LES DOSSIERS TECHNIQUES

Comment réussir le déploiement d'un SOC

Mars 2017

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11 rue de Mogador - 75009 Paris
Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88
clusif@clusif.fr – www.clusif.fr

Table des matières

Table des illustrations

Remerciements

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Les responsables du groupe de travail :

Martine	**GUIGNARD**	*Imprimerie Nationale*
Jean-Marc	**BOURSAT**	*Devoteam*

Les contributeurs :

Grégory	**ADROT**	*Armand Thiery*
Laurent	**BERRIER**	*Atexio*
Laurent	**BOURHIS**	*Veolia Environnement*
Eric	**CHARLEMAGNE**	*Airbus Defence & Space*
Thierry	**CHIOFALO**	*Intrinsec*
Henri	**CODRON**	*Schindler*
Javier	**GONZALEZ**	*Airbus Defence & Space*
Jean-Marc	**GREMY**	*Cabestan Consultants*
Florence	**HANCZAKOWSKI**	*Clusif*
Jacques	**HULLU**	*AP-HP*
Andrei	**IAKOVLEV**	*Hewlett Packard Enterprise*
Raphael	**ILLOUZ**	*Nes Conseil*
Marek	**KUREK**	*Euro Information*
Céline	**LANDRY**	*PCA Peugeot Citroën Automobile*
Vincent	**LE TOUX**	*Engie*
Benoit	**MARION**	*Wavestone*
Garance	**MATHIAS**	*Avocat*
Jean	**OLIVE**	*CGI France SAS*
Lazaro	**PEJSACHOWICZ**	*CNAMTS*
Serge	**PRISO**	*Econocom*
Tristan	**SAVALLE**	*Advens*
Rolland	**TRANG**	*Indépendant*

Le **CLUSIF** remercie également les adhérents ayant participé à la relecture.

I. Introduction

I.1. Description du sujet

Le CLUSIF a lancé un groupe de travail dont le thème est « Comment réussir le déploiement d'un SOC » (Security Operations Center). Le document présent est le résultat du travail réalisé par les participants de ce groupe de travail.

L'intitulé du Groupe de Travail et du document en résultant est elliptique puisqu'il sous-entend un certain nombre de questions auxquelles ce groupe de travail a dû répondre parmi lesquelles :

- Qu'est-ce qu'un SOC ? Est-ce un outil informatique (matériel, progiciel ou composite) ? Est-ce une organisation humaine ? Ou bien un ensemble des deux ? Est-ce un projet ? Ou bien un service ? Ou bien les deux ?
- En termes de fonctionnalités, le SOC est-il une affaire de spécialistes et d'experts ou bien concerne-t-il toute l'entreprise ? Son intérêt est-il juste de détecter l'attaque de type APT déclenchée par des pirates de haut niveau qui veulent porter atteinte au fonctionnement de l'entreprise ? Ou bien de suivre les nombreux événements de tous les jours dont des attaques plus aléatoires et de permettre ainsi à l'entreprise d'améliorer en permanence ses outils de prévention ?
- Pourquoi une entreprise souhaite-t-elle déployer un SOC ? Et qui est le porteur d'un tel projet : RSSI, ou autre ?
- Comment le SOC s'intègre-t-il dans une entreprise ? Reprend-il à son compte des services déjà en place dans l'entreprise, par exemple le NOC (Network Operations Center) ? Dans quelle mesure la mise en place des équipes du SOC va-t-elle bousculer l'organisation de l'entreprise ?
- Quel est le modèle économique d'un SOC ? Sur quel périmètre va-t-on le déployer et à quel coût ? Pour quel ROI ?
- Une fois que l'on a répondu à toutes ces questions, comment s'y prend-on pour déployer le SOC ? L'entreprise va-t-elle implémenter elle-même son SOC ou bien en externaliser tout ou partie ? Quels sont les nouveaux profils ou nouvelles compétences à intégrer pour déployer un tel projet ? Quelles sont les différentes phases d'un projet SOC ?
- Et par la suite, quels indicateurs servent à mesurer l'efficience du SOC ? Comment communiquer les résultats des mesures d'efficacité à l'ensemble de l'entreprise ?

I.2. A qui s'adresse ce document ?

Ce document s'adresse aux Directeurs des Systèmes d'Information, aux Responsables de la Sécurité des Systèmes d'Information mais aussi aux Directeurs Opérationnels et Métiers qui s'intéressent à la cyber sécurité et qui souhaiteraient savoir pourquoi et comment la mise en place d'un centre opérationnel de sécurité peut les aider dans cette démarche.

.

I.3. Définitions

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information www.ssi.gouv.fr
APT	Advanced Persistent Threat Menace persistante avancée Il s'agit d'attaques perfectionnées menées contre des entreprises ou des ressources ciblées, avec des moyens conséquents.
CAPEX	Terme Financier pour Capital Expenditure soit dépenses d'investissement en français
CERT	Computer Emergency Response Team - Équipe d'intervention d'urgence en informatique. Cette organisation a également un rôle de veille et il doit encourager la prise de conscience en matière de sécurité. Une organisation CERT fournit une assistance technique 24 heures sur 24 sur les incidents[1] en sécurité d'ordinateurs et de réseaux. Le CERT est une marque appartenant au Software Engineering Institute de l'université Carnegie Mellon University à Pittsburgh, PA. Cet acronyme peut être remplacé par CSIRT pour lever les droits d'usage de cette marque.
CMDB	Configuration Management Database
CNIL	Commission Nationale de l'Informatique et des Libertés Autorité française de contrôle en matière de protection des données personnelles.
CREST	Centre of Research and Evidence on Security Threats http://www.crest-approved.org/
CSIRT	Un CSIRT est un centre d'alerte et de réaction aux attaques informatiques. Cette appellation est privilégiée en Europe, CERT étant une marque déposée aux États-Unis par l'Université Carnegie-Mellon.
ETP	Equivalent Temps Plein est une unité de mesure : d'une charge de travail ; ou plus souvent, d'une capacité de travail ou de production.
ETSI	European Telecommunications Standards Institute ou Institut Européen des Normes de Télécommunications
KPI	Key Performance Indicator : Indicateur clé de performance.

[1] Des exemples de définition d'incident sont donnés dans le document PDIS de l'ANSSI ou dans l'ISO 27035.

MSSP	Managed Security Services Provider – Prestataire de services de sécurité gérés
NOC	Network Operations Center
OIV	Opérateur d'Importance Vitale. Un opérateur d'importance vitale (OIV) est, en France, une organisation identifiée par l'État comme ayant des activités indispensables ou dangereuses pour la population[2].
OPEX	Terme financier pour Operationnal Expanditure soit dépenses d'exploitation en français
PCA	Plan de Continuité des Activités
PDIS	Prestataire de Détection d'Incident de Sécurité
PRIS	Prestataire de Réponse aux Incidents de Sécurité
RED TEAM	Groupe indépendant qui met à l'épreuve une organisation (le SOC) afin de mesurer son efficacité
RGS	Référentiel Général de sécurité Ce référentiel fixe, selon le niveau de sécurité requis, les règles que doivent respecter certaines fonctions contribuant à la sécurité des informations, parmi lesquelles la signature électronique, l'authentification, la confidentialité ou encore l'horodatage.
ROI	Return On Investment – Retour sur investissement
SI	Système d'Information
SIEM	Security Information and Event Management est un outil facilitant la collecte et le traitement d'informations dans le but de détecter des alertes de sécurité et d'organiser leur traitement. Le SIEM est généralement l'outil principal d'une organisation SOC, d'où la confusion des deux acronymes pour des non spécialistes.
SIRP	Security Incident Response Platform : outil de gestion des tickets d'incident

[2] Pour la définition complète, se référer à l'article R 1332-1 du code de la Défense.

SOC	Security Operations Center
VABF	Vérification d'aptitude au bon fonctionnement (équivalent à recette)
VSR	Vérification de service régulier

I.4. Objectifs du document.

Ce document a pour but de partager l'expérience des membres du CLUSIF qui ont mis en place ce type de système et de faire part des difficultés rencontrées mais aussi des succès obtenus.

Les travaux du Groupe de Travail nous ont amenés à constater que la littérature concernant les SOC était assez peu fournie et qu'il n'existe pas de standard pour construire un tel système.

Nous nous sommes appuyés sur le document du MITRE[3] qui traite du sujet et qui décrit en 10 points comment déployer un SOC. Par ailleurs, la définition des PDIS (Prestataires de Détection d'Incident de Sécurité) et PRIS (Prestataires de Réponse aux Incidents de Sécurité) par l'ANSSI a apporté un début de standard mais celui-ci concerne principalement les Opérateurs d'Importance Vitale (OIV).

L'offre du marché en matière de SOC s'étoffe et des grands groupes informatiques sont en train de se positionner dans le domaine tant sur la partie conseil que sur la partie réalisation et exploitation.

Ce document peut fournir une aide afin de se retrouver dans les offres de sous-traitance de SOC ou pour construire un SOC internalisé, étant entendu qu'il ne donne pas de consigne dogmatique d'internaliser ou d'externaliser ce service.

[3] Massachusetts Institute of Technology Research & Engineering.

II. Objectifs d'un SOC

Le SOC s'adresse à des organisations qui désirent maîtriser leurs risques et augmenter le niveau de sécurité de leur système d'information tout en contrôlant le coût correspondant.

Pour ce faire, l'objectif de l'organisation va être de répartir son effort sur les trois temps de la sécurité : la prévention, la détection et la réaction. Elle intégrera également la problématique de conformité qui, en fonction des secteurs, peut fournir une incitation forte voire une obligation.

Pour répondre à cet objectif, l'organisation est amenée à mettre en place des dispositifs opérationnels et des dispositifs de pilotage.

II.1. Le SOC répond aux objectifs de l'entreprise

Le SOC fait partie des dispositifs opérationnels mis en place pour répondre au besoin de détection et a donc pour finalité l'augmentation du niveau de sécurité de la structure.

L'objectif du SOC va alors être d'apporter une réponse, ou une contribution de réponse, industrialisée et efficace sur chacun des trois temps évoqués et, le cas échéant, sur le besoin de conformité.

Cet objectif se décline sur plusieurs plans tels que l'apport fonctionnel ou l'interaction avec les autres dispositifs de l'organisation. Ces différents plans sont détaillés dans les paragraphes suivants.

II.2. Les fonctions rendues par le SOC

Comme évoqué ci-dessus, le SOC permettra d'améliorer la gestion de la sécurité sur les trois temps de la sécurité :

- Sur la détection des incidents, en permettant ou améliorant la détection des incidents de sécurité. Pour ce faire, le SOC met en place un mécanisme permettant de savoir ce qui se passe sur le système d'information et de détecter des conditions d'incident. Ce mécanisme s'appuie sur des outils de collecte complétés d'outils de corrélation dont les résultats seront traités par des analystes sécurité et dont les paramètres sont enrichis par des experts élaborant de nouveaux scénarios de détection pertinents ;
- Sur la réaction aux incidents, en permettant d'agir plus vite[4] et plus efficacement en fournissant des informations pertinentes aux équipes d'investigations en leur donnant accès aux outils du SOC ;
- Sur la prévention des incidents, en prenant en charge, par exemple, tout ou partie de la gestion des menaces et des vulnérabilités.

[4] Cf. le document « Cellules de crises et SI » du CLUSIF

II.3. Le SOC n’est pas constitué que de technologie

Pour répondre aux objectifs qui lui sont assignés, le SOC s’appuie sur des outils mais, comme tout dispositif de sécurité, le SOC ne se résume pas à une liste de produits achetés sur étagère et agglomérés les uns aux autres, dont on s’attendrait à voir sortir une information pertinente sans produire plus d’effort.

Le SOC est une organisation ayant des fonctions opérationnelles s’appuyant sur des processus documentés (donc connus et répétables), des ressources humaines et des ressources techniques.

II.4. Le SOC est un dispositif opérationnel

Le SOC a un rôle majeur de surveillance du SI et l'équipe qui le compose ne fait pas d’analyse de risque, n'organise pas la gestion de crise et ne conçoit pas de plan de continuité d'activité…cependant le SOC contribue de façon plus ou moins forte à chacun de ces sujets et peut, par exemple, jouer un rôle actif en cas de crise cyber, être intégré au plan de continuité ou encore être contributeur dans son rôle d'expert sécurité à l’analyse de risque.

II.5. Le SOC n’a pas pour objectif de remplacer le CSIRT (ou CERT)

Le SOC ne remplace pas nécessairement le CSIRT, mais est en interaction forte avec celui-ci. Les compétences sont différentes et l'ANSSI a d'ailleurs défini deux qualifications distinctes (Cf. II.8). Le SOC doit alerter tandis que le CSIRT doit enquêter et traiter l'origine du problème de sécurité. Le SOC ne remplace pas la cellule de gestion de crise. Par contre, il fournit un support opérationnel en se mettant au service de ces activités. Ceci permettant d’améliorer la gestion de l’incident pour, in fine, réduire les pertes opérationnelles directes et minimiser la probabilité de nouvelles occurrences.

II.6. Le SOC doit s’interfacer avec les autres processus de la gestion de la sécurité

Le SOC ne doit surtout pas fonctionner seul mais doit s’intégrer aux processus existants en communiquant de façon fluide avec ceux-ci.

Le SOC n’est donc pas un dispositif qu’on « pose » sur une organisation, toute organisation ayant déjà des éléments en place, processus ou outils. Le SOC est un dispositif qui va venir enrichir le système global afin de contribuer à la finalité qui est de maintenir un niveau de sécurité propre à satisfaire les exigences de sécurité des parties intéressées de l’organisation au meilleur coût. Pour cette raison, le SOC devra intégrer l’ensemble des parties concernées au-delà du seul RSSI.

Une des étapes importantes de la conception d'un SOC est donc de définir quels sont les processus ou sous-processus opérationnels qui seront traités dans le SOC, et quels sont ceux qui seront traités à l'extérieur d'un SOC.

Une autre étape est de (re)définir les responsabilités dans le processus global de la surveillance du SI, en faisant attention à ne pas mélanger la surveillance de bon fonctionnement du SI (au sens supervision) et la surveillance sécurité du SI (au sens détection d'anomalies marquant un problème de sécurité).

II.7. Le SOC doit être sécurisé

En tant que brique majeure de la sécurité opérationnelle, le SOC en lui-même doit être correctement maîtrisé. C'est bien sûr le cas en matière de disponibilité, mais également en termes de confidentialité et d'intégrité au regard des données sensibles traitées. La traçabilité des actions du SOC doit aussi être assurée. Par ailleurs, dans certains cas, le besoin de sécurité du SOC peut être formalisé à travers des exigences règlementaires. Ces mesures s'appliquent aussi bien à la sécurité physique que logique.

II.8. Quelques textes de référence

Aujourd'hui, plusieurs exigences ou qualifications font directement ou indirectement référence au SOC. C'est notamment le cas des recommandations de la CNIL et des référentiels d'exigence de l'ANSSI au travers des textes suivants :

- **Recommandations CNIL**

« *Le responsable d'un système informatique doit mettre en place un dispositif de traçabilité adapté aux risques associés à son système. Celui-ci doit enregistrer les évènements pertinents, garantir que ces enregistrements ne peuvent être altérés, et dans tous les cas conserver ces éléments pendant une durée non excessive.*

Les journaux doivent conserver les évènements sur une période glissante ne pouvant excéder six mois (sauf obligation légale, ou demande de la CNIL, de conserver ces informations pour une durée plus longue).

