

ARCHITECTURES ET DÉPLOIEMENT DE SUPERVISION DE SÉCURITÉ

GUIDE ANSSI

ANSSI-PG-TBD
19/03/2026

PUBLIC VISÉ :

Développeur

Administrateur

RSSI

DSI

Utilisateur

DOCUMENT DE TRAVAIL

Informations



Attention

Ce document rédigé par l'ANSSI s'intitule « **Architectures et déploiement de supervision de sécurité** ». Il est téléchargeable sur le site cyber.gouv.fr.

Il constitue une production originale de l'ANSSI placée sous le régime de la « Licence Ouverte v2.0 » publiée par la mission Etalab.

Conformément à la Licence Ouverte v2.0, le document peut être réutilisé librement, sous réserve de mentionner sa paternité (source et date de la dernière mise à jour). La réutilisation s'entend du droit de communiquer, diffuser, redistribuer, publier, transmettre, reproduire, copier, adapter, modifier, extraire, transformer et exploiter, y compris à des fins commerciales. Sauf disposition réglementaire contraire, les recommandations n'ont pas de caractère normatif; elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Évolutions du document :

| VERSION | DATE | NATURE DES MODIFICATIONS |
|---------|------------|--|
| 0.9 | 19/03/2026 | Version pour appel public à commentaires |

Table des matières

| | | |
|----------|---|-----------|
| 1 | Introduction | 4 |
| 1.1 | Objectif du guide | 5 |
| 1.2 | Organisation du guide | 5 |
| 2 | Composants d'architecture pour la supervision de sécurité | 6 |
| 2.1 | SI supervisé | 6 |
| 2.1.1 | Modèle de ressources techniques d'un SI | 7 |
| 2.1.2 | Modèle de responsabilités opérationnelles | 8 |
| 2.1.3 | Périmètres de responsabilité | 8 |
| 2.1.4 | Contraintes des périmètres de responsabilité sur la supervision | 9 |
| 2.2 | SI de supervision de sécurité | 12 |
| 2.2.1 | Types de supervision de sécurité | 13 |
| 2.2.2 | Fonctions internes de la supervision de sécurité | 15 |
| 2.2.3 | Contraintes des fonctions de supervision sur l'architecture | 16 |
| 2.2.4 | Interfaces entre les fonctions | 17 |
| 2.2.5 | Contraintes de sécurité sur les interfaces entre les fonctions | 18 |
| 2.3 | SI d'administration | 20 |
| 2.3.1 | SI d'administration du SI supervisé | 20 |
| 2.3.2 | SI d'administration du SI de supervision | 21 |
| 2.4 | L'hypervision de sécurité | 22 |
| 2.5 | La supervision multimétiers | 22 |
| 3 | Architectures de supervision de sécurité dédiée | 23 |
| 3.1 | Supervision dédiée sur site | 23 |
| 3.1.1 | Architecture sur site | 23 |
| 3.1.2 | Enjeu : mutualisation de moyens entre les SI de supervision et d'administration | 24 |
| 3.1.3 | Cas d'usage identifiés | 25 |
| 3.2 | Supervision dédiée dans le cloud | 25 |
| 3.2.1 | Architecture avec outils de supervision opérés par le client | 26 |
| 3.2.2 | Enjeu : accès distant des analystes | 27 |
| 3.2.3 | Architecture avec outils de supervision opérés par le fournisseur | 27 |
| 3.2.4 | Enjeu : réversibilité vis-à-vis du fournisseur | 28 |
| 3.2.5 | Cas d'usage identifiés | 28 |
| 3.3 | Supervision dédiée à distance | 29 |
| 3.3.1 | Architecture entre des infrastructures distantes | 29 |
| 3.3.2 | Enjeu : distance entre les fonctions | 30 |
| 3.3.3 | Cas d'usage identifiés | 30 |
| 3.4 | Supervision dédiée multimétiers | 30 |
| 3.4.1 | Enjeu : topologie de collecte complexe | 30 |
| 3.4.2 | Cas d'usage identifiés | 30 |
| 4 | Architectures de supervision de sécurité mutualisée | 31 |
| 4.1 | Supervision mutualisée sur site | 31 |
| 4.1.1 | Architecture mutualisée interne | 31 |

| | | |
|----------------------|---|-----------|
| 4.1.2 | Enjeu : séparation des données | 32 |
| 4.1.3 | Cas d'usage identifiés | 32 |
| 4.2 | Supervision mutualisée à distance | 32 |
| 4.2.1 | Architecture mutualisée distante | 32 |
| 4.2.2 | Enjeu : latéralisation entre SI supervisés | 33 |
| 4.2.3 | Cas d'usage identifiés | 33 |
| 4.3 | Supervision mutualisée externalisée | 33 |
| 4.3.1 | Architecture de supervision par un tiers | 33 |
| 4.3.2 | Enjeu : gestion de la complexité du modèle de responsabilité | 34 |
| 4.3.3 | Cas d'usage identifiés | 34 |
| 5 | Architectures composites de supervision de sécurité | 35 |
| 5.1 | Utiliser une supervision dédiée sur chaque infrastructure | 35 |
| 5.1.1 | Architecture de supervision distribuée | 35 |
| 5.1.2 | Enjeu : maintenir la proximité de la supervision de sécurité en environnement complexe | 36 |
| 5.1.3 | Cas d'usage identifiés | 36 |
| 5.2 | Combiner plusieurs supervisions dédiées et l'hypervision | 37 |
| 5.2.1 | Architecture de supervision distribuée avec hypervision | 37 |
| 5.2.2 | Enjeu : équilibrer les besoins d'une vue unique avec les besoins en sécurité des différents SI supervisés | 37 |
| 5.2.3 | Cas d'usage identifiés | 38 |
| 5.3 | Combiner la supervision dédiée, la supervision distante et l'hypervision | 38 |
| 5.3.1 | Architecture de supervision mixte | 38 |
| 5.3.2 | Enjeu : maîtrise des coûts en environnement complexe | 39 |
| 5.3.3 | Cas d'usage identifiés | 39 |
| 5.4 | Combiner plusieurs niveaux de supervision | 39 |
| 5.4.1 | Architecture de supervision à deux niveaux | 39 |
| 5.4.2 | Enjeu : spécialisation de la supervision | 40 |
| 5.4.3 | Cas d'usage identifiés | 40 |
| 5.5 | Concevoir une supervision renforcée | 41 |
| 5.5.1 | Enjeu : privilégier les contraintes cyber pour la supervision de certains périmètres | 41 |
| 5.5.2 | Cas d'usage identifiés | 41 |
| Annexe A | Légende des visuels | 42 |
| A.1 | Forme des contours | 42 |
| A.2 | Couleur des contours | 42 |
| A.3 | Couleur des fonds | 42 |
| Bibliographie | | 43 |

1

Introduction



Attention

L'ANSSI lance un appel à commentaires public sur les architectures de supervision, ayant vocation à alimenter son chantier de construction de doctrine en la matière. Le présent guide est le support de cet appel à commentaires. À ce titre, il est présenté dans un état non finalisé. En particulier, les recommandations ne sont que des ébauches. De même, les enjeux seront étoffés et détailleront la mise en œuvre de certaines recommandations afin d'atteindre un objectif spécifique.

L'ANSSI publie une collection de guides sur la supervision de sécurité. Cette collection a vocation à décrire les principes de fonctionnement et les bonnes pratiques autour de la recherche et la découverte d'incidents de sécurité au sein des systèmes d'information (SI).

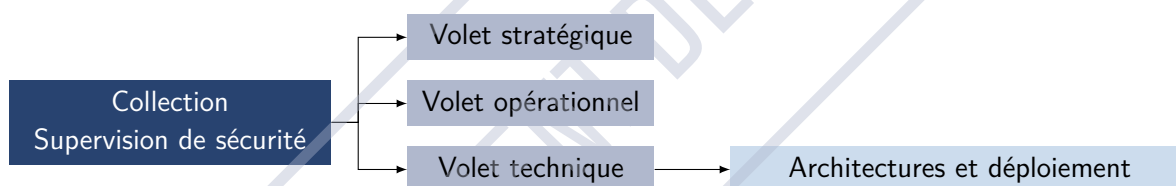


FIGURE 1 – Collection de guides sur la supervision de sécurité

Comme le montre la figure 1, le présent document fait partie du volet technique. Il propose des modèles d'architecture de SI de supervision de sécurité adaptés à diverses options de déploiement.



Attention

Ce guide présente des orientations possibles pour répondre aux exigences des SI de supervision de sécurité. Les propositions d'architecture sont des aides à la conception ou à l'analyse, elles n'ont donc pas vocation à être instanciées en l'état.

En premier lieu, les composants architecturaux de base sont détaillés pour permettre de comprendre la construction d'un SI de manière générale, et d'un SI de supervision en particulier. Des recommandations sont données pour la sécurité du SI de supervision. En second lieu, des modèles d'architecture permettent d'aborder de manière progressive, la multiplicité des enjeux qui se présentent pour adapter un SI de supervision au(x) SI qu'il doit superviser. L'introduction de chaque nouvel enjeu permet de montrer comment les recommandations précédentes peuvent être mises en œuvre.

1.1 Objectif du guide

La supervision de sécurité est définie¹ comme l'ensemble des moyens et des activités concourant, dans les meilleurs délais, à la détection et à la qualification d'un incident de sécurité sur un périmètre supervisé, ainsi qu'au choix de la réaction appropriée lorsque cet incident est avéré. Ces moyens peuvent être humains, organisationnels, techniques et financiers.

Ce guide s'intéresse spécifiquement aux moyens techniques. Certes, le guide « Piloter un projet de supervision » [3] recommande de « commencer à superviser avec les moyens en place ». Cependant, il est un moment où le déploiement de moyens dédiés à la supervision de sécurité devient incontournable.

Le présent guide vient en complément de la section 3.6 du guide « Piloter un projet de supervision » [3], qui présente succinctement le SI de supervision. Il offre des modèles d'architecture pour répondre aux principaux cas de déploiement.

Plutôt que de cataloguer des possibilités infinies qui s'offrent à qui souhaite créer ou comprendre une supervision de sécurité, ce guide s'attache à présenter des briques de base permettant de construire un système de supervision adapté au contexte spécifique de l'entité.

Ces mêmes briques peuvent également être utilisées pour morceler un système complexe existant en sous-systèmes plus simples à appréhender, et rapporter des systèmes existants à des cas connus. Par exemple, pour une supervision complexe dans son ensemble, il est possible de reconnaître localement des parties de supervision dédiées, d'autres mutualisées et, à une échelle plus large, un modèle composite connu ou qui mériterait d'être décrit.

1.2 Organisation du guide

Le chapitre 2 présente les briques de bases et les contraintes auxquelles un SI de supervision est soumis.

Les chapitres 3, 4 et 5 proposent des pistes permettant de résoudre ces contraintes, en s'appuyant sur des scénarios de déploiement. Ces scénarios ont été choisis pour présenter les problématiques et les pistes de solutions de manière progressive. Il est à noter que ces problématiques vont souvent se cumuler dans des déploiements réels. Cela signifie que les pistes de solutions sont avant tout des aides à la réflexion plutôt que des objectifs en soi.

1. Voir le guide « Supervision de sécurité - Piloter un projet de supervision » [3] de l'ANSSI.

2

Composants d'architecture pour la supervision de sécurité

Les contraintes architecturales qui pèsent sur un SI de supervision dérivent en premier lieu de la physionomie du SI supervisé et, en second lieu, des choix de conception retenus pour le SI de supervision. Le présent chapitre détaille la conception des SI et la notion d'externalisation, qui influence la physionomie des SI supervisés. Il présente également le SI de supervision et les impacts de l'externalisation sur son fonctionnement. Il aborde également des composants essentiels tels que le SI d'administration et l'hypervision de sécurité. Enfin, un cas spécifique de fonctionnement est présenté au travers de la supervision multi-métier.

2.1 SI supervisé

La raison d'être de la supervision de sécurité est de surveiller l'activité d'un ou de plusieurs SI, que l'on qualifie de SI supervisés. Pour rappel, la supervision de sécurité est une mesure de sécurité défensive qui permet d'identifier une attaque, qui aide à en comprendre les conséquences et enfin, qui assiste dans la reprise de contrôle du SI attaqué.

Dans certains cas, le SI supervisé peut se résumer à quelques postes qui accèdent à un serveur de fichiers partagés. Dans ce cas, la compréhension du fonctionnement technique et organisationnel est très simple. En revanche, il arrive souvent que le SI supervisé soit très complexe, construit en couches successives, chacune suivant un schéma de délégation spécifique. Adopter un niveau d'analyse pertinent pour mettre sous supervision ces SI complexes nécessite la mise à disposition de modèles adaptés.

Cette section présente les contraintes d'architectures qui pèsent sur des SI, et par conséquent sur leur supervision de sécurité. Deux modèles simplifiés y sont proposés. L'un représente les ressources d'un SI, tandis que l'autre représente les délégations possibles sur ces ressources.



Systeme d'information

Un système d'information (SI) est :

- un ensemble défini de ressources (humaines, techniques, organisationnelles, financières),
- soumis à des besoins (métiers, opérationnels, sécuritaires),
- dont la satisfaction repose sur des responsables identifiés.

2.1.1 Modèle de ressources techniques d'un SI

La définition d'un SI nous montre que ses ressources sont de plusieurs types. Au sein des ressources techniques, toutes ne sont pas uniformes : ni de même importance, ni de même sensibilité, ni de même niveau de dépendance.

Pour qu'un besoin métier soit satisfait (ex. : la gestion des RH), il faut un ensemble de fonctionnalités utilisables par des utilisateurs (ex. : une application). Cette **ressource applicative** peut dépendre de **ressources logiques** pour fonctionner dans de bonnes conditions de disponibilité (ex. : des conteneurs, des machines virtuelles, des réseaux virtuels, des services comme le stockage de données ou de fichiers). Ces ressources logiques dépendent elles-mêmes de **ressources physiques** (ex. : des serveurs spécialisés pour le calcul ou le stockage dans un centre de données, des liens réseau physiques et les équipements associés).

