Cartographie du système d'information à l'usage de la sécurité numérique

Pourquoi une cartographie du système d'information à usage de la sécurité numérique ?

La sécurité numérique constitue un enjeu majeur pour les systèmes d'information. Les attaques informatiques sont de plus en plus nombreuses et complexes, dans un environnement en constante évolution, notamment avec l'augmentation des échanges d'information et des accès aux systèmes d'information.

La cartographie est un outil essentiel à la maitrise du système d'information. Elle permet d'avoir connaissance de l'ensemble des constituants du système d'information et d'obtenir une meilleure lisibilité de celui-ci en le présentant sous différentes vues. L'élaboration d'une cartographie du système d'information s'intègre dans une démarche générale de gestion des risques et répond à quatre enjeux de sécurité numérique :

- contribuer à la maitrise du système d'information : la cartographie permet de disposer d'une vision commune et partagée du système d'information au sein de l'organisme. Elle facilite également la capitalisation d'expérience et la prise de décision grâce à un langage simple et visuel, ce qui permet de manière générale d'améliorer le niveau de maturité de l'organisme en matière de sécurité numérique ;
- contribuer à la cyberprotection du système d'information : la cartographie permet d'identifier les systèmes les plus critiques et les plus exposés, d'anticiper les possibles chemins d'attaque de ces systèmes et de mettre en place des mesures pour assurer leur protection ;
- contribuer à la cyberdéfense du système d'information : la cartographie permet de réagir plus efficacement en cas d'incident ou d'attaque numérique, de qualifier les impacts et de prévoir les conséquences des actions défensives réalisées ;
- contribuer à la cyberrésilience du système d'information : la cartographie permet d'identifier les activités clés de l'organisme et s'impose comme un outil indispensable à la gestion de crise, qu'elle soit cyber ou non.

Ce guide présente une démarche pour aider les organismes à élaborer des cartographies de leurs systèmes d'information, en vue de répondre aux besoins opérationnels de la sécurité numérique. Il propose une approche simple, pratique et progressive du travail de cartographie. Il peut être utilisé par tout organisme quelle que soient sa nature, sa taille, la complexité de son système d'information ou sa maturité en la matière. Il vise en premier lieu les Opérateurs d'Importance Vitale (OIV)[1], mais il est également adapté aux autres organismes du secteur public et privé.

[1] Tels que définis par l'article L. 1332-1 du code de la défense. Les OIV pourront en particulier s'appuyer sur le présent guide pour se conformer à la règle « cartographie » (cf. annexe I des arrêtés sectoriels fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale, pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense).

Qu'est-ce qu'une cartographie ?

De manière générale, le terme de cartographie désigne une représentation schématique d'un ensemble d'informations permettant de disposer d'une vision synthétique de celle-ci. Les informations représentées sont choisies de manière pertinente pour répondre efficacement à une ou des questions posées.

Les cartographies comportent plusieurs dimensions. Par exemple, les cartes géographiques intègrent les infrastructures routières et les villes pour répondre au besoin des usagers. Les informations représentées peuvent être plus ou moins nombreuses selon les besoins. Par exemple, on peut choisir de représenter l'altitude, les stations essence ou encore les péages.

Dans un contexte numérique, la cartographie permet de représenter le système d'information d'un organisme ainsi que ses connexions internes et avec l'extérieur. Cette représentation peut être plus ou moins détaillée en incluant par exemple les biens matériels, logiciels, les réseaux de connexion, mais aussi les informations, activités et processus qui reposent sur ces biens. Le niveau de granularité choisi dépend de la question posée. Par exemple : quel est le niveau de confiance global de l'organisme envers les membres de son écosystème ? Combien de systèmes sont concernés en cas de publication d'une nouvelle vulnérabilité sur un logiciel du marché ?

Concrètement, la cartographie doit permettre :

- de réaliser l'inventaire patrimonial du système d'information : il contient la liste des composants du système d'information et leur description détaillée ;
- de présenter le système d'information sous forme de vues : elles constituent des représentations partielles du système d'information, de ses liens et de son fonctionnement. Elles sont destinées à rendre lisibles et compréhensibles des aspects du système d'information de nature à être exploités par exemple dans les opérations de sécurité numérique.

De manière générale, la cartographie est composée de 3 « visions » allant progressivement du métier vers la technique, elles-mêmes déclinées en « vues[2] » :

- Vision « métier » :
  - vue métier de l'écosystème, présentant les différentes entités ou systèmes avec lesquels le système d'information interagit pour remplir sa fonction ;
  - vue métier du système d'information, qui le représente au travers de ses processus et de ses informations principales, qui sont les biens essentiels au sens de la méthode d'analyse de risques EBIOS[3].

[2] Le découpage retenu ici est adapté dans le cadre de la construction d'une cartographie à l'usage de la sécurité. Il est cohérent avec les standards d'architecture ou d'urbanisation des systèmes d'information.

[3] Expression des Besoins et Identification des Objectifs de Sécurité, en référence au guide méthodologique du 25 janvier 2010 publié par l'ANSSI.

- Vision « applicative » :
    - vue des applications, décrivant les composants logiciels du système d'information, les services qu'ils offrent et les flux de données entre eux ;
    - vue administration, qui répertorie les périmètres et les niveaux de privilèges des utilisateurs et des administrateurs.
- Vision « infrastructure » :
    - vue des infrastructures logiques qui illustre le cloisonnement logique des réseaux notamment par la définition des plages d'adresses IP, des VLAN et des fonctions de filtrage et routage ;
    - vue des infrastructures physiques, décrivant les équipements physiques qui composent le système d'information ou qui sont utilisés par celui-ci.