Prévoir au minimum la journalisation des accès des utilisateurs incluant leur identifiant, la date et l'heure de leur connexion, ainsi que la date et l'heure de leur déconnexion. Le format de l'horodatage doit de préférence prendre comme référence le temps UTC.

Dans certains cas, il peut être nécessaire de conserver également le détail des actions effectuées par l'utilisateur, telles que les données consultées par exemple.

Les précautions à prendre sont les suivantes :

- *Informer les utilisateurs de la mise en place d'un tel système.*

- *Protéger les équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés.*
- *Établir des procédures détaillant la surveillance de l'utilisation du traitement et procéder périodiquement à l'examen des informations journalisées.*
- *Le responsable de traitement doit être informé dans les meilleurs délais des failles éventuelles de sécurité.*
- *En cas d'accès frauduleux à des données personnelles, le responsable de traitement devrait le notifier aux personnes concernées. »*

- **Référentiels d'exigence ANSSI**

Le document PDIS de l'ANSSI *« constitue le référentiel d'exigences applicables à un prestataire de détection des incidents de sécurité (PDIS). Il a vocation à permettre la qualification de cette famille de prestataires. Il couvre les différents modes de service : internalisé, externalisé, dédié ou mutualisé. »*

Le document PRIS de l'ANSSI *« constitue le référentiel d'exigences applicables aux prestataires de réponse aux incidents de sécurité (PRIS). Il a vocation à permettre la qualification de ces prestataires. Il permet aux commanditaires de disposer de garanties sur les compétences du prestataire et de ses analystes, sur la qualité des activités de réponse aux incidents de sécurité réalisées, sur la capacité du prestataire à adopter une approche globale de l'incident de sécurité et une démarche d'analyse adaptée. Il peut également être utilisé, à titre de bonnes pratiques, en dehors de tout contexte réglementaire. Il n'exclut ni l'application des règles générales imposées aux prestataires en leur qualité de professionnel et notamment leur devoir de conseil vis-à-vis de leurs clients, ni l'application de la législation nationale. ».*

II.9. En résumé

Le SOC est une opportunité d'optimiser la gestion opérationnelle de la sécurité en la structurant autour de processus communicants, d'outils et de ressources humaines adaptés.

Il peut prendre différentes formes du moment qu'il répond à ce besoin de sécurité opérationnelle de façon adaptée dans un contexte donné. Il peut ainsi fournir une vue technique ou bien des vues métier, être ou pas associé à un CSIRT, être interne ou externalisé et être centralisé ou réparti sur différentes entités. La forme la plus appropriée est dictée par l'environnement, différent dans chaque organisation.

La mise en œuvre d'un SOC est ainsi une opération particulièrement structurante pour une organisation. En effet, plus qu'un choix de solutions techniques et de ressources humaines, il s'agit avant toutes choses de construire une organisation qui soit capable de prendre en charge des pans importants de la gestion opérationnelle de la sécurité.

III. Catalogue de services et fonctions d'un SOC

Le but de ce chapitre est de décrire le catalogue de services et les principales fonctions d'un SOC. Ce chapitre se concentre sur les services rendus tandis que le chapitre IV s'intéressera à la structure de fonctionnement du SOC, et donc aux fonctions support nécessaires tels que le pilotage ou le reporting.
Ce catalogue ne vise pas à être exhaustif, mais à présenter l'étendue des services qui peuvent être inclus dans un SOC. Un SOC ne se limite pas à un outil (le SIEM) ni à un service (l'analyse de logs), mais peut englober un nombre important de services relatifs à la sécurité opérationnelle. Pour autant, tous les services présentés ci-dessous ne doivent pas nécessairement être implémentés ni intégrés à un SOC donné.
La construction du SOC, et notamment la phase de construction initiale (ou BUILD), est abordée dans le chapitre V : c'est alors que le choix des services à implémenter est fait (notamment en fonction de la stratégie du SOC et des risques à couvrir).
La stratégie du SOC devra également permettre de définir la feuille de route d'ajout incrémental de services, au fur et à mesure de la croissance et de la montée en maturité du SOC, et de l'évolution du cadre des menaces.

Ces services peuvent être fournis intégralement par un SOC interne à l'organisation, par un ou des prestataires (MSSP), ou bien par une solution hybride des deux (interne + externe).

On peut regrouper les services d'un SOC en 4 principales catégories aux objectifs distincts :

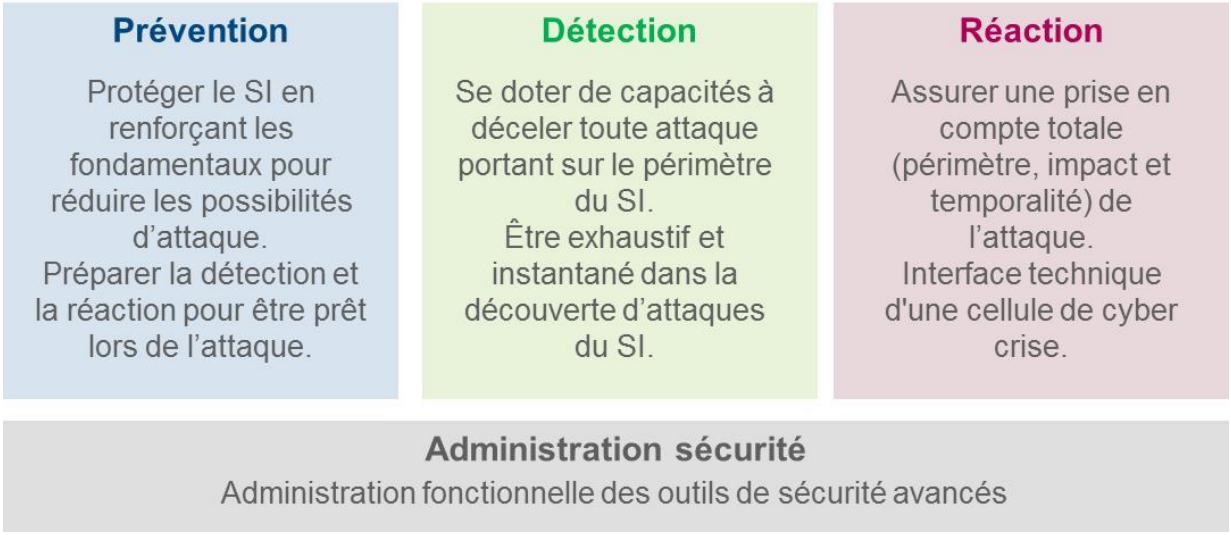


Figure 1. Catalogue des services

Aux fonctions de prévention, détection et réaction qui correspondent aux différents temps du traitement de l'incident, s'ajoute la fonction d'administration des outils propre au SOC (habilitations, administration technique et fonctionnelle, etc.) qui peut faire partie du SOC de par ses adhérences sur le périmètre technique d'une part (ces outils sont proches du SOC voire

concourent à la détection), et sur le périmètre fonctionnel d'autre part (la gestion des habilitations et des dérogations participent à la prévention et à la détection d'incidents).

Au sein de chacune de ces fonctions on peut identifier les services suivants qui pourront être liés directement ou indirectement au SOC :

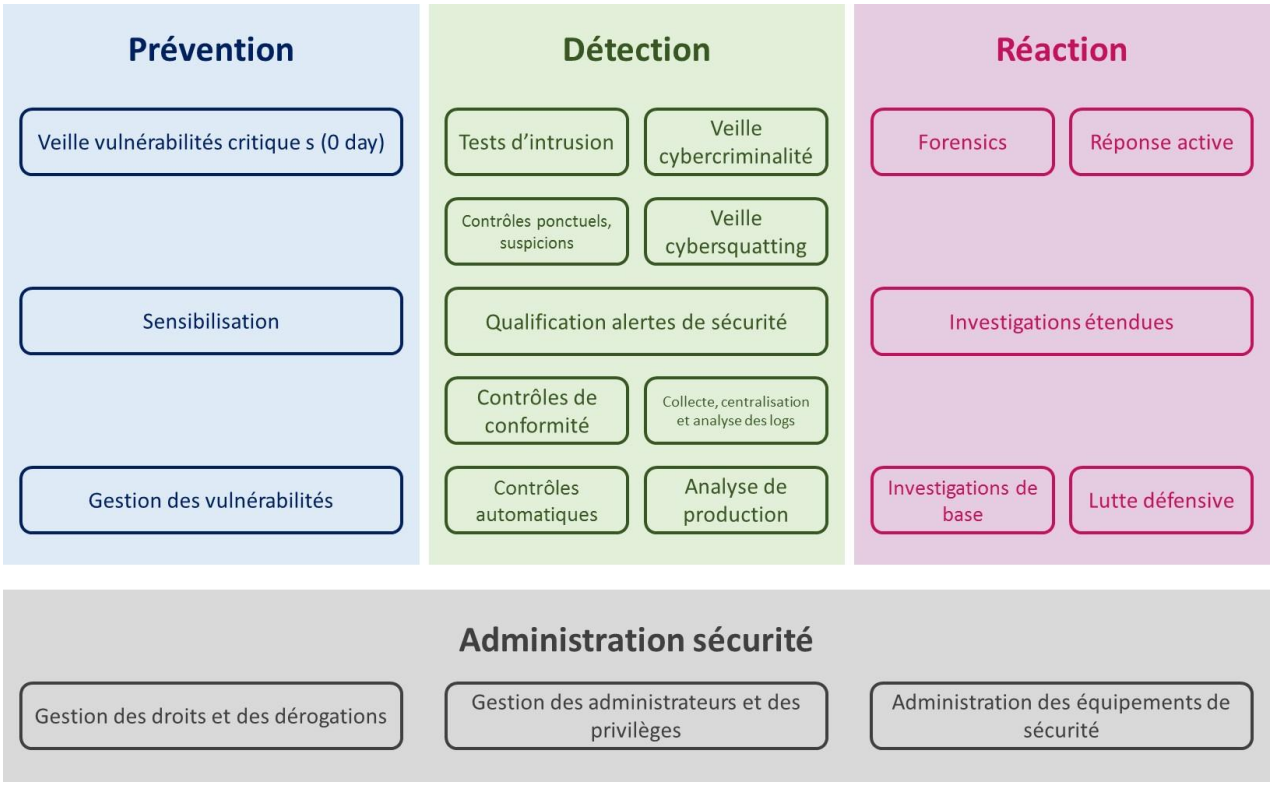


Figure 2. Exemple de catalogue des services de sécurité opérationnelle

Pour certains de ces services, la frontière est mince entre SOC et CSIRT. Il n'y a pas de définition de cette frontière, mais il reste certain que le SOC et le CSIRT, lorsque les deux existent, doivent travailler conjointement sur la majorité des fonctions sécurité.

III.1. Fonction de prévention sécurité

Le SOC doit être vu comme un outil de prévention sur la base des informations traitées et des actions préventives qui peuvent en découler. La prévention passe également par des actions de sensibilisation auprès des interlocuteurs du SOC.

III.1.1. Gestion des vulnérabilités

Ce service peut être rendu par le SOC ou si ce n'est pas le cas, le SOC doit bénéficier des informations sur les vulnérabilités connues du système d'informations pour affiner ses analyses d'impacts des événements de sécurité.

La gestion des vulnérabilités comprend la veille, la qualification, les préconisations puis le suivi du déploiement des patchs indiqués.

Elle s'effectue également en lien avec le service de détection de vulnérabilités et de contrôle sur les actifs du périmètre surveillé par le SOC.

III.1.2. Implication dans le processus de sensibilisation

Les incidents remontés par le SOC peuvent être le déclenchement d'actions de sensibilisation. Ces actions peuvent être ciblées pour recadrer par exemple un utilisateur déviant, ou généralisées pour toucher plus de monde sur des données plus transverses.

III.2. Fonction de détection

La fonction de détection est toujours à la base du SOC. La détection nécessite le traitement d'informations remontées par le SI surveillé. Ce traitement est plus ou moins automatisé selon les outils mis en place, mais il nécessite encore aujourd'hui un traitement manuel par des analystes sécurité. Les outils servent à analyser le volume d'informations et à réduire au maximum l'effort d'analyse. Une deuxième difficulté réside sur la pertinence des données analysées. Les outils doivent être configurés pour analyser des données en relation avec des scénarios de détection prédéterminés. Ces outils classiques peuvent être complétés par des outils d'analyse de comportements. Deux cas de figure peuvent arriver : trop de données inutiles engorgent les outils avec le risque de rater un événement permettant la mise en exergue d'un incident de sécurité, ou au contraire, il manque des données nécessaires à la détection et à la qualification de certains incidents. Le SOC doit continuellement adapter le paramétrage de ses outils pour limiter l'occurrence de faux positifs ou de vrais négatifs par exemple en adaptant les niveaux de seuil de détection.

III.2.1. Collecte des événements de sécurité et qualification des incidents

L'objectif de ce service est de disposer d'une vision centralisée des événements de sécurité, permettant de réaliser des rapprochements et des corrélations mettant en évidence des incidents potentiels.

Le SOC a besoin de collecter de l'information et généralement ces informations sont des logs générés par les différents composants du système d'information y compris les outils de surveillance d'accès au web et aux réseaux sociaux. Par extension, le SOC peut concentrer des alertes « prédéfinies » par un tiers ou remontées par les services support utilisateur.

Ce service nécessite la mise en place de la collecte des informations avec des enjeux d'architecture et des impacts potentiels sur les sources d'information, détaillés dans le chapitre 4.

Les informations collectées sont analysées pour déterminer d'éventuelles anomalies ou incidents. Cette analyse nécessite des outils de traitements de logs ou des SIEM, complétés par les outils de gestion documentaire et la messagerie pour les informations en dehors des logs.

III.2.2. Contrôle

Des contrôles de sécurité de divers niveaux peuvent être portés par le SOC.

Les contrôles basés sur des scanneurs de vulnérabilités configurés pour analyser les vulnérabilités visibles sur le système d'information, permettent de remonter au SOC l'état de sécurité des actifs du SI, et d'identifier d'éventuelles vulnérabilités ou menaces.

Les contrôles de conformité aux standards techniques permettent quant à eux de vérifier le respect des politiques de sécurité (ex : présence de droits administrateurs sur les postes, logiciels interdits,…), qui peuvent constituer autant de sujets à traiter.

Des audits manuels peuvent également être réalisés par des auditeurs indépendants ou appartenant au SOC. Au niveau d'expertise le plus élevé, des tests d'intrusion peuvent être réalisés afin d'éprouver sans prévenir au préalable la perméabilité des systèmes.

III.2.3. Veille sur les menaces et « threat intelligence »

Même si le SOC n'est pas en charge de maintenir la cartographie des risques, le SOC doit connaitre les menaces qui pèsent sur l'infrastructure surveillée et maintenir à jour le niveau des menaces pour renforcer si besoin certains contrôles ou actions de surveillance spécifiques à une menace.

À un premier niveau, le SOC peut réaliser une veille sur le « cybersquatting » et le défacement des sites webs, afin de suivre et de protéger l'image de marque et les données hébergées. Cela se traduit concrètement par la supervision des enregistrements de noms de domaines proches de ceux de l'entreprise, la surveillance des sites exposés, et le suivi sur les réseaux sociaux des mentions de l'entreprise.

