Certifications de sécurité Endress+Hauser

Des appareils de terrain vers le Cloud

Facilitez votre conformité en matière de cybersécurité avec un partenaire de confiance :
Les instruments de mesure et les composants d'Endress+Hauser assurent un fonctionnement fiable des installations de process dans d'innombrables sites, dans le monde entier.

La cybersécurité dans les installations industrielles et l'Internet Industriel des Objets revêtent une importance croissante.

Pour prouver la qualité de nos produits, nous avons testé nos systèmes par rapport à certaines des normes de sécurité les plus connues dans le monde des technologies de l'information (IT) et des technologies d'exploitation (OT), et nous avons obtenu la certification correspondante.

Contact :
Veuillez contacter l'entité locale Endress+Hauser
www.addresses.endress.com

Plus de détails sur Netilion ?

netilion.endress.com/fr

Sécurisez les exigences du cycle de vie du développement des produits

Afin de protéger au mieux les installations de production de ses clients, Endress+Hauser pose les bases d'un fonctionnement sécurisé dès la phase de planification et de développement de ses produits et services.

L'organisme de certification Allemand TÜV Rheinland a confirmé que ce processus de développement des produits, ainsi que la gestion du cycle de vie des produits, répondent aux normes internationales les plus élevées avec la certification selon la norme IEC 62443-4-1.

Sécurité de l'information est cruciale

Endress+Hauser Digital Solutions est le centre de compétences pour l'IIoT et la digitalisation au sein du groupe Endress+Hauser. Cette entité a obtenu la certification ISO 27001 pour la sécurité de l'information. Le système est conçu pour garantir la conformité à la réglementation applicable, comme les règlements sur la protection des données (DSMS, RGPD).

Le respect de cette norme internationale a marqué une nouvelle étape pour l'organisation.

- Premièrement, la sécurité des données et des informations du client est assurée.
- Deuxièmement, un organisme de certification tiers a confirmé que notre système garantit l'exactitude, l'adéquation et l'amélioration continue de nos mesures de sécurité.

Sécurité du cloud pour Netilion

Un organisme de certification tiers a confirmé que l'écosystème IIoT Netilion répond aux exigences de la norme ISO 27017. Cette norme internationalement reconnue contient des exigences supplémentaires pour les plateformes cloud sécurisées. Les services basés sur le cloud offrent une grande variété de fonctionnalités utiles. En même temps, ils peuvent augmenter la surface d'attaque des entreprises – ce qui accroît la crainte de les utiliser. La conformité aux exigences de la norme ISO 27017 garantit que les clients peuvent faire confiance à l'écosystème Netilion pour fournir un port sécurisé pour leurs données.

Endress+Hauser
People for Process Automation

Fonctions et caractéristiques Pour se conformer à toutes les exigences, il est nécessaire d'avoir des fonctions et des caractéristiques appropriées implémentées dans le logiciel. Voici quelques-unes des mesures de sécurité que nous prenons.

Chiffrement des mots de passe Afin d'assurer la confidentialité des mots de passe des utilisateurs, nous ne les enregistrons pas en clair. Les mots de passe côté utilisateur sont chiffrés par « bcrypt + sel + poivre » et nous enregistrons seulement le code de hachage dans notre base de données.

OAuth Pour prendre en charge une identification sûre de l'utilisateur pendant l'utilisation du logiciel, nous utilisons un processus de jeton d'accès (token) permettant d'identifier les utilisateurs par rapport à nos services Cloud. Les mots de passe de l'utilisateur sont uniquement transmis pour la création de jetons. Cela complique les tentatives de hameçonnage et garantit une autorisation sûre.

Canaux de communication chiffrés uniquement Le canal de communication vers notre service Cloud est toujours établi via une connexion https sûre et chiffrée. Ainsi, toutes les données utiles sont chiffrées selon les normes industrielles et nos ordinateurs Cloud sont authentifiés de manière fiable par un certificat émis par une autorité de certification de renommée mondiale.