Les vues sont composées de différents objets, dont des exemples sont proposés en annexe 1. Dans chaque vue, un objet pivot permet de faire le lien avec les vues adjacentes afin d'identifier les dépendances entre les objets du système d'information.

Comment construire une cartographie du système d'information à usage de la sécurité numérique ?

Les principaux facteurs de succès d'une démarche de cartographie sont son caractère pragmatique, participatif et pérenne. Il est nécessaire que chacune des parties prenantes s'inscrive dans une démarche de cartographie **incrémentale** (enrichissement par de nouvelles vues) et **itérative** (affinement des vues déjà constituées). Il s'agit donc, selon les objectifs et les besoins de l'organisme, de cartographier au fur et à mesure les différentes vues, et d'enrichir les vues déjà décrites en ajoutant des objets, des caractéristiques et des liens de dépendance. Certains détails pourront être temporairement incomplets et affinés lors de l'itération suivante afin de respecter le calendrier du projet.

Afin d'emporter l'adhésion des acteurs, la démarche de construction d'une cartographie doit s'intégrer aux processus de l'organisme et dans le cycle de vie du système d'information. Elle se décompose en 5 étapes, dont la mise en œuvre est directement liée d'une part à la nature du système d'information à cartographier, et d'autre part aux objectifs visés par l'organisme selon son niveau de maturité et les enjeux de sécurité numérique.

Etape n°1 : Comment initier la démarche de cartographie ?

Définir les enjeux de la cartographie, les acteurs à mobiliser, le périmètre du système d'information à représenter, le niveau de granularité de l'inventaire et les types de vues à réaliser, les différentes étapes d'itération et le calendrier associé.

Etape n°2 : Quel modèle dois-je adopter ?

Recenser toutes les informations disponibles en rassemblant les inventaires et schémas de représentation du système d'information déjà constitués. Définir le modèle de représentation de l'inventaire et des différentes vues ainsi qu'une nomenclature pour les différents objets.

Etape n°3 : Quel outillage dois-je utiliser ?

Identifier les outils à utiliser pour la construction de la cartographie et son maintien à jour.

Etape n°4 : Comment construire ma cartographie pas à pas ?

Construire l'inventaire en mettant à jour, le cas échéant, les informations recensées et en les complétant en suivant le modèle défini. Représenter les différentes vues de la cartographie selon le modèle.

Etape n°5 : Comment pérenniser ma cartographie ?

Diffuser et promouvoir la cartographie au sein de l'organisme. Mettre en place un processus de mise à jour de la cartographie et la gouvernance[4] associée.

[4] On entend ici par gouvernance, l'identification des rôles et responsabilités de chacun sur la pérennisation du projet de cartographie et la comitologie permettant de piloter et suivre sa mise à jour.

Table des matières

Etape n°1 : Comment initier la démarche de cartographie ?

Dans la première étape, vous allez définir avec l'ensemble des parties prenantes tous les éléments nécessaires à l'initialisation et au bon déroulement du projet de cartographie.

1 / Identifier les enjeux et les parties prenantes de la construction de la cartographie

En premier lieu, il est nécessaire de définir clairement les objectifs et les enjeux du projet de cartographie, pour répondre aux besoins de l'organisme. Les objectifs du projet de cartographie doivent être validés au niveau d'un sponsor et partagés par toutes les parties prenantes. Le sponsor du projet est un membre de la direction de l'organisme et se positionne à la tête de la gouvernance du projet de cartographie.

Dans le cas où la démarche de cartographie du système d'information est uniquement dédiée à la sécurité numérique, elle implique un nombre limité de parties prenantes. Le responsable de la sécurité des systèmes d'information (RSSI) doit jouer le rôle de coordinateur et se positionner en responsable de la mise en place et du suivi de la démarche.

Dans le cas où l'organisme a l'ambition d'engager une démarche plus globale et complète de cartographie de son système d'information, intégrant les besoins de sécurité numérique, le directeur des systèmes d'information (DSI) peut être responsable du projet et coordonner une équipe comprenant un plus grand nombre de parties prenantes (par exemple, architectes, urbanistes, RSSI, responsables sûreté, etc.), dont il est indispensable de définir clairement les rôles et responsabilités. La mise en place de cette équipe projet doit être accompagnée et soutenue par les directions.

Note : Il est primordial que les équipes SI et SSI travaillent en collaboration pour que le résultat de la cartographie couvre les besoins des deux équipes, et ce, en particulier si le RSSI n'est pas positionné au sein de la DSI. Une cartographie uniquement SSI ne pourra pas être maintenue au fil des évolutions du système d'information. Une cartographie uniquement SI ne sera pas adaptée à l'usage de la sécurité numérique.

2 / Cadrer le périmètre à cartographier

Dans un second temps, il est indispensable de formaliser le périmètre à cartographier afin de s'assurer que toutes les parties prenantes de la démarche partagent la même vision.

Quels que soient les objectifs fixés, il est recommandé de cartographier dans un premier temps les systèmes les plus exposés ou les plus critiques (pour les opérations, pour l'économie de l'entreprise, pour la Nation). Ces systèmes sont les plus sensibles au regard de leurs besoins de sécurité et les plus vulnérables par rapport à leur exposition aux menaces.

3 / Définir la cartographie cible et la trajectoire de construction

La définition de la cible consiste à identifier l'ensemble des vues à réaliser ainsi que leur niveau de granularité. La granularité des différentes vues de la cartographie est à adapter au contexte et aux objectifs recherchés. Elle peut donc varier d'un système d'information à l'autre selon sa criticité ou l'importance accordée à celui-ci.

La trajectoire de construction de la cartographie permet de prévoir les différentes itérations et les grands jalons dans l'avancement de la cartographie. Il est recommandé d'adopter une trajectoire progressive basée sur l'atteinte échelonnée de niveaux de maturité croissante.

La définition de la cible et de la trajectoire permet de déterminer les responsabilités des différentes parties prenantes, d'estimer les ressources à prévoir et de définir le calendrier. Une proposition pour construire la cartographie en atteignant différents stades de maturité est détaillée en annexe 2.

Pour un système d'information de taille importante, il est recommandé de commencer par une cartographie limitée à certaines vues et centrée sur les systèmes critiques ou exposés, qui sera complétée avec d'autres vues par la suite. Pour un système d'information de petite taille, il est envisageable de réaliser une cartographie cumulant plusieurs vues dès le départ.

Etape n°2 : Quel modèle dois-je adopter ?

Durant la deuxième étape, vous allez rassembler l'ensemble des inventaires et schémas de représentation du système d'information déjà constitués. Ensuite, vous allez définir le modèle de représentation de l'inventaire et des différentes vues. En pratique, la définition du modèle s'effectue en parallèle de la collecte afin d'ajuster le modèle en fonction des retours obtenus.

1 / Collecter et analyser les éléments de cartographie existants

L'étude de l'existant contribue à accélérer la démarche de cartographie puisqu'elle permet de rassembler l'ensemble du travail déjà effectué pour constituer une base de départ.

L'organisation d'entretiens individuels avec les acteurs de la sécurité numérique, la conception et l'exploitation du système d'information est l'occasion de présenter la démarche de réalisation d'une cartographie, de recueillir les informations existantes et d'identifier des premiers manques (par rapport au modèle de cartographie construit en parallèle). Il est recommandé de prêter une attention particulière aux actions suivantes :

- recueillir et analyser l'ensemble des documents relatifs à la description du système d'information, aux normes utilisées et à l'inventaire des ressources et des actifs ;
- identifier les outils d'inventaire actuellement en place ;
- identifier les processus existants concernant l'alimentation et la mise à jour des informations patrimoniales;
- identifier les difficultés rencontrées dans la constitution et l'utilisation des précédentes cartographies.

2 / Définir le modèle de cartographie

La définition d'un modèle de cartographie permet à l'organisme de disposer d'un référentiel commun, ce qui assurera le succès de la communication et du partage d'information entre tous les acteurs de l'organisme. Le contenu du modèle varie selon les vues à développer, choisies dans l'étape n°1.

Pour chacune des vues de la cartographie, il convient de choisir les objets et attributs qui seront représentés ainsi que leur format :

- les objets sont un ensemble d'éléments référencés dans la cartographie, qui sont les biens essentiels et les biens supports au sens de la méthode d'analyse de risques EBIOS. Des listes d'objets sont présentées pour chaque vue en annexe 1 : elles contiennent à la fois des objets retrouvés habituellement dans les modèles d'urbanisation, mais aussi des objets répondant spécifiquement à l'usage de la sécurité numérique ;
- les attributs sont des informations essentielles aux futures analyses, dont certaines ont trait à la sécurité numérique. Par exemple, on peut distinguer pour une application son type (développement interne, logiciel, progiciel, …), ses besoins de sécurité ou encore son exposition vis-à-vis de l'extérieur. Le modèle de cartographie doit définir la liste des

attributs correspondant à chaque objet choisi, avec une priorité pour ceux liés à la sécurité numérique. Des listes d'attributs sont présentées pour chaque objet en annexe 1 ;

- enfin, la définition du modèle de cartographie inclut la définition de la représentation graphique attendue pour chaque objet et attribut ainsi que le respect d'une nomenclature permettant de disposer d'informations homogènes. La fonction des objets et attributs doit se traduire dans leur représentation afin de faciliter leur exploitation par la suite.

Etape n°3 : Quel type d'outils dois-je utiliser ?

Dans cette troisième étape, vous allez définir le ou les outils logiciels que vous utiliserez pour mener à bien votre projet de cartographie. Le choix d'un outillage plus ou moins spécialisé dépend du niveau de maturité visé et du contexte.

L'utilisation d'un logiciel spécifique (logiciel de modélisation du système d'information ou logiciel d'architecture d'entreprise) s'avère rapidement indispensable dès lors que le volume de données et/ou le nombre de contributeurs deviennent importants.

Le choix de l'outillage doit répondre aux besoins suivants :

- assurer la collecte des éléments à recueillir ;
- constituer l'inventaire ;
- réaliser les vues et les liens entre les vues ;
- mettre en œuvre et contrôler le processus de maintien à jour de la cartographie.

Il est possible que des outils d'inventaire, de gestion de mouvements matériels ou de modélisation d'infrastructure soient déjà en place dans l'organisme ou que certains systèmes proposent des cartographies sur certains périmètres. L'objectif du projet de cartographie n'est pas de remplacer les outils existants. Il convient, cependant, de s'assurer que les outils en place conviennent toujours aux usages et d'identifier dans quelle mesure ils peuvent être utilisés pour la réalisation du projet de cartographie. Si les outils en place ne conviennent pas, le choix d'un nouvel outil pourra être proposé.

Les outils de modélisation du système d'information permettent, en plus de la réalisation de schémas et d'inventaires, de simplifier les actions de mise à jour et le partage des informations. Par exemple, certains répercutent automatiquement les changements effectués sur les vues dans l'inventaire (et inversement) afin de garantir une cohérence d'ensemble et des interdépendances entre les éléments du système d'information. Les fonctions d'automatisation des processus proposées dans certains logiciels permettent de réaliser des étapes de validation et des relances auprès des acteurs responsables des mises à jour sur un périmètre.

Peu de logiciels permettent de réaliser directement la collecte des informations. Néanmoins, les plus flexibles peuvent s'interfacer avec des outils de collecte informatique (outil de gestion de parc, gestion d'adresses IP, …).

Ainsi, les outils de modélisation du système d'information facilitent la réalisation et permettent un gain de temps important. Ils garantissent la cohérence du contenu et de la représentation des systèmes, tant sur le fond que sur la forme, et facilitent leur lecture. Les cartographies sont également centralisées au sein d'un référentiel unique avec un accès facilité pour les acteurs concernés.

Dans tous les cas, et pour un partage de l'information réussi, il est fortement recommandé[5] que la cartographie soit exportable sur un support électronique, et dans un format qui puisse être lu avec les principaux logiciels bureautiques du marché, en vue d'une utilisation en lecture seule.

[5] Pour les Opérateurs d'Importance Vitale (OIV), cette recommandation devient obligatoire dans le cadre de la règle « cartographie »

Etape n°4 : Comment construire ma cartographie pas à pas ?

Dans la quatrième étape, vous allez réaliser l'inventaire et construire les vues cartographiques à l'aide de l'outillage choisi lors de l'étape précédente et selon la trajectoire définie lors du cadrage.

La réussite d'un projet de cartographie passe notamment par le caractère progressif de la démarche. La construction de l'inventaire et des différentes vues doit être réalisée pas à pas, de manière incrémentale (enrichissement par de nouvelles vues) et itérative (affinement des vues déjà constituées).

Il convient de porter une attention particulière à la sensibilité des informations qui seront contenues dans l'inventaire et dans les vues de la cartographie. Si le besoin de protection le justifie, le chef de projet ou le RSSI peut décider que la cartographie porte une mention de protection[6] (confidentiel entreprise, diffusion restreinte[7] voire classification et protection au titre du secret de la défense nationale[8]).

1 / Réaliser l'inventaire du système d'information

La réalisation de l'inventaire du système d'information se base sur les éléments recueillis durant l'étude de l'existant. L'objectif est de compléter ces informations avec celles qui ont été définies dans le modèle, au cours de l'étape 2.

Pour construire l'inventaire exhaustif des éléments d'une vue, une approche peut consister à explorer les éléments en procédant de proche en proche, en partant d'une liste d'objets et en parcourant les liens de dépendance.

Il est également possible de compléter l'inventaire en s'appuyant sur :

- des entretiens ciblés et préparés sur la base des éléments déjà collectés lors de la phase d'étude de l'existant ;
- des outils de collecte automatique tels que les outils de gestion de parc ou les logiciels de supervision ;
- des données extraites depuis des applications spécifiques (bases de données, tableaux de bord, etc.) ;
- des documents internes, comme par exemple les plans de continuité et de reprise d'activité ou les analyses de risques.

[6] Pour les systèmes d'information d'importance vitale (SIIV), il est spécifié dans la règle « cartographie » que la cartographie dans son ensemble est marquée Diffusion Restreinte, et peut le cas échéant être classée Confidentiel Défense.
[7] Au sens de l'instruction interministérielle n°901 relative à la protection des systèmes d'information sensibles (n°901/SGDSN/ANSSI)
[8] Au sens de l'instruction générale interministérielle n°1300 sur la protection du secret de la défense nationale (n°1300/SGDSN/PSE/PSD)

2 / Construire les vues de la cartographie

Tous les objets et attributs de l'inventaire ne doivent pas forcément être représentés sur les vues de la cartographie : les vues peuvent avoir différents niveaux de granularité. Toutefois, l'exhaustivité des liens entre les objets pivots est importante pour l'analyse des impacts de sécurité numérique. Ces schémas sont généralement les premiers éléments à être exploités lors d'audits ou d'analyses post-incidents car ils permettent une compréhension rapide du système d'information.

Les vues de la cartographie sont générées par des outils dédiés. Il est important de considérer chaque schéma comme un extrait à un instant T et non comme un schéma définitif ou un état final. Dans le cas où une vue non-définie par l'outillage serait nécessaire, il n'est pas recommandé que celle-ci soit réalisée manuellement à partir d'extractions. La plupart des outils possèdent des modules complémentaires ou des extensions : cette voie est à privilégier.

Note : Chaque schéma doit comporter un titre, une date, un numéro de version et une légende.

Pour représenter l'ensemble des éléments qui composent chaque vue, il est possible, comme pour la construction de l'inventaire, de procéder de proche en proche. Un élément ajouté est ainsi immédiatement relié aux éléments déjà représentés. Il est rappelé que la représentation des différents éléments doit respecter le formalisme défini au cours de l'étape 2.

Etape n°5 : Comment pérenniser ma cartographie ?

Les quatre étapes précédentes ont permis de constituer une première vision du patrimoine de l'organisme. Or, une cartographie n'est utile que si elle est communiquée au plus grand nombre et si les informations qu'elle contient sont fiables et à jour. Ainsi, pour être pérenne et conserver sa valeur, la cartographie doit être partagée et revue régulièrement. C'est l'objet de cette cinquième étape.

1 / Communiquer sur la cartographie

Pour être la plus efficace possible, l'étape de communication doit faire partie du processus de mise à jour de la cartographie. Toutefois, il est indispensable de prêter attention à la sensibilité voire au caractère confidentiel de certaines informations. Il est donc recommandé de limiter les accès aux différentes vues de la cartographie, pour que seules les personnes concernées puissent y accéder. Par exemple, les vues d'infrastructure seront accessibles uniquement à la DSI alors que la vue métier pourra être partagée plus largement.

La cartographie doit notamment être tenue à disposition du RSSI et du CERT[9] de l'entité (ou dispositif équivalent). Les Opérateurs d'Importance Vitale doivent également la communiquer à l'ANSSI[10] à sa demande, notamment en cas de besoin de coordination opérationnelle suite à une attaque informatique d'ampleur.

Note : La cartographie du système d'information constitue un bien essentiel de l'organisme. Aussi, des mesures doivent être prises pour garantir sa disponibilité et sa confidentialité :

- *une sauvegarde de la cartographie doit être réalisée régulièrement sur un support de stockage sécurisé. Elle doit notamment être accessible en cas de coupure du réseau. La conservation d'une version papier la plus à jour possible permet de répondre à cet impératif.*
- *la cartographie ne doit pas être stockée sur le système d'information qu'elle représente. En effet, un attaquant qui se serait infiltré dans le SI aurait alors à sa portée toutes les informations concernant l'architecture du système. De plus, les accès à la cartographie doivent être limités aux personnes ayant le besoin d'en connaitre (par exemple, les métiers pour les vues qui les concernent, la DSI, les membres de la cellule de crise) afin de réduire le risque de fuite.*

2 / Tenir la cartographie à jour

Quelles que soient la taille et la nature de l'organisme, il est important de disposer des ressources suffisantes pour maintenir le travail de cartographie réalisé. Ces ressources sont à ajuster selon le stade de maturité. Il est indispensable de définir une fonction spécifique en charge du contrôle des mises à jour, du recueil des besoins d'évolution du modèle et de l'assistance aux équipes contributrices au projet de cartographie.

[9] Computer Emergency Response Team ou équipe de réponse à incidents.
[10] Agence Nationale de la Sécurité des Systèmes d'Information.

Les actions de revue de la cartographie doivent être structurées via un processus d'amélioration continue et une gouvernance bien définis, afin d'éviter notamment l'apparition de versions multiples. Une bonne pratique consiste à instaurer des campagnes de mises à jour régulières, en sollicitant les acteurs concernés pour qu'ils vérifient et actualisent les informations de leur périmètre. Les parties prenantes pourront dans le cadre de la revue de la cartographie répondre aux questions suivantes :

- est-ce que l'on étend le périmètre de la cartographie ?
- est-ce que l'on vise le niveau de maturité supérieur ?
- est-ce que l'on cherche à affiner certaines vues déjà représentées ?
- quel délai est souhaité pour réaliser les prochaines actions ?

Une autre bonne pratique consiste à intégrer une étape de mise à jour de la cartographie dans les projets d'évolution du système d'information.

Facteurs clés de réussite

La construction d'une cartographie peut se révéler complexe et se heurter à des difficultés organisationnelles, humaines, techniques ou calendaires. Les conseils contenus dans cette partie permettront d'aboutir plus facilement à un résultat satisfaisant.

Adopter un mode projet et pérenniser le résultat

La construction de la cartographie doit s'appuyer sur une stratégie de développement fixant des priorités et des objectifs réalistes de contenus et de calendrier, dont la mise en œuvre doit être pilotée en mode projet et supportée par la hiérarchie au plus haut niveau de l'organisme. Afin de favoriser la pérennité de la cartographie, il convient de privilégier une information macroscopique et tenue à jour, par rapport à une information détaillée, entretenue de manière épisodique et au prix d'efforts trop lourds.

Construire la cartographie par itérations

Cartographier à court terme l'ensemble d'un système d'information avec l'exhaustivité des informations utiles et des vues afférentes est souvent très difficile, voire irréalisable. La cartographie doit s'inscrire dans une démarche d'amélioration continue à la fois incrémentale et itérative. Cette démarche permet d'élargir le périmètre de représentation de la cartographie, d'augmenter son niveau de maturité et d'industrialiser toujours davantage les processus engagés afin de répondre aux nouvelles exigences de sécurité numérique.

Adopter un modèle de cartographie comme langage commun

Afin de faciliter le partage d'informations, les parties prenantes doivent s'appuyer sur un langage commun. La définition du modèle de cartographie est une étape structurante de la démarche, qui permet de créer des concepts partagés entre les différents acteurs. Il est essentiel que ces concepts soient clairement définis et adaptés au contexte d'utilisation. Ainsi, chaque partie prenante doit s'être approprié ces définitions sans ambigüité et de manière concrète.

Communiquer à toutes les étapes du projet

La communication au sein d'un projet de cartographie est essentielle quel que soit le stade d'avancement de la démarche. En particulier, il est important de communiquer sur la démarche en début de projet en appuyant sur son utilité et ses objectifs (par exemple, amélioration significative de la maitrise du système d'information, de la réactivité en cas de panne, de la gestion des évolutions du système, etc.) afin de réduire la perception d'une démarche complexe. Cette communication doit permettre de fédérer les acteurs autour de la démarche. Une fois celle-ci aboutie, il est également indispensable de diffuser la cartographie et de la tenir à disposition des équipes qui pourraient en avoir l'usage (selon son niveau de confidentialité).

Entretenir la cartographie

La mise à jour de la cartographie est une étape indispensable de la démarche afin de pouvoir garantir une synchronisation entre les évolutions du système d'information et leur représentation

dans l'inventaire et les vues. Il est donc nécessaire de définir et mettre en place un processus de mise à jour de la cartographie et sa gouvernance afférente. Les actions de revue de la cartographie doivent être réalisées de manière régulière et structurée.

Annexes

Annexe 1 : Définition et contenu des différentes vues

Lors de l'étape d'initialisation de la cartographie, il est indispensable de définir la cible et la trajectoire à suivre pour l'atteindre. Cette annexe définit les différentes vues présentées succinctement lors de l'étape 1 et propose des éléments de contenu pour chacune d'elles. Les éléments proposés pour les différentes vues n'ont pas forcément vocation à tous être représentés sur des schémas.

A chaque élément est associé un niveau de granularité. Trois niveaux de granularité croissants sont adoptés dans ce guide :

- granularité de niveau 1, minimale : informations indispensables ;
- granularité de niveau 2, intermédiaire : informations importantes ;
- granularité de niveau 3, fine : informations utiles.

Les objets et attributs mentionnés dans les différents tableaux de cette annexe, ainsi que les niveaux de granularité associés, sont des propositions cohérentes avec la trajectoire proposée en annexe suivante. Chaque organisme, lors de la définition de sa cible de cartographie et de sa trajectoire, est libre de définir de nouveaux objets ou attributs et de choisir le niveau de granularité de chaque élément, selon ses besoins.

Note : Les attributs mentionnés en bleu sont spécifiques à l'usage de la sécurité numérique.

1 / Vue métier de l'écosystème

La vue métier de l'écosystème décrit l'ensemble des entités ou systèmes qui gravitent autour du système d'information considéré dans le cadre de la cartographie. Cette vue permet à la fois de délimiter le périmètre de la cartographie mais aussi d'avoir une vision d'ensemble de l'écosystème sans se limiter à l'étude individuelle de chaque entité.

Objet	Attribut	Granularité	Objet pivot
Entité ou système	Identification et description	1	
	Type d'entité ou de système (interne, externe : fournisseur, client, etc.)	1	
	Niveau de sécurité (ex : maturité, mesures de sécurité en place ou définies au niveau contractuel – degré de confiance, homologation)	1	
	Liste des processus soutenus	1	Vue 2
	Point de contact sécurité de l'entité (ex : RSSI)	1	
Relation	Nature (fourniture de biens, de services, partenariat commercial, etc.)	1	
	Lien contractuel ou règlementaire	2	
	Niveau d'importance fonctionnelle de la relation	2	

2 / Vue métier du système d'information

La vue métier du système d'information décrit l'ensemble des processus métiers de l'organisme avec les acteurs qui y participent, indépendamment des choix technologiques faits par l'organisme et des ressources mises à sa disposition. La vue métier est essentielle car elle permet de repositionner les éléments techniques dans leur environnement métier et ainsi de comprendre leur contexte d'emploi.

Un processus est décrit de bout en bout depuis l'événement déclencheur jusqu'au résultat final fourni, indépendamment du cloisonnement qui existe dans l'organisme. Pour les processus transverses sous gouvernance de plusieurs entités, une organisation doit être prévue pour les décrire dans leur entièreté en conservant une perception partagée par tous les acteurs.

Dans cette vue sont également recensées les informations de l'organisme, dont certaines peuvent avoir un caractère critique et représenter des cibles de choix lors d'attaques.

Objet	Attribut	Granularité	Objet pivot
Macro-processus	Identification et description	2	
	Eléments entrants et sortants	2	
	Liste des processus qui le composent	2	
	Critères de sécurité (DICT)	2	
	Propriétaire	3	
Processus	Identification et description	1	
	Eléments entrants et sortants		
	Liste des activités qui le composent (ou des opérations qui le composent, si les niveaux de maturité 1 ou 2 [11] sont ciblés)		
	Liste des entités ou systèmes associés		Vue 1
	Liste des applications qui le soutiennent		Vue 3
	Critères de sécurité (DICT)		
	Propriétaire		
Activité	Identification et description	3	
	Liste des opérations qui la composent		
Opération	Identification et description	1	
	Liste des tâches qui la composent	3	
	Liste des acteurs qui interviennent	2	
Tâche	Identification et description	3	
Acteur	Nom et moyens de contact	2	
	Nature : personne, groupe, entité, etc.		
	Type : interne ou externe à l'organisme		
Information	Identification et description	1	
	Propriétaire		
	Administrateur		
	Stockage (type, localisation)		
	Processus lié		
	Critères de sécurité (DICT)		

[11] Tel que défini dans l'annexe 2.

	Sensibilité : donnée à caractère personnel, donnée médicale, donnée classifiée, etc.		

3 / Vue des applications

La vue des applications permet de décrire une partie de ce qui est classiquement appelé le système informatique. Cette vue décrit les solutions technologiques qui supportent les processus métiers, principalement les applications.

Dans le cadre de la vision sécurité numérique, une importance forte est donnée aux flux applicatifs. Cette vue est particulièrement intéressante pour visualiser les échanges d'informations d'un point de vue logiciel. Les modalités d'échange sont ici caractérisées en détail.

Objet	Attribut	Granularité	Objet pivot
Domaine applicatif	Identification et description	2	
	Responsable		
	Liste des blocs applicatifs qui le composent		
Bloc applicatif	Identification et description	2	
	Responsable		
	Liste des applications qui le composent		
Application	Identification et description	1	
	Liste de la (des) entité(s) utilisatrice(s)	2	Vue 1
	Entité responsable de l'exploitation	2	
	Responsable SSI	1	
	Type de technologie : client lourd, web, etc.	1	
	Type d'application : développement interne, logiciel, progiciel, script, plateforme EAI/ESB, etc.	1	
	Volume d'utilisateurs et profils	2	
	Flux associés	1	
	Critères de sécurité (DICT)	1	
	Exposition à l'externe	1	
	Liste des processus utilisant l'application	1	Vue 2
	Liste des services applicatifs délivrés par l'application	2	
	Liste des bases de données utilisées par l'application	1	
	Liste des serveurs logiques soutenant l'application	1	Vue 5
Service applicatif	Identification et description	2	
	Liste des modules qui le composent		
	Flux associés		
Module	Identification et description	2	
	Flux associés		
Base de données	Identification et description	1	
	Liste de la (des) entité(s) utilisatrice(s)	2	Vue 1
	Entité responsable de l'exploitation	2	
	Responsable SSI	1	
	Type de technologie	1	
	Flux associés	1	
	Liste des informations contenues	1	Vue 1
	Critères de sécurité (DICT)	1	

	Exposition à l'externe	1	
Flux	Identification et description	1	
	Emetteur: application, module, base de données, etc.		
	Récepteur : application, module, base de données, etc.		
	Chiffrement		

4 / Vue administration

La vue administration est un cas particulier de la vue des applications. Elle répertorie les périmètres et les niveaux de privilèges des administrateurs.

La représentation schématique de cette vue est utile uniquement si une gestion centralisée des droits d'administration sur les équipements est en place, comportant plusieurs périmètres d'administration. Dans le cas où les droits sur les équipements ne sont gérés que par des comptes locaux, elle est réduite à la constitution d'une liste des comptes et des droits associés pour chaque équipement.

Objet	Attribut	Granularité
Zone d'administration	Identification et description	1
	Groupe d'administrateurs et niveaux de privilèges	
	Liste des éléments contenus dans la zone	
	Liste des secrets associés à l'administration des ressources	
Service d'annuaire d'administration	Identification et description	1
	Solution : Active Directory, Novell, NT4, Samba, etc.	
Forêt Active Directory/ Arborescence LDAP	Identification et description	1
	Domaines appartenant à la forêt/l'arborescence	
	Relations inter-forêts/inter-arbres : domaines, bidirectionnelle, filtrée, transitive, etc.	
Domaine Active Directory/ LDAP	Identification et description	1
	Nombre de contrôleurs de domaines	
	Nombre de comptes utilisateurs rattachés	
	Nombre de machines rattachées	
	Relations inter-domaines : domaines, bidirectionnelle, filtrée, etc.	

5 / Vue des infrastructures logiques

Cette vue correspond à la répartition logique du réseau. Elle illustre le cloisonnement des réseaux et les liens logiques entre eux, en outre, elle répertorie les équipements réseau en charge du trafic.

Les emplacements logiques des équipements de sécurité (IDS, IPS, SIEM, etc.) sont également recensés dans cette vue.

Objet	Attribut	Granularité	Objet pivot
Réseau	Identification et description	1	
	Type de protocole		
	Responsable d'exploitation		
	Responsable SSI		

	Sous-réseaux rattachés		
	Niveau de sensibilité ou de classification		
Sous-réseau	Identification et description	1	
	Adresse/Masque		
	Passerelle		
	Plage d'adresses IP : adresse de début, de fin		
	Méthode d'attribution des IP : fixe ou dynamique		
	Responsable d'exploitation		
	DMZ ou non		
	Liste des sous-réseaux interconnectés		
	Possibilité d'accès sans fil		
Passerelle d'entrée depuis l'extérieur	Caractéristiques techniques	1	
	IP publique et privée		
	Type d'authentification		
Entité extérieure connectée	Nom, Responsable SSI, contacts SI	2	
	Réseaux internes interconnectés à l'entité		
Commutateur (switch)	Identification : identifiant et adresse IP	1	
	Caractéristiques techniques : modèle, version du logiciel embarqué	1	
	Règles de filtrage des flux réseaux	2	
	Equipement physique de support (si virtualisé)	2	Vue 6
Routeur	Identification : identifiant et adresse IP	1	
	Caractéristiques techniques : modèle, version du logiciel embarqué	1	
	Règles de filtrage des flux réseaux	2	
	Equipement physique de support (si virtualisé)	2	Vue 6
Equipement de sécurité	Identification (identifiant, adresse IP, adresse MAC) et description	1	
	Caractéristiques techniques : modèle, OS et version, version du logiciel embarqué	1	
	Equipement physique de support (si virtualisé)	2	Vue 6
Serveur DHCP	Identification (identifiant, adresse IP si fixe, adresse MAC) et description	2	
	Caractéristiques techniques : modèle, OS et version		
	Serveur physique de support (si machine virtuelle)		Vue 6
Serveur DNS	Identification (identifiant, adresse IP si fixe, adresse MAC) et description	2	
	Caractéristiques techniques : modèle, OS et version		
	Serveur physique de support (si machine virtuelle)		Vue 6
Serveur logique	Identification (identifiant, adresse IP, adresse MAC) et description	1	
	Caractéristiques techniques : modèle, OS et version	1	
	Services réseaux actifs		
	Serveur physique de support	2	Vue 6
	Applications liées	1	Vue 3

6 / Vue des infrastructures physiques

La vue des infrastructures physiques permet de décrire les équipements physiques qui composent le système d'information ou qui sont utilisés par celui-ci. Cette vue correspond à la répartition géographique des équipements réseaux au sein des différents sites de l'organisme. Elle offre une vision d'ensemble des actifs connectés au réseau de télécommunication de l'entreprise.

Objet	Attribut	Granularité	Objet pivot
Site	Identification et description	1	
	Bâtiments rattachés		
Bâtiment/Salle	Identification et description	1	
	Baies rattachées		
Baie	Identification et description	1	
	Liste des machines hébergées		
Serveur physique	Identification : identifiant, adresse IP, nom DNS	1	
	Caractéristiques techniques : type, modèle, OS et version		
	Emplacement physique : site, bâtiment, salle, baie		
	Serveur(s) logique(s) rattaché(s)		Vue 5
	Liste des commutateurs reliés		
	Responsable d'exploitation		
Poste de travail	Identification	2	
	Caractéristiques techniques : type (fixe ou portable), modèle, OS et version		
	Emplacement physique : site, bâtiment, salle		
Infrastructure de stockage	Identification	2	
	Caractéristiques techniques : type (NAS, SAN, disque dur, etc.), modèle		
	Emplacement physique : site, bâtiment, salle, baie		
Périphérique	Identification	2	
	Caractéristiques techniques : type (imprimante, scanner, etc.), modèle		
	Responsable d'exploitation		
Téléphone	Identification	2	
	Caractéristiques techniques : type (fixe ou portable), modèle		
	Emplacement physique : site, bâtiment, salle		
Commutateur physique	Identification	1	
	Commutateur(s) logique(s) rattaché(s)		Vue 5
	Caractéristiques techniques : niveau (L1, L2, L3, etc.), modèle, version du logiciel embarqué		
	Emplacement physique : site, bâtiment, salle, baie		
	VLAN associé		
Routeur physique	Identification	1	
	Routeur logique associé		Vue 5
	Caractéristiques techniques : modèle, version du logiciel embarqué		
	Emplacement physique : site, bâtiment, salle, baie		
	VLAN associé		

Borne wifi	Identification	2	
	Caractéristiques techniques : modèle		
	Emplacement physique : site, bâtiment, salle, baie		
Equipement de sécurité physique	Identification et description	1	
	Equipement(s) de sécurité logique(s) rattaché(s)		Vue 5
	Caractéristiques techniques : type d'équipement (sonde, pare-feu, SIEM, etc.), modèle, OS et version, version du logiciel embarqué, adresse IP, adresse MAC		
	Emplacement physique : site, bâtiment, salle		
WAN	Identification	1	
	MAN ou LAN rattachés		
MAN	Identification	1	
	LAN rattachés		
LAN	Identification	1	
VLAN	Identification et description	1	
	Commutateurs associés		

Annexe 2 : Proposition de cible et de trajectoire de construction de la cartographie

La première étape d'initialisation de la démarche permet notamment de définir la cartographie cible et la trajectoire de sa construction. Cette annexe propose un exemple de cible et de trajectoire pour construire la cartographie en atteignant différents stades de maturité.

Lors de la définition des objectifs de la cartographie, il est possible de s'orienter vers une démarche uniquement dédiée à la sécurité numérique, pilotée par le RSSI, ou une démarche plus globale pilotée par le DSI qui répond à l'ensemble des besoins liés à la cartographie. Les besoins du projet de cartographie doivent être validés au niveau d'un sponsor, membre de la direction de l'organisme.

Le niveau de maturité cible est ensuite défini en adéquation avec le choix de démarche projet :

- Maturité de niveau 1 : la démarche vise à élaborer une cartographie comprenant les premiers éléments indispensables aux opérations de sécurité numérique. Ce niveau est considéré comme une **étape intermédiaire**, centrée sur un nombre limité de vues, pour aboutir de manière progressive au niveau de maturité 2 ;
- Niveau de maturité 2 : la démarche vise à élaborer une cartographie dédiée à la sécurité numérique dans laquelle l'ensemble des vues sont représentées. Les systèmes d'information d'importance vitale (SIIV) doivent disposer d'une cartographie ayant ce niveau de maturité *a minima* ;
- Niveau de maturité 3 : la démarche vise à élaborer une cartographie exhaustive et détaillée, qui intègre les besoins de sécurité numérique. Le niveau de granularité des différentes vues est plus fin de manière à obtenir une vision complète du système d'information.

Le tableau ci-dessous présente les informations collectées pour chaque niveau de maturité.

Objets/Attributs concernés	Démarche de cartographie dédiée à la sécurité numérique		Démarche globale de cartographie
	Maturité de niveau 1	Maturité de niveau 2	Maturité de niveau 3
Vue métier de l'écosystème			
Granularité 1	X	X	X
Granularité 2			X
Vue métier du système			
Granularité 1	X	X	X
Granularité 2		X	X
Granularité 3			X
Vue des applications			
Granularité 1	X	X	X
Granularité 2			X
Vue administration			
Granularité 1		X	X
Vue des infrastructures logiques			

Granularité 1	X	X	X
Granularité 2		X	X
Vue des infrastructures physiques			
Granularité 1		X	X
Granularité 2			X

Annexe 3 : Glossaire

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
Bien essentiel	Information ou processus jugé comme important pour l'organisme
Bien support	Bien sur lequel reposent les biens essentiels. On distingue notamment les systèmes informatiques, les organisations et les locaux
DICT	Critères de sécurité : Disponibilité, Intégrité, Confidentialité, Traçabilité
DMZ	*Demilitarized zone* – Zone réseau isolée à la fois du réseau interne et du réseau externe, contenant les services accessibles depuis l'extérieur
DSI (le/la)	Directeur/Direction du Système d'Information
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité – Méthode d'analyse de risques cyber proposée par l'ANSSI
LPM	Loi de Programmation Militaire – Outil législatif qui va permettre aux Opérateurs d'Importance Vitale pour la Nation de mieux se protéger et à l'ANSSI de mieux les soutenir en cas d'attaque informatique
OIV	Opérateur d'Importance Vitale – Opérateur public ou privé dont les activités sont indispensables au bon fonctionnement et à la survie de la Nation
RSSI	Responsable de la Sécurité du Système d'Information
Service d'annuaire d'administration	Applicatif regroupant les données sur les utilisateurs ou équipements informatiques de l'entreprise et permettant leur administration
SIIV	Systèmes d'Information d'Importance Vitale – Systèmes pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation
Zone d'administration	Ensemble de ressources (personnes, données, équipements) sous la responsabilité d'un (ou plusieurs) administrateur(s)