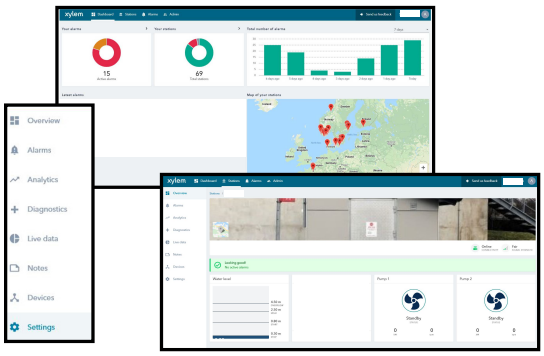
POLITIQUES DE CONFIDENTIALITÉ ET DE SÉCURITÉ

90027104_2.0



Avensor™

1 Cybersécurité chez Xylem

La cybersécurité des produits est désormais un impératif du marché pour gagner la confiance de nos clients. Xylem reconnaît cet impératif et vise à accroître la confiance que nos clients accordent à nos produits et services. Nos clients expriment clairement leurs inquiétudes quant à la sécurité d'un ensemble de solutions cloud de plus en plus interconnectées. L'équipe Xylem chargée de la cybersécurité peut aider les services informatiques de nos clients à maximiser la capacité de gestion analytique et de la performance. Les normes de sécurité les plus rigoureuses sont respectées tout au long du processus.

2 Protection de la confidentialité

Xylem respecte une politique de confidentialité qui inclut les éléments du Règlement général sur la protection des données (RGPD) de l'Union européenne (UE). Tout comme le RGPD, la politique de confidentialité de Xylem est prévue pour aider nos clients à comprendre les éléments suivants :

- Quelles sont les données collectées par Xylem
- De quelle manière Xylem utilise les données
- La sécurité utilisée par Xylem pour protéger les données
- Les droits accordés par la loi applicable

Pour plus d'informations sur la politique de confidentialité, voir *Plus d'informations* en page 2.

3 Sécurité des données

Xylem priorise la disponibilité, l'intégrité et la confidentialité de toute l'expertise que nous fournissons à nos clients. La sécurité de ces produits et services est régie par le Xylem programme de cybersécurité des produits.

4 Le programme de cybersécurité des produits Xylem

Notre mission est d'apporter l'innovation et les meilleurs services du secteur à l'industrie mondiale de l'eau. C'est pourquoi Xylem a élaboré un programme de sécurité des produits conforme à l'industrie et au modèle des trois lignes de défense.

Première ligne de défense

Chaque unité commerciale chez Xylem dispose d'une équipe dédiée à la sécurité des produits qui prend en charge les lignes de produits concernées. Ces équipes ont les fonctions suivantes :

- Renforcer la sécurité des produits
- Traiter les vulnérabilités et les incidents
- Travailler en partenariat avec les clients pour fournir des niveaux d'assurance élevés

Ces équipes sont également dimensionnées pour refléter la taille de chaque portefeuille de produits.

Deuxième ligne de défense

L'équipe chargée de la sécurité globale des produits a les fonctions suivantes :

- Surveiller les risques dans tout le portefeuille de produits Xylem
- Servir de point d'escalade pour les problèmes
- Représenter la voix unifiée de la sécurité des produits Xylem

Cette équipe mondiale fournit plusieurs services qui sont dirigés par des experts de l'équipe de l'entreprise et largement remplis par des partenaires commerciaux de sécurité. Cette organisation crée une échelle pour chaque unité commerciale. Ces services sont primordiaux :

- L'équipe de réponse aux incidents de sécurité des produits surveille les vulnérabilités dans l'espace industriel et dans notre chaîne d'approvisionnement. Ils sont prêts à aider les clients en cas d'incidents de cybersécurité impliquant nos produits.
- Les capacités de services partagés garantissent que les plates-formes technologiques incluent la sécurité des logiciels et s'alignent sur les nouvelles réglementations du secteur.

La fourniture de ces services permet aux équipes chargées de la sécurité des produits de se concentrer sur ce qu'elles font le mieux – être des experts en produits et des partenaires consultatifs auprès des ingénieurs.

