Piloter un Projet de Supervision de Sécurité

Lead a Security Supervision Project

Cyril Poirret[1,*,†]

[1] *Agence Nationale de la Sécurité des Systèmes d'Information, 51 boulevard de La Tour-Maubourg 75700 PARIS 07 SP, France*

Abstract

Security supervision is a key activity in securing information systems. Together with threat intelligence and incident response, it plays a key role in handling security incidents.

This operational-level document sets out best practices for organizing and managing a security monitoring service. In particular, the resources it proposes can help to create a security supervision capability.

Keywords

security supervision, security incident detection, security incident analysts, supervision strategy, supervision process, detection rules, supervision information system, stakes and risks

Résumé

La supervision de sécurité est une activité clé pour la sécurisation des SI. Avec le renseignement sur la menace, et la réponse à incidents, elle participe au traitement des incidents de sécurité.

Le présent document, de niveau opérationnel, expose les meilleures pratiques pour organiser et piloter un service de supervision de sécurité. Les ressources qu'il propose peuvent notamment aider à la création d'une capacité de supervision de sécurité.

1. Introduction

L'ANSSI publie un ensemble de guides sur la supervision de sécurité. Ce corpus documentaire a pour vocation de 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).

Le présent document est de niveau opérationnel. Il aide à comprendre l'organisation et le pilotage d'un service de supervision de sécurité. En premier lieu, le lecteur y trouvera la définition de la supervision de sécurité, et la description de l'écosystème dans lequel elle s'inscrit. En second lieu seront détaillés les éléments organisationnels et techniques qui composent une supervision de sécurité. Seront ensuite décrits les enjeux qui entourent la supervision de sécurité puis, pour finir, des recommandations visant à orienter la construction d'une capacité de supervision de sécurité.

2. Définir la supervision de sécurité

2.1. Définition

Supervision de sécurité

La supervision de sécurité désigne l'ensemble des moyens et des activités concourant, dans les meilleurs délais, à la détection et à la qualification d'un incident[1] 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.

C&ESAR'25: Computer & Electronics Security Application Rendezvous, Nov. 19-20, 2025, Rennes, France

assistance-technique@ssi.gouv.fr (C. Poirret)

https://cyber.gouv.fr/supervision-securite (C. Poirret)

Il est fréquent d'entendre parler de "détection d'incidents", voire de "détection" pour désigner la "supervision de sécurité". Les aspects de qualification et de choix de la réaction appropriée sont néanmoins indissociables.

2.2. Distinction entre supervision informatique et supervision de sécurité

La vie d'un SI est ponctuée de multiples événements anormaux. Une part de ces événements est intrinsèque à l'utilisation de l'informatique. Ils peuvent être liés à l'exploitation de SI (ex. : taux d'occupation élevé des disques après plusieurs années de production). Ils peuvent être provoqués par des éléments techniques d'un niveau de qualité insuffisant (ex. : défauts logiciels). Souvent, leurs effets sont aisément observables (ex. : consommation excessive de ressource, indisponibilité). Dans tous les cas, ils relèvent de la **supervision informatique**[2], qui a vocation à relever les anomalies techniques et anticiper les dysfonctionnements liés à l'exploitation normale d'un SI.

Une autre part des événements peut être provoquée intentionnellement (ex. : exploitation de vulnérabilités, surcharge des capacités, mise hors service du SI, altération de son fonctionnement, fuite d'informations, prépositionnement silencieux). Ils sont la conséquence d'une activité malveillante. Cette dernière peut également inclure des techniques de dissimulation, rendant les événements peu observables et difficiles à détecter. Ces événements relèvent de la **supervision de sécurité**.

Cette représentation, reposant sur la nature des événements, aide à comprendre les périmètres théoriques de deux formes de supervision. Cependant, sur le terrain, elles sont souvent intriquées.

En effet, la supervision de sécurité peut également être utilisée pour détecter des anomalies techniques non intentionnelles liées à la sécurité. C'est le cas lorsque des règles de conformité vérifient la bonne application des règles de la politique de sécurité des systèmes d'information (PSSI). Ainsi, les écarts à la PSSI peuvent renseigner sur l'état technique du parc (ex. : niveau de mise à jour et taux de couverture du déploiement d'un correctif).

À l'inverse, la supervision technique peut concourir à la détection d'incidents de sécurité. Par exemple, certaines anomalies techniques (ex. : indisponibilité, saturation des capacités) peuvent être le signe d'une possible compromission et nourrir la qualification d'un incident de sécurité.

2.3. L'écosystème de la supervision de sécurité

La supervision de sécurité contribue, avec le renseignement sur la menace[3] et la réponse à incidents, au traitement des incidents de sécurité. De plus, elle interagit avec d'autres fonctions internes de l'organisation : la gouvernance et la gestion opérationnelle des systèmes d'information. La figure 1 présente l'écosystème rapproché de la supervision de sécurité, qui articule ces différentes fonctions.

La supervision de sécurité n'est donc pas une fonction indépendante. Pour être efficace, elle doit s'intégrer dans un écosystème et interagir de manière fluide avec différentes fonctions.

La **gestion opérationnelle des systèmes d'information** (ou gestion des SI) couvre les dimensions métiers, les infrastructures et les aspects préventifs de la sécurité des SI, quelle que soit la répartition des fonctions au sein de l'entité. Cela inclut en particulier la planification, l'intégration, la maintenance et l'exploitation de tout type d'éléments techniques (ex. : services et applications, infrastructures techniques, segmentation et cloisonnement, dispositifs techniques de sécurité). Les interactions de la supervision de sécurité avec la gestion des SI vont dans les deux sens. La supervision de sécurité ne peut se déployer de façon pertinente que sur la base de connaissances statiques ou dynamiques[4] détenues par la gestion des SI. Par ailleurs, la supervision va solliciter régulièrement les équipes techniques de la

[1]La directive NIS2 [1] définit un incident comme "un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles".

[2]Ce terme est une traduction de *information technologies monitoring*. Cette supervision peut se focaliser sur différents aspects du SI. Par exemple, l'état des éléments d'infrastructure (supervision technique), ou la qualité des services rendus (supervision de service).

[3]L'acronyme anglais CTI pour *Cyber Threat Intelligence* est le plus couramment utilisé.

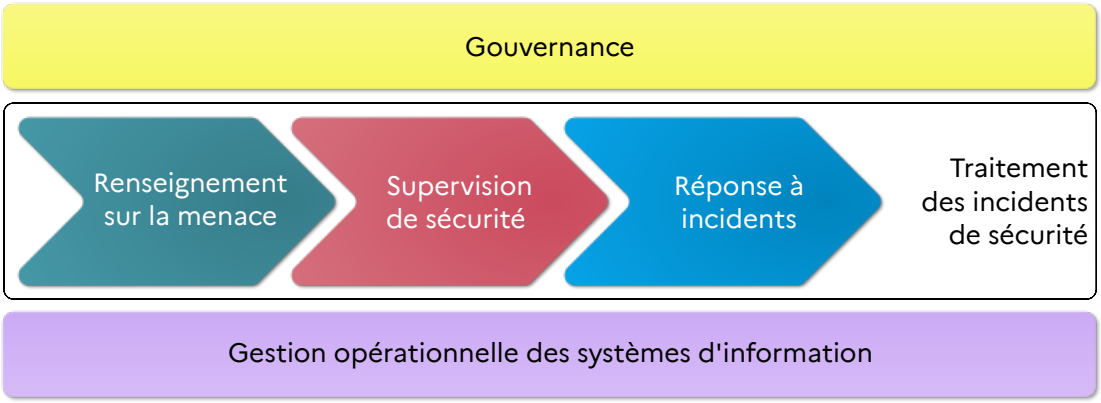

Figure 1: Écosystème rapproché de la supervision de sécurité

gestion des SI pour contextualiser les alertes et améliorer sa compréhension des activités détectées. Cet échange soutient le processus d'amélioration continue du périmètre supervisé et de la supervision.

La **gouvernance** inclut toutes les fonctions décisionnelles de l'entité (schématiquement, le comité exécutif, ou conseil de direction). Les relations entre la supervision et la gouvernance sont réciproques. La gouvernance fournit notamment les moyens financiers et humains. Elle sponsorise la supervision de sécurité et la rend crédible en tant que ligne de défense. Par ailleurs, elle formalise des orientations cyber au travers de la PSSI. En outre, elle valide la stratégie de supervision de sécurité. Pour sa part, la supervision de sécurité décline une stratégie de supervision de sécurité conformément aux orientations cyber. De plus, elle produit des éléments permettant le suivi et la valorisation de son activité.

Le **renseignement sur la menace** contribue au traitement des incidents de sécurité en fournissant à la supervision de sécurité les ressources indispensables pour la conception et l'amélioration des règles de détection. La qualité et la complexité de ces ressources varient selon les sources. Il s'agit parfois de listes d'indicateurs de compromission[7] (ex. : adresse IP, noms de domaine). En revanche, il peut s'agir de formes beaucoup plus riches de renseignements, obtenues par diverses actions d'investigation et d'enrichissement de l'information sur la menace. Si sa qualité conditionne l'efficacité de la détection, il faut toutefois un alignement entre le niveau des renseignements acquis et la capacité de la supervision de sécurité à intégrer ces éléments. Par ailleurs, l'offre existante permet de facilement externaliser le renseignement sur la menace, voire même la création de règles de détection. Dans une telle hypothèse, la supervision de sécurité sélectionne les renseignements d'intérêt pour son contexte spécifique.