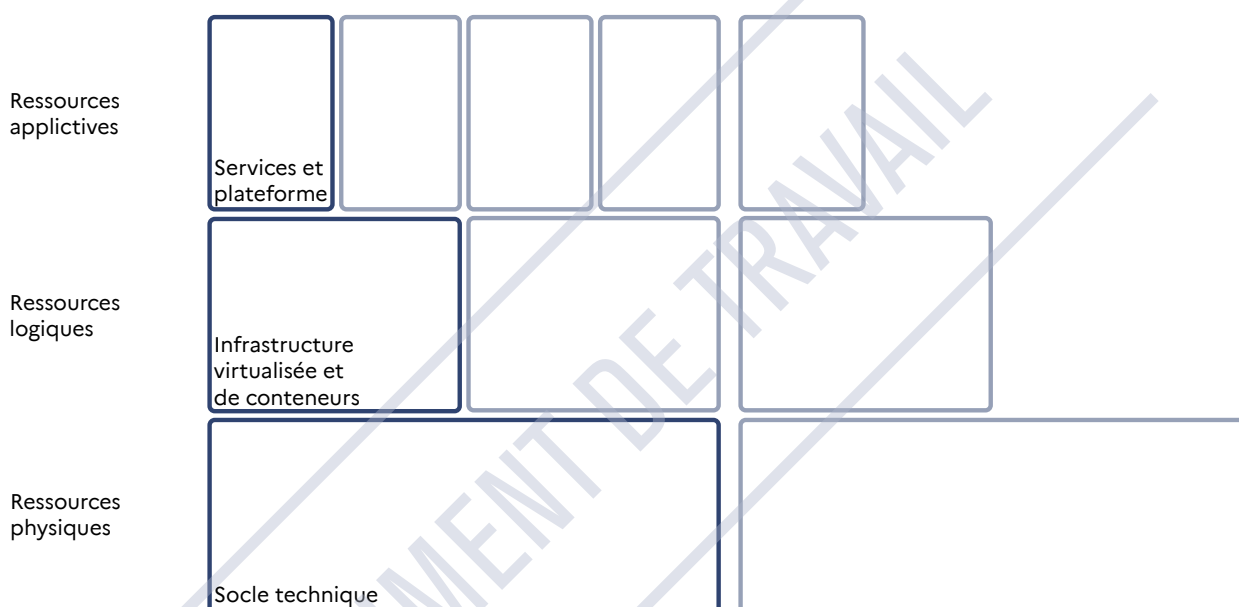


FIGURE 2 – Modèle de dépendance des ressources techniques d'un SI

De plus, ces dépendances sont « pyramidales » ou englobantes. Par exemple, une ressource logique (une machine virtuelle) qui s'exécute sur un hyperviseur dépend bien sûr du serveur physique sur lequel elle s'exécute, mais aussi de toute l'infrastructure de virtualisation et de stockage qui entoure ce serveur, et lui permet de fonctionner. Enfin, ces dépendances sont transitives. Par exemple, l'application RH installée sur une machine virtuelle dépend de fait de l'ensemble de l'infrastructure de virtualisation.

Les ressources applicatives, logiques et physiques constituent une grille de lecture simplifiée du fonctionnement des SI. Cette grille aide à comprendre les interactions en cas de délégation de responsabilités. Par exemple, clarifier les responsabilités que l'on devrait exiger d'un fournisseur de ressources physiques dont dépendent les ressources logiques que l'on opère.

En revanche, si ce modèle permet de couvrir la majorité des cas de délégation de responsabilités, les cas spécifiques doivent être interprétés de manière plus fine. Par exemple, une entité qui maîtrise les ressources sous-jacentes aux ressources physiques (ex. : un bâtiment abritant une salle serveur

ou un centre de données) doit approfondir des aspects spécifiques tels que les alimentations en énergie, leur redondance et la continuité en cas de coupure de ces alimentations, le refroidissement, les accès physiques, les adductions réseau... Certains de ces éléments sont considérés comme des SI industriels, et leur couverture complexifie d'autant le SI de supervision de sécurité.

2.1.2 Modèle de responsabilités opérationnelles

Du point de vue de l'architecture, le recours à l'externalisation implique de se demander « Qui fait où ? » La gestion des ressources techniques est-elle maîtrisée par l'entité, ou déléguée à un prestataire ? Le prestataire intervient-il sur site ou à distance ? Les ressources techniques sont-elles sur un site de l'entité, sur un site du prestataire ou hébergé par un tiers ?

Le présent paragraphe s'intéresse à la notion de responsabilité opérationnelle, c'est-à-dire la responsabilité de l'exploitation des ressources. En d'autres termes, la façon dont on garantit le fonctionnement de ressources informatiques, quel que soit le type de délégation et d'externalisation auquel elles sont soumises. Différentes modalités peuvent être identifiées pour répartir la responsabilité et la localisation de l'exploitation des ressources techniques :

- la maîtrise interne : l'entité gestionnaire du SI (ex. : la DSI) assure par elle-même l'hébergement et les opérations (p. ex. : messagerie électronique).
- la délégation interne : l'entité gestionnaire du SI assure l'hébergement et délègue tout ou partie des opérations (p. ex. : la tierce maintenance applicative ou l'infogérance des postes de travail).
- la délégation externe : l'entité gestionnaire du SI délègue tout ou partie de l'hébergement et des opérations (p. ex. : location d'emplacements et de liens réseau dans un centre de données).
- le cloud : Il met à disposition des ressources techniques, et permet à l'utilisateur de provisionner, configurer et supprimer ces ressources en autonomie. Ce type de délégation peut être interne ou externe.

Là encore, ce modèle ne rend pas compte de toute la complexité de la délégation, mais permet de balayer de manière simple la plupart des cas rencontrés.



Attention

La mutualisation de ressources techniques n'est envisageable que pour des ressources dont on a la responsabilité opérationnelle. Par exemple, il n'est pas possible de mutualiser des ressources entre un SI d'administration et un SI de supervision si l'un des deux est externalisé. De plus, la mutualisation n'est possible que si elle n'impacte pas les besoins de sécurité de l'un ou l'autre des SI dont on souhaite mutualiser des ressources. C'est pourquoi il est important d'analyser les risques de la mutualisation, et d'envisager la mutualisation ressource par ressource, et non SI par SI.

2.1.3 Périmètres de responsabilité

Lorsqu'un SI dépasse une masse critique, il devient très complexe pour l'entité gestionnaire de le maîtriser uniformément. Il est très fréquent que les ressources soient découpées en périmètres,

qui correspondent souvent aux périmètres de responsabilité d'une entité. Par exemple, la DSI peut maintenir en interne la responsabilité des éléments techniques du SIRH, et externaliser la responsabilité des éléments techniques relatifs au site institutionnel.

Plus largement, chaque niveau de ressources (physiques, logiques ou applicatives) est découpé en périmètres et la responsabilité sur ces périmètres peut être déléguée de manière indépendante. Par exemple, certaines ressources physiques peuvent se trouver dans le bâtiment qui accueille les utilisateurs, tandis que d'autres sont louées dans un centre de données, et que d'autres encore sont incluses dans des offres *cloud* de type IaaS ou SaaS.



SI supervisé

Un SI supervisé, ou périmètre supervisé, est un sous-ensemble cohérent d'un SI, composé de ressources techniques relevant d'un responsable identifié et pour lequel des moyens de supervision de sécurité sont mis en œuvre.



FIGURE 3 – Représentation type d'un SI supervisé

2.1.4 Contraintes des périmètres de responsabilité sur la supervision

Pour rappel, l'analyse permettant de découper un SI en périmètres de responsabilité repose sur les modalités de délégations et d'externalisation. De plus, elle est implicitement orientée vers les responsabilités relatives à l'exploitation des ressources.

Puisque ce guide traite de la supervision de sécurité, il est également nécessaire de s'intéresser à la manière de surveiller l'activité de ces périmètres de manière cohérente. En somme, réussir à savoir, malgré le modèle de délégation et d'externalisation, si un périmètre est attaqué.

Pour y parvenir, il est nécessaire de traiter deux niveaux distincts. Le premier concerne les ressources que l'entité exploite elle-même. Le second concerne les ressources sous-jacentes dont l'entité a délégué l'exploitation.

Concernant les ressources dont l'entité a la responsabilité, elles peuvent être sur site, ou éventuellement dépendre d'autres ressources hébergées par un prestataire. C'est tout l'enjeu du présent guide que d'identifier des pistes permettant de traiter au mieux une large variété de cas.

R

Superviser la sécurité des ressources dont on a la responsabilité

Il est recommandé que l'entité conçoive et mette en œuvre une stratégie de supervision adaptée à l'ensemble des ressources dont elle a la responsabilité. L'entité peut choisir de déléguer la responsabilité de la supervision indépendamment de la responsabilité opérationnelle. La délégation ne soustrait pas l'entité à ses obligations

légales et réglementaires.



Attention

Une entité n'est légitime à superviser que les ressources dont elle a la responsabilité opérationnelle. Cela signifie que dans le cadre de ressources mutualisées entre différentes entités (par exemple, plusieurs clients hébergés sur une même infrastructure de virtualisation cloud), les différentes entités ne pourront pas superviser les ressources dont elles dépendent (dans notre exemple, l'infrastructure de virtualisation). Elles ne pourront superviser que les ressources mises à disposition, et dont elles ont la responsabilité (toujours dans notre exemple, des machines virtuelles qu'elles opèrent elles-mêmes, ainsi que les données et les applications qui en dépendent). En effet, la supervision des ressources mutualisées divulgue des informations sur toutes les ressources qui en dépendent. Par conséquent, la supervision de ces ressources est du ressort exclusif du prestataire qui opère cette ressource (dans notre exemple, le fournisseur cloud).

Concernant les ressources dont l'entité a délégué la responsabilité, il s'agit surtout de traiter la façon dont ces responsabilités sont déléguées pour un ensemble de ressources. L'entité doit notamment s'assurer que les garanties apportées par la supervision de sécurité des ressources déléguées correspond à ses besoins.

R

Vérifier les conditions de supervision de sécurité des ressources externalisées

Puisque l'on ne peut superviser que des ressources dont on a la responsabilité, un enjeu de la délégation consiste à s'assurer que la supervision de sécurité réalisée par le fournisseur sur ses ressources (les ressources louées et les ressources sous-jacentes) est réalisée dans des conditions qui conviennent au commanditaire.

Pour chaque périmètre délégué, le commanditaire est responsable du choix du prestataire et du respect, par ce dernier, des éventuelles obligations réglementaires auxquelles il est soumis. Pour déléguer tout en remplissant ses obligations, une entité doit appliquer les quatre recommandations suivantes.

R

S'assurer que les obligations légales et réglementaires auxquelles l'entité est soumise sont compatibles avec la délégation, et que les offres des prestataires sont susceptibles de répondre au besoin dans le respect de ces obligations

En particulier, pour la supervision de sécurité, il faut s'assurer que les ressources mises à disposition par le fournisseur ainsi que les ressources sous-jacentes bénéficient d'une supervision de sécurité répondant aux obligations légales et réglementaires du commanditaire.

R

Choisir le prestataire de manière éclairée, en comparant les besoins et les contraintes de l'entité, avec l'offre commerciale et technique du prestataire, le contrat-type et le cas échéant, les conditions générales d'utilisation

En ce qui concerne la supervision de sécurité, cela signifie qu'il faut s'intéresser aux ressources du prestataire qui sont supervisées et au niveau de supervision réalisée (ex. : conformité au référentiel d'exigences PDIS). Il peut également être utile de comprendre quelles informations sont partagées avec le commanditaire (ex. : incidents avérés pour certains niveaux de gravité) et quels éléments techniques sont mis à sa disposition (ex. : tableau de bord, console de gestion d'événements de sécurité).

R

Négocier le report d'obligations sous forme de clauses contractuelles.

Si des éléments de supervision de sécurité ne sont pas alignés avec le besoin, ils peuvent potentiellement être négociés avec le fournisseur. C'est le vecteur privilégié pour amener un fournisseur à fournir un niveau d'assurance quant au niveau de la supervision qu'il réalise sur les ressources qu'il loue et les ressources sous-jacentes (par exemple, la conformité de la supervision de sécurité au référentiel d'exigences PDIS). Cependant, il s'agit d'une négociation dans la mesure où le prestataire est libre d'accepter ces clauses, de les refuser, ou encore de proposer des contreparties (ex. : financières).

i

Information

Le prestataire n'est tenu d'exécuter que ce pour quoi il s'est engagé contractuellement avec le client. Le client peut essayer de négocier des clauses différentes de celles figurant au contrat type. L'influence que peut avoir le client dans une telle négociation est proportionnelle à l'intérêt du fournisseur à satisfaire les demandes du client (ex. : compensations financières, importance du contrat relativement au chiffre d'affaires du prestataire, gain d'image, pénétration d'un marché). Cette négociation disparaît dans de très nombreux cas d'utilisation du cloud ; elle est remplacée par l'acceptation de clauses générales d'utilisations à l'inscription sur la plateforme. Cela change totalement la nature de la relation entre l'entité et son prestataire, en particulier dans la satisfaction d'un besoin client concernant les fonctions de sécurité telles que la supervision de sécurité.

R

Reporter dans l'analyse de risque toute disposition de la politique de sécurité qui n'est pas entièrement couverte par le service du prestataire et accepter les risques résiduels qui en découlent

Tout élément ou contrainte de la supervision de sécurité qui n'est pas satisfait par le fournisseur de manière satisfaisante fait l'objet d'un report de risque dans l'analyse de risque et, le cas échéant, de risques résiduels que le commanditaire doit accepter.

i

Information

Lorsqu'une entité choisit de déléguer, elle garde toujours la responsabilité d'endosser les risques résiduels, quels que soient le niveau et le type de délégation ou de transfert

de responsabilité qu'elle a mis en place. Dans le domaine de la cybersécurité, l'un des apports de l'analyse de risque est l'évaluation objective de ce risque résiduel afin d'en conserver la maîtrise.

2.2 SI de supervision de sécurité

Comme il a été rappelé en introduction, il est recommandé de « commencer à superviser avec les moyens en place ». Pour autant, ce guide aide à construire une architecture à partir du moment où des moyens dédiés à la supervision de sécurité sont nécessaires.

Le terme de « SI de supervision » est à comprendre de manière extensive : il désigne aussi bien un SI déjà organisé et mature, qu'un petit nombre de ressources préexistantes qui sont la base d'un futur SI.