La « threat intelligence » va plus loin en ce sens en réalisant une surveillance dans les milieux pirates des menaces en cours ou à venir vers l'entreprise ou son secteur d'activité. Le SOC permet alors de suivre les menaces externes réelles, concernant d'autres acteurs ou partenaires du même secteur d'activité ou de l'entreprise elle-même.

III.3. Fonction de réaction

La mise en œuvre d'un SOC oblige une réflexion de l'entreprise sur sa capacité à réagir à un incident de sécurité. Détecter sans réagir n'est clairement pas une solution. L'enjeu du SOC est d'adapter son niveau de support à la réaction à l'organisation de l'entreprise sachant que le SOC ne peut pas être le seul à réagir (le CSIRT entre fréquemment dans la partie).

III.3.1. Investigations et contribution à l'analyse

En cas d'identification d'un incident, le SOC peut avoir un rôle à jouer (souvent en complément du CSIRT) dans la réalisation d'investigations permettant de mieux comprendre l'attaque en cours. Le SOC a en effet à sa disposition le SIEM et d'autres outils de détection, d'investigation et d'analyse post mortem qui permettent de réaliser des opérations d'investigation : analyse des logs passés, filtrage des logs, rapports de scans sur des actifs particuliers, opérations sur les produits de sécurité des postes de travail (antivirus, HIPS,…).

III.3.2. Participation à la réaction

Le SOC peut également contribuer à la réaction dans la limite de son périmètre de responsabilité, via ses activités d'administration d'outils de sécurité. L'activation d'une règle IPS, la fermeture d'un compte administrateur ou VPN, l'ajout d'une règle pare-feu sont des exemples de réactions pouvant faire intervenir le SOC.

III.4. Fonction d'administration sécurité

Au-delà de son infrastructure et de ses outils propres (Logs manager, SIEM et autres), le SOC peut exploiter les composants sécurité ainsi que l'infrastructure de collecte.

Ce service doit être rendu – pour l'infrastructure SOC - par l'équipe SOC. Pour les autres composants sécurité, le SOC peut être en charge ou non. Dans ce dernier cas, le SOC se doit d'être en relation directe avec l'équipe d'exploitation sécurité.

Le SOC se doit d'avoir la connaissance des architectures surveillées et d'être averti lorsqu'elles évoluent. Le SOC doit également avoir un droit de regard sur les principaux moyens de détection d'incident comme :

Sondes de détection d'intrusion

Ces équipements sont conçus pour remonter des alertes suite à la détection de trafic suspect. Ces équipements nécessitent une veille sécurité active aussi bien pour les règles gérées par l'outil que pour l'outil lui-même. Il convient d'adapter en continu les politiques de détection et ce travail peut être confié au SOC.

Enfin le SOC peut assurer la maintenance corrective et évolutive des sondes.

Anti-virus

La menace de crise virale est souvent prise en compte par un SOC ; ce qui suppose une veille sécurité et une surveillance de l'application des mises à jour.

Ce type de surveillance sous-entend une implication du SOC dans la gestion des crises virales et l'application d'un processus d'alerting spécifique à une infection virale.

Data Loss Prevention

Le risque de fuite d'information peut être réduit par une surveillance effectuée par le SOC. Dans ce cas, le SOC se doit d'adapter les politiques de détection suite aux retours sur les alertes DLP. Il peut également prendre en charge la maintenance correctrice et évolutive et gérer la communication sur les incidents détectés par le dispositif DLP de l'entreprise.

IV. Structure et fonctionnement d'un SOC

Ce chapitre décrit la structure de fonctionnement d'un SOC, qui peut être adapté en fonction des services qu'il offre à l'entreprise. L'objectif est de donner les grands principes de fonctionnement d'un SOC, puis de donner des exemples de processus, de structuration des équipes, d'instances de pilotage, et des moyens nécessaires au SOC.

Au niveau macroscopique, un SOC peut être représenté ainsi :

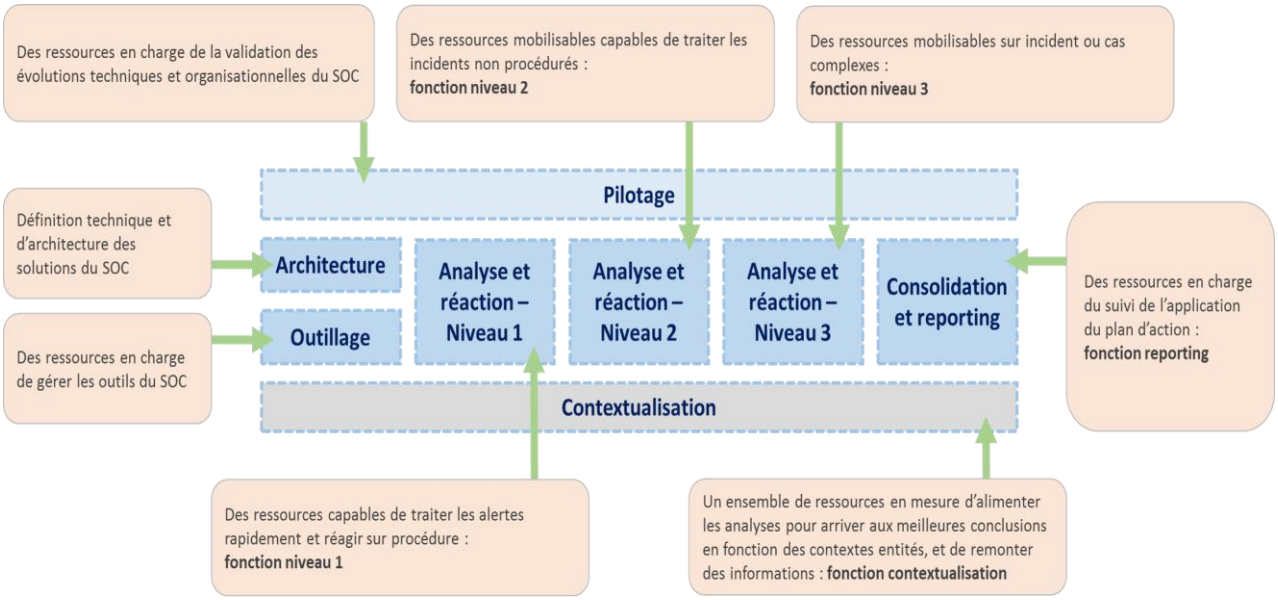


Figure 3 - Structure d'un SOC

Sont nécessaires à son fonctionnement :

- Une fonction MOA ou de pilotage : détachée de la gestion purement opérationnelle du SOC, elle vise à définir ses objectifs et sa stratégie, et valider les évolutions techniques, organisationnelles et fonctionnelles à planifier.
- Une fonction opérationnelle, répartie en niveaux 1, 2 et 3 :
  - Niveau 1 : analyse des événements en continu, avec capacité de traitement des événements et alertes procédurées
  - Niveau 2 : expertise complémentaire au niveau 1, permettant d'investiguer sur les événements et alertes non procédurées
  - Niveau 3 : expertise ponctuelle intervenant sur les alertes qualifiées et les crises ;
  - Ces trois niveaux sont sous la responsabilité d'un Responsable (Responsable du SOC).
- Une fonction en charge de la gestion et du maintien en conditions opérationnelles des outils du SOC (SIEM, ticketing, SIRP, sondes, scanneurs, …)
- Une fonction consolidation et reporting, en charge du suivi des alertes traitées et des plans d'action associés, ainsi que du reporting interne et externe au SOC

- Une fonction contextualisation : il s'agit de l'interface vers la DSI, les exploitants sécurité, et les sources d'événements. La contextualisation est nécessaire à la fois dans la construction des scénarios de détection, dans la capture d'événements, pour comprendre le contexte associé (ex : mise en production d'un projet générant de nouveaux événements), et dans la proposition et l'application de plans d'action, afin qu'ils soient adaptés et pertinents localement.

Seront décrits dans les parties suivantes : les principaux processus appliqués par le SOC, les ressources humaines d'un SOC avec les différents rôles à remplir, les instances de pilotages et les principaux moyens matériels d'un SOC.

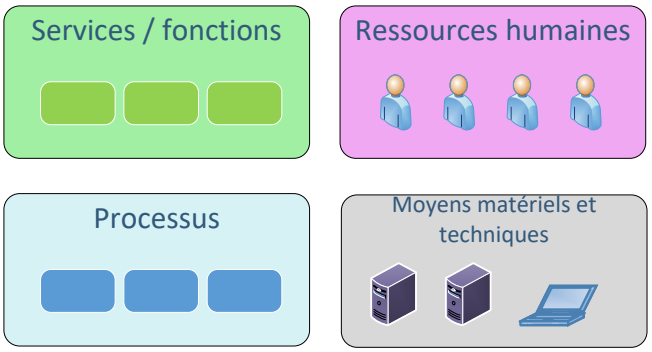


Figure 4 : Architecture générale d'un SOC

IV.1. Processus du SOC

De nombreux processus doivent être définis au sein du SOC en fonction de son catalogue de services. Ici nous nous limitons à décrire les processus liés à la supervision des évènements de sécurité :

- Processus de détection ;
- Processus de qualification ;
- Processus de supervision, de contrôle et d'administration du SOC ;
- Processus de veille.

Au-delà de ces processus décrits ci-après, d'autres sont également à définir tels que la gestion du paramétrage des sources de traces, la supervision des réseaux, la gestion des incidents (réaction, coordination, suivi et remédiations), la gestion des crises, la gestion du personnel, la gestion des compétences, etc.

Ces processus ne sont pas abordés dans ce chapitre.

Une règle de détection doit répondre à des objectifs précis et être réaliste (potentiellement "actionnable"). Elle doit répondre aux questions suivantes :

- Quel est l'objectif ? Quels sont les risques à couvrir ?

- Quelles sont les sources d’information nécessaires ?
- Quelles sont les informations de contexte nécessaires pour la mise en œuvre ?
- Quelle est l’origine de la règle de détection ?
- Que faire si la règle se déclenche ?
- Quel est la sévérité associée en fonction des actifs concernés ?
- Que doit faire un opérateur de niveau 1 ?
- Que doit faire un opérateur de niveau 2 ?
- Quelle organisation et réaction en heure ouvrée et en heure non ouvrée ?
- Dans quel cadre une crise est-elle déclenchée ?

Chaque règle de détection doit avoir une réponse associée en cas de déclenchement et après élimination des faux positifs. Si aucune réponse n'est associée à l'alerte, elle n'a vraisemblablement pas de sens dans le contexte de l'organisation de la surveillance et consomme des ressources en général uniquement dans un but de statistiques (dans un rapport dont la périodicité est à définir en fonction des enjeux).

IV.1.1. Processus de détection

Le processus de détection est principalement axé sur les moyens de supervision des risques et la réception d'alertes. Néanmoins la supervision opérationnelle des propres équipements du SOC doit également faire partie de ce processus.

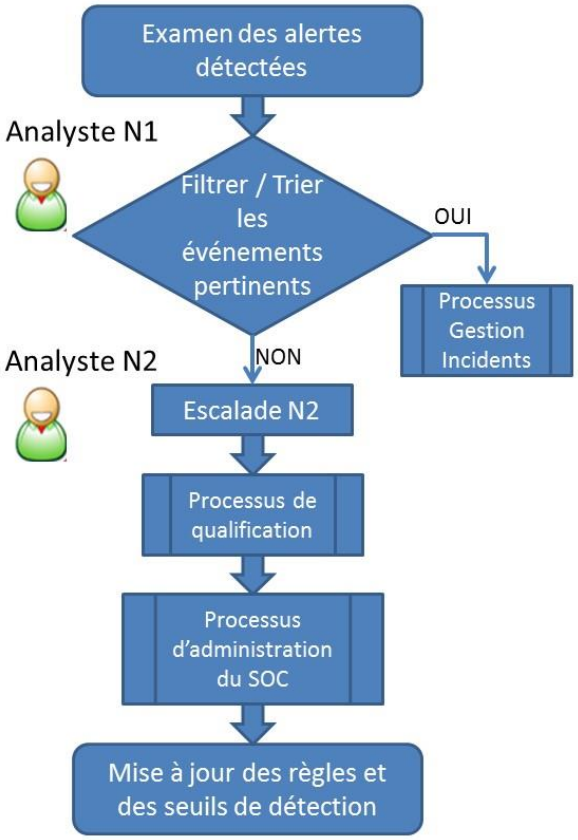
Entrées	Activités	Sorties
▪ Tableaux de bord de la sécurité ▪ Toutes sollicitations dont l'origine est : échanges avec les exploitants ; Help Desk ; d'une cellule d'alerte ▪ Résultats du processus de veille ▪ Résultats du processus de supervision, de contrôle et d'administration		➢ Alertes de sécurité à entrer dans le processus de Gestion Incidents ➢ Identification de cas nécessitant des actions en boucle de retour à passer au processus d'administration du SOC (mise à jour de règles de détection, réglages de seuils d'alerte, élimination de faux positifs, etc.)

Figure 5 : Processus de détection

Détails des activités :

Les analystes examinent

- les alertes détectées par les outils du SOC,
- les informations sur la veille sécurité SI,
- les sollicitations externes des autres équipes opérationnelles ou du help desk,

- éventuellement, les incidents provenant des outils de supervision des réseaux ou des systèmes.

La première activité composant ce processus est de filtrer les évènements entrants pour ne retenir que les éléments pertinents (notamment suppression des faux positifs à partir des bases de connaissance du SOC) et d'opérer un tri selon des critères de pertinence de l'évènement.

Cette activité est à la charge d'un analyste dit de niveau 1. Cette tâche doit être rapide. Si l'analyste niveau 1 ne peut effectuer un tri et communiquer de manière exploitable l'alerte au processus de gestion d'incident (c'est-à-dire si l'alerte n'a pas déjà été rencontrée et n'a pas de procédure associée), il doit faire appel à un niveau 2.

Le niveau 2 exécute le processus de qualification et le processus d'administration fonctionnelle du SOC pour mettre à jour les règles et les seuils de détection, amender les critères et seuils d'invocation du niveau 2.

La supervision des indicateurs de sécurité par les analystes peut être impactée par la charge de travail de l'équipe SOC. À défaut, ce processus est activé sur les éléments accumulés[5] en début et en fin de journée de fonctionnement du SOC.

Il est à noter que bien que le processus de gestion des incidents n'est pas traité dans ce chapitre, il convient de définir les procédures associées (éradication d'un malware sur un poste, mise en liste noire d'urls, autres…).

Chaque organisme traitera ensuite ses alertes en fonction de sa propre stratégie de gestion de risques (réactivité quitte à bloquer un utilisateur sur un faux positif, ou bien ne bloquer que les alertes avérées quitte à perdre du temps).

[5] Notamment pendant les heures où le SOC ne fonctionne pas ou en cas de retard de traitement. Cf. Contrôle du processus de détection.

IV.1.2. Processus de qualification

Le processus de qualification est un ensemble de tâches attribuées au rôle d'analyste niveau 2 du SOC.