La **réponse à incidents** contribue au traitement des incidents de sécurité en fournissant différentes stratégies d'action (ex : résolution purement technique des incidents mineurs, remédiation[8], gestion de crise[9]). À ce titre, la relation avec la supervision de sécurité est à double sens. D'une part, la supervision de sécurité active la réponse à incidents, et lui fournit tous les éléments de caractérisation de l'incident. D'autre part, la réponse à incidents peut solliciter les services de la supervision de sécurité. Notamment, pour localiser sur un SI, le périmètre des actions malveillantes afin d'optimiser l'effort de réponse. Ou encore, opérer un suivi à l'issue d'une réponse à incidents pour surveiller d'éventuelles persistances ou reprises d'activités malveillantes.

La mise en œuvre du traitement des incidents sous forme d'un processus linéaire tel que présenté en figure 1 constitue une cible intéressante pour un projet de supervision de sécurité. Cependant, l'état de

[4]Les connaissances sont statiques lorsqu'on parvient à les documenter (ex. : cartographie du SI[5], analyse de risque[6], procédures d'exploitation, matrice de flux, planification des opérations, dossier d'architecture des dispositifs techniques de sécurité existants). Les connaissances dynamiques concernent des événements relatifs à la vie du SI (ex. : pratiques d'administration, statut d'une opération en cours, incidentologie).
[5]Voir le guide "Cartographie du système d'information" [2] de l'ANSSI.
[6]Voir le guide "La méthode EBIOS Risk Manager - Le Guide" [3] de l'ANSSI.
[7]L'acronyme anglais IoC pour *Indicator of Compromise* est le plus couramment utilisé.
[8]Voir le guide "Cyberataques et remédiation - Les clés de décision" [4] de l'ANSSI.
[9]Voir le guide "Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique" [5] de l'ANSSI.

l'art en la matière correspond à une organisation en boucle fermée. Dans ce cas, les activités de réponse à incidents ont la capacité d'alimenter le renseignement sur la menace (ex. : éléments obtenus par analyse forensique), en enrichissant sa connaissance et orientant ainsi ses recherches. Cette configuration spécifique correspond à un haut niveau de maturité (en particulier, la maîtrise interne de toutes ces activités).

2.4. Les événements de sécurité

Une fonctionnalité clé de la supervision de sécurité est l'analyse de données. Cette analyse est opérée en deux temps : d'abord, par une étape automatisée, ensuite par une étape manuelle.

La première étape identifie des événements significatifs (ie : événements de sécurité, alertes) à partir d'extraits d'activité du SI. Elle est réalisée par des systèmes automatisés, qui peuvent être chaînés (ex. : capteur distribué, outil d'analyse centralisé). Elle vise à traiter un gros volume de données en réduisant le plus possible le taux d'erreur. Le volume d'événements significatifs produit ne doit pas excéder la capacité de traitement de la seconde étape.

Ces événements de sécurité sont ensuite vérifiés, et éventuellement qualifiés en incidents de sécurité. Cette seconde étape est réalisée par une équipe d'analystes, qui s'appuie sur différentes méthodes (ex. : recoupement, pivot, corrélation, investigation). L'objectif est d'identifier les événements qui caractérisent un incident de sécurité, en comprenant le plus précisément possible les activités malveillantes qui en sont à l'origine.

Un classement fréquemment utilisé pour rendre compte de l'efficacité de la première étape s'appuie sur la matrice de confusion[10]. Cette méthode confronte la prédiction d'un système automatisé à la réalité. Elle permet de distinguer quatre catégories :

- les vrais positifs : le système prédit correctement la présence d'une activité malveillante ;
- les vrais négatifs : le système prédit correctement l'absence d'une activité malveillante ;
- les faux positifs : le système prédit mal l'absence d'une activité malveillante ;
- les faux négatifs : le système prédit mal la présence d'une activité malveillante.

Les deux premières catégories correspondent au fonctionnement attendu (absence d'erreur). La troisième catégorie induit une surcharge inutile des capacités de traitement en aval du système automatisé (dans le cas présent, l'équipe d'analystes). Cependant, elle est facilement observable. La dernière catégorie correspond à des cas où le système automatique ne remplit pas son rôle (dans le cas présent, détecter une activité malveillante). Et elle est difficile à observer.

3. Les composantes d'une supervision de sécurité

Les objectifs métier de la supervision de sécurité s'appuient sur des moyens humains, organisationnels et techniques spécifiques. Le présent chapitre propose un panorama de ces moyens : les personnes et ce qu'elles font, les données, les systèmes techniques qui les traitent et les règles de traitement.

3.1. Les analystes

Les analystes composent l'équipe de supervision de sécurité. La fonction la plus évidente consiste à vérifier des événements de sécurité et, le cas échéant, qualifier des incidents de sécurité.

Mais cela ne représente qu'une petite partie des missions de l'analyste. Ses compétences lui permettent d'intervenir en soutien de chacun des processus de la supervision décrits dans la section 3.4. Le panel d'activités est si large qu'il permet la spécialisation des profils.

De manière générale, ces activités comprennent des tâches complexes, et des prises de décisions soumises au contexte. Par exemple, les recoupements à faire pour un type d'alerte donné, les pivots

[10]Voir le cours "Confusion matrix" [6] de la *Mahatma Gandhi Central University*.

à réaliser dans les différentes sources de données, les activités qui méritent d'être creusées dans un contexte et pas dans un autre. C'est pour cela qu'elles ne sont pas automatisables à l'heure actuelle.

Toutes les composantes d'une supervision de sécurité décrites dans le présent chapitre sont au service des analystes.

3.2. Les données de supervision

La section 2.4 décrit l'analyse des données réalisée par la supervision de sécurité. L'efficacité de cette analyse dépend des caractéristiques des données traitées :

- elles sont **signifiantes** : elles reflètent l'activité du SI ;
- elles sont **pertinentes** : pour chaque type de source de données (ex. : logs de parefeux), le point de capture doit avoir du sens au regard des enjeux de sécurité (ex. : aider à détecter un événement redouté) ;
- elles sont **diversifiées** : elles proviennent de multiples sources de données (ex. : logs système, logs de parefeux, trafic réseau). Cela permet, par exemple, d'effectuer des pivots d'une donnée à l'autre sur la base d'un champ commun (ex. : pivoter d'une donnée décrivant du trafic réseau à une donnée décrivant des activités systèmes sur la base d'un couple adresse IP et horodatage). En contrepartie, il est nécessaire de normaliser les données avant leur traitement ;
- elles sont **enrichies** : filtrer les données les moins signifiantes, ajouter de l'information (ex. : géolocalisation d'une adresse IP) ou agréger des événements similaires permet d'améliorer la lisibilité de la donnée. Cela ouvre la voie à des corrélations plus riches que les pivots.

Les caractéristiques des données de supervision découlent de la stratégie de supervision.

3.3. La stratégie de supervision

La stratégie de supervision est un document conçu par l'équipe de supervision de sécurité pour son usage interne. De fait, son élaboration vise à répondre concrètement à ses besoins. Par exemple, décrire les objectifs, les moyens, les priorités, la trajectoire, les meilleurs choix du point de vue de la supervision de sécurité. Il s'agit en premier lieu d'un outil de réflexion, qui conduit à la rédaction d'un document formel au fil de la montée en maturité de la supervision de sécurité.

Au cœur de la réflexion sur la stratégie de supervision se trouve le lien entre :

- des objectifs de sécurité (ex. : ce que je veux détecter, ce que je veux suivre) correspondant aux orientations de sécurité actées par la gouvernance (ex. : PSSI) ;
- des familles de données de supervision (ex. : des journaux système, de l'activité réseau) et des points de collecte pertinents (ex. : en bordure du SI, au sein d'une zone spécifique) ;
- des règles de détection qui analysent les données de supervision collectées.

Ce document précise également les moyens mobilisés (ex. : financiers, humains, organisationnels, techniques). De plus, il aide à comprendre le fonctionnement général de la supervision vis-à-vis du périmètre supervisé. Enfin, il aide à formaliser le fonctionnement de la supervision de sécurité (ex. : les processus), tant d'un point de vue général que les déclinaisons spécifiques à chaque SI supervisé.

La structure et le contenu de la stratégie de supervision sont étroitement liés aux objectifs de supervision. Ces objectifs peuvent être orientés vers la menace (ex. : détecter un acteur de la menace spécifique, détecter des tactiques et techniques d'attaque comme les exfiltrations de données) ou vers la surveillance du SI (ex. : détecter tout type d'activité inhabituelle sur un actif donné, détecter un écart à la politique de sécurité).

La rédaction d'une stratégie de supervision s'appuie sur des éléments d'entrée fournis par la gouvernance et par la DSI (cf. section 2.3 décrivant l'écosystème de la supervision). La qualité et la complétude de ces éléments sont très liées à la maturité de la gestion opérationnelle des SI. Par exemple, la cartographie est rarement exhaustive, la PSSI n'existe pas toujours.

Les éléments requis dans une stratégie de supervision sont les moyens alloués (financiers, humains), et l'analyse de risque du SI supervisé. Lorsqu'il n'existe pas d'analyse de risque formalisée, une analyse partielle doit être réalisée pour identifier le périmètre du SI, le niveau de menace maximum auquel ce SI est exposé (ex. : menace hacktiviste et isolée, menace cybercriminelle et systémique ou menace étatique et ciblée), et les principaux événements redoutés. Cette analyse doit être complétée par une démarche formelle[11] dès que possible.

