LOCKSELF

DSI & Automatisation

Comment gagner en productivité et en sécurité grâce à l'API de votre coffre-fort numérique ?

Martin Bonneau
Administrateur Systèmes

Patrick Trouillard
Urbaniste des SI

Sylvain Nohannic
DSI

DARVA

Up Coop

THALOS
ADVANCED MARITIME SOLUTIONS

INTERVIEWS

Édito

Lucas Tadajewski
Co-fondateur et CTO de LockSelf

Selon le rapport 2024 MuleSoft de Salesforce, **la quasi-totalité des entreprises (99%) utilisent des API, mais peu d'entre elles en ont fait un levier stratégique***.

Les API (Application Programming Interface ou « Interface de Programmation d'Application ») sont des interfaces logicielles permettant, à l'aide de scripts, d'automatiser un certain nombre de tâches dans le système d'information d'une organisation.

Bien plus qu'un simple outil technique, elles sont indispensables pour **améliorer l'efficacité opérationnelle du SI (48%),** et aident également à satisfaire les exigences des équipes métiers (46%).*

Mais quels avantages et quelles tâches automatiser avec son coffre-fort numérique grâce à l'API ? Les intérêts sont multiples.

Automatiser son coffre-fort numérique c'est avant tout un gain de temps, de productivité, qui permet de **libérer les équipes de la DSI** mais aussi les équipes métiers de tâches chronophages. C'est aussi, un véritable levier pour **éradiquer le risque d'erreur humaine, limiter le Shadow IT et sécuriser les process de toute l'organisation.**

Par exemple, en intégrant l'API LockSelf dans vos scripts de création de VM (Virtual Machine ou Machine Virtuelle), vous pouvez automatiser la sauvegarde sécurisée des mots de passe de ces terminaux et garantir que ces identifiants soient uniques, complexes et partagés aux seules personnes ayant droit d'y accéder. Finis également les mots de passe stockés en clair dans les scripts.
Vous pouvez aussi automatiser la **rotation de mots de passe d'accès aux serveurs, programmer des exports chiffrés** de vos données ou encore **créer des alertes** sur des tentatives d'accès suspectes aux yeux de vos politiques de sécurité interne.

Dans ce livre blanc, vous découvrirez comment démultiplier la sécurité informatique au sein de votre organisation, à travers plusieurs retours d'expériences et des cas d'usages d'automatisation du coffre-fort numérique LockSelf.

Inspirez-vous-en, toutes les actions réalisables par un utilisateur humain connecté sur son compte sont automatisables via notre API et tous les outils peuvent être interconnectés avec votre coffre-fort LockSelf.

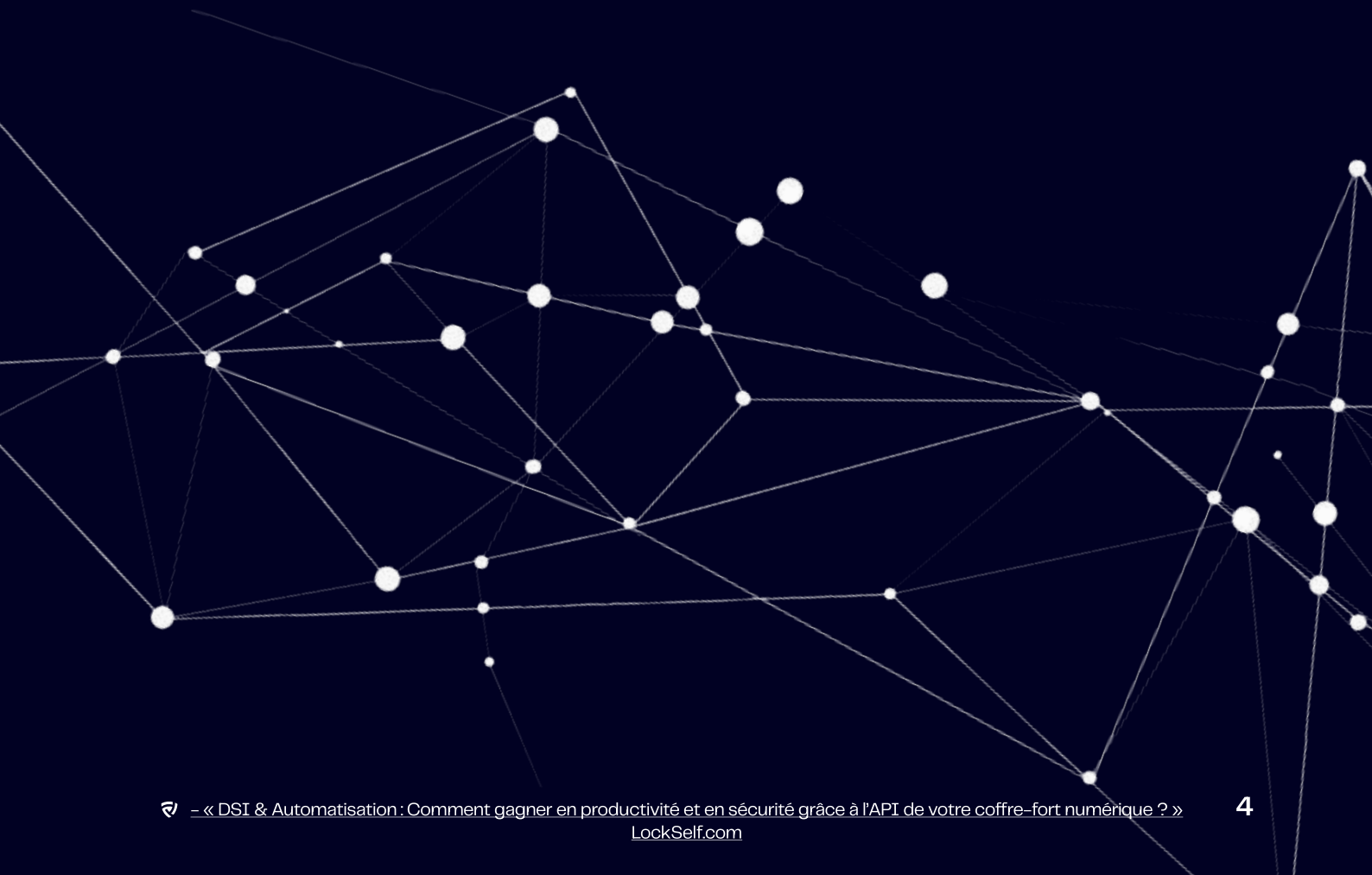
Délestez-vous des tâches chronophages et sécurisez de nombreux processus métiers !

*Source : 2024 Connectivity Benchmark Report – MuleSoft de Salesforce – En collaboration avec Deloitte Digital.

Sommaire

Économiser 3 semaines de travail à temps plein avec l'API LockSelf

Retour d'expérience de Patrick Trouillard, Urbaniste des SI chez UpCoop



“ En plus d’être un outil de sécurité, LockSelf avec son API nous permet de gagner en productivité. ”

Patrick Trouillard
Urbaniste des systèmes d’information
Société UpCoop

Retour d’expérience

Bonjour Patrick, pouvez-vous nous présenter votre métier et l’organisation dans laquelle vous travaillez ?

UpCoop maison-mère du groupe Up présent dans 23 pays est la 1ère société coopérative et participative (SCOP) de France, à être devenue une entreprise à mission. Depuis 60 ans, **UpCoop propose des solutions de paiement et des services à utilité sociale et locale.**

Nous proposons principalement des moyens de paiement tels que les titres-restaurant UpDéjeuner, les chèques culture, les titres cadeaux UpCadhoc, le titre UpSport&Loisirs et des solutions tout en un comme UpOne.

Nos titres de paiement et plateformes de gestion ont pour vocation de donner aux entreprises, aux CSE, aux collectivités et pouvoirs publics les moyens d’**améliorer le pouvoir d’achat et la qualité de vie des salariés et des populations au cœur des territoires.**

En 2017, le Groupe Up a notamment lancé UpCohésia, un dispositif 100 % dématérialisé de cartes qui simplifie la mise en place et la gestion des aides publiques. Les demandeurs d’asile éligibles perçoivent par exemple une aide de l’État français leur permettant de vivre décemment sur le territoire en attendant le traitement de leur demande. Avec UpCohésia, l’État, les collectivités et les ONG remettent à ces personnes des cartes de paiement créditées du versement des subventions.