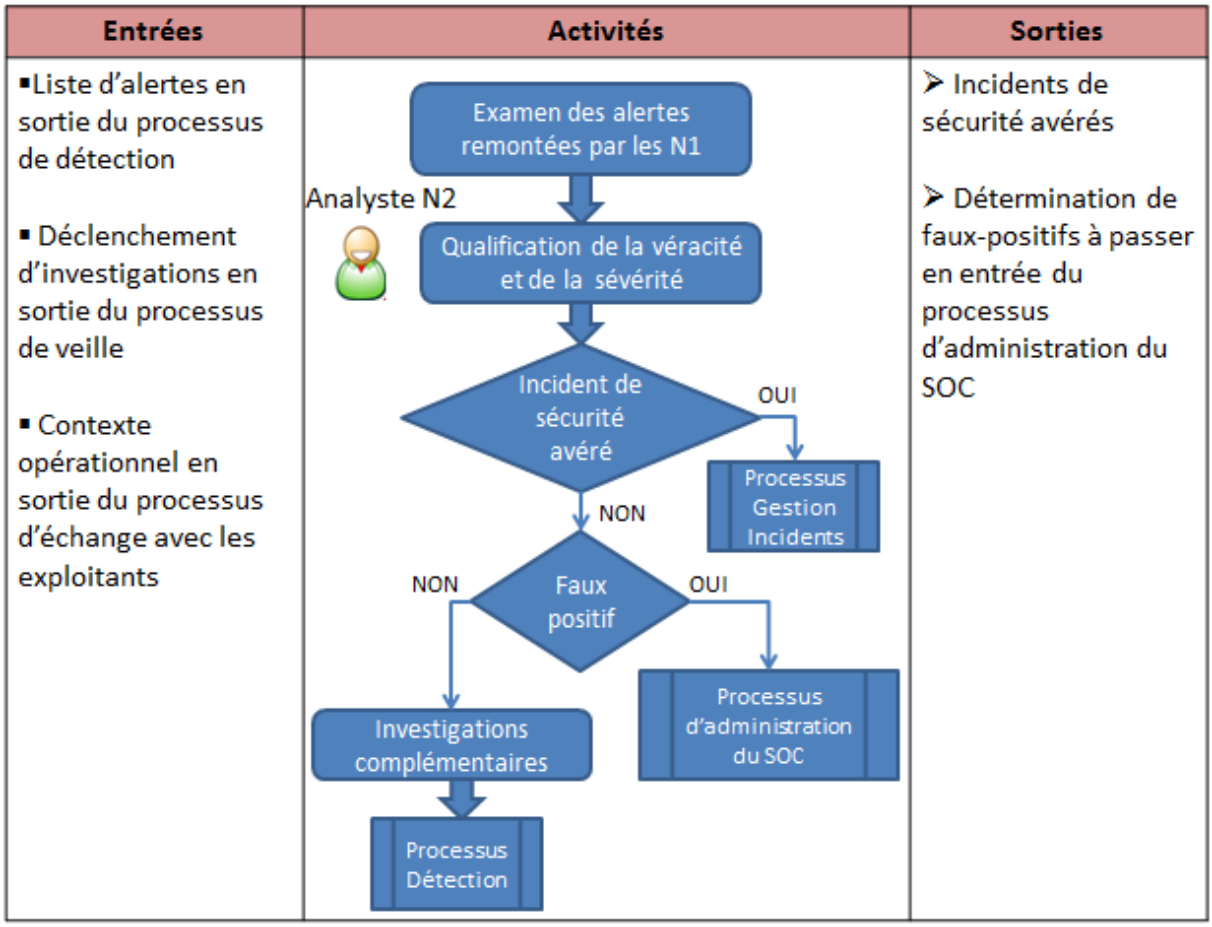


Figure 6 : Processus de qualification d'incident

Détails des activités :

Ces tâches incluent :

- L'étude des lots d'alertes remontées par les analystes niveau 1 après tri et priorisation ;
- L'enrichissement et la contextualisation des informations liées aux alertes remontées par les analystes niveau 1 ;
- La détermination de la véracité et de la sévérité de l'incident de sécurité sous-jacent ;
- Dans le cas d'un incident de sécurité avéré, la détermination de la nécessité de passer ces alertes à un processus de gestion d'incidents ;
- L'isolation et la description des faux-positifs afin de les passer en entrée du processus d'administration du SOC.

Les investigations de qualification conduites par les analystes de niveau 2 conduisent :

- Soit à l'émission d'une alerte avérée à passer à un processus de gestion d'incident ;
- Soit à la nécessité de procéder à davantage d'investigations ou de détecter d'autres événements liés, ce qui renvoie en entrée du processus de détection.

IV.1.3. Processus de supervision, de contrôle et d'administration du SOC

La supervision concerne uniquement le périmètre du SI du SOC. Le SI du SOC doit être supervisé par les analystes.

La définition de niveaux (ou seuils) doit être contrôlée afin de ne pas saturer les processus de détection et de qualification.

Les processus de détection, de qualification, ainsi que le processus de veille impliquent des opérations d'administration du SOC. Le processus d'administration du SOC implémente notamment la « boucle de retour » permettant l'amélioration continue des performances des fonctions de détection et de qualification du SOC.

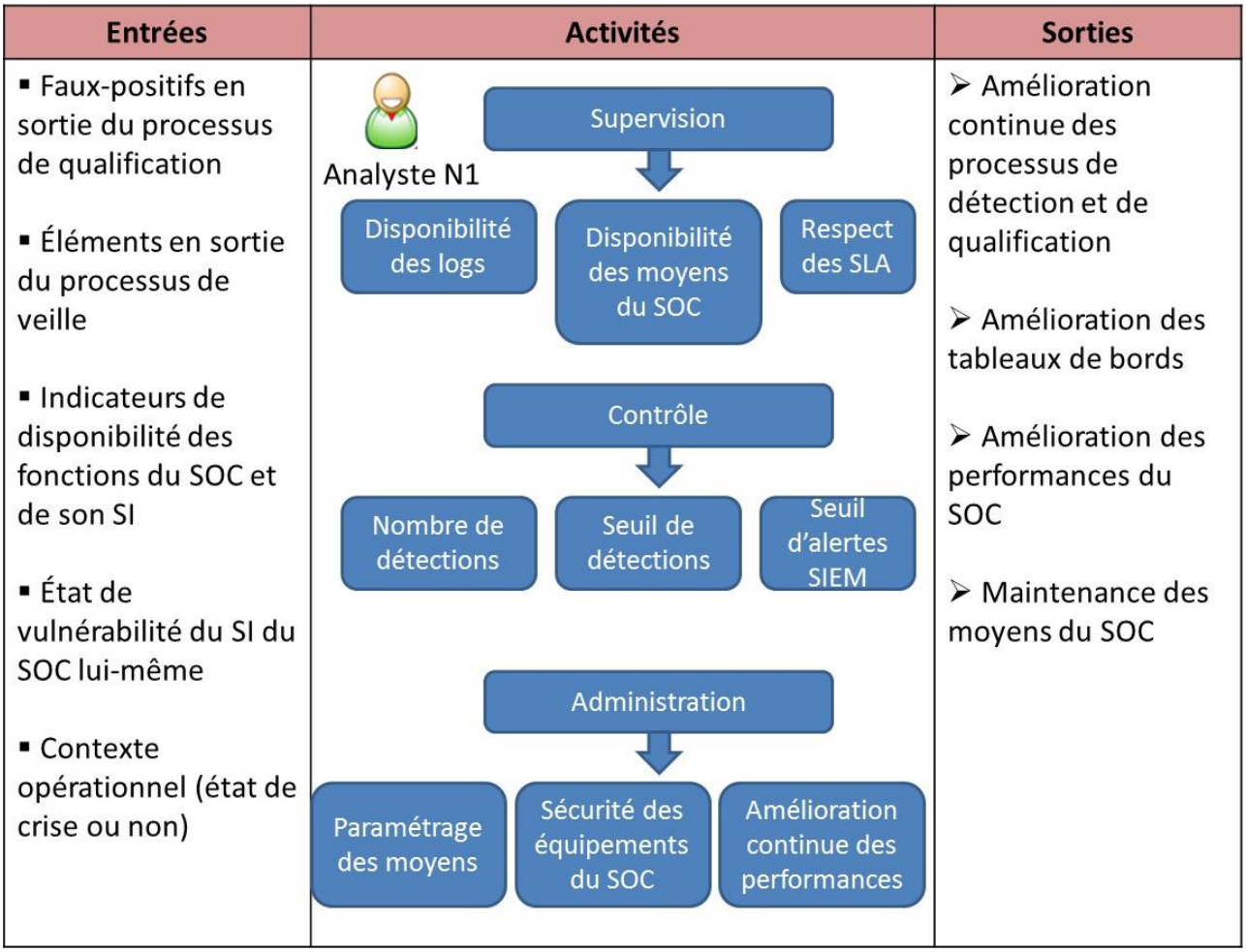


Figure 7 : Processus de supervision, contrôle et administration du SOC

Détails des activités :

Supervision :

- La disponibilité des traces produites localement par les sources ;
- La disponibilité et le fonctionnement attendu des moyens du SOC ;
- L'efficacité des services du SOC (SLA) ;
- La sécurité du SI du SOC notamment en termes de confidentialité/intégrité des traces et d'intégrité des processus de détection et de qualification.

Les indicateurs envisageables sont :

- Mesurer le nombre par unité de temps d'entrées dans le processus de détection. Ces entrées nécessitant un tri de la part des analystes de niveau 1, le nombre maximal d'entrée ne doit pas être supérieur à la capacité de traitement par le SOC ;
- Mesurer le nombre par unité de temps d'alertes générées par le SIEM à traiter par les analystes de niveau 1 ; ce nombre maximal ne doit pas conduire à laisser un volume résiduel d'alertes jamais traitées et augmentant avec le temps ;
- Etc.

Ces mesures conduisent à réaliser les adaptations suivantes :

- Revoir l'affectation en ressources humaines lors de montées en charge récurrentes du processus de détection ;
- Ne pas traiter les entrées au-delà des maximums fixés ci-avant. Si ces maximums sont régulièrement dépassés, le processus de d'administration du SOC doit être invoqué et permettre de moduler le nombre de ces entrées ou de modifier les seuils d'alerte ;
- Etc.

Un outil de mesure de la maturité du SOC peut également apporter une aide (par exemple « Cyber Security Incident Response Maturity Assessment » produite par le CREST).

Administration :

Alors que la plupart des actions d'administration du SOC ont pour objet de paramétrer finement les moyens, certaines d'entre elles consistent aussi à maintenir et améliorer la disponibilité et la sécurité des équipements du SOC (serveurs, infrastructure de sauvegarde, postes de travail des analystes, réseau dédiée du SOC, etc.).

IV.1.4. Processus de veille

Le SOC se trouve confronté en permanence aux vulnérabilités du SI, aux cyber menaces et aux attaquants qui en sont à l'origine. La veille dans ces domaines est donc une fonction centrale du SOC pour garder un tempo de défense convenable. Tous les membres du SOC doivent plus ou moins être impliqués dans ce processus. Cependant cette implication revêt une importance particulière.

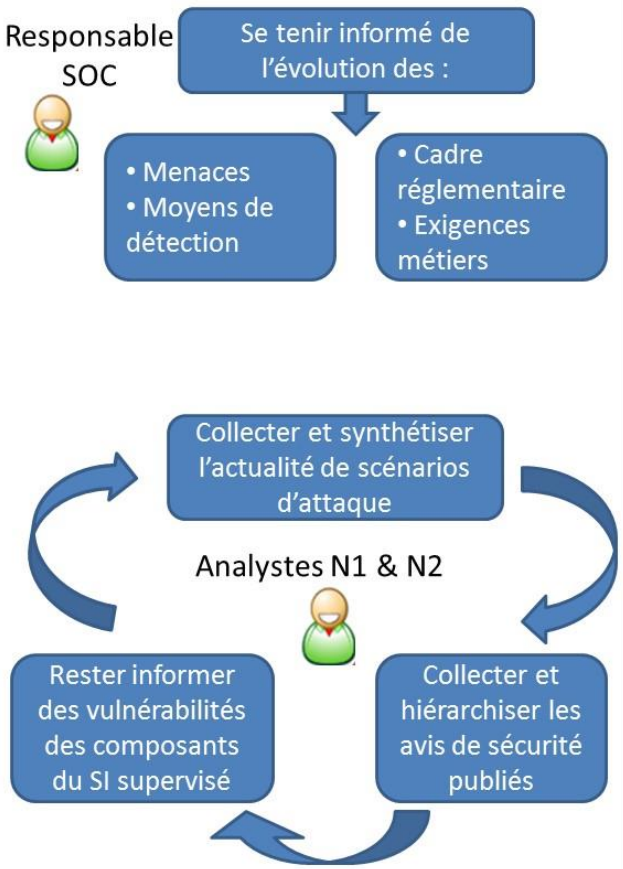
Entrées	Activités	Sorties
▪ CERTs et autres sources d'information sur l'actualité de la cybermenace ▪ Évolutions des exigences de sécurité des métiers ▪ Scans de vulnérabilité sur le SI ▪ Contexte opérationnel transmis par les équipes d'exploitants		➢ Nouvelles (ou amélioration des) règles de détection ➢ Amélioration du processus de qualification ➢ Amélioration du processus de supervision ➢ Expression de besoins d'évolution ou de provisions budgétaires pour le SOC ➢ État des vulnérabilités du SI supervisé

Figure 8 : Processus de veille

Détails des activités :

- Le Responsable du SOC doit s'assurer que son équipe se tient à jour des grandes tendances d'évolution des menaces et des moyens de détection ainsi que de l'évolution du cadre réglementaire et des exigences des métiers. Il doit également suivre la mise en œuvre des actions correctives ou préventives à moyen et long terme.
- Les analystes doivent : collecter et synthétiser l'actualité en matière de scénarios d'attaque ; collecter et hiérarchiser les avis de sécurité publiés ; rester informés des vulnérabilités des composants du SI supervisé. Ils doivent également s'assurer de l'efficacité des règles en fonction de nouvelles vulnérabilités et alertes (publiées par un CSIRT interne ou externe à l'organisation).

IV.1.5. Interfaces

Ce chapitre traite des interfaces opérationnelles que le SOC doit mettre en place avec les exploitants du SI. Les autres interactions que le SOC peut avoir avec les métiers, les fonctions RSSI ou le support ne sont pas traitées dans ce chapitre. Dans ce contexte, ce chapitre est sans a priori sur l'externalisation ou non des fonctions du SOC car cela n'influe que peu sur la description de ces interfaces.

Dans certaines organisations, plusieurs SOC peuvent être mis en œuvre. En général, il s'agit d'un SOC centralisé et des SOC locaux dans des périmètres spécifiques (métiers ou géographique). Dans une telle organisation, les échanges entre ces SOC se révèlent également d'une grande importance à la fois pour le partage des informations de détection afin d'identifier une attaque pouvant toucher plusieurs périmètres mais également pour mener des réactions collectives et/ou centralisées.

Tous les exploitants peuvent être amenés à échanger avec le SOC qu'ils soient responsables d'équipements de sécurité ou non. Les interactions entre le SOC et les exploitants sont bidirectionnelles.

Les informations utilisées par le SOC pour remplir ses fonctions de détection et de qualification ne se limitent pas aux informations obtenues à travers ses moyens propres. Les informations obtenues via les exploitants techniques ont aussi une importance.