Le reste du document peut présenter des différences sur le fond ou sur la forme, selon le contexte de la supervision et la maturité de l'entité gérant le SI supervisé. Dans tous les cas, il est recommandé d'être pragmatique et de se limiter à du contenu utile et actionnable pour les équipes de supervision.

Voici quelques exemples d'éléments à intégrer à la stratégie de supervision :

- **Les objectifs de supervision et les données associées** : liste les activités malveillantes à détecter et les scénarios de menace associés, identifie les sources de données qui permettraient de détecter chaque scénario, et le type de données qu'il est nécessaire d'extraire de ces sources (ex. : journaux d'activité du serveur mandataire au niveau de verbosité "info") .
- **L'architecture technique de la supervision** : prend en compte les choix techniques structurants (ex. : choix de technologies, choix d'implémentation, choix d'agencements), les types de règles métier associés (ex. : *workflow* adapté, langage de règle de détection). Lorsque des périmètres nécessitent ce niveau de détail, les choix de capteurs, et leurs implantations sur le SI supervisé, etc.
- **La gouvernance de la supervision** : inclut les parties prenantes et leurs rôles et responsabilités. En particulier, la description du niveau d'externalisation pour chaque processus décrit dans la cartographie proposée sur la figure 2.

Le rythme de révision de ce document dépend de la maturité de la supervision de sécurité. Dans les premiers mois après sa création, il va s'étoffer régulièrement au rythme des élargissements de périmètres. Dans un second temps, des mises à jour annuelles permettent d'intégrer les évolutions des pratiques et la montée en maturité. Ce n'est qu'au-delà d'un certain niveau de maturité que les révisions sont plus espacées.

> La stratégie de supervision est différente de la convention de service (ou contrat de service) en cas d'externalisation. Cette dernière ne s'adresse pas aux mêmes parties prenantes, et ne présente pas le même niveau de détail. Elle stipule à un client les stratégies que le prestataire s'engage à déployer pour fournir son service. Un tel document peut présenter de façon détaillée certains éléments cités ci-dessus, sous forme de stratégie d'analyse, stratégie de collecte, stratégie de notification, stratégie d'incidents, etc.

3.4. Les processus de la supervision

3.4.1. Processus métier

La figure 2 propose une vue synthétique des processus métier qu'il est nécessaire d'animer. Y sont représentées des activités récurrentes, qui encerclent les processus d'analyse, et des activités relationnelles, plus proches des différentes parties prenantes de l'écosystème de la supervision de sécurité. En revanche, la capitalisation, qui s'applique à tous les processus et permet à la supervision d'apprendre, n'est pas matérialisée.

Voici quelques détails pour chacun des processus :

- **Définition des attentes et des moyens** : rassemble les activités de conception de la stratégie de détection, et la déclinaison de cette stratégie en orientations pour chacun des autres processus.
- **Indicateurs et tableaux de bord** : fournissent de l'information décisionnelle pour décrire l'activité de la supervision de sécurité, et orienter les décisions opérationnelles, tactiques (internes) et stratégiques (au niveau de la *gouvernance*).

[11] Voir le guide "La méthode EBIOS Risk Manager - Le Guide" [3] de l'ANSSI.

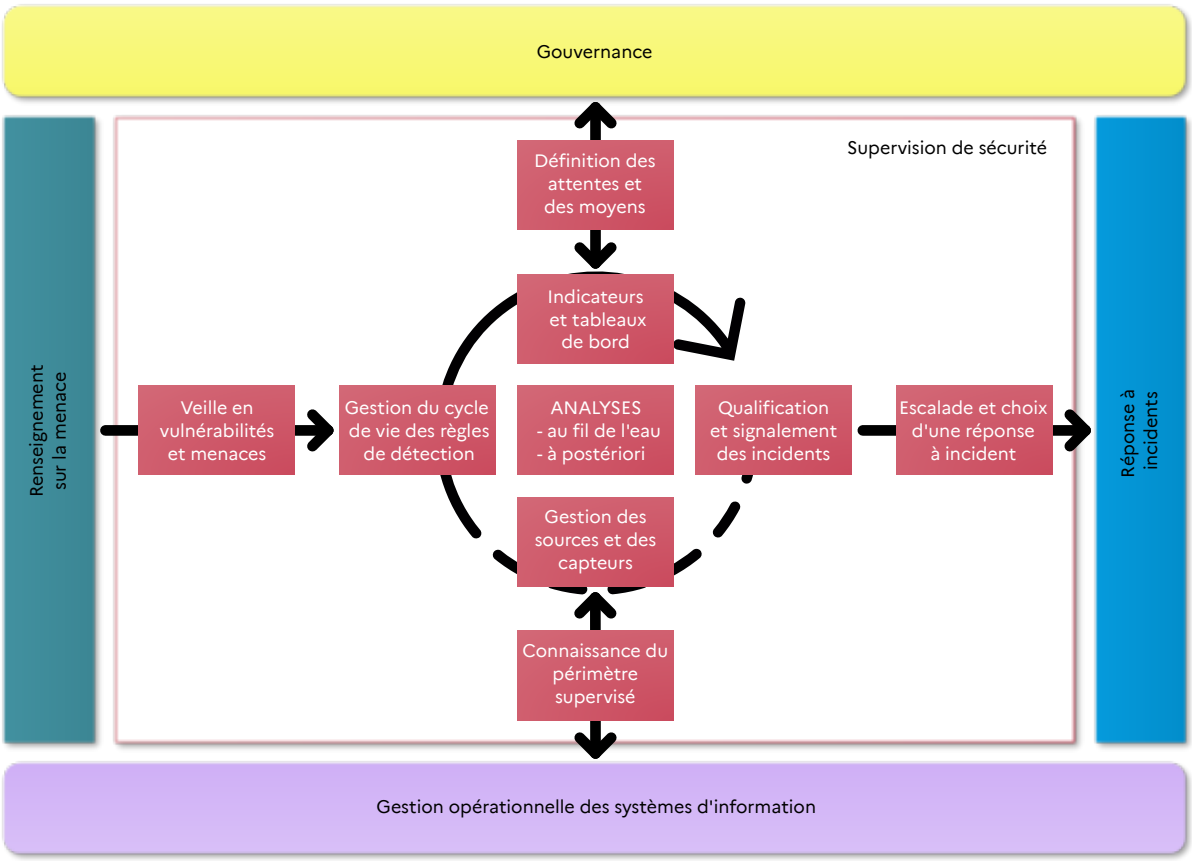

Figure 2: Cartographie des processus métiers

- **Veille en vulnérabilités et menaces** : travaille en lien avec le *renseignement sur la menace* et l'écosystème élargi du traitement des incidents de sécurité (les CERT (*Computer Emergency Response Team*), l'InterCERT France[12] et les autres communautés d'intérêts), pour obtenir des éléments adaptés au périmètre supervisé. Ces éléments concernent la menace, par exemple les tactiques, techniques et procédures correspondantes à des acteurs de la menace identifiés. Ils concernent également les vulnérabilités auxquelles le périmètre supervisé est sensible, en fonction de son architecture et de son implémentation.
- **Gestion du cycle de vie des règles de détection** : à partir des éléments collectés par la veille en vulnérabilités et menaces, consiste à ajouter des règles (conçues en interne ou obtenues auprès d'un tiers), à les tester et les adapter au contexte d'emploi, puis à les maintenir en condition opérationnelle. Le cas échéant, elles peuvent être décommissionnées. Cela implique de gérer le stockage, le versionnement et le statut des règles.
- **Connaissance du périmètre supervisé** : s'appuie sur toutes les composantes de la *gestion opérationnelle des SI* (métiers, infrastructures et sécurité des SI) pour développer la connaissance de chaque SI supervisé selon deux axes. En premier lieu, connaître le SI en le cartographiant selon différents points de vue (ex. : technologies, données, processus, métiers). Et en second lieu, connaître les risques auxquels ce SI est soumis, en les analysant de manière formelle.
- **Gestion des sources et des capteurs** : choisis et fait évoluer une combinaison de sources et de capteurs pour chaque SI du périmètre supervisé. Cette combinaison doit viser un équilibre entre le besoin de détection, la couverture fonctionnelle des sources et capteurs choisis, et les coûts d'acquisition et d'exploitation.
- **Analyse au fil de l'eau** : se déroule sur des données de détection, au fil de leur collecte et de leur

[12] Communauté française de CERT, ouverte aux entités disposant d'une équipe de supervision de sécurité ou de réponse à incidents.

traitement (ex. : enrichissement). Cette analyse automatisée consiste à confronter les données collectées aux règles de détection afin de générer des alertes. Selon la source de données, cette analyse est réalisée soit au plus proche de la collecte, dans un capteur (ex. : sonde réseau), soit après centralisation des données.

- **Analyse à postériori** : sélectionne une fenêtre temporelle passée, éventuellement un sous-ensemble de données, et y applique certaines règles de détection. Cela permet de rechercher des éléments techniques qui n'étaient pas connus au moment où les données ont été collectées et stockées. Une telle analyse permet d'identifier après coup une menace inconnue auparavant (ex. : exploitation d'une faille jour zéro). Elle permet également de remonter le fil d'une compromission lorsque celle-ci est détectée.
- **Qualification et signalement des incidents** : produisent *in fine* des incidents avérés, associés à une criticité, une description des activités malveillantes relevées, et toutes les alertes qui ont alimenté la description. Qualifier un incident consiste à vérifier la légitimité d'une activité qui a levé une ou plusieurs alertes. L'objectif est d'éliminer les faux positifs. Pour ce faire, il est parfois nécessaire de signaler l'incident à la DSI, qui a la connaissance pour contextualiser l'activité relevée et déterminer sa légitimité. Ce processus produit *in fine* des incidents avérés, associés à une criticité, une description des activités. malveillantes relevées, et toutes les alertes qui ont alimenté la description.
- **Choix et suivi d'une réponse à incidents** : proposent une réponse à apporter à chaque incident et assurent le suivi de cette réponse. La proposition initiale est établie sur la base de la criticité associée à l'incident et de la description de l'activité malveillante qui en est à l'origine. Le suivi assure une meilleure interaction avec l'équipe de réponse à incidents, qui est amenée à réévaluer la proposition initiale. Par ailleurs, les capacités de réponse doivent être préparées en amont pour être pleinement opérationnelles. Cela garantit une continuité de traitement de l'incident entre la supervision et la réponse.

