

# Checklist pour combler les failles de sécurité de la chaîne logistique

Les attaques sur la chaîne logistique comptent parmi les menaces de cybersécurité les plus critiques et les plus difficiles à contrer. Les attaques SolarWinds, Polyfill.io, 3CX et MOVEit ont montré qu'en ciblant les fournisseurs logiciels, les hackers pouvaient compromettre des secteurs entiers à grande échelle.



30 %

des violations de données en 2024 impliquent désormais un tiers, soit une hausse de 15 % par rapport à 2023<sup>1</sup>

Les évaluations traditionnelles des fournisseurs portent généralement sur leur santé financière et la sécurité de leur infrastructure, mais elles passent à côté de l'origine principale des vulnérabilités : le processus de développement logiciel.

## La vulnérabilité invisible : le processus de développement logiciel

### Attaques historiques sur la chaîne logistique

Entreprise	Secteur	Date	Impact
Polyfill.io	Réseau de diffusion de contenu (CDN)	2024	Des milliers de sites Web touchés
3CX	Services VoIP	2023	Des milliers d'entreprises affectées
MOVEit	Transfert de fichiers	2023	Plus de 2 000 organisations touchées
SolarWinds	Logiciels informatiques	2020	Plus de 18 000 organisations compromises

Les contrôles de sécurité au moment de l'exécution ne peuvent pas corriger rétroactivement du code vulnérable. Si des failles sont introduites lors du design ou du développement, les clients restent exposés jusqu'à la publication d'un correctif.

Le cycle de vie de développement sécurisé (SSDLC) intègre la sécurité à chaque étape du développement, du design jusqu'à la maintenance post-déploiement.

## Comment évaluer un processus de développement logiciel

Pour garantir une assurance basée sur des preuves, l'évaluation doit couvrir six dimensions :



### Gouvernance et politiques :

Politiques documentées, rôles de sécurité formalisés, supervision exécutive.



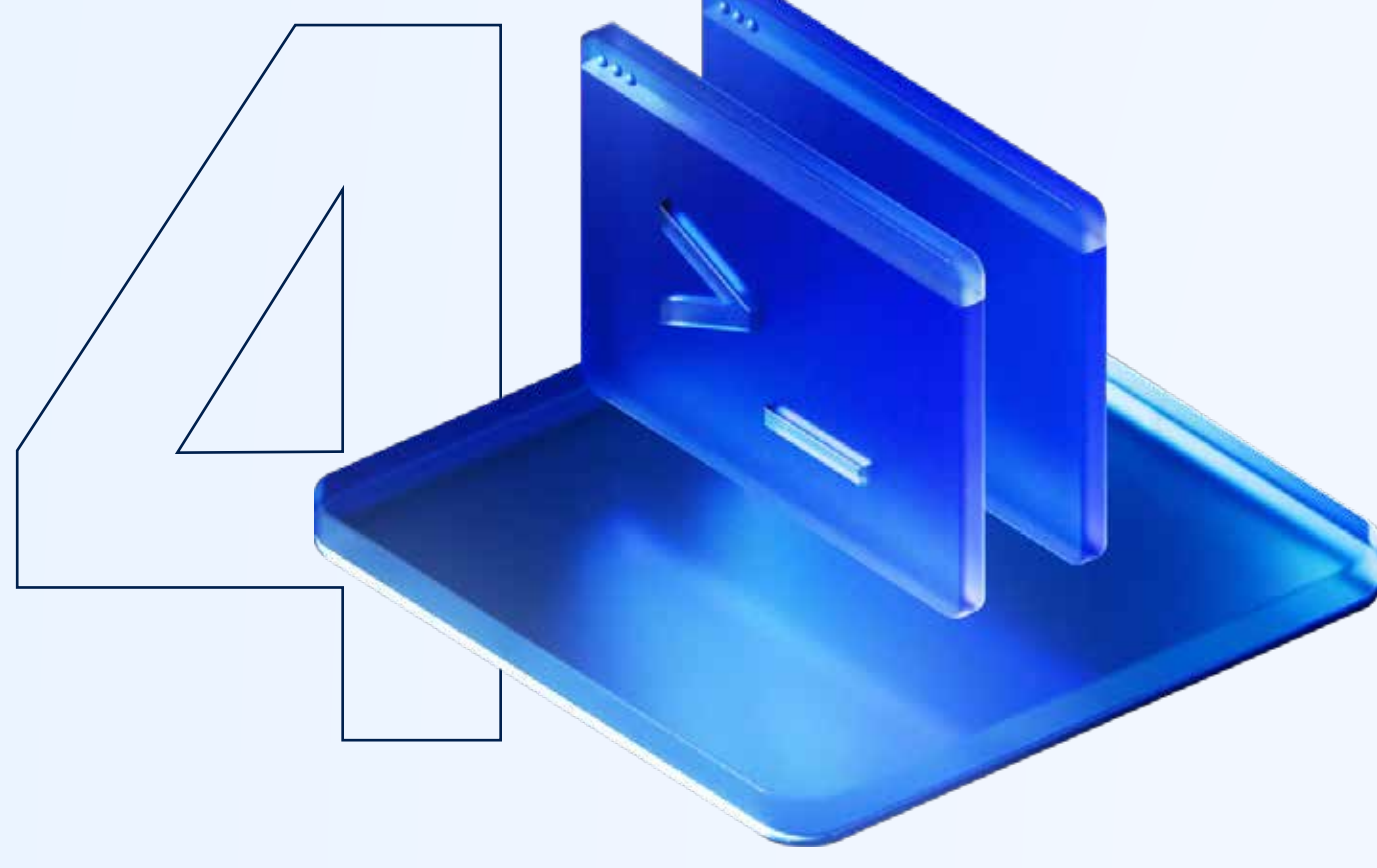
### Gestion des risques et design :

Modélisation des menaces, exigences de sécurité, revues de conception.



### Pratiques de développement :

Formation des développeurs, normes de codage sécurisé, revue de code.



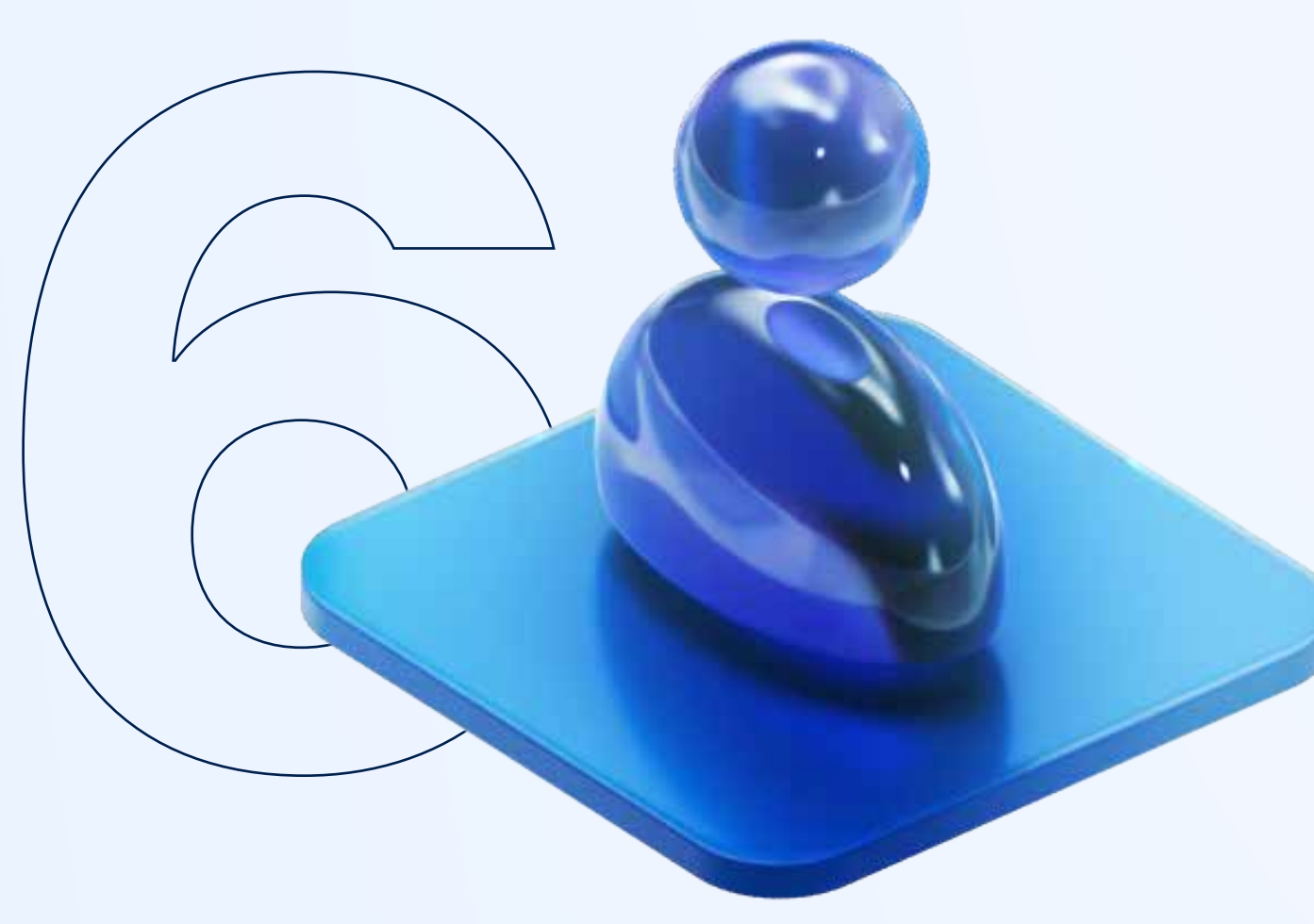
### Vérification et validation :

Tests automatisés, tests d'intrusion, validation par un tiers.



### Publication et déploiement :

Pipelines renforcés, signature de code, segmentation des environnements.



### Maintenance et surveillance :

Gestion des vulnérabilités, délais de correctifs, notifications clients.

# Acronis : l'excellence SSDLC certifiée

Acronis démontre son leadership SSDLC grâce à des certifications indépendantes :



**CEI 62443-4-1**  
Développement sécurisé pour les environnements OT



**Certification ISO/CEI 27001**  
Gestion de la sécurité de l'information

**ISO/CEI 27017/27018**  
Sécurité et confidentialité des services cloud



**CSA STAR Niveau 2**  
Évaluation indépendante de la sécurité cloud

## Ces certifications sont rares et difficiles à obtenir.

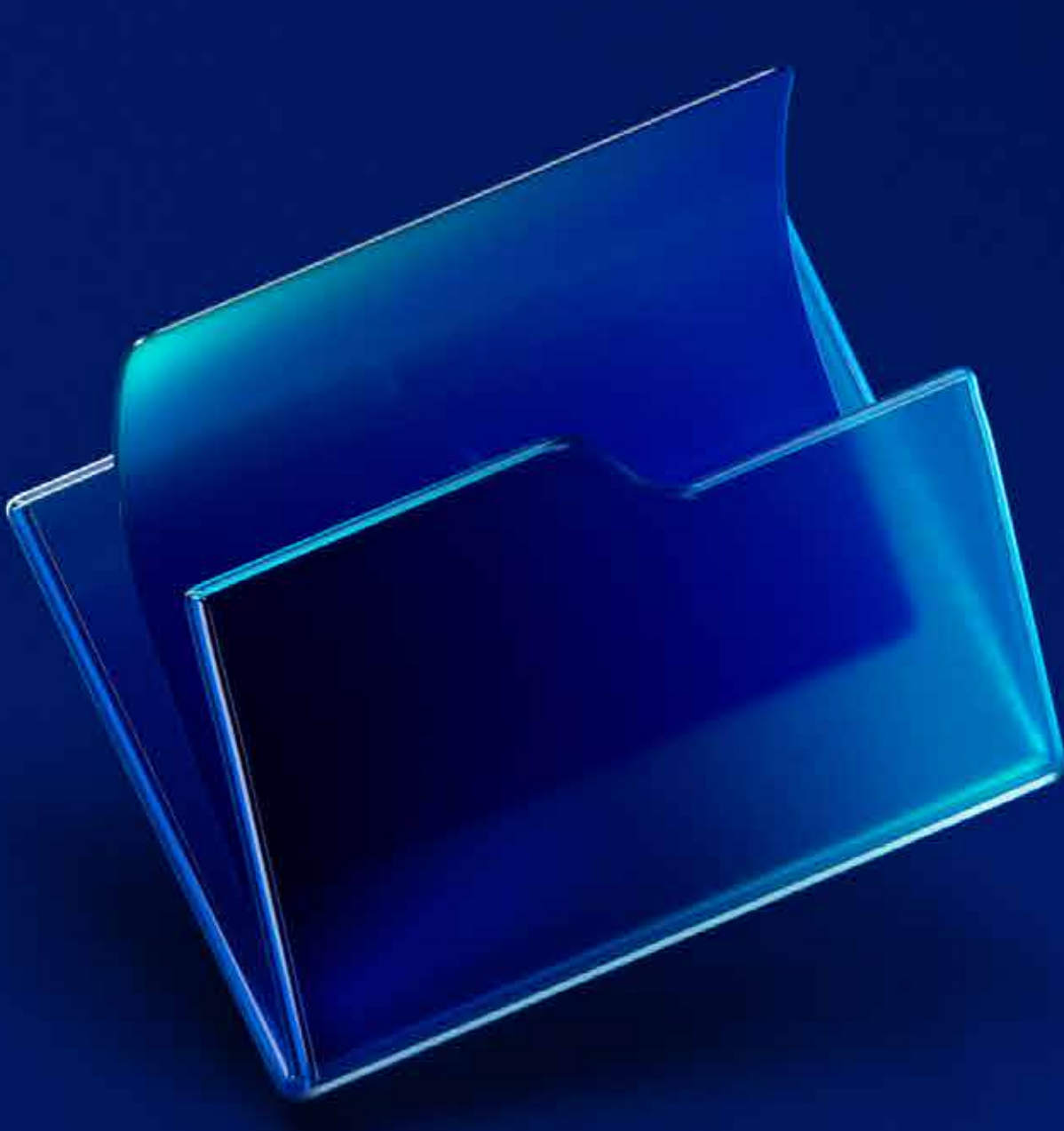
La norme CEI 62443-4-1 représente la référence absolue pour le développement sécurisé dans les environnements industriels. Elle confirme qu'Acronis conçoit ses produits en donnant priorité à la sécurité, permettant à ses clients OT de réduire leur risque lié à la chaîne logistique et de simplifier leur conformité (NIS 2, DORA, etc.).



### En savoir plus

## Renforcez la sécurité de votre chaîne logistique grâce à l'approche certifiée d'Acronis :

- [Consulter la certification CEI 62443-4-1 d'Acronis](#)
- [Lire le livre blanc complet sur le SSDLC](#)
- [Découvrir les solutions de cyberprotection Acronis](#)
- [Planifier un entretien individuel avec un ingénieur solutions Acronis](#)



## À propos d'Acronis

Acronis est une entreprise de cyberprotection mondiale qui propose cybersécurité, protection des données et gestion des terminaux nativement intégrées pour les fournisseurs de services managés (MSP), les PME et les services informatiques des grandes entreprises. Les solutions Acronis sont conçues pour identifier les cybermenaces modernes, les prévenir, les détecter et agir en conséquence, et pour corriger et restaurer les systèmes, avec un temps d'arrêt minimal, de façon à garantir l'intégrité des données et la continuité de l'activité. La solution de sécurité Acronis est la plus complète du marché pour les MSP en réponse à la diversité des besoins des environnements informatiques distribués.

Société suisse fondée à Singapour en 2003, Acronis possède 15 bureaux dans le monde et emploie des collaborateurs dans plus de 45 pays. Acronis Cyber Protect est disponible en 26 langues et dans 150 pays. Elle est utilisée par plus de 20 000 fournisseurs de services pour protéger plus de 750 000 entreprises. Pour en savoir plus, consultez le site [www.acronis.com](http://www.acronis.com).

<sup>1</sup> Verizon. "2025 Data Breach Investigations Report."