MANDIANT
NOW PART OF Google Cloud

AUTOMATED DEFENSE
FICHE TECHNIQUE

Breach Analytics pour Chronicle

Points forts

- Identifiez vos adversaires et leurs motivations
- Bénéficiez d'un accès précoce à l'information grâce au module Mandiant Threat Intelligence
- Décelez rapidement les IOC catégorisés
- Économisez des heures de travail pour vos analystes

Évitez une compromission majeure grâce à un signalement précoce des menaces

Le nombre de compromissions a explosé au cours des 10 dernières années. À chaque attaque, le mode opératoire des acteurs cyber se fait plus agressif et plus sophistiqué. Dès lors qu'un incident fait la une des médias, tous les RSSI et professionnels de la sécurité du monde entier se posent la même question : « Sommes-nous également touchés ? ».

Mandiant Breach Analytics pour Chronicle s'appuie sur les recherches des équipes de réponse aux incidents Mandiant et sur une CTI approfondie pour réduire systématiquement l'exposition de votre entreprise aux risques en présence. Autre avantage, ses fonctionnalités d'automatisation vous permettent de détecter de façon proactive et continue la présence et les mouvements de nouveaux adversaires dans vos systèmes, tout cela à un coût bien inférieur à celui de vos processus manuels existants.

CTI temps réel

Pour se protéger face aux dernières menaces, les référentiels open-source et les technologies traditionnelles basées sur les règles ou les signatures ne suffisent pas. Le laps de temps entre la détection d'une menace, l'écriture d'une règle et son déploiement SIEM crée en effet une fenêtre d'exposition pendant laquelle l'entreprise est vulnérable. Quant aux référentiels open-source, ils sont par nature accessibles à tous, y compris aux attaquants. Résultat, certains indicateurs de compromission (IOC) peuvent facilement passer sous vos radars. Breach Analytics vous permet de réduire ce temps d'exposition tout en améliorant vos décisions de sécurité.

Breach Analytics s'appuie sur toute la puissance de Mandiant Intel Grid™ et la richesse de ses informations, dont certaines ne sont pas encore publiées ou catégorisées. La solution rassemble ainsi les derniers IOC observés par les experts Mandiant de la réponse aux incidents, les insights de nos analystes CTI et nos observations effectuées pour nos clients Managed Defense sur la ligne de front cyber. Elle compare continuellement ces éléments à vos données de cybersécurité actuelles et historiques pour vous informer immédiatement en cas de compromission.

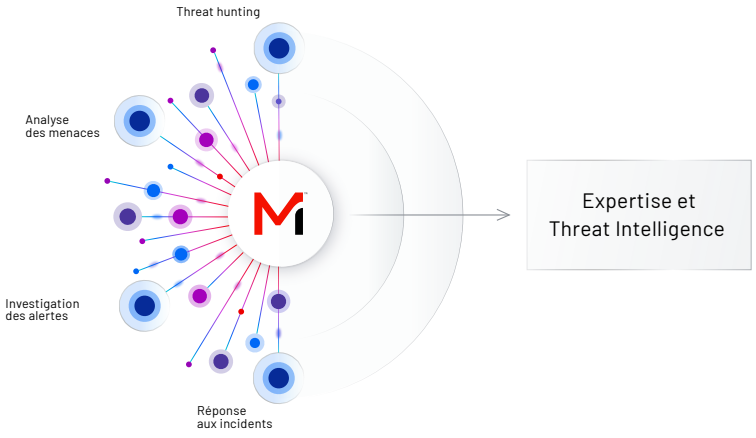

FIGURE 1. Mandiant Intel Grid™

Priorisation rapide des IOC les plus urgents

Les IOC détectés sont classés par ordre de priorité, d'une part sur la base d'informations contextuelles signalées dans les alertes, et d'autre part en fonction de l'IC-Score Mandiant, un algorithme de data science qui évalue le degré de malveillance de l'attaque. Le but : écarter les indicateurs bénins pour aider les équipes de sécurité à se concentrer sur les IOC les plus urgents.

Le mode opératoire et les motivations des attaquants ne cessent d'évoluer. Face à la sophistication des menaces, les systèmes considérés comme sécurisés à un instant t peuvent vite présenter de nouvelles vulnérabilités. D'où l'importance de réduire au maximum le délai de détection et de donner davantage de temps à l'investigation. C'est pourquoi Breach Analytics assure une veille de la prévalence géographique et sectorielle d'une attaque, tout en suivant les opérations de réponse aux incidents en cours.

Rentabilité accélérée

Les utilisateurs des services Google Cloud Chronicle SIEM peuvent déployer Breach Analytics en toute simplicité via la plateforme SaaS Mandiant Advantage. Une fois opérationnelle, la solution permet aux équipes d'accéder à toute la CTI Mandiant 24h/7j. Elles peuvent ensuite passer au crible les journaux système et réseau sur l'intégralité de leur environnement IT (terminaux, réseaux, on-prem et dans le cloud) pour détecter et analyser les IOC tapis sous la surface. Il leur suffit ensuite d'exécuter leur plan d'action pour réduire l'impact de l'attaque. Enfin, Breach Analytics réduit le nombre de faux positifs et donc le délai moyen de détection (MTTD), à savoir le laps de temps entre le moment où un attaquant s'introduit sur votre réseau et l'instant où il se fait repérer.

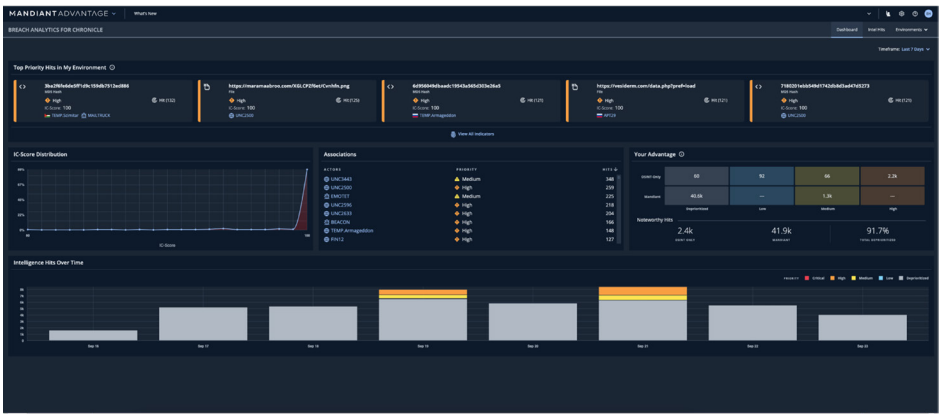

FIGURE 2. Les IOC critiques sont priorisés sur la base de deux critères : rapidité et pertinence. Les clients peuvent contacter les experts Mandiant en un clic pour une réponse accélérée.

Sources et indicateurs

Mandiant Breach Analytics s'appuie sur une grande variété de données.

- Sources d'indicateurs
  - OSINT
  - Liste d'indicateurs Mandiant
- Types d'indicateurs
  - Domaines
  - Adresse IP
  - Hachage (SHA1, SHA256, SHA512, MD5)
  - URL

L'avantage Mandiant

- > 200 000 heures par an consacrées à la réponse aux incidents
- > 3 000 cybercriminels suivis à la trace simultanément
- > 600 consultants dans plus de 25 pays
- > 300 chercheurs en sécurité et analystes CTI
- > 70 contrôles de sécurité tiers pris en charge

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
NOW PART OF Google Cloud