MANDIANT

FICHE PRODUIT

CYBER THREAT PROFILE

Fondez vos décisions de sécurité sur les menaces qui vous concernent vraiment

EN BREF

- Anticipez les changements dans le profil risque de votre entreprise en fonction des nouveaux facteurs de menaces
- Offrez une visibilité à 360° aux équipes de direction, de cyberdéfense et de gestion du risque pour orienter la stratégie et les investissements de sécurité
- Préparez de manière proactive les équipes opérationnelles à l'aide d'exercices ciblant des menaces réelles
- Validez vos technologies à l'aune des modes opératoires de vos cyberennemis
- Identifiez les cibles stratégiques de votre entreprise à la lumière des vulnérabilités et malwares détectés
- Inspectez le système de télémétrie réseau interne pour détecter tout accès non autorisé en cours ou antérieur

Le tandem clé d'un profil de cybermenace complet : une connaissance approfondie du champ des menaces externes et une compréhension claire de votre environnement opérationnel interne.

Cernez les menaces dont vous êtes la cible

Les cyberattaquants comme leurs modes opératoires évoluent et s'adaptent constamment aux lignes de défense, compliquant ainsi la tâche aux professionnels de sécurité. Pour bien identifier les menaces qui pèsent sur elle, une entreprise doit prendre en compte un certain nombre d'éléments clés : son secteur, ses emplacements géographiques, ses ressources stratégiques, ses objectifs de sécurité propres, l'historique des menaces dont elle a fait l'objet et sa posture de défense. Pour aboutir à une compréhension globale et pertinente du champ des menaces, toutes ces informations doivent être réexaminées régulièrement, aussi bien d'un point de vue interne qu'externe.

C'est là que Mandiant Cyber Threat Profile intervient pour dresser un tableau composite des cybermenaces les plus sérieuses pour votre entreprise. Ce tableau décrit, d'une part, la manière dont ces menaces peuvent se matérialiser et, d'autre part, l'impact potentiel sur votre entreprise et vos partenaires, à court et long termes. Le Cyber Threat Profile fait partie intégrante d'une stratégie de sécurité axée sur la Threat Intelligence, garante d'une protection proactive qui réduit les cyber-risques.

Cyber Threat Profile : les atouts

Un profil de cybermenace procure des avantages stratégiques, opérationnels et tactiques :

- Permet aux dirigeants de visualiser le champ des menaces pour guider leurs investissements de sécurité
- Améliore la communication entre les équipes métiers et des opérations de sécurité
- Oriente les décisions relatives à l'architecture de sécurité en fonction des motivations, capacités et intentions des attaquants
- Recense les profils d'adversaires pertinents pour cibler les processus de modélisation des menaces
- Délimite efficacement le périmètre des investigations pour réduire la pression sur les équipes de réponse aux incidents
- Intègre la Threat Intelligence aux activités de gestion des vulnérabilités pour enrichir les scores CVE

Ensemble, les avantages du Cyber Threat Profile vous aident à prendre des décisions de sécurité axées sur les cyber-risques et non plus seulement sur les bonnes pratiques ou des données subjectives et aléatoires.