3.4.2. Processus support

La supervision de sécurité s'appuie également sur des processus support. Ils mobilisent des compétences techniques différentes entrant dans le domaine général de la gestion des SI. La liste suivante ne prétend pas être exhaustive, les processus support d'un SI de supervision étant les mêmes que ceux de tout SI.

- **Planification et management du périmètre technique** : prennent en compte et gèrent les besoins de la supervision. En particulier, le niveau de disponibilité visé, les débits souhaités, les durées de rétention nécessaires, les compétences techniques disponibles, et les coûts de démarrage et de maintenance.
- **Conception et architecture du SI** : assurent la conception globale du SI de supervision, la revue et l'amélioration de sa couverture fonctionnelle, ainsi que la revue et l'amélioration de sa sécurité.
- **Intégration des briques techniques** : met en place et configure les briques techniques conformément aux besoins.
- **Exploitation du SI** : gère l'annuaire, ainsi que le maintien en condition opérationnelle et de sécurité des briques techniques.

3.5. Les règles métier

3.5.1. Règles de gestion

Les règles de gestion formalisent les choix retenus pour implémenter les processus métier et la matrice de communication au sein d'une structure. Par exemple : qui répond au téléphone en heures non ouvrées ? Qui doit être notifié et selon quels critères d'escalade ? Combien de fois relance-t-on un interlocuteur ?

Elles transparaissent dans les processus, les procédures opérationnelles et les fiches réflexe de la base de connaissances propre à la supervision de sécurité. Elles peuvent être traduites sous forme de

workflows ou de paramètres de configuration dans les outils informatiques. C'est tout l'intérêt de leur formalisation : adapter des outils aux besoins du métier, et non l'inverse.

3.5.2. Règles de détection

Les règles de détection sont une déclinaison technique de la stratégie de supervision. Elles comportent trois dimensions en proportions variables : la connaissance de la menace, la prise en compte du contexte technologique et la maîtrise de l'agencement technique spécifique à un SI.

Les règles sont intégrées dans des systèmes automatisés tels que décrits dans la section 2.4 traitant des événements. Elles représentent la partie "programmable" de ces systèmes, qui peut traiter des flux de données brutes ou enrichies. Elles définissent les critères d'émission d'un événement de sécurité, qui sera traité en aval du système automatisé.

Les règles peuvent être génériques (appliquées sur un large spectre de données enrichies) ou spécifiques (appliquées au niveau d'un capteur, sur le type de données brutes captées). Elles peuvent être transcrites dans des formats d'échange plus ou moins spécialisés (ex. : SIGMA, YARA, JSON-MISP, pseudo-code). Elles peuvent reposer sur une signature (résumé de caractéristiques déjà rencontrées) ou être comportementales (c.-à-d. détecter une déviance par rapport à un comportement appris). Les règles et leur complexité évoluent avec la maturité de la supervision de sécurité.

La conception des règles de détection doit être effectuée avec le souci de réduire le taux d'erreur du système automatisé. C'est-à-dire réduire l'écart entre les alertes générées et celles qui correspondent effectivement à une activité malveillante (cf. paragraphe 2.4). Dans cette optique de réduction du taux d'erreur, il est également nécessaire d'adapter la sensibilité des règles aux spécificités du SI supervisé. Une méthode fréquemment utilisée par les analystes consiste à ajouter une liste d'exemptions à une règle pour assouplir le critère d'émission d'un événement de sécurité (*white listing*).

3.6. Le SI de supervision

La capacité de supervision nécessite la mise en place d'outils adaptés. La présente section décrit un système de supervision type, illustré par la figure 3, sous l'angle des familles d'outils utilisés par les analystes.

> Lorsque l'on souhaite doter un SI d'une capacité de détection, la première étape consiste à s'appuyer sur des solutions déjà déployées sur le SI. Par exemple, l'antivirus détecte certaines actions malveillantes. C'est pour cela que les attaquants tentent parfois de le désactiver. Pourtant, ces deux types d'activités (alertes antivirales et tentatives de désactivation) sont rarement surveillées. L'antivirus illustre le cas d'un outil souvent présent sur le SI qui constitue une source d'information à forte valeur ajoutée.

- **Les collecteurs** sont disséminés sur le périmètre supervisé. Ils acheminent des événements (ex. : journaux d'activité) vers la partie centralisée du SI de supervision, sans les altérer. Une chaîne de collecte peut être réalisée à base d'agents de transfert (ex. : rsyslog, Windows Event Forwarding, agent *beats pour Elasticsearch, Splunk Forwarder), ou à base de file d'attente de messages (*message queuing*). En outre, la topologie de la chaîne de collecte doit s'adapter à de nombreux facteurs liés au SI supervisé et au SI de supervision.
- **Les capteurs** sont également disséminés sur le périmètre supervisé (ex. : sonde réseau, antivirus). Ils analysent localement certaines activités du SI (ex. : activité réseau, système, applicative, utilisateur) et émettent des alertes. En général, les capteurs sont gérés par une console centrale. Certains capteurs peuvent être pilotés (ex. : remonter, à la demande, un contenu de fichier dont le nom apparaît dans une alerte). Certains peuvent réaliser des actions de réponse à incidents prédéfinies (ex. : mettre un fichier en quarantaine, interdire un flux réseau, verrouiller un compte utilisateur).

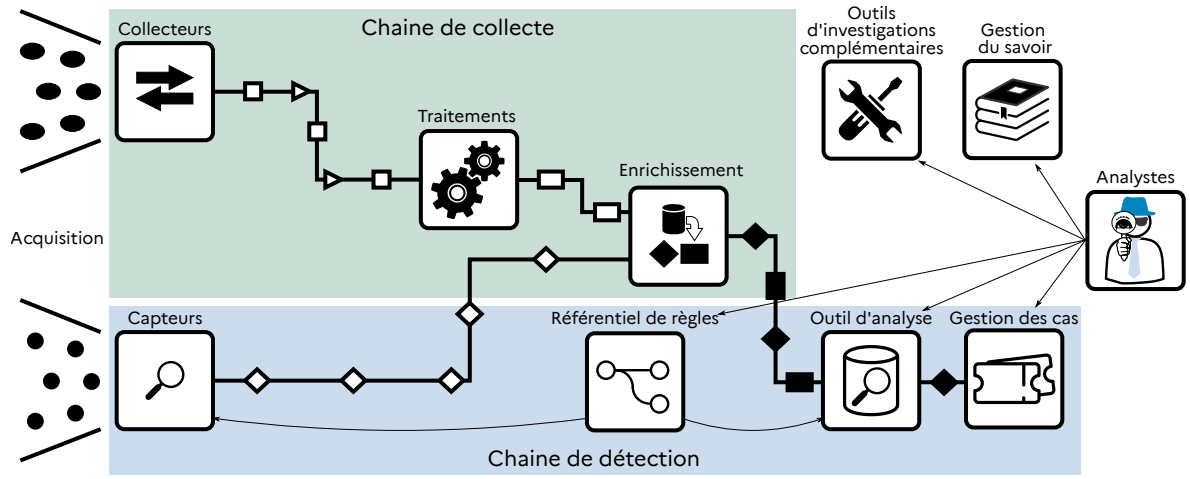

Figure 3: Architecture fonctionnelle d'un SI de supervision de sécurité

- **Les traitements** incluent la normalisation des événements pour faciliter leur analyse (ex. : ajout ou renommage des colonnes d'un fichier journal). Ils comprennent également le filtrage des événements non pertinents (ex. : multiples événements Windows correspondant à une seule ouverture de session).
- **L'enrichissement** ajoute de la valeur aux données traitées, soit à partir de bases spécialisées (ex. : GeoIP), soit par agrégation (ex. : rassembler plusieurs événements, identiques ou apparentés, en un seul de poids supérieur).
- **L'outil d'analyse** stocke et indexe les événements et les alertes pour en faciliter l'exploitation. Il utilise des règles de détection pour automatiser une partie de l'analyse et générer des alertes. Il propose des interfaces graphiques et des visualisations de données (*data visualisation*) qui aident à analyser ces données en permettant des recherches, des tris, des filtres. L'analyste utilise cet outil pour traiter chaque alerte, qualifier les incidents de sécurité, et identifier les faux positifs.
- **L'outil de gestion de cas** (*ticketing*) permet de suivre, de tracer et de coordonner les différentes activités d'investigation des analystes. Il peut également intégrer des capacités d'automatisation de certaines actions d'investigation.
- **Le référentiel de règles** soutient le cycle de vie des règles, quel que soit le dispositif sur lequel elles sont déployées.
- **Les outils d'investigations complémentaires** permettent aux analystes de lever le doute sur des éléments identifiés par l'outil d'analyse. La conception de ces outils vise au moins deux objectifs. Le premier est de limiter le risque associé à l'analyse d'éléments potentiellement dangereux (ex. : détonation de binaire dans une *sandbox*). Le second est de réduire le risque de fournir à un potentiel attaquant, de l'information sur les activités de défense à travers des actions d'investigation (ex. : bases locales de condensats (*hash*) de fichiers et autres bases de connaissance hors-ligne).
- **Les outils de gestion de la connaissance** mettent à disposition divers types d'informations sur le fonctionnement de la supervision de sécurité (ex. : fiches réflexe, procédures), sur le périmètre supervisé (ex. : cartographie du périmètre supervisé, nomenclature) ou sur les règles de détection (ex. : déploiement, documentation). Ils permettent la capitalisation du savoir.

