

CYBERMOIS 2026 – SEMAINE 2

Objets connectés : la porte d'entrée qu'on oublie

Note de sensibilisation – Green Earth Digital



Bornes de recharge, onduleurs solaires, capteurs, compteurs, GTB... Utiles à la performance, ils sont aussi des points d'accès à votre réseau.

Des équipements utiles... et connectés

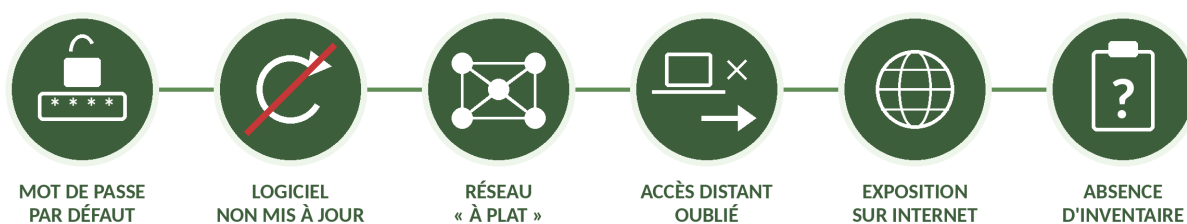
On installe des équipements connectés pour mesurer, piloter et optimiser : produire de l'énergie solaire, recharger une flotte de véhicules, suivre des consommations ou surveiller une installation à distance. Chacun de ces équipements est en réalité un petit ordinateur, relié au réseau de l'entreprise ou à Internet. Une fois mis en service, il est souvent oublié : personne ne change ses identifiants, ne met à jour son logiciel ni ne vérifie qui peut s'y connecter.

Énergie	Onduleurs photovoltaïques, systèmes de stockage, compteurs communicants, sous-comptage.
Mobilité électrique	Bornes de recharge IRVE et leurs plateformes de supervision.
Bâtiment	Gestion technique du bâtiment (GTB/GTC), climatisation, éclairage, contrôle d'accès, vidéosurveillance.
Industrie	Capteurs de process, passerelles IoT, télésurveillance d'équipements, maintenance prédictive.
Accès distants	Plateformes cloud du fabricant, modems 4G, applications mobiles de supervision.

Un objet connecté non sécurisé, c'est une porte du réseau laissée ouverte.

01 POURQUOI CES ÉQUIPEMENTS SONT VULNÉRABLES

Faible	Situation fréquente	Risque
Mot de passe par défaut	L'identifiant d'usine (souvent publié dans la notice) n'est jamais changé.	Prise de contrôle de l'équipement par n'importe qui.
Logiciel jamais mis à jour	Le firmware reste dans sa version d'installation pendant des années.	Exploitation de failles connues et documentées.
Réseau « à plat »	L'équipement est sur le même réseau que les postes de travail ou les serveurs.	Rebond de l'attaquant vers le reste du système d'information.
Accès distant oublié	L'accès ouvert pour le fabricant ou l'installateur n'est jamais refermé ni contrôlé.	Connexion non maîtrisée depuis l'extérieur.
Exposition sur Internet	L'interface d'administration est accessible directement depuis Internet.	Équipement repérable et attaquant à distance.
Absence d'inventaire	Personne ne sait précisément combien d'équipements sont connectés, ni où.	Ce qui n'est pas connu ne peut pas être protégé.



Ce qui n'est pas connu **ne peut pas être protégé.**

02 CE QUI PEUT ARRIVER

Un équipement connecté compromis ne reste pas un problème isolé. Selon son rôle et son raccordement, il peut entraîner :

Intrusion dans le réseau	L'équipement sert de point d'entrée pour atteindre les postes, les serveurs ou les systèmes industriels.
Arrêt ou détournement	Borne indisponible, onduleur arrêté, climatisation ou éclairage pilotés à distance par un tiers.
Données faussées	Des mesures de consommation ou de production altérées conduisent à de mauvaises décisions énergétiques et à un reporting erroné.
Impact sur la sécurité	Un capteur ou un automate détourné peut fausser la surveillance d'une installation ou d'un procédé.
Atteinte à l'image	Équipement utilisé pour attaquer d'autres cibles, fuite de données, perte de confiance des clients et partenaires.

La performance énergétique repose sur des données fiables. Des données non protégées ne sont pas des données fiables.

