DIGICERT® CRYPTO DISCOVERY

Comment découvrir et inventorier tous les assets cryptographiques au sein d'un référentiel central

Présentation

La découverte des ressources cryptographiques permet de créer un référentiel central pour gérer différents groupes d'assets. Grâce à ce registre, les équipes peuvent appliquer des politiques, identifier les vulnérabilités, mettre à jour les algorithmes et intégrer l'automatisation selon les cibles ou catégories de certificats souhaitées.

DigiCert® Trust Lifecycle Manager (TLM) fournit une visibilité et un contrôle centralisés pour analyser, importer et gérer les clés de chiffrement et les certificats dans votre environnement. Cet outil vous permet également d'unifier la gestion PKI et de planifier la transition vers les algorithmes post-quantiques.

TLM exploite différents mécanismes pour découvrir votre portefeuille complet de certificats et vous éviter des pannes coûteuses.

Chiffres clés

> 50 000
certificats serveurs d'entreprise

1 200
certificats d'entreprise non gérés

47 %
des entreprises possèdent des certificats non autorisés

500 000 $
Coût horaire des pannes liées aux certificats

Mécanismes de découverte

Intégration à CertCentral et CA Manager
Cette intégration simplifie la gestion du cycle de vie des certificats (CLM), de l'émission jusqu'à la centralisation. Chaque certificat est ainsi inventorié en toute simplicité. Cette fonctionnalité full-stack est absente de la majorité des autres solutions CLM dites « agnostiques », c'est-à-dire compatibles avec toutes les autorités de certification (AC).

Intégration aux AC tierces
La majorité des outils développés par les AC ne peuvent identifier que leurs propres certificats. Un point qui nourrit l'argumentaire des solutions CLM agnostiques traditionnelles.
DigiCert Trust Lifecycle Manager a la particularité de jouer sur les deux tableaux.

Analyse basée sur les ports
L'analyse basée sur les ports est le moyen le plus élémentaire de découvrir les certificats qui ne proviennent pas directement d'une AC. Concrètement, une solution CLM dépose un capteur au sein de votre environnement IT et effectue le gros du travail de recherche des certificats.

Capteurs compatibles avec les certificats d'équilibreur de charge
Trust Lifecycle Manager actionne ses capteurs pour automatiser les certificats situés derrière les équilibreurs de charge : une fonctionnalité essentielle au vu du nombre de certificats typiquement associés à ces dispositifs.

Outils d'analyse avec agent
L'analyse basée sur les ports ne détecte pas certains certificats, notamment ceux installés sur les serveurs web Apache ou Microsoft IIS. Pour les découvrir, TLM utilise des agents qui recueillent des informations propres à ces certificats.

Outils d'analyse des vulnérabilités
TLM exploite des solutions de détection des vulnérabilités qui passent déjà votre réseau au crible, dressant et actualisant un inventaire et un plan complets de votre environnement d'entreprise.

Avantages de DigiCert® Discovery

Plus de visibilité
Obtenez une vue centralisée de tous les assets cryptographiques de votre environnement d'entreprise, tant pour leur gestion que pour l'émission de certificats

Moins de risques
Algorithmes trop faibles ; fichiers binaires non signés ; certificats vulnérables, non conformes ou arrivant à expiration… identifiez et corrigez rapidement tous les problèmes.

Plus de conformité
Évitez l'émission de certificats non autorisés et assurez-vous que vos politiques de sécurité sont bien respectées.

Crypto-agilité
Première étape de toute transition vers la cryptographie post-quantique, la découverte d'assets tient compte de la nature dynamique des ressources cryptographiques et offre une visibilité totale.

Intégration à Tenable
TLM assure la découverte de certificats de Tenable, qui utilise différents types de plug-in pour analyser et détecter les données.

Intégration à Qualys
Grâce à l'intégration des produits DigiCert à Qualys Vulnerability Management, Discovery and Response (VMDR), les clients peuvent gérer et automatiser les assets cryptographiques que détectent leurs outils d'analyse des vulnérabilités.

AWS Private CA et Microsoft CA
À l'heure où la migration vers le cloud se poursuit, les entreprises doivent gérer et détecter les différents certificats émis par AWS Private CA, Microsoft CA et d'autres AC, et ce afin de les importer et de les recenser dans leur inventaire central.

À vous de jouer

Pour en savoir plus sur les services PKI DigiCert®, contactez votre responsable de compte DigiCert ou envoyez un e-mail à sales@digicert.com.

À propos de DigiCert, Inc.

Leader mondial de la confiance numérique, DigiCert apporte aux entreprises et aux particuliers les outils qui leur permettront d'échanger et de communiquer de façon sereine et sécurisée dans l'univers du digital. Sa plateforme DigiCert® ONE assure aux organisations une visibilité centralisée et un contrôle inégalé sur leurs besoins en certificats publics et privés pour sécuriser tout leur environnement : site web, accès et communications d'entreprise, logiciels, identités, contenus et appareils.

Les solutions primées de DigiCert sont l'aboutissement d'un leadership incontesté en matière de standards, de support et de service, ce qui fait de nous le partenaire privilégié des organisations du monde entier. Pour plus d'informations, rendez-vous sur digicert.com/fr ou suivez-nous sur LinkedIn @digicert.