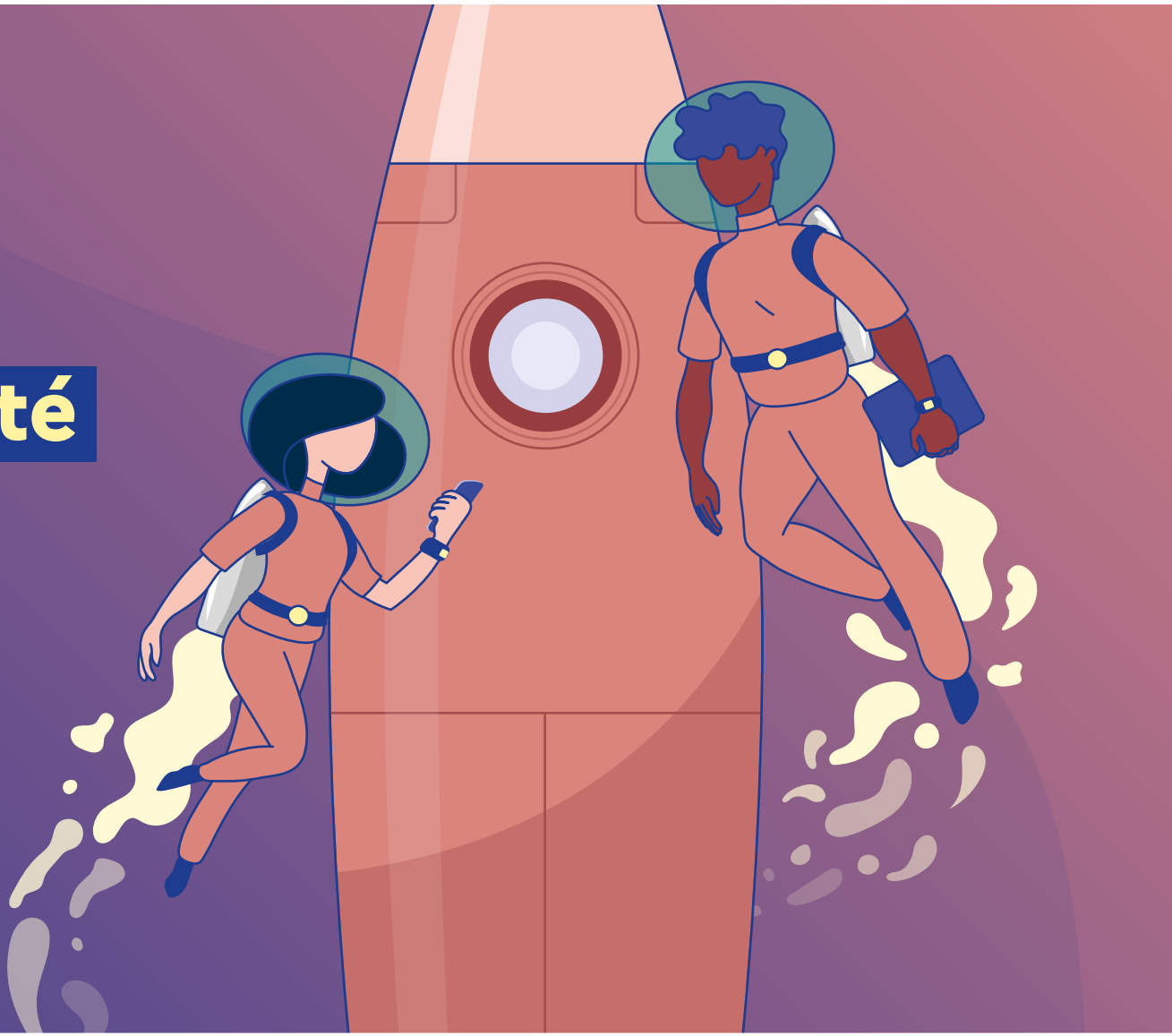
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Guide de cybersécurité

à l'usage des start-up du numérique



LA FRENCH TECH

↘ Notes

Ce guide propose des pistes d'action utiles à l'ensemble des acteurs du numérique. Toutefois, il traite en particulier des start-up développant un produit logiciel, et non de celles se focalisant sur la prestation de services intellectuels. En outre, les start-up opérant dans le secteur de la Défense ou manipulant des informations classifiées sont assujetties à des règles particulières, non couvertes par ce document.

Une start-up est une jeune entreprise innovante qui développe une solution technologique pour créer de nouveaux usages, services ou produits, avec une ambition de forte croissance. Il s'agit donc généralement d'une TPE nouvellement créée, dont l'activité n'est pas encore stabilisée. Spécifiquement, **une start-up du numérique** propose des biens ou services en lien avec les technologies de l'information et de la communication (TIC), quels que soient les secteurs d'activité.

édito

par

Julie Huguet

Directrice de la Mission French Tech

et

Vincent Strubel

Directeur général de l'ANSSI

La rapidité est au cœur de la dynamique des start-up. Innover, tester et s'adapter en permanence est une nécessité. Dans ce contexte, la cybersécurité est parfois reléguée au second plan, alors que la donnée est devenue une ressource stratégique et la résilience un impératif. **Une faille n'est jamais anodine :** elle peut affecter la confiance et remettre en cause le développement de l'entreprise.

Le panorama de la cybermenace de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)[5] souligne que les petites ou jeunes entreprises constituent la catégorie d'entités la plus affectée par les compromissions par rançongiciel.

Dans un contexte où le passage à l'échelle entraîne l'augmentation de la surface d'exposition, **intégrer la cybersécurité sans freiner l'agilité devient un levier de compétitivité.**

Ce guide marque **la convergence des missions de l'ANSSI et de la Mission French Tech,** et permet de sensibiliser l'écosystème des start-up à la nécessité de **considérer la cybersécurité comme un pilier stratégique, et d'ancrer la confiance au cœur de leur développement.**

Il est conçu pour les jeunes entreprises technologiques, souvent caractérisées par des équipes restreintes, des moyens limités et des compétences encore en développement en matière de sécurité numérique.

En préambule, une frise illustre le parcours type d'une start-up du numérique. **Treize enjeux de sécurité** y sont mis en évidence, rattachés à des étapes-clés de la vie de l'entreprise. Chacun d'eux fait ensuite l'objet d'une fiche pratique, offrant une présentation synthétique des risques et proposant des mesures adaptées.

À l'heure de la course mondiale à l'innovation technologique, la French Tech et l'ANSSI se réjouissent d'unir leurs forces pour aider les start-up et scale-up à **se prémunir durablement contre les menaces numériques.**

Les atteintes numériques ont progressé de 74% en cinq ans, et on compte plus de **17 100 cas** affectant les systèmes d'information sur l'année 2024[1].

Pour ce qui relève de son périmètre, l'ANSSI a traité **4386 évènements de sécurité** en 2024, dont **1361 incidents,** ce qui représente **une hausse de 18%** par rapport à l'année précédente[2].

Les cyberattaques ne sont plus réservées à des organismes ou des secteurs sensibles mais concernent un nombre croissant de victimes potentielles[3], avec une multiplicité croissante des outils et infrastructures utilisés[4].

1 Rapport annuel sur la cybercriminalité 2025, COMCYBER-MI, Ministère de l'Intérieur : les « atteintes aux systèmes d'information » font référence aux atteintes aux systèmes de traitement automatisé de données (ASTAD) qui regroupent 56 Natures d'Infractions (NATINF) consultables à ce lien. Cette notion englobe majoritairement des cyberattaques mais ne se restreint pas à celles-ci.

2 Rapport d'activité 2024 de l'ANSSI : les incidents sont les événements de sécurité pour lesquels l'ANSSI confirme qu'un acteur malveillant a conduit des actions avec succès sur le système d'information de la victime.

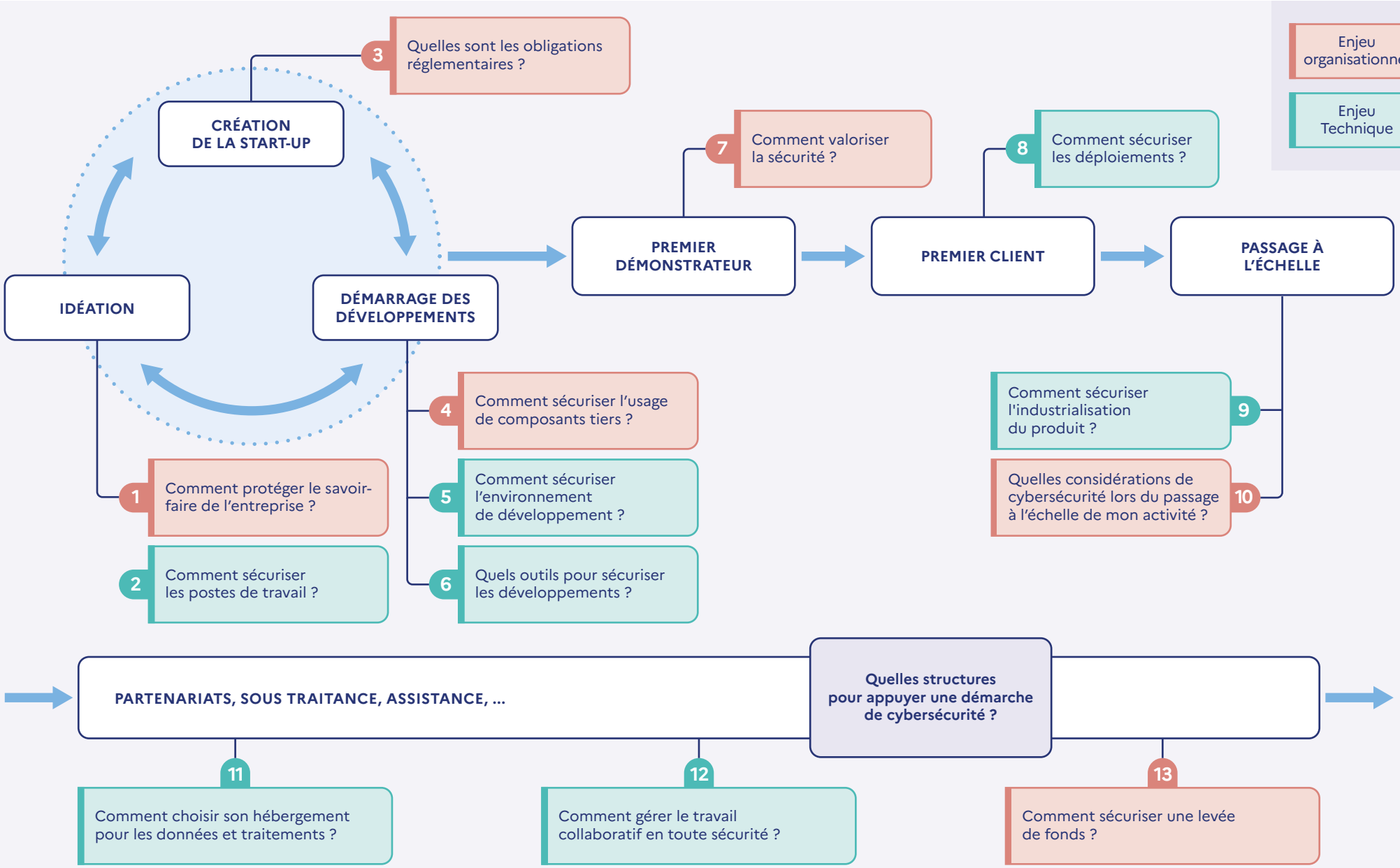
3 Threat landscape report 2024, CERT-EU

4 Panorama de la cybermenace 2024, ANSSI

5 Panorama de la cybermenace 2024, ANSSI

Cycle de vie d'une start-up : des premiers souffles à l'âge de raison

Tour d'horizon des bonnes pratiques de cybersécurité, aux différents stades de maturité d'une start-up

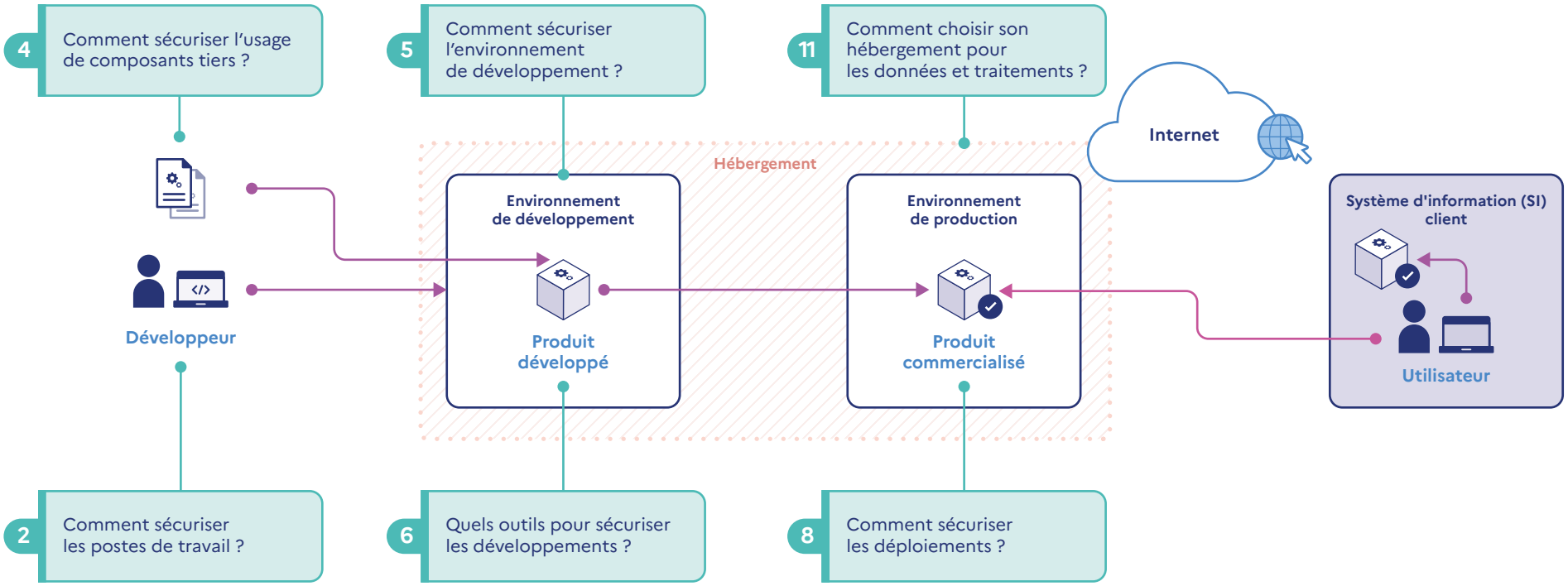


La frise chronologique présentée met en lumière les principales étapes d'un projet de start-up. Elle ne constitue pas une recommandation et ne prétend pas refléter exhaustivement la diversité des réalités des start-up du numérique.

Les trois étapes que sont l'idéation, la création de l'entité juridique et le lancement des développements ne sont pas présentées dans un ordre chronologique précis, celui-ci pouvant varier selon les contextes.

La gestion de la sous-traitance et des partenariats est, quant à elle, représentée de manière transverse, tout au long du cycle de vie de l'entité.

Focus sur les enjeux techniques mentionnés dans la frise chronologique, à la lumière du cycle de vie du produit :



Les enjeux techniques ci-dessus sont particulièrement pertinents pour développer une offre de services chez les incubateurs ou les accélérateurs de start-up, par la mise à disposition d'outils ou de plateformes permettant de répondre aux exigences des fiches.

1

Comment protéger le savoir-faire de l'entreprise ?

DESCRIPTION

Il est primordial d'identifier et de protéger l'ensemble des informations qui représentent une valeur pour l'entreprise, dès la phase d'idéation. Ces informations peuvent être regroupées en 3 grandes familles :

→ Données commerciales, financières et RH : business plan, levées de fonds, prospects, contrats, partenariats.

→ Données techniques : architectures logicielles, configurations, code source produit, documentation.

→ Données des clients : données de production alimentant le produit, journaux d'évènements, alertes.

Il est important d'estimer la criticité, la sensibilité de chaque donnée en se posant la question : « *Quelles seraient les conséquences d'une perte, d'une indisponibilité, d'une fuite ou d'une modification malveillante de cette donnée et quel serait l'impact pour l'entreprise ou ses clients ?* ».
Par exemple, les aspects différenciants ou novateurs de l'entreprise peuvent être considérés comme des éléments critiques à protéger en priorité.

L'objectif consiste ainsi à protéger en confidentialité ces informations (seules les personnes légitimes y ont accès) mais également en disponibilité (elles sont accessibles sans difficultés) et en intégrité (elles sont préservées de toute modification illégitime).

PRINCIPAUX RISQUES

→ Fuite du code source du produit, de la base clients/prospects, de la stratégie commerciale

→ Espionnage industriel

→ Perte de données à la suite d'un incident (entraînant : arrêt de l'activité, faillite, risque juridique)

→ Atteinte à la réputation de l'entreprise (diffusion d'informations sensibles au grand public)

→ En cas de mise à disposition en open-source : fuite involontaire de données ou métadonnées publiées avec le code, les paquets, les images conteneurs, les tickets, la documentation (incident fréquent pour des start-up)

→ Perte de propriété intellectuelle (notamment des brevets)

RECOMMANDATIONS

→ Identifier et catégoriser les données sensibles (techniques, commerciales, financières, clients)

→ Chiffrer les données sensibles avant tout envoi vers des tiers (clé USB, email, espace de partage sur Internet)

→ Sauvegarder régulièrement les données, en incluant une sauvegarde hors-ligne, au moins une fois par mois

→ Instaurer une gestion stricte des droits d'accès à l'information (et aux sauvegardes)

→ Effectuer une revue des comptes utilisateurs et des droits d'accès associés, idéalement tous les six mois

→ Faire preuve de vigilance en situation de mobilité et de coworking (filtre de confidentialité écran, partage de connexion 4G/5G plutôt que Wi-Fi publics, verrouillage automatique du poste, pas de connexion de clés USB inconnues)

→ Sensibiliser les développeurs aux bonnes pratiques opérationnelles, notamment pour prévenir les fuites de données (séparation des secrets par environnement, supprimer les informations sensibles de la documentation)

→ En cas de diffusion en open-source : contrôler régulièrement la nature des données présentes dans les dépôts publics du produit (présence de secrets, d'informations sensibles, de données personnelles) ; disposer à la fois de dépôts privés et publics

POUR ALLER PLUS LOIN

GUIDES ANSSI

- Essentiel « Données et traitements sensibles »
- Essentiel « Se protéger des fuites de données »
- Essentiel « Sauvegarde des systèmes d'information »
- Guide « Bonnes pratiques à l'usage des professionnels en déplacement »

AUTRES RESSOURCES

- Guide de la sécurité économique par le SISSE
- Portail dédié au contre-espionnage de la DGSI
- Dispositif de protection du potentiel scientifique et technique de la Nation (PPST)

2

Comment sécuriser les postes de travail ?

DESCRIPTION

Un incident impactant un poste de travail, qu'il soit dédié au développement ou à une autre fonction, peut rapidement s'étendre à tous les systèmes et paralyser l'activité de l'entreprise. Par ailleurs, la majorité des attaques informatiques prend sa source sur les postes de travail des utilisateurs à travers l'envoi de pièces jointes malveillantes, l'usage de sites Internet détournés, la connexion de clés USB malveillantes ou l'utilisation de vulnérabilités non encore corrigées. Il est donc primordial d'adopter des bonnes pratiques d'hygiène dès le démarrage de l'activité.

PRINCIPAUX RISQUES

→ Propagation d'une compromission vers d'autres postes de travail ou d'autres ressources de l'entreprise

→ Vol ou perte du poste de travail et des données qui sont stockées uniquement sur celui-ci

→ Fuite d'informations sensibles à la suite d'une compromission

→ Indisponibilité de l'outil de travail et impact sur la production

→ Piégeage du poste de travail (qui peut inclure un objectif de persistance)

RECOMMANDATIONS

→ Séparer strictement les usages personnels et professionnels, dédier un poste de travail aux activités de l'entreprise

→ Activer les mises à jour de sécurité automatiques sur le poste de travail

→ Activer les fonctions de sécurité natives des systèmes d'exploitation (démarrage sécurisé, chiffrement des disques, pare-feu, antivirus)

→ Travailler avec un compte utilisateur, sans privilèges d'administrateur local sur le poste de travail

→ Réaliser les opérations d'administration à privilèges depuis un poste de confiance (si possible : poste dédié)

→ N'installer que des outils provenant de sources de confiance et systématiquement vérifier l'innocuité au préalable sur un poste dédié à cet usage (soumettre le fichier à un antivirus)

→ Utiliser des mots de passe robustes et différents pour l'ouverture de session sur le poste et l'accès aux applications métier. Activer l'authentification multifacteur quand elle est disponible.

→ Utiliser un gestionnaire de mots de passe (ex : KeePass) de préférence hors-ligne (surtout pour les secrets de comptes administrateurs). Ne pas enregistrer les mots de passe dans les navigateurs Internet.

→ Configurer une durée courte (5 minutes maximum) de verrouillage automatique de la session des postes de travail et penser à verrouiller systématiquement ces derniers en cas d'absence, surtout dans des environnements exposés.

→ Sécuriser les réseaux de connexion pour les postes de travail :

- Maîtriser l'infrastructure réseau locale (Wi-Fi / filaire) du SI de la start-up et les moyens de connexion à Internet
- S'assurer que seuls les ordinateurs professionnels de la start-up se connectent au réseau (Wi-Fi/filaire) de celle-ci
- S'assurer que la connexion est sécurisée pour l'accès aux ressources distantes (accès web en https, utilisation d'un VPN)
- Configurer le pare-feu des postes de travail pour n'autoriser que les flux strictement nécessaires aux besoins métiers de la start-up

POUR ALLER PLUS LOIN

GUIDES ANSSI

- « Guide d'hygiène informatique »
- Guide « Recommandations relatives à l'authentification multifacteur et aux mots de passe »

3

Quelles sont les obligations réglementaires ?

DESCRIPTION

Dans sa réponse à la menace cyber, l'Europe se dote progressivement d'un corpus réglementaire comprenant des exigences de sécurité à destination des entreprises du numérique qui souhaitent commercialiser des produits. Il est primordial de se poser au plus tôt la question des réglementations applicables, malgré les possibles incertitudes sur la cible ou sur la finalité du produit, et quand bien même la situation viendrait à évoluer pendant la phase de développement. En effet, certaines exigences pourraient imposer de revoir complètement le design technique du produit ou bien fixer des limitations incompatibles avec les objectifs initiaux du projet.

Il est également important de vérifier l'adéquation entre la stratégie commerciale et les potentiels coûts d'entrée liés à la réglementation applicable aux clients visés (documentation à réaliser, audits à effectuer, etc.).

PRINCIPAUX RISQUES

→ Retard de développement voire impossibilité de mise sur le marché du produit par défaut de prise en compte de la législation en vigueur

→ Sanction financière en cas de contrôle a posteriori par les autorités

→ Perte d'accès à certains marchés publics ou privés faute de conformité réglementaire.

RECOMMANDATIONS

→ Analyser les réglementations applicables au produit et à la start-up (structure juridique, environnement de développement), notamment pour la cybersécurité :

- Lister les exigences techniques du corpus réglementaire qui pourraient avoir un impact sur le développement du produit ; vérifier si des référentiels d'exigences existent pour les données que le produit est amené à manipuler (exemples : HDS pour les données de santé, RGPD pour les données personnelles).
- Être vigilant sur le fait que certaines réglementations peuvent s'appliquer dans le cas de produits open-source.
- Ne pas hésiter à se faire aider par des organisations (associations professionnelles, autorités de référence, cabinets juridiques, incubateurs, accélérateurs) ou des plateformes dédiées comme MonEspaceNIS2

→ Réaliser un suivi régulier sur la partie réglementaire :

- Etablir un processus de veille pour identifier les changements de façon pro-active.
- Intégrer, dans la feuille de route de l'entreprise, la gestion et le suivi des exigences organisationnelles (documentation, définition de rôles) et techniques et la charge de travail que cela implique en interne.
- Offrir aux clients de la visibilité sur la mise en place et le respect des exigences applicables au produit et à la start-up

→ Au-delà des réglementations applicables au produit, il est nécessaire d'être vigilant sur les réglementations des différents pays lorsqu'une start-up souhaite se développer à l'international : risques lors des déplacements à l'étranger, contraintes liées aux lois à portée extraterritoriale.

POUR ALLER PLUS LOIN

- Instruction interministérielle n°901 relative à la sécurisation des systèmes d'information sensibles, incluant les systèmes d'information « Diffusion Restreinte » (DR)
- Instruction générale interministérielle n°1300 relative à la sécurisation des systèmes d'information classifiés de défense nationale
- LPM relative à la cybersécurité des opérateurs d'importance vitale français (OIV)
- NISv2 relatif à la cybersécurité des entreprises essentielles (EE) et importantes (EI) européennes
- RGPD relatif à la protection des données personnelles
- Réglementations sectorielles ou thématiques : IA Act, Cyber Resilience Act, règlement DORA, etc.

4

Comment sécuriser l'usage de composants tiers ?

DESCRIPTION

Le développement d'un produit s'appuie généralement sur des composants, bibliothèques, et outils développés par des tiers.
Cette chaîne d'approvisionnement logicielle comporte des risques de cybersécurité spécifiques, que les composants soient open-source ou propriétaires.

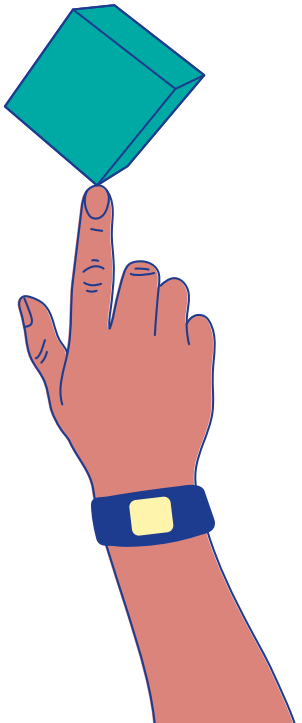
Il convient de mener une analyse des dépendances logicielles dès la phase de conception du produit, afin de faire les bons choix d'architecture logicielle à long terme, et de disposer ainsi d'une vision d'ensemble des risques qui pourraient peser sur le produit en cas d'incident sur une dépendance.

PRINCIPAUX RISQUES

→ Compromission des SI des clients du produit via une attaque sur la chaîne d'approvisionnement logicielle.

→ Perte de maîtrise de la sécurité du produit à la suite d'un changement majeur sur une dépendance (faillite du mainteneur, abandon du produit par la communauté open-source, vulnérabilité non corrigée)

→ Incompatibilité technique avec ou entre des dépendances du produit pouvant entraîner une régression du niveau de sécurité général (nécessité d'utiliser une version d'une dépendance non maintenue ou obsolète)



RECOMMANDATIONS

→ Proscrire le redéveloppement de modules de sécurité dont la robustesse fait consensus au sein de la communauté scientifique – en particulier, il est fortement déconseillé de réimplémenter des bibliothèques cryptographiques soi-même.

→ En cas d'utilisation de composants tiers open-source : anticiper le risque de changement de licence par la communauté pouvant impliquer un usage moins permissif et le risque de ne plus avoir à disposition les correctifs de sécurité.

→ Prévoir les besoins de réversibilité pour les composants tiers jugés à risque (criticité fonctionnelle dans le produit), en particulier s'ils sont open-source.

Caractériser le niveau de maintenance des composants tiers et identifier par anticipation une solution alternative au cas où ils cesseraient d'être maintenus.

→ Superviser les signalements de vulnérabilités affectant les dépendances du produit et procéder à leur mise à jour. A court terme, activer les audits natifs (npm, pip-audit) et définir des règles de mise à jour automatique (renovate, dependabot) via la mise en place de politiques de sécurité (fusion automatique des correctifs mineurs).

→ Disposer à tout instant d'un inventaire à jour des vulnérabilités présentes dans le produit développé par la start-up, incluant les dépendances tierces.

→ Pour aller plus loin dans la gestion des vulnérabilités et licences : générer systématiquement une SBOM par build et l'analyser à l'aide d'un outil de Software Composition Analysis (SCA), qui peut éventuellement être implémenté dans une chaîne CI/CD (voir fiche 6).

→ Porter une vigilance particulière aux noms des paquets et des bibliothèques logicielles tierces utilisées, qui pourraient être source de malveillance (utilisation d'un nom très proche du nom légitime).

POUR ALLER PLUS LOIN

GUIDES ANSSI

• Essentiel « Sélection d'un logiciel libre »

• Guide « A Shared Vision of Software Bill of Materials (SBOM) for Cybersecurity » (co-publication CISA)

5

Comment sécuriser l'environnement de développement ?

DESCRIPTION

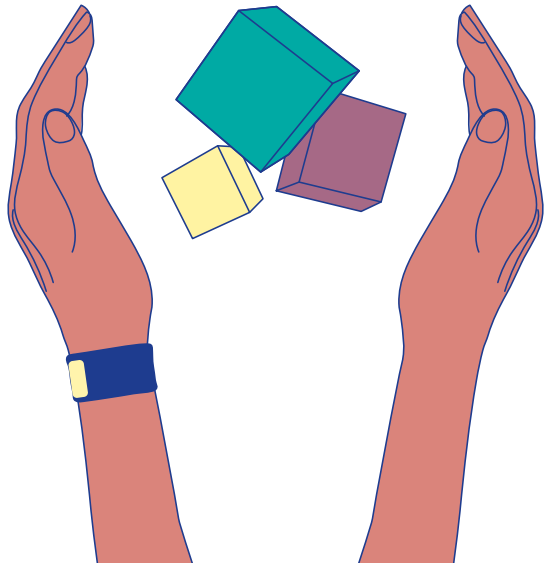
L'environnement de développement est l'ensemble des outils, configurations et infrastructures utilisé par les développeurs pour concevoir, coder, tester et déboguer une application. Il centralise des données sensibles : le code source du produit et les données d'identification. Or, d'une part le code source dévoile des savoir-faire de l'entreprise, d'autre part le produit livré au client est généré à partir du code source, qui doit donc être exempt de vulnérabilités et de comportements malveillants (afin de ne pas exposer les clients aux cyberattaques).

Sécuriser l'environnement de développement permet de contrôler les processus de lecture et de modification des données sensibles, dans un contexte où les attaques sur la chaîne d'approvisionnement logicielle sont en constante augmentation.

PRINCIPAUX RISQUES

→ Défaut de protection de la propriété intellectuelle

→ Exposition des entreprises clientes à des cyberattaques et atteinte à l'image de la start-up



RECOMMANDATIONS

→ Sécuriser les accès aux différents composants de l'environnement de développement :

- Gérer les droits d'accès en utilisant le principe du moindre privilège : n'accorder aux développeurs que les permissions strictement nécessaires à leurs tâches.
- Utiliser des mots de passe forts et un gestionnaire de mots de passe pour l'accès aux composants.
- Utiliser si possible l'authentification multifacteur (MFA) pour les opérations les plus sensibles.
- Réduire au strict minimum les communications entre les environnements de développement, d'intégration et de production pour limiter la propagation d'une attaque. Mettre en place un filtrage réseau strict pour gérer ces flux.

→ Ne jamais stocker des données sensibles de production dans l'environnement de développement (en particulier des secrets). Ne pas dupliquer les bases de données de production vers l'environnement de développement et préférer l'usage de bases de données de développement créées spécifiquement à cet usage.

→ Signer les commit lors de mises à jour, pour vérifier l'intégrité et l'origine du code source (idéalement dans la chaîne CI/CD).

→ Mettre en place dès que possible la relecture de code par un pair, sous l'angle de la cybersécurité.

→ Utiliser uniquement des outils et plug-in de développement jugés de confiance et éviter que chaque développeur personnalise lui-même son environnement, pour limiter le risque d'utiliser des composants non sûrs.

→ Maintenir à jour les composants de l'environnement de développement pour éviter les vulnérabilités connues.

→ Journaliser les activités pour retracer qui a pu accéder ou modifier des données sensibles en cas d'incident.

→ Ne jamais stocker de mots de passe ou de clés en clair, généraliser l'usage de gestionnaires de secrets.

→ Former tous les développeurs aux bonnes pratiques de sécurité et de développement sécurisé. S'appuyer éventuellement sur des services proposés par les incubateurs eux-mêmes.

POUR ALLER PLUS LOIN

GUIDES ANSSI

- Essentiel « Se protéger des fuites de données »
- Essentiel « DevSecOps »
- Essentiel « Sélection d'un logiciel libre »
- Essentiel « Base de données relationnelles »
- Guide « Recommandations relatives à l'administration sécurisée des SI »

6

Quels outils pour sécuriser les développements ?

DESCRIPTION

L'environnement de développement intègre généralement plusieurs outils, dont certains seront utilisés pour améliorer la sécurité du code applicatif et des composants autour de celui-ci. Si le choix des outils dépend de plusieurs critères (langage de développement, nombre de projets, criticité du produit), il est primordial de disposer de certaines catégories d'outils dès le démarrage des développements.

Il convient également d'être vigilant dans l'usage de certains outils d'assistance au développement. En particulier, l'IA peut être utilisée pour générer du code source, mais également pour toutes les étapes de l'ingénierie logicielle (documentation, génération de tests unitaires, correction automatique de vulnérabilités). Son usage implique un risque de perte de maîtrise.

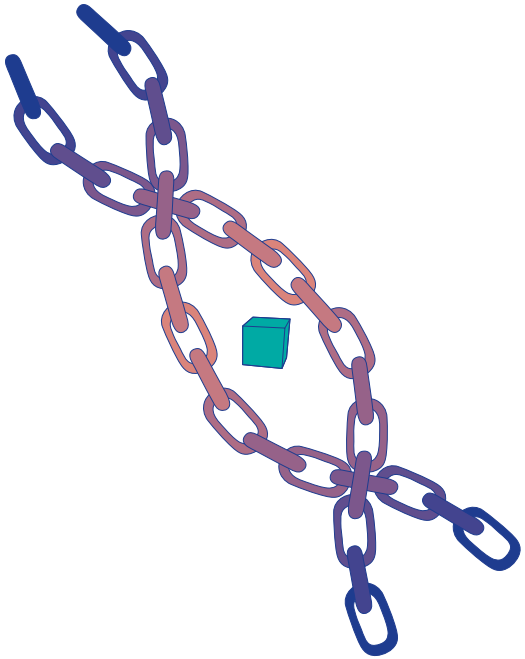
PRINCIPAUX RISQUES

→ Cyberattaque chez les clients via l'exploitation d'une vulnérabilité du produit

→ Perte de maîtrise de la sécurité du code en cas d'assistance par IA

→ Atteinte à l'image en cas de vulnérabilités triviales découvertes sur le produit

→ Accumulation de vulnérabilités non-corrigées (« dette cyber ») sur le produit et perte de maîtrise de la qualité du code



RECOMMANDATIONS

→ Favoriser le choix de langages de développement proposant nativement des propriétés de sécurité (memory-safe).

→ Implémenter, dès le démarrage des développements, les éléments suivants pour renforcer la sécurité de la chaîne d'intégration :

- Outil de gestion des versions et branches du produit ;
- Outil de test de sécurité statique de code (SAST) ;
- Outil de gestion des composants logiciels tiers (SCA/SBOM) ;
- Outil de gestion des secrets (coffre-fort, PKI).

→ Pour accélérer la mise en place de la chaîne d'intégration, il est possible de s'appuyer sur des outils open-source éprouvés et maintenus, et/ou sur des services managés SaaS (en ayant conscience des éventuels risques liés à la protection des données sensibles).

Il est également possible de choisir un incubateur proposant ces services.

→ Implémenter un outil de test de sécurité dynamique de code (DAST) une fois que les autres outils sont déjà éprouvés (notamment les outils SAST).

→ Dans le cas où le livrable du produit est mis à disposition sous la forme d'une architecture logicielle complexe (par exemple une plateforme multiservices), il est important de sécuriser dès la conception (par exemple au moyen de l'IaC, voir fiche 8) l'ensemble des composants techniques autres que le code applicatif :

- Configuration des machines virtuelles ou conteneurs utilisés, ainsi que leur orchestration (ex : kubernetes)
- Configuration des services utilisés : serveurs web, bases de données, middlewares, répartiteurs de charge.
- Architecture technique interne (côté client et serveur) : cloisonnement des modules du produit, filtrage des flux internes entre composants, gestion de la journalisation, gestion des comptes techniques internes.

→ Faire preuve de vigilance lors de l'utilisation de l'IA en tant qu'assistant au développement logiciel :

- Instaurer un cadre d'utilisation de l'IA pour les développeurs (contraintes d'utilisation, interdiction pour certains modules critiques) ;
- Vérifier systématiquement le code généré par IA et maintenir une expertise technique forte dans les équipes, notamment sur la cybersécurité ;
- Ne pas transmettre d'informations sensibles (clés API, données métiers) aux modèles d'IA, a fortiori si ceux-ci sont en SaaS.

POUR ALLER PLUS LOIN

GUIDES ANSSI

- Essentiel « DevSecOps »
- Guide « AI Coding Assistants » (co-publication / BSI)
- Guide « Règles de programmation pour le développement d'applications sécurisées en Rust »
- Guide « Régles de programmation pour le développement sécurisé de logiciels en langage C »
- Guide CISA « A Shared Vision of Software Bill of Materials (SBOM) for Cybersecurity | CISA » (cosignature ANSSI)

7

Comment valoriser la sécurité ?

DESCRIPTION

Longtemps considérée comme un simple centre de coût, la cybersécurité est désormais reconnue comme un levier de création de valeur, en particulier sur les aspects suivants :

→ Construire la résilience numérique de l'entreprise et pérenniser son activité (limiter le risque de cyberattaques, accéder à certains marchés, faciliter la conformité réglementaire, rassurer les partenaires) ;

→ Améliorer la confiance des utilisateurs dans le produit (fidélisation, stabilité) notamment pour la protection de leurs données internes et personnelles ;

→ Innover et se différencier sur le marché en intégrant de nouvelles technologies de sécurité ;

→ Permettre aux équipes de se focaliser sur les fonctionnalités métier dans le produit plutôt que d'avoir à gérer de nombreuses corrections de sécurité non prévues.

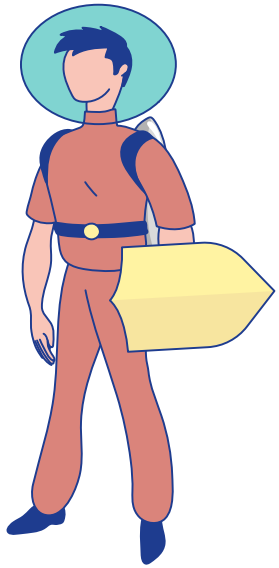
PRINCIPAUX RISQUES

→ Perte de confiance des utilisateurs, clients et donneurs d'ordre si l'aspect cybersécurité n'est pas suffisamment investi

→ Atteinte à l'image de l'entreprise si les démonstrateurs du produit ne sont pas suffisamment sécurisés

→ Perte de maîtrise de la sécurité du produit

→ Perte d'accès à des marché exigeants d'un point de vue cybersécurité



RECOMMANDATIONS

→ Établir un socle de bonnes pratiques de sécurité dans l'environnement de développement (guides, tests de sécurité, etc.) tel qu'indiqué dans les fiches 5 et 6. S'assurer que le produit n'impose pas des prérequis potentiellement dangereux pour les SI des clients (exiger des privilèges démesurés pour l'installation ou l'utilisation courante).

→ Intégrer des mesures de sécurité pour garantir l'innocuité du produit lors de démonstrations en environnement client (isolation, filtrage des flux, chiffrement des données, effacement sécurisé en fin de démonstration).

→ Prévoir une configuration « durcie » (hardening) du produit et documenter sa mise en œuvre

→ Étudier l'intégration de technologies de sécurité innovantes dans le produit en tant que différenciant sur le marché (cryptographie, gestion des secrets, authentification)

→ Éviter la mutualisation des données et des accès des clients sur un seul environnement centralisé (ex : instance Cloud) dans le cas où le produit est encore en cours de développement (démonstrateur). Préférer la duplication de ces environnements et en dédier un pour chaque client si possible.

→ Rendre visibles les mesures de sécurité autour du produit :

- Intégrer, dans le contrat, des engagements de la start-up relatifs à la protection des données du client.
- Implémenter, dès la phase de prospection, des échanges sécurisés avec les clients (plateforme sécurisée de stockage des documents, chiffrement des documents par email, traçabilité de tous les échanges notamment oraux).
- Mettre à disposition un fichier security.txt (RFC 9116) sur le site Internet de l'entreprise, et également un document security.md dans le cas d'utilisation de systèmes de dépôts, afin de rendre accessibles les informations et contacts relatifs à la sécurité du produit.
- Pour aller plus loin, considérer la mise en œuvre d'une politique de Coordinated Vulnerability Disclosure (CVD).

→ Intégrer le RSSI ou les équipes sécurité des clients lors des discussions préalables aux déploiements de démonstrateurs, afin de gagner leur confiance et d'en faire des « alliés » dans le processus d'achat.

→ Maintenir une veille réglementaire régulière, afin de disposer d'éléments de décisions permettant d'orienter la stratégie de la start-up, tel qu'indiqué dans la fiche 3.

POUR ALLER PLUS LOIN

AUTRES

Bonnes pratiques pour l'établissement d'une politique *Coordinated Vulnerability Disclosure (CVD)* :

- NIS coordination Group : se reporter à la section 5 du document Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies
- OpenSSF Vulnerability Disclosure Working Group : oss-vulnerability-guide/maintainer-guide.md at main · ossf/oss-vulnerability-guide · GitHub

8

Comment sécuriser les déploiements ?

DESCRIPTION

Le déploiement désigne ici les actions permettant de déployer et administrer l'infrastructure supportant le produit (ex : serveurs centralisés) ; ainsi que de construire le livrable final à partir du code source, et de le déployer dans cette infrastructure. **Cette activité est critique, car elle impacte directement la production.** Tout incident peut affecter le fonctionnement de la start-up, sa réputation, ou encore son équilibre économique. Cette phase de déploiement inclut une phase préalable d'intégration et d'agrégation des composants techniques nécessaires, qui peut être rendue complexe dans le cas où plusieurs fournisseurs seraient impliqués (notamment si ces derniers n'ont pas la même maturité).

Si les déploiements étaient historiquement réalisés par des administrateurs humains disposant de privilèges élevés sur l'infrastructure, le Cloud permet désormais d'automatiser tout ou partie des déploiements.

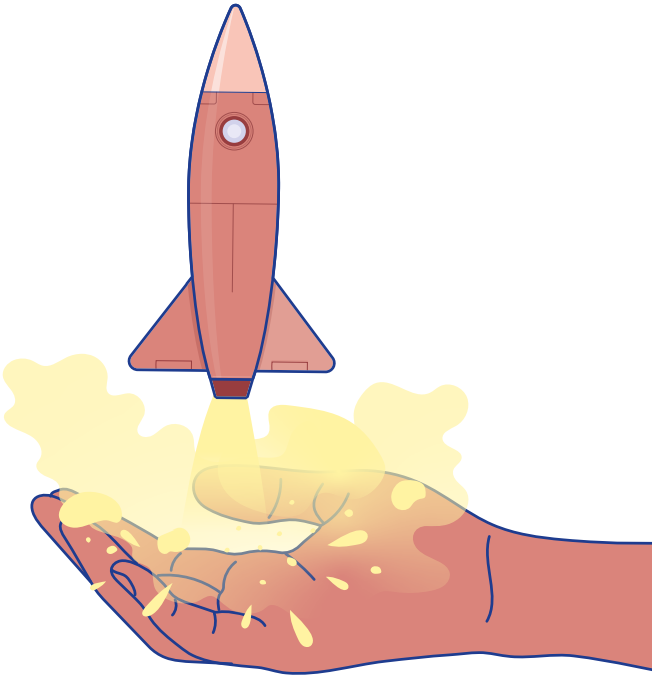
Cette démarche d'Infrastructure as Code (IaC) nécessite de repenser la sécurité des déploiements en considérant le code (scripts, fichiers de configuration) et les comptes techniques (Non Human Identity - NHI) utilisés au même titre que les outils et les comptes des administrateurs humains.

PRINCIPAUX RISQUES

→ Déploiement de code malveillant en production

→ Compromission de la production : vol de données, arrêt du service, destruction de données, code, sauvegarde

→ Défaut d'application des correctifs de sécurité dû à une défaillance de la chaîne de déploiement



RECOMMANDATIONS

→ Mettre en place une journalisation et une supervision adaptées lors des déploiements pour faciliter l'investigation en cas d'incidents.

→ Limiter le nombre et les privilèges des comptes d'administration humains ; privilégier l'utilisation de comptes éphémères pour les NHI.

→ Instaurer une revue régulière (idéalement tous les six mois) des comptes, ainsi que des droits et privilèges de ces derniers.

→ Appliquer un durcissement des composants de l'infrastructure centralisée (VM, conteneurs, services réseaux) en suivant par exemple les guides des éditeurs.

→ Séparer si possible l'environnement d'intégration (CI) de l'environnement de déploiement (CD).

→ Automatiser le processus d'intégration et de construction du livrable final (tests et compilation automatiques).

→ Automatiser le processus de déploiement en appliquant les règles de développement sécurisé à l'IaC.

→ Utiliser des secrets et des configurations dédiés à la production.

→ Signer les éléments logiciels construits (artefacts) pour en vérifier l'intégrité avant déploiement en production.

→ Vérifier régulièrement la conformité des configurations, en lien avec les politiques de sécurité logicielles.

→ Privilégier une infrastructure de production immuable, en cohérence avec la démarche d'automatisation et d'IaC.

→ Instaurer des mécanismes de retour arrière en cas d'incident (blue/green, rolling update, canary testing).

POUR ALLER PLUS LOIN

GUIDES ANSSI

- Essentiel « Se protéger des fuites de données »
- Essentiel « DevSecOps »
- Essentiel « Virtualisation »
- Guide « Recommandations de configuration d'un système GNU/Linux »
- Guide « Agilité et sécurité numérique : méthode et outils à l'usage des équipes projet »
- Guide « Recommandations de sécurité relatives aux déploiements de conteneur Docker »
- Fondamental « Sécurisation d'une infrastructure VMware »
- Guide « Recommandations relatives à l'administration sécurisée des SI »

9

Comment sécuriser l'industrialisation du produit ?

DESCRIPTION

Le passage à l'échelle et la commercialisation d'un produit auprès de plusieurs clients implique d'adapter les processus internes à la montée en charge au sein de l'entreprise. Cela implique, en particulier, de structurer la gestion des aspects suivants :

- Le maintien en condition opérationnelle du produit (MCO) ;
- Le maintien en condition de sécurité du produit (MCS) y compris la détection et le traitement des incidents de sécurité ;
- L'automatisation d'autres processus métiers en lien avec le produit, et les risques associés.

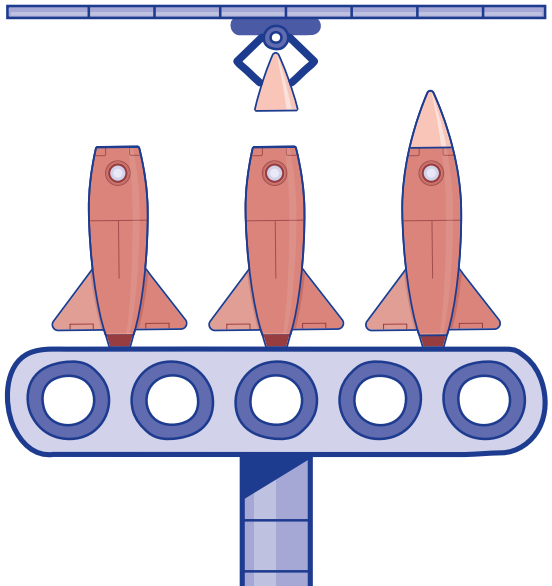
Ces aspects visent, d'une part, à renforcer la confiance des clients quant à la capacité de l'entreprise à maintenir un produit à jour et sécurisé, et d'autre part, à permettre de répondre à une demande plus conséquente.

PRINCIPAUX RISQUES

→ Complexité inhérente au maintien de versions hétérogènes du produit en production

→ Vulnérabilités du produit persistantes dans le temps

→ Atteinte à l'image de l'entreprise en cas de défaillance du produit



RECOMMANDATIONS

→ Limiter la diversité des environnements techniques autour du produit :

- Définir une architecture technique de référence pour la gestion du produit, et la rendre duplicable et adaptable pour certains besoins spécifiques si nécessaire.
- Limiter la coexistence de versions différentes en production. Instaurer une approche de développement modulaire pour adresser les besoins spécifiques. S'autoriser à refuser certaines demandes de clients qui pourraient mettre en défaut la sécurité du produit.
- Etablir un processus de déploiement massif de correctif en urgence, proposer éventuellement des contre-mesures temporaires aux clients dans l'attente du déploiement de correctif.
- Automatiser un maximum d'actions sur la plateforme de gestion (envoi automatique d'emails, test automatique de sécurité) mais conserver une étape de validation humaine dans la chaîne de décision.

→ Disposer d'un outil de supervision et de détection centralisé des incidents de sécurité, même minimaliste (collecteur de journaux, SIEM). Il est possible de s'appuyer sur des solutions disponibles en SaaS, notamment celles intégrées aux environnements Cloud hébergeant le produit ou encore sur des services proposés par les incubateurs.

→ Faire preuve de transparence vis-à-vis des clients en cas de découverte de vulnérabilité ou d'incident de sécurité sur le produit et les dépendances du produit. Prévenir également l'ANSSI via le CERT-FR.

→ Documenter le produit, notamment en interne, en matière de sécurité des composants et d'architecture (matrice des flux, durcissement, inventaire des comptes). Maintenir à jour la documentation le plus régulièrement possible.

POUR ALLER PLUS LOIN

GUIDES ANSSI

- Essentiel « DevSecOps »
- Guide « Maîtriser les risques de l'infogérance. Externalisation des systèmes d'information »
- Guide « Maîtrise du risque numérique - l'atout confiance »
- Corpus « La supervision de sécurité »

10

Quelles considérations de cybersécurité lors du passage à l'échelle de mon activité ?

DESCRIPTION

La croissance de l'activité d'une entreprise s'accompagne d'une complexification de l'organisation et de l'écosystème de parties prenantes ; de l'évolution continue des mesures de sécurité (voir fiche 9) ; ainsi que de l'exposition accrue de l'activité de l'entreprise au monde extérieur.

Dans ce contexte de transformation, au-delà des considérations liées au produit, il est nécessaire de prendre des mesures stratégiques et organisationnelles pour assurer le passage à l'échelle de l'activité en toute sécurité en augmentant la taille des équipes, en adaptant leur outillage au volume d'activité, en veillant à préserver la résilience des solutions.

PRINCIPAUX RISQUES

→ Augmentation du risque d'attaques ciblées due à la visibilité ou notoriété du produit ou de l'entreprise.

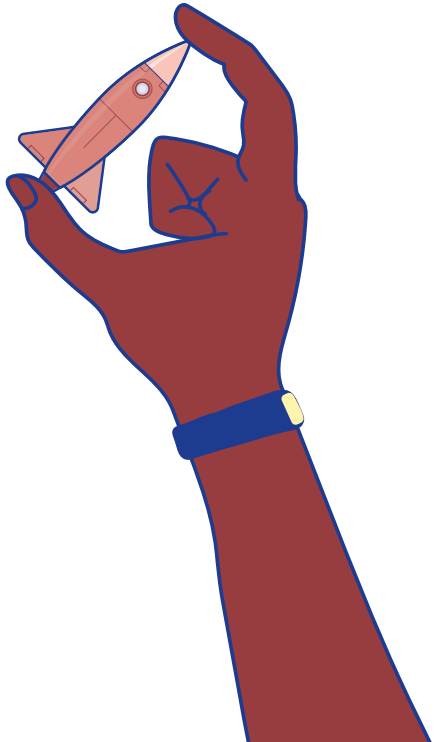
→ Perte de maîtrise des mesures de sécurité sur le SI due à l'augmentation du volume et de la surface d'attaque.

→ Perte de confiance et atteinte à l'image de l'entreprise en cas de non-maîtrise de la qualité de services.

→ Multiplication des tickets de sécurité et incapacité à les traiter efficacement.

→ Perte de culture sécurité au sein de l'équipe en cas de croissance rapide.

→ Perte de maîtrise de l'activité lors du processus d'internationalisation (lois à portée extraterritoriale, espionnage).



RECOMMANDATIONS

→ Dédier des effectifs à la cybersécurité

- Créer un ou plusieurs postes dédiés à la cybersécurité (RSSI) avec, par exemple, une personne par ligne de produits, zone géographique, activité, niveau de sensibilité de SI, etc.
- Prévoir une activité de supervision de sécurité et de veille des menaces cyber.
- Analyser les risques préalablement à tout recours à la sous-traitance.
- Être vigilant lors du recrutement des équipes (charte de bonne conduite, vérification de l'adéquation entre le profil et le niveau de responsabilité) et appréhender la notion d'administrateurs du système ainsi que les privilèges associés.

→ Adapter l'outillage à l'augmentation de l'activité

- Évaluer la capacité des outils existants à passer à l'échelle : ne pas chercher à remplacer à tout prix ; limiter le nombre d'outils utilisés.
- Adapter la stratégie d'hébergement : recours au Cloud et à des services SaaS, en gardant à l'esprit les enjeux de protection des données sensibles (voir fiche 11).
- Étudier la possibilité de s'appuyer sur des solutions « clés en main » facilitant le passage à l'échelle : IA, automatisation, Data Centric Security, etc.

→ Assurer la résilience

- Instaurer des mesures de sécurité proportionnées à la croissance de l'entreprise, en s'appuyant sur le guide d'hygiène de l'ANSSI. Porter une attention particulière aux bonnes pratiques d'administration du SI (séparation des postes de bureautique et des postes d'administration, durcissement des configurations serveurs, cloisonnement des ressources par niveau de sensibilité).
- Mettre en place un processus de gestion de crise : plan de continuité des activités (PCA), plan de reprise des activités (PRA), plan de réponses aux incidents.
- Former régulièrement le personnel et favoriser son implication dans la démarche de sécurité.

→ Etudier les besoins de certification et de qualification

- Analyser les exigences réglementaires qui pourraient porter sur le produit, en fonction des secteurs d'activité visés, et étudier la pertinence de certifier ou qualifier celui-ci (CSPN, Critères communs)
- Identifier les besoins de recourir à des produits ou services qualifiés en fonction des attentes des clients ou de contraintes réglementaires (ex : SecNumCloud, HDS).

POUR ALLER PLUS LOIN

GUIDES ANSSI

- Page Web sur la certification / qualification de l'ANSSI
- « Guide d'hygiène informatique »
- Guide « Recommandations relatives à l'administration sécurisée des SI »
- Guide « Recommandations relatives au nomadisme numérique »
- Guide « Passerelle d'interconnexion à Internet »

AUTRES

- ISO 27001
- Guide d'homologation

11

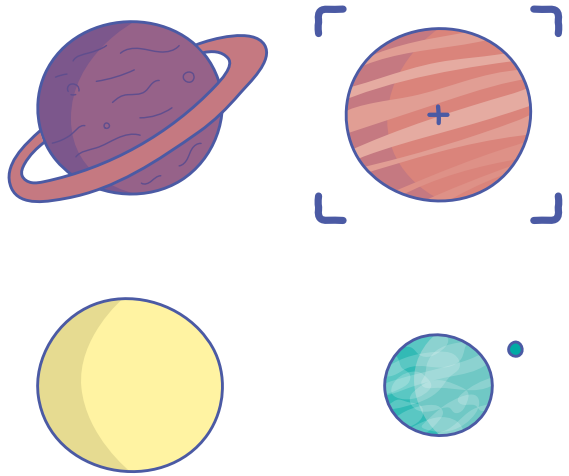
Comment choisir son hébergement pour les données et traitements ?

DESCRIPTION

Lors du choix d'un hébergement, il est essentiel de considérer l'ensemble des activités de la start-up et de ne pas se limiter au service ou produit. On associe généralement l'hébergement à l'infrastructure soutenant un service numérique, et la protection des données à celles confiées par les clients. Or, ces aspects ne représentent qu'une partie du périmètre à protéger et il est nécessaire d'estimer la criticité et la sensibilité de chaque donnée en se demandant, tel qu'indiqué en fiche 1 : « *Quelles seraient les conséquences d'une perte, d'une indisponibilité, d'une fuite ou d'une modification malveillante de cette donnée et quel serait l'impact pour l'entreprise ou les clients ?* ».

L'usage de services Cloud accélère la mise sur le marché mais peut engendrer une dépendance liée à la complexité de la réversibilité ou à la difficulté de maitrise des coûts (facturation à la demande, nouvelles options payantes). Par ailleurs, la sécurité des données et traitements n'est assurée qu'en partie par le fournisseur du service cloud : il est de la responsabilité de l'utilisateur du service de correctement le configurer et d'en compléter la sécurité avec ses propres mesures de protection.

Il est à noter qu'un acteur exploitant un service Cloud ou fournissant un hébergement est en capacité, avec plus ou moins d'efforts, d'accéder aux données et traitements qui lui sont confiés. Il convient donc de s'interroger sur la valeur que ces données pourraient représenter pour ces acteurs (notamment vis-à-vis de lois à portée extraterritoriale) et de mettre en perspective la solution développée par la start-up et le catalogue de l'hébergeur Cloud (possible concurrence).



PRINCIPAUX RISQUES

- → Divulgation d'information sensible
- → Perte de données
- → Indisponibilité du service
- → Perte de confiance des clients, atteinte à l'image de l'entreprise

RECOMMANDATIONS

→ Classer les données par familles et évaluer leur criticité (voir fiche 1) ; identifier les composants et services Cloud manipulant des données sensibles.

→ Sélectionner l'hébergement et les services adaptés à la criticité des données en se rappelant que le Cloud n'est pas la solution unique. Recourir aux solutions qualifiées SecNumCloud pour tout hébergement de données critiques dans le Cloud. Éventuellement réinternaliser (« on premise ») les données les plus sensibles.

→ Activer l'authentification multifacteur (MFA) pour accéder aux services Cloud. Veiller à la bonne politique de gestion des droits (voir fiche 12) et cloisonner les rôles des administrateurs de ressources Cloud.

→ S'assurer de la réversibilité des services implémentés dans le Cloud, en cas de volonté de changer de fournisseur. En particulier, éviter d'utiliser des fonctionnalités propres à un seul fournisseur de Cloud, notamment celles de sécurité.

SPÉCIFIQUE ÉTATIQUE

Quand le marché visé contient des administrations d'État, prendre en compte, dès la conception, l'exigence de recourir à des offres qualifiées SecNumCloud pour les données sensibles. L'objectif est d'utiliser dès le début ce type d'offres ou de faciliter la migration afin d'être conforme à la doctrine « Cloud au centre » de l'État français. En complément, certaines réglementations nationales imposent également des exigences sur l'hébergement des SI, comme par exemple l'II 901 relative aux systèmes d'informations sensibles et DR.

POUR ALLER PLUS LOIN

GUIDES ANSSI

- Guide « Recommandations pour l'hébergement des SI sensibles dans le cloud »
- Doctrine Cloud au centre.

AUTRES

- Loi SREN (Article 31) : www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000049563610

12

Comment gérer le travail collaboratif en toute sécurité ?

DESCRIPTION

Même au sein d'une structure de petite taille, il demeure indispensable de préciser les rôles et niveaux d'accès de chacun sur le système d'information. Par commodité – ou par excès de confiance – il pourrait être tentant d'allouer les mêmes droits à tous les collaborateurs sur l'ensemble des composants du SI. Or, restreindre les accès au strict besoin opérationnel réduit l'ampleur des dégâts en cas d'incident de sécurité.

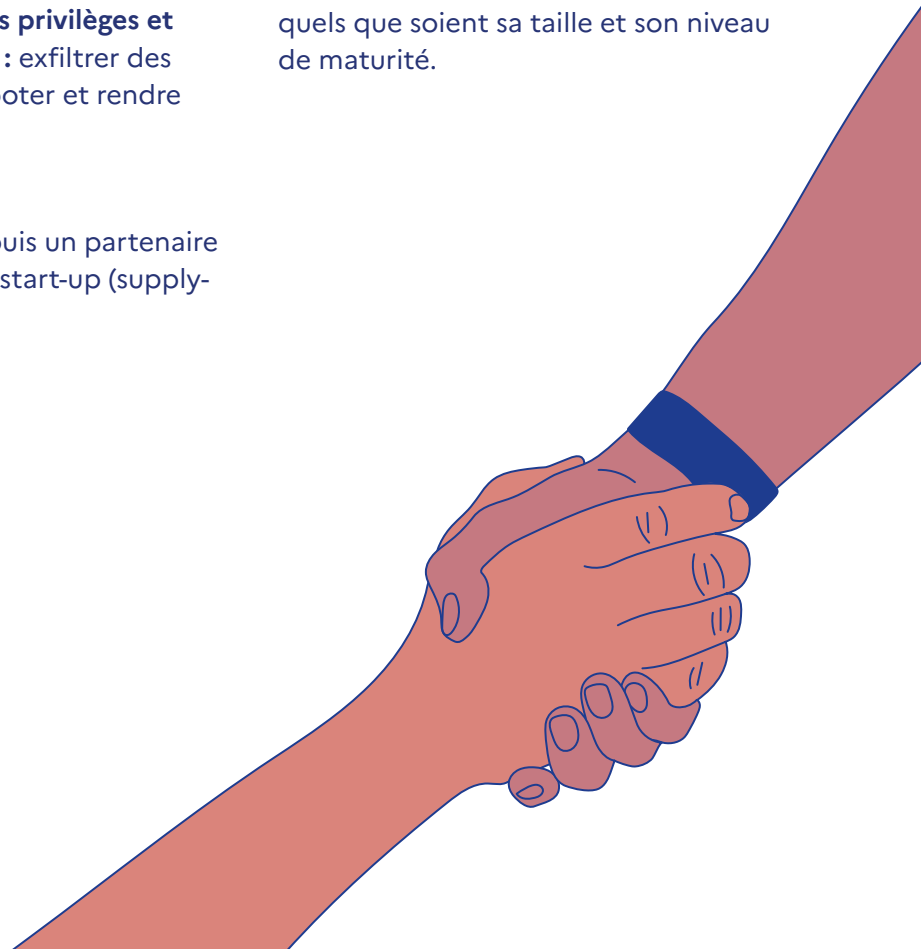
Les attaquants peuvent tirer profit d'un laxisme dans la gestion des droits pour élever leurs privilèges et atteindre leur objectif : exfiltrer des données sensibles, saboter et rendre indisponibles les services métier, ou encore insérer du code malveillant dans le produit. Ainsi, le principe de « moindre privilège » et la gestion du « besoin d'en connaître » sont essentiels dans la sécurisation d'un SI, quels que soient sa taille et son niveau de maturité.

PRINCIPAUX RISQUES

→ Fuite d'informations sensibles

→ Accès privilégié illégitime sur le SI

→ Compromission depuis un partenaire ou vers un client de la start-up (supply-chain attack)



RECOMMANDATIONS

→ Définir des rôles préétablis en fonction du métier de l'utilisateur devant accéder au SI : développeur, administrateur, commercial, testeur, comptable, etc.

→ Créer un compte utilisateur spécifique pour chaque rôle, quand bien même un utilisateur aurait plusieurs rôles.

→ Utiliser des outils de partage d'information permettant une gestion de rôles et des droits d'accès, et une journalisation suffisamment granulaire (RBAC).

→ Instaurer une revue des rôles et des droits d'accès, idéalement au moins une fois tous les six mois.

→ Mettre en place un processus d'arrivée et de départ des collaborateurs dans l'entreprise.

→ En cas d'attribution de droits d'accès temporaires, établir une traçabilité et s'assurer de la bonne désactivation des accès une fois le travail terminé.

→ Utiliser uniquement des moyens professionnels pour le travail collaboratif ; et ne pas communiquer via des outils personnels (réseaux sociaux, emails personnels).

→ Vérifier systématiquement l'identité des personnes présentes lors de réunions audio ou en visioconférence.

→ Stocker les informations sensibles dans des environnements permettant une protection en confidentialité (chiffrement à l'état de l'art).

→ Identifier les données les plus sensibles (voir fiche 1) et intégrer un indicateur visuel pour les communications contenant ces éléments (emails, documents).

→ Instaurer des règles claires pour la communication et les échanges avec des partenaires externes à l'entreprise.

POUR ALLER PLUS LOIN

GUIDES ANSSI

- Guide « Recommandations relatives à l'administration sécurisée des SI »
- Guide « Maîtriser les risques de l'infogérance. Externalisation des systèmes d'information »
- Guide « Maîtrise du risque numérique - l'atout confiance »
- Essentiel « Se protéger des fuites de données »

13

Comment sécuriser une levée de fonds ?

DESCRIPTION

Au cours du processus de levée de fonds, la start-up doit communiquer des informations sensibles pour présenter son activité aux tiers concernés (banque d'affaires, investisseurs, cabinets d'audit ou d'avocats). Les documents transmis peuvent contenir des données stratégiques, confidentielles, ou à caractère personnel (projections d'activité et financière, éléments techniques ou juridiques, etc.). **Il est donc essentiel d'encadrer l'accès à ces informations en adoptant une hygiène contractuelle rigoureuse, avec la mise en place d'accords de confidentialité (NDA)** à faire signer aux tierces parties. En outre, il est essentiel de s'assurer que les données partagées à l'extérieur seront traitées avec le bon niveau de protection, notamment en ce qui concerne leur confidentialité et la traçabilité des accès.

PRINCIPAUX RISQUES

- → Atteinte à la confidentialité de données sensibles
- → Espionnage industriel
- → Captation de données
- → Perte de confiance de tiers notamment les investisseurs.

RECOMMANDATIONS

→ Identifier le niveau de sensibilité des données qui doivent être transmises dans le cadre de la levée de fonds. Plus les données sont sensibles (celles dont la compromission serait la plus problématique), plus les mesures de protection doivent être strictes et le partage limité. Ainsi, la présentation aux investisseurs (le « pitch deck »), diffusé largement au début du processus de levée de fonds, ne doit contenir que des informations non sensibles, c'est-à-dire disponibles en sources ouvertes ou non stratégiques. Ultérieurement, lors des phases d'audit préalable (« due diligences ») ou de négociation exclusive, des informations plus sensibles pourront être partagées, sous réserve d'avoir fait signer des accords de confidentialité (NDA).

→ Préférer les systèmes de communication chiffrés pour la transmission d'informations sensibles (email et pièces jointes chiffrés et signés, messagerie chiffrée de bout en bout, etc.) qui limitent le risque d'interception voire de modification des informations échangées.

→ S'assurer que la data room est hébergée par un fournisseur de service de confiance (tel qu'un hébergeur qualifié SecNumCloud) apportant des fonctionnalités de cybersécurité (chiffrement des données, contrôle d'accès, traçabilité). Il convient de prendre en compte la localisation géographique des datacenters et les réglementations à portée extraterritoriale auxquelles sont soumis l'hébergeur. A chaque étape, et en particulier lors de la phase d'exclusivité, il est nécessaire de révoquer les accès des participants qui quittent le projet.

→ S'assurer que les tiers auxquels des données sensibles sont confiées sont sensibilisés aux risques de cybersécurité et mettent en place des mesures de protection adaptées au sein de leurs propres systèmes d'information.

POUR ALLER PLUS LOIN

GUIDES ANSSI

- Essentiel « Se protéger des fuites de données »

AUTRES

- Portail dédié au contre-espionnage de la DGSI
- Portail de la DGE dédié à la sécurité économique

Quelles structures pour appuyer une démarche de cybersécurité ?

Lorsqu'une start-up débute son activité, elle a tout intérêt à entrer en contact avec les structures susceptibles de l'accompagner dans sa démarche de cybersécurité afin de bénéficier des potentiels dispositifs d'accompagnement ou outils de diagnostics, de la documentation dédiée, d'un réseau de coopération, ou encore d'aides financières.

① Structures d'aide en cybersécurité

ANSSI
https://cyber.gouv.fr/

→ Ressources cyber mises à disposition de tous (guides, fiches pratiques)

→ Pour les start-up du numérique évoluant dans le domaine de la cybersécurité :

- Il est utile de se faire connaître de la Division Industrie et Technologies de l'ANSSI : industries@ssi.gouv.fr
- Il est possible de contacter le Centre de coordination cyber français (NCC-FR) hébergé par l'ANSSI pour connaître les possibilités en matière de financements européens : ncc-fr.anssi@ssi.gouv.fr

MonAideCyber
https://messervices.cyber.gouv.fr/services/mon-aide-cyber-aidants.html

Service de l'ANSSI offrant un diagnostic cyber personnalisé rapide et gratuit, ainsi que des propositions de mesures de sécurité priorisées, via l'intervention d'un Aidant cyber.

17cyber
https://17cyber.gouv.fr/
et Cyber malveillance
https://www.cybermalveillance.gouv.fr/

Plateformes de référence pour assister les entreprises victimes de cybermalveillance, les sensibiliser au risque cyber, les informer sur les menaces numériques et les moyens de s'en protéger. 17cyber propose un outil de diagnostic, qu'il est possible d'intégrer à un site web. Cyber malveillance propose également différents guides cyber pour les dirigeants et collaborateurs.

CNIL
https://www.cnil.fr/fr/startup-comment-faire-de-votre-conformite-rgpd-un-avantage-concurrentiel

Conseils et fiches pratiques dédiées aux start-up pour la sécurité des données personnelles, la conformité au RGPD, ou encore la prévention des risques.

Campus Cyber régionaux

Points de contact en région qui permettent d'accéder à un panel d'offres de services cyber existants. Ils proposent des services pour la montée en compétences, l'accompagnement, les diagnostics. Certaines de ces structures hébergent également des incubateurs et accélérateurs.

② Structures d'accompagnement autres

Aides au développement et à l'innovation des régions et territoires

→ Le site officiel aides-entreprises.fr recense les aides financières existantes, notamment celles proposées par les collectivités territoriales (départements, régions, communautés de communes).

→ Le site francenum.gouv.fr répertorie les aides proposées par les régions et propose également un moteur de recherche dédié.

→ Certaines collectivités publient également les aides qu'elles proposent sur leur site.
Par exemple : PM'up et TP'up en Ile-de-France.

Les Capitales et Communautés French Tech
https://lafrenchtech.gouv.fr/fr/le-reseau-de-proximite/

→ Le réseau French Tech propose des actions d'accompagnement et évènements sur les sujets de préoccupation des start-up, dont la cybersécurité.

→ Les plateformes French Tech Central de certaines Capitales French Tech permettent une prise de rendez-vous directe et individuelle avec les référents locaux de l'ANSSI.

→ Les entreprises peuvent retrouver leur Capitale de référence dans l'annuaire du réseau.

Bpifrance
https://bpifrance-creation.fr/encyclopedie/aides-a-creation-a-reprise-dentreprise/aides-a-linnovation/recapitulatif-principales

Organisme d'accompagnement des entreprises, de l'amorçage jusqu'à leur cotation en octroyant des bourses, des crédits et en intervenant en garantie et en fonds propres. Assure, en outre, des services d'accompagnement et de soutien aux entreprises dans leurs projets d'innovation, de croissance externe et d'export, en partenariat avec Business France.

Service économique de l'État en région
https://www.entreprises.gouv.fr/espace-entreprises/etre-accompagne/contacter-un-service-economique-de-letat-en-region

Appui aux filières stratégiques et à l'animation de la politique territoriale d'innovation et de transformation numérique des entreprises.

Les chambres de commerce et d'industrie
https://www.cci.fr/contact

Accompagnement des entreprises à toutes les étapes de leur développement.

Délégués à l'information stratégique et à la sécurité économiques (DISSE)
https://www.entreprises.gouv.fr/espace-entreprises/etre-accompagne/annuaire-des-disse-en-region

Prise en charge des questions relatives à la sécurité économique des entreprises.

La Direction générale de la sécurité intérieure (DGSI) partage régulièrement des « flashs ingérences » qui sensibilisent à divers risques.

La Direction générale des entreprises (DGE) met à disposition une page dédiée à destination des entreprises constituée de 28 fiches thématiques sur la sécurité économique, qui aborde, entre autres, des recommandations sur le numérique et la cybersécurité.

Structures de pilotage de politiques publiques

La Mission French Tech lafrenchtech.gouv.fr

La Mission French Tech est la mission de l'État chargée de soutenir la structuration et la croissance de l'écosystème des start-up françaises, en France et à l'international. Rattachée à la Direction Générale des Entreprises, au sein du ministère de l'Économie, des Finances et de la Souveraineté Industrielle et Numérique, elle fédère et anime l'écosystème de la French Tech avec un réseau de 17 Capitales et 97 Communautés French Tech labellisées, en France et à l'international.

La Mission French Tech accompagne les start-up les plus matures à travers le programme French Tech Next40/120, mais également des start-up émergentes positionnées sur des secteurs identifiés comme stratégiques pour la souveraineté numérique et l'excellence technologique avec le programme French Tech 2030. Elle accompagne notamment des entreprises qui développent des technologies de cybersécurité comme solutions aux enjeux développés dans ce guide.

Avec l'initiative Je choisis la French Tech et la sensibilisation des start-up aux enjeux de cybersécurité, la Mission French Tech pousse les acteurs publics et privés français à l'adoption de solutions développées par les start-up françaises, pour renforcer la performance économique de ces dernières tout en assurant le sécurité économique des premières.

Enfin, à travers le programme French Tech Tremplin, la Mission French Tech permet à des personnes éloignées de l'entrepreneuriat de créer leur start-up, partout en France.

Le Secrétariat général pour l'investissement (SGPI)

Le Secrétariat général pour l'investissement est chargé, sous l'autorité du Premier ministre, d'assurer la cohérence et le suivi de la politique d'investissement de l'État à travers le déploiement du plan France 2030.

Le plan France 2030 vise à transformer durablement des secteurs clés de l'économie (énergie, hydrogène, automobile, aéronautique ou encore espace) par l'innovation technologique et l'industrialisation.

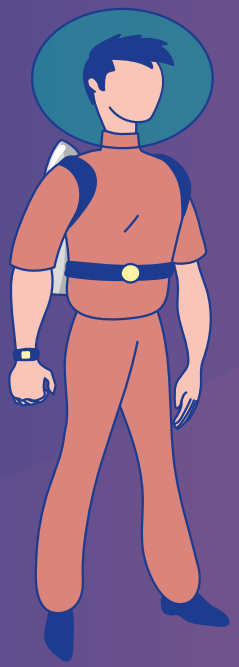
Au sein du plan France 2030, la cybersécurité est vue non seulement comme un facteur de résilience face à une menace systémique qui pèse sur l'ensemble des secteurs de l'économie, mais également comme une filière économique porteuse.

Spécifique au secteur de la Défense

Pour les start-up visant des prestations au profit du ministère des Armées, un premier niveau de maturité cyber, dit niveau fondamental, s'impose progressivement dans les relations entre la DGA et l'industrie.
Les exigences associées figurent au sein d'un référentiel :
Référentiel de maturité cyber - armement.defense.gouv.fr

Par ailleurs des dispositifs de soutien aux start-up et PMEs du secteur défense sont décrits sur le site dédié :
https://armement.defense.gouv.fr/soutien-start-ups-pme-et-eti/soutien-au-fonctionnement-financement-rh

L'Agence de l'innovation de défense (AID) propose un guichet unique pour les entreprises souhaitant présenter spontanément leurs projets ou solutions et éventuellement bénéficier d'un accompagnement.
Les propositions peuvent être déposées à ce lien :
https://www.defense.gouv.fr/aid/deposez-votre-projet/guichet-unique



Pour toutes les questions techniques relatives au contenu du guide :

conseil.technique@ssi.gouv.fr

Version 1.0 – Février 2026

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.cyber.gouv.fr