MANDIANT
NOW PART OF Google Cloud

FICHE TECHNIQUE
MANDIANT ADVANTAGE

Threat Intelligence

En bref

Pour les professionnels de la sécurité chargés de la gestion CTI

- Excellente visibilité sur les acteurs et les malwares émergents
- Référentiel centralisé de descriptions des vulnérabilités connues avec scores de sévérité CVSS
- Capacité à rechercher des indicateurs de compromission connus et à intégrer le Mandiant Indicator Confidence Score (IC-Score) à n'importe quelle page web grâce au plug-in de navigateur

La persistance des attaquants nécessite une attention de tous les instants. De même, les professionnels de la sécurité doivent mieux connaître l'ennemi auquel ils sont confrontés. Mandiant s'appuie sur des données issues d'une variété de sources (compromissions, machines, opérations et cybercriminels), traitées et analysées par plus de 300 experts dans 23 pays couvrant une trentaine de langues, pour proposer cinq formules d'abonnement basées sur différents cas d'usage. L'objectif : fournir aux entreprises une Threat Intelligence actualisée en permanence pour insuffler davantage de vitesse et de précision dans leurs opérations de sécurité.

Ces abonnements, disponibles via Mandiant Advantage, offrent aux entreprises de toutes tailles des informations récentes et pertinentes sur les menaces. Elles peuvent ainsi se focaliser sur les incidents les plus urgents et prendre les mesures nécessaires.

Mandiant Advantage Threat Intelligence Free

Gestion centrale des menaces et vulnérabilités connues

La centralisation et la gestion de la Threat Intelligence sont souvent considérées comme les tâches les plus laborieuses et chronophages pour les analystes sécurité. Mandiant Advantage Threat Intelligence Free offre aux entreprises de toutes tailles un accès gratuit à des informations sur les attaquants, les vulnérabilités et les malwares connus. En prime, cette formule d'abonnement fournit une excellente visibilité sur le danger des différentes menaces à l'aide des IC-Scores calculés par Mandiant, le tout complété par des descriptions des vulnérabilités connues et leurs scores CVSS (Common Vulnerability Scoring System). Ainsi, les professionnels de la sécurité ont toutes les cartes en main pour prendre de meilleures décisions sans augmenter leurs dépenses d'investissement et d'exploitation.

Au menu :

- Tableaux de bord sur les tendances mondiales en matière de vulnérabilités, de malwares et de cybercriminels
- Accès à des indicateurs open-source avec IC-Score Mandiant
- Vues et notation des vulnérabilités sur la base d'une CTI open-source
- Analyse de l'actualité avec avis et commentaires des experts Mandiant
- Threat Intelligence accessible via le portail et le plug-in de navigateur

Avantages

Pour les analystes sécurité, les experts de la réponse aux incidents, les responsables des opérations de sécurité et les analystes CTI

- **Tri et priorisation des alertes.** Utilisez une Threat Intelligence en temps quasi réel pour prioriser et contextualiser les événements de sécurité, avec à la clé une réduction de l'accoutumance aux alertes et une amélioration de l'efficacité globale du SOC
- **Détection des menaces cachées.** Téléchargez des indicateurs et adoptez de nouveaux outils de détection pour repérer les activités des malwares et des attaquants susceptibles de se dissimuler dans votre environnement
- **Accélérez vos temps de réponse.** Utilisez le framework MITRE ATT&CK pour fournir à vos analystes sécurité des éclairages sur les comportements des attaquants, et ainsi déterminer le stade d'avancement d'éventuelles attaques et la meilleure réponse à y apporter

Mandiant Advantage Threat Intelligence Security Operations

Renforcez l'efficacité ET la productivité du SOC

Les équipes du centre opérationnel de sécurité (SOC) croulent sous des événements de sécurité qui accaparent leur attention et demandent des investigations manuelles laborieuses. L'abonnement Mandiant Advantage Security Operations fournit aux analystes sécurité et aux experts de la réponse aux incidents des informations constamment actualisées sur les cybercriminels, les malwares et les vulnérabilités. Ainsi, il les aide à prioriser les alertes et à dresser un portrait-robot des attaquants, de leurs méthodes et de leurs motivations. En corrélant les alertes générées par le SOC aux informations de Mandiant et aux indicateurs CTI open-source (OSINT), les équipes de sécurité peuvent baser leurs activités de tri, d'investigation et de réponse sur des informations plus fiables, et ainsi gagner en rapidité et en efficacité tout en réduisant l'accoutumance aux alertes. Elles anticipent, identifient et neutralisent les menaces en toute confiance grâce à une visibilité sur les campagnes cyber qui touchent leur secteur ou leur région. En prime, Mandiant Advantage Security Operations offre aux équipes de sécurité un historique des détections de cybermenaces émergentes grâce à des données détaillées sur les acteurs et les indicateurs de compromission, disponibles via Mandiant Advantage et l'API.

