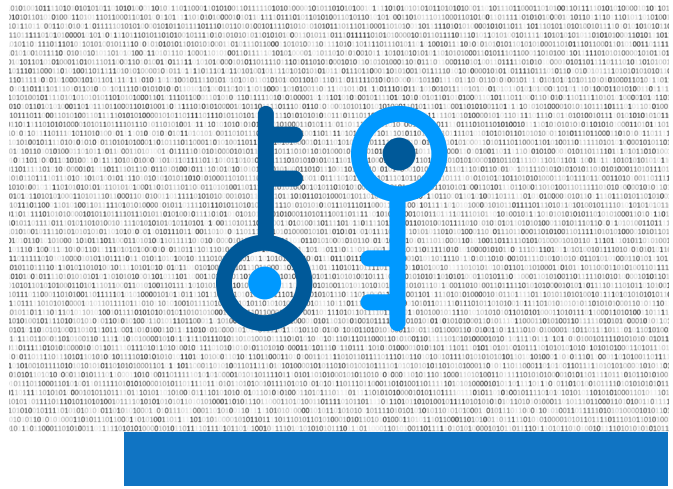
DEVOPS : LES 10 QUESTIONS QUE LES RSSI DEVRAIENT SE POSER

digicert®

01 CONTRÔLE DES CLÉS

Disposons-nous des contrôles nécessaires pour surveiller et gérer l'accès à nos clés de signature dans toute l'entreprise ?

Sans contrôle, vos clés peuvent être utilisées par des cybercriminels pour signer des logiciels préalablement infectés par des malwares, laissant croire à vos clients que ceux-ci sont dignes de confiance. C'est pourquoi il est indispensable d'effectuer un suivi de toutes vos clés de signature, sans quoi vous mettez en danger vos clients, votre réputation et la santé financière de votre entreprise.



02 CONTRÔLE DES DROITS DE SIGNATURE

Parmi nos collaborateurs, savons-nous qui est autorisé à signer des logiciels et à décider de la manière dont les clés sont utilisées ?

Les signatures doivent s'effectuer dans le plus strict respect des politiques d'usage des clés. Faute de contrôle et de visibilité, les signataires peuvent enfreindre les politiques internes et réglementations en vigueur. C'est pour éviter ce genre d'entorse que les systèmes de traçage et de monitoring permettent aux administrateurs de contrôler les autorisations d'accès aux clés et d'intervenir en cas d'abus.

03 MONITORING DE LA GÉNÉRATION DE CLÉS

Savons-nous quels certificats de signature de code ont été générés avec nos clés ?

Un logiciel signé représente une sorte de contrat de confiance entre votre entreprise et ses utilisateurs. Faute d'un suivi précis des émissions de certificats réalisées avec vos clés de signature, des certificats en apparence légitimes pourront être générés pour signer sous votre identité des logiciels compromis ou des versions non autorisées.

04 CONTRÔLE DES MODIFICATIONS ET DES RÉVOCATIONS

En cas d'incident, de changement de poste ou de départ d'un collaborateur, pouvons-nous révoquer ses droits d'accès aux clés ?

Lorsqu'un salarié quitte votre entreprise, vous devez automatiquement révoquer ses droits de signature. De même, tout changement de fonction doit entraîner la modification des permissions d'accès selon les besoins du nouveau rôle. La gestion des utilisateurs vous permet de déterminer les privilèges de signature de chacun en fonction de son rôle, de ses responsabilités et des projets sur lesquels il travaille. Vos clés et vos certificats sont ainsi utilisés par les bonnes personnes au bon moment.

05 AUTHENTIFICATION MULTIFACTEUR

Nos utilisateurs doivent-ils s'authentifier au moyen de plusieurs facteurs avant de pouvoir signer du code, générer des clés ou créer des certificats ?

La signature, la génération de clés et la création de certificats sont des opérations sensibles qu'il vous faut protéger. Permettre à des utilisateurs non autorisés de réaliser ce genre d'action, c'est vous exposer à une éventuelle compromission de votre sécurité, voire à la signature d'un logiciel infecté par un malware, synonyme d'attaque de la supply chain. Pour éviter ce genre de déconvenue, l'authentification multifacteur permet d'authentifier avec certitude l'identité des individus. Ainsi, seuls les utilisateurs autorisés ont accès aux outils de signature.

06 SÉCURITÉ MATÉRIELLE DES CLÉS

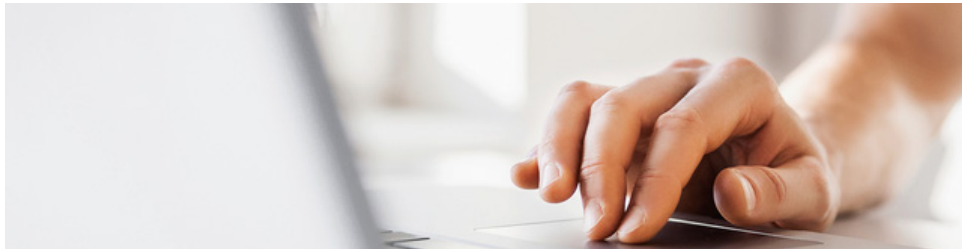
Nos jetons, nos clés USB et nos modules de stockage (HSM) sont-ils tracés et sécurisés ?

Vous devez protéger vos clés matérielles de signature de code comme vous le feriez avec vos clés de maison ou de voiture. De même, vous devez savoir à chaque instant où se trouve chaque clé et entre quelles mains.

07 CLÉS UNIQUES

Nos développeurs partagent-ils des certificats de signature de code ?

Le partage de clés est extrêmement répandu dans le monde du DevOps, à tel point que de nombreux référentiels recommandent cette pratique dans leurs guides d'utilisation. Attention : lorsque vos développeurs partagent des clés, vous perdez le contrôle et la visibilité sur vos signatures. Impossible de savoir qui a signé quoi et quand. Et si un jour vous êtes amené à révoquer un certificat, tout logiciel signé à l'aide de ce certificat pourrait apparaître comme non sécurisé aux yeux de vos utilisateurs.



08 CODE REPRODUCTIBLE

Notre code est-il reproductible, de manière à ce qu'aucun malware ne soit injecté durant le processus de développement ?

Un code reproductible vous permet de répliquer un processus de développement donné et de comparer les versions résultantes. Si les binaires sont identiques, vous pouvez signer et publier votre logiciel en toute confiance, sachant qu'il y a très peu de chance qu'il ait été infecté par un malware. C'est là un des moyens de défense les plus efficaces contre les attaques de la supply chain, surtout si vous utilisez du code open-source et des bibliothèques tierces.

09 AUDIT DES ÉVÉNEMENTS DE SIGNATURE

Surveillons-nous et auditons-nous tous les événements de signature au sein de notre entreprise ?

La sécurité ne se limite pas au lancement public de votre logiciel. Les processus CI/CD internes doivent être sécurisés avec autant de rigueur qu'un logiciel en bout de supply chain ou lors de sa sortie sur le marché. Lors de tout lancement, peu importe que le logiciel sorte de votre environnement ou non, vous devez savoir qui a signé quoi et quand. Cela vous aidera non seulement à éviter des accidents et des tentatives d'attaques, mais aussi à préserver votre conformité tout en renforçant votre sécurité.

10 SIGNER TOUT, TOUJOURS

Sommes-nous certains que tout le code et tous les logiciels lancés sont signés ?

Signer un logiciel, c'est garantir l'intégrité de votre code et de vos logiciels aux yeux de vos partenaires et de vos clients. Une fois le code et les containers Docker analysés et sécurisés durant le développement à l'aide de clés et de droits d'accès correctement gérés, les logiciels doivent encore être signés avant leur livraison. L'avantage est triple : le logiciel est protégé pendant sa transmission, une piste d'audit est créée et vos clients ou vos partenaires peuvent s'assurer que vous avez vérifié l'intégrité du logiciel avant de le lancer. Ensemble, les outils d'automatisation et les services managés de signature de code améliorent considérablement l'efficacité de vos activités de signature, évitant par là même toute interruption ou retard dans vos processus CI/CD.

La sécurité du DevOps ne devrait jamais passer au second plan. Si vous vous demandez comment protéger vos processus CI/CD et toute la supply chain logicielle, vous êtes déjà sur la bonne voie.

Contactez-nous pour découvrir comment corriger les écarts de sécurité et boucler la boucle du DevOps. PKI_info@digicert.com