anticiper les attaques et à renforcer votre sécurité sur la base de données précises et complètes. Mandiant Advantage Security Validation a pour vocation de valider l'efficacité de vos contrôles et votre aptitude à détecter, neutraliser et signaler des menaces anticipées. Son action automatique et continue vous offre une visibilité sur l'efficacité de vos contrôles de sécurité face aux assauts. Vous pouvez ainsi mettre en lumière les lacunes, les erreurs de configuration et les pistes d'amélioration sur l'ensemble de votre architecture de sécurité. Avec Security Validation, vos équipes de sécurité ont toutes les cartes en main pour tester et optimiser en permanence vos cyberdéfenses. Ce qui a l'avantage de rassurer vos parties prenantes sur votre capacité à neutraliser les attaques ciblées.

Fondée sur la CTI de pointe de Mandiant, Digital Risk Protection vous permet de vous concentrer sur les menaces qui planent réellement sur votre entreprise et de prioriser vos ressources en conséquence. Vous bénéficiez d'une vue complète sur toute votre surface d'attaque externe, ainsi que sur l'open, le deep et le dark web pour être prêt le jour J.

Pour en savoir plus, rendez-vous sur **www.mandiant.fr**

**Mandiant**
11951 Freedom Dr, 6th Fl, Reston, VA 20190
+1(703)935-8012
+1 833.3 MANDIANT (362.6342)
info@mandiant.com

**À propos de Mandiant**

Depuis 2004, Mandiant® s'impose comme le partenaire de confiance des entreprises soucieuses de leur sécurité. Aujourd'hui, l'expertise et la Threat Intelligence leader de Mandiant sous-tendent des solutions dynamiques qui aident les organisations à développer des programmes plus efficaces et à instaurer une plus grande confiance dans leurs cyberdéfenses.

MANDIANT®
YOUR CYBERSECURITY ADVANTAGE