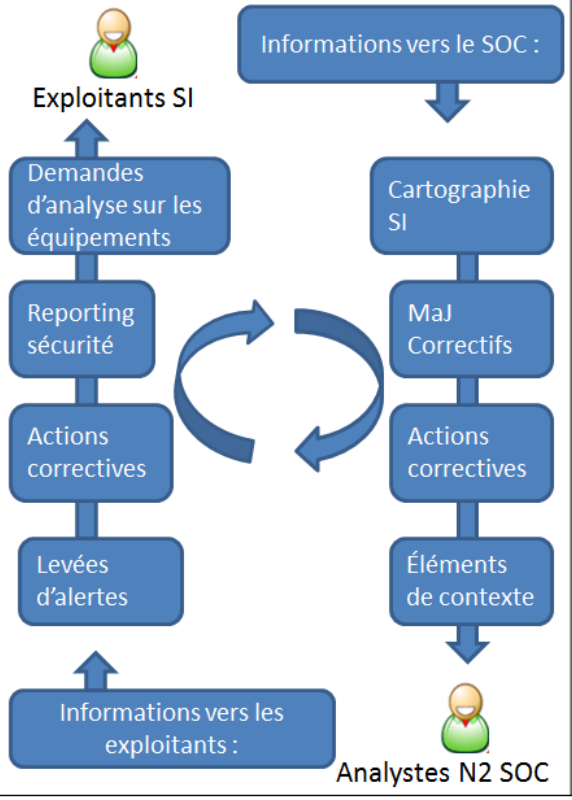
Entrées	Activités	Sorties
▪ informations opérationnelles ▪ informations métiers ▪ Événements liées au SI ▪Recommandations du SOC		➢ partage d'informations de détection ➢Identifications d'attaques multi-périmètres ➢Mener des réactions collectives et/ou centralisées

Figure 9 : Interfaces du SOC

IV.1.5.a. Informations à destination du SOC

Les analystes niveau 2 du SOC ont besoin d'informations opérationnelles (techniques et métier), afin de déterminer un contexte autour des alertes de sécurité qu'ils traitent. Le SOC est donc amené à solliciter les exploitants et les correspondants métier pour obtenir ces informations régulièrement. Les exploitants informent également le SOC d'événements liés au SI dans leurs périmètres organisationnels, fonctionnels et techniques.

La nature de ces échanges peut être (liste non exhaustive) :

- La cartographie du SI et des réseaux (mise à jour régulièrement) ;
- Le compte rendu de l'état de mise en œuvre des actions correctives ;
- L'état de mise à jour et d'installation de correctifs sur les systèmes ;
- L'état de mise en production de nouvelles applications ;
- Des éléments de contexte à fournir au SOC pour aider à la tâche de qualification des incidents.

IV.1.5.b. Informations à destination des exploitants

De même, le SOC n'a pas toujours la responsabilité de mettre en place les paramétrages sur les sources de traces consommées par le SIEM. Le SOC n'a pas non plus la charge de procéder aux actions correctives suites à des incidents de sécurité.

Le SOC peut également être amené à émettre des recommandations (voire des directives/priorités selon la sévérité des cas à traiter) à destination des exploitants. C'est aux exploitants chacun dans leur périmètre d'implémenter les actions liées à ces recommandations.

La nature de ces échanges peut être (liste non exhaustive) :

- La levée d'alertes de la part du SOC à destination des exploitants ;
- Le suivi du SOC sur les actions correctives à mettre en œuvre par les exploitants ;
- Le reporting à destination des exploitants sur l'état de sécurité du SI en temps de crise ou non ;
- Les demandes de vérifications sur les équipements pour améliorer la qualification des incidents.

IV.1.6. Reporting

Les capacités de reporting sont à maintenir régulièrement par le SOC dans le but de :

- Mettre en avant les indicateurs de sécurité les plus pertinents ;
- Améliorer la capacité de détection visuelle des analystes en groupant visuellement les indicateurs partageant des liens de corrélation ;
- Permettre simultanément d'avoir une vision globale du niveau de sécurité du SI et de faire, au besoin, un « zoom » sur un événement en particulier sur un équipement supervisé en particulier ou concernant un utilisateur du SI en particulier ;
- Créer des tableaux de bord spécifiques pour les exploitants afin de répondre à leurs attentes par rapport au SIEM et à les impliquer dans le projet ;

- Créer des rapports pour démontrer la performance du SOC aux métiers.

IV.1.6.a. Indicateurs de contrôle et de suivi de l'activité du SOC

Le SOC se doit d'assurer des indicateurs reflétant son activité et le périmètre surveillé. Le SOC (analystes niveau 1 en général) produit donc périodiquement un ensemble de paramètres tels que :

- Le nombre de sources supervisées dont l'éventuelle inactivité peut traduire un dysfonctionnement ou une attaque ;
- Le niveau de mise à jour de la cartographie des réseaux surveillés ;
- Les indicateurs de volumétrie traitée par le SIEM en nombre d'événements collectés par unité de temps par catégorie de sources de traces ;
- Le niveau de remplissage de la base de conservation des traces.

Le SOC doit disposer de moyens pour mesurer son efficacité.

- Indicateurs du temps minimal/moyen/maximal entre la génération d'un événement par une source et la fin de son traitement (collecte, centralisation, normalisation, corrélation, alerte ou non) ;
- Indicateurs du temps minimal/moyen/maximal de traitement d'une recherche dans les traces ;
- Indicateurs sur le taux de disponibilité des composants techniques du SOC.

Le SOC doit également être en mesure d'évaluer la qualité de la détection et de la qualification :

- Disposer, à intervalles de temps réguliers, d'un état des lieux des règles de détection (Nombre de règles, Ajouts/modifications ou suppressions de règles)
- Disposer de la liste des règles de détection n'ayant jamais été déclenchée durant une certaine durée de temps ;
- Disposer d'indicateurs de la qualité de la détection :
    - Nombre d'événements ayant conduit à une levée d'alerte par unité de temps ;
    - Nombre de ces événements qualifiés comme faux-positifs ;
    - Nombre de règles de détection déclenchées par unité de temps ;
    - Volume de remplissage de la base de conservation des traces par unité de temps.
- Disposer d'indicateurs d'évaluation de la qualité de la qualification :
    - Délai maximal de qualification d'un incident ;
    - Délai moyen de qualification d'un incident de sécurité selon son niveau de gravité ;
    - Délai moyen de mise à jour des règles de détection suite à une demande du commanditaire ;
    - Durée moyenne d'une recherche unitaire d'incident ;
    - Nombre et taux d'erreurs de qualification d'incident ;
    - Taux d'évènements non reconnus et donc non pris en compte par les outils techniques d'analyse.

IV.1.6.b. Indicateurs stratégiques du SOC

La stratégie conseillée en général pour la mise en place d'un SOC est articulée en itérations successives de déploiement et d'enrichissement. Ces déploiements impliquant des périmètres et finalités de détection de plus en plus étendus, il n'est raisonnable de passer à l'itération suivante que si le rodage et les opérations de l'itération précédente sont satisfaisants.

Afin d'évaluer ces aspects, des indicateurs doivent être constitués. Ils incluent :

- La consolidation des indicateurs évaluant les opérations du SOC (cf. ci-dessus) ;
- Le taux de disponibilité de la fonction de détection du SOC ;
- Le taux de disponibilité des dispositifs techniques du service de détection (SIEM) ;
- Le nombre d'incidents avérés sur le système d'information du SOC (qualification).

Ces indicateurs permettent au chargé de pilotage du SOC d'apporter des arguments pertinents quant aux décisions de GO/NO GO à l'itération suivante.

IV.2. Ressources humaines du SOC

IV.2.1. Rôles et responsabilités au sein du SOC

L'organisation du SOC dépend bien entendu du catalogue de service qu'il offre mais également du contexte organisationnel interne. Nous décrivons ici l'organisation minimum liée à un service de détection et de qualification des évènements de sécurité, comme pourrait le rendre un prestataire MSSP. Les rôles sont les suivants :

- Maitrise d'ouvrage ;
- Responsable opérationnel ;
- Analyste de niveau 1 ;
- Analyste de niveau 2 ;
- Expert niveau 3 (pouvant être hors de l'organisation du SOC) ;
- Maintenance des équipements du SOC ;
- Maintenance des règles du SIEM ;
- Rôle de veille ;
- Coordination et suivi de la gestion des incidents de sécurité ;
- Amélioration de reporting.

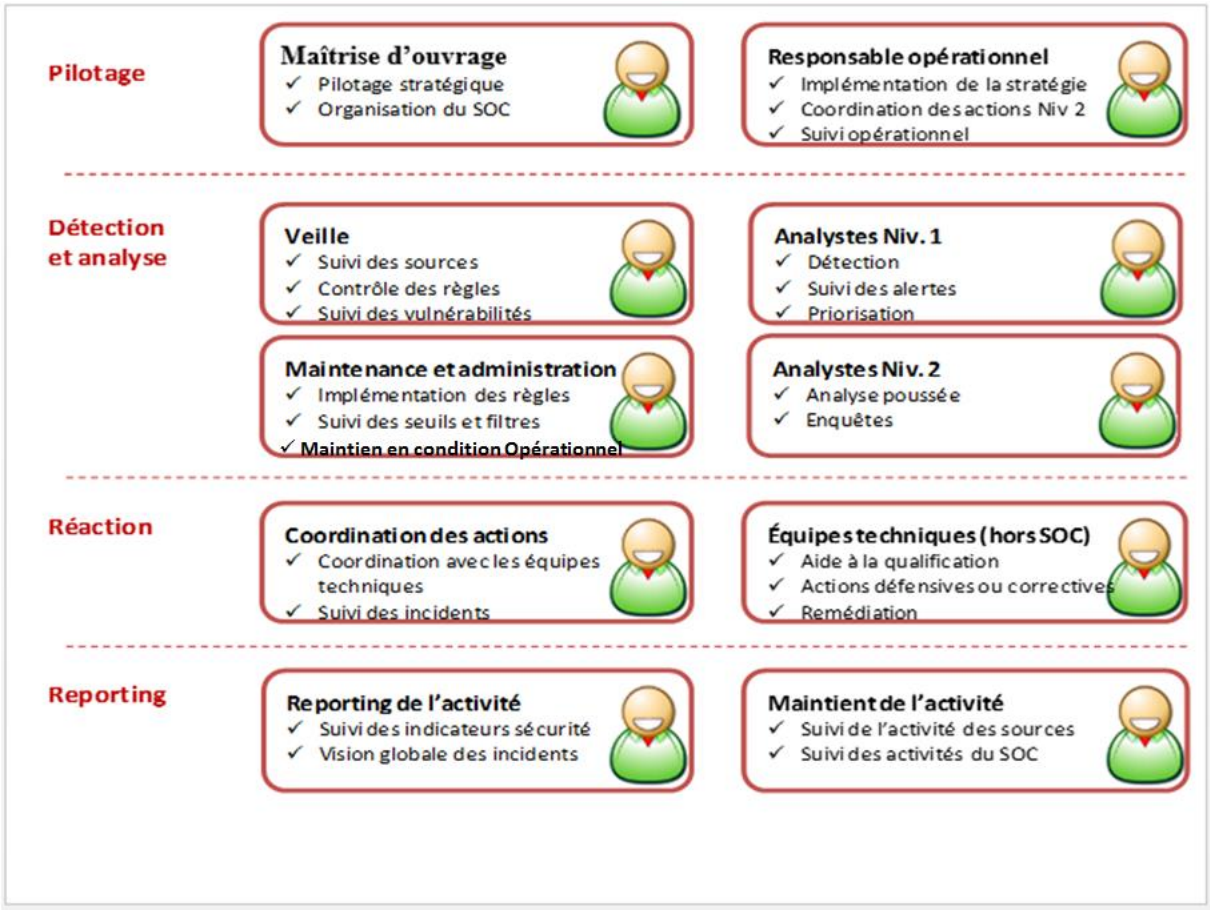


Figure 10 : L'organisation humaine du SOC

Les personnes qui se voient affecter des rôles et responsabilités au sein du SOC peuvent ne pas être dédiées à cette activité. Il est donc très important d'établir clairement :

- Les jours et plages horaires où la personne est en charge de responsabilités au sein du SOC ;
- Un moyen de passage de relai entre deux personnes ;
- Un planning permettant suffisamment de rotations des personnels de l'équipe pour couvrir convenablement les plages horaires de fonctionnement du SOC ;
- Un état des lieux des compétences afin de garantir un niveau de compétence minimal pendant les horaires de fonctionnement du SOC ;
- Des astreintes et scénarios de mobilisation d'urgence.

Plusieurs de ces rôles, détaillés ci-dessous, peuvent être affectés à une seule personne suffisamment disponible et compétente. De plus, ces rôles peuvent être tout ou partie sous-traités en support au SOC en cas de :

- Compétences insuffisantes ;
- Disponibilité faible des personnes ;
- Montée en puissance lors de périodes de crise ;
- Maintien ou évolution du référentiel documentaire du SOC et notamment des règles de corrélation.

IV.2.1.a. Maîtrise d'ouvrage du SOC

Ce rôle :

- Détermine les besoins du SOC (extensions d'outillages voire prestations externes) ;
- Assure la qualité, la fréquence et la correction de la détection, analyse, qualification, priorisation et résolution des incidents de sécurité ;
- Affecte les rôles du SOC à des personnes compétentes et est garant du maintien de ces compétences ;
- Anime les réunions du comité stratégique sur les activités du SOC et les évolutions de périmètre.

IV.2.1.b. Rôles opérationnels

Responsable opérationnel du SOC

- S'assure du maintien en condition opérationnelle et de l'évolution de l'outillage du SOC (SIEM et autres outils de supervision) ;
- Implémente les évolutions décidées par le comité stratégique (nouvelles sources, nouvelles règles, nouveaux périmètres) ;
- Coordonne les opérations du SOC, notamment l'évolution des seuils et processus d'invocation d'analystes niveau 2 ;
- Collecte des informations permettant d'alimenter les indicateurs de performance du SOC ;
- Exprime, justifie et chiffre les besoins de maintenance ou d'extension du SOC et de son outillage ;
- Anime les réunions périodiques du comité opérationnel ;
- Gère les ressources et le planning d'activité du SOC ;
- Rend compte au responsable du SOC de l'activité du SOC.

Analyste niveau 1

- Surveille en temps réel les consoles des outils du SOC et les indicateurs de sécurité maintenus par le SOC ;
- Trie dans les événements de sécurité pour déterminer les événements intéressants ;
- Gère les incidents mineurs et les règles de détection génériques ;
- Invoque des analystes de niveau 2 en cas d'incident nécessitant une attention particulière. Le traitement des alertes par les analystes de niveau 1 doit rester dans une fourchette d'une à 15 minutes. Au-delà l'escalade de niveau 2 est à faire. Les analystes de niveau 1 ne doivent pas s'engager dans des analyses poussées pour garantir le traitement d'un maximum d'événements de sécurité et d'alertes.

Analyste niveau 2

Un Analyste Niveau 2 est un rôle qui suppose plus d'expérience et d'expertise que le niveau 1. Ce rôle ne nécessite pas forcément un plein temps. Il peut être cumulé selon l'organisation avec d'autres rôles exigeant aussi une expertise sécurité importante.

Il est responsable :

- D'investigations poussées pouvant s'étaler sur plusieurs jours à plusieurs semaines (dans les cas extrêmes d'analyse de malware ou de full packet capture) ;
- D'assurer le suivi des actions correctives, suite à la détection d'un incident de sécurité complexe impliquant des compétences dans plusieurs domaines techniques et donc plusieurs exploitants ;
- D'améliorer la capacité de détection du SOC et de réduire les faux positifs traités par le niveau 1.