Cependant, le présent guide n'entre pas dans le détail de la composition de ce SI de supervision. Un document dédié² détaillera les technologies et leurs possibles implémentations au sein d'un tel SI.



Information

Il est rappelé que comme tout projet technique, un SI de supervision de sécurité est soumis à l'optimisation du rapport coût/efficacité. L'efficacité est ici comprise comme la capacité à identifier des activités malveillantes sur un SI supervisé. Cela implique notamment de trouver un optimum concernant le type et le taux de couverture du SI supervisé. C'est cet optimum qui est recherché dans le processus de conception d'une stratégie de supervision de sécurité. Ce processus est décrit dans le guide « Piloter un projet de supervision » [3].

R

Maîtriser les risques induits par la supervision de sécurité sur le SI supervisé

Une analyse de risque formelle permet d'évaluer les risques susceptibles de se propager depuis le SI de supervision vers le SI supervisé.

R

Maîtriser les risques liés à la mutualisation de moyens entre le SI supervisé et le SI de supervision

Éviter autant que possible les dépendances techniques du SI de supervision avec le SI supervisé (éviter de dépendre des mêmes briques sous-jacentes). Lorsque le contexte ne permet pas de faire autrement (ex. cloud), inclure cette dépendance dans l'analyse de risque et en tenir compte dans la construction d'une stratégie de supervision. (ex. : SI de supervision et SI supervisé dépendent de l'infrastructure de virtualisation du fournisseur cloud)

2. FIXME Voir le guide « Supervision de sécurité - Technologies et implémentation » [?] de l'ANSSI.

R

Le SI de supervision de sécurité doit être cloisonné

Le SI de supervision doit être cloisonné vis-à-vis du (des) SI supervisé(s) afin de maîtriser les risques issus de ce(s) dernier(s). De plus, le SI de supervision doit être structuré en zones de sécurité, permettant notamment de protéger les données traitées. Enfin, le cœur de confiance du SI de supervision de sécurité doit être identifié et protégé de manière adéquate par ces différentes mesures de cloisonnement.

R

Le SI de supervision de sécurité doit être supervisé en sécurité

Il est recommandé de concevoir une stratégie de supervision dédiée au périmètre du SI de supervision. Cette stratégie de supervision peut être portée par le SI de supervision lui-même, ce qui oblige à lui appliquer la recommandation 2.2.1

2.2.1 Types de supervision de sécurité



Supervision de sécurité dédiée

Un SI de supervision surveille l'activité d'un seul SI supervisé (cf. figure 4).

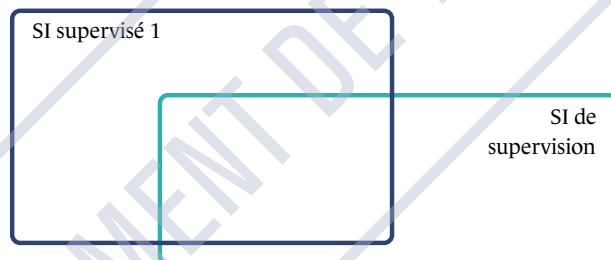


FIGURE 4 – Principe de la supervision de sécurité dédiée



Supervision de sécurité mutualisée

Un SI de supervision surveille l'activité de plusieurs SI supervisés (cf. figure 5).

R

Les données de supervision issues de différents SI supervisés doivent être cloisonnées

Les données de supervision issues des différents périmètres supervisés doivent être cloisonnées les unes des autres au plus tôt et tout au long des traitements au sein du SI de supervision. Les modalités de cloisonnement de ces données doivent être adaptées, notamment selon :

- la ressource technique considérée ;
- l'écart du point de vue des besoins de sécurité entre les différents SI supervisés considérés.

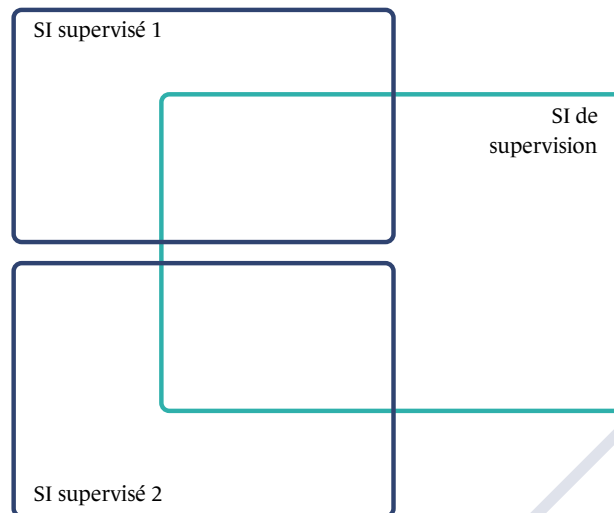


FIGURE 5 – Principe de la supervision de sécurité mutualisée



Supervision de sécurité locale

Le SI supervisé et le SI de supervision sont colocalisés ou reliés à travers un réseau maîtrisé (non géré par un tiers).



Information

Deux contraintes nous intéressent spécifiquement ici dans l'utilisation d'un réseau maîtrisé :

- l'absence de contraintes techniques liées à la distance (ex. : débits élevés liés au partage de certaines ressources d'une plateforme technique comme un cœur de réseau);
- l'absence de contraintes de cybersécurité liées à l'acheminement via des réseaux tiers (ex. : chiffrement implicitement pris en charge par un socle technique commun).



Information

Puisqu'on parle de la localisation relative du SI de supervision par rapport à un SI supervisé, il est également possible de superviser localement des ressources dans le cloud.



Supervision de sécurité distante

Le SI supervisé et le SI de supervision ne sont pas colocalisés et sont reliés à travers un réseau non maîtrisé (ex. : réseau public comme Internet)



Information

Deux contraintes nous intéressent spécifiquement ici dans l'utilisation d'un réseau non maîtrisé :

- l'existence de contraintes techniques liées à la distance (ex. : débits contraints liés

à des réseaux longue distance);

- l'existence de contraintes de cybersécurité liées à l'acheminement via des réseaux tiers (ex. : nécessité de protéger les données transmises en confidentialité vis-à-vis d'un réseau public).

Dans certains cas, une supervision mutualisée peut être locale, par exemple, au sein de grosses entités (ex. : ministère, entreprise composée de plusieurs unités métiers), où la taille et la structure de responsabilité des périmètres fonctionnels peut les apparenter à des SI différents partageant un socle technique minimal. Dans de nombreux cas, une supervision mutualisée est une supervision distante.

2.2.2 Fonctions internes de la supervision de sécurité

Un SI de supervision répond aux caractéristiques d'un SI, détaillées dans la section précédente. Aussi, il peut être découpé en périmètres, relevant de responsabilités distinctes, et opérés à des endroits différents.

La figure 6 propose une représentation des périmètres fonctionnels de la supervision de sécurité. Le descriptif interne des fonctions pourra faire l'objet d'un futur guide ANSSI.

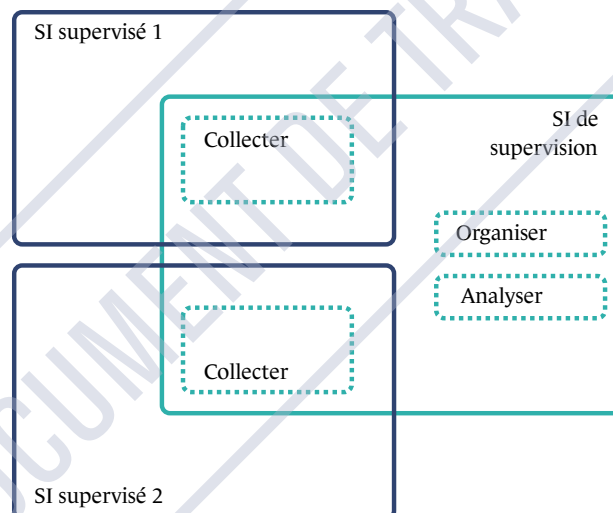


FIGURE 6 – Fonctions internes de la supervision de sécurité



Information

Ce découpage est un choix de modélisation qui présente ses avantages et ses inconvénients, il n'a pas de valeur prescriptive. Son objectif est de repérer les contraintes architecturales qui pèsent sur un SI de supervision.

Voici quelques détails sur chaque fonction :

- **Collecter** : acquisition et transport de données depuis le SI supervisé vers le SI de supervision. Les données collectées sont avant tout des données de supervision. Cependant, des données de contexte/connaissance du SI supervisé (ex. : extraits de CMDB) peuvent également être collectées par des moyens adaptés. Exemples de fonctionnalités :

- > transport des données sur le périmètre supervisé ;
- > transfert des données depuis le périmètre supervisé vers le SI de supervision ;
- > centralisation des données vers le SI de supervision.

■ **Analyser** : traitement automatisé des données transmises par la collecte afin de détecter des activités potentiellement malveillantes et d'en fournir une synthèse à des fins de levée de doute. Exemples de fonctionnalités :

- > traitement des données (enrichissement, normalisation, filtrage, agrégation) ;
- > évaluation des données sur la base de règles de détection ;
- > synthèse des activités malveillantes sous forme d'alertes contextualisées.

■ **Organiser** : coordination des travaux des analyses pour la levée de doute et les investigations complémentaires permettant de qualifier un incident. Exemples de fonctionnalités :

- > synthèse et priorisation des alertes émises par les traitements automatiques ;
- > main courante et capitalisation du savoir ;
- > outils d'investigations complémentaires.



Attention

Certains éléments techniques de la fonction Collecter font partie du SI supervisé. Par conséquent, cette fonction dépend du SI supervisé, et sa mise en œuvre ou sa maintenance dépend des administrateurs du SI supervisé. Il en découle qu'une éventuelle délégation de la responsabilité de la fonction Collecter est forcément partielle. Selon leur nature, les administrateurs du SI supervisé gardent certaines responsabilités sur ses ressources (ex. : déploiement, MCO/MCS).

Les fonctions Collecter, Analyser et Organiser concourent à la sécurisation des données de supervision. De plus, elles ont un rôle différencié dans cette sécurisation. L'articulation des contraintes de sécurité au sein des fonctions vise à offrir une cohérence graduelle dans la sécurisation des données de supervision.



Exemple

Voici comment pourrait s'organiser la segmentation des données à travers les fonctions Collecter et Analyser dans une logique graduelle :

- au sein de la fonction Collecter, la segmentation doit être réalisée par des ressources logiques (ex. : VM dédiée, processus et permission du système d'exploitation dédiés) ;
- au sein de la fonction Analyser, cette segmentation doit être faite au minimum par le biais de ressources applicatives (ex. : droits d'accès, volume de stockage dédié).

2.2.3 Contraintes des fonctions de supervision sur l'architecture

Dans le prolongement de la question introductive « qui fait où? », deux grandes responsabilités sont à distinguer :

- pour la partie fonctionnelle, il s'agit d'identifier qui est responsable de la fourniture du service (une équipe du commanditaire ou une équipe d'un prestataire).
- pour la partie technique, il s'agit d'identifier où sont localisées les ressources techniques dont dépend chaque fonction de supervision de sécurité (sur le SI du commanditaire, sur le SI du prestataire de supervision, sur le SI d'un prestataire d'hébergement).

Les différents cas applicables à ces contraintes représentent une combinatoire élevée et la multiplicité des cas ne permet pas de tous les détailler. Aussi, dans les architectures présentées aux chapitres 3, 4 et 5, des choix arbitraires sont présentés et expliqués pour chaque architecture type. Chaque architecture peut être adaptée à d'autres choix, à condition d'adapter le niveau de sécurité appliqué aux interfaces entre les fonctions suivant les recommandations présentées ci-dessous et dans les paragraphes suivants.

2.2.4 Interfaces entre les fonctions

La figure 7 est une ébauche de représentation des interfaces internes et externes de la supervision de sécurité. Les interfaces internes relient les trois fonctions de la supervision de sécurité (Collecter, Analyser, Organiser). Les interfaces externes relient la supervision à divers éléments extérieurs ("prod" pour SI supervisé, "IA" pour des outils externes d'enrichissement par IA, "CTI" pour des sources de données sur la menace, "réponse" pour une équipe de remédiation, "net" pour un accès démarqué à Internet...).