4. Les enjeux d'un projet de supervision de sécurité

La problématique que cherche à résoudre la supervision de sécurité est complexe. Elle consiste à distinguer les activités malveillantes des activités légitimes, avec un niveau de fiabilité élevé, malgré l'incertitude induite par l'évolution des menaces, des techniques d'attaque, et du SI supervisé. Il

en résulte que l'efficacité des solutions techniques existantes pour superviser dépend de nombreux facteurs (ex. : volume et qualité des données à traiter, fiabilité et sensibilité des dispositifs de traitement automatique).

Par conséquent, créer cette capacité et la maintenir dans le temps nécessitent d'importants moyens. Il est donc essentiel d'avoir une bonne compréhension des enjeux pour mobiliser ces ressources au mieux.

Ce chapitre passe en revue les différentes familles d'enjeux inhérents à la supervision de sécurité. Le grand nombre de thèmes couverts par cette énumération ne doit pas provoquer un effet paralysant face à l'ampleur de la tâche. L'ambition poursuivie ici est de balayer un large panel d'enjeux pour donner l'opportunité de les reconnaître lorsqu'ils se présentent. Enfin, ce chapitre s'achève sur un changement de perspective permettant d'aborder les risques liés à ces enjeux.

4.1. Les enjeux stratégiques

Les enjeux stratégiques se présentent principalement au sein de la gouvernance.

- **Questionner le sentiment de sécurité**. Un investissement conséquent et une mise en œuvre rigoureuse ne doivent pas occulter le caractère mouvant tant de la menace que du SI supervisé. Cet enjeu peut être surmonté en impliquant la gouvernance dans la démarche d'amélioration continue de la supervision de sécurité. En effet, informer les décideurs des améliorations envisagées et des évolutions du contexte est une manière de matérialiser le fait que l'outil est imparfait. Cela permet également de maintenir une certaine conscience que le budget est très souvent le facteur limitant pour l'atteinte du résultat. La supervision de sécurité doit développer une image basée sur la confiance, sans verser dans l'excès.
- **Garantir la continuité de l'amélioration continue**. En particulier, lorsque la supervision de sécurité produit des résultats positifs stables, et détecte des activités malveillantes jusqu'à un certain seuil de complexité, il peut être nécessaire de poursuivre les investissements pour détecter des activités malveillantes plus avancées. Obtenir cet effort de la part des sponsors peut s'avérer très difficile en absence de preuve irréfutable. Le défi est de parvenir à positionner la supervision au juste niveau des menaces contre lesquelles l'entité souhaite se protéger. Une bonne manière de traiter cet enjeu consiste à baser sa stratégie de supervision sur une analyse de risque. De plus, évoquer avec la gouvernance l'écart à la cible matérialise la distance qu'il reste à parcourir et les effets de seuil qui peuvent jalonner le parcours.
- **Faire preuve de discernement technique**. Cela évite d'acquérir des produits, sans parvenir à les utiliser à bon escient pour couvrir efficacement le périmètre à superviser. Cet enjeu peut être surmonté grâce à une stratégie de supervision reposant sur une analyse de risque, en particulier en identifiant les capteurs, les sources de données et les règles les plus pertinents pour détecter les méthodes d'attaque qui mènent aux événements redoutés.
- **Garder les objectifs cyber en ligne de mire**. Cela permet notamment de se prémunir du biais de performance, qui revient à porter une attention excessive à la performance d'un dispositif. Si les indicateurs de performance sont à même de rendre compte de l'activité d'une supervision, aucun ne permet de mesurer si elle remplit son rôle de détection et de caractérisation d'activités malveillantes. Par exemple, le temps moyen de résolution des incidents, ou encore, le nombre d'incidents mensuels peuvent masquer des activités malveillantes non détectées.

4.2. Les enjeux projet

Les contraintes qui s'appliquent à un projet sont souvent représentées par un triangle "coût, qualité, délais"[13] qui met en évidence les dépendances entre les trois sommets (ex. : réduire le budget impacte le délai et/ou la qualité). Dans le contexte d'un projet de supervision de sécurité, il est important de concevoir un compromis adapté entre ces trois contraintes.

[13] Martin Barnes, 1969, cité par Vahidi et Greenwood, [7].

- Le **budget** doit être cohérent avec le périmètre supervisé, et les objectifs de détection. Dans une logique d'amélioration continue, il est recommandé de prévoir plusieurs itérations, sur plusieurs exercices budgétaires. Cela permet également d'échelonner les coûts d'une façon prévisible (ex. : élargir le périmètre, enrichir les sources de données de détection, ajouter des fonctionnalités). En outre, le coût de maintenance de la capacité de supervision de sécurité doit être considéré avec attention.
- La **qualité** correspond à la cible fonctionnelle du projet, qui dépend du périmètre et du contexte. Elle est définie dans la stratégie de supervision. Par conséquent, utiliser la qualité comme facteur d'ajustement du projet accroît fortement le risque d'une supervision inefficace. En revanche, il est recommandé de fixer des sous-objectifs, qui pourront être atteints par itérations successives, dans une logique d'amélioration continue. Cela permet d'avancer progressivement, et de surveiller la trajectoire du projet.
- La **planification** du projet doit être considérée sur le long terme. En effet, la construction de la capacité est autant un projet technique qu'un projet de transformation organisationnelle et d'acquisition de compétences et d'expérience. Cela signifie que le facteur humain a plus d'impact que les délais de réalisation technique. Par conséquent, la planification doit reposer sur la progression de l'équipe de supervision, qui évolue par paliers. Ces paliers représentent le temps incompressible d'"assimilation" et de "maturation" des savoirs acquis par l'expérience.

4.3. Les enjeux humains

Ce paragraphe s'intéresse aux enjeux humains qui découlent spécifiquement de l'activité de supervision de sécurité. Il exclut les enjeux humains génériques (ex. : erreurs, négligences, actions malveillantes) et ceux liés au domaine d'activité de la cybersécurité (ex. : disponibilité des profils).

- Éviter la **fatigue des alertes**. Cette forme spécifique de fatigue est inhérente au fait de travailler en aval d'un système automatisé (cf. section 2.4). Elle se manifeste suite au traitement répétitif de faux positifs très semblables. Cette fatigue entraîne la récurrence d'analyses partielles, et l'augmentation du nombre d'incidents non détectés. Pour les analystes, elle se traduit par de la démotivation et du désintérêt pour le métier. Il est à noter que cette fatigue peut être difficile à déceler, et qu'elle peut s'installer même au sein d'une supervision qui produit de bons résultats.
- Identifier et atténuer les **divers biais** susceptibles de fausser l'appréciation des analystes : l'excès de confiance, et les biais de confirmation, d'automatisation, de complaisance, de normalité, d'information partagée, d'heuristique, et de disponibilité.
- Reconnaître et **célébrer les succès**. L'analyste est exposé beaucoup plus fréquemment à des faux positifs qu'à des incidents avérés. Cela entre en résonance avec notre tendance naturelle à accorder plus d'importance à l'échec qu'au succès. La conscientisation des succès n'est alors pas suffisante, il faut leur donner une portée qui résiste à l'usure des multiples faux positifs.
- Adapter le **management** aux spécificités des métiers de la supervision en le sensibilisant aux nombreuses tâches récurrentes (ex. : vérification d'alertes, investigations, déploiements) qui peuvent rapidement devenir intenables lorsqu'une difficulté se présente. On pourra également s'assurer que le management dispose des leviers pour tenir compte des progrès ou difficultés individuelles, par exemple en mettant en place des actions de soutien (ex. : acquisition ou renforcement de compétences, développement du savoir-être comme la gestion du stress, de la communication, des conflits).
- Gérer les **carrières**. Outre le recrutement de profils techniques adaptés, il convient d'être particulièrement attentif à la capacité à acquérir de nouvelles connaissances pour faire évoluer l'expertise au regard des évolutions du contexte de supervision.
- Prévenir l'**instrumentalisation du personnel**. Comme toutes les personnes en charge de fonctions critiques sur le SI, les différents profils impliqués dans un service de supervision sont susceptibles d'être ciblés. Selon le niveau de menace auquel est exposé le périmètre supervisé, différents risques doivent être pris en compte de manière adéquate (ex. : les vols d'authentifiants opportunistes, l'ingénierie sociale, ou encore la corruption).

- Adopter une **posture défensive adéquate**. Les choix en matière de stratégie de supervision (ex. : environnement trop contraint qui alourdit les procédures, sources de données mal choisies qui augmentent les faux positifs) peuvent représenter un frein pour attirer les talents capables de découvrir des activités malveillantes avancées. Cela peut également empêcher la fidélisation des profils déjà présents.

4.4. Les enjeux techniques

Les enjeux techniques, difficiles à identifier et à anticiper, concernent les systèmes techniques du SI de supervision de sécurité.