03 LES BONS RÉFLEXES, DE L'ACHAT À LA FIN DE VIE

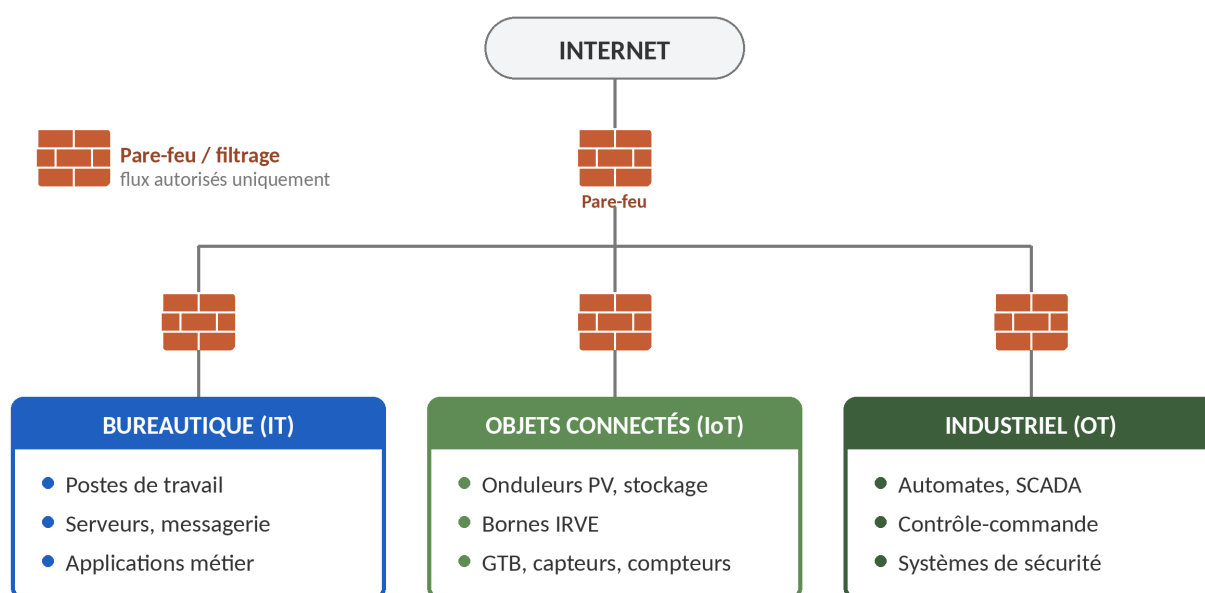
À L'ACHAT ✓ Intégrer des exigences de sécurité au cahier des charges. ✓ Vérifier que le fabricant publie des mises à jour. ✓ Demander comment fonctionnent les accès distants. ✓ Privilégier les équipements qui imposent le changement du mot de passe.	À L'INSTALLATION ✓ Changer immédiatement les identifiants par défaut. ✓ Placer l'équipement sur un réseau dédié, séparé de la bureautique. ✓ Désactiver les services et ports inutiles. ✓ Ne pas exposer l'interface d'administration sur Internet.
EN EXPLOITATION ✓ Tenir un inventaire à jour des équipements connectés. ✓ Appliquer les mises à jour du fabricant. ✓ Limiter, autoriser et tracer les accès des prestataires. ✓ Surveiller les comportements inhabituels.	EN FIN DE VIE ✓ Réinitialiser l'équipement avant sa sortie du site. ✓ Supprimer ses comptes et accès sur les plateformes associées. ✓ Retirer l'équipement de l'inventaire. ✓ Effacer les données qu'il contient.

04 LA SÉCURITÉ DÈS LA CONCEPTION

Sécuriser un équipement après coup coûte plus cher et reste souvent incomplet. Les projets photovoltaïques, IRVE, GTB ou IoT gagnent à intégrer la cybersécurité dès leur conception :

01	Connaître	Recenser chaque équipement connecté, son rôle, son emplacement et son responsable.
02	Cloisonner	Isoler les objets connectés du réseau principal et des systèmes industriels.
03	Authentifier	Des identifiants uniques et robustes, jamais ceux d'usine.
04	Maintenir	Planifier les mises à jour comme une opération de maintenance à part entière.
05	Contrôler les accès distants	Accès limités dans le temps, nominatifs, autorisés et tracés.
06	Contractualiser	Inclure des clauses de sécurité dans les contrats fournisseurs et installateurs.
07	Intégrer aux risques	Prendre en compte ces équipements dans l'analyse des risques et les plans de continuité.

Exemple de cloisonnement : chaque famille d'équipements dans sa propre zone, séparée par un filtrage.



Chaque zone est isolée : un équipement compromis ne donne pas accès aux autres.

05 AUTO-DIAGNOSTIC : SIX QUESTIONS À SE POSER

1	Savez-vous combien d'équipements connectés compte votre site, et où ils se trouvent ?	Oui ☐ Non ☐
2	Les mots de passe par défaut ont-ils tous été changés ?	Oui ☐ Non ☐
3	Ces équipements sont-ils séparés du réseau bureautique et des systèmes industriels ?	Oui ☐ Non ☐
4	Savez-vous qui peut s'y connecter à distance, et comment ?	Oui ☐ Non ☐
5	Les mises à jour sont-elles suivies et appliquées ?	Oui ☐ Non ☐
6	Ces équipements figurent-ils dans votre analyse des risques ?	Oui ☐ Non ☐

Un seul « non » ou « je ne sais pas » suffit à justifier un diagnostic.

L'ACCOMPAGNEMENT DE GREEN EARTH DIGITAL

Green Earth Digital accompagne les entreprises vers des environnements plus performants, connectés, sécurisés et durables. Sur les objets connectés, nous intervenons notamment pour :

Inventaire et diagnostic	Recensement des équipements connectés et évaluation de leur niveau d'exposition.
Sécurisation IoT et OT	Cloisonnement des réseaux, durcissement des équipements, maîtrise des accès distants.
Projets PV, IRVE et GTB	Conception et déploiement de solutions intégrant la sécurité dès le départ.
Performance énergétique	Pilotage des consommations à partir de données fiables et protégées.
Sensibilisation	Formation des équipes techniques, des services généraux et des prestataires.

CONNECTER • SÉCURISER • MAINTENIR • MAÎTRISER

Parce qu'un équipement performant doit aussi être un équipement sûr.

Green Earth Digital

Performance • Connectivité • Sécurité • Durabilité

Pour échanger sur vos enjeux : info@greeneearth-digital.fr / sales@greeneearth-digital.fr