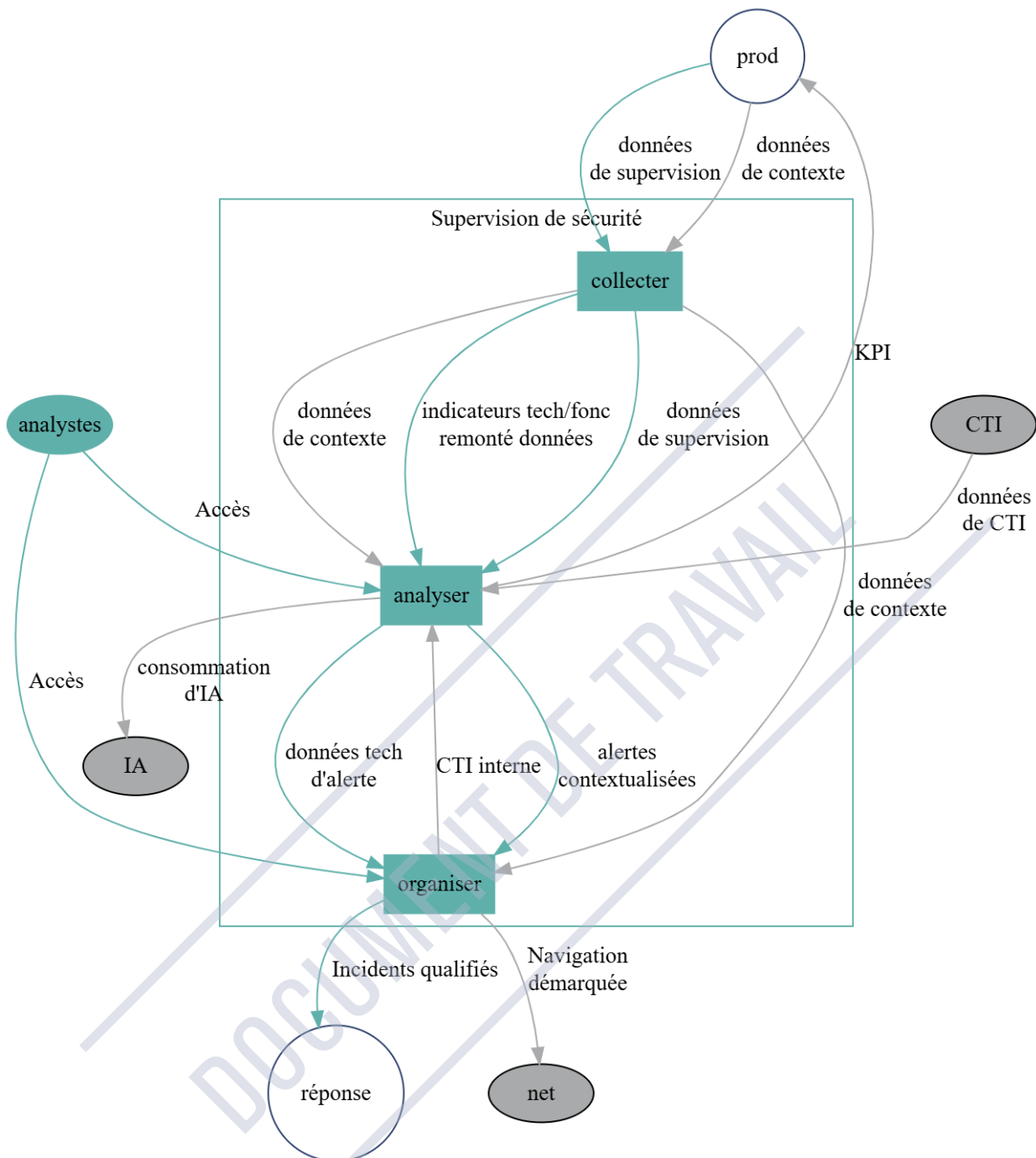


FIGURE 7 – Représentation fonctionnelle des flux de données de la supervision de sécurité

2.2.5 Contraintes de sécurité sur les interfaces entre les fonctions

Afin de simplifier l'adaptation des modèles d'architecture proposés, nous allons nous concentrer sur les contraintes de sécurité qui pèsent sur les interfaces entre les fonctions.

Ces contraintes de sécurité sont génériques, et chaque modèle des chapitres 3 à 5 sera accompagné de contraintes spécifiques additionnelles.

La figure 7 met en évidence des interfaces notables, avec des contraintes spécifiques :

- entre le SI supervisé (prod) et collecter ;
- entre collecter et analyser ;
- entre analyser et organiser ;
- les autres interfaces.

La plupart des flux répondent à des contraintes classiques de sécurisation selon qu'ils soient transportés au sein d'un réseau interne ou d'un réseau tiers (ex. : Internet). Leur sécurisation est facilitée par des protocoles adaptés à ce type d'usage, offrant des capacités natives de sécurisation et sont facilement routables et encapsulables (ex. : flux de navigation vers des interfaces web, flux d'API).

De plus, si les flux entre le SI supervisé (prod) et Collecter ne répondent pas à cette description du fait des protocoles utilisés, la dépendance technique des deux périmètres implique qu'ils soient traités de manière « locale » (sur les mêmes équipements, au sein du même périmètre technique et de responsabilité). C'est l'objet de la fonction Collecter de faire passer ces données au sein depuis le périmètre de sécurité du SI supervisé vers le périmètre de sécurité du SI de supervision.

- R** | Tous les flux sont protégés en confidentialité et en intégrité
- R** | Les flux entre le SI supervisé et Collecter sont surveillés en disponibilité
- R +** | Tous les flux sont surveillés en disponibilité
- R** | **Le risque lié à la disponibilité du lien réseau est maîtrisé pour les flux entre des fonctions distantes**
Il est recommandé de surveiller la disponibilité, de prévoir des systèmes de mémoire cache côté expéditeur pour couvrir des périodes d'indisponibilité des équipes prévisibles (p. ex. : un week-end prolongé), de surveiller le taux d'occupation de ces systèmes de mémoire cache, et enfin les volumes moyens des flux afin d'adapter les cache dans la durée.
- R** | **Les flux entre le SI supervisé et Collecter sont unidirectionnels**
Ils transitent depuis le SI supervisé vers Collecter.
- R** | **Les flux entre Collecter et Analyser sont unidirectionnels**
Ils transitent depuis Collecter vers Analyser.

Les contraintes sur les flux entre Collecter et Analyser sont plus difficiles à aborder pour deux raisons :

- La remontée de données de supervision repose fréquemment sur des protocoles conçus pour fonctionner localement (c.-à-d. au sein d'un centre de données ou d'un réseau local). Par conséquent, les fonctions de sécurité ne sont pas activées par défaut. En outre, ces protocoles ne sont généralement pas conçus pour fonctionner de manière asynchrone et tolérer des coupures de lien.
- S'agissant de données de supervision, leur volume dépend de la taille et de l'activité du SI supervisé. Si certains périmètres sont réputés peu verbeux (ex. : les SI industriels), d'autres induisent d'importants volumes de journaux (ex. : une architecture applicative évolutive qui repose sur un orchestrateur de conteneurs et qui est exposée sur Internet).

Ces contraintes spécifiques font l'objet de propositions d'architecture permettant d'établir des compromis sur les coûts entre les volumes de données à transporter et les briques techniques supplémentaires à maintenir.

2.3 SI d'administration

Les bonnes pratiques d'administration sécurisée [2] recommandent qu'on inclue à tout SI, un périmètre dédié à son administration, dit SI d'administration. Ceci est vrai tant pour un SI supervisé (cf. section 2.3.1) que pour un SI de supervision (cf. section 2.3.2).

Pour rappel, ces bonnes pratiques couvrent tant les SI sur site que les SI dépendant des infrastructures d'un prestataire (ex. : infogérance, cloud).

2.3.1 SI d'administration du SI supervisé

La seconde recommandation du guide « Piloter un projet de supervision » [3] spécifie que la pertinence de la supervision de sécurité est assujettie au fait que le SI supervisé ait atteint un seuil de cybersécurité nominal. L'existence de ressources dédiées à l'administration est un préalable à l'atteinte de ce seuil.

R -

Appliquer au SI supervisé les recommandations minimales relatives à l'administration

Il est recommandé d'appliquer au SI supervisé les recommandations 27 à 29 du guide d'hygiène informatique [1] qui sont spécifiquement dédiées aux moyens d'administration.

R

Appliquer au SI supervisé les recommandations relatives à l'administration

Il est recommandé d'appliquer au SI supervisé les recommandations relatives à l'administration sécurisée d'un système d'information [2].

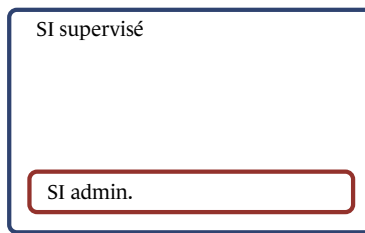


FIGURE 8 – Représentation type d'un SI supervisé incluant un SI d'administration



Exemple

Un des points qui illustre la nécessité des moyens d'administration concerne la non-dissémination des activités privilégiées. Lorsque des moyens sont dédiés à l'administration (ex. : VLAN d'administration), les activités privilégiées sont contenues sur ces moyens dédiés. Par conséquent, une activité privilégiée identifiée sur le reste du SI a de fortes probabilités de correspondre à une anomalie, plus facile à repérer et à qualifier.



La supervision de sécurité couvre le périmètre du SI d'administration

Il est recommandé de concevoir une stratégie de supervision dédiée au périmètre du SI d'administration.

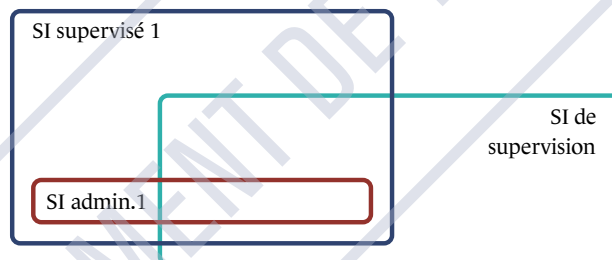


FIGURE 9 – Principe de la supervision de sécurité dédiée incluant l'administration

2.3.2 SI d'administration du SI de supervision

Le SI de supervision de sécurité doit lui aussi disposer de moyens d'administration.



Appliquer au SI de supervision les recommandations relatives à l'administration

Il est recommandé d'appliquer au SI de supervision les recommandations relatives à l'administration sécurisée d'un système d'information [2]



Appliquer au SI de supervision les recommandations minimales relatives à l'administration

Il est recommandé d'appliquer au SI de supervision les recommandations 27 à 29 du guide d'hygiène informatique [1] qui sont spécifiquement dédiées aux moyens d'administration.

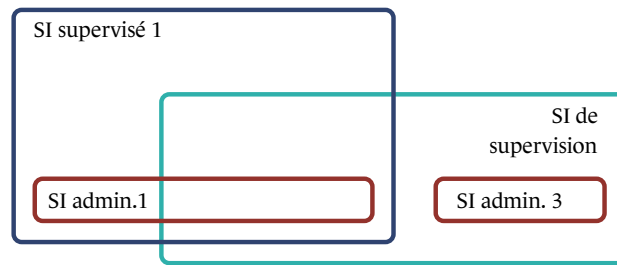


FIGURE 10 – Principe de la supervision de sécurité dédiée avec son SI d'administration

Par ailleurs, l'administration fonctionnelle des outils est réalisée par les analystes.

2.4 L'hypervision de sécurité

L'hypervision a pour objectif d'offrir, en un point unique, la visibilité sur la supervision de plusieurs périmètres d'un SI. C'est un composant qui complète la supervision de sécurité. Sa mise en œuvre doit respecter les besoins de sécurité des SI supervisés couverts.

Le présent guide formulera des recommandations visant à :

- mettre en place la supervision des différents périmètres, indépendamment des difficultés à réaliser l'hypervision ;
- favoriser l'hypervision à une supervision mutualisée entre des SI dont les besoins de sécurité sont trop différents.

2.5 La supervision multimétiers

La sécurité du système d'information n'est pas la seule chose que l'on cherche à superviser au sein des systèmes techniques. Par exemple, les responsables de production cherchent à superviser des métriques opérationnelles. De leur côté, les responsables de maintenance cherchent à superviser des métriques aidant à mettre en place une maintenance prédictive. En somme, différents métiers utilisent différentes stratégies de supervision.

La supervision multi-métier a pour objectif de rassembler les remontées de données de supervision en mettant en commun les moyens qui vont centraliser les données relatives aux différentes stratégies de supervision (ex. : la stratégie de supervision de sécurité, la stratégie de supervision technique et la stratégie de maintenance prédictive).

Le présent guide formulera des recommandations visant à :

- maîtriser chaque stratégie individuellement avant de les rassembler ;
- limiter la mise en commun de moyens techniques pour réaliser les différentes stratégies de supervision ;
- redistribuer les données relatives à chaque stratégie vers une équipe dédiée ;

3

Architectures de supervision de sécurité dédiée

Le présent chapitre aborde la supervision de sécurité dédiée à un unique SI supervisé.

Les deux premières sections examinent les situations où toutes les fonctions du SI de supervision s'appuient sur un socle technique commun, également partagé par le SI supervisé : l'une sur site, la seconde dans le cloud. La troisième section examine les situations où le SI de supervision et le SI supervisé ne dépendent plus du même socle technique. Enfin, la quatrième section explore un cas spécifique de supervision de sécurité dite multimétiers.

3.1 Supervision dédiée sur site

Dans la présente section, la supervision de sécurité est dédiée et le SI supervisé ainsi que le SI de supervision dépendent du même socle technique. Tous ces éléments sont gérés sur site, c'est-à-dire par des moyens internes à l'entité qui les utilise.

3.1.1 Architecture sur site

La figure 11 prend l'exemple d'un SI sur site (ou *on-premise*). Ce SI embarque toutes les ressources techniques permettant de soutenir les utilisateurs, les applicatifs, et un SI d'administration correctement cloisonné, conformément au guide d'administration sécurisée [2].

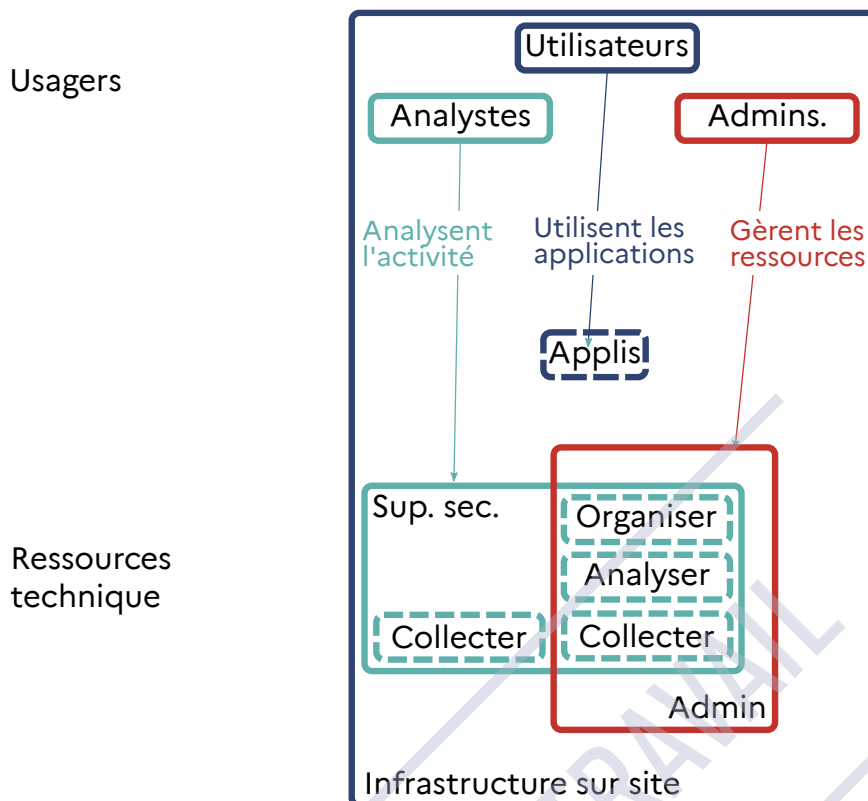


FIGURE 11 – Superviser un SI sur site

Dans ce contexte, créer un SI de supervision de sécurité impose de cloisonner ce dernier du SI supervisé en utilisant les moyens adéquats, alors que les deux SI s'appuient sur un socle technique commun. On peut noter que cette exigence est la même pour le SI d'administration du SI supervisé. De plus, le SI de supervision peut partager certaines ressources techniques avec le SI d'administration du SI supervisé, dans le respect des besoins de sécurité du SI d'administration.