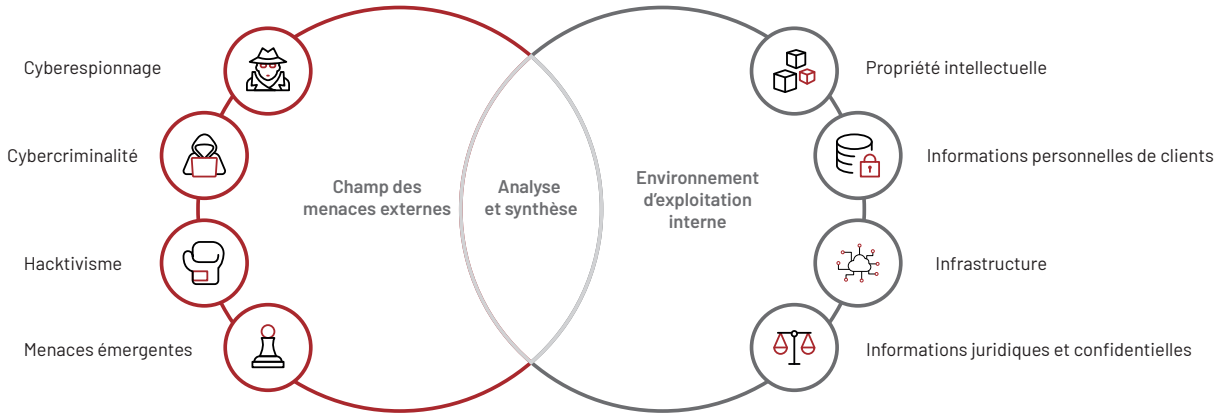

FIGURE 1. Éléments d'un Cyber Threat Profile efficace

Un profil de cybermenace est la clé de voûte d'une stratégie de cybersécurité holistique. Il peut servir à de multiples fonctions organisationnelles et constituer aussi bien la base que le moteur d'autres activités de gestion des menaces : modélisation, validation de la sécurité, traque, exercices et simulations d'attaque, tests d'intrusion, etc. Mais avant toute chose, il convient d'identifier les résultats attendus. C'est pourquoi les profils de cybermenace établis par les experts Mandiant s'articulent sur trois niveaux. Fort d'une expérience de plusieurs années à développer ces profils, Mandiant adapte son approche aux spécificités de chaque client et au degré de précision souhaité. Chaque niveau s'appuie sur les détails des menaces recueillis au stade précédent et inclut l'ensemble des livrables déjà fournis.

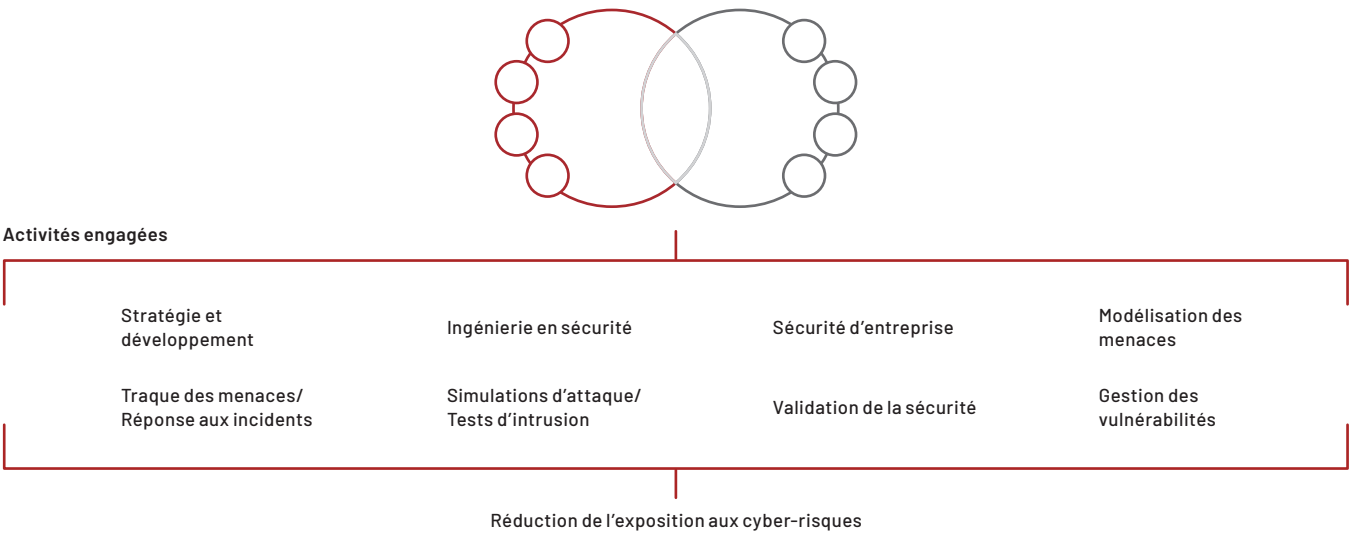

FIGURE 2. Cyber Threat Profile : mise en application

TABLEAU 1. Niveaux d'un profil de cybermenace

Niveau 1 Quelles sont les menaces à prioriser ?	Niveau 2 Comment préparer les équipes opérationnelles ?	Niveau 3 Quelles menaces se sont matérialisées dans notre environnement ?
Le niveau 1 s'adresse principalement aux acteurs **stratégiques** de l'entreprise. Les menaces sont présentées au niveau organisationnel : il s'agit de celles qui ont ciblé ou pourraient cibler des utilisateurs et opérations de l'entreprise. Ce niveau renseigne les responsables de la sécurité sur les motivations et intentions des attaquants. Les résultats de ce premier niveau aideront à identifier les auteurs de cyberattaques, les raisons qui font de l'entreprise une cible de choix et les ressources convoitées par ces adversaires.	Le niveau 2 intègre les données du premier niveau et se concentre sur les acteurs **opérationnels** de l'entreprise tout en facilitant les décisions stratégiques. À ce niveau, les menaces externes sont corrélées avec des cibles internes de haute importance (ressources critiques) pour que l'entreprise puisse prioriser ses cyberdéfenses en fonction de l'impact potentiel des menaces. Le niveau 2 vous montre comment différents scénarios de menaces pourraient nuire gravement à l'environnement opérationnel.	Le niveau 3 inclut tous les résultats du deuxième niveau et concerne les acteurs **tactiques** de l'entreprise. Il fournit une visibilité opérationnelle sur l'efficacité des lignes de défense actuelles et apporte une clarté finale sur les cyber-risques pesant sur l'entreprise. Les experts Mandiant analysent la télémétrie de sécurité interne pour réaliser une évaluation, étayée par des faits, des ciblages présents et passés de l'entreprise. L'objectif : permettre une priorisation précise des menaces et une allocation pertinente des ressources.
Livrables du niveau 1 : rapport complet (au format PDF) détaillant les cybermenaces dommageables qui correspondent à votre localisation, votre secteur, votre infrastructure et vos opérations.	**Livrables du niveau 2 :** tous les livrables du niveau 1 avec en plus un utilitaire personnalisé (au format Microsoft Excel) qui recense les menaces identifiées, y compris les vulnérabilités connues et les malwares associés, sur vos ressources les plus précieuses. L'utilitaire inclut également un overlay MITRE ATT&CK.	**Livrables du niveau 3 :** tous les livrables des niveaux 1 et 2 avec en prime la télémétrie de sécurité du client et des analyses des menaces réalisées par Mandiant. Également au menu : une heat map des cyber-risques assortie de recommandations de contre-mesures selon les problèmes identifiés dans l'environnement. Un appendice technique (au format Microsoft Excel) dresse la liste des groupes de malwares identifiés et des indicateurs à surveiller, des vecteurs d'exploitation et des hôtes internes impliqués.

Degré de préparation aux menaces

Les fonctions de Cyber Threat Intelligence constituent le fil d'Ariane de la gestion des menaces sur l'entreprise. En effet, les responsables de la protection des métiers et des cyberdéfenses ont besoin d'une Threat Intelligence de pointe pour éclairer chacune de leurs décisions. Faute de quoi, impossible d'exploiter ces informations cruciales et de gagner en efficacité opérationnelle. Le service Cyber Threat Profile représente la première étape pour bâtir une entreprise axée sur la Threat Intelligence.

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

Mandiant
11951 Freedom Drive,
6th Fl, Reston, VA 20190, USA
00 1 833.3MANDIANT (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