Troisième ligne de défense

L'équipe d'audit interne chez Xylem vérifie régulièrement les unités commerciales pour s'assurer de l'efficacité globale du programme. La qualité et l'efficacité du programme sont importantes tant pour le conseil d'administration de Xylem que pour le comité interne de cyber-risque.

Le comité de cyber-risque reçoit des métriques mensuelles. Ces métriques illustrent les efforts internes continus pour améliorer la sécurité des produits Xylem qui sont en cours de développement et ceux qui sont utilisés sur le terrain.

5 Avensor™

Avensor™ utilise la plate-forme cloud Xylem, une infrastructure intelligente qui permet le traitement, la transformation et l'analyse des données de capteur. Lorsque Avensor™ est combiné avec la plate-forme cloud Xylem, il s'aligne au programme de sécurité des produits Xylem. Le programme contribue à activer chaque plateforme afin que nos clients puissent recueillir des informations précieuses et prendre des décisions fondées sur les données en toute sécurité.

Déploiement

Avensor™ et la plate-forme cloud Xylem sont déployés sur Amazon Web Services (AWS) et fonctionnent dans des centres de données à haute disponibilité. Ceci inclut toutes les données telles que des sauvegardes. Les emplacements sont évalués en permanence et alignés sur les besoins de nos clients, ainsi que sur les exigences de conformité applicables.

6 Accès aux centres de données et contrôle

Environnement de sécurité du cloud

Xylem soutient le recours à des partenaires informatiques cloud de classe mondiale pour favoriser l'évolution et renforcer la protection de la sécurité. En collaboration avec AWS, nous fonctionnons selon un modèle de responsabilité partagée qui permet à tous les participants de se concentrer sur leurs points forts.

Les responsabilités partagées sont réparties de la manière suivante :

- AWS est responsable de la sécurité du cloud, ce qui inclut la sécurité des centres de données AWS. Pour plus d'informations, voir *Plus d'informations* en page 2.
- Xylem est responsable de la sécurité dans le cloud. Nous utilisons les méthodes et les ressources fournies par AWS pour assurer la configuration sécurisée de nos applications et définir l'accès correct aux données.

Les aspects connexes comprennent :

- Protection contre les attaques par déni de service distribué (DDoS) au niveau du réseau
- Pare-feu d'application Web (WAF) pour se protéger contre les menaces au niveau de la couche application
- Des réseaux privés pour isoler certains flux de données de l'internet public
- Gestion à distance des services via un réseau privé virtuel (VPN)
- Authentification multi-facteurs (MFA) pour l'administration du cloud et le contrôle d'accès basé sur les rôles
- Chiffrement standard des données en transit et des données au repos, par exemple TLS, VPN et AES
- Journalisation et surveillance permanentes de la sécurité
- Plusieurs instances de service à haute disponibilité (HA) qui sont déployées dans plusieurs zones

Sécurité des produits

Le cycle de vie du développement de logiciels (SDLC) comprend des activités qui favorisent le développement de produits sûrs et fiables.

Les aspects connexes comprennent :

- Cadre de sécurité basé sur les bonnes pratiques, par exemple la politique Xylem et la norme IEC 62443
- Modélisation des menaces et profilage des risques pour identifier les risques de sécurité
- Examens de l'architecture qui tiennent compte des risques identifiés et conception pour les considérations de sécurité
- Sensibilisation à la sécurité pour soutenir l'effort de développement, par exemple par des techniques de code sécurisé
- Test de sécurité automatisé et manuel pour vérifier et identifier les vulnérabilités de sécurité
- Collaboration étroite avec l'équipe chargée de la sécurité des produits

7 Plus d'informations

- Pour plus d'informations sur le programme de cybersécurité des produits Xylem et pour contacter notre équipe chargée de la sécurité, accédez à xylem.com/security.
- Pour plus d'informations sur les pratiques de sécurité d'AWS, rendez-vous sur https://aws.amazon.com/compliance/shared-responsibility-model/.
- Pour plus d'informations sur la politique de confidentialité de Xylem, voir https://www.xylem.com/en-us/support/privacy/.

Xylem Water Solutions Global Services AB 556782-9253
361 80 Emmaboda
Sweden
Tel: +46-471-24 70 00
Fax: +46-471-24 74 01
http://tpi.xyleminc.com

90027104_2.0_fr-FR_2021-03_GSI_Avensor™

xylem
Let's Solve Water