digicert®

Evaluation des logiciels et adoption des politiques en matière de signature de code

Bonnes pratiques à prendre en compte pour renforcer la sécurité dans le processus de publication de logiciels, sans ralentir le pipeline CI/CD.

GUIDE D'ACHAT

Introduction

Les attaques de la supply chain logicielle et d'autres formes de propagation de malwares peuvent nuire à la confiance des clients et s'avérer longues et coûteuses à corriger. Ces attaques très médiatisées peuvent entraîner des compromissions de données, des demandes de rançon voire un arrêt complet des systèmes.

Parallèlement, les points de vulnérabilité dans la sécurité des logiciels ont proliféré. Le développement Agile a augmenté la fréquence du nombre de versions délivrées. Le déploiement et l'orchestration dans le cloud ont redéfini les codes du déploiement de logiciels. Quant à la prolifération des appareils connectés, elle impose de sécuriser les mises à jour de firmware et les communications.

Aujourd'hui plus que jamais, les entreprises doivent améliorer la sécurité de leurs cycles de développement logiciel (CLM). Les logiciels de signature de code centralisent la gestion des activités de signature de code, assurant ainsi la standardisation et l'application de politiques et de pratiques qui réduisent les vulnérabilités des logiciels.

Lors de l'évaluation et de l'implémentation de solutions logicielles de signature de code, les critères suivants devraient guider vos décisions :

1. Flexibilité de la configuration
2. Méthodes complètes de stockage et de traitement des clés
3. Intégration et automatisation des workflows
4. Rapports centralisés et flexibles
5. Contrôle des processus de déploiement du code
6. Déploiement souple et évolutif

Ce guide d'achat s'adresse aux clients qui souhaitent améliorer la sécurité de leurs logiciels. Au sommaire :

- Critères d'évaluation des plateformes logicielles de signature de code
- Conseils de clients pour l'adoption de politiques et de pratiques réussies de signature de code

Flexibilité de la configuration

La configuration détaillée des structures de comptes, des rôles et des autorisations des utilisateurs permet aux entreprises de cadrer les fonctions du système sur leurs besoins organisationnels spécifiques.

Objectifs

- Centralisation de la gestion des clés de signature et des certificats à l'échelle de l'entreprise
- Mapping des structures et des fonctions de comptes selon les impératifs de sécurité
- Restriction des accès système à des utilisateurs désignés
- Élimination des points de vulnérabilité uniques pour les fonctions critiques
- Application d'une politique Zero Trust pour l'accès aux comptes
- Efficacité améliorée pour l'octroi et la révocation de privilèges système

Fonctionnalités essentielles

- Importation de clés et de certificats pour consolider l'ensemble du portfolio de clés et de certificats
- Centralisation des configurations de compte et structures d'utilisateurs, y compris la configuration de l'autorité de certification intermédiaire (ICA) et de ses attributs
- Rôles et autorisations granulaires des utilisateurs avec contrôles des politiques d'accès
- Autorisations par quorum pour les fonctions nécessitant une approbation bipartite
- Prise en charge de l'authentification multifacteur (MFA)
- Profils au niveau groupe

Politiques et pratiques de signature de code – Conseil n°1

Les clients font état de différentes méthodes pour associer la politique de signature de code à l'utilisation du logiciel de signature de code. Certains disent avoir formalisé la politique dans un document. D'autres ont misé sur l'accompagnement et la formation pour guider les pratiques en matière de signature de code, et d'autres encore se sont appuyés sur l'utilisation de logiciels pour l'application centralisée des politiques.

Politiques et pratiques de signature de code – Conseil n°2

Les clients ont mis l'accent sur les trois principales préoccupations en matière de gestion des clés : désignation d'un responsable de la gestion des clés, spécification du lieu de stockage des clés, et définition et application des autorisations de signature.