- Être **constant**. Couvrir le périmètre supervisé avec un équilibre coût/efficacité stable.
- Rester **aligné**. Maintenir une cohérence entre le système de supervision et le périmètre supervisé, en particulier parce que ce dernier évolue continuellement.
- Être **flexible**. S'adapter aux variations de charge qui peuvent découler de l'actualité (ex. : campagne d'attaques visant un secteur particulier), ou bien de la vie du SI supervisé (ex. : opérations de refonte impactant des règles de détection).
- Maintenir l'**expertise**. Garder le contrôle sur un empilement complexe de couches techniques.
- Anticiper et faire face aux **effets de seuil** et leurs impacts sur les performances des outils. Ils sont susceptibles d'affecter tout type d'outil (ex. : stockage, traitement). Ils sont très difficiles à prévoir. Ils se détectent souvent après dépassement, lorsque l'outil devient très lent. Ils peuvent orienter les décisions de répartir les fonctions techniques dans des outils spécialisés, dans le but de réduire la charge d'outils intégrés.

4.5. Les enjeux métier

Outre la mise en œuvre des prescriptions du présent document, les principaux enjeux qui permettent à la supervision de sécurité d'atteindre ses objectifs opérationnels de détection sont :

- Maximiser la **disponibilité des sources de données**. Il est probable qu'un attaquant cherche à camoufler son activité malveillante en empêchant la remontée des données de supervision. Ces techniques de dissimulation peuvent être difficiles à repérer (ex. : indisponibilité totale ou partielle d'une source de donnée). C'est pourquoi il peut être intéressant de surveiller la disponibilité des éléments techniques de collecte (cf. section 2.2).
- Choisir des **données représentatives**. Il est recommandé de diversifier les sources de données. Cela permet d'enrichir sa vision de l'activité du SI (ex. : réseau et système, en bordure et en interne). De plus, un travail de sélection des sources qualitatives s'avère le plus souvent profitable à long terme. Il limite le volume de données à traiter et privilégie les points de collecte permettant d'identifier les activités malveillantes redoutées.
- Maîtriser le **nombre d'incidents**. Un nombre excessif d'incidents est souvent symptomatique du manque de maîtrise d'un SI. Les pratiques mal encadrées et la généralisation des procédures d'exception génèrent trop d'alertes de sécurité. Cela peut également être lié à une mauvaise coordination entre la supervision et les opérations programmées sur le SI. Dans tous les cas, cela nécessite un plan d'action permettant d'aligner le SI avec les pratiques d'hygiène informatique.
- Réduire le **nombre de faux positifs**. Ils augmentent lorsque les règles ne sont pas adaptées aux spécificités du SI supervisé. Par exemple, des règles trop sensibles déclenchent de nombreux faux positifs. Pour maîtriser leur volume, il est recommandé d'investir dans l'adaptation des règles de supervision au SI supervisé.
- Ancrer la supervision dans un **fonctionnement collaboratif**. Si la supervision ne parvient pas à s'articuler pleinement avec son écosystème tel que décrit sur la figure 1, elle se prive des interactions (cf. section 2.3) pourtant indispensables à son bon fonctionnement. Il est recommandé de soigner les relations au sein de cet écosystème, et d'investir le temps nécessaire à leur développement.

4.6. Les enjeux juridiques

Il existe différents enjeux juridiques dans le cadre réglementaire français. D'une part, plusieurs textes recommandent ou imposent l'utilisation de la supervision de sécurité. D'autre part, les conditions de mise en œuvre de la supervision sont susceptibles d'être encadrées.

Le terme juridique consacré est "la journalisation"[14]. Elle est définie comme une mesure de sécurité, et elle poursuit plusieurs objectifs, dont l'adaptation du niveau de sécurité au niveau de risque, et l'imputabilité des actions menées sur un SI. Pour y parvenir, elle s'appuie sur la capacité de tracer diverses activités, la centralisation de ces traces, leur conservation, et leur analyse. De fait, la journalisation recouvre les différents aspects de la supervision de sécurité décrits dans le présent document.

Divers cadres réglementaires portent des recommandations ou des obligations de journalisation pour les SI, ou STAD (systèmes de traitement automatisés de données). Voici quelques textes à portée générale ou plus spécifique[15] :

- le RGPD[16] (règlement général sur la protection des données), qui traite des données à caractère personnelles ;
- la transposition nationale de la directive européenne NIS (*Network and Information System Security*, ou sécurité des réseaux et de l'information) ;
- les arrêtés sectoriels d'application de la LPM (loi de programmation militaire) 2015-2019, fixant les règles de sécurité des systèmes d'information d'importance vitale ;
- la loi de 2004 pour la confiance dans l'économie numérique[17] ;
- la PSSIE[18] (politique de sécurité des systèmes d'information de l'État).

Par ailleurs, les systèmes de supervision, lorsqu'ils traitent des données personnelles, sont eux-mêmes encadrés par le RGPD. L'objectif est de maintenir un équilibre entre l'apport en sécurité de la supervision et le risque qu'elle fait courir sur la protection de la vie privée.

4.7. Les enjeux cyber

Parmi tous les défis à relever à travers la supervision de sécurité, les enjeux cyber ont une place centrale. En premier lieu, la supervision de sécurité concourt à la défense des SI. En second lieu, elle s'appuie sur son propre SI à défendre. Enfin et surtout, le SI de supervision est interconnecté à un voire plusieurs SI supervisés qu'elle contribue à défendre, et peut ainsi constituer une porte d'entrée supplémentaire pour l'attaquant. La présente section détaille ces éléments afin d'étayer la logique de sécurisation d'une supervision de sécurité.

4.7.1. La sécurité du SI de supervision

Le SI de supervision doit être défendu au même titre que tout SI. En effet, il est sujet aux risques cyber classiques. On pense notamment aux vecteurs de risques tels que les utilisateurs (ex. : analystes, administrateurs), les partenaires, les interconnexions avec d'autres SI, des éléments techniques potentiellement vulnérables.

Il est donc nécessaire de prévoir la supervision du SI de supervision. Cela passe par la conception d'une stratégie de supervision dédiée au SI de supervision. Sur le plan technique, des moyens de mise sous supervision (capteurs, collecteurs) doivent être déployés sur le SI de supervision. Enfin, les données issues de ces moyens peuvent être traitées par les outils du SI de supervision.

[14]Le lecteur est invité à consulter la "recommandation relative aux mesures de journalisation" [8] de la CNIL.
[15]Voir l'annexe D "Aspects juridiques et réglementaires" du guide "Le guide de journalisation" [9] de l'ANSSI.
[16]Voir le "règlement général sur la protection des données" [10] de l'Union Européenne.
[17]Voir la "loi pour la confiance dans l'économie numérique" [11].
[18]Voir la "politique de sécurité des systèmes d'information de l'État" [12].

	Atteinte à la confidentialité de la supervision	Atteinte à l'intégrité de la supervision
Superivision dédiée	La supervision devient, pour l'attaquant, une source d'information sur le périmètre supervisé. L'attaquant obtient un avantage stratégique sur les défenseurs pour faire persister son attaque.	La supervision peut être utilisée par un attaquant pour couvrir ses activités sur le périmètre supervisé (ex. : supprimer des journaux, altérer la collecte). Elle peut également être utilisée pour obtenir des privilèges excessifs sur le périmètre supervisé (ex. : compromission d'un agent logiciel disposant de privilèges élevés).
Supervision externalisée et mutualisée	La supervision devient une cible de choix pour l'attaquant. Effectivement, ce dernier accepte de déployer plus d'efforts sachant qu'il obtiendra de l'information sur plusieurs cibles potentielles.	La supervision peut en plus être utilisée pour déjouer les mesures de cloisonnement qui séparent les périmètres supervisés. L'attaquant utilise la supervision de sécurité pour rebondir d'un SI supervisé à l'autre.

Table 1
Exemples de reports de risques

4.7.2. Le SI de supervision comme brique de sécurité

La supervision participe activement à la cyberdéfense du périmètre supervisé. À ce titre, elle représente une cible d'intérêt pour les attaquants souhaitant rester persistants dans le SI supervisé. Elle est donc soumise à des risques spécifiques en lien avec la sécurité des opérations. Par exemple, un attaquant qui aurait compromis le SI de supervision aurait un avantage face à l'équipe de réponse à incidents.

4.7.3. Lien entre le SI de supervision et le SI supervisé

Le SI de supervision est interconnecté au SI supervisé, qui porte les valeurs métier de l'organisation. Il est recommandé de maîtriser les risques propagés par l'existence de ce lien technique :

- les risques touchant la **confidentialité** ou l'**intégrité** du SI de supervision ont un **impact intrinsèque** sur le SI supervisé (cf. tableau 1 "Exemples de reports de risques") ;
- les risques touchant la **disponibilité** du SI de supervision **ne doivent pas impacter** le SI supervisé ;
- les risques du SI supervisé **ne doivent pas impacter** la supervision de sécurité (ex. : le chiffrement malveillant de tout un élément de stockage du SI supervisé ne doit pas se répercuter sur le SI de supervision). En somme, le SI de supervision doit être insensible aux risques métier du SI supervisé.

4.7.4. La supervision de sécurité mutualisée

La supervision de sécurité peut être mutualisée entre plusieurs SI supervisés. Ces SI peuvent appartenir à la même entité (cas de la mutualisation interne) ou à plusieurs entités (cas de la mutualisation chez un prestataire). Enfin, ces SI supervisés peuvent être opérés sur les infrastructures de l'entité, sur les infrastructures d'un fournisseur de service *cloud*, ou en hybride.