Rôle de maintenance des équipements du SOC

Les sources de traces, l'infrastructure et les moyens utilisés par le SOC nécessitent des actions de maintien en condition opérationnelle (configuration, de maintenance, amélioration). De la qualité de ces actions dépendent l'efficacité du SOC. Elles doivent donc être réalisées par des personnes habilitées compétentes.

Dans une petite organisation, ces activités peuvent-être sous la responsabilité de l'analyste niveau 2.

Rôle de maintenance des règles du SIEM

Les règles de détection et les seuils/critères d'alertes implémentés dans le SIEM nécessitent des actions régulières comme :

- Les règles de corrélation doivent être créées et simplifiées par la suite pour permettre de détecter des scénarios précis ;
- Les règles doivent être amendées en cas de faux positifs trop nombreux ;
- Les seuils et critères de détection doivent être implémentés a priori puis réglés en fonction du nombre d'alertes levées par le SIEM afin de ne pas noyer l'information utile ;
- Les seuils et critères d'alertes doivent être pilotés en fonction du nombre d'attaques que subit le SI. En période de crise (ex. Déni de Service Distribué), les alertes doivent être levées avec des seuils plus élevés afin de ne pas noyer le SIEM et le SOC sous la masse d'incidents à traiter.

Dans une petite organisation, ces activités devraient-être sous la responsabilité de l'analyste niveau 2.

Rôle de veille

Tous les membres du SOC sont à différents niveaux impliqués dans le processus de veille.

Les activités des principaux acteurs sont mentionnées dans IV.1.4 le processus de veille.

Rôle de coordination et suivi de la gestion des incidents de sécurité

Une fois la qualification faite des alertes, les incidents de sécurité avérés doivent être traités en réaction. Ce traitement en réaction nécessite selon la sévérité et la complexité de l'incident :

- Des actions permettant de cloisonner l'incident ;
- Des actions correctives simples ou multiples à implémenter par un voire plusieurs exploitants ;
- Des actions séquencées et coordonnées entre les exploitants pour l'efficacité de la défense du SI ;
- Des actions ayant différentes priorités, dont certaines à moyen/long terme nécessitant un suivi récurrent.

Le rôle de coordination et de suivi de la gestion des incidents consiste à orchestrer ces actions de manière optimale sans négliger besoins/impératifs opérationnels et métier des exploitants.

Ce rôle est à la limite entre l'objectif principal d'un SOC axé sur la détection et l'objectif d'une équipe CSIRT axé sur la réaction. Quelle que soit l'organisation, le SOC doit connaitre les vulnérabilités du SI qu'il surveille et la non correction d'un incident est une vulnérabilité majeure.

IV.2.1.c. Rôle de Reporting

Ce rôle :

- Réalise les indicateurs de contrôle et de suivi de l'activité du SOC (analyste N1 en général) ;
- Fournit les indicateurs stratégiques du SOC (responsable opérationnel en général) ;
- Les activités sont mentionnées dans Reporting_Reporting.

IV.2.2. Interface avec les services externalisés

Dans le cas où une partie ou la totalité des rôles du SOC sont externalisés en MSSP, le commanditaire doit quand même mettre en place un certain nombre de ressources.

Parmi celles –ci :

- Le Chef de Projet (en phase de « Build ») ou Gestionnaire du service du SOC (en phase de « Run ») en charge de la bonne réalisation des prestations demandées et du respect des SLA pour la partie contractuelle. Par ailleurs, le RSSI ou le service de gestion des risques fournit les analyses de risques sur les SI lors de la mise en place du SOC, valide les alertes et leur qualification lors du déploiement et gère leur mise à jour par la suite en accord avec les événements constatés ;
- Un responsable métier qui fait normalement le lien entre la DSI interne du client et le SOC externalisé pour fournir les éléments de CMDB et autres informations sur le contexte du SI, et pour vérifier que la remontée des traces ou des éléments d'analyse s'effectue bien côté client ;
- Une ou plusieurs personnes chargées d'analyser les alertes et incidents remontés par le prestataire, de déterminer la pertinence de l'incident, éventuellement d'ouvrir un ticket auprès des services informatiques pour corriger un problème (configuration de pare-feu ou de serveur par exemple) et de clôturer l'alerte ou l'incident.

IV.3. Structures de pilotage

La gouvernance du SOC doit s'appuyer sur une ou plusieurs instances de suivi et pilotage.

A titre d'illustration, voici un exemple d'organisation qui a pu être mise en place :

- Comité de suivi opérationnel (ComOP) – Réunions selon une fréquence hebdomadaire ;
- Comité de pilotage (COPIL) – Réunions selon une fréquence mensuelle ;
- Comité stratégique (COSTRA) – Réunions selon une fréquence trimestrielle.

Quelle que soit l'organisation du SOC, le but de ces comités est de faire le point entre toutes les parties prenantes du SOC. Ils rassemblent donc les équipes en charge d'opérer le SOC et les équipes des métiers applicatifs de l'entreprise (ou les équipes chargées de faire le lien entre ces deux entités).

IV.3.1. Comité opérationnel hebdomadaire (ComOP)

Les ComOP sont organisés toutes les semaines.

En phase de « Build », ils sont animés par le chef de projet. Ils permettent de coordonner toutes les activités du Build.

En phase de « Run », ils sont animés par le responsable opérationnel du SOC. Ils permettent d'effectuer une revue des incidents de la période précédente (par ex. fournir un complément d'information pour permettre une action de remédiation par les métiers applicatifs ou confirmer la fermeture d'un ticket). Les participants au ComOP planifient les actions de la semaine à venir en fonction de la criticité des incidents en cours. Les points et difficultés majeurs sont remontés au niveau des comités de pilotage mensuel.

IV.3.2. Comité de pilotage (COPIL)

C'est une réunion mensuelle qui a pour but de s'assurer le bon pilotage du service. Elle est animée par le responsable opérationnel du SOC. L'accent est mis sur :

- le bilan de la période écoulée d'un point de vue service de supervision (quantitatifs et qualitatifs) : incidents critiques, principales requêtes, résultats des changements effectués, statut des actions ;
- le tableau de bord projet synthétisant les KPI contractuels (ex. nombre d'incident, nombre de ticket clos, secteurs du SI les plus touchés par les incidents) ;
- l'évolution du périmètre du service et la stratégie de prise en compte des changements ou actions demandés le mois précédent.

IV.3.3. Comité stratégique (COSTRA)

Les COSTRA sont organisés chaque trimestre. Ils rassemblent au niveau direction les parties prenantes (Entité en charge du budget du SOC, les différents métiers de la DSI ou des autres entités bénéficiant des services du SOC). Ils permettent une véritable communication interne pendant laquelle il est possible de mesurer le retour sur investissement du SOC ou au contraire les points de blocage qu'il convient de lever. L'ordre du jour type est le suivant :

- le bilan de la période écoulée : synthèse des moments forts, tableau de bord projet et du service ;
- les risques et changements ayant un impact potentiel sur le bon déroulement du service ;
- le cas échéant, la stratégie de prise en compte des évolutions sur la période à venir et le planning prévisionnel correspondant.

À titre d'information, le référentiel PDIS de l'ANSSI propose une gouvernance de SOC basée uniquement sur les comités opérationnels et stratégiques avec une périodicité différente.

IV.4. Moyens du SOC

IV.4.1. Moyens humains

Un SOC est une organisation nécessitant des compétences sécurité dont le rôle clé est celui d'analyste. Il est possible de répartir les compétences d'analyste sur plusieurs personnes, mais le SOC nécessite les compétences suivantes :

- Compétences techniques :
  - Expérience en administration des systèmes ;
  - Expérience en administration d'équipements de type NIDS[6] ;
  - Connaissance approfondie des protocoles réseau et expertise dans l'analyse de flux réseau ;
  - Expérience en virtualisation, containérisation, Cloud suivant les choix technologiques.
- Compétences en sécurité :
  - Connaissance des principales techniques d'attaques liées aux scénarios visés ;
  - Connaissances de base en cryptographie et protocoles de sécurité ;
  - Connaissances des produits de sécurisation réseau ;
  - Expérience en interprétation de résultats de scanneurs de vulnérabilités ;
  - Capacité de veille technique sur les alertes de vulnérabilité et l'évolution des cyber menaces.
- Connaissances spécifiques du SI de l'entreprise :
  - Topologie du SI et points d'accès externes ;
  - Topologie applicative et connaissances des flux considérés comme « normaux » ;
  - Populations à risque ;
  - Périodes de charge ;
  - Lacunes opérationnelles et de sécurité du SI.

IV.4.2. Moyens logistiques

La nature de l'activité d'un SOC et le besoin de protéger les informations manipulées incitent à définir dès le démarrage d'un projet SOC les moyens logistiques. Ces moyens sont l'un des

[6] Network Intrusion Detection System

facteurs déterminants de l'efficacité et l'efficience des opérations du SOC. Il s'agit de déterminer :

- La localisation physique des équipes SOC et de son SI propre ;
- Les mesures de sécurité physique des locaux du SOC (accès, secours) ;
- Le matériel dédié au SOC et son réseau cloisonné dédié ;
- L'architecture applicative du SOC, et en particulier un annuaire dédié ;
- Les moyens de communication du SOC avec les exploitants et les échanges avec le processus de gestion des incidents.

Ces moyens doivent intégrer des solutions dégradées en cas de crise.

IV.4.3. Moyens applicatifs

Le SOC doit bénéficier d'une architecture applicative lui permettant

- De générer l'information ;
- De collecter et conserver l'information ;
- De traiter l'information afin d'identifier des évènements actionnables (incidents ou autres) ;
- De communiquer à l'extérieur du SOC :
    - sur les incidents ou autres évènements actionnables ;
    - pour assurer tout autre reporting.
- D'intervenir sur le SI de l'entreprise (si la mission du SOC inclut ceci) ;
- D'assurer son propre fonctionnement.

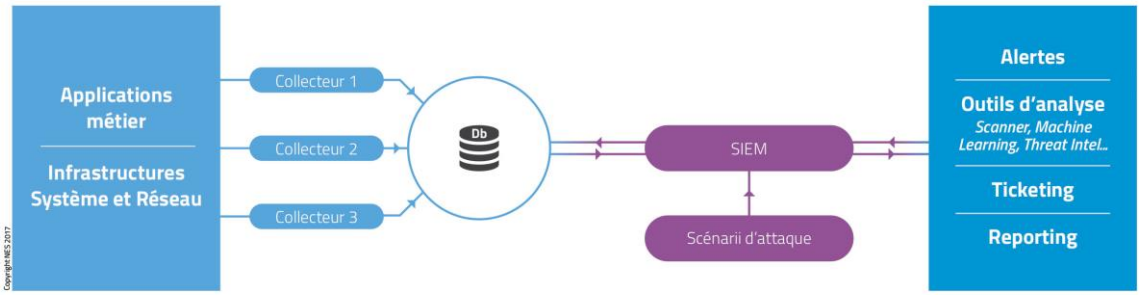


Figure 11 : Schéma de principe de l'architecture SOC

Le SOC a aussi besoin d'interagir avec le reste du SI de l'entreprise : accéder à des bases d'information telles que des annuaires, des bases d'inventaire (CMDB), des bases de vulnérabilités pour enrichir la qualification des évènements de sécurité remontés et/ou coordonner les réactions en cas d'incident.

IV.4.3.a. Génération de l'information

Les traces sur les équipements sont une source première pour la chaine de traitement des informations et des événements de sécurité.

On peut distinguer plusieurs types de sources de traces / évènements :

a. Composants standards du SI

Les composants (équipements, applications) standard du système d'information sont en place indépendamment du SOC, ils ont un rôle fonctionnel ou d'infrastructure - tels les serveurs, routeurs. Ils fournissent des traces sécurité « brutes ».

Pour mettre en place la génération des traces sur les équipements standards, il faut choisir les types d'équipement et les options de verbosité à paramétrer. La démarche consiste à repartir des risques et des scénarios d'attaque que le SOC souhaite pouvoir détecter. Pour aider à réaliser ces choix, les travaux de l'ETSI offrent une taxonomie des scénarios et des indicateurs de détection. Ainsi, à partir des risques, il est possible de sélectionner les équipements contribuant à les détecter et de paramétrer leur verbosité.

b. Composants sécurité du SI

Il s'agit de composants à fonction sécurité qui ne sont pas nécessairement sous la responsabilité du SOC. Traditionnellement, ils sont en place bien avant la création d'un SOC, sont opérés par diverses équipes, et lorsqu'un SOC voit le jour, ne passent pas forcément sous son contrôle. À noter que pour les composants (équipements, applications) les plus avancées, nécessitant une expertise sécurité pointue, il peut être bénéfique de les passer sous la responsabilité du SOC.

Exemples :

- **Anti-malware classique**
- **Anti-malware de type « bac à sable »**
- **EDR (Détection et réponse sur les endpoints)**

  Les EDRs sont une technologie émergeante. Il s'agit d'outils et solutions qui mettent l'accent sur la détection et le blocage d'activités suspectes directement sur les PC et autres équipements présents sur le réseau (serveurs etc.). Elles s'appuient également sur des moteurs d'intelligence artificielle. Les EDR complètent les antivirus classiques.

- **Pare-feu**
- **Scanneurs de vulnérabilités**

  Dans un dispositif globalement « connecté » à un SIEM, les scanneurs permettent d'identifier en amont les vulnérabilités en continu et alimenter le SIEM, d'envisager des plans d'actions préventifs ou des actions palliatives en attendant la correction de failles.

- **Outils de vérification de conformité sécurité**

Pour tous ces composants, il convient de les « connecter » à un SIEM du SOC, afin de l'alimenter en évènements sécurité. Comme pour les composants standards du SI, un travail de détermination du bon paramétrage de la génération des évènements à destination du SOC, est nécessaire.

Beaucoup de ces composants incluent des fonctions de traitement des évènements sécurité détectés et d'intervention sur le SI intégrés, telles que les solutions anti-malware. Nous n'abordons pas cet aspect dans ce document.

c. Composants spécialisés à destination d'un SOC

Ce sont des applications / équipements spécialisés dans la génération des évènements sécurité. Leur choix et déploiement conditionnent tout le reste. Ces moyens effectuent un traitement hautement spécialisé des données, dont le SIEM serait incapable, et génèrent des évènements sécurité adaptés à la corrélation dans le SIEM. Si pour les équipements standard, le SOC n'est qu'un client de la génération de traces, pour les moyens spécialisés, le SOC doit être le moteur, demandeur de leur déploiement, leur propriétaire dans la plupart des cas. Il s'agit de moyens de type :

- **Détection / prévention d'intrusion hôte / réseau**

  En mode prévention, ces sondes effectuent une intervention sur le SI, nous n'abordons pas cet aspect dans ce document.

- **Machine Learning**

  Le machine learning est un concept qui, appliqué au SOC, permet de détecter, trier, qualifier plus rapidement et avec plus de fiabilité qu'un humain les alertes, incidents avérés et les faux positifs.

  L'exemple de machine learning le plus connu associé à la sécurité est l'antispam.

Les algorithmes ne sont pas fondamentalement nouveaux. Par exemple l'algorithme bayésien utilisé par l'antispam. Basés sur des estimateurs, un set de données valides et un set de données invalides, l'algorithme établit un arbre de décision pour déterminer la validité d'une nouvelle donnée basée sur l'historique et la probabilité associée à cette décision.

