HIN Endpoint Security Service et
HIN Endpoint Security Tool-Suite

Description des prestations

Introduction et domaine d'application

«HIN Endpoint Security Service» et «HIN Endpoint Security Tool Suite» sont l'objet de cette description des prestations.
Cette description fait partie intégrante de la description des caractéristiques de l'abonnement HIN ou du HIN Gateway et la complète.

1. Conseil

L'assistance et le conseil par des spécialistes sont fournis sans garantie et selon l'approche du «meilleur effort». L'assistance et le conseil sont fournis par téléphone, e-mail ou à distance. Les interventions sur place ne sont effectuées que dans des cas exceptionnels et uniquement contre des indemnités supplémentaires. Il n'y a aucun droit à une durée ou une portée particulière du conseil ou de l'assistance. D'un commun accord, l'assistance peut cependant être prolongée par le client s'il prend les coûts en charge.

2. Configuration requise

L'utilisation de l'Endpoint Security Service est liée à un certain nombre d'exigences système et de conditions techniques et organisationnelles. HIN se réserve le droit de refuser le service pour n'importe quel périphérique, organisation ou personne. Vous trouverez d'autres conditions sur la page web.

3. Mise en service

HIN s'engage à mettre le service à la disposition du client dans un délai de deux semaines après la mise en service. La mise en service doit alors être réalisée par le client lui-même.

4. Alerte, temps de réaction

Les alertes ont lieu aux heures de service HIN (du lundi au vendredi, de 8h00 à 18h00). Le temps de réponse est généralement de 2 heures (meilleur effort) par téléphone, via un logiciel de protection ou par e-mail.

5. Détection, prévention et élimination des logiciels malveillants

HIN ne garantit pas (i) l'exactitude, l'exhaustivité, l'actualité ou la fiabilité des contenus fournis dans le cadre des services d'alerte et du logiciel de détection de logiciels malveillants ou (ii) la coordination ou la disponibilité en temps opportun des services d'alerte.
HIN et ses concédants et fournisseurs n'offrent aucune garantie, condition, promesse ou assurance, expresse ou implicite, légale ou autre, concernant le service ou tout logiciel tiers. En particulier, HIN et ses concédants et fournisseurs ne garantissent pas que le service sera en mesure de détecter et/ou d'identifier et d'éliminer correctement les menaces (nuisibles ou autres), les applications ou d'autres composants.

6. Restrictions

Le licencié, respectivement le client du service, ne peut pas utiliser le service avec ou en relation avec des applications critiques en termes de sécurité s'il y a des raisons de croire que la défaillance du produit peut entraîner des dommages corporels conséquents, des pertes matérielles ou des pertes en vie. Toute utilisation se fait aux risques et périls du licencié et celui-ci confirme qu'il dégage HIN de toute responsabilité liée à une telle utilisation non autorisée.
Le licencié, respectivement le client du service, n'est pas autorisé à modifier le service et les produits associés, ni à les analyser par rétro-ingénierie.
Il est interdit de transférer ou d'accorder l'accès au service et aux produits associés à des tiers.

7. Sauvegarde des données

Le licencié reconnaît et accepte que seul le licencié est responsable de la sécurisation de toutes ses données et qu'il doit prendre les mesures appropriées pour protéger ces informations. HIN et ses concédants de licence tiers n'assument aucune responsabilité pour les données perdues ou corrompues.

8. Stockage de données

HIN ne collecte qu'une très petite quantité de données personnelles en plus des données collectées par HIN dans le cadre de l'identité électronique. Ces données sont nécessaires afin de protéger l'Endpoint, d'appliquer des stratégies de sécurité et de mettre des rapports à disposition. Les données suivantes sont collectées:

- Informations sur la stratégie – Paramètres (en fonction des composants de stratégie) ou exemples d'exceptions
- Informations concernant le périphérique – Nom du périphérique, dernier utilisateur, informations concernant le système d'exploitation, statut
- Événements – Type, par exemple web, périphérique, logiciel malveillant, informations concernant le périphérique (noms de fichiers et de chemins, emplacements réseau, connexions, etc.)
- HIN n'enregistre pas l'intégralité de l'historique de navigation des utilisateurs finaux; seuls les événements web concernant les pages web bloquées et les pages web, pour lesquelles il y a eu une mise en garde, sont enregistrés à des fins de rapport.

Les données sont sauvegardées de manière sécurisée dans le cloud Sophos à Francfort. On peut consulter la déclaration de protection des données de SOPHOS Central en cliquant sur le lien suivant:
https://www.avanet.com/assets/pdf/sophos-central-datenschutz.pdf

HEALTH INFO NET AG
novembre 2018