GUIDE DES BONNES PRATIQUES TLS 2022

Simplifiez et sécurisez vos processus grâce aux cinq piliers de la gestion du cycle de vie des certificats.

digicert®

GESTION PROACTIVE DES CERTIFICATS, UNE NÉCESSITÉ ABSOLUE

L'administration du cycle de vie de vos certificats s'impose comme un impératif face à l'essor continu des cas d'usage PKI. On observe en effet une augmentation exponentielle des pages web, des équipements, des systèmes et des serveurs dont les identités digitales et la sécurité doivent être gérés. D'où l'importance de suivre des pratiques de gestion des certificats garantes de la protection et de l'agilité cryptographique dont votre organisation a besoin. Dans cet eBook, nous vous proposons un framework à la fois simple et détaillé qui vous permettra de rester à la pointe de la sécurité numérique tout en garantissant votre conformité sur le long terme.

SOMMAIRE

RECHERCHE

Dressez l'inventaire complet de vos ressources cryptographiques

Identifiez l'exposition aux exploits connus

Repérez les failles de vos suites de chiffrement et versions TLS

GESTION ET REPORTING

Protégez vos clés privées

Définissez les priorités de remédiation

Contrôlez les certificats Wildcard émis et distribués

Déployez des certificats TLS adaptés à chaque cas d'usage

Contrôlez l'ensemble des certificats d'usine

Vérifiez la mise à jour des correctifs système

Sécurisez l'accès aux solutions de gestion des certificats

Intégrez votre plateforme aux systèmes ITSM

Examinez les alertes et les actions requises

NOTIFICATION

Hiérarchisez les notifications et les procédures d'escalade

Définissez des seuils de notification

Suivez les logs CT (Certificate Transparency)

Programmez des alertes CAA et empêchez les requêtes de certificats non autorisées

AUTOMATISATION

Automatisez le cycle de vie des certificats

Renforcez votre agilité cryptographique

Automatisation

Automatisez vos processus métiers

Personnalisez les intégrations à l'aide d'API

UNIFICATION

Implémentez une couverture totale des racines sur le réseau

Choisissez des services de recherche et d'importation couvrant toutes les AC

DRESSEZ L'INVENTAIRE COMPLET DE VOS RESSOURCES CRYPTOGRAPHIQUES

La découverte des certificats, socle essentiel des bonnes pratiques PKI

En faisant l'impasse sur l'indexation rigoureuse de ses certificats, votre entreprise s'expose à des risques de sécurité insoupçonnés. L'utilisation d'un service de recherche capable de détecter et de neutraliser les vulnérabilités (certificats non autorisés ou sur le point d'expirer, clés et hachages faibles, logiciels de serveurs obsolètes, etc.) constitue l'une des solutions les plus efficaces afin de se prémunir des interruptions et autres formes de perturbation.

Pour commencer, demandez à vos Autorités de certification (AC) de vous transmettre une liste des certificats émis. Mais attention : leur inventaire ne comprendra ni les certificats de vos AC internes, ni certains certificats installés sur des équipements connectés à votre infrastructure. C'est pourquoi l'analyse du réseau représente une étape incontournable du processus de détection. Les entreprises peuvent également compléter leur inventaire en inspectant les serveurs à la recherche de clés, d'algorithmes et de certificats utilisateurs ; en important les racines privées puis en identifiant les certificats émis à partir de celles-ci ; sans oublier les données issues d'autres outils de recherche.

À retenir :

Les services de recherche incarnent le premier pilier des bonnes pratiques de gestion PKI. Ils dépeignent un tableau complet et détaillé des ressources cryptographiques de votre entreprise. L'analyse, l'inspection et d'autres méthodes de détection peuvent être déployées en fonction de la stratégie d'atténuation des risques, afin de garantir une découverte et une remédiation constantes des vulnérabilités.

CONSTRUISEZ UNE VUE UNIFIÉE DE VOTRE PORTFOLIO :

- Analyses réseau
- Inspection des serveurs et des fichiers
- Découverte des racines privées
- Importation de données d'outils tiers

IDENTIFIEZ L'EXPOSITION AUX EXPLOITS CONNUS

Protégez vos systèmes contre les attaques ciblées.

Votre inventaire doit également inclure des détails sur les systèmes d'exploitation (Windows, Linux, etc.) et les applications (par exemple Apache) installés sur les serveurs. Pour combler les failles de sécurité potentielles, vous devez veiller à ce que chaque système soit mis à jour vers la dernière version disponible.

Ce point est important, car votre entreprise pourrait être vulnérable à des exploits critiques tels que Heartbleed, POODLE (SSLv3), FREAK, LogJam ou encore DROWN. Pensez aussi à évaluer la sécurité des OS et des certificats de vos serveurs web.

À retenir :

En identifiant la version des serveurs, des équilibreurs de charge, des frameworks d'applications, de l'infrastructure cloud, des bases de données et d'autres systèmes IT, vous pouvez neutraliser en amont les exploits et les vulnérabilités.

APACHE® Windows 11

REPÉREZ LES FAILLES DE VOS SUITES DE CHIFFREMENT ET VERSIONS TLS

Examinez les suites cryptographiques et les versions de certificats TLS/SSL.

Ces éléments sont généralement configurés sur vos serveurs web. De nombreuses attaques spécifiques à TLS/SSL ciblent des versions anciennes du protocole (par exemple, l'attaque POODLE sur SSL 3.0) ou des suites cryptographiques obsolètes (par exemple, l'attaque ROBOT sur le chiffrement RSA). Nous vous conseillons d'utiliser les versions les plus récentes de TLS, y compris TLS 1.2 et 1.3.

Qu'est-ce qu'une suite cryptographique ?

Il s'agit d'un ensemble d'algorithmes configurés sur un serveur web, dont l'objectif est de sécuriser les connexions TLS/SSL du réseau.

PROTÉGEZ VOS CLÉS PRIVÉES

À l'instar de la réutilisation d'un mot de passe, la réutilisation d'une clé vous expose à des risques inutiles.

Une clé privée est un fichier permettant de chiffrer et de déchiffrer les données qui transitent entre votre serveur et les clients. Elle est créée par le propriétaire du certificat au moment de la requête CSR (demande de signature de certificat). L'Autorité de certification (AC) qui émet votre certificat ne crée ni ne détient votre clé privée. Hormis vos administrateurs, personne ne doit jamais avoir accès à ces éléments. Une bonne pratique consiste à générer une nouvelle paire de clés pour chaque certificat. Par ailleurs, ne réutilisez jamais la même requête CSR, car en procédant ainsi, vous réutiliseriez automatiquement la même clé privée.

De plus :

- Vérifiez l'absence de clés faibles
- Recherchez les clés compromises
- Pour un stockage sécurisé, utilisez un coffre de clés, un jeton ou un HSM

À retenir :

Pour gagner du temps, certains sont tentés de réutiliser les CSR. Problème : cette démarche duplique les clés et multiplie les risques. En automatisant les requêtes et les processus de renouvellement, vous pouvez réduire de façon drastique l'effort manuel requis pour la génération de CSR et le provisionnement de vos certificats.

PRIORISEZ LA REMÉDIATION

Éliminez les clés, les suites cryptographiques et les hachages vulnérables, ainsi que toute ressource obsolète dans votre portfolio.

Les certificats contiennent des clés publiques et des signatures susceptibles d'être vulnérables aux attaques. Les certificats qui utilisent des clés d'une longueur inférieure à 2048 bits ou des algorithmes de hachage obsolètes, comme MD5 et SHA-1, ne sont plus autorisés sur les serveurs web publics. Toutefois, certains peuvent persister sur vos sites web internes. Si c'est le cas, vous devez immédiatement les remplacer.

Plus important encore, vous devez vérifier les versions des certificats TLS/SSL et des suites cryptographiques compatibles avec vos serveurs web. Pensez toujours à activer les dernières versions de TLS, y compris TLS 1.2 et TLS 1.3. De même, vous devez impérativement utiliser les suites cryptographiques les plus récentes, comme AES. Vous pouvez aussi consulter cette liste pour connaître les suites obsolètes qui ne sont plus utilisées.

Versions TLS/SSL obsolètes et vulnérables :

- SSL v2
- TLS 1.0
- SSL v3
- TLS 1.1

CONTRÔLEZ LES CERTIFICATS WILDCARD ÉMIS ET DISTRIBUÉS

L'émission de certificats Wildcard introduit d'autres problèmes de sécurité.

Les certificats Wildcard, qui permettent aux administrateurs de protéger plusieurs domaines à l'aide d'une seule clé privée, présentent pourtant des risques de sécurité intrinsèques pour cette même raison. Ainsi, le vol ou la perte d'une telle clé constituerait un point de compromission unique pour tous les serveurs associés au certificat. L'utilisation d'une même clé privée sur le réseau, ou encore son partage entre plusieurs départements, multiplie les chances que celle-ci soit égarée ou dérobée – auxquels cas il vous faudra remplacer l'ensemble des certificats affectés. De plus, si le certificat est révoqué pour une raison ou une autre, la clé privée devra être mise à jour sur tous les serveurs concernés. D'autre part, pour éviter les perturbations dues au déplacement de données sur le réseau, toutes ces opérations devront être exécutées en une seule fois.

Enfin, malgré leur attractivité initiale (économie de temps et d'argent), la gestion du renouvellement ou du remplacement imprévu de certificats Wildcard peut entraîner une charge de travail considérable pour les entreprises.

À retenir :

Lorsque vous utilisez un certificat Wildcard, il est impératif de protéger votre clé privée. De plus, pour atténuer les dangers inhérents au partage d'une clé unique sur le réseau, il peut être judicieux d'en créer une nouvelle pour chaque copie de votre certificat Wildcard, tout en implémentant un système de sécurité spécifique à ces ressources. Nous vous conseillons en outre de déployer une solution d'automatisation sur l'ensemble des serveurs associés au certificat : vous gagnerez ainsi du temps, réduirez l'erreur humaine et diminuerez le risque de perte de vos clés.

DÉPLOYEZ DES CERTIFICATS TLS ADAPTÉS À CHAQUE CAS D'USAGE

Choisissez un niveau d'assurance adéquat pour sous-tendre vos opérations.

Si vous sécurisez un site Internet qui collecte les identifiants ou les informations des utilisateurs, par exemple via des formulaires, nous vous invitons à opter pour un certificat à haute assurance afin de vous prémunir contre toute forme d'imitation de votre marque et de votre interface web.

Le choix d'un certificat TLS à validation étendue (EV) offre à cet égard les meilleures garanties. Les certificats EV sont couramment utilisés par les pouvoirs publics, les multinationales, les banques ou encore les prestataires de services financiers. Leur processus de validation ultra rigoureux, qui se décline en seize phases, vérifie différents détails tels que les coordonnées du demandeur de certificat, sa fonction et son intitulé de poste. Cette étape inspecte également les données de placement sur liste de blocage, le nom de domaine, le numéro d'enregistrement, la juridiction ainsi que l'agrément de l'entreprise.

Les certificats TLS à validation d'organisation (OV) occupent la deuxième marche du podium. Ils valident les droits de propriété sur le domaine et examinent toutes les coordonnées de votre entreprise. Ceci implique notamment la confirmation de l'adresse physique, un appel téléphonique visant à authentifier la demande de certificat, un recoupement avec les listes de blocage, ainsi que des contrôles antifraude et antimalware.

Enfin, les certificats TLS à validation de domaine (DV) offrent le niveau le plus bas en matière d'authentification des identités. Étant donné le risque d'imposture, ils ne sont jamais recommandés pour les sites qui gèrent des données sensibles. D'autre part, même si des certificats TLS privés sont utilisés sur des systèmes internes, il est important que la racine privée soit correctement propagée aux utilisateurs afin de garantir la sécurité.

CAS D'USAGE DES CERTIFICATS :

VALIDATION ÉTENDUE (EV)

- Banques et services financiers
- Entreprises du CAC 40
- Grands groupes internationaux
- Sites d'e-commerce
- Conformité (p. ex., HIPAA, PCI)

VALIDATION D'ORGANISATION (OV)

- Pages de connexion
- Sites web d'entreprise
- Conformité (p. ex., HIPAA, PCI)

VALIDATION DE DOMAINE (DV)

- Blogs
- Sites web personnels
- Sites web qui ne gèrent pas de transactions et ne recueillent pas de données personnelles

CONTRÔLEZ L'ENSEMBLE DES CERTIFICATS D'USINE

Les certificats des fournisseurs sont conçus dans une optique de praticité, mais pas nécessairement de sécurité.

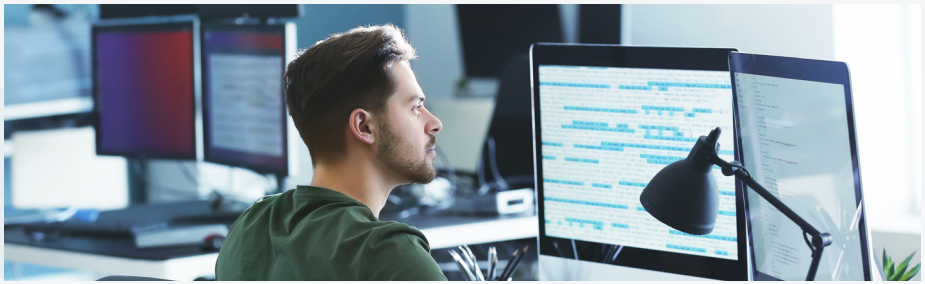
Ils sont émis par des fabricants de matériel afin d'être préinstallés sur leurs équipements en usine. Le problème de ces certificats est qu'ils ne sont pas conçus pour être déployés sur des réseaux en production. Il s'agit en général de certificats auto-signés, expirés ou utilisant des clés faibles par défaut. De fait, ils ne sont pas considérés comme fiables par les navigateurs. Beaucoup d'organisations possèdent des milliers de certificats d'usine sans même le savoir. Chacun de ces certificats doit être supprimé et remplacé par un certificat de confiance (au minimum un certificat TLS/SSL privé). Pour simplifier cette opération, utilisez des outils d'automatisation récents basés par exemple sur des API ou des URL ACME.

VÉRIFIEZ LA VERSION DES CORRECTIFS SYSTÈME

Il est important de patcher régulièrement vos serveurs, sans quoi vous vous exposez aux cyberattaques les plus dévastatrices.

Les correctifs assurent la mise à jour des OS, des serveurs, des frameworks d'applications, des bases de données et d'autres logiciels et ressources informatiques, qu'ils protègent contre d'éventuelles vulnérabilités. Il peut s'agir par exemple des systèmes Windows et Linux, de vos équilibreurs de charge ou de vos serveurs web.

Ces mises à jour aident à éviter les attaques comme celles liées au bug Heartbleed – une faille de sécurité découverte dans la bibliothèque logicielle cryptographique d'OpenSSL. Cette vulnérabilité aboutissait à l'injection d'une porte dérobée (backdoor) permettant aux hackers de lire la mémoire des systèmes affectés – et donc d'épier les communications ou de voler les données des services et des utilisateurs.



SÉCURISEZ L'ACCÈS AUX SOLUTIONS DE GESTION DES CERTIFICATS

Privilégiez des outils sûrs tels que l'authentification à deux facteurs et l'authentification unique (SSO).

L'authentification à deux facteurs (2FA), ou multifacteur (MFA), requiert l'utilisation de plusieurs méthodes de sécurité (par exemple l'envoi d'un code sur un autre de vos équipements) afin de pouvoir se connecter aux ressources. Ces techniques vous aident à renforcer les défenses de vos plateformes de gestion des certificats lorsque vous consultez et gérez votre portfolio.

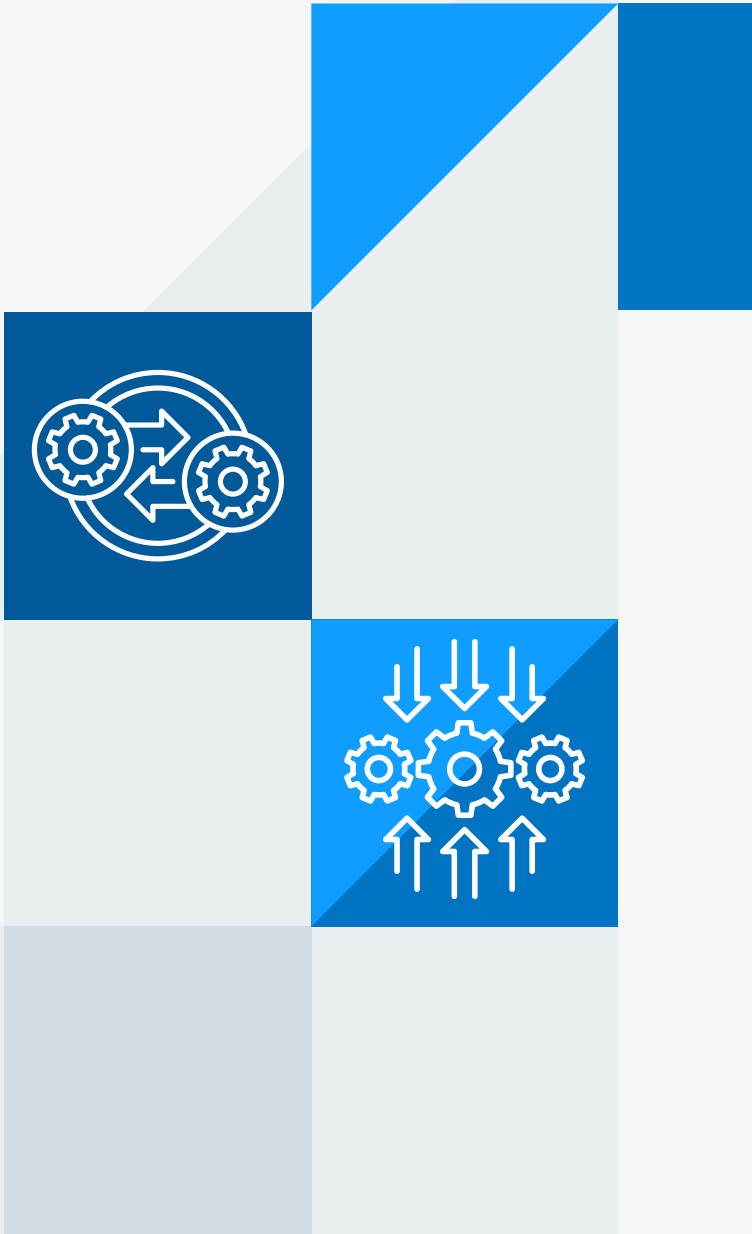
Quelques exemples d'authentification 2FA/MFA :

- Authentification 2FA à l'aide d'un appareil mobile
- Appli d'authentification 2FA
- Générateur de jetons 2FA

INTÉGREZ VOTRE PLATEFORME AUX SYSTÈMES ITSM

Les plateformes de gestion des certificats peuvent s'intégrer à d'autres solutions logicielles telles que ServiceNow pour s'interfacer de façon transparente à vos fonctions IT opérationnelles.

Si votre entreprise doit composer avec des environnements IT complexes, vous avez tout intérêt à intégrer votre plateforme de gestion des certificats à un système ITSM (gestion des services informatiques) – comme ServiceNow – pour créer des flux d'approbation en phase avec vos processus, et ce tout au long du cycle de vie des certificats. Grâce à cette approche, vos collaborateurs pourront demander les certificats TLS dont ils ont besoin, sans que vous ayez à leur donner directement accès à vos systèmes de gestion. De plus, l'utilisation d'une solution ITSM pour régir les processus d'escalade ré l'erreur humaine tout en améliorant la disponibilité des systèmes.



EXAMINEZ LES ALERTES ET LES ACTIONS REQUISES

Appuyez-vous sur des tableaux de bord faisant apparaître les éléments qui nécessitent une action ou une investigation.

L'utilisation d'un tableau de bord centralisé, capable de suivre le statut des ressources préalablement identifiées, constitue un excellent premier pas. Mais vous devez également veiller à la clarté, à l'enrichissement ainsi qu'à l'exploitabilité des données présentées.

Votre système de reporting doit vous permettre :

- De voir la totalité de vos certificats à partir d'une seule console
- D'élaborer, de télécharger, de planifier ou d'intégrer des rapports détaillés
- D'identifier facilement les problèmes et les actions spécifiques à engager (certificats non autorisés, expiration imminente, non-conformité, etc.)
- D'afficher vos données sous forme de représentations graphiques intuitives, faciles à partager et indiquant clairement la marche à suivre

HIÉRARCHISEZ LES NOTIFICATIONS ET LES PROCÉDURES D'ESCALADE

Définissez et automatisez les destinations ainsi que les méthodes de notification.

Évitez l'expiration de certificats et autres compromissions de sécurité en établissant des hiérarchies pour vos procédures de notification et d'escalade. Ces hiérarchies doivent être définies par groupe de certificats et selon les paramètres suivants :

- Le déclencheur de la notification
- La méthode de communication (p. ex., e-mail, alertes, Slack, ITSM)
- Le destinataire de la notification
- Les seuils d'escalade

Pensez également à vérifier que vos contacts e-mail sont bien à jour au regard de l'AC émettrice, de façon à recevoir toutes les notifications de renouvellement ou d'incident potentielles.

DÉFINISSEZ DES SEUILS DE NOTIFICATION

Paramétrez et automatisez des préavis de renouvellement à 90, 60 ou 30 jours avant l'expiration de vos certificats.

Ces différents rappels vous permettront de prendre les devants et d'éviter ainsi toute expiration accidentelle de certificat. Nous recommandons de renouveler un certificat au moins 15 jours avant sa date d'expiration pour vous laisser le temps de tester et de vérifier le nouveau certificat. Si votre processus de contrôle des modifications est plus long, un délai de 32 jours sera plus approprié.

Enfin, une bonne pratique consiste également à définir des seuils d'alerte relatifs aux certificats expirés.

SUIVEZ LES LOGS CT (CERTIFICATE TRANSPARENCY)

Tout certificat public non enregistré dans un log CT (Certificate Transparency) ne sera pas considéré comme fiable par les navigateurs.

Utilisez un outil de surveillance des logs CT afin de détecter rapidement les certificats non autorisés, ainsi que pour identifier et corriger les certificats émis par erreur. Ces journaux CT offrent une traçabilité aux AC émettrices de certificats TLS/SSL pendant le processus de validation. Si un tiers émet un certificat pour votre nom de domaine, que ce soit à des fins malveillantes ou en infraction avec vos politiques, la surveillance des logs CT détecte l'anomalie et vous alerte immédiatement.

PROGRAMMEZ DES ALERTES CAA ET EMPÊCHEZ LES REQUÊTES DE CERTIFICATS NON AUTORISÉES

Un registre CAA (Autorisation d'Autorité de certification) est un enregistrement DNS répertoriant les AC habilitées à émettre des certificats pour votre domaine.

En 2017, le CA/Browser Forum a soumis la proposition de vote 187 exigeant de toutes les AC qu'elles vérifient systématiquement les enregistrements DNS CAA et qu'elles se conforment aux dispositions prévues pour le domaine en question. Les responsables de domaine peuvent ainsi déclarer les AC habilitées à émettre un certificat pour leur domaine. Le registre CAA permet également de recevoir des notifications en cas de demande de certificat auprès d'une AC non autorisée.

AUTOMATISEZ LE CYCLE DE VIE DES CERTIFICATS

Simplifiez le renouvellement, l'installation et la génération de CSR pour vos certificats.

L'automatisation s'impose comme une nécessité opérationnelle pour les entreprises qui souhaitent gérer efficacement un nombre élevé de certificats. En automatisant différentes tâches de gestion manuelles, vous pouvez réduire les erreurs humaines ainsi que le temps et les ressources que mobilisent de vastes portfolios de certificats de courte durée.

L'automatisation des certificats :

- Simplifie les processus d'émission, de remplacement et de renouvellement des certificats
- Évite les interruptions de service en éliminant l'erreur humaine et en barrant la route aux mauvaises configurations
- Soulage les équipes de support IT grâce au provisionnement automatique des utilisateurs
- Accélère la remédiation en remplaçant les certificats compromis en toute efficacité

RENFORCEZ VOTRE AGILITÉ CRYPTOGRAPHIQUE

La cryptographie post-quantique se profile à l'horizon.

Quels que soient leur secteur d'activité et les standards cryptographiques futurs, les entreprises peuvent pérenniser la sécurité de leurs opérations en misant dès aujourd'hui sur des outils d'automatisation prenant en charge l'émission et le renouvellement des certificats. Ce faisant, elles réduiront le temps nécessaire à la gestion, au suivi ou au remplacement des certificats lors d'un incident de sécurité. De plus, l'automatisation permet également de simplifier la mise à jour des algorithmes cryptographiques.

AUTOMATISEZ VOS PROCESSUS MÉTIERS

Définissez des règles d'accès, des workflows, des modèles et des intégrations.

L'automatisation de la gestion des certificats s'étend au-delà du provisionnement, de l'installation et du renouvellement de vos certificats TLS. En appliquant cette approche à vos processus métiers, vous pouvez rationaliser l'administration de vos infrastructures PKI sur l'ensemble de votre portfolio de certificats et de ressources cryptographiques. Règles d'accès prédéfinies, automatisation des workflows d'approbation et de notification, enrôlement automatique, clés sécurisées, intégration aux systèmes d'entreprise… l'automatisation des processus métiers constitue un précieux atout pour renforcer votre posture de sécurité et simplifier vos opérations.

PERSONNALISEZ LES INTÉGRATIONS À L'AIDE D'API

Bénéficiez d'une intégration directe entre votre plateforme de gestion des certificats et vos systèmes d'entreprise.

Rationalisez l'administration des certificats avec vos systèmes, processus ou produits existants grâce aux intégrations par API. Parmi les exemples les plus courants, on trouve l'intégration aux systèmes ITSM, de façon à aligner l'activité des certificats sur les processus liés aux fenêtres de changement, ou encore des outils de détection ciblés qui aident à créer une vue unifiée de tout le portfolio de certificats.

IMPLÉMENTEZ UNE COUVERTURE TOTALE DES RACINES SUR LE RÉSEAU

Les racines des AC les plus récentes ou de taille modeste ne sont pas forcément incluses dans les magasins de certificats de tous les navigateurs, en particulier les plus anciens.

Respectez les bonnes pratiques en n'utilisant que des certificats provenant d'une AC de confiance et offrant une couverture étendue des racines. Vérifiez que ces certificats sont bien présents dans les magasins de clés des navigateurs, récents ou non, afin de garantir leur compatibilité avec 99,9 % des plateformes et navigateurs clients.

Autrefois, les racines de certaines Autorités de certification n'étaient pas systématiquement ajoutées aux nouvelles versions des navigateurs. Résultat, les internautes accédant aux plateformes concernées étaient accueillis par des messages d'erreur. Autant dire qu'un tel incident peut avoir de sérieuses répercussions sur le taux de conversion et la réputation d'un site web.

CHOISISSEZ DES SERVICES DE RECHERCHE ET D'IMPORTATION COUVRANT TOUTES LES AC

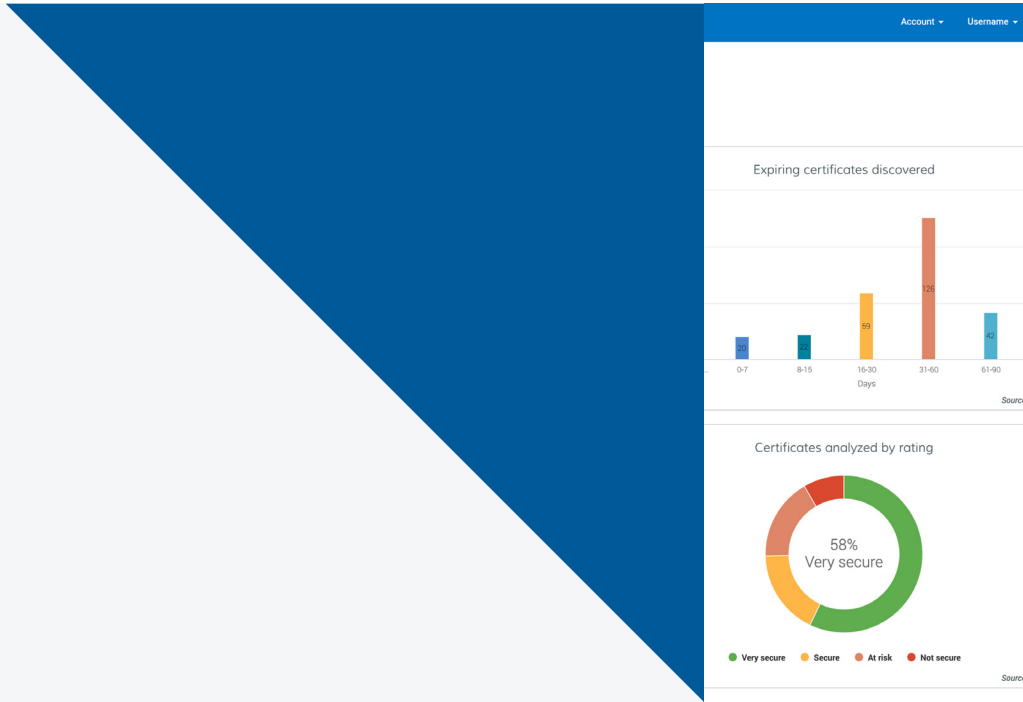
Misez sur une plateforme de gestion prenant en charge les certificats de différentes AC.

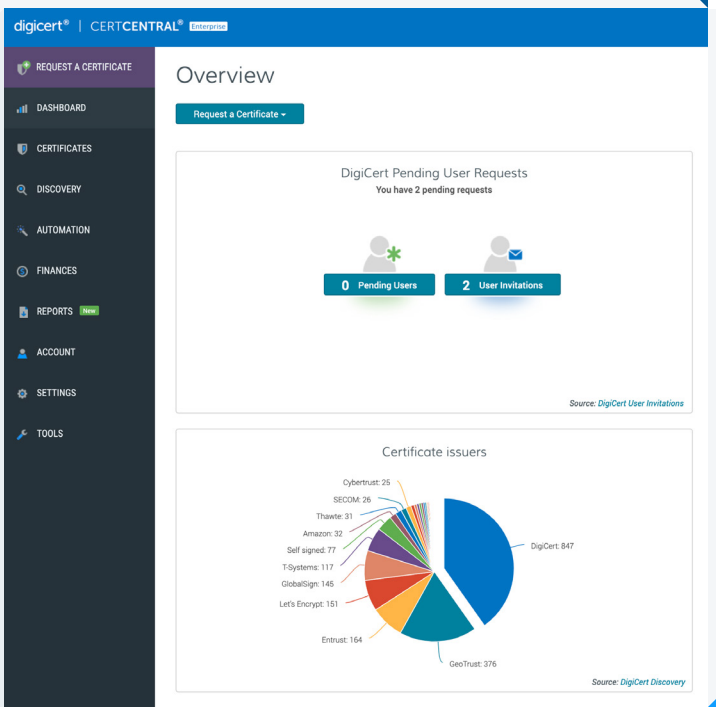
L'utilisation d'une solution indépendante des Autorités de certification vous permet de suivre et de gérer chacun de vos certificats – peu importe le type ou l'AC émettrice – au sein d'une plateforme unifiée. Optez pour des outils de détection capables d'importer les certificats racines privés afin d'effectuer des recherches depuis ces racines ou à partir d'autres ressources cryptographiques. Une telle approche peut ensuite aboutir à une vue exhaustive et unifiée de votre portfolio de certificats.

CONCLUSION

Mettez fin aux pratiques fastidieuses de gestion du cycle de vie des certificats.

Recherche, gestion et reporting, notification, unification et surtout automatisation de votre portfolio : les solutions DigiCert de gestion du cycle de vie des certificats vous offrent toutes les clés pour implémenter les cinq piliers des bonnes pratiques TLS. Nos outils complets et intuitifs représentent le choix idéal pour renforcer ou bâtir votre programme de gestion proactive des certificats.





MISEZ SUR UNE GESTION PROACTIVE DE VOS CERTIFICATS

Simplifiez la gestion du cycle de vie de vos certificats pour mieux vous recentrer sur des activités plus stratégiques pour votre entreprise. Avec DigiCert, vous bénéficiez d'une gamme de produits qui vous aideront à implémenter toutes les bonnes pratiques de certification. Contactez-nous par **e-mail** pour échanger ensemble sur vos besoins, ou rendez-vous sur notre site web pour demander une **démo complète**.