Kiteworks

FICHE PRODUIT

Accélérer la détection et la réponse aux menaces

Service de détection et de réponse embarqué (MDR)

La MDR accélère la détection des menaces sans alourdir la charge de travail des équipes

Les organisations ont de plus en plus de mal à faire face au nombre croissant de cyberattaques. Budgets limités, difficultés de recrutement, elles font souvent appel à un service MDR externalisé pour assurer l'ensemble du cycle, de la détection de la menace à la réponse à distance.

Chez Kiteworks, nous proposons un module de MDR dédié à la suite Kiteworks Enterprise, inclus dans votre abonnement. Il est intégré à votre infrastructure de sécurité IT, à vos process et aux services de MDR de l'entreprise.

Détection, télésurveillance et réponse

Votre système s'intègre automatiquement au service Kiteworks Embedded MDR pendant le déploiement initial, quand vous autorisez la connexion de l'appliance virtuelle au serveur MDR/mise à jour dans le cloud.

Nous avons développé un système avancé de détection des menaces à l'intérieur de l'appliance virtuelle durcie. La télésurveillance alerte automatiquement le Centre d'opérations de sécurité (SOC) de Kiteworks avec les indicateurs de compromission (IOC) et le contexte nécessaire.

- Détecte les activités suspectes
- Surveille les fichiers, les ports, les services, les processus, les interfaces web ou encore les utilisateurs
- Protège la confidentialité des informations sensibles conformément aux règles de conformité
- Mesures correctives automatisées au niveau local, telles que le blocage d'une adresse IP

Surveillance continue et Threat Intelligence

Les équipes SOC de Kiteworks, compétentes et expérimentées, supervisent la télésurveillance de tous les systèmes Kiteworks du monde entier en permanence. Leur connaissance approfondie du produit leur permet de détecter et d'analyser rapidement les menaces isolées, les tendances et les attaques coordonnées.

Avantages

Détection et télésurveillance intégrées

SOC et ingénierie de sécurité 24/7

Threat Intelligence ciblée

Auto-patching à distance

La coordination entre le développement de produits et le SOC accélère le temps de réponse

Les ingénieurs Kiteworks en charge des questions de sécurité travaillent main dans la main avec les équipes SOC pour analyser les menaces et les vulnérabilités potentielles. Ils évaluent le niveau de risque et d'exposition et surveillent aussi :

- Les flux externes de threat intelligence
- Les vulnérabilités identifiées par les bounty hunters (black box et white box)
- Les résultats des tests d'intrusion par des tiers
- Les recherches de vulnérabilités.

Réponses automatiques à tous les systèmes Kiteworks du monde entier

La particularité du MDR d'entreprise est la capacité à coordonner une réponse à une attaque individuelle à distance. La solution Kiteworks Embedded MDR va plus loin, puisqu'elle applique une réponse à l'ensemble de la suite Kiteworks en même temps, plutôt qu'à un seul client à la fois. Toutes les appliances virtuelles durcies sont identiques. Par conséquent, les ingénieurs Kiteworks élaborent des correctifs puis les appliquent à distance à tous les systèmes connectés du client. Après avoir analysé les renseignements sur les menaces provenant des produits

Kiteworks ou autres et avoir identifié les menaces. Kiteworks utilise plusieurs méthodes de correction, parmi lesquelles :

- **Mises à jour des règles WAF intégrées**. Identifie et bloque les nouvelles menaces liées au Web et aux API REST
- **Correctifs sur le code**. Corrige les vulnérabilités du système d'exploitation, de l'open source et du code écrit par Kiteworks*.
- **Alertes via la console admin**. Informe vos administrateurs de la nécessité de prendre des mesures d'atténuation spécifiques.

À noter que les mises à jour des règles et du code WAF prennent effet immédiatement et automatiquement, sans intervention de votre part.

Le produit Kiteworks exige la mise à jour régulière des coordonnées de votre organisation pour garantir l'efficacité des échanges entre notre équipe SOC et votre administration en cas de menace critique.

Le MDR embarqué de Kiteworks réduit le risque cybernétique

La solution MDR embarquée de Kiteworks utilise un logiciel intégré pour la détection, la télésurveillance et les mises à jour du système. Avec le savoir-faire des ingénieurs SOC et sécurité, le gain de temps pour la détection et la réponse aux menaces est considérable. Cela réduit de fait le risque de compromission des informations sensibles, d'entrave au bon déroulement de l'activité et d'atteinte à la réputation de votre organisation. Sans compter le gain de temps et d'énergie pour vos équipes IT déjà surchargées.

* Le correctif à distance sur le code est prévu pour fin 2024. Toutes les offres sont susceptibles d'être modifiées sans préavis.