Ce dispositif a également servi pour venir en aide aux réfugiés ukrainiens du fait de la guerre avec la Russie. UpCohésia s'inscrit ainsi dans le **cadre très réglementaire** des émetteurs de monnaie électronique et c'est dans ce contexte que **nous avons fait le choix d'utiliser l'ensemble de la suite LockSelf.**

Je suis pour ma part **responsable de l'architecture SI, data et de la sécurité.** J'ai une vision globale du SI qui me permet d'assurer une cohérence dans son évolution et de faire respecter des directives d'urbanisation (cela consiste à capitaliser sur l'utilisation de l'existant avant de commanditer un nouvel outil). J'ai également sous mon giron les **enjeux de sécurité**, ce qui nous permet dans la conception même du système d'information d'en assurer sa sûreté. J'interviens en général en amont des projets avec des équipes d'architectes techniques, d'architectes fonctionnels et d'architectes sécurité.

Vous avez fait le choix de mettre en place la suite LockSelf. Quels étaient vos besoins ?

Nous nous sommes aperçu qu'au sein de l'écosystème Microsoft Office 365 que nous utilisons, certaines règles concernant le **partage de fichiers** n'étaient pas respectées.

Par exemple, au lieu de partager un fichier avec une personne, certains documents (parfois très sensibles) se retrouvaient partagés à l'ensemble de l'organisation, à un service complet, voire même vers l'extérieur.

Il nous fallait répondre immédiatement à cette problématique. Nous avons ainsi fait le choix de prendre un outil tiers pour venir **sécuriser les usages.**

Nous avons choisi LockSelf pour des raisons de **confidentialité**, de **stockage sécurisé** et de **simplicité** pour transférer et récupérer des documents sensibles à l'interne comme vers l'externe.

La vertu de LockSelf c'est de **mettre l'accent sur la segmentation et la traçabilité.**

Je sais tout de suite :

- Qui accède à mon fichier
- Quand est-ce qu'il y accède
- Et jusqu'à quand il y a accès

C'est un véritable **outil dédié au partage sécurisé.**

Lors de l'appel d'offres de l'État pour dématérialiser le versement des subventions, LockSelf nous a permis d'avoir un avantage indéniable pour proposer notre solution UpCohésia. La certification ANSSI de LockSelf et le fait que l'outil soit 100% français sont venus rassurer les différentes parties prenantes sur la façon dont les **informations sensibles** seraient récupérées et stockées.

En effet, pour ce type de service, nous avons des obligations légales concernant la validation de l'identité de la personne qui percevra la subvention. C'est un processus identique pour tout établissement bancaire ou de crédit. Au vu de la population concernée par ce projet nous ne pouvions pas proposer de "self-enrolling". Ainsi, ce sont les collectivités elles-mêmes qui nous font parvenir les cartes d'identité des bénéficiaires. Ces informations sensibles (cartes d'identité) nécessitent un **traitement hautement sécurisé.** En proposant de transférer et de stocker ces éléments sensibles grâce à un **outil français, sécurisé et certifié,** nous avons remporté l'appel d'offres.

LockSelf est ainsi venu répondre à un besoin de sécurisation des flux et des fichiers que nous échangeons avec nos partenaires externes ou clients.

Pourquoi le choix de LockSelf ? Quels sont, selon vous, ses avantages ?

LockSelf, offre un **outil dédié à la sécurité et à la traçabilité des données,** ce qui en fait une solution vraiment professionnelle.

Nous avons ainsi une gestion plus granulaire des droits d'accès que sur Microsoft Office 365 qui ne venait pas couvrir tous nos besoins en termes de partage sécurisé. L'usage est également plus simple.

LockTransfer a aussi un côté rassurant pour nos clients qui se disent "Ah ils ont un outil sécurisé pour les transferts qui est vraiment professionnel".

Émily Boittiaux

Responsable des opérations pour le secteur public d'UpCohésia nous détaille l'utilisation de LockTransfer et LockFiles par ses équipes.

" Lors du déploiement de UpCohésia auprès de structures publiques, nous avons été amenés à mettre en place une solution sécurisée pour le recueil de documents d'identité. Ce type de documents implique nécessairement une **forte confidentialité, un transfert sécurisé et un stockage chiffré.**

Déployer LockSelf nous a permis de **gérer finement les droits de partage et la durée de partage de chaque fichier.**

LockSelf nous sert ainsi à deux niveaux :

1. Dans le cadre de ce projet, les **boîtes de dépôts LockTransfer** sont ainsi utilisées pour venir **récupérer des documents sensibles** (carte d'identité) auprès des services compétents de l'État notamment, nous permettant de valider l'éligibilité des bénéficiaires. Chacun de nos clients dispose ainsi d'un accès "invité" à une boîte de dépôt dans laquelle il va pouvoir déposer les pièces d'identité ou tout autre fichier sensible.

2. Une fois ces pièces d'identité récupérées, nous les déposons dans LockFiles pour les stocker dans la durée de façon sécurisée. LockFiles nous sert aujourd'hui de **coffre-fort numérique sécurisé pour stocker les documents sensibles** que nous réceptionnons et pour lesquels nous avons une obligation de conservation tout au long de la relation avec le bénéficiaire.

   Nous avons ainsi un dossier par client et un nommage bien spécifique afin de pouvoir retrouver facilement chacune des pièces.

Ce sont des échanges de données personnelles que nous ne voulons pas et ne pouvons pas faire transiter via de simples mails.

Nous avons également un usage plus standard de LockTransfer, pour envoyer tout type de documents en interne ou vers l'externe. Cela vient remplacer l'utilisation d'un simple mail qui ne serait pas sécurisé. "

Serge Bertaina Dubois

Directeur de l'expérience client chez UpCoop,
nous détaille leur cas d'usage API.

Vous avez fait le choix de vous appuyer sur l'API LockSelf. Pouvez-vous nous détailler vos cas d'usages ?

" En plus d'être un outil de sécurité, **LockSelf avec son API nous permet de gagner en productivité.**

Aujourd'hui les API nous permettent d'automatiser un certain nombre de processus répétitifs, à faible valeur ajoutée pour les collaborateurs et qui étaient jusqu'alors fait de façon manuelle.

J'ai en charge depuis 2018 chez UpCoop l'intégration, le maintien en condition opérationnelle, la veille technologique, le paramétrage et les développements autour de la solution Zendesk.

Avant, tout cela était réalisé à la main. C'est-à-dire que pour chaque financeur, nos équipes créaient un ticket et y intégraient le fichier Excel pour l'envoyer. Chaque début de mois nous recevions une liste de plusieurs centaines de financeurs à qui nous devions envoyer ces fichiers-là manuellement.

J'ai ainsi développé des scripts python pour permettre la génération de tickets en masse.

Désormais avec notre script Python et l'API LockSelf :

- Le fichier envoyé par notre équipe BI contenant tous les financeurs et leurs bénéficiaires est récupéré par l'API.
- Un nouveau fichier excel pour chaque financeur est créé automatiquement.
- Le script va ensuite vérifier dans LockSelf si une boîte de dépôt préexiste déjà au nom du financeur et venir si tel est le cas la supprimer (afin d'éviter que des fichiers antérieurs restent en base de données).
- La nouvelle boîte de dépôt est créée automatiquement dans LockTransfer pour chaque client.
- Le fichier correspondant est déposé dedans.
- Et un ticket est créé dans le même temps sur Zendesk, indiquant au financeur qu'il recevra un email de LockSelf lui permettant de télécharger son fichier des bénéficiaires de façon sécurisée.

Notre client peut ensuite récupérer son document et le redéposer une fois complété dans la boîte de dépôt, ce qui assure la sécurité et la traçabilité des fichiers échangés.

