Orange
Cyberdefense

Managed Threat Detection [log]

pour Microsoft Sentinel

La détection managée des menaces dans le cloud consiste à surveiller vos environnements en temps réel et à réagir de manière à minimiser les dommages pour votre organisation.

Opportunités et risques du cloud

La complexité de la gestion de la cybersécurité sur une surface d'attaque élargie croît de manière exponentielle à mesure que les organisations accélèrent leurs programmes de transformation numérique et l'adoption de services cloud. La visibilité et la gestion des menaces telles que les accès non autorisés, les détournements de comptes et les activités réseau suspectes deviennent de plus en plus difficiles dans un environnement cloud en grande partie non géré par les équipes informatiques de l'organisation.

Pour éviter de devoir recruter une équipe de spécialistes de Cloud Security, Orange Cyberdefense permet aux organisations qui investissent dans les technologies Microsoft sur site et dans le cloud de rentabiliser rapidement leur investissement dans la cybersécurité grâce à la détection managée des menaces pour Microsoft Sentinel.

Sécuriser le cloud avec Microsoft Sentinel

Microsoft Sentinel est une plateforme de gestion de l'information et des événements de sécurité (SIEM) basée sur le cloud qui fournit des analyses de sécurité optimisées par l'IA, offrant aux chasseurs de menaces expérimentés d'Orange Cyberdefense des renseignements exploitables pour détecter les indicateurs potentiels d'attaque et de compromission, enquêter sur ces indicateurs et y remédier.

En se connectant à vos principales sources de données et en collectant des logs, qu'il s'agisse d'utilisateurs, d'applications, de produits de sécurité et/ou de points de terminaison fonctionnant sur site ou dans des clouds tiers, les spécialistes d'Orange Cyberdefense analysent les événements de sécurité de votre déploiement Microsoft Sentinel et deviennent votre partenaire en cybersécurité en surveillant les menaces potentielles 24/24, 7/7 et 365 jours par an.

Pourquoi Orange Cyberdefense ?

La détection de votre cloud et la réponse aux menaces sont entre les meilleures mains :

- **Ingénierie de détection**
  Avec plus de 10 ans d'expérience dans la détection managée des menaces, Orange Cyberdefense apporte aux plateformes de sécurité de Microsoft une mine de connaissances, y compris des centaines de techniques de détection complémentaires permettant d'améliorer les capacités de détection inhérentes au produit.
- **Une méthodologie éprouvée**
  Déterminez, visualisez et améliorez votre capacité de détection grâce à notre cadre de détection des menaces et à l'intégration de notre vaste datalake de renseignements sur les menaces.
- **Couverture de la réponse**
  Bénéficiez de la plus large gamme d'options de services de réponse. Complétez vos propres capacités de manière optimale.
- **Expérience et expertise**
  Des capacités mondiales, plus de 150 analystes, fournissant des services CyberSOC 24/24, 7/7, 365 jours par an, sont à votre disposition.
- **Sécurité et partenariat**
  Nos équipes locales travaillent en étroite collaboration avec nos clients pour améliorer en permanence les capacités de détection et de réponse.
- Orange Cyberdefense est membre de l' Association de sécurité intelligente de

Découvrez-en plus sur la détection gérée et la réponse (MDR) sur orangecyberdefense.com/global/mdr/

Avantages :

Visibilité complète de la détection : obtenez des informations sur les environnements internes, cloud et SaaS pour détecter les menaces de cybersécurité.

Sécurité fondée sur le renseignement : nous investissons massivement dans la recherche et le développement afin de détecter les dernières tactiques, techniques et procédures et d'y répondre.

Réponse active : une large gamme d'options de réponse active est disponible 24/24 et 7/7 pour satisfaire vos besoins en matière d'opérations de sécurité.

Gain de temps et d'argent : nous utilisons des techniques innovantes afin de garantir l'examen des incidents dans leur contexte et de réduire autant que possible le bruit.

Détection intelligente

Le défi de la détection réside dans le fait qu'il n'existe pas un seul type de technologie qui réponde à tous les besoins en matière de détection. Il existe des options visant à effectuer la détection à partir des données de journal, des données de réseau et des données de points de terminaison.

Il existe des activités menaçantes qui se produisent en dehors de votre infrastructure et qui peuvent représenter un risque pour vos activités, qu'il convient de détecter. Vous ne pouvez probablement pas résoudre tous les problèmes en même temps, mais vous pouvez choisir un partenaire de sécurité disposant d'un portefeuille MDR complet qui peut vous guider vers les meilleurs investissements.

Orange Cyberdefense propose un portefeuille de détection complet qui couvre non seulement la triade SOC (log, réseau et point de terminaison), mais aussi la détection des menaces qui pèsent sur vos activités sur le Web ouvert, le Web profond et le dark Web. Vous pouvez commencer par celui qui répond le mieux à vos besoins actuels, puis l'étendre au fur et à mesure que votre activité l'exige.

Notre datalake de renseignement recueille et transmet des données sur les menaces à travers nos différents services et notre clientèle mondiale, ce qui nous permet de fournir une perspective globale et locale sur la détection des comportements anormaux.

Nous assurons votre protection !

Les services MDR d'Orange Cyberdefense sont modulaires et un client peut sélectionner un ou plusieurs de ces composants en fonction de ses propres ressources, ou plus important encore, lorsque Orange Cyberdefense peut combler efficacement les lacunes là où ces ressources n'existent pas.

Une fois que vous avez mis en place votre service de détection des menaces, celui-ci peut être combiné avec le service de réponse dont vous avez besoin afin de compléter vos propres capacités.

Tous les services sont soutenus par notre réseau mondial de 18 SOC et 14 CyberSOC qui ont les yeux rivés sur l'écran 24/24 et 7/7, ainsi que par nos équipes CERT internationalement reconnues et membres de CREST, TF-CSIRT et FIRST.

Quels que soient vos besoins en matière de réponse, nos services de réponse managée aux menaces complètent et étendent vos capacités en fonction de vos besoins. Nous vous aidons à contenir les menaces avant qu'elles ne causent des dommages durables, tandis que nos services de réponse aux incidents et de criminalistique numérique vous permettent d'accéder à la demande à l'une des CSIRT les plus vastes et les plus compétentes qui soient.

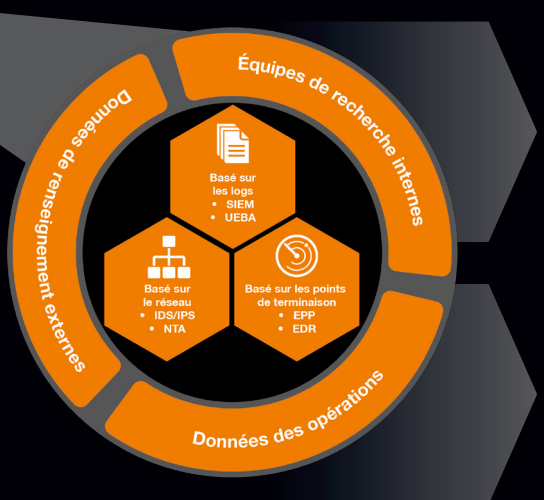
Les avantages d'un MDR fondé sur l'intelligence

Intelligence Data Lake d'Orange Cyberdefense

- Renseignements provenant des opérations MDR, CERT, CSIRT
- Renseignement externe
- Collaboration avec les forces de l'ordre
- R&D interne

Activités internes

- Détection des activités suspectes
- Analyse et classification des incidents
- Notification et rapports



Meilleure détection

- Connaissance avancée des IoC
- Détection précoce des grandes campagnes
- Analyse et corrélation supérieures
- Filtrage efficace du « bruit » et des faux positifs
- CyberSOC 24/24 et 7/7

Meilleure réponse

- Suivi plus rapide des causes de l'incident Faster tracking of incident causes
- Détection plus rapide des vecteurs d'attaque
- Confinement rapide et criminalistique
- CSIRT 24/24 et 7/7