Méthodes complètes de stockage et de traitement des clés

Les contrôles granulaires du stockage et du traitement des clés permettent aux entreprises d'éliminer les incohérences internes dans les pratiques de gestion des clés, tout en empêchant l'accès et l'utilisation non autorisés ou erronés de ces clés.

Objectifs

- Choisir la méthode de stockage des clés qui correspond le mieux aux besoins de sécurité (par exemple, confiance publique ou privée)
- Implémenter des contrôles plus stricts pour les projets sensibles
- Limiter l'accès lors d'investigations sur des menaces éventuelles
- Définir les pratiques différenciées d'utilisation de clés pour les environnements de production et de test
- Appliquer le modèle d'utilisation des clés adapté aux exigences de la plateforme logicielle cible
- Réduire l'utilisation de clés comportant des éléments cryptographiques obsolètes, faibles ou non conformes
- Augmenter l'efficacité et réduire les erreurs humaines

Fonctionnalités essentielles

- Options de stockage des clés pour les modules de sécurité matériels (HSM) ou stockage sur support chiffré
- La gestion des profils d'accès aux clés qui déterminent qui peut accéder à quelles clés et à quel moment : signature en ligne et hors ligne, pour permettre une réponse rapide
- Différents types de clés de signature pour la production et les tests
- Modèles d'utilisation des clés statiques, dynamiques et avec rotation
- Contrôle granulaire des profils de paires de clés
- Modèles de profils de certificats avec workflow de génération en un clic

Politiques et pratiques de signature de code – Conseil n°3

Les clients ont indiqué que la conformité interne/réglementaire et les exigences des clients et des plateformes étaient les principales raisons pour lesquelles des politiques et des pratiques de signature de code devaient être mises en place.

Intégration et automatisation des workflows

L'intégration et l'automatisation permettent d'éviter les erreurs manuelles, d'améliorer l'efficacité, d'assurer la cohérence des pratiques de signature et de soutenir les objectifs TTM (time-to-market) du développement Agile.

Objectifs

- Assurer la sécurité sans ralentir le processus de développement
- Améliorer la sécurité et la conformité de l'entreprise, tout en offrant une meilleure ergonomie aux utilisateurs par rapport aux processus de signature manuelle
- Minimiser le risque d'interception du code source pendant le processus de signature

Fonctionnalités essentielles

- Intégration aux pipelines CI/CD, avec diverses options d'interface : ligne de commande, console ou API
- Prise en charge de multiples plateformes CI/CD
- Accès et privilèges préconfigurés et centralisés pour les développeurs et les serveurs de production
- Modèles de certificats et génération de certificats préconfigurés
- Signature du hash pour éviter de transférer le code source

Politiques et pratiques de signature de code – Conseil n°4

Les clients considèrent comme très efficace leur politique de signature de code, laquelle est appliquée par le biais d'un logiciel de signature de code et gérée par les équipes IT ou sécurité.

Politiques et pratiques pour la signature de code – Conseil n°5

Les clients ont noté que les équipes IT et sécurité ont apporté une contribution essentielle à la création de leurs politiques de signature de code. Parmi les contributeurs cités par les clients sur le site on trouve différentes fonctions : RSSI, gestion de la conformité et du risque, DevOps, SecOps, gestion des produits, et équipes IT et de cybersécurité.

Contrôles du processus de déploiement du code

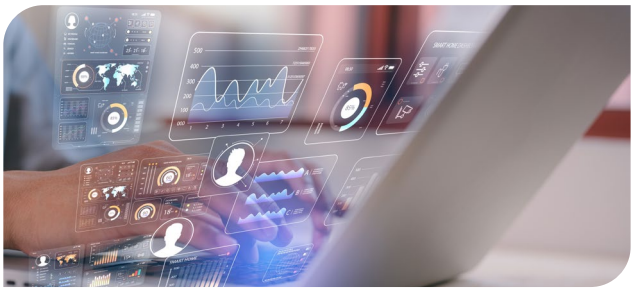
Les contrôles du processus de déploiement du code procèdent à des vérifications supplémentaires qui peuvent aider à prévenir l'injection de malware lors de la compilation elle-même.

Objectifs

- Réduire les possibilités d'activités malveillantes au cours du processus de déploiement

Fonctionnalités essentielles

- Attributs et contrôles des fenêtres de déploiement du code qui définissent les droits d'accès des utilisateurs, les fenêtres programmées et d'autres critères qui limitent l'accès aux seuls utilisateurs autorisés
- Fonctions de comparaison des versions qui utilisent le principe de versions reproductibles pour définir une version de référence qui est ensuite utilisée comme point de comparaison avec les versions suivantes



Rapport centralisé et flexible

La centralisation des rapports permet d'accélérer les mesures correctives, de se conformer aux exigences en matière d'audit et d'identifier les problèmes ou les menaces éventuels.

Objectifs

- Visibilité et contrôle complets des activités de signature de code
- Savoir qui a signé quoi et quand, de manière à accélérer la remédiation
- Assurer la conformité aux exigences d'audit

Fonctionnalités essentielles

- Journalisation et reporting centralisés à des fins d'audit et de suivi des activités
- Filtres de reporting, avec exportation dans des types de fichiers bruts et formatés

Politiques et pratiques de signature
Politiques et pratiques de signature de code – Conseil n°6

Les clients ont souligné l'importance de la normalisation du processus de signature du code, de sa documentation, de sa traçabilité, de sa sécurité et de l'attribution de responsabilités, ainsi que de la garantie de la source et de l'intégrité des progiciels de l'entreprise pour les clients en aval.

Déploiement flexible et évolutif

Les entreprises doivent exiger un choix de modèles de déploiement afin de couvrir les différents besoins de déploiement au sein de leur organisation. Elles doivent aussi évaluer l'évolutivité des solutions par rapport à leurs besoins prévus en matière de signature.

Objectifs

- Mode de déploiement adapté aux préférences de l'entreprise
- Capacité à prendre en charge un volume important de signatures
- Configuration efficace avec évolutivité à la demande

Fonctionnalités essentielles

- Options on-prem, cloud ou hybrides pour répondre à l'ensemble des besoins de l'organisation
- Mise en place rapide et efficace des AC intermédiaires pour les entités ayant des exigences spécifiques en matière de configuration de la sécurité
- Architecture basée sur des conteneurs avec orchestration pour une évolutivité rapide et optimale

Synthèse

Les logiciels de signature de code peuvent réduire de manière significative les points de vulnérabilité dans les processus de déploiement de logiciels. Les solutions aux configurations flexibles et aux fonctionnalités complètes sont les mieux adaptées aux objectifs des politiques et pratiques de signature de code d'une entreprise. Ces solutions assurent sur trois fronts :

Protection

- Éliminez les points de vulnérabilité qui peuvent conduire au vol ou à l'utilisation abusive des clés
- Empêchez l'injection de malware dans le processus de diffusion du code

Gestion

- Assurez une posture de sécurité et une conformité homogènes au sein des équipes de compilation
- Centralisez la visibilité et le contrôle sur les activités de signature

Productivité

- Améliorez l'efficacité et réduisez les erreurs humaines
- Créez de l'agilité dans les changements cryptographiques et la conformité

Prêt à vous lancer ?

Nos solutions SSL, PKI et IoT protègent les données de grandes entreprises dans le monde entier. Avec DigiCert, ces clients peuvent opérer en toute sérénité. Quels que soient vos besoins, nos experts sont à votre écoute.

Pour plus d'informations, appelez le 1.801.770.1736, écrivez à pki_info@digicert.com ou visitez le site digicert.com/software-trust-manager

© 2025 DigiCert, Inc. Tous droits réservés. DigiCert est une marque déposée de DigiCert, Inc. aux États-Unis et dans d'autres pays. Toutes les autres marques, déposées ou non, sont des marques commerciales de leurs détenteurs respectifs.