Au menu :

- Mandiant Advantage Threat Intelligence Free
- Vues dynamiques alternées sur les malwares et les acteurs avec matrice MITRE ATT&CK, explorateur d'objets et téléchargements d'indicateurs
- Accès aux indicateurs de compromission connus de Mandiant (adresse IP, domaine, hachage de fichier, URL) avec scores de virulence
- Analyse de l'actualité avec avis et commentaires des experts Mandiant
- Comptes-rendus trimestriels sur les menaces et support de base (provisionnement et onboarding)
- Visibilité en temps réel sur les campagnes de menaces les plus actives et les plus pertinentes

Avantages

- **Détection des menaces inconnues.** Bénéficiez d'un accès évolutif et personnalisable à une CTI recueillie en première ligne et finalisée par nos experts. Identifiez les menaces mondiales hors du périmètre de votre entreprise grâce aux informations de Mandiant sur les compromissions
- **Cyberdéfense éclairée.** Améliorez votre stratégie de sécurité grâce à une vue complète et contextualisée sur les vulnérabilités, les attaquants, leurs activités et leur impact potentiel sur votre entreprise
- **Définition des priorités.** Accédez instantanément à des informations détaillées et pertinentes sur les menaces qui planent sur votre entreprise pour mieux prioriser vos tâches de sécurité, prévenir efficacement les attaques et réduire l'accoutumance aux alertes
- **Réduction des risques de cybersécurité.** Renforcez les contrôles de sécurité et simulez les tactiques d'acteurs spécifiques au cours d'exercices Red Team

Mandiant Advantage Threat Intelligence Fusion

Threat Intelligence complète pour toutes les équipes de sécurité d'une entreprise

Pour approfondir leurs connaissances sur les attaquants, les équipes de sécurité consultent souvent des tonnes d'informations publiques, mais rarement objectives, sur les menaces. Résultat : elles croulent sous une avalanche de données inconnues, mais censées être fiables, qu'elles doivent ensuite rapprocher avec des profils de menaces établis en interne. Mandiant Advantage Fusion est la seule source CTI dont votre équipe de sécurité a vraiment besoin. Cette formule d'abonnement leur offre un accès illimité à la Threat Intelligence de Mandiant, y compris les activités malveillantes passées, présentes et futures. Pour vous fournir une vue complète, Fusion étudie le champ des menaces sous tous ses aspects : cybercrime, cyberespionnage, renseignement stratégique, intelligence cyberphysique et CTI liée aux opérations des attaquants. Ainsi, vous accédez à des rapports CTI finalisés (FINTEL) basés sur les analyses stratégiques des experts Mandiant, la télémétrie mondiale de tiers, les missions de réponse aux incidents de Mandiant et les résultats d'études techniques, le tout à partir d'une seule et même console avec fonction de recherche.

Au menu :

- Accès aux fonctionnalités de Mandiant Advantage Threat Intelligence Free et Security Operations, et modules complémentaires Vulnerability et Digital Threat Monitoring
- Filtrage par type de rapport, région, secteur d'activité, attaquant ou nom de malware
- Rapports FINTEL avec compte-rendu narratif complet couvrant tout le contexte et l'analyse, de la stratégie à la tactique

Avantages

Pour les analystes de vulnérabilités, les responsables de données ou système/IT, les responsables risque et les analystes CTI

- **Visibilité.** Triez les données sur les vulnérabilités par technologie, attaquant et source d'exploitation
- **Priorisation.** Analysez les données en fonction du niveau de risque et de probabilité d'exploitation pour vous concentrer sur les vulnérabilités les plus urgentes
- **Notifications.** Tenez-vous informés des vulnérabilités zero-day
- **Installation rapide.** Intégrez le module à vos outils d'analyse des vulnérabilités via le plug-in de navigateur ou l'API

Mandiant Advantage Vulnerability (module complémentaire)

Réduisez au maximum votre surface d'attaque

Nouvelles applications, expansion constante des infrastructures IT, sites géographiquement distribués… les analystes cybersécurité peuvent vite se sentir dépassés face à un environnement si divers et complexe. D'autant que l'analyse des informations de vulnérabilité mobilise du temps et des énergies. Même dotées d'un système d'évaluation simplifié, les équipes ne savent souvent pas par où commencer. Grâce à un système de notation unique basé sur la facilité d'exploitation d'une vulnérabilité, la probabilité d'un exploit et la menace perçue, le module complémentaire de Threat Intelligence Mandiant Advantage Vulnerability permet aux équipes de gestion des risques de cybersécurité d'évaluer, de prioriser et de corriger les vulnérabilités détectées à l'échelle de l'entreprise.

