RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

ANSSI

COLLECTION
SUPERVISION DE SÉCURITÉ

SUPERVISION DE SÉCURITÉ
LES CLÉS DE DÉCISION

L'ANSSI publie une collection de guides sur la supervision de sécurité, dont l'organisation est décrite par la figure 1. 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).

Le présent document, à portée stratégique, définit les principaux piliers conceptuels de la supervision de sécurité.

La supervision de sécurité participe, avec le renseignement sur la menace et la réponse à incidents, au traitement des incidents de sécurité. Elle se définit 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.

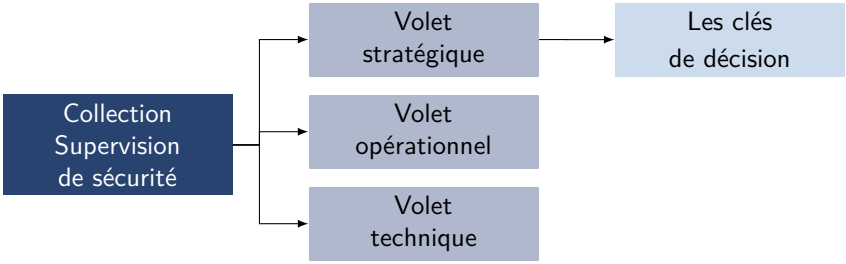

Figure 1 – *Collection de guides sur la supervision de sécurité*

QU'EST-CE QUE LA SUPERVISION DE SÉCURITÉ ?

Une cyberattaque est définie comme un « ensemble coordonné d'actions menées dans le cyberespace qui visent des informations ou les systèmes qui les traitent, en portant atteinte à leur disponibilité, à leur intégrité ou à leur confidentialité »[1]. Une cyberattaque peut être ponctuelle ou s'inscrire dans la durée.

En pratique, il est possible de décomposer une cyberattaque en un enchaînement d'étapes unitaires. C'est ce que font les attaquants, en s'organisant pour se répartir les tâches, et en se professionnalisant pour monter en compétences sur chaque étape. C'est également ainsi que sont construites les méthodes d'analyse de risques (p. ex. EBIOS *Risk Manager*, ISO 27005) ou les modèles d'analyse des attaques (p. ex. Cyber Kill Chain, MITRE ATT&CK).

De plus, une cyberattaque consiste à interagir avec le SI de la future victime. Cela signifie que la majorité des étapes unitaires décrites ci-dessus laissent des traces qui lui sont spécifiques.

En utilisant ces deux propriétés (découpage de l'attaque en étapes unitaires et traces spécifiques à chaque étape unitaire), il est possible de détecter les signes d'une attaque, si possible avant qu'elle ne soit terminée. Autrement dit, avant que l'attaquant n'atteigne ses objectifs.

La supervision permet de repérer, sur un système d'information (SI), les activités qui pourraient être des étapes unitaires malveillantes, et génère des alertes. Après avoir fiabilisé et caractérisé ces alertes, l'équipe de supervision transmet des incidents de sécurité avérés (et leur description enrichie) à une équipe de réponse à incidents.

1. Cf. la recommandation de la commission d'enrichissement de la langue française concernant le vocabulaire de la défense : cyberdéfense (liste de termes, expressions et définitions adoptés) [3] publiée au Journal officiel.

POURQUOI SUPERVISER LA SÉCURITÉ D'UN SYSTÈME D'INFORMATION ?

Aujourd'hui, sur un vol commercial, on n'imagine pas qu'un commandant de bord accepte de décoller si les passagers embarquent sans contrôle de leur identité et des bagages transportés. Ces vérifications sont obligatoires et normalisées à l'international, en cohérence avec la nature du trafic aérien et avec la menace connue.

Comparativement, de nombreuses organisations s'appuient sur des systèmes d'information (SI) dont l'activité est peu contrôlée. Pourtant, la perte de confiance dans un SI menace l'existence même de l'organisation qui en dépend.

Tout comme les contrôles à l'embarquement constituent un maillon essentiel de la maîtrise du risque qui pèse sur les passagers, la supervision de sécurité intervient dans la maîtrise du risque qui pèse sur les organisations, massivement dépendantes de leurs SI.

La supervision de sécurité aide les organisations à maîtriser le risque cyber, caractérisé par la hausse du nombre et du niveau des attaques. C'est pourquoi elle fait l'objet d'obligations réglementaires croissantes, aux niveaux national (ex. : loi pour la confiance dans l'économie numérique, loi de programmation militaire) et européen (ex. : directive NIS, règlement général sur la protection des données).

