

Trois étapes clés pour sécuriser votre chaîne d'approvisionnement logicielle



61%



des entreprises installées aux États-Unis ont subi les conséquences directes d'une attaque sur la chaîne d'approvisionnement logicielle entre avril 2022 et avril 2023.

60%



des entreprises fournissant des solutions logicielles critiques imposeront l'utilisation de SBOM d'ici 2025, contre moins de 20 % en 2022.

90%



des outils d'analyse de composition logicielle (SCA) devraient permettre de générer des SBOM et de les vérifier pour sécuriser la consommation de ressources logicielles open source, contre 30 % en 2022.

Source: Gartner

La chaîne d'approvisionnement est vulnérable



Transparence et contrôle limités

De nombreuses entreprises utilisent des outils de sécurité disparates, ce qui rend impossible d'observer pleinement la chaîne d'approvisionnement logicielle dans son ensemble.



Complexité et lourdeur opérationnelles

Il est difficile de tenir les délais de lancement des nouvelles versions logicielles à l'international



Surface d'attaque en expansion

Les attaquants ciblent la chaîne d'approvisionnement à chaque étape du cycle de développement logiciel, même en environnement d'exécution.



Risques liés aux logiciels open source

Très accessibles, les logiciels open source sont utilisés par tous les types d'entreprises et dans tous les secteurs, et sont une cible privilégiée.



Friction entre les équipes de développement et de sécurité

Les incidents de sécurité passent parfois à travers les mailles du filet et ne sont pas identifiées ni corrigées en temps opportun.

Que faire?



Voici six étapes pour sécuriser votre chaîne d'approvisionnement logicielle



1. **Présélectionnez** les packages open source qui entrent dans l'entreprise



2. **Analysez** les packages (SCA) pour rechercher les vulnérabilités open source dans le code source et les fichiers binaires



3. **Analysez** le code propriétaire ou interne (SAST)



4. **Réduisez** le nombre de faux positifs et le bruit dans les analyses grâce à l'analyse contextuelle



5. **Détectez** les problèmes de sécurité potentiels dans les configurations ou les bibliothèques open source utilisées dans le code



6. **Protégez** vos applications métier des vulnérabilités critiques en environnement d'exécution

Transformez votre approche de la sécurité de la chaîne d'approvisionnement logicielle

avec des conseils pratiques issus du rapport JFrog « Chaîne d'approvisionnement logicielle : état des lieux en 2024 », accompagnés des recommandations de plus de 1 200 leaders du secteur.

Télécharger le rapport →