Informations utilisateur Lorsqu'il accède à son compte, l'utilisateur est en mesure de visualiser les activités passées. Les mêmes mécanismes sont utilisés pour les services bancaires en ligne pour détecter les utilisations frauduleuses possibles ou les tentatives de connexion échouées.

Processus En cas d'incidents de sécurité graves qui peuvent se produire dans un environnement sûr, nous avons établi des processus internes pour réagir aussi rapidement que possible afin d'informer toutes les parties affectées pour protéger nos clients de tout danger.

Emplacement du serveur Nous travaillons avec les partenaires d'hébergement Cloud les plus puissants au monde et n'utilisons que des serveurs situés en Europe. Ces serveurs sont exploités conformément au droit européen qui est l'un des plus stricts au monde. Nos clients peuvent être assurés que leurs données sont soumises aux normes de sécurité des données les plus élevées au monde.

Sécurité des données de l'Edge Device Un edge device est un point critique dans l'architecture car il représente le point d'accès depuis et vers l'installation de l'utilisateur. Un appareil FieldEdge n'enregistre que les données du terrain et les transmet dans le cloud. Si l'utilisation d'une fonction Netilion nécessite l'écriture dans un appareil de terrain, celle-ci est documentée et elle doit être reconnue au préalable par l'utilisateur.

Les FieldEdge sont mis à jour à distance depuis Netilion quand la communication est établie. Ainsi, tous les ports entrants de l'accès à Internet aux appareils FieldEdge sont bloqués. Pour garantir la sécurité des téléchargements, ces mises à jour sont signées et vérifiées par rapport au fichier original pour éviter toute manipulation.

Dès le début, les exigences de la norme IEC 62443 ont servi de base au développement des FieldEdge.

Données client Toutes les données sont la propriété exclusive du client. Nous nous réservons le droit d'accéder à ces données pour fournir nos services. Si nous partageons les données client avec des fournisseurs de services tiers, nous informons nos clients de cette coopération avant de procéder à l'échange de données et nous nous assurons que ce fournisseur de services agit conformément aux conditions et lignes directrices définies.

Gouvernance Toutes les activités et mesures sont prises pour protéger Netilion et les données qui s'y trouvent dans le cadre d'un système plus vaste, où tous les processus sont régis par des politiques, normes, processus et instructions détaillés. Cette approche holistique garantit que toutes les parties de la chaîne de valeur de l'information sont clairement identifiées et protégées en fonction de leurs besoins.

France

Endress+Hauser France
3 rue du Rhin
68330 Huningue
info.fr.sc@endress.com
www.fr.endress.com

Agence Export
3 rue du Rhin
68330 Huningue
Tél. (33) 3 89 69 67 38
Fax (33) 3 89 69 55 10

Agence Paris-Nord
91300 Massy

Agence Ouest
33700 Mérignac

Agence Est
69800 Saint-Priest

Tél. 0 825 888 001 Service 0,15 € / min + prix appel

Fax 0 825 888 009 Service 0,15 € / min + prix appel

Canada

Endress+Hauser Canada
6800 Côte de Liesse
St Laurent, Québec
Tél. (514) 733-0254
Fax (514) 733-2924

Endress+Hauser Canada Ltd
1075 Sutton Drive
Burlington, Ontario
Tél. (905) 681-9292
Fax (905) 681-9444
info.ca.sc@endress.com
www.ca.endress.com

Belgique/Luxembourg

Endress+Hauser Belgium
17-19 Rue Carli
B-1140 Bruxelles
Tél. (02) 248 06 00
Fax (02) 248 05 53
info.be.sc@endress.com
www.be.endress.com

Suisse

Endress+Hauser Switzerland
Kägenstrasse 2
CH-4153 Reinach
Tél. (061) 715 75 75
Fax (061) 715 27 75
info.ch.sc@endress.com
www.ch.endress.com

PU01272S/14/FR/05.21

Endress+Hauser

People for Process Automation