QUE PEUT-ON ATTENDRE DE LA SUPERVISION DE SÉCURITÉ ?

La supervision de sécurité modifie la gestion opérationnelle du risque cyber. Elle permet de quitter le mode purement réactif et d'évoluer vers un mode proactif. *In fine*, elle contribue à empêcher une compromission du SI, ou tout du moins à en limiter les conséquences.

Grâce à la supervision de sécurité, l'organisation peut réagir avant que l'attaque ait des effets perceptibles. La supervision s'appuie sur une connaissance fine de l'activité nominale du SI et des cybermenaces. Cela permet de réagir à une activité anormale au plus tôt pour limiter les effets de la compromission. En cas de crise majeure, cela permet de

disposer d'un meilleur niveau d'information, et de moyens d'investigation pertinents.

De plus, la proximité des équipes de gestion opérationnelle des SI et de supervision de sécurité ouvre la voie à une démarche d'amélioration mutuelle et continue. D'un côté, la gestion du SI supervisé doit être suffisamment rigoureuse pour que le système de supervision puisse prendre en compte ses changements. D'un autre côté, la supervision peut aider à corriger les dysfonctionnements ou les écarts du SI supervisé. Cela conduit, sur le temps long, à faire de meilleurs choix de sécurité, et *in fine*, à améliorer la qualité du SI supervisé.

QUELS SONT LES PRÉREQUIS DE LA SUPERVISION DE SÉCURITÉ ?

La supervision de sécurité vise à identifier des activités malveillantes de façon fiable au milieu des activités légitimes menées sur un SI. Pour y parvenir, il est nécessaire de :

- maîtriser techniquement son SI. Cela peut se traduire par la mise en place de pratiques d'hygiène informatique [2] ;
- connaître les risques auxquels le SI est exposé (ex. : nature de l'activité de l'organisation, forces et faiblesses des briques techniques, état de la menace) ;
- mettre en place des moyens techniques dédiés à la supervision de sécurité. Ces moyens doivent être adaptés aux caractéristiques du SI supervisé (ex. : taille, technologies, agencement) ;
- mobiliser des moyens humains et une organisation adaptée à la supervision de sécurité, même lorsque des choix d'externalisation sont faits.

2. Cf. « Guide d'hygiène informatique : renforcer la sécurité de son système d'information en 42 mesures » [1] de l'ANSSI.

QUI MOBILISER POUR LA SUPERVISION DE SÉCURITÉ ?

Les intervenants qui concourent au bon fonctionnement de la supervision de sécurité s'organisent en deux cercles, autour de l'équipe d'analystes.

Tous ces intervenants peuvent être externalisés. C'est d'ailleurs le plus réaliste pour des petites entités. En revanche, des canaux d'échange avec les prestataires doivent être mis en place pour aider la supervision de sécurité à remplir son rôle.

Figure 2 – *Acteurs autour de la supervision de sécurité*

Au centre, l'**équipe d'analystes** est composée de profils spécialisés qui vont traiter des alertes pour qualifier les incidents de sécurité. Des compétences complémentaires (managériales, techniques) peuvent également être requises, selon la taille de l'équipe. Et puisqu'elle concentre beaucoup de savoirs sur l'organisation et son SI, son maintien en interne présente une importante plus-value.

Le premier cercle concerne le dispositif de gestion des incidents de sécurité. Il est constitué des équipes de renseignement sur la menace, et de réponse à incidents. Le **renseignement sur la menace** fournit une matière première plus ou moins raffinée permettant la détection d'activités malveillantes. La **réponse à incidents** prend en charge les incidents de sécurité avérés pour les traiter selon les intérêts de l'organisation (ex. : investigation, éviction de l'attaquant, rétablissement de la confiance dans le SI et de ses fonctions métier).

Le second cercle concerne l'ancrage de la supervision de sécurité dans le contexte interne à l'organisation. D'un côté, l'équipe de **gouvernance** fournit les soutiens décisionnel et financier. Elle se doit également de préciser des objectifs macroscopiques. Par exemple, au cours d'une analyse des risques[3] qui pèsent sur l'organisation, elle exprime les enjeux métier saillants auxquels la supervision de sécurité doit répondre.

D'un autre côté, l'équipe de **gestion opérationnelle des SI** est mise à contribution pour sa connaissance du périmètre supervisé : elle détient la connaissance du SI, de ses éléments techniques et de ses limites fonctionnelles. C'est également l'interlocutrice privilégiée pour lever le doute sur des activités potentiellement malveillantes. Face à certains incidents avérés, elle va avoir la meilleure capacité de réaction. Enfin, dans l'idéal, elle prend en charge la construction et la maintenance du SI dédié à la supervision.