Au menu :

- Vues et notation des vulnérabilités par Mandiant, y compris niveau d'exploitation, niveau de risque, évaluation des vulnérabilités zero-day et activités observées par nos experts sur le terrain
- Rapports complets sur les vulnérabilités, y compris identifiants des CVE, technologies vulnérables, vecteurs d'exploit et rapports pertinents
- Comptes-rendus trimestriels sur les menaces et support de base (provisionnement et onboarding)

Avantages

Pour les analystes CTI, les juristes, les équipes RP et de communication d'entreprise, et les dirigeants

- **Visibilité sur les menaces externes.** Identifiez les menaces hors du périmètre de votre entreprise, y compris sur le darknet
- **Configuration simplifiée.** Une fois vos paramètres de recherche définis, Mandiant Advantage surveille en permanence de multiples forums, réseaux sociaux, pastebins et publications liées à des attaquants
- **Fiabilité.** Réduisez le nombre de faux positifs et de faux négatifs grâce à un portail fiable et protégé
- **Accélérez vos temps de réponse.** Préparez votre réponse pour limiter les dégâts et protéger les ressources et les informations de votre entreprise

Mandiant Advantage Digital Threat Monitoring (module complémentaire)

Signalement précoce des expositions aux menaces externes

Les solutions de cyberdéfense traditionnelles se concentrent généralement sur les ressources et les événements au sein de votre réseau. Mais dans le monde hyperconnecté d'aujourd'hui, il est indispensable d'étendre la protection aux ressources qui se situent au-delà de ce périmètre : votre marque, vos identités, votre communauté de partenaires, etc. Le module Digital Threat Monitoring de Mandiant Advantage surveille le darknet pour détecter en amont les expositions de vos ressources aux menaces externes. Ainsi, vous protégez votre marque, votre infrastructure et vos partenariats stratégiques contre les menaces. Vous pouvez détecter les compromissions, les expositions et les cybermenaces à travers l'Internet public, le deep web et le darknet à l'aide de termes de recherche personnalisés. Vous pouvez par la suite automatiser, analyser et générer des alertes pour les correspondances suspectes.

Au menu :

- Outils de recherche de mots-clés personnalisés pour la surveillance des opérations de reconnaissance et des activités du darknet
- Option d'accès aux analystes Mandiant pour la configuration, le tri et les investigations via les services Managed DTM, On Demand Support et Expertise On Demand
- Chaque alerte comporte divers attributs (statut, origine, gravité, etc.), ainsi que des informations visant à faciliter la gestion des ressources sous surveillance.
- Comptes-rendus trimestriels sur les menaces et support de base (provisionnement et onboarding)

Portefeuille des services de Threat Intelligence Mandiant Advantage

	Free	Security Operations	Fusion
TYPES D'ACCÈS			
Plateforme Mandiant Advantage et plug-in de navigateur	○	○	○
API	○	○	○
ACCÈS AUX DONNÉES			
Indicateurs – open-source – avec scores Mandiant	○	○	○
Attaquants – open-source et de notoriété publique	○	○	○
Malwares et familles de malwares – open-source	○	○	○
Tableaux de bord temps réel – attaquants, malwares et vulnérabilités	○	○	○
Indicateurs – système Mandiant propriétaire – avec scores et contexte		○	○
Attaquants – système Mandiant propriétaire – UNC, Temp, APT et FIN		○	○
Malwares et familles de malware– système Mandiant propriétaire		○	○
Vues alternées en temps réel sur les attaquants et les malwares – MITRE ATT&CK et graphes		○	○
Données et vues sur les campagnes actives		○	○
VULNERABILITY			
Descriptions des vulnérabilités publiques/connues	○	○	○
Score d'exploitation et de risque par Mandiant	+ module Vulnerability		○
Analyse des vulnérabilités par Mandiant	+ module Vulnerability		○
DIGITAL THREAT MONITORING (DTM)			
Surveillance du darknet	+ Digital Threat Monitoring		○
Alertes et outils de recherche	+ Digital Threat Monitoring		○
ANALYSE ET CTI SUR LES ATTAQUANTS			
Bulletin d'analyse	○	○	○
Comptes-rendus trimestriels sur les menaces		○	○
Reporting stratégique – région, secteur, tendances			○
Motivations, méthodes, outils et comportements des attaquants			○
Rapports			○
Alertes sur les activités malveillantes, menaces émergentes et rapports sur les tendances			○
Rapports d'étude Mandiant			○

Vous pouvez vous abonner aux modules Vulnerability et Digital Threat Monitoring séparément.

Pour en savoir plus, rendez-vous sur **www.mandiant.com/intelligence**

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®
NOW PART OF Google Cloud