3.1.2 Enjeu : mutualisation de moyens entre les SI de supervision et d'administration

Lorsque le SI de supervision et le SI supervisé, ainsi que son SI d'administration, partagent certaines ressources d'un socle technique commun, il est possible de mutualiser certaines ressources techniques entre le SI d'administration du SI supervisé et le SI de supervision. Cette mutualisation doit se faire dans le respect des besoins de sécurité du SI d'administration et du SI de supervision. De plus, les risques spécifiques amenés par cette pratique doivent être mentionnés dans l'analyse de risque du SI supervisé. Ces risques doivent être couverts ou réduits par des moyens préventifs et/ou défensifs.

Cette mutualisation est possible lorsque le SI d'administration est préexistant, et respecte les recommandations du guide d'administration sécurisée [2].



Exemple

Voici quelques exemples d'éléments susceptibles d'être mutualisés entre le SI d'administration et le SI de supervision, accompagnés des précautions les plus évidentes :

- L'image standardisée des postes d'administration et celle des postes de supervision peuvent être les mêmes. Précaution : les postes affectés à la supervision de sécurité doivent être dédiés à cet usage.
- L'annuaire des comptes d'administration et celui des comptes de supervision peuvent être les mêmes. Précaution : les comptes affectés à la supervision de sécurité doivent être dédiés à cet usage.
- L'infrastructure réseau, dont les moyens de filtrage, peut servir à la fois le SI d'administration et le SI de supervision. Précaution : des zones dédiées à la supervision de sécurité doivent être matérialisées à l'intérieur du périmètre de sécurité du SI d'administration.
- Le SI d'administration peut être utilisé pour administrer les ressources du SI de supervision et apporter les mises à jour. Précaution : les flux dédiés aux différents périmètres doivent être isolés de manière adéquate, de manière à limiter le risque de rebond entre les périmètres.

3.1.3 Cas d'usage identifiés

Parmi les SI qui correspondent à ce cas, on peut citer :

- les SI historiques sur site ;
- les SI d'un fournisseur cloud, y compris celui dont il loue les ressources ;
- les SI sensibles réglementés qui répondent à des obligations de maîtrise du socle technique (ex. : SI classifiés de défense) ;
- les SI interagissant avec le monde physique, tels que les SI industriels (ex. : usine, transport) ou médicaux (ex. : imagerie médicale).

3.2 Supervision dédiée dans le cloud

Dans la présente section, la supervision de sécurité est toujours dédiée, et le SI supervisé et le SI de supervision dépendent toujours du même socle technique. En revanche, ils ne sont pas hébergés sur site, mais chez un tiers externe (infogérance ou cloud).

Ici la gestion des ressources physiques est déléguée à un prestataire (IaaS). L'entité gère des ressources logiques et y adosse des ressources applicatives à destination de ses utilisateurs. La présente section se concentre sur la supervision, maîtrisée par l'entité, de ces ressources logiques et applicatives.

La localisation des utilisateurs est indifférente. D'un côté du spectre, ils peuvent être dans une infrastructure maîtrisée, au sein d'un bâtiment appartenant à l'entité. De l'autre côté du spectre,

ils peuvent être sur Internet avec des équipements personnels , toutes les possibilités entre ces deux extrêmes étant possibles.



Information

Ce cas est un scénario courant de supervision de sécurité pour des ressources localisées sur une infrastructure cloud. En effet, les ressources physiques étant déléguées, on y aborde le partage de responsabilité. De plus, les ressources logiques offrent une maîtrise suffisante pour implanter des points de collecte et choisir des sources de données de supervision pertinentes. En revanche, c'est très rarement le cas pour des ressources applicatives, où les possibilités de supervision dépendent entièrement de ce qui a été prévu au développement, et ne sont donc pas à la main de l'entité cliente.

3.2.1 Architecture avec outils de supervision opérés par le client

La figure 12 montre une supervision de sécurité déployée au sein des ressources logiques qui soutiennent les ressources applicatives.

DOCUMENT DE TRAVAIL

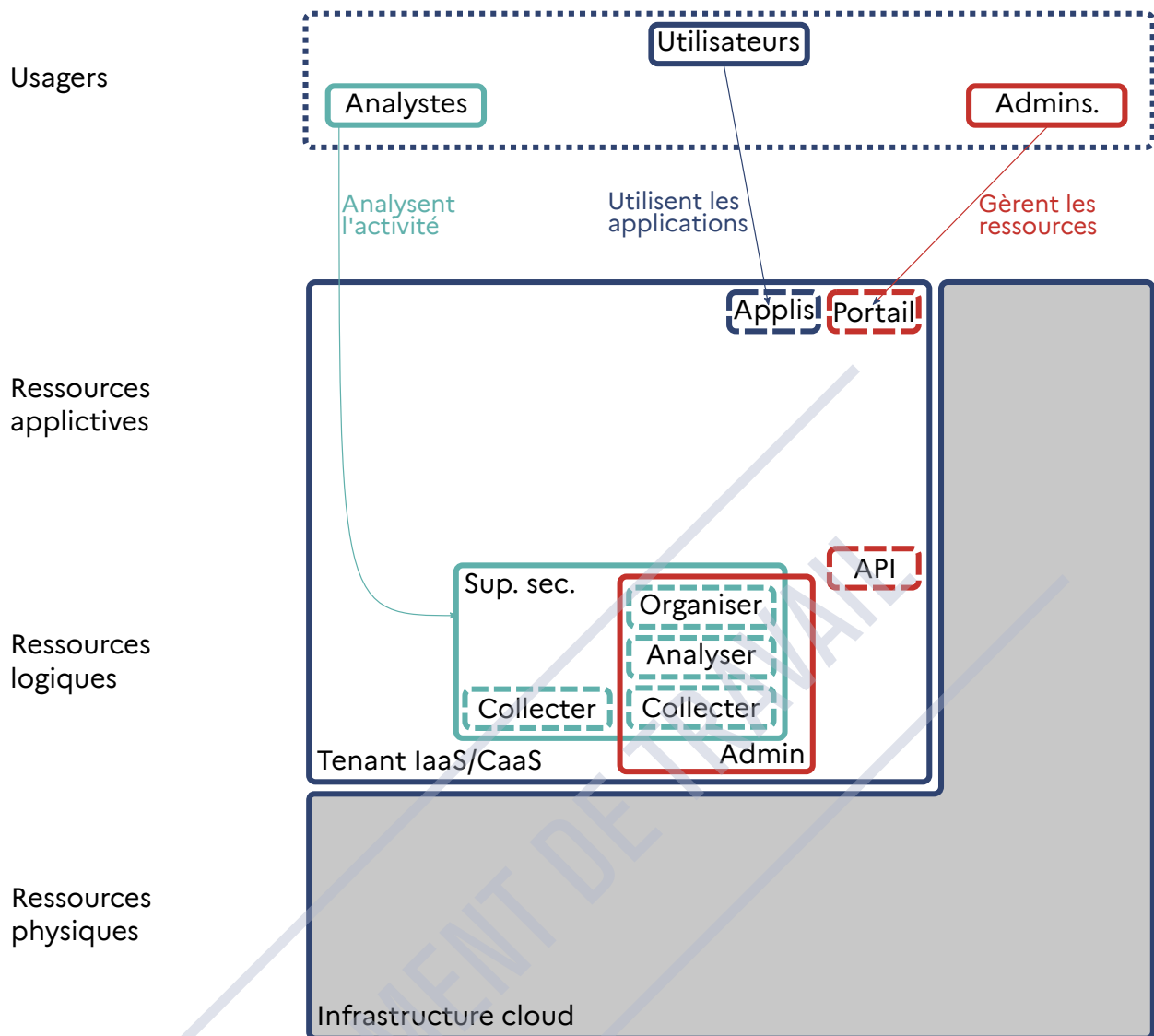


FIGURE 12 – Superviser le cloud avec des ressources en IaaS

3.2.2 Enjeu : accès distant des analystes

La sécurité des accès distants des analystes doit être prise en compte, dès lors que les accès traversent des ressources/réseaux non maîtrisées. Leurs besoins en sécurité (disponibilité, intégrité, confidentialité) doivent être assurés au juste niveau.

3.2.3 Architecture avec outils de supervision opérés par le fournisseur

La figure 13 montre une supervision de sécurité déployée chez le même fournisseur, mais qui prend la forme d'un service managé.

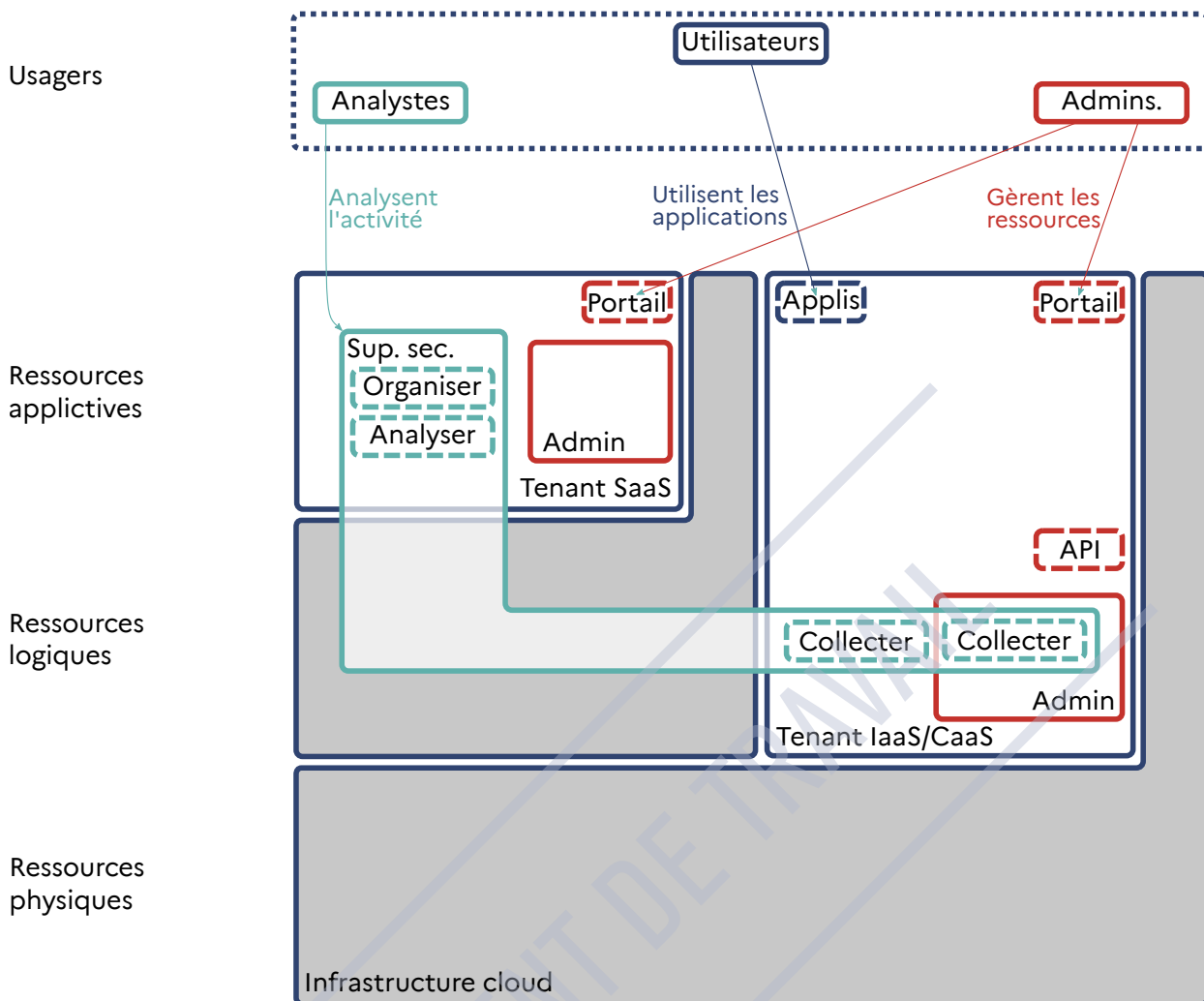


FIGURE 13 – Superviser le cloud avec un service managé

3.2.4 Enjeu : réversibilité vis-à-vis du fournisseur

Le cas de la figure 12 met en lumière un équilibre entre effort et réversibilité :

- Le service managé qui soutient les fonctions Analyser et Collecter est sans doute adapté pour s'interfacer avec les spécificités des ressources logiques du fournisseur (ex. : en environnement virtualisé ou conteneurisé). Le fournisseur peut éventuellement fournir des modèles de configuration simplifiant les interconnexions. Tous ces éléments sont susceptibles de réduire l'effort de mise en œuvre.
- Toutes les facilités apportées par les services managés rendent d'autant plus difficile la réversibilité vers d'autres outils de supervision. Cette réversibilité induit un effort significatif et sans garantie de résultat pour parvenir à faire fonctionner des outils différents dans un contexte donné, sans même parler de reproduire les fonctionnalités attendues.

3.2.5 Cas d'usage identifiés

Le recours à une infrastructure cloud hébergeant applications et supervision se retrouve notamment pour :

- les SI de petites entités ne disposant pas d'infrastructures en propre;
- les SI d'entités dont l'enjeu est de saisir un marché sans devoir investir dans des infrastructures;
- les SI d'une entité fille qui s'appuie entièrement sur les moyens fournis par une entité mère.

3.3 Supervision dédiée à distance

Contrairement aux deux sections précédentes, les SI supervisés et de supervision dépendent d'infrastructures différentes.

3.3.1 Architecture entre des infrastructures distantes

La figure 14 montre un SI supervisé reposant sur des ressources physiques dont la gestion est déléguée à un prestataire. Le SI de supervision est dans la même configuration, avec un prestataire différent.

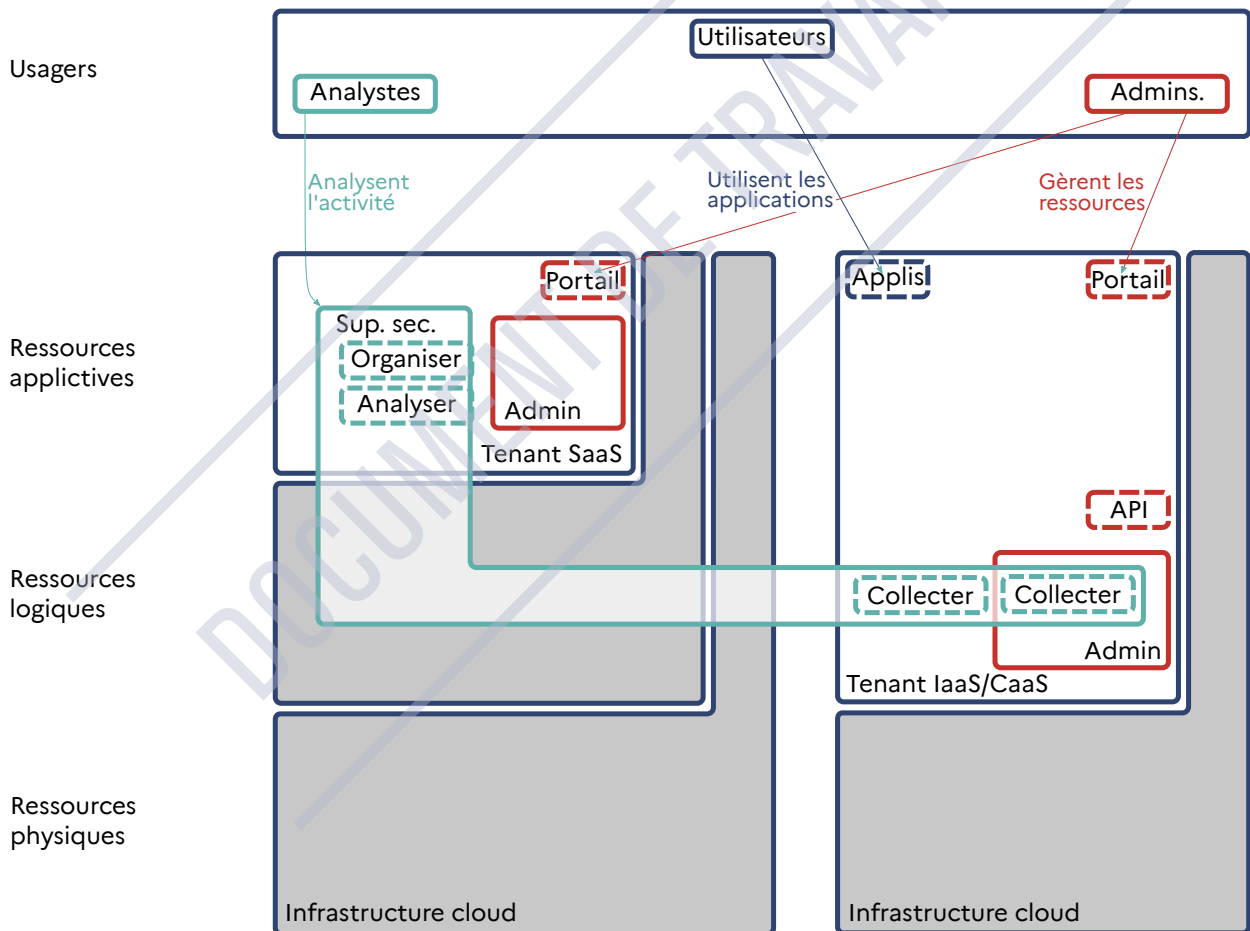


FIGURE 14 – Superviser un cloud depuis un autre cloud

Le choix de représenter deux infrastructures déléguées à des tiers est arbitraire, de même que le fait de localiser sur la même infrastructure les fonctions Analyser et Organiser. Cela signifie que ce scénario peut aussi être appliqué si l'une des infrastructures est sur site, ou si la fonction

Analyser est indifféremment sur l'infrastructure qui soutient le SI de supervision de sécurité, ou le SI supervisé.

3.3.2 Enjeu : distance entre les fonctions

3.3.3 Cas d'usage identifiés

Parmi les SI correspondant à ces cas, on peut citer :

- les SI dont l'infrastructure sur site est supervisée à partir d'une infrastructure cloud ;
- les SI dont l'infrastructure cloud est supervisée à partir d'une infrastructure sur site ;
- les SI dont l'infrastructure cloud est supervisée à partir d'une autre infrastructure cloud.

3.4 Supervision dédiée multimétiers

Comme évoqué dans la section 2.5, il peut être souhaitable de mettre en commun la fonction Collecter pour assurer les remontées de différentes supervisions.

3.4.1 Enjeu : topologie de collecte complexe

Des éléments seront détaillés afin d'aider à réaliser une topologie de collecte adaptée. En particulier, qui manipule une plus grande diversité de données, et qui doit redistribuer ces données à des consommateurs différents (les analystes cyber, les responsables de production et les responsables de maintenance).

3.4.2 Cas d'usage identifiés

Parmi les SI correspondant à ces cas, on peut citer :

- les SI industriels et médicaux, pour lesquels la supervision de fonctionnement et la supervision pour la maintenance prédictive sont fréquentes.
- les SI de protection physique.

4

Architectures de supervision de sécurité mutualisée

Le présent chapitre aborde la supervision de sécurité mutualisée, qui met en œuvre en un point unique les stratégies de supervision de plusieurs SI supervisés, soit par la mutualisation sur une infrastructure interne (section 4.1), sur des infrastructures distantes (section 4.2), soit par l'externalisation du service de supervision de sécurité (section 4.3).

4.1 Supervision mutualisée sur site

La présente section traite de la mutualisation de la supervision de sécurité sur site. Ce cas se présente lorsqu'un SI est assez important pour distinguer divers périmètres de haut niveau qui consomment les ressources d'un socle commun (ex. : réseau de transport de données, fonctions d'infrastructures, équipe d'administrateurs).

4.1.1 Architecture mutualisée interne

La figure 15 montre plusieurs périmètres fonctionnels dépendant d'un socle technique commun. L'un de ces périmètres fonctionnels (le plus à gauche) dessert les accès des utilisateurs, c'est-à-dire les postes de travail et tous les moyens permettant à ces postes d'accéder aux ressources du SI dans des conditions de sécurité compatibles avec la politique de sécurité des systèmes d'information (PSSI). Les deux autres périmètres fonctionnels sont dédiés à des applicatifs métiers.

Sur cette figure, le choix du périmètre qui héberge les fonctions Analyser et Organiser est arbitraire. De même, les moyens d'administration sont dédiés à chaque périmètre d'administration, mais sous certaines conditions (ex. : respect des contraintes les mieux disantes), ces moyens d'administration auraient pu être mutualisés.

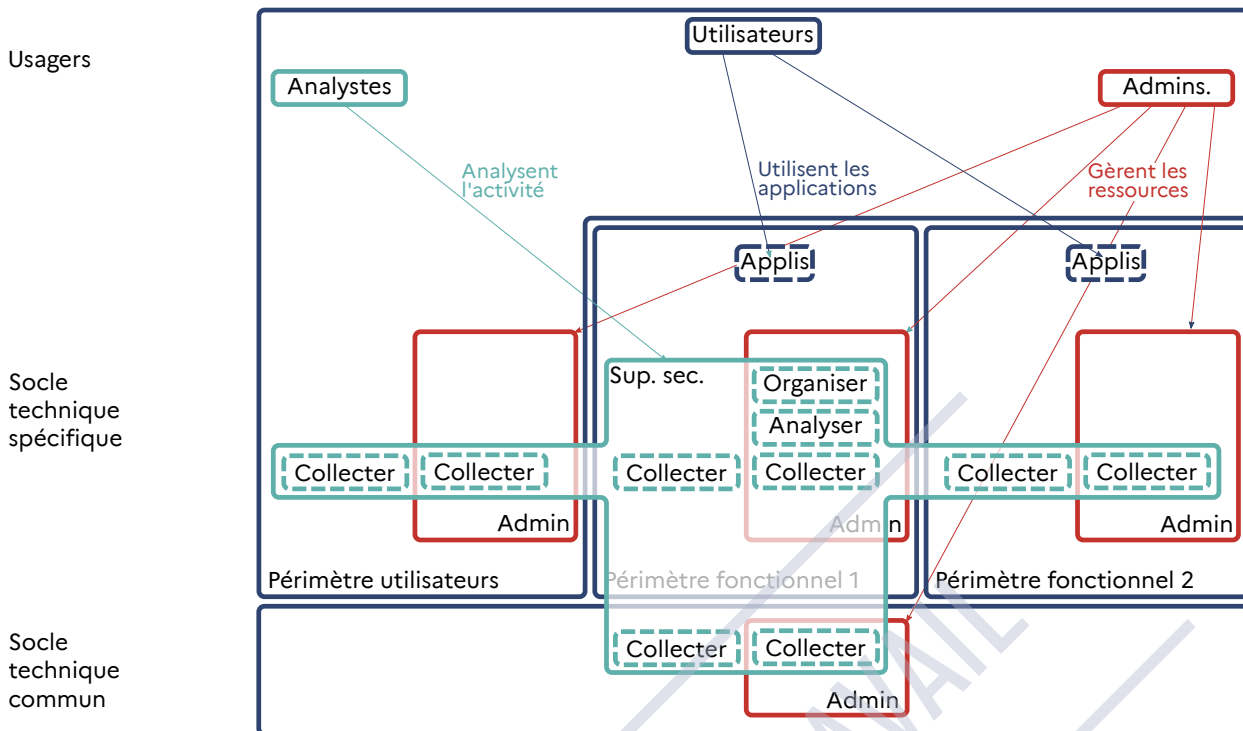


FIGURE 15 – Supervision mutualisée sur une infrastructure interne

4.1.2 Enjeu : séparation des données

4.1.3 Cas d'usage identifiés

Parmi les SI correspondant à ces cas, on peut citer :

- les SI sur site en multisite ;
- les SI organisés en périmètres (ex. : métiers, fonctionnels, technologiques).

4.2 Supervision mutualisée à distance

Dans la présente section, la supervision mutualisée est opérée à distance des périmètres supervisés.

4.2.1 Architecture mutualisée distante

La figure 16 présente des périmètres dépendant tous d'infrastructures distinctes. L'un des périmètres, sur site, dessert les accès utilisateurs et des applications. Un autre périmètre, dépendant des infrastructures d'un prestataire, dessert d'autres applicatifs. Enfin, un troisième périmètre dépendant des infrastructures d'un autre prestataire, dessert les fonctions Analyser et Organiser sous forme de services managés.

Sur cette figure, le choix d'utiliser un service managé est arbitraire. S'il correspond à l'usage général, ce modèle d'architecture s'adapte à d'autres modalités de mise en œuvre, y compris en séparant les fonctions Analyser et Organiser sur plusieurs services managés.

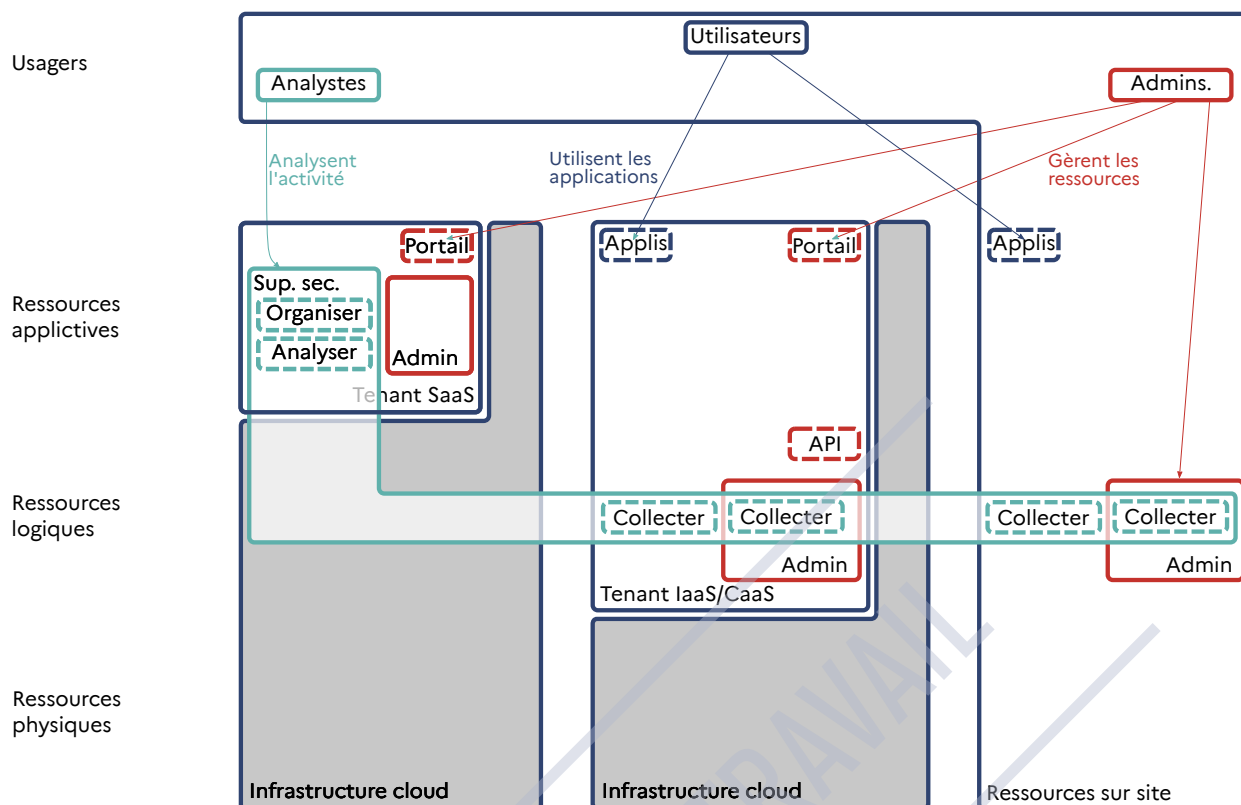


FIGURE 16 – Supervision mutualisée à distance

4.2.2 Enjeu : latéralisation entre SI supervisés

4.2.3 Cas d'usage identifiés

Parmi les SI correspondant à ces cas, on peut citer :

- les SI répartis sur différentes infrastructures internes et/ou de différents prestataires ;
- la supervision de sécurité hébergée en dehors des infrastructures des SI supervisés.

4.3 Supervision mutualisée externalisée

La présente section aborde l'externalisation du service de supervision auprès d'un tiers. Il ne s'agit plus seulement de traiter de la localisation des fonctions de la supervision de sécurité, mais également de tenir compte de l'équipe d'analystes qui dépend d'un tiers.

4.3.1 Architecture de supervision par un tiers

La figure 17 représente un périmètre comprenant les analystes et les administrateurs du fournisseur de service de sécurité managé (MSSP). Les administrateurs gèrent les outils qui relèvent de la responsabilité du MSSP. Les analystes accèdent à une fonction Organiser spécifique au MSSP (indépendamment du client, ce qui accroît l'efficacité de ses équipes) et à la fonction Analyser (qui est ici géré par le MSSP, mais pourrait également être géré par un client, selon les conditions contractuelles).

La partie droite représente un des SI supervisés par le MSSP, en gardant en tête que le fournisseur a un nombre variable de clients, et souhaite sans doute superviser divers types de SI répondant à diverses obligations réglementaires cyber (concrètement, à différents niveaux de sécurité).

Le choix de représenter le SI supervisé au sein de ressources logiques dépendant des infrastructures d'un prestataire est arbitraire, il pourrait s'agir de ressources applicatives dépendant des infrastructures d'un prestataire, ou d'infrastructures sur site.

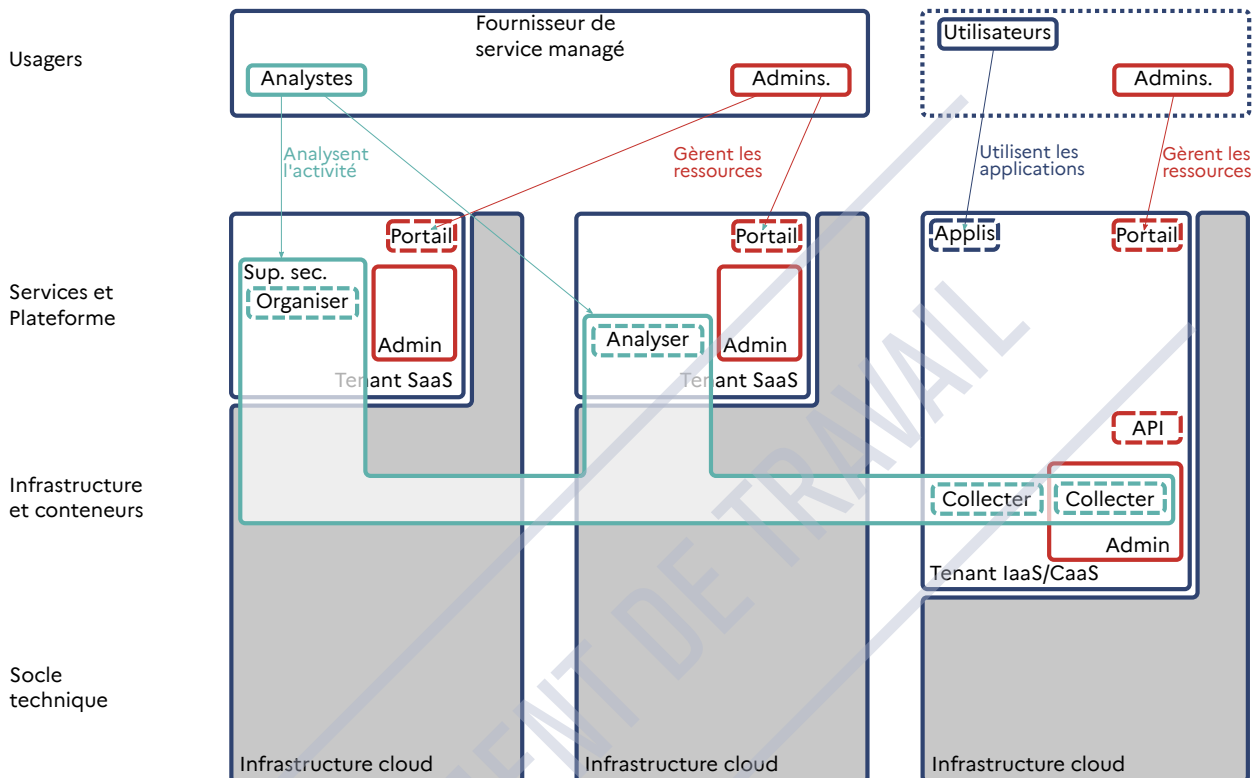


FIGURE 17 – Supervision externalisée

4.3.2 Enjeu : gestion de la complexité du modèle de responsabilité

Le choix de séparer les fonctions Organiser et Analyser permet d'observer la complexité du modèle de délégation lorsque le MSSP choisit de déléguer ses outils. Rassembler ces deux fonctions simplifie également les contraintes de distance, de même que les positionner dans une infrastructure sur site géré par le MSSP.

4.3.3 Cas d'usage identifiés

Parmi les SI correspondant à ces cas, on peut citer :

- la supervision de sécurité déléguée à un MSSP opérant sa propre infrastructure de supervision ;
- la supervision de sécurité déléguée à un MSSP déléguant l'ensemble des infrastructures de supervision à des tiers ;
- la supervision de sécurité déléguée à un MSSP déléguant la fonction Organiser à des tiers, tout en maintenant la fonction Analyser sous la responsabilité du client.

5

Architectures composites de supervision de sécurité

Le présent chapitre aborde des modèles d'architectures composites de supervision de sécurité. Il s'appuie sur des modèles vus précédemment afin de répondre à des cas d'usage plus complexes.

Le principal élément différenciant de ces architectures est le chaînage de plusieurs fonctions Analyser. Cela permet, par exemple, de résoudre des situations où le traitement local est plus intéressant que l'acheminement des données vers des traitements centralisés, sans pour autant sacrifier une visibilité consolidée sur l'activité des différents périmètres. Cela permet également de s'adapter à des évolutions des périmètres difficiles à anticiper (ex. : une fusion/acquisition). La contrepartie évidente de ces architectures est leur coût de maintenance et d'intégration.

5.1 Utiliser une supervision dédiée sur chaque infrastructure

Le modèle de supervision distribuée sur différentes infrastructures consiste à démultiplier l'ensemble des fonctions de la supervision sur chaque périmètre pour qu'ils bénéficient d'une supervision locale.

Le modèle de supervision distribué implique qu'on ne dispose à priori pas d'une vision unique sur l'ensemble des périmètres.

5.1.1 Architecture de supervision distribuée

La figure 19 présente des périmètres dépendant tous d'infrastructures distinctes. L'un des périmètres, sur site, dessert les accès utilisateurs et des applications. Un autre périmètre, dépendant des infrastructures d'un prestataire, dessert d'autres applicatifs. Enfin, un troisième périmètre, dépendant des infrastructures d'un autre prestataire, dessert encore d'autres applicatifs. Chaque périmètre dispose d'une supervision de sécurité dédiée.

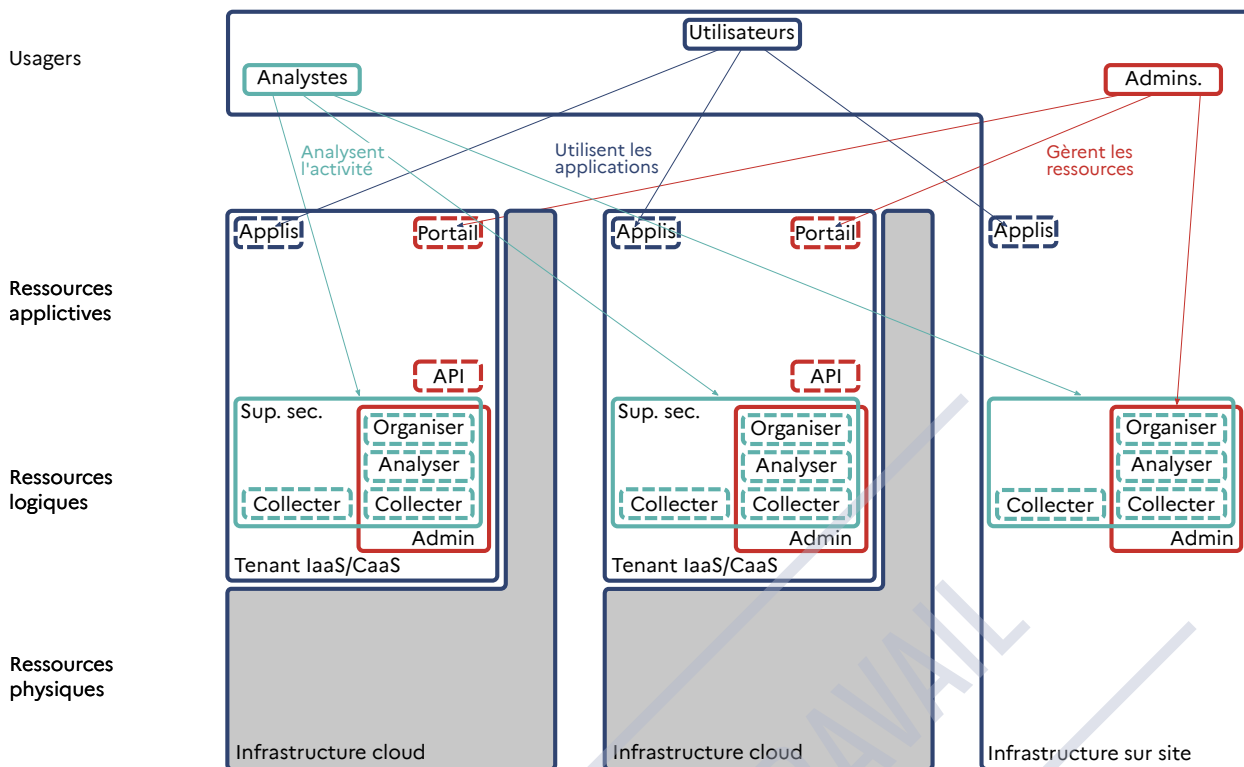


FIGURE 18 – Supervision distribuée

5.1.2 Enjeu : maintenir la proximité de la supervision de sécurité en environnement complexe

Cette solution est utile lorsque le coût de la centralisation des données excède le coût du traitement local, en particulier lorsque les périmètres produisent de gros volumes de données. Elle peut également permettre de déplacer la charge du calcul vers chaque périmètre de collecte. Enfin, elle peut réduire l'effort d'intégration des données de supervision, notamment lorsque les prestataires responsables des infrastructures sous-jacentes aux SI supervisés proposent des solutions incluant l'intégration des données issues de leurs socles techniques.

5.1.3 Cas d'usage identifiés

Parmi les SI correspondant à ces cas, on peut citer :

- les SI disposant d'un périmètre sur site avec leur propre supervision, et des périmètres hébergés dans le cloud et générant trop de données de supervision ;
- les SI reposant sur des périmètres hébergés dans le cloud chez différents fournisseurs proposant des outils de supervision intégrés à leurs infrastructures.

5.2 Combiner plusieurs supervisions dédiées et l'hypervision

Le présent modèle reprend le principe de la supervision distribuée, et y ajoute la fonction d'hypervision, permettant d'observer l'activité des SI supervisés depuis un point unique.

5.2.1 Architecture de supervision distribuée avec hypervision

La figure 19 présente des périmètres dépendant tous d'infrastructures distinctes. L'un des périmètres, sur site, dessert les accès utilisateurs et des applications. Un autre périmètre, dépendant des infrastructures d'un prestataire, dessert d'autres applicatifs. Enfin, un troisième périmètre, dépendant des infrastructures d'un autre prestataire, dessert encore d'autres applicatifs. Chaque périmètre dispose d'une supervision de sécurité dédiée, et une hypervision est proposée pour observer l'activité des SI supervisés depuis un point unique.

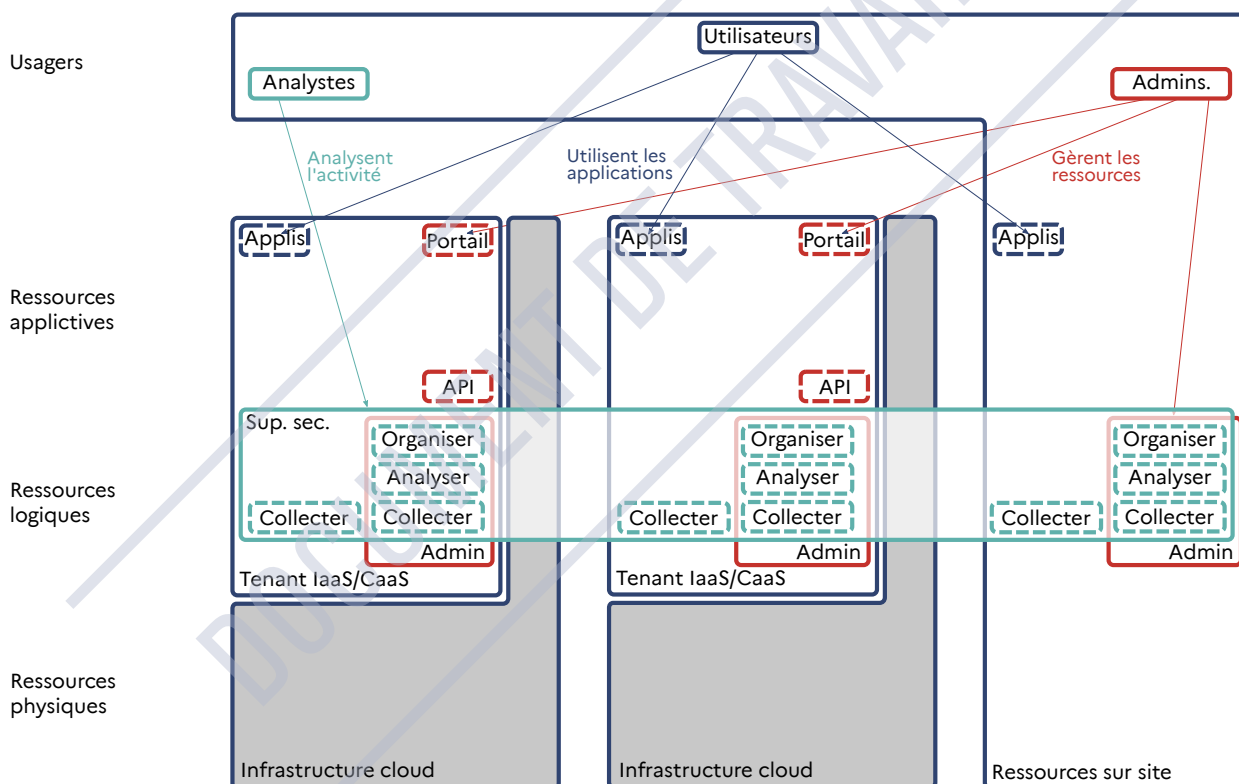


FIGURE 19 – Supervision distribuée avec hypervision

5.2.2 Enjeu : équilibrer les besoins d'une vue unique avec les besoins en sécurité des différents SI supervisés

En théorie, n'importe quel périmètre peut endosser ce rôle du moment que l'on permet aux événements de sécurité et/ou aux alertes de sécurité de transiter dans de bonnes conditions de sécurité vers le périmètre choisi pour l'hypervision.

Cependant, la contrainte de sécurité des données en transit, ainsi que le respect des besoins de sécurité des SI supervisés, sont susceptibles de dicter le ou les périmètres en mesure de recevoir l'hypervision, ou au contraire, le ou les périmètres qui ne peuvent pas y être rattachés.

5.2.3 Cas d'usage identifiés

Parmi les SI correspondant à ces cas, on peut citer :

- hypervision de ressources sur site et dans le cloud ;
- hypervision multi-cloud.

5.3 Combiner la supervision dédiée, la supervision distante et l'hypervision

Le modèle de supervision mixte autorise que chaque périmètre ne possède pas sa propre supervision de sécurité. Ces périmètres sont donc en supervision distante, tandis que d'autres sont en supervision locale.

Ce modèle ne présume pas de la présence d'une hypervision, et n'importe quel périmètre disposant des fonctions Analyser et Organiser peut endosser ce rôle, du moment où les conditions de sécurité des informations transitaires sont assurées.

5.3.1 Architecture de supervision mixte

La figure 20 présente des périmètres dépendant tous d'infrastructures distinctes. L'un des périmètres, sur site, dessert les accès utilisateurs et des applications. Un autre périmètre, dépendant des infrastructures d'un prestataire, dessert d'autres applicatifs. Enfin, un troisième périmètre, dépendant des infrastructures d'un autre prestataire, dessert encore d'autres applicatifs. Seuls deux périmètres disposent d'une supervision de sécurité dédiée. Le troisième possède les fonctions Collecter, qui remontent les données de supervision vers l'une ou l'autre des fonctions Analyser existante.

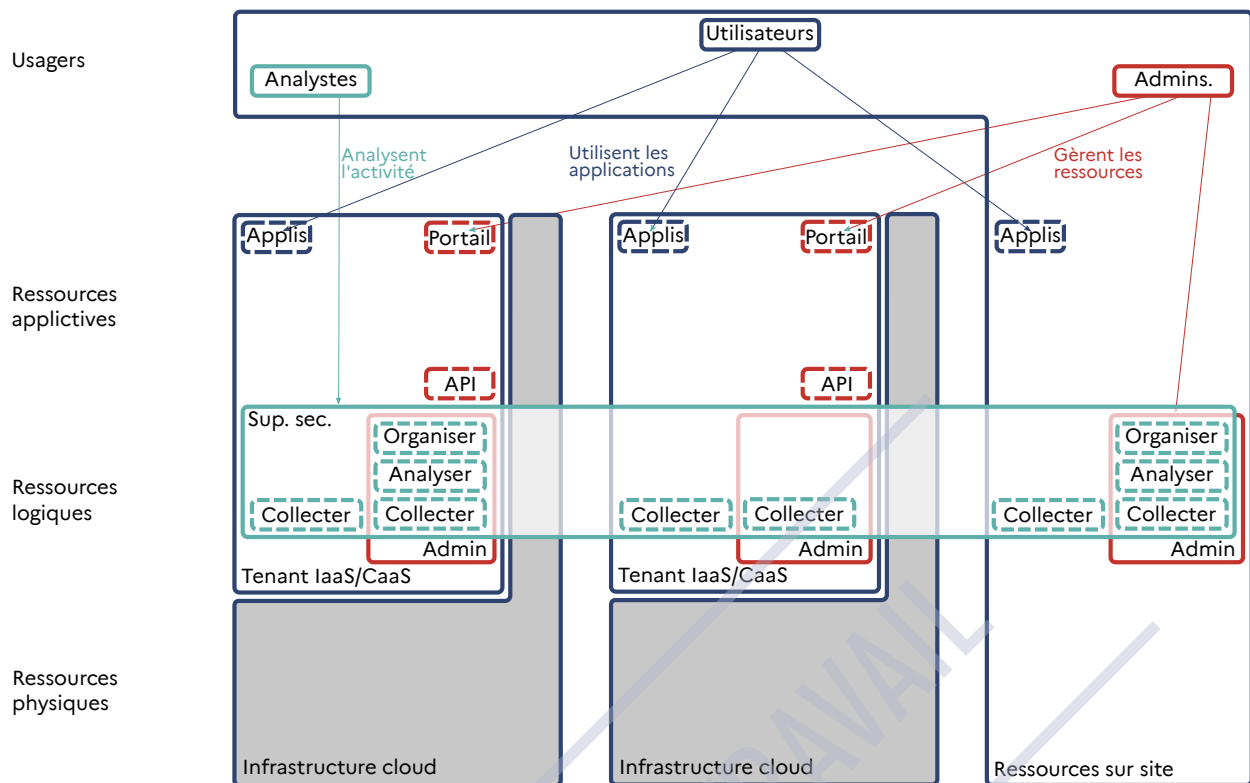


FIGURE 20 – Supervision mixte

5.3.2 Enjeu : maîtrise des coûts en environnement complexe

5.3.3 Cas d'usage identifiés

Parmi les SI correspondant à ces cas, on peut citer :

- les SI disposant d'un périmètre sur site avec leur propre supervision, et des périmètres hébergés dans le cloud et générant des quantités variables de données de supervision ;
- les SI reposant sur certains périmètres hébergés dans le cloud chez des fournisseurs proposant des outils de supervision intégrés à leurs infrastructures, et d'autres n'offrant pas ces facilités.

5.4 Combiner plusieurs niveaux de supervision

Quel que soit le modèle de supervision pré-existant, ce modèle consiste à lui adjoindre un niveau supplémentaire de supervision distant. Ce niveau supplémentaire permet de s'adapter à de nouveaux enjeux de supervision, tels que des besoins de sécurité spécifiques (ex. : disponibilité, confidentialité) ou l'exposition à différents niveaux de menace (ex. : systémique, stratégique). Cette solution permet de répartir les efforts de supervision afin d'accroître l'assurance qu'un incident est visible.

5.4.1 Architecture de supervision à deux niveaux

Sur la figure 21, la partie droite montre une supervision dépendant des infrastructures d'un prestataire, accédée par une équipe d'analystes distincte et gérée par une équipe d'administrateurs

distincte également. Le choix de la physionomie de cette supervision de sécurité est arbitraire, le modèle s'adaptant à tout type de supervision (ex. : sur site du fournisseur de ce second service de supervision).

Les parties centrale et droite montrent deux périmètres distants desservis par une supervision mutualisée. Ce choix est totalement arbitraire, le modèle s'adaptant à tout type de situation préexistante.

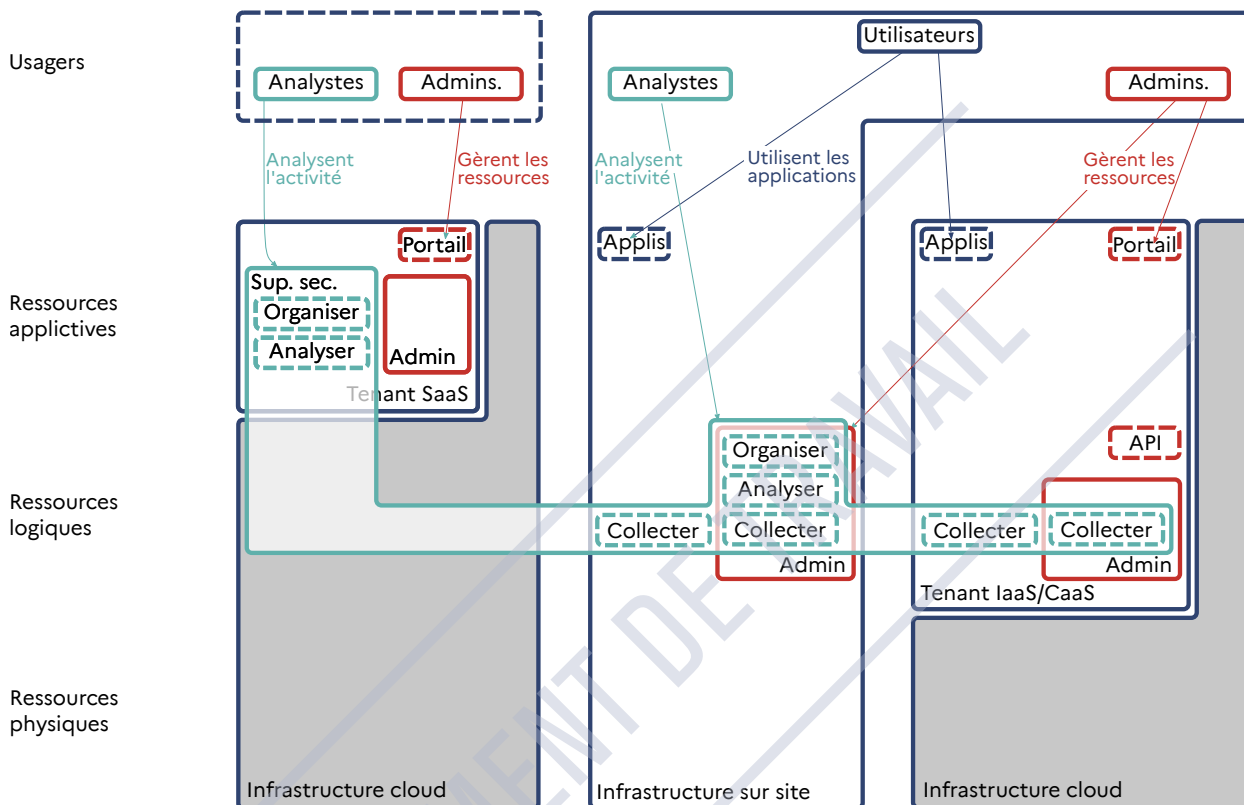


FIGURE 21 – Supervision à deux niveaux

5.4.2 Enjeu : spécialisation de la supervision

La supervision préexistante se concentre généralement sur les menaces courantes, plus faciles à gérer de par la proximité des équipes et la fréquence nécessaire aux levées de doute. L'équipe distante, quant à elle, gère des menaces de plus haut niveau par un effort spécifique de connaissance de la menace (CTI), de recoupement d'activités sur divers périmètres et des capacités de recherche d'antécédents.

5.4.3 Cas d'usage identifiés

Parmi les SI correspondant à ces cas, on peut citer :

- les SI disposant d'une supervision interne ne répondant pas à un niveau d'exigence spécifique, et d'une supervision externe répondant à un niveau d'exigence réglementaire ;

5.5 Concevoir une supervision renforcée

La mise en œuvre de la supervision de sécurité n'a pas à être uniforme. Certains SI supervisés peuvent nécessiter des moyens de supervision renforcés par rapport aux autres. Soit de par la criticité de ce SI, soit de façon temporaire pour répondre à une actualité.

Bien plus que proposer un modèle d'architecture de supervision, la présente section élargit les possibilités de conception d'une telle architecture. En effet, il n'est plus ici seulement question de s'adapter aux contraintes de topologie du SI supervisé pour optimiser le rapport coût/efficacité.

5.5.1 Enjeu : privilégier les contraintes cyber pour la supervision de certains périmètres

5.5.2 Cas d'usage identifiés

Parmi les SI correspondant à ces cas, on peut citer :

- les SI d'entités dont les activités dépendent de contextes réglementaires différents ;
- les SI d'entités dont les branches métiers expriment des besoins en sécurité très différents.

Annexe A

Légende des visuels

A.1 Forme des contours

Ligne continue : SI ou périmètre technique (= des objectifs métier et un responsable de ces objectifs)

Ligne discontinue : fonctions du SI (collecter, analyser, organiser, API, portail, appli...)

Ligne pointillée : périmètres sans responsable (Internet est un périmètre technique dont la responsabilité n'est pas établie)

A.2 Couleur des contours

Trait bleu : éléments relevant du SI supervisé

Trait rouge : éléments relevant du SI d'administration

Trait vert : éléments relevant du SI de supervision

A.3 Couleur des fonds

Fond blanc : ressources sous la responsabilité de l'entité

Fond gris : ressources sous la responsabilité d'un prestataire

Bibliographie

- [1] *Guide d'hygiène informatique : renforcer la sécurité de son système d'information en 42 mesures.*
Guide ANSSI-GP-042 v2.0, ANSSI, septembre 2017.
<https://cyber.gouv.fr/hygiene-informatique>.
- [2] *Recommandations relatives à l'administration sécurisée des systèmes d'information.*
Guide ANSSI-PA-022 v3.0, ANSSI, mai 2021.
<https://cyber.gouv.fr/guide-admin-si>.
- [3] *Supervision de sécurité - Piloter un projet de supervision.*
Technical Report ANSSI-PG-113 v1.0, ANSSI, juillet 2025.
<https://cyber.gouv.fr/supervision-securite>.

DOCUMENT DE TRAVAIL

DOCUMENT DE TRAVAIL

Version 0.9 - 19/03/2026 - ANSSI-PG-TBD
Licence ouverte / Open Licence (Étalab - v2.0)

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
cyber.gouv.fr / conseil.technique@ssi.gouv.fr