QUAND DÉMARRER UN PROJET DE SUPERVISION DE SÉCURITÉ ?

Le meilleur moment pour investir dans la supervision de sécurité, c'est avant la prochaine attaque : au plus vite. Cela étant dit, pour bâtir une supervision efficace et pérenne, le SI supervisé doit satisfaire des prérequis en matière de maturité cyber.

En effet, tenter de superviser un SI qui n'est pas conforme au niveau standard du guide d'hygiène informatique de l'ANSSI met en péril l'atteinte des objectifs de supervision. Il est donc souvent nécessaire de consentir un effort préalable qui vise à assainir les pratiques pour mieux distinguer les activités légitimes des d'activités malveillantes (ex. : normalisation de la création des comptes à privilège).

3. Cf. « La méthode EBIOS Risk Manager - Le Guide » [2] de l'ANSSI.

COMMENT CONSTRUIRE LA SUPERVISION DE SÉCURITÉ ?

La supervision de sécurité revêt deux composantes complémentaires : une composante technique (des moyens spécifiques) et une composante organisationnelle (des partenaires, des pratiques à adapter, des canaux d'échange). Il est essentiel de construire ces deux composantes conjointement.

L'effort de construction d'une supervision de sécurité dépend essentiellement de deux choses : l'existant et les contraintes projet (le budget, la cible fonctionnelle et le délai de réalisation). Il n'existe donc pas deux projets de supervision identiques. De plus, l'hypothèse d'externaliser tout ou partie des fonctions de la supervision de sécurité multiplie les possibilités.

En revanche, l'organisation de cet effort peut avantageusement s'appuyer sur un MVP[4], qui permet de commencer à détecter au plus vite, même avec des outils perfectibles et même sur des périmètres imparfaitement couverts. Cela permet la montée en compétence progressive des analystes, et facilite l'alignement des outils avec la réalité et les besoins du terrain. La figure 3 illustre la construction du MVP et son amélioration progressive.

4. Un MVP (*minimum viable product* ou produit minimum viable) se définit comme « la version d'un nouveau produit qui permet à une équipe de recueillir le maximum d'apprentissages validés sur les clients avec le moins d'effort possible ».

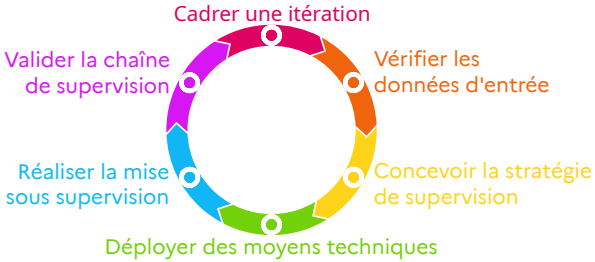

Figure 3 – *Construction itérative de la supervision de sécurité*

Cadrer une itération : choisir un objectif atteignable (ex. : périmètre limité, nombre réduit d'événements redoutés).

Vérifier les données d'entrée : recueillir les documents génériques (ex. : PSSI, analyse de risque) et spécifiques au périmètre (ex. : dossier d'homologation, rapport d'audit).

Concevoir la stratégie de supervision : associer aux scénarios opérationnels choisis des familles de données, des points de collecte, et des règles de détection pertinents.

Déployer des moyens techniques : mettre en place les points de collecte, gérer la remontée des données sélectionnées.

Réaliser la mise sous supervision : centraliser, enrichir et stocker les données sélectionnées, fiabiliser les règles de détection sur ces données.

Valider la chaîne de supervision : valider le bon fonctionnement des processus de supervision de sécurité pour ce périmètre.

Cette approche repose sur une construction itérative du SI de supervision : d'une part, en ne couvrant que quelques fonctions essentielles (ex. : acquisition et collecte de certaines activités, outils d'analyse automatisée et d'analyse manuelle), d'autre part, en visant un périmètre réduit pour la mise sous supervision. En d'autres termes, cela revient à couvrir un périmètre restreint, et le couvrir avec une qualité potentiellement réduite. Cela limite les volumes de données à traiter. Une fois cette capacité minimale construite, la progression en maturité peut, en fonction du contexte, suivre divers scénarios, dont trois exemples sont illustrés par la figure 4.