Chacun de ces cas présente des risques spécifiques qu'il convient d'analyser. En revanche, tous ces cas mettent en jeu deux besoins antinomiques. Sur le plan sécuritaire, il s'agit d'un besoin de cloisonnement, pour :

- maîtriser la propagation des risques, en particulier entre les différents périmètres supervisés (cf. tableau 1 "Exemples de reports de risques") ;
- assurer la confidentialité des règles sensibles dont l'usage est réservé à certains SI supervisés.

Sur le plan fonctionnel, il s'agit d'un besoin de mutualisation pour :

- améliorer la pertinence de la supervision, en centralisant dans un outil d'analyse, les données de plusieurs périmètres supervisés ;
- optimiser les ressources et les coûts d'exploitation et d'utilisation, en partageant des éléments techniques entre plusieurs périmètres.

C'est pourquoi la sécurisation d'une supervision mutualisée est difficile à concevoir. Elle passe nécessairement par des compromis en faveur de l'un ou l'autre de ces besoins, selon les besoins des SI supervisés.

4.7.5. Logique de sécurisation

La logique de sécurisation d'une supervision de sécurité est façonnée par les divers enjeux cyber.

- Dans **tous** les cas :
  - le SI de supervision doit être structuré en zones de sécurité dans une logique de défense en profondeur, permettant notamment de protéger son cœur de confiance[19] ;
  - une **analyse de risque formelle** permet d'évaluer les risques susceptibles de se propager depuis le SI de supervision vers le périmètre supervisé ;
  - une **stratégie de supervision spécifique** doit être conçue pour le SI de supervision, en particulier, pour couvrir les risques qui ne peuvent être réduits par des mesures de prévention.
- Les besoins de sécurité de la supervision **non mutualisée** sont **équivalents** à ceux du SI supervisé. Conformément à la doctrine d'administration sécurisée[20], le SI de supervision peut partager certains moyens techniques avec le SI d'administration du SI supervisé, dans le respect des besoins de sécurité de ce dernier.
- Les besoins de sécurité de la supervision **mutualisée** correspondent aux besoins de sécurité du SI supervisé qui a **les besoins les plus élevés**[21]. De plus, l'effet d'accumulation des données au sein d'un SI de supervision mutualisé peut nécessiter la hausse de ses besoins de sécurité. Enfin, l'équilibre entre cloisonnement et mutualisation au sein du SI de supervision dépend également des caractéristiques des liens techniques entre le SI de supervision et chaque SI supervisé, en particulier, le niveau de garantie d'unidirectionnalité[22] **sur l'ensemble des liens**.

4.8. Des enjeux aux risques

Si l'on change de perspective, les enjeux présentés dans le présent chapitre peuvent être utilisés comme un catalogue de risques. En revanche, la richesse de ce catalogue mérite quelques éléments de priorisation :

- les risques correspondant aux enjeux humains doivent toujours être pris en compte, quel que soit l'état de maturité de la supervision de sécurité. En effet, le capital humain représente toute la force vive d'une supervision de sécurité. Parmi ces risques, le risque de fatigue des alertes est le plus probable, avec un impact important pour l'équipe ;

[19] Le cœur de confiance (ou *trusted core*) est défini comme la partie d'un SI sur laquelle repose la sécurité de la totalité du SI. Voir l'article correspondant dans le CyberDico [13] de l'ANSSI.

[20] Voir le chapitre 9 "Sauvegarde, journalisation et supervision de la sécurité" du "guide administration sécurisée" [14] de l'ANSSI.

[21] Cela signifie que le SI de supervision est soumis aux contraintes les mieux-disantes. Cela signifie aussi qu'un SI ne peut être supervisé que par un SI de supervision répondant à des contraintes au moins équivalentes.

[22] Les garanties d'unidirectionnalité ne sont pas les mêmes selon que le lien traverse un pare-feu (filtrage réseau sur les niveau 2 à 4 du modèle OSI), une zone démilitarisée (DMZ) telle que définie dans le guide de "recommandations relatives à l'interconnexion d'un système d'information à Internet" [15] de l'ANSSI (une fonction de rupture protocolaire entourée de deux pare-feux), ou une diode réseau (dispositif unidirectionnel au niveau 1 du modèle OSI).

- les risques correspondant aux enjeux cyber sont importants à prendre en compte ;
- les risques correspondant aux enjeux métiers sont également importants ;
- pour chaque famille d'enjeux, il est intéressant de choisir et prioriser les risques pertinents dans le contexte d'un projet de supervision de sécurité spécifique.

Pour finir, ces risques doivent être attribués aux bons acteurs pour en garantir le suivi :

- les risques liés aux enjeux stratégiques ne disparaissent pas lorsque le projet avance. Le chef de projet doit les transférer au management de la supervision de sécurité. Dans une moindre mesure, il en va de même des risques correspondant aux enjeux de projet, et aux enjeux juridiques ;
- une méthode pour gérer les risques liés aux enjeux métier, technique et cyber consiste à en répartir le suivi au sein des différents chantiers à réaliser. En revanche, il faut distinguer ceux qui doivent être repris et suivis par le management de la supervision de sécurité, de ceux qui restent attachés à un chantier, et dont le suivi est mis en pause jusqu'à la prochaine itération.

5. Recommandations

Les recommandations qui sont proposées ici permettent d'optimiser l'effort de construction d'une supervision de sécurité. Sans prétendre à l'exhaustivité, elles aident à tracer les grandes lignes de la démarche. De fait, elles doivent être adaptées au contexte et aux spécificités de chaque projet.

5.1. Acquérir de la connaissance sur le SI à superviser

Cette connaissance doit être recueillie selon plusieurs axes : les risques, les technologies, l'architecture et la vie du SI (ex. : interventions, méthodes d'administration). C'est à l'intersection de ces savoirs que se conçoit une stratégie de détection efficace (cf. section 3.3 décrivant la stratégie de supervision).

5.2. Préparer le SI avant de le superviser

Avant toute chose, il est recommandé d'élever le niveau de sécurité du SI supervisé à un seuil de cybersécurité nominal. En effet, tenter de superviser un SI qui n'est conforme ni aux principes de défense en profondeur, ni aux mesures d'hygiène informatique[23] est une perte de temps et d'argent. Ces ressources seront mieux employées dans une phase préalable d'amélioration du SI. Cette étape rendra le projet de supervision plus fluide et plus viable.

5.3. Commencer à superviser avec les moyens en place

Il est possible d'atteindre un premier niveau de supervision du SI, même imparfait, sans investissement supplémentaire. Il est recommandé de miser sur la connaissance de l'existant et l'utilisation des outils de sécurité déjà déployés (ex. : un antivirus ou l'activation de la journalisation sur un autre dispositif de sécurité). Tout investissement supplémentaire présente le risque de diluer la capacité à faire entre la supervision et l'attention portée aux nouveaux moyens (intégration, déploiement, maintenance). Pour commencer, il est donc plus efficace de démarrer les processus de la supervision en limitant l'ajout de moyens techniques. Par ailleurs, la maintenance du SI de supervision aux équipes d'exploitation. Cela permet de préserver les ressources de la supervision pour les évolutions et l'amélioration continue.

5.4. Adopter une démarche ascendante et diversifier les données

En adoptant une démarche ascendante (*bottom-up*), il est recommandé de partir des sources de données disponibles et pertinentes, pour commencer à satisfaire certains objectifs de détection. C'est seulement dans un second temps qu'il est intéressant d'ajouter des sources, en visant un optimum entre :

[23] Voir le "Guide d'hygiène informatique : renforcer la sécurité de son système d'information en 42 mesures" [16] de l'ANSSI.

- la couverture du périmètre à superviser ;
- la représentativité des activités sur le périmètre supervisé (ex. : système, réseau, applicatif, industriel) ;
- la prise en compte des objectifs de supervision.

Cette démarche itérative s'inscrit dans l'amélioration continue de la supervision.

5.5. Porter un intérêt particulier aux postes de travail

Le point faible utilisé par de nombreuses attaques de masse (ex. : rançongiciels) est le poste de travail, sur lequel l'utilisateur peut naviguer sur le Web et lire ses courriels. Ces postes sont des éléments du SI fortement distribués et exposés. En premier lieu, il est recommandé de s'assurer que les principes d'hygiène informatique sont correctement appliqués. En second lieu, il est recommandé de s'intéresser aux éléments de sécurité déjà déployés (ex. : antivirus). Il est utile de comprendre les alertes levées par ces systèmes pour traiter efficacement les causes et résoudre les problèmes soulevés. Le cas échéant, une solution dédiée aux équipements terminaux (ex. : *endpoint detection and response*, ou EDR) peut être déployée pour bénéficier, entre autres, d'une visibilité plus riche sur l'activité du parc. Si le périmètre des postes de travail est un point de départ, d'autres périmètres doivent être traités avec attention (ex. : équipements de bordure, interconnexion entre réseaux, services exposés, annuaire centralisé).

5.6. Adopter une démarche humble face au volume de données

Dès lors que des outils dédiés à la supervision de sécurité sont mis en place se pose la problématique de la centralisation des données. Il est recommandé de limiter le volume des données. Voici quelques axes pour y parvenir :

- déterminer l'activité malveillante recherchée, et les scénarios de menace associés ;
- sélectionner des sources pertinentes pour détecter ces scénarios de menace ;
- choisir un niveau de journalisation adapté ;
- filtrer des événements récurrents inutiles ;
- agréger des événements apparentés ;
- adapter la période de rétention au besoin réel d'analyse à postériori.

Il est également recommandé de traiter en dehors du périmètre de la supervision de sécurité, les autres besoins qui reposent sur les traces d'un SI, mais qui ne concourent pas directement à la recherche d'activité malveillante (ex. : archivage de journaux, obligations réglementaires concernant la traçabilité sur le SI, maintenance préventive).

5.7. Avancer progressivement vers la maturité

Afin de rendre progressive la montée en maturité et de l'adapter aux situations initiale et finale de chaque entité, il est recommandé d'adopter une démarche "des petits pas" selon trois axes :

- Les processus peuvent être initialisés progressivement, en partant du processus de connaissance du périmètre supervisé (cf. section 3.4 décrivant les processus de la supervision). De plus, certains processus peuvent être initialisés par le biais de l'externalisation (ex. : veille en vulnérabilités et menaces).
- Les outils dédiés peuvent être implémentés graduellement, à partir des premiers capteurs, fonction technique par fonction technique (ex. : exploiter des alertes dans les consoles de chaque outil, puis centraliser les alertes, puis enrichir les données centralisées).

- Les périmètres peuvent être couverts par avancées successives, sans chercher à avancer trop vite. Pour chaque périmètre, il est recommandé de choisir judicieusement les familles d'équipements à couvrir de façon exhaustive.

Se reporter, par exemple, à la méthode de construction itérative de la supervision de sécurité[24].

5.8. Mettre en cohérence les ressources avec les ambitions

La création d'une supervision de sécurité s'apparente à une course de fond. Il faut donc gérer judicieusement ses ressources financières comme humaines. Le budget doit être conçu sur du moyen/long terme. Les ressources humaines doivent être enrichies au fil du développement du système. Les attentes opérationnelles doivent être réalistes, quitte à évoluer en fonction des succès constatés.

5.9. Gérer l'incertitude

L'incertitude est une composante de la supervision de sécurité. Il n'y a jamais de certitude d'avoir choisi les bonnes sources de données, ou d'avoir retenu des critères (règles, comportements) suffisamment pertinents. Il n'y a jamais de certitude non plus quant au résultat de la supervision, en particulier en absence de résultat : est-ce qu'il ne se passe rien, ou est-ce que je ne détecte pas ce qu'il se passe ? Il est recommandé de mettre en place des mesures aidant à maîtriser l'incertitude, au niveau technique, organisationnel, notamment en vérifiant la pertinence et l'efficacité de la détection par le biais d'exercices réguliers (ex. : plateforme de tests automatisés, tests de pénétration *redteam* sur le périmètre supervisé). Dans un premier temps, ces exercices peuvent impliquer les analystes dans un esprit coopératif. Par la suite, ils peuvent être menés en aveugle dans un esprit d'émulation.

5.10. Cultiver la confiance vis-à-vis des parties prenantes

Le capital confiance acquis par une supervision de sécurité est une ressource précieuse qui conditionne son efficacité. Cette confiance se gagne rarement sur des faits d'armes retentissants. Elle se bâtit progressivement, en particulier auprès des bénéficiaires directs comme les administrateurs du SI. Il est recommandé de répartir clairement les rôles et responsabilités, et d'adopter une démarche transparente ("dire ce qu'on fait et faire ce qu'on dit"). De plus, la supervision doit rester neutre pour éviter la critique des uns (mauvaises pratiques des équipes techniques) ou des autres (incidents de sécurité non détectés par l'équipe de supervision). Par ailleurs, il est primordial de partager régulièrement les axes de progression du dispositif de supervision de sécurité et les indicateurs produits avec les autorités du SI supervisé. Cette pratique permet de les éclairer sur ce que le dispositif produit et sur les informations qui aident les équipes de la DSI à mieux protéger leur SI.

6. Conclusion

Avant, il y avait la détection d'incidents de sécurité. La doctrine de l'agence en la matière se concentrait dans un référentiel d'exigence[25]. Ce dernier s'inscrit dans le contexte particulier de la défense des intérêts de la nation. Il permet de mettre en relation certains opérateurs dits "vitaux" avec des offreurs de service de confiance.[26]. La doctrine qui en découle s'est donc avérée impossible à généraliser.

Au moment de moderniser cette doctrine, la démarche retenue consiste à écrire ce qu'est une bonne supervision de sécurité, avant d'écrire des exigences cyber. En d'autres termes, décrire une cible fonctionnelle, avant de décrire la cible de sécurité. Le premier volet de cette démarche est un guide de niveau stratégique[27], qui évoque toutes les bonnes raisons de faire de la supervision de sécurité.

[24]Voir le guide "Supervision de sécurité, les clés de décision" [17] de l'ANSSI. En particulier, la figure 2 et sa description.
[25]voir le Référentiel des prestataires de détection d'incidents de sécurité [18] (PDIS) de l'ANSSI.
[26]L'ANSSI délivre des qualifications, qui attestent qu'un prestataire respecte les exigences d'un référentiel.
[27]Voir le guide "Supervision de sécurité, les clés de décision" [17] de l'ANSSI.

Le présent article constitue le second volet de cette démarche. Il liste les éléments attendus d'une supervision de sécurité. Il peut servir à piloter un projet, à construire une expression de besoin, ou encore à organiser des tests d'efficacité. Pour autant, de nombreux sujets mériteraient d'être développés : les interactions entre les processus métier, la méthode pour créer une stratégie de sécurité, les contraintes sur le lien entre le SI de supervision et le SI supervisé, la construction d'un SI de supervision, etc.

L'ANSSI va poursuivre cette démarche avec deux volets à venir. L'un évoquera la mise sous supervision et le lien entre SI de supervision et SI supervisé. L'autre proposera des pistes pour construire un SI de supervision. A l'issue de ces travaux, le référentiel PDIS évoluera vers une nouvelle version.

Declaration on Generative AI

During the preparation of this work, the author(s) used Perplexity and DeepL in order to: Paraphrase and reword, and Text Translation. After using these tool(s)/service(s), the author(s) reviewed and edited the content as needed and take(s) full responsibility for the publication's content.

References

[1] NIS2, Directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, Referentiel, Parlement européen, 2022. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/fra.

[2] ANSSI-PA-046, Cartographie du système d'information, Guide ANSSI-PA-046 v1.0, ANSSI, 2018. https://cyber.gouv.fr/publications/cartographie-du-systeme-dinformation.

[3] ANSSI-PA-048, La méthode EBIOS Risk Manager - Le Guide, Guide ANSSI-PA-048 v1.0, ANSSI, 2018. https://cyber.gouv.fr/ebios-rm.

[4] ANSSI-COLLEC-REMED-CLES, Cyberataques et remédiation - Les clés de décision, Guide, ANSSI, 2023. https://cyber.gouv.fr/piloter-la-remediation-dun-incident-cyber.

[5] ANSSI-PA-089, Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique, Guide ANSSI-PA-089 v1.0, ANSSI, 2021. https://cyber.gouv.fr/publications/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-strategique.

[6] CONFUSION-MATRIX, Confusion matrix, Cours, Mahatma Gandhi Central University, Motihari (Bihar), India, 2020. https://web.archive.org/web/20220319220257/https://mgcub.ac.in/pdf/material/20200429020322e5dac20f58.pdf.

[7] TRI-PROJ, Triangles, Tradeoffs and Success: a Critical Examination of some Traditional Project Management Paradigms, Article, Northumbria University, Newcastle-upon-Tyne, UK, 2022. https://web.archive.org/web/20231229141249/https://www.irbnet.de/daten/iconda/CIB16214.pdf.

[8] CNIL-JOURNALISATION, Recommandation relative aux mesures de journalisation, Recommandation, CNIL, 2021. https://www.cnil.fr/fr/la-cnil-publie-une-recommandation-relative-aux-mesures-de-journalisation.

[9] ANSSI-PA-012, Recommandations de sécurité pour l'architecture d'un système de journalisation, Guide DAT-PA-012 v2.0, ANSSI, 2022. https://cyber.gouv.fr/guide-journalisation.

[10] RGPD, Règlement Général sur la Protection des Données, Referentiel, Parlement européen, 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj/fra.

[11] LCEN, Loi pour la confiance dans l'économie numérique, Referentiel, Parlement européen, 2004. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000801164/.

[12] ANSSI-PG, Politique de sécurité des systèmes d'information de l'État (PSSIE), Référentiel Version 1.0, ANSSI, 2014. https://cyber.gouv.fr/pssie.

[13] CYBERDICO, Le CyberDico, Information, ANSSI, 2025. https://cyber.gouv.fr/le-cyberdico.

[14] ANSSI-PA, Recommandations relatives à l'administration sécurisée des systèmes d'information, Guide ANSSI-PA-022 v3.0, ANSSI, 2021. https://cyber.gouv.fr/guide-admin-si.

[15] ANSSI-PA, Recommandations relatives à l'interconnexion d'un système d'information à Internet, Guide ANSSI-PA-066 v3.0, ANSSI, 2020. https://cyber.gouv.fr/guide-interconnexion-si-internet.

[16] ANSSI-GP-042, Guide d'hygiène informatique : renforcer la sécurité de son système d'information en 42 mesures, Guide ANSSI-GP-042 v2.0, ANSSI, 2017. https://cyber.gouv.fr/hygiene-informatique.
[17] ANSSI-GP-112, Supervision de sécurité - Les clés de décision, Guide ANSSI-GP-112 v1.0, ANSSI, 2025. https://cyber.gouv.fr/supervision-securite.
[18] ANSSI-PG, Prestataires de détection des incidents de sécurité. Référentiel d'exigences, Référentiel Version 2.0, ANSSI, 2017. https://cyber.gouv.fr/pdis.