Une fois le fichier redéposé dans Zendesk, notre équipe chargée de la création des cartes est également notifiée via l'automatisation API et disposent de tous les éléments nécessaires à la création des nouvelles cartes par client.

Ce processus nous permet vraiment de gagner en productivité, d'assurer la conformité au RGPD et de garantir une bonne traçabilité pour le service client grâce à la création du ticket Zendesk.

La demande initiale a également été portée par les équipes DPO (Déléguées à la protection des données), pour un traitement conforme aux politiques de sécurité des données. Des fichiers Excel contenant des données personnelles ne pouvant être envoyés par email en clair.

LockTransfer est également utilisé et vraiment bien acquis par les équipes métiers sur de la gestion d'envois occasionnels.

Au sein de l'équipe nous nous servons également beaucoup de LockPass pour sécuriser l'ensemble de nos différents accès. "

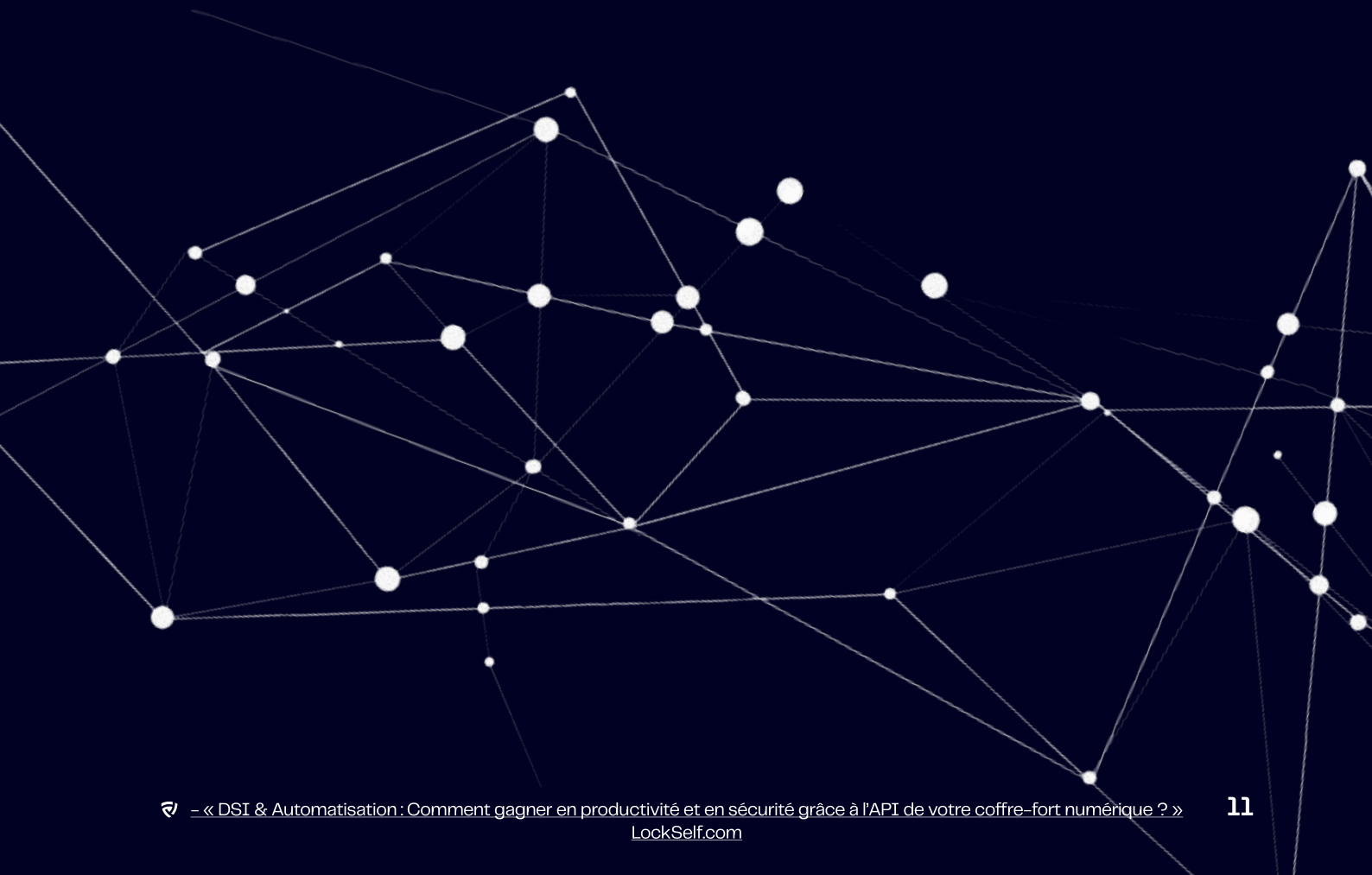
Aujourd'hui, le R.O.I est évident : cette automatisation avec **l'API LockSelf nous a permis de gagner 3 semaines de travail à temps plein chaque mois.**

Pour nous c'est un véritable succès de robotisation d'un processus manuel extrêmement chronophage.

L'outil est ainsi bien intégré à notre SI pour **faciliter le travail des collaborateurs tout en le sécurisant.**

10 cas d'usages API pour automatiser votre cybersécurité

Finis les tâches chronophages pour la DSI et place à la sécurisation automatisée des processus métiers



Top 10 des cas d'usages API pour booster votre coffre-fort LockSelf

Faites passer votre coffre-fort numérique LockSelf au niveau supérieur grâce aux automatisations via l'API et gagnez jusqu'à 3 semaines de travail à temps plein chaque mois ! Finis les tâches chronophages pour la DSI et place à la sécurisation automatisée des processus métiers.

1. Création automatisée des VM (Machines virtuelles)
2. Synchronisation des mots de passe de LockPass vers une solution VAULT
3. Transfert sécurisé de fichiers sensibles en un clic
4. Création automatisée de boîtes de dépôts
5. Duplication d'une arborescence type
6. Rotation des mots de passe d'accès serveur
7. Export global chiffré des mots de passe
8. Gérer et manager ses utilisateurs de façon automatique
9. Récupération de l'historique des logs
10. Création d'alertes sur les connexions suspectes

L'automatisation de tâches avec l'API nécessite des capacités en développement et doit être effectuée par des équipes techniques (DSI, administrateur système et réseaux, développeurs etc...).

1 Création automatisée des VM (Machines Virtuelles)

L'API LockSelf est souvent utilisée dans le cadre de la création d'un nouveau serveur ou du déploiement d'une VM (Virtual Machine), afin d'**ajouter automatiquement le mot de passe choisi pour cette nouvelle machine dans votre gestionnaire de mots de passe LockPass.**

> **" Nous utilisons également l'API LockSelf au niveau de la création de nos machines virtuelles (VM) pour venir enregistrer automatiquement l'accès à ces nouvelles machines dans LockSelf et les partager directement avec les bonnes personnes grâce à la segmentation des droits dans LockPass. "**
> – Témoignage d'un Responsable du Système d'Information en ESN.

Via l'API et grâce à un script, il est possible d'intégrer dans le déploiement automatisé de vos VM le processus suivant :

1. Génération d'un mot de passe fort, unique et répondant à la politique de mot de passe de sa catégorie grâce à l'interconnexion avec un générateur de mots de passe.
2. Changement du mot de passe par défaut de la machine par ce nouveau mot de passe généré.
3. Ajout de ce nouvel accès au sein de votre coffre-fort de mots de passe LockPass pour que celui-ci soit directement partagé aux bonnes personnes ou groupes de personnes nécessitant l'accès.

Grâce à ce premier cas d'usage, **vos serveurs et VM sont déployés et sécurisés en autonomie.**

En plus d'offrir **un vrai gain de temps,** cela vous permet de **gagner en sécurité** en évitant que le mot de passe de la machine ne transite par un autre appareil et qu'un mot de passe par défaut et utilisé sur différentes machines soit adopté.

Ce cas d'usage offre un **gain de sécurité sur la complexité, l'unicité et le stockage sécurisé des mots de passe** lors du déploiement des serveurs et VM.

2

Synchronisation des mots de passe de LockPass vers une solution VAULT

Certains de nos clients se servent également de ces possibilités d'automatisation pour **venir alimenter leur Vault.** Grâce à l'API, ils vont créer une synchronisation automatique qui va prendre les secrets présents dans **LockSelf, leur source de vérité,** pour l'intégrer également dans leur **outil Vault, dédié aux robots.** Cela facilite ensuite l'utilisation en automatique de ces mots de passe pour les machines, notamment grâce à la compatibilité du Vault avec la solution d'automatisation ANSIBLE.

Cette interconnexion entre LockSelf et une solution Vault permet également de pouvoir **automatiser d'autres processus** par la suite. Par exemple, lorsqu'une **mise à jour sur un grand nombre de serveurs** doit être faite, cela permet de se connecter en seulement quelques clics à l'ensemble des machines, via un outil tiers pour récupérer les mots de passe de connexion dans le Vault, qui aura préalablement récupéré les mots de passe dans LockSelf.

Ce cas d'usage permet de **faciliter l'utilisation à grande échelle des mots de passe serveurs** tout en conservant votre coffre-fort **LockPass comme source de vérité pour la gestion des accès.**

3

Transfert sécurisé de fichiers sensibles en un clic

Prenons un cas d'usage concret : Votre COMEX signe un contrat sous NDA (accord de non-divulgation) avec un nouveau partenaire. Grâce à l'API, vous pouvez **automatiser l'envoi du contrat,** une fois signé, via votre outil de transfert sécurisé LockTransfer. Le document sera **envoyé par un canal chiffré** à votre destinataire qui le recevra par email ou via un espace dédié (boîte de dépôt LockTransfer) selon votre choix.

Le transfert ne se fait ainsi plus en clair mais via un **outil sécurisé, validé par la DSI.** Vous limitez ainsi le risque qu'ils utilisent des outils tiers non-sécurisés pour transférer ces données (**Shadow IT**).

Ce cas d'usage peut s'appliquer à tous les services **traitant des données à caractère sensible** au sein de votre organisation.

Par exemple, en intégrant l'API LockSelf avec les processus métiers du service juridique, vous êtes en mesure de leur simplifier l'envoi de documents sensibles mais aussi de les sécuriser.

4 Création automatisée de boîtes de dépôts

L'API LockSelf vous permet également d'automatiser la création de boîtes de dépôts, pour **réceptionner de façon sécurisée des documents sensibles.**

Prenons l'exemple de votre équipe RH (Ressources Humaines), qui a besoin de récupérer des documents sensibles dans le cadre d'une embauche (pièce d'identité, contrat de travail...). Avec **l'API de votre coffre-fort LockSelf** il est possible de simplifier le processus de récupération de ces éléments **en automatisant la création de boîtes de dépôts** directement depuis votre CRM interne.
Il suffit de créer au sein de votre CRM un bouton "Créer une boîte de dépôt".

Dans votre script il faudra inscrire les éléments à récupérer :

- Nom de la boîte de dépôt (par exemple "Récupération documents pour l'embauche de Monsieur X"),
- Descriptif des documents à fournir,
- Adresse mail d'envoi de la boîte de dépôt,
- Date d'expiration,
- Date d'archivage,
- Droits d'accès.

5 Duplication d'une arborescence type

Dans le cadre de missions d'infogérance, la duplication d'une arborescence type de façon automatique est souvent très utile.

Par exemple, nos clients travaillant en ESN sont amenés à gérer plusieurs mots de passe pour leurs clients (infogérance); via un script adapté aux usages internes et faisant appel à l'API LockSelf ils vont pourvoir, à chaque signature d'un nouveau client, **automatiser la création d'une catégorie dans LockPass, reprenant l'arborescence type** à respecter selon leurs process.

Votre RH aura simplement à cliquer sur le bouton dans son CRM et une boîte de dépôt dédiée à votre nouvelle recrue sera automatiquement créée et envoyée à la bonne personne, lui demandant les éléments à joindre et **garantissant le cloisonnement et la date d'expiration des données récoltées selon les pré-requis légaux** et garantis par ce processus déployé par la DSI.

Cela offre une **traçabilité** à l'entreprise quant au **traitement des données personnelles**, permet d'en garantir la **sécurité** et la **conformité** aux règles étatiques (**RGPD**) et fait **gagner un temps considérable** aux équipes métiers qui n'ont plus besoin de réaliser l'ensemble de ces actions à la main.

6

Rotation des mots de passe d'accès serveur

Ce cas d'usage réel et très concret s'adresse plutôt à des profils spécialisés en systèmes et réseaux.
En effet, à l'aide d'un script appelant l'API LockSelf il est possible de modifier le mot de passe d'un serveur ou service pour ensuite venir le remplacer automatiquement dans LockPass.

En ajoutant une logique de répétition automatisée à ce script, celui-ci vous permet de mettre en place une **rotation des mots de passe de vos serveurs** sans avoir à y penser !

Bonus : Avec la nouvelle fonctionnalité d'historisation des mots de passe dans LockPass la version précédemment utilisée pour se connecter à la machine sera automatiquement gardée en mémoire !

7

Export global chiffré des mots de passe

En cybersécurité, le principe de **sauvegarde externalisée** est essentiel et les mots de passe n'échappent pas à cette règle.
Cependant, programmer chaque semaine ou chaque mois des exports de tous vos mots de passe sur un support externe sécurisé peut très vite s'avérer chronophage.

Afin de conserver toujours une copie sécurisée et à jour de leurs secrets certains de nos clients ont choisi d'utiliser l'API. Ainsi, tous les mois et de façon automatique, un export global de tous leurs mots de passe est **exécuté de façon chiffrée vers un support sécurisé.**

Dans le cadre du PRA (**Plan de Reprise d'Activité**), cela leur permet de garantir l'accès à leurs mots de passe, même en cas d'impossibilité d'accéder à LockSelf sur leurs machines.

Les cas d'usages suivants sont également réalisables via l'API, cependant des fonctionnalités optionnelles natives sont également disponibles permettant de faciliter leur mise en œuvre ! 👇

8 Gérer et manager ses utilisateurs de façon automatique

Onboarder un nouvel utilisateur sur LockSelf et manager ses droits d'accès aux différentes ressources (fichiers, transferts, mots de passe) peut se faire automatiquement via l'API.

Pour cela, il faudra par exemple indiquer dans votre script :

- Si Monsieur ou Madame X appartient à tel service, alors lui donner accès à tel et tel groupe dans LockSelf.
- Ou encore, demander au script de valider automatiquement chaque jour que les droits des utilisateurs sont conformes à la politique interne en allant interroger via l'API les rapports de droits dans LockSelf.
- Etc...

Ainsi, **la gestion des droits d'accès de l'ensemble de vos utilisateurs est automatisée** et vos nouveaux collaborateurs ont **automatiquement accès aux bons mots de passe et ressources**, facilitant leur onboarding.

Si vous disposez d'un annuaire d'entreprise (Active Directory ou autre) vous pouvez également opter pour une réplication de vos groupes AD dans LockSelf très facilement via notre option dédiée d'interconnexion AD. Une autre option permettant une connexion en SSO à LockSelf à l'ensemble de vos utilisateurs est également disponible en option.

9

Récupération de l'historique des logs

Saviez-vous que LockSelf vous permet en tant qu'administrateur de la solution de récupérer l'historique de l'ensemble des actions effectuées sur votre coffre-fort numérique ? Ces logs sont consultables dans l'onglet dashboard de votre interface LockSelf.

Via l'API ou avec notre option syslog (format de sortie .json) vous pouvez également faire le choix d'exporter ces logs en continu ou de façon régulière afin de pouvoir par la suite les assimiler et les traiter.

Cette **historisation des logs** offre une véritable **traçabilité de l'ensemble des actions effectuées** (quel mot de passe à été utilisé, quand, par quel user API etc...).

Ces logs peuvent aussi être exportés pour être intégrés dans un SIEM.

10

Création d'alertes sur les connexions suspectes

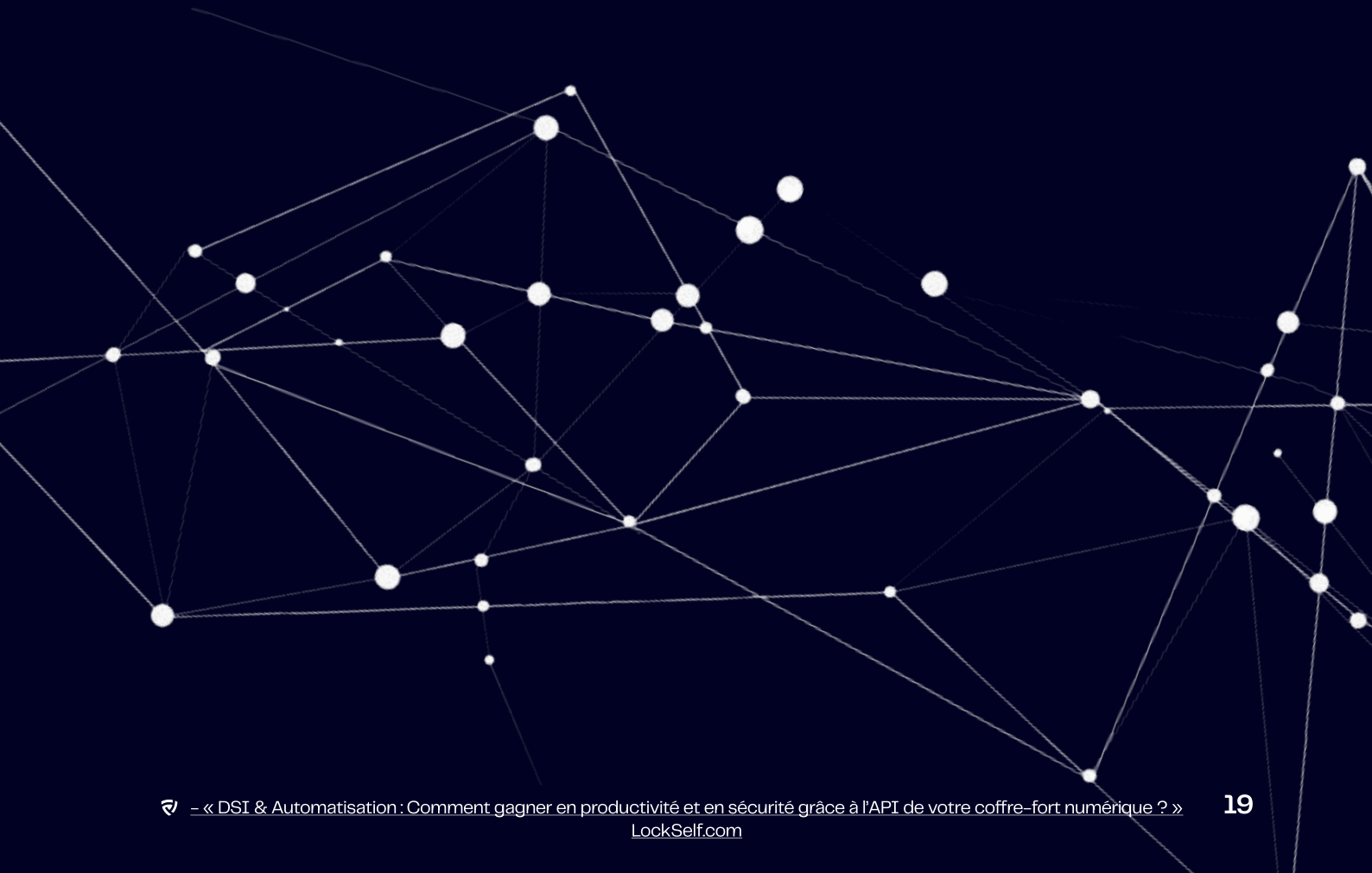
L'API LockSelf peut également vous servir à **automatiser des alertes** sur des actions bien précises que vous souhaitez surveiller. Vous pouvez par exemple choisir d'être informé en cas d'un nombre de tentatives élevées de connexion à un compte sur un court laps de temps ou encore sur des horaires inhabituels d'activités.

L'API vous offre l'avantage de réaliser tout type d'action de façon très modulable pour s'adapter à tous les besoins de vos équipes techniques et métiers.

Notre API suit également l'évolution de nos produits et est en constante évolution. Ainsi pour toute nouvelle fonctionnalité déployée sur LockSelf, l'API offrira de **nouvelles possibilités d'automatisation !**

Unifier les processus de cybersécurité grâce l'API

Retour d'expérience de Sylvain Nohannic, DSI chez THALOS.



“ Nous utilisons l’API LockSelf pour inscrire automatiquement chaque nouveau navire sur notre solution anti-spams.”

Sylvain Nohannic
DSI chez THALOS

Retour d’expérience

Bonjour Sylvain, pouvez-vous nous présenter votre métier et l’organisation dans laquelle vous travaillez ?

Chez THALOS nous sommes **créateur de solutions digitales pour le monde maritime** depuis plus de 25 ans. Nous sommes une soixantaine de collaborateurs répartis sur 3 sites, avec notre siège en France, une filiale à l’île Maurice et une autre à Taïwan.

Notre cœur de métier c’est de **gérer et sécuriser la connectivité satellitaire entre des navires et la terre** et vice-versa, pour répondre à de multiples besoins avec notre solution « OceanBox ».

Nous nous occupons de la configuration et du déploiement de nos solutions aussi bien à bord des bateaux que sur les chantiers navals partout dans le monde. Nous installons les antennes, toute la partie connectique, gérons l’informatique embarquée et les réseaux à bord, la mise en place de firewall applicatifs de niveau 4, jusqu’à la proposition de forfaits de communication entre la terre et la mer et nous gérons également toute la partie optimisation, sécurité et compression de flux et des informations.

Aujourd’hui **nous équipons près d’un millier de navires dans le monde** avec nos solutions.

Au-delà de notre casquette connectivité, nous sommes **développeurs de solutions pour améliorer l'efficacité opérationnelle des navires** avec notre système de supervision électronique des opérations « OceanLive ». Cette solution collecte, exploite et analyse des données de bord (notamment des vidéos) qui sont transmises chaque jour à l'armement pour la gestion des opérations de pêche.

Nous développons également une solution d'aide à la pêche : le logiciel « CATSAT » déployé à bord. Tous les matins nous récupérons auprès de notre partenaire CLS , des données satellitaires et des cartographies de l'ensemble du globe. Ces données permettent de comprendre la dynamique des océans avec des informations comme la température de l'eau, le courant, la salinité, l'évolution du plancton etc... Cela permet ensuite à nos clients de cibler des zones de pêche favorables.

Aujourd'hui je suis **DSI chez THALOS.** J'ai notamment en charge le département IT, pour lequel nous nous occupons de l'ensemble de l'infrastructure informatique avec la gestion de nos deux data centers en propre, ainsi que le déploiement en cours d'une solution chez Google Cloud Platform. La mise en place de cette nouvelle solution d'hébergement dans le cloud intervient pour répondre à un besoin stratégique : celui de pouvoir déployer une partie de nos solutions de connectivité au plus proche des zones d'opérations de nos clients (avec des données géographiquement localisées dans le cloud).

Aujourd'hui un bateau en Chine passe par notre data center en France pour se connecter au reste du monde. Nous avions ainsi des problématiques de latence. Bientôt ce bateau se connectera directement à un point de présence THALOS en Chine dans le cloud. Cela nous permet également de rendre notre site en France moins critique en cas de problématique technique.

Nous gérons également l'administration des systèmes et la sécurité de l'entité THALOS, que ce soit au niveau cyber, gestion des accès, serveurs etc...

Enfin, nous allons de plus en plus vers une offre de prestation de services de sécurité à l'intérieur de certains navires pour nos clients, pour lesquels nous allons déployer de l'antivirus ou de l'EDR à leur demande.

En termes de cybersécurité, y a-t-il des spécificités liées au secteur maritime ? Lesquelles sont-elles ?

Le secteur maritime à de grosses spécificités en termes de cybersécurité avec la **gestion des communications** d'une part, et le public d'autre part (les pêcheurs n'étant pas des profils informatiques de formation).

C'est dans cette optique que **THALOS a intégré il y a 3 ans maintenant l'association France Cyber Maritime**, créée en partenariat avec l'ANSSI et d'anciens membres des renseignements de la marine.

Cette association basée à Brest a permis de créer une taskforce avec un collège d'utilisateurs et un collège de solutions orientées pour le milieu maritime. THALOS y est adhérent dans le collègue solutions de par les offres de connectivité et de sécurité que nous proposons à bord des navires.

Le Maritime CERT à Brest, en collaboration avec l'association France Cyber Maritime, vont également pouvoir, en cas d'attaque, mettre en relation les entités ciblées avec les bons prestataires pour **apporter rapidement des solutions sur des problématiques qui sont spécifiques au domaine maritime.**

Vous avez fait le choix de mettre en place notre gestionnaire de mots de passe LockPass. Avant son déploiement, comment gériez-vous les mots de passe en interne ?

Avant le déploiement de LockPass **nous étions sur KeePass** (voire pour certains collaborateurs sur des fichiers Excel) et chaque service avait son propre fichier. **Il n'y avait pas de centralisation.**

Nos techniciens, chargés d'installer nos solutions sur les navires, utilisaient par exemple une base KeePass protégée par un simple mot de passe.

En prenant en compte le nombre d'équipements et de ressources par navire cela représentait une base de mots de passe conséquente. À tel point que nous avons constaté des dérives, telles que l'utilisation d'un même mot de passe pour des équipements identiques sur des navires différents.

Il nous fallait **mettre en place un outil permettant de centraliser et de gérer finement les droits d'accès à chaque mot de passe.**

Après avoir fait un benchmark des solutions existantes, nous avons shortlisté LockPass et Bitwarden. Le choix s'est porté sur LockPass du fait que la solution soit française et certifiée par l'ANSSI. À fonctionnalités équivalentes, cela a vraiment fait la différence.

Le fait d'avoir proposé l'outil **LockPass nous a permis de réimplanter facilement et rapidement les bonnes pratiques** en termes de gestion des différents accès : **mots de passe uniques et robustes.**

Nous avons fait le choix de prendre la solution **LockSelf en On-premises** pour pouvoir gérer nous-même la sécurité de nos données. C'est dans notre culture d'entreprise chez THALOS de privilégier l'hébergement en interne lorsque cela est possible.

Avec LockPass nous avons voulu fournir une solution fonctionnelle et unique pour gérer les mots de passe de l'entreprise.

C'est aussi **moins pénible qu'un client lourd, en termes de gestion, d'administration et de mise à jour des postes utilisateurs**, avec un réel danger au niveau de la sécurité en cas de vol d'une machine.

Aujourd'hui l'intégralité de nos collaborateurs utilisent LockPass au quotidien !

Comment êtes-vous organisé dans l'outil ?

Nous avons opté pour **une arborescence par métier** (commerce, IT, technique etc...), **avec des sous-arborescences par projet.**

Si je prends par exemple l'équipe technique chez THALOS qui gère de nombreux navires, ils vont avoir une branche par armateur, par bateau et des déclinaisons spécifiques pour chaque bateau.

Lorsque nous avons un nouveau navire qui rejoint notre base de données, **nous utilisons également l'API pour dupliquer l'arborescence dans LockPass afin de gagner du temps et de ne pas recréer chaque catégorie à la main.** Nous avons créé ce template d'arborescence à l'aide d'un script qui relie un outil que nous avons en interne avec LockSelf via l'API.

Nous utilisons également l'API pour inscrire automatiquement chaque nouveau navire sur notre solution anti-spams grâce aux noms de domaines que nous rentrons dans LockSelf.

Vous avez fait le choix de prendre l'accès à l'API LockSelf.

Pouvez-vous nous détailler vos cas d'usages ?

Nous avions une problématique propre à notre secteur, liée au fait que nos techniciens partent souvent à l'étranger parfois sans accès à Internet pendant plusieurs jours. Sur ces missions, ils ont **besoin de pouvoir récupérer les bons accès aux outils, même hors ligne.**

Dans 95% des cas, nos techniciens ont de la connectivité sur les navires sur lesquels ils partent en mission et utilisent l'application web de LockSelf. Dans moins de 5% des cas, ils ont la nécessité d'accéder à leurs mots de passe sans connexion. C'est un besoin limité mais auquel nous devions répondre avec notre outil de gestion des mots de passe.

Lorsque nos techniciens vont installer des switch, des modems, des firewalls etc... sur des bateaux, ils ont besoin d'avoir accès à ce qui a été défini au préalable comme étant les mots de passe de ces équipements. Mais sans connectivité à bord du bateau ils n'auront pas la possibilité d'accéder à LockSelf.

La vraie difficulté pour nos techniciens ce n'est pas tant d'accéder à leurs mots de passe en mer (puisqu'ils disposent d'une connexion internet et de dispositifs de communication), mais plutôt sur terre lors de la construction des navires sur les chantiers navals. Quand ils interviennent dans ce cadre, ils vont travailler **sur des bateaux sur lesquels les communications satellites ne sont pas encore installées !**

LockSelf répondait vraiment à tous nos besoins, nous avions simplement besoin de venir **répondre à cette contrainte opérationnelle en attendant que la fonctionnalité soit développée en natif.**

Aujourd'hui pour pallier à cela nous avons fait le choix de conserver **KeePass comme outil de backup.** Mais pour que ce palliatif fonctionne correctement il est nécessaire que la base KeePass soit systématiquement à jour.

Ainsi, nous avons fait le choix d'**automatiser l'ensemble du processus grâce à l'API de LockSelf.**

Tous les matins :

- Nous faisons un export de notre base LockSelf complète via l'API,
- Nous la déchiffrons par la suite avec le bon certificat
- Nous requêtons suite à cela uniquement la branche qui concerne le technicien qui doit partir en mission et qui a besoin de ses accès offline pendant celle-ci.
- Nous allons ensuite rendre cet export compatible au format KeePass
- Rechiffrer le CSV
- Et le déposer dans l'architecture NAS du technicien.

Le tout via un script automatisé.

Nos techniciens ont ainsi un export quotidien de leurs mots de passe à jour qui est fait. Cela permet à ceux qui doivent partir en déplacement de prendre le dernier fichier en date, de le décompresser en local sur leur machine et de l'intégrer à un KeePass.

Bien sûr, une fois qu'il n'a plus besoin de l'export et qu'ils reviennent de mission, les techniciens suppriment cette base KeePass.

C'est le processus que nous avons mis en place afin de permettre à nos techniciens d'**accéder, le temps de leur mission offline, aux mots de passe strictement nécessaires à celle-ci.**

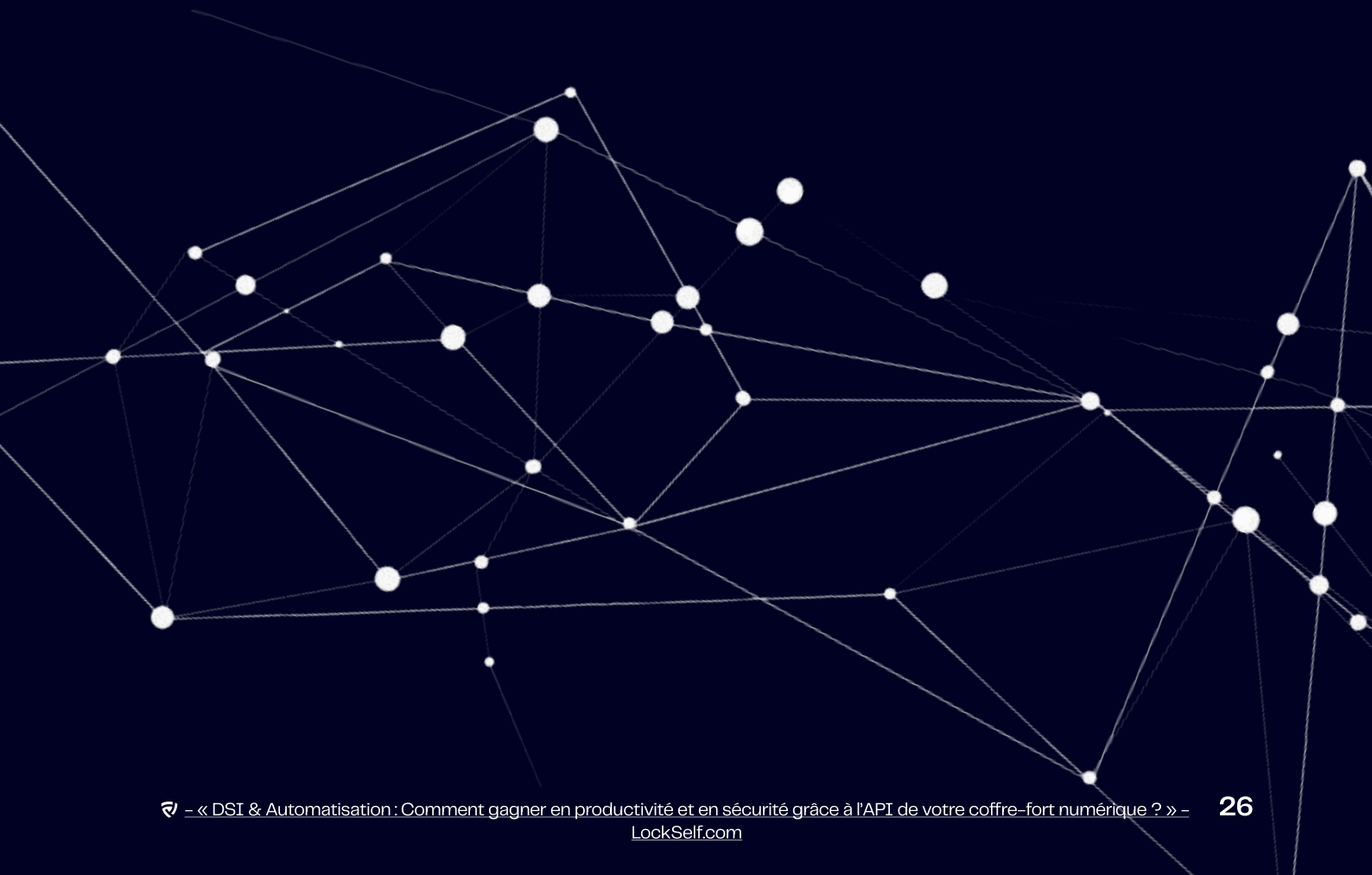
Nous sommes également **en train de mettre en place une solution de supervision unifiée** avec différents outils que nous utilisons.

Notre objectif est de nous **créer un tableau de bord multi-produits,** nous permettant notamment de remonter les nombreuses données de notre outil de test de vulnérabilités Qualys, ainsi que celle de notre EDR, de notre anti-virus et évidemment de LockSelf.

Nous sommes ainsi en train de voir ce que les API de nos différents outils nous permettent de récupérer comme informations, de façon à centraliser certaines métriques. L'usage de l'API LockSelf va donc prendre tout son sens avec ce projet, en nous permettant notamment de **remonter les logs et de créer des alertes.**

L’automatisation comme levier de sécurisation des accès

Retour d’expérience de Martin Bonneau, Administrateur Systèmes chez DARVA.



“L’automatisation grâce à l'API est un véritable levier de sécurisation pour la gestion et le stockage des mots de passe.”

Martin Bonneau
Administrateur Systèmes chez DARVA

Retour d’expérience

Bonjour Martin, pouvez-vous nous présenter votre métier et l’organisation dans laquelle vous travaillez ?

DARVA est un éditeur au service de l’assurance.

Nous concevons et développons des plateformes collaboratives et des outils d’échange à forte dimension technologique pour relier les assureurs et leurs partenaires (experts, réparateurs, assisteurs...). Acteur incontournable dans la chaîne de la gestion des sinistres en France, nous traitons chaque année plus de 8 millions de dossiers sinistres.

Nous proposons également des solutions pour la résiliation des contrats d’assurance, la facturation électronique ou encore pour l’hébergement de données.

DARVA compte aujourd’hui près de 200 collaborateurs sur son site proche de Niort (Chauray).

Nous sommes à ce jour **une cinquantaine de collaborateurs au sein de la DSI**, divisés en plusieurs pôles : Infrastructure, Réseaux, Bureautique, Exploitation, Assistance, Architecture et Sécurité.

Je suis pour ma part Administrateur Systèmes au sein de l'équipe infrastructure. Nous gérons le commissionnement des serveurs, la virtualisation, et autres actions en lien avec l'infrastructure du data center.

Nous sommes **responsables de la mise en place des outils et des infrastructures physiques et virtuelles.**

Vous avez fait le choix de mettre en place notre gestionnaire de mots de passe LockPass.

Avant son déploiement, comment gériez-vous les mots de passe en interne ?

Avant de commissionner LockPass nous avions KeePass comme solution "officielle" en place.

Chaque collaborateur pouvait avoir sa propre base et en fonction de ses missions, avoir accès à des bases KeePass partagées. **La segmentation et la traçabilité n'était pas optimale en l'état.**

Vis-à-vis des contraintes de sécurité qui sont les nôtres cela n'était pas suffisant. Notre suivi des accès n'était pas satisfaisant selon nos critères de sécurité.

À l'époque, nous n'avions pas l'obligation de mettre en place **une solution comme LockPass** mais cela nous a permis de **nous mettre en conformité** en avance de phase. Une gestion professionnelle des accès à tous les niveaux étant un véritable **pré-requis de sécurité aujourd'hui.**

Décommissionner KeePass pour déployer LockPass nous a permis deux choses :

1. **Segmenter les accès** et voir très rapidement qui a accès à quoi, quels mots de passe ont été utilisés etc...

2. **Sécuriser et piloter la gestion des accès à l'échelle de toute l'organisation.**

Aujourd'hui, la mise en place de LockPass vient répondre à ce besoin de **centralisation des mots de passe,** de **segmentation des droits,** de **traçabilité sur l'utilisation des accès** et une nécessité réglementaire, liée à notre métier, de **conserver l'intégralité de nos secrets en interne** sur nos data centers.

Lors de la mise en place de LockPass nous avons décidé de **migrer l'ensemble des collaborateurs de la société sur cette solution.** Certaines équipes métiers ont été au départ un peu réfractaires, mais une fois les premiers mots de passe et utilisateurs onboardés dans la solution il y eut un véritable effet « boule de neige » et l'adoption s'est faite rapidement.

Nous avons dans un premier temps fait un test de l'outil sur l'équipe production et support client afin de valider la **simplicité d'utilisation et de migration de l'existant.** Ayant réussi à migrer simplement nos quelques milliers de mots de passe, nous avons ensuite poussé la solution auprès de l'ensemble des équipes DARVA.

Afin de faciliter le déploiement et l'adoption **nous avons intégré LockPass sur l'ensemble des postes de nos collaborateurs via GPO.** Nous avons ensuite formé tout le monde à l'utilisation de l'outil grâce aux **formations dispensées par les équipes LockSelf.** Enfin, nous avons bloqué la possibilité de pouvoir enregistrer les mots de passe sur les navigateurs ou dans toute autre extension afin qu'il ne soit possible d'enregistrer ses mots de passe que dans LockPass.

Désormais LockPass est déployé sur l'ensemble de nos collaborateurs et prestataires en missions longues, ce qui correspond à plusieurs centaines de personnes.

La certification de LockPass par l'ANSSI est un **vecteur de facilitation dans le cadre des audits** et obligations auxquels nous sommes contraints.

Côté organisation nous avons créé **une catégorie et un groupe par service** permettant de **responsabiliser les équipes au partage au moindre privilège de leurs secrets.**

Vous avez fait le choix de prendre l'accès à l'API LockSelf. Pouvez-vous nous détailler vos cas d'usages ?

Aujourd'hui nous utilisons l'API dans deux cas d'usages :

1. En premier lieu **pour créer des machines virtuelles (VM).** Ce qui facilite l'automatisation de déploiement.

   Cette automatisation grâce à l'API est un véritable levier de sécurisation pour la gestion et le stockage des mots de passe.

2. En second lieu pour **créer des bases de données de façon automatisée.**

   Nous sommes en cours de déploiement sur ce cas d'usage. Cela va nous permettre, lorsqu'une base de données est créée, déployée ou que de nouveaux utilisateurs sont créés, de venir **automatiser le processus dans son ensemble et notamment la création des mots de passe associés.**

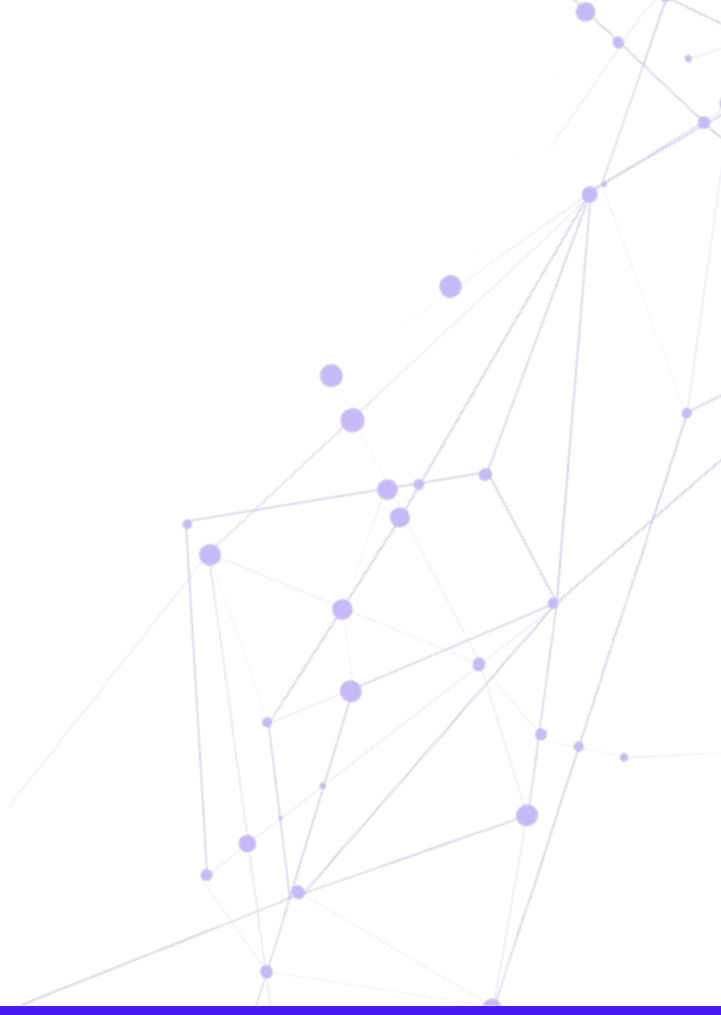
Vous êtes fervent utilisateur du Dashboard LockSelf. Comment l'utilisez-vous ?

Le Dashboard nous offre **des données intéressantes et pertinentes** grâce à **un vrai travail UI / UX** et une **gestion des logs optimisée.**

L'une des données vraiment intéressante pour nous c'est le fait de pouvoir **identifier les utilisateurs inactifs.** Par définition, ce sont des collaborateurs qui n'utilisent pas LockSelf, et qui n'ont, de fait, pas une gestion conforme de leurs mots de passe, vis-à-vis de notre politique interne.

Nous attendons avec impatience l'API du Dashboard sur laquelle travaillent les équipes LockSelf ! Nous aimerions extraire les informations du Dashboard, notamment sur la force des mots de passe, afin de pouvoir mener des campagnes de sensibilisation et **proposer le renforcement des mots de passe faibles** auprès des collaborateurs concernés.

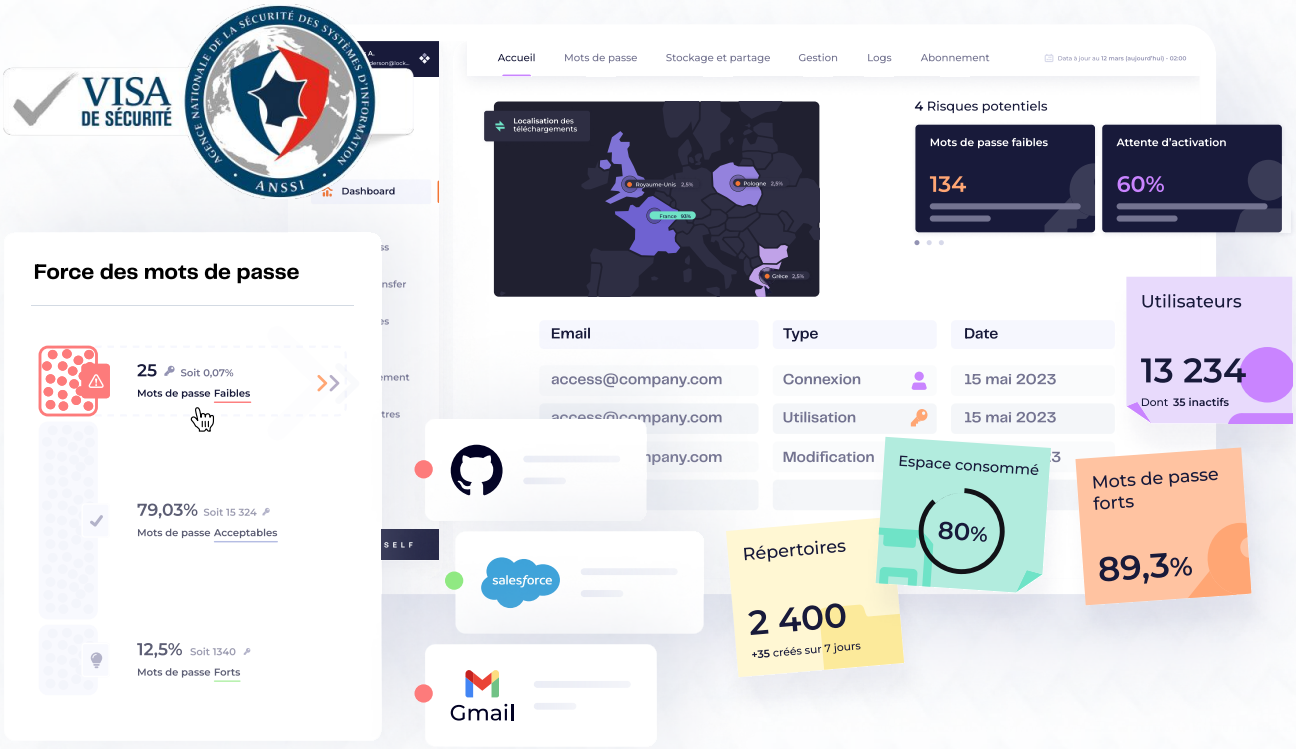
L'historisation des logs dans LockSelf nous permet également de savoir très rapidement si un mot de passe est corrompu, ou bien qui l'utilise et de conforter les auditeurs dans nos démarches de sécurisation et de gestion des accès.



Aujourd'hui, la mise en place de LockPass vient répondre à ce besoin de **centralisation des mots de passe,** de **segmentation des droits**, de **traçabilité sur l'utilisation des accès** et une nécessité réglementaire, liée à notre métier, de **conserver l'intégralité de nos secrets en interne** sur nos data centers.

LOCKSELF

Transfert et stockage sécurisé de fichiers
Gestionnaire centralisé de mots de passe
Certifié par l'ANSSI



Essayez gratuitement

100% Français
Dédié aux entreprises
et aux collectivités

- « DSI & Automatisation : Comment gagner en productivité et en sécurité grâce à l'API de votre coffre-fort numérique ? »
LockSelf.com

LOCKSELF

Gestionnaire de mots de passe – Transfert & stockage sécurisé de fichiers

LockSelf.com