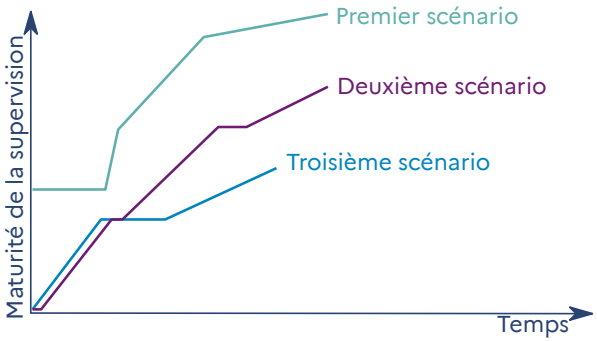

Figure 4 – *Scénarios de construction de la supervision de sécurité*

Premier scénario pour une organisation ayant déjà quelques moyens permettant d'observer l'activité de son SI, et un large panel de compétences. Elle est soumise à une contrainte réglementaire imposant un niveau d'exigence élevé : **cette organisation a intérêt à identifier sa cible à l'aide d'une analyse de risque, et planifier soigneusement sa trajectoire en amont.**

Deuxième scénario pour une organisation qui n'a pas de moyens de supervision, mais des compétences en informatique et en gestion de projets. Elle n'est pas soumise à une contrainte réglementaire, mais elle souhaite être conforme à des pratiques sectorielles pour des raisons de compétitivité. Elle peut structurer son projet en chantiers successifs ayant des objectifs progressifs : **en s'appuyant sur des analyses d'écarts à chaque étape, elle pourrait avancer progressivement et maîtriser sa trajectoire.**

Troisième scénario pour une organisation qui n'a pas de moyens de supervision, et peu de ressources humaines. Elle n'est soumise à aucune contrainte réglementaire, et souhaite défendre ses actifs numériques : **elle peut s'appuyer sur une démarche de conformité pour couvrir les fonctions et les périmètres indispensables. Dans un second temps, elle peut capitaliser sur l'expérience acquise pour mener une analyse de risque et réaligner sa supervision.**

QUELLES SONT LES CONTRAINTES BUDGÉTAIRES DE LA SUPERVISION DE SÉCURITÉ ?

La supervision de sécurité est une capacité. Elle présente donc un coût de construction et un coût d'entretien. Les budgets de construction et d'entretien doivent être cohérents avec les objectifs poursuivis et s'inscrire dans la gestion existante des budgets informatiques, et cyber le cas échéant.

Le préalable à la supervision de sécurité est de maîtriser les pratiques sur le SI. Cette maîtrise nécessite des efforts préliminaires, matérialisés par exemple sous forme d'un plan d'action pour l'alignement sur les pratiques d'hygiène informatique. Ces efforts préexistants se poursuivent pendant, et probablement au-delà, de la construction de la supervision.

La supervision de sécurité doit être considérée comme un investissement informatique et cyber. Dans le cadre d'une construction d'une capacité interne, cet investissement doit courir sur plusieurs années. Dans le cadre d'une externalisation, la capacité est construite par le prestataire, et l'investissement se concentre sur la mise en supervision des périmètres sélectionnés.

Enfin, l'acquisition ponctuelle d'un produit ne permet pas de construire une supervision de sécurité efficace. L'investissement doit couvrir tant la construction que l'amélioration continue des outils et des méthodes.

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] *La méthode EBIOS Risk Manager - Le Guide*.
Guide ANSSI-PA-048 v1.5, ANSSI, mars 2024.
https://cyber.gouv.fr/publications/la-methode-ebios-risk-manager-le-guide.

[3] *Recommandation de la commission d'enrichissement de la langue française concernant le vocabulaire de la défense : cyberdéfense (liste de termes, expressions et définitions adoptés)*.
Référentiel, Journal Officiel de la République Française, septembre 2017.
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000035583357/.

COLLECTION
SUPERVISION DE SÉCURITÉ

La supervision de sécurité se définit 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.

La supervision de sécurité participe, avec le renseignement sur la menace et la réponse à incidents, au traitement des incidents de sécurité.

Fruit d'une riche expérience en tant qu'opérateur du service de supervision de sécurité de l'État, ainsi que dans l'accompagnement de prestataires et de bénéficiaires de services de supervision, l'ANSSI publie une collection de guides sur la supervision de sécurité, décrivant les principes de son pilotage et de sa bonne mise en œuvre : le volet stratégique, le volet opérationnel et le volet technique.

Ce volet stratégique apportera les clés de décision nécessaires pour fixer des objectifs et passer à l'action.

Version 1.0 – 25 juillet 2025
Ref : ANSSI-GP-112

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