Cette méthode parait donc prometteuse pour remplacer certaines étapes liées à une prise de décision.

Cependant l'efficacité de cette méthode dépend du jeu de données fourni en amont qui doit être le plus représentatif possible. En effet il est constitué de cas passés et non de cas futurs.

Concernant les estimateurs, ils sont efficaces dans le cadre de l'antispam car ils s'appuient sur une norme (RFC) qui définit tous les cas possibles et les estimateurs sont calculés par un équipement ayant accès à toutes les données nécessaires. Dans un système ouvert, on pourra s'interroger sur l'exhaustivité des estimateurs (existe-il un indicateur actuel permettant de détecter une attaque future ?).

En 2016 il existe plusieurs produits offrant de telles capacités à travers le terme « user behavior analytics ». On notera à l'heure actuelle que ces algorithmes sont définis par les constructeurs et ne sont pas partagés (car c'est la valeur de l'outil) et que les produits sont concentrés sur des activités particulières de l'utilisateur (réseau uniquement, active directory uniquement, …) et non analysés de bout en bout.

- **Outils d'analyse comportementale (UBA)**

  Il s'agit de solutions distinctes interopérables avec les SIEM actuels ou déjà intégrées dans les SIEM dits 2.0 qui permettent des analyses encore plus fines afin de détecter des APT et autres malwares sophistiqués. Ils s'appuient sur des techniques de « Machine learning » qui consistent à « apprendre » les usages du SI en régime dit « normal » puis d'alerter lorsque des écarts sont détectés. In fine, cette approche contribue également à élaborer des « kill chain » valides.

- **Analyse de trafic DNS**

  Il s'agit de solutions analytiques permettant d'identifier des systèmes infectés en se basant sur le trafic réseau DNS. L'absence d'intervention sur les serveurs DNS eux-mêmes est un grand plus.

IV.4.3.b. Collecte et conservation de l'information

a. Collecte et conservation des traces / évènements

La gestion des traces / évènements constitue un service important pour la détection d'incident de sécurité et la réalisation d'enquêtes. La première pierre à l'édifice consiste à mettre en place une infrastructure pour collecter et conserver les traces sous le contrôle du SOC.

La centralisation de l'information est nécessaire pour corréler des évènements qui ont lieu sur des équipements différents et pour pouvoir détecter des attaques complexes.

Elle pose plusieurs problématiques importantes :

- La collecte sur l'équipement peut être réalisée par un agent propriétaire de l'éditeur, installé sur l'équipement ou sans agent par transmission des données via des modalités standards (FTP, Syslog, SNMP, NTP). La première a l'avantage de pouvoir offrir des services de filtrage, de compression et de chiffrement natif, mais en étant intrusive et limitée à l'offre de l'éditeur. L'autre a l'avantage d'être plus ouverte mais plus difficile à maintenir.

Dans certains cas d'usage (par exemple lors d'opérations de maintenance), il faut permettre la désactivation de la fonction de collecte pour un type de traces données afin d'éviter la pollution de la base de conservation.

- L'architecture de collecte peut être centralisée ou distribuée. La collecte en un point central est bien évidement la solution la plus pratique mais elle peut se heurter à des contraintes de performance, d'architecture réseau voir de besoin hétérogène de sécurité des informations.
- La technologie utilisée pour la base de traces est importante et notamment ses qualités de performance, de secours et de scalabilité. En cas de sinistre, de panne ou de dysfonctionnement impactant la base de conservation des traces, accepte-t-on de perdre les données brutes ? Une solution de secours sur un autre site doit prendre en compte la taille des canaux intersites pour absorber la charge. Une solution de secours permettra d'assurer la continuité de la collecte en cas de panne mais elle ne suffira pas à protéger la base contre une erreur se propageant sur les 2 systèmes et détruisant tout ou partie des données. Une solution de sauvegarde peut être envisagée pour éviter de perdre l'ensemble des données. Cette solution devra permettre le traitement sur des volumes important de données, tout en laissant une base ouverte.
- Enfin la définition de la qualité de la conservation des preuves et des traces remontées notamment si ces dernières doivent pouvoir être utilisées en justice. Des bonnes pratiques de mise en œuvre dans le stockage des traces, décrites dans la section 3.3 et l'annexe C de la note technique de l'ANSSI DAT-NT-012/ANSSI/SDE intitulée « Recommandations de sécurité pour la mise en œuvre d'un système de journalisation. »

b. Collecte et gestion de l'information sur le contexte

- **Gestion de la connaissance du contexte interne**

Un des enjeux majeurs d'un SOC est de pouvoir correctement qualifier les incidents. Cette qualification nécessite un niveau minimal de connaissance du contexte du SI surveillé. Cette connaissance passe par une gestion propre de la connaissance du SOC et par l'usage de la base de données de gestion de configuration (CMDB) du SI surveillé si elle existe et si les données qu'elle contient sont pertinentes et suffisantes.

La CMDB contient des informations sur les composants du système d'information (appelés *configuration items* ou CI) et des détails sur les relations importantes entre eux.

Ainsi, un incident impactant un CI peut être qualifié de mineur si la CMDB indique que le CI est en cours de dé-commissionnement ou au contraire de critique si le CI est un des composants majeurs d'une application critique.

Cf. document du CLUSIF « Gestion des vulnérabilités informatiques / Vers une meilleure gestion des risques opérationnels – TOME 2 – Chapitre IV.3.2 ».

« […] Un premier enrichissement de cet inventaire consiste à décrire les interdépendances entre les actifs identifiés et les applications métier avec des outils de type CMDB (Configuration Management DataBase). Chaque actif (service applicatif Web, base de données, etc.) doit ainsi avoir son propriétaire, typiquement une fonction Métier en affectant toutes les machines et services inventoriés à des opérationnels, qu'il s'agisse d'actif servant une application métier ou du poste de travail d'un collaborateur de cette fonction Métier. »

La base de connaissance (Knowledge Base ou KB) est un outil essentiel pour les analystes de niveau 1 qui, face à un incident renseigné dans cette base, seront en mesure de réagir sans faire obligatoirement intervenir les analystes niveau 2.

- **Gestion de la connaissance du contexte externe**

Afin de tirer le meilleur parti de l'information disponible en interne, il est indispensable de la mettre en rapport avec le contexte des menaces externes. Cela permet d'identifier plus rapidement et plus efficacement les attaques, et orchestrer la réponse. Il existe aujourd'hui sur le marché des fournisseurs spécialisés de « threat intelligence », et l'approche standard est d'intégrer une sélection des fils correspondants d'informations dans le SOC.

IV.4.3.c. Traitement de l'information

Nous parlons ici d'un traitement propre au SOC. De nombreux composants / applications sécurité incluent un traitement intégré, telles que les solutions anti-malware - nous n'abordons pas ces aspects ici.

a. Corrélation automatisée - SIEM

Le SIEM est l'outil principal du SOC (mais pas le seul). Le SIEM met à disposition des tableaux de bord permettant à partir de l'analyse des traces / évènements et des informations sur le contexte, de détecter et de qualifier certains incidents de sécurité. Il est composé de nombreuses fonctionnalités dont :

- Normalisation des traces : une fois les traces stockées, des parseurs doivent réaliser une analyse syntaxique des différents messages afin d'extraire les informations qu'ils contiennent et les présenter sous un format plus intelligible pour l'utilisateur et le moteur de corrélation.
- Enrichissement : suite à l'étape de normalisation, les données extraites des journaux peuvent être enrichies avec des données externes afin d'améliorer la compréhension du contexte dans lequel apparait un évènement et d'accroitre la capacité de détection d'évènements anormaux ainsi que d'améliorer le processus de qualification. Se pose alors le problème pour les outils des capacités d'interconnexion avec des bases de

données externes afin de recueillir des informations sur la nature des applications, des utilisateurs, ou de leurs activités. Par exemple : le port présent dans une trace brute peut être complété par le nom de l'application qui l'utilise ; une adresse IP peut être complétée par le nom de l'ordinateur ou de l'utilisateur associé ; etc.

- La détection des incidents en pseudo temps réel (sur le flux d'évènements) ou en post mortem (des règles de corrélation visant à détecter des évènements liés les uns aux autres sur une durée plus ou moins longue). Des règles, filtres et des seuils sont définis pour détecter l'apparition d'événements spécifiques et déclencher des alertes automatiques. Pour permettre le partage d'expérience et le contrôle du dispositif, l'outillage doit permettre d'exporter de manière claire la liste des paramétrages utilisés.

De plus, suite à la découverte d'une attaque, il doit être possible de retracer son déroulement via une analyse post-incident (forensics). Pour cela, la solution doit permettre de rejouer d'anciens évènements pour mener des investigations.

Le suivi des incidents doit permettre de marquer les fausses alertes afin d'éviter une pollution de la supervision.

- La gestion des incidents peut être dissociée de l'outillage d'analyse mais elle doit permettre notamment de lier une alerte à un ticket de traitement d'incident et son statut.
- Les interfaces : l'outil doit permettre de naviguer de manière ergonomique par le biais d'interfaces graphiques pour accéder aux différentes fonctions de recherche, de consultation ou d'alerte. Une fonction de recherche doit permettre de réaliser des recherches avancées sur les traces en utilisant un ou plusieurs critères.
- L'outil doit permettre de définir des rapports et des tableaux de bord selon les profils des équipes destinatrices et leur périmètre de responsabilité. L'expérience montre que le mieux est de permettre à chaque destinataire de définir ses tableaux de bord dans l'outil.
- Le reporting : L'objectif est de fournir des statistiques diverses sur l'infrastructure, les actifs qui la composent, les évènements et les incidents détectés. Il est souhaitable que l'outil puisse fournir des interfaces vers des outils externes de présentation des données.

b. Analyse avancée de données

Le SIEM est typiquement chargé d'une analyse et corrélation automatique des logs sur un relatif court terme. Afin de constituer une connaissance nouvelle, pouvoir prédire de futures attaques et définir de nouvelles règles de corrélation et d'alerte automatique, il est utile d'appliquer de l'intelligence humaine aux logs divers et variés, collectés sur une longue durée. Il s'agit de faire appel à des outils d'analyse avancées, permettant d'effectuer des analyses ad-hoc et sur du « big data ». Il est à noter qu'une certaine maturité du SOC et des compétences pointues sont nécessaires pour tirer parti de ces outils.

c. Suivi des alertes / incidents

Les alertes / incidents nécessitent un suivi dans le temps, jusqu'à la fin de leur traitement par le SOC : mettre à jour et consulter leur statut et contenu, ceci par de nombreuses personnes. Des outils adaptés sont nécessaires. En fonction du périmètre de l'intervention du SOC dans la gestion des incidents, le choix se fera entre des outils intégrés au SIEM, des plateformes spécialisées **SIRP (Security Incident Response Platform)** ou d'autres outils.

IV.4.3.d. Communication

La communication du SOC à l'extérieur, sur les incidents, sur d'autres évènements actionnables, et en général, s'appuiera en grande partie sur les capacités natives de tableaux de bord et de reporting du SIEM et des autres composants mis en place dans le SOC pour le traitement de l'information, d'où l'importance de ce critère dans le choix des outils.

IV.4.3.e. Intervention sur le SI de l'entreprise

Nous parlons ici d'une intervention propre au SOC, au-delà des actions automatiques intégrées dans les solutions de sécurité telles que l'anti-malware ou l'IPS.

a. Investigation et recherche active de menaces

L'investigation d'une alerte ou d'un incident est facilitée par des moyens spécialisés d'analyse de systèmes (i.e. visibilité sur les postes de travail) et de réseau (i.e. « sniffers ») et qui ne sont pas forcément intégrés dans la chaine automatisée de collecte et traitement de traces / évènements. Ces moyens permettent d'approfondir à la demande la connaissance de la situation dans le système d'information, dans le cadre d'investigation sur une alerte / incident, ou bien dans le cadre de recherche active de menaces.

b. Réponse automatisée

Traditionnellement, une fois l'alerte qualifiée et la réalité d'un incident établie, tout changement dans le système d'information, toute circonscription des menaces et remédiation se faisaient d'une façon manuelle. Il est aujourd'hui possible d'aller au-delà, et d'automatiser cette réponse, du moins partiellement – pour des attaques bien comprises et dans des limites agrées au sein de l'entreprise. Ceci nécessite la mise en place de moyens d'ordonnancement liés aux outils de détection (SIEM), ainsi que de moyens de circonscription de menaces ; les moyens spécialisés de ce type doivent être sous la responsabilité du SOC ; les composants standards du système d'information seront actionnés si possible également (i.e. pare-feu). L'automatisation des réponses libère les ressources humaines du SOC pour des tâches à plus forte valeur ajoutée.

IV.4.3.f. Support du fonctionnement du SOC

Le SOC se doit de gérer sa base de connaissances et stocker les documents qu'il produit ou qu'il a reçu (documents d'architecture par exemple). Un cyberwiki interne est tout à fait adapté à cet usage.

Enfin le SOC doit sécuriser sa propre infrastructure, ce qui implique en général une gestion propre de ses identifiants dans un annuaire dédié.

V. Mise en place d'un SOC

Dans ce chapitre, nous présenterons les différentes phases du déploiement d'un SOC suivant le schéma suivant :

- Définir son projet ;
- Le vendre à l'entreprise ;
- Déterminer les besoins : budget, équipe, outils, … ;
- Build : Mise en place du projet ;
- Run : Opérer le soc ;
- Premier bilan, retour d'expérience ;
- Comment poursuivre le déploiement d'un SOC.

Et pour chaque phase, nous essaierons de mettre en avant des recommandations utiles.

V.1. Définir son projet SOC

Le projet de mise en place d'un SOC apparait dans l'entreprise suite à une réflexion concernant la stratégie globale de l'entreprise, la place de la sécurité des systèmes d'information dans cette stratégie, les évolutions tant dans l'environnement externe de l'entreprise qu'en interne.

Le besoin de mise en place d'un SOC peut donc être le fruit de différentes préoccupations. Par exemple, de nouvelles contraintes légales ou réglementaires, ou le nombre d'incidents de sécurité en hausse mais de plus en plus difficiles à localiser, ou encore une évolution des services de l'entreprise vers une externalisation de plus en plus grande.

Cette étape est portée par le promoteur interne du SOC.

Les principaux sujets à traiter à ce stade sont :

1. **Les objectifs du projet**

   Les objectifs de la mise en place d'un SOC sont avant tout liés à la stratégie de l'entreprise. Ils doivent pouvoir être appréhendés et approuvés par toutes les parties prenantes, y compris celles qui ne sont pas du tout impliquées dans la sécurité.

   Le chapitre 2 du présent document Objectifs d'un SOC présente les principales motivations pour la mise en place d'un SOC.

   Le promoteur du SOC devra faire la synthèse entre la stratégie de l'entreprise définie par son COMEX (comité exécutif) et les bénéfices apportés par le SOC.

   En effet, la mission essentielle du SOC est la gestion des incidents de sécurité : détection, réaction et prévention. En quoi cette mission est-elle vitale pour l'entreprise ?

   Les arguments qui peuvent être mis en avant sont :

   - La conformité réglementaire (exemple des OIV en France) ;

- La transformation numérique de l'entreprise et son usage toujours plus important de services accessibles via Internet et donc l'exposition de données sensibles à l'extérieur ou le risque d'interruption des services de l'entreprise ;
- Le SOC est une organisation plus efficace pour la lutte contre les incidents liés à la cyber sécurité.

 *Le promoteur se doit de convaincre toutes les parties prenantes. Qui, aujourd'hui n'est pas sensibilisé par la presse grand public aux risques que font courir aux entreprises les attaques informatiques ? Il peut donc s'appuyer sur de nombreux exemples afin de prouver la nécessité d'un tel service, ceci d'autant plus si l'entreprise est particulièrement exposée aux risques d'internet.*

2. La couverture du projet

La couverture du projet comporte deux axes : d'une part, les systèmes d'information à surveiller en priorité, d'autre part la liste des services surveillés depuis l'infrastructure informatique jusqu'aux applications.

Le SOC demande une quantité de travail importante pour produire des résultats et il est nécessaire de limiter sa couverture dans un premier temps afin d'obtenir des résultats rapides et concluants. Se fixer des objectifs trop importants amènerait à avoir des résultats à une échéance trop longue qui décrédibiliserait le projet.

D'autre part, le choix des systèmes d'information doit être pertinent. Faire surveiller des SI peu utilisés et sans usage critique ne permet pas de mobiliser les intervenants. Il faut donc sélectionner les SI importants de l'entreprise pour lesquels la mise en place de ce type de services est véritablement justifiée.

Enfin, si on associe à l'image du SOC la cyber sécurité, il est nécessaire de commencer par l'infrastructure informatique : équipement réseau, pare-feu, sondes, systèmes d'exploitation des serveurs, postes de travail,… C'est là que l'on peut détecter les principaux vecteurs d'attaques : rootkits, élévations de privilèges, modification des politiques de sécurité des équipements, …

La stratégie de couverture par analyses des applications implique un travail conjoint avec les métiers, les éléments à analyser étant spécifiques à chaque type d'activité.

 *Le promoteur doit choisir une couverture du projet à la fois réaliste au niveau des délais et significative pour les parties prenantes.*

3. Les contraintes à prendre en compte

Il convient de lister les contraintes inhérentes à l'organisation qui peuvent avoir un impact direct sur le projet :

- S'il s'agit d'un OIV, il devra nécessairement externaliser une partie de son SOC à moins qu'il ne se donne la possibilité de passer la certification PDIS/PRIS mais il faut noter que celle-ci est réservée aux entreprises qui ont déjà une expérience notable de ce type d'activité ;
- Contexte international ;
- Contexte réglementaire : par exemple loi informatique et libertés ;
- Contraintes sur les architectures (infrastructures) qui vont impacter les choix d'outils. Accepte-t-on que les outils du SOC soient gérés par les équipes informatiques ?
- Contraintes sur les ressources humaines. Un SOC, par la nature de son fonctionnement (plage de couvertures par exemple) et les services qui le constituent (SLA par exemple) implique une certaine mobilisation en termes d'ETP. Est-on capable de la mobiliser en interne ou devra-t-on faire appel au recrutement ou à une externalisation partielle ? En cas de recrutement interne, combien de temps cela prendra-t-il ?
- Contrainte budgétaire. Quel est le budget mobilisable par l'organisation pour la mise en œuvre de cette solution ? Voir aussi le ratio CAPEX/OPEX acceptable par l'entreprise.

 *Lister les contraintes et évaluer leurs impacts sur le projet amène à faire des choix concernant l'organisation du SOC et son éventuelle externalisation.*

V.2. Vendre le projet SOC à son entreprise

À la suite de la première étape, le promoteur interne du SOC a pu mettre au point un document qu'il va pouvoir présenter à toutes les entités concernées de l'entreprise.

Nous lui conseillons de commencer par les entités métiers afin qu'elles lui permettent de corriger et d'améliorer sa présentation.

Une présentation au COMEX est également indispensable. Il appartiendra à celui-ci de donner un avis positif ou négatif sur la mise en œuvre de ce projet. Le COMEX devra, le cas échéant, donner au promoteur du projet les moyens requis à sa mise en œuvre.

Ce passage devant le COMEX devra permettre de déterminer :

- Les bénéfices à attendre du SOC, les éventuelles obligations (OIV) ;
- Le périmètre du projet ;
- L'ensemble des ressources qui devront lui être affectées ;
- L'organisation proposée ;
- Les délais de mise en place et les échéances pour les premiers résultats ;

- L'enveloppe budgétaire suivant les trois phases : mise en place, exploitation et réponses à incident.

Il va de soi que le processus de décision par le COMEX est progressif et qu'il va falloir :

- Sensibiliser, faire preuve de pédagogie et obtenir l'adhésion au projet ;
- Libérer la communication autour des incidents de sécurité en utilisant les moyens de communication internes. Bien souvent, les parties prenantes ont l'impression qu'il n'y a jamais d'incident de sécurité dans l'entreprise car ils n'en entendent jamais parler ;
- Avant de lancer le SOC, il faut peut-être commencer par matérialiser le concept de cyber-sécurité au travers d'indicateurs liés à l'activité de l'entreprise. Les revues qualité peuvent présenter régulièrement un rapport sur ces incidents et leurs conséquences ;
- Le promoteur se doit d'étudier les solutions disponibles sur le marché ou bien explorer ce que des sociétés positionnées sur des secteurs d'activité similaire ont pu mettre en place.

L'accord du COMEX de l'entreprise est indispensable pour lancer la mise en place d'un SOC. Pour l'obtenir, il est nécessaire d'effectuer tout un travail préparatoire pour sensibiliser l'entreprise aux incidents de sécurité et à leurs conséquences. Enfin, il est nécessaire de fournir à ce COMEX tous les éléments dont il a besoin pour prendre sa décision. Les éléments budgétaires à court et moyen terme peuvent être décisifs.

V.3. Lancement du projet et détermination des besoins

La première étape du projet est de désigner le pilote du SOC qui peut être la même personne que le promoteur (mais cela n'est pas systématique). Celui-ci va s'entourer des premiers collaborateurs qui vont permettre de déterminer l'ensemble des besoins et de les obtenir.

Au nombre de ces besoins, citons :

- L'architecture du SOC ;
- Les outils ;
- Les ressources humaines ;
- Les moyens de pilotage : comitologie, … ;
- Les SLA, indicateurs et reporting attendus ;
- Le fonctionnement (24x7 ou pas) ;
- Le budget ;
- Les moyens internes ou partiellement ou totalement externalisés.

Il convient de faire valider le document final par les entités métiers consultées lors de la première étape.

À l'issue de cette phase, le promoteur et le pilote du SOC disposent d'un document complet à destination du COMEX avec une visibilité budgétaire sur au moins trois ans et un ROI permettant de faire un lancement complet de projet.

A ce stade et même si on ne souhaite pas externaliser le SOC, la bonne démarche peut être de rédiger un cahier des charges qui recense les exigences concernant tous les points cités ci-dessus. Ceci permet de disposer d'un document de synthèse qui pourra être suivi tout au long du projet et de ne pas oublier en cours de route des points critiques.

Nous allons revenir sur chacun de ces points :

V.3.1. Architecture du SOC

Le chapitre précédent L'architecture applicative a présenté un schéma de principe de l'architecture d'un SOC dont il est possible de s'inspirer.

Le Chef de projet technique, responsable de la mise en place du projet devra définir cette architecture.

Pour cela, il devra recenser le catalogue de service suivant le périmètre défini dans la phase précédente. Il devra ensuite en déduire les SI spécifiques à mettre en place et le socle sur lequel ces outils devront être installés.

Le socle de l'architecture devra prendre en compte :

- Les contraintes ou obligations internes à l'entreprise. En effet, l'entreprise peut avoir défini des architectures de référence et avoir qualifié des plates-formes qui doivent être utilisées pour monter l'architecture ;
- Les adhérences avec les politiques de sécurité. Par exemple, il peut être demandé au SOC d'être complétement cloisonné des SI de l'entreprise et d'être exploité par une équipe distincte. Il peut aussi être demandé que la collecte des logs se fasse uniquement en mode push et d'éviter le mode pull où les collecteurs vont interagir avec les serveurs de l'entreprise ;
- Et éventuellement les contraintes réglementaires auxquelles sont soumis notamment les OIV. Le document PDIS de l'ANSSI donne un certain nombre d'exigences sur le cloisonnement du SOC et sur les problèmes de surveillance et d'administration de celui-ci.

Dernière étape, le Chef de Projet technique doit faire valider cette architecture par toutes les parties prenantes : l'équipe SOC, la DSI, le RSSI.

À moins que le SOC ne soit complétement externalisé, l'architecture du SOC doit respecter les standards définis par l'entreprise tout en apportant toute l'offre de service demandée dans la phase préalable.

V.3.2. Les outils du SOC

Le chapitre précédent Moyens du SOC présente, entre autres, les moyens applicatifs du SOC, dont la mise en place se concrétise au travers des « outils ».

Dans le présent chapitre, nous souhaitons attirer l'attention sur l'importance stratégique de certains outils pour le SOC et les problématiques qu'ils peuvent poser.

Citons les sondes d'intrusion. Le choix des sondes est important et doit répondre aux besoins de l'entreprise par rapport à ses métiers. La prise en main des sondes est aussi une opération délicate et qui peut solliciter des ressources pour un temps assez long. Cet outil nécessite la compétence de personnel qualifié aussi bien pour leur configuration que pour leur utilisation si on ne veut pas se retrouver submergé par un flot d'alertes inexploitables.

Le choix du SIEM et sa bonne maîtrise est aussi déterminant dans le succès du SOC. Les SIEM sont des outils complexes qui demandent aussi du personnel formé et compétent aussi bien pour les configurer que pour les mettre à jour. Il sera généralement nécessaire d'avoir une équipe dédiée sur le SIEM qui en maîtrisera tous les aspects et qui sera en mesure de configurer les alertes conformément aux demandes du client.

Les « outils » du SOC, tel le SIEM, nécessitent de vraies compétences en la matière pour en tirer parti. Par exemple, dans de nombreux cas, suite au premier échec du projet SOC, le SIEM a été jugé « mauvais » et remplacé par un autre – mais avec le même type d'échec à l'arrivée – car le travail de réflexion, de conception fonctionnelle a été négligé.

Dans la phase initiale du projet, le choix de ces outils demandera la rédaction d'un cahier des charges dédié et l'analyse des solutions du marché. La durée de cette phase de sélection est à prendre en compte lors de la définition du planning global du projet.

Par la suite, il sera nécessaire de s'assurer de la bonne formation et compétence des équipes sur ces technologies. Et cette réflexion peut amener à externaliser certains outils. C'est le point de vue de l'ANSSI concernant les SOC qui s'assure par la qualification PDIS de la maîtrise des entreprises qualifiées sur les outils de détection d'incident.

Certains outils doivent être sélectionnés avec soin afin de répondre aux besoins de détection d'incidents. Ils demandent aussi d'être exploités par des équipes correctement formées et compétentes.

V.3.3. Les ressources humaines du SOC

Les différents rôles du SOC ont été décrits dans le chapitre Rôles et responsabilités au sein du SOC.

Les compétences nécessaires aux analystes du SOC ont été décrites dans le chapitre Moyens humains.

Il convient de s'assurer de la mise en place d'une organisation cohérente autour du SOC.

Le pilote du SOC devra donc définir cette organisation et définir les ressources disponibles dans l'entreprise pour remplir certains rôles et celles qui devront être recrutées. Il devra aussi préciser les rôles SOC qui occupent un plein temps et ceux qui ne sont requis qu'en partie du temps.

Par exemple, les analystes de niveau 1 sont dédiés au SOC. Alors que les analystes niveau 2 n'interviennent qu'en cas de problème particulier.

Idem pour les rôles opérationnels. Des ingénieurs réseaux qui s'occupent des pare-feu peuvent monter en compétence sur des sondes IDS. Le SIEM de par ses particularités risque de monopoliser à plein temps un spécialiste.

La mise en place de cette nouvelle organisation requière l'aide des ressources humaines et son cheminement restera du ressort de chaque entreprise.

 *Le pilote du SOC doit mettre en place l'organisation humaine et les bonnes ressources. Il doit s'assurer de la disponibilité, des compétences et de la formation continue de ces ressources.*

V.3.4. La gouvernance

La comitologie possible d'un SOC a été décrite au chapitre précédent Structures de pilotage.

Les comités doivent être mis en place et démarrer dès le lancement du projet.

V.3.5. Les SLA, indicateurs et reporting

A ce stade, il est important de mettre en place l'outillage qui va permettre de surveiller les SLA, de produire les indicateurs et les différents rapports sur l'activité du SOC.

Parmi tout ceci, il faut distinguer différents types de rapports :

- Les SLA, indicateurs qui permettent de vérifier la mise en place du SOC et son efficacité en exploitation ;
- Les indicateurs et rapports concernant le nombre d'événements analysés, le nombre d'alertes et d'incidents détectés, le taux de faux positifs, … ;
- Le suivi financier de l'activité du SOC.

V.3.6. Le fonctionnement (24x7 ?)

Il est nécessaire de déterminer si le fonctionnement du SOC en 24x7 est requis. Il faut distinguer la surveillance des SI du système d'alertes.

Il est à peu près évident que la collecte des logs et la détection d'incidents doivent fonctionner en 24x7. En revanche, la question de l'utilité d'un service d'alerte en 24x7 peut se poser si les utilisateurs ne sont présents que pendant les heures ouvrées.

Autre argument, dans la plupart des SI, les alertes sont générées par des utilisateurs durant les heures de travail comme les ouvertures de mails ou la navigation web.

Il faut exclure les entreprises internationales avec un SOC mutualisé pour lesquelles cette notion diffère.

Reste à chaque entreprise le soin de déterminer suivant la nature de ses activités si elle a besoin d'un système d'alerte en 24x7.

V.3.7. Le budget

Le budget d'un SOC est relativement complexe et se répartit selon les axes suivants :

- Frais de personnel : que ce soit des ressources internes ou des recrutements, il convient de prévoir l'ensemble des personnes nécessaires au bon fonctionnement du SOC. Certains profils rares sur le marché peuvent avoir des prétentions salariales importantes ;
- Achats de matériels informatiques et licences des outils : ils font partie des investissements et certaines entreprises préfèrent répartir le budget plus en OPEX qu'en CAPEX ce qui amènerait à choisir une solution où l'infrastructure informatique est en mode cloud ;
- Les frais de maintenance récurrents et inhérents tant à l'achat de matériels que de logiciels sont à projeter sur plusieurs années ;
- Les frais d'abonnement éventuels à des services comme les CSIRT par exemple, sont à inclure dans le projet.

Externaliser tout ou partie du SOC provoque une restructuration de ces postes budgétaires avec des modèles CAPEX/OPEX différents suivant la répartition des services.

Nous allons par la suite parler du déploiement du projet et reviendront sur les budgets inhérents à chaque phase.

V.3.8. L'externalisation totale ou partielle du SOC

L'externalisation du SOC est une question fréquente qui apparaît lors du cadrage des projets SOC. Il n'y a bien entendu pas de réponse unique, les contraintes et attentes étant fort différentes d'un contexte à l'autre. Certaines organisations sont soumises à des exigences limitant les possibilités d'externalisation (voir Annexe 1b).

La majorité des principes exposés dans le présent document s'applique que le SOC soit interne ou externe à l'organisation.

L'externalisation de tout ou partie du SOC est à envisager, aux différentes phases du déploiement du SOC, pour des raisons très variées :

- Besