



TROIS ÉTAPES CLÉS POUR SÉCURISER VOTRE CHAÎNE D'APPROVISIONNEMENT LOGICIELLE

CHAQUE MAILLON DE LA CHAÎNE REPRÉSENTE UN
POINT D'ENTRÉE POTENTIEL POUR LES MENACES.
VOICI LES CONSEILS À APPLIQUER.

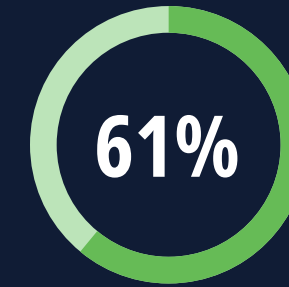


INTRODUCTION

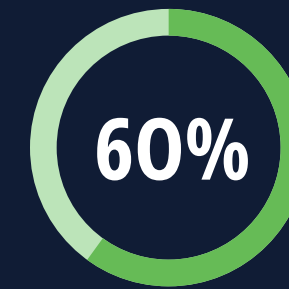
La chaîne d'approvisionnement logicielle d'une entreprise couvre l'ensemble des composants, outils et processus qu'elle utilise pour développer et distribuer ses logiciels. Des dépendances tierces aux processus internes, chaque maillon de cette chaîne représente un point d'entrée potentiel pour les menaces de sécurité.

Une étude récente menée par Gartner montre une augmentation à trois chiffres du nombre d'attaques visant le code, les outils, les composants open source et les processus de développement, pour lesquels la visibilité et les capacités de protection sont souvent insuffisantes. Résultat : d'après Gartner, entre avril 2022 et avril 2023, près des deux tiers (61 %) des entreprises installées aux États-Unis ont subi les conséquences directes d'une attaque sur leur chaîne d'approvisionnement logicielle.

Le coût de ce type d'attaque se chiffre à 1,7 million de dollars américains en moyenne d'après un rapport de l'institut Cyentia. Ce montant inclut les coûts directs liés à la réponse et à la remédiation, mais aussi les coûts indirects liés à la perte de productivité et de chiffre d'affaires.



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.



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



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.

1. PRÉSÉLECTIONNER TOUS LES PACKAGES OPEN SOURCE AU NIVEAU DU POINT D'ENTRÉE

Les trois pratiques clés présentées dans ce livrable permettront aux équipes de sécurité de renforcer la protection de leur entreprise contre l'utilisation de la chaîne d'approvisionnement logicielle (SSC) à des fins malveillantes.

Le recours aux logiciels open source (OSS) est de plus en plus courant dans le développement des logiciels modernes, et de nombreuses entreprises s'appuient aujourd'hui sur une myriade de bibliothèques et de composants OSS. Si les composants open source offrent de nombreux avantages, ils augmentent également la complexité de la chaîne d'approvisionnement logicielle. C'est pourquoi les entreprises doivent faire preuve de précaution aux étapes de gestion et de présélection des packages qu'elles utilisent, et s'assurer de leur sécurité, de leur conformité et de leur qualité.

Une approche préventive de la sécurité (au lieu de réactive) facilite le repérage et le traitement précoces des menaces dans le cycle de vie du développement logiciel (SDLC), avant même que les développeurs ne commencent à coder. La correction des vulnérabilités identifiées tôt est à la fois plus rapide et moins coûteuse.



2. APPLIQUER LA SÉCURITÉ DE FAÇON HOMOGÈNE À CHAQUE ÉTAPE DU SDLC

Chercher à appliquer la sécurité de façon homogène à chaque étape du SDLC est une pratique essentielle à la sécurisation de la chaîne d'approvisionnement logicielle dans sa globalité. Il convient pour cela d'appliquer à la fois des mesures préventives (approche «shift left») et des méthodes de réponse (approche «shift right»).

La détection précoce des menaces dans le cycle de développement favorise le déploiement de correctifs nécessaires, et évite toute amplification des risques.

Combinée à une démarche de sécurité «shift right», cette approche aboutit à la production de logiciels plus sûrs, dès la conception, et garantit l'identification et la correction rapides des éventuelles vulnérabilités introduites dans le logiciel après sa publication.



3. FAVORISER LA COLLABORATION ENTRE DEVOPS ET SECOPS

Cela va de soi : pour véritablement garantir l'intégrité et la sécurité de la chaîne d'approvisionnement logicielle, les entreprises doivent éliminer toute friction entre les équipes sécurité et DevOps. Cet environnement de travail collaboratif fluide permet d'identifier, de catégoriser et de traiter les menaces avec un maximum d'efficacité.

Pour livrer des applications sûres, les équipes sécurité et DevOps doivent collaborer en parfaite harmonie. Les plateformes de chaîne d'approvisionnement logicielle offrent une vue de l'ensemble du SDLC, facilitant l'application de politiques de sécurité unifiées.



HITACHI VANTARA MAINTIENT UNE POSTURE DE SÉCURITÉ HOMOGÈNE

Hitachi Vantara, filiale à 100 % du groupe Hitachi, est un fournisseur de systèmes de stockage de données desservant plus de 6 300 clients dans plus de 100 pays, dont plus de 80 % des entreprises du classement Fortune 100.

Plus de 30 équipes intégrées au fil d'acquisitions successives opéraient de façon cloisonnée, à la fois sur site et dans le cloud. Les différents groupes de développeurs ne pouvaient pas partager rapidement leurs artefacts volumineux aux nombreux autres sites, avec pour conséquence le ralentissement de workflows déjà complexes. En l'absence d'une approche unifiée de la gestion de la chaîne d'approvisionnement logicielle de l'entreprise, il était pratiquement impossible d'assurer une protection homogène contre les vulnérabilités open source sur l'ensemble des pipelines.

Hitachi Vantara a choisi la plateforme de chaîne d'approvisionnement logicielle de JFrog comme un référentiel DevOps centralisé : l'entreprise est ainsi capable de gérer et de partager ses fichiers binaires entre tous ses sites, y compris les métadonnées de l'ensemble des 14 types de packages requis. JFrog a assuré le déploiement de trois plateformes sur site desservant plus de 700 ingénieurs, en répliquant les dépôts stratégiques au niveau de chaque site.

Résultat: une réduction des délais de traitement des builds de **25-30 %**.

La sécurité renforcée permet la mise en cache des composants open source distants (notamment ceux hébergés sur DockerHub) pour tous les sites, tout en protégeant la totalité de la chaîne d'approvisionnement logicielle d'Hitachi Vantara contre les vulnérabilités répertoriées.

«Un outil qui passe au crible tout ce qu'il intercepte et le consigne dans un dépôt de référence central, automatiquement et sans aucune personnalisation requise, c'est très, très puissant,» confie Larry Grill, DevSecOps Sr. Manager d'Hitachi Vantara.

BILAN ET PERSPECTIVES

Le nombre d'attaques ciblant la chaîne d'approvisionnement logicielle, ainsi que les coûts associés, ne devraient pas baisser dans les mois à venir. C'est pourquoi il est important de mettre en œuvre ces trois bonnes pratiques dès aujourd'hui : présélectionner les packages open source au niveau de leur point d'entrée, appliquer la sécurité sur l'ensemble du SDLC, et favoriser une collaboration étroite entre les équipes DevOps et SecOps.

Renforcez la sécurité de votre chaîne d'approvisionnement logicielle grâce aux conseils de plus de 1 200 experts du secteur, détaillés dans le rapport JFrog « Chaîne d'approvisionnement logicielle : état des lieux en 2024 ». Apprenez à gérer l'explosion du nombre de packages open source, à catégoriser efficacement vos projets de remédiation et à contrer la prolifération des outils de sécurité afin d'améliorer la productivité de vos développeurs. Adoptez les meilleures stratégies de gestion des CVE critiques et découvrez comment l'IA transforme les pratiques de sécurité.

[Télécharger le rapport](#)

À PROPOS DE JFROG

La plateforme de chaîne d'approvisionnement logicielle JFrog forme un système unique d'enregistrement au service des entreprises pour une construction, une gestion et une distribution rapide et sécurisée de leurs logiciels, tout en garantissant leur disponibilité, leur traçabilité et leur inviolabilité. Les fonctionnalités de sécurité intégrées permettent également d'identifier et de neutraliser les menaces et les vulnérabilités. Hybride, universelle et multicloud, la plateforme de JFrog est disponible à la fois sous forme de services auto-hébergés ou de services SaaS compatibles avec tous les grands fournisseurs de services cloud. Des millions d'utilisateurs et plus de 7 000 clients du monde entier, dont une majorité des entreprises classées au Fortune 100, font confiance à JFrog pour soutenir leur transformation numérique en toute sécurité.

Suivez-nous:

