Cybersécurité et protection des données

Notre engagement pour la fiabilité
et la sérénité de vos opérations industrielles

Avec Creative IT et Qubes, vos données sont protégées, vos opérations sont sécurisées, votre confiance est renforcée

LA PROTECTION DE VOTRE PARTENAIRE CREATIVE IT POUR VOUS GARANTIR UNE CONTINUITÉ DE SERVICE

La cybersécurité au sein de notre entreprise est une réalité déjà bien ancrée depuis 2020 avec des mesures concrètes :

- **Formations** régulières des salariés à la cybersécurité
- **Campagnes de tests** internes pour mesurer la résistance des systèmes informatiques et des collaborateurs *(tests de phishing)*
- Mise en place de **logiciels de sécurité** et de gestion de mots de passe
- **Renforcement de la protection** de nos serveurs internes et des serveurs sur lesquels nous préparons les applications clients

- **Réalisation d'un audit et d'un pentest** par une entreprise extérieure *(le dernier en 2025)*
- **Application du TSS Security Framework** pour le respect des exigences de notre maison mère TSS avec 52 points de sécurité à respecter parmi lesquels
  - la gestion des actifs
  - la gestion des vulnérabilités
  - la gestion des accès aux systèmes internes et externes *(MFA, gestion des comptes utilisateur, audit d'autorisation)*
  - la protection contre la perte de données *(politique de backup, déploiement de Endpoint Protection, gestion des firewall)*
  - la surveillance du réseau *(logs et alertes déployés pour surveiller l'activité sur le réseau)*
  - une politique de sécurité concernant les e-mails *(DMARC, DKIM, SPF)*
  - une politique de gestion d'incident *(gestion de crise, PRA, politique de communication)*

LA PROTECTION DE VOTRE APPLICATION QUBES POUR VOUS GARANTIR UNE CONTINUITÉ DE SERVICE

La cybersécurité au sein de votre application Qubes est notre priorité depuis 2020 :

- Intégration des **protocoles sécurisés standards** comme https, LDAPs, SMTPs, etc.
- Possibilité d'**authentification double facteur** pour les utilisateurs
- Outil de diagnostic sur le **niveau de protection des serveurs** et de l'application client *(que le client peut lancer lui-même à tout moment)* avec vérification des configurations http, des protections contre les attaques CSRF, de la complexité des mots de passe des utilisateurs, du contenu des fichiers logs Qubes, de l'utilisation de composants de développement obsolètes, des versions des différents systèmes *(OS, SGBD ...)* ; avec recommandations de mises à jour pour la correction des failles connues, etc.
- **Conformité au Top 10 OWASP** et autres règles de sécurité dans le développement de la nouvelle version du logiciel

Prochaine version **Qubes v12 spéciale cybersécurité** en 2026

Qubes