AUTOMATISATION TLS: RÉSULTATS DE VOTRE BILAN DE MATURITÉ

Faites le point sur les processus d'automatisation actuels de votre entreprise, son exposition au risque et les pistes d'amélioration potentielles.

digicert®

QUI DIT PROCESSUS MANUELS DIT VULNÉRABILITÉS

Découvrez de bonnes pratiques innovantes pour gérer vos certificats TLS

Face à la prolifération des certificats TLS à gérer et des risques à maîtriser, les responsables IT recherchent aujourd'hui des solutions plus agiles et efficaces pour protéger la sécurité digitale de leur entreprise. En ce sens, les produits d'automatisation TLS leur offrent davantage de contrôle sur leurs workloads complexes.

Automatisation: un impératif absolu

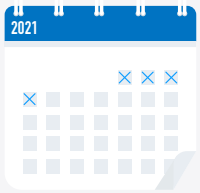
Tous les experts en sécurité digitale vous le diront : l'automatisation des certificats TLS constitue la solution optimale pour préparer les entreprises aux vulnérabilités de demain. Tout d'abord, l'automatisation permet de simplifier les tâches complexes de gestion des certificats. Prenons l'exemple de la fonction de recherche de la console DigiCert CertCentral®. Avec elle, les entreprises peuvent automatiquement suivre et identifier tous les certificats internes et externes à leurs réseaux.

Ensuite, lorsqu'elles automatisent le cycle de vie complet des certificats TLS, elles évitent les interruptions de services et failles de sécurité que peuvent provoquer des expirations imprévues de certificats. Ces entreprises sont ainsi mieux préparées à répondre aux nouvelles normes réglementaires que les Autorités de certification (AC) se doivent de faire appliquer. Souvent, le processus impose le remplacement ou la réémission rapide de certificats, sans parler du besoin de se projeter dès aujourd'hui dans l'ère de la cryptographie post-quantique. Pour toutes ces raisons et bien d'autres encore, les entreprises ont besoin de processus agiles et efficaces afin de préserver la sécurité de leur écosystème numérique.

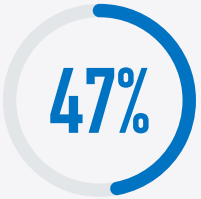
Votre sécurité est-elle à la hauteur?

DigiCert propose un bilan du degré de préparation à l'automatisation TLS conçu pour aider votre entreprise à dresser un état des lieux de son utilisation actuelle des fonctions de recherche et d'automatisation des certificats TLS. Vos réponses serviront ensuite à formuler quelques recommandations pour optimiser votre niveau de sécurité. Ce bilan vous oriente également vers les modèles de déploiement les plus en phase avec vos enjeux. PME, ETI, grande entreprise... nos solutions répondent aux exigences des organisations de toute taille de toute taille, quelque soit le nombre de certificats qu'elles possèdent. Pour s'adapter aux enjeux de votre entreprise, une solution d'automatisation optimale doit répondre à vos exigences et aux spécificités de vos ressources IT.

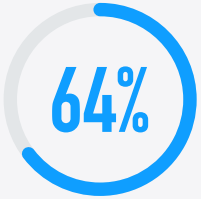
LA SÉCURITÉ DIGITALE EN CHIFFRES



1 à 4 jours par mois consacrés à la gestion des certificats



47% du temps de travail moyen des professionnels IT dédié à la gestion des certificats

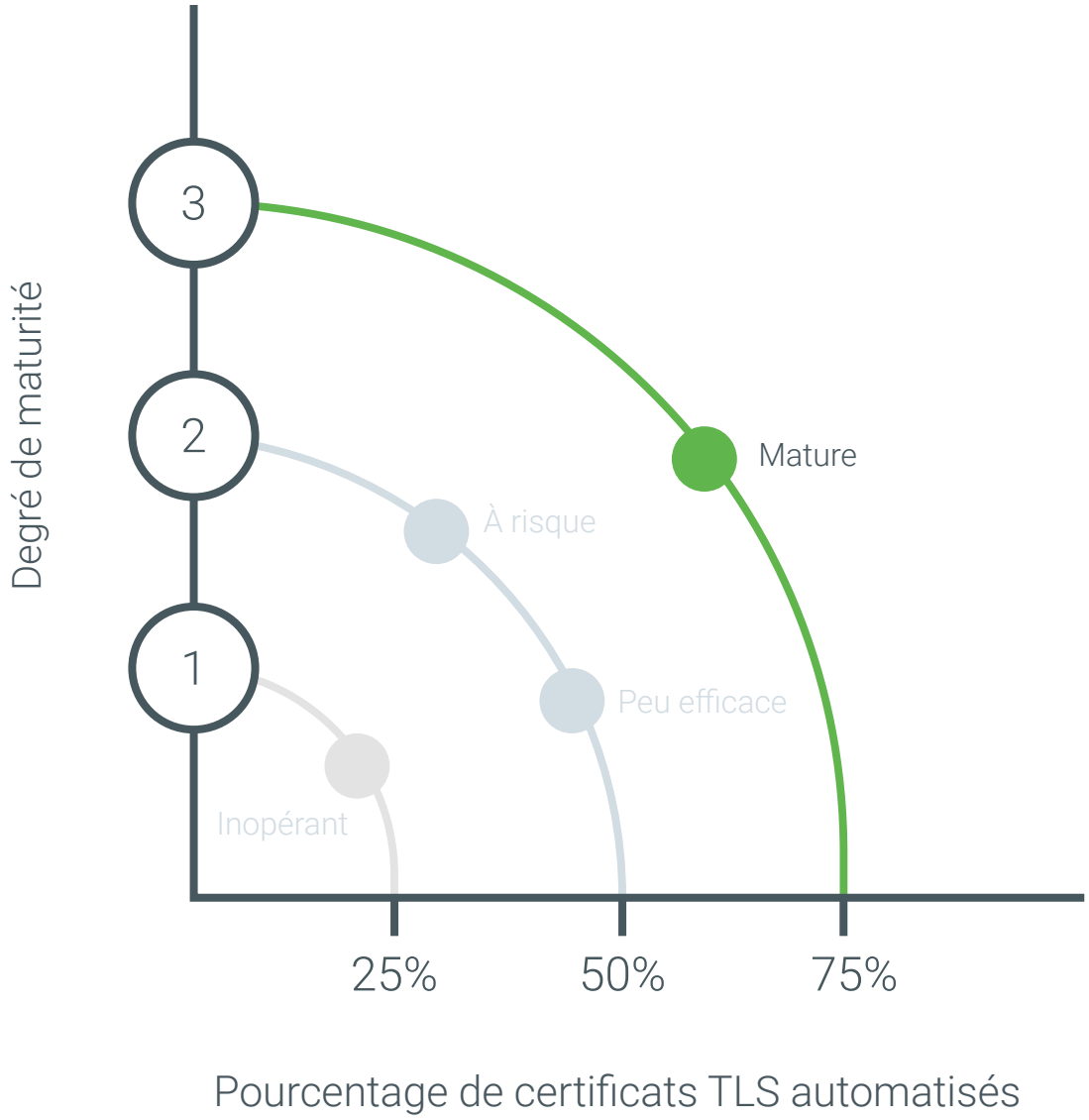


64% identifient un certificat non répertorié tous les mois

38% estiment que la durée nécessaire pour gérer les certificats pose un problème majeur

Source:
TLS Certificate Automation Research YouGov Report, février 2021

AUTOMATISATION TLS: LE MODÈLE DE MATURITÉ



VOS RÉSULTATS

Mieux comprendre votre niveau de sécurité

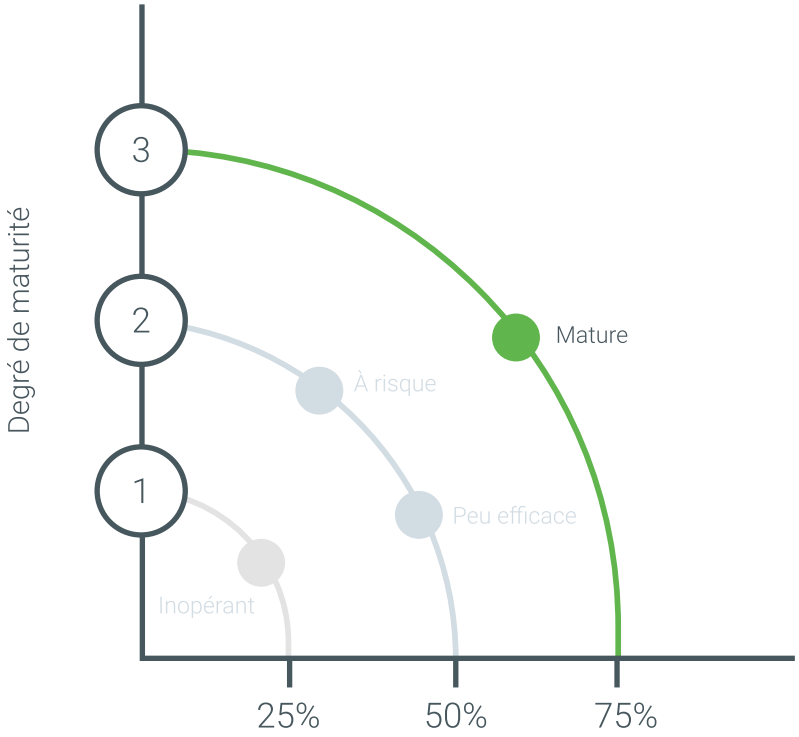
Niveau de sécurité:

PROACTIF ET MATURE

NIVEAU DE RISQUE GLOBAL: FAIBLE

Vous bénéficiez de processus d'automatisation efficaces et contrôlés, mais aussi d'une visibilité complète sur l'ensemble des certificats TLS/SSL de votre environnement. Ces atouts vous permettent d'adopter une approche proactive des questions de conformité et des prochaines évolutions sectorielles, tout en évitant les pannes dues à l'expiration imprévue d'un certificat. Les entreprises matures maîtrisent leur portfolio de certificats de bout en bout et automatisent jusqu'à 75 % de leurs certificats. Elles ont également intégré l'automatisation à leurs politiques de sécurité.

Explorez d'autres solutions pour automatiser jusqu'à 100 % de vos certificats. Vous serez ainsi prêt à affronter les menaces de demain, à remplacer rapidement des certificats en cas de problème et à vous projeter dès maintenant dans une optique de cryptographie post-quantique.



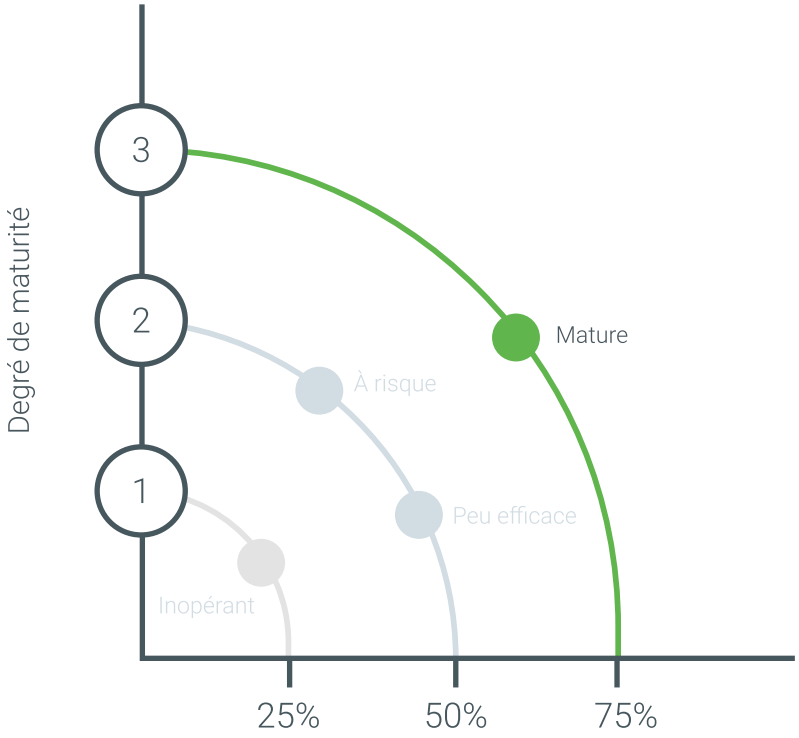
SUIVEZ LE GUIDE

Mesures concrètes pour renforcer votre sécurité

Niveau de sécurité:
PROACTIF ET MATURE

Voici quelques mesures que nous vous invitons à adopter
en priorité **dans les 12 prochains mois:**

- Continuez à intégrer l'automatisation à votre politique standard pour la gestion des certificats
- Automatisez les déploiements multiples sous divers modèles (hébergé et/ou sur site)
- Programmez un inventaire automatique mensuel de vos certificats sur tous les domaines web primaires ou noms de domaines qualifiés (FQDN)
- Envisagez l'utilisation de DigiCert Automation Manager: notre outil de gestion sur site, containerisé et basé sur un agent permet de créer une seule connexion sécurisée à tous les certificats TLS derrière votre pare-feu
- Optez pour l'automatisation basée sur des capteurs: cette fonction hébergée simplifie la gestion des certificats via l'interface CertCentral
- Faites de la crypto-agilité une priorité en recourant systématiquement à l'automatisation pour anticiper les menaces futures, notamment celles de la cryptographie post-quantique



SÉCURITÉ TLS: FAITES LE POINT

Comparez vos résultats aux autres niveaux de maturité

Niveau de sécurité:
RÉACTIF

NIVEAU DE RISQUE GLOBAL: ÉLEVÉ

Vos pratiques actuelles de gestion des certificats contraignent votre entreprise à camper dans une posture réactive face aux interruptions et vulnérabilités causées par des problèmes de certificats, mais aussi aux nouvelles exigences des AC. Parmi les principaux facteurs qui peuvent nuire à votre sécurité: un manque de visibilité et de réactivité. Le recours à des processus manuels inefficaces expose votre entreprise à toutes sortes d'incidents de sécurité potentiels.

Dans les PME, le manque de visibilité sur un inventaire empêche souvent de détecter des problèmes de certificats: erreurs de configuration, hachages, clés, suites cryptographiques trop faibles, etc. Quant aux grandes entreprises, elles peinent généralement à garder le contrôle de tous leurs certificats. Faute de solution adéquate, des angles morts apparaissent et des certificats peuvent être installés à votre insu en différents endroits de votre environnement, soit autant de points d'entrée potentiels pour les malwares.
À ce niveau de maturité, les entreprises s'exposent à un risque élevé d'interruptions coûteuses.

Niveau de sécurité:
À AMÉLIORER

NIVEAU DE RISQUE GLOBAL: MOYEN

En optant pour une plateforme de gestion TLS/SSL centralisée, votre entreprise a pris un bon départ. Néanmoins, votre équipe pourrait encore gagner en agilité afin de remédier plus rapidement aux pannes et autres problèmes. Sans outils d'automatisation, la moindre résolution peut vite se transformer en une opération complexe, inefficace et chronophage, notamment dans les environnements distribués ou complexes. Les processus manuels ne sont pas non plus adaptés à des opérations groupées, telles que le remplacement des certificats de fournisseur par défaut (qui sont en général auto-signés ou utilisent des clés faibles) ou le contrôle des déploiements de certificats adaptés.

En termes d'efficacité, il n'existe pas d'approche universelle de l'automatisation. De même, certains modes de déploiement (sur site, cloud ou hybrides) seront mieux adaptés que d'autres.

Niveau de sécurité:
PROACTIF ET MATURE

NIVEAU DE RISQUE GLOBAL: FAIBLE

Vous bénéficiez de processus d'automatisation efficaces et contrôlés, mais aussi d'une visibilité complète sur l'ensemble des certificats TLS/SSL de votre environnement. Ces atouts vous permettent d'adopter une approche proactive des questions de conformité et des prochaines évolutions sectorielles, tout en évitant les pannes dues à l'expiration imprévue d'un certificat. Les entreprises matures maîtrisent leur portfolio de certificats de bout en bout et automatisent jusqu'à 75 % de leurs certificats. Elles ont également intégré l'automatisation à leurs politiques de sécurité.

Explorez d'autres solutions pour automatiser jusqu'à 100 % de vos certificats. Vous serez ainsi prêt à affronter les menaces de demain, à remplacer rapidement des certificats en cas de problème et à vous projeter dès maintenant dans une optique de cryptographie post-quantique.

NOS RECOMMANDATIONS

Découvrez tous les avantages des solutions TLS à implémenter

Niveau de sécurité:
RÉACTIF

Voici quelques mesures que nous vous invitons à adopter en priorité **dans les 90 prochains jours:**

- Utilisez un outil capable de centraliser la gestion des certificats: DigiCert CertCentral® est doté de fonctions qui vous permettent de suivre, émettre, révoquer et remplacer tous les certificats depuis une seule et même console
- Déployez un outil de recherche pour visualiser l'ensemble de vos certificats: lancez des analyses ciblées afin de détecter tout changement dans votre environnement et d'obtenir des données contextualisées sur les problèmes de certificats potentiels
- Privilégiez les bonnes pratiques en matière de gestion TLS: sensibilisez et formez vos équipes au suivi du portfolio de certificats dans son intégralité et protégez votre environnement grâce à divers outils (stockage de clés standardisé, composants du cycle de vie, processus de décommissionnement et suivi des logs CT)
- Configurez des processus d'automatisation pour la gestion profils, programmes, alertes et intégrations tierces

Niveau de sécurité:
À AMÉLIORER

Voici quelques mesures que nous vous invitons à adopter en priorité **dans les 6 prochains mois:**

- Déployez des processus d'automatisation à la hauteur de vos exigences: API, URL ACME, agent Managed ACME, automatisation reposant sur des capteurs
- DigiCert Automation Manager... nous vous proposons des solutions à la hauteur de vos exigences de sécurité
- Programmez un inventaire automatique mensuel de vos certificats sur tous les domaines web primaires ou noms de domaines qualifiés (FQDN)
- Identifiez les opportunités de consolidation de vos systèmes ou budgets pour votre portfolio TLS: concentrez-vous sur l'innovation, l'efficacité et l'amélioration des processus
- Faites de l'automatisation une partie intégrante des politiques de gestion du cycle de vie des certificats TLS/SSL de votre entreprise
- Utilisez notre assistant d'automatisation: unique sur le marché, l'assistant DigiCert vous guide pas à pas pour choisir le modèle de déploiement adapté à vos enjeux

Niveau de sécurité:
PROACTIF ET MATURE

Voici quelques mesures que nous vous invitons à adopter en priorité **dans les 12 prochains mois:**

- Continuez à intégrer l'automatisation à votre politique standard pour la gestion des certificats
- Si besoin, automatisez les déploiements multiples sous divers modèles (hébergé et/ou sur site)
- Programmez un inventaire automatique mensuel de vos certificats sur tous les domaines web primaires ou noms de domaines qualifiés (FQDN)
- Envisagez l'utilisation d'Automation Manager pour les déploiements de certificats à grande échelle
- Faites de la crypto-agilité une priorité en recourant systématiquement à l'automatisation pour anticiper les menaces futures, notamment celles de la cryptographie post-quantique

BÉNÉFICIEZ DES MEILLEURS CONSEILS

Nos solutions d'automatisation ne reposent pas sur un modèle standard: elles s'adaptent à vos enjeux. Contactez votre chargé de compte ou écrivez-nous à contactus@digicert.com pour connaître les solutions les mieux adaptées à votre programme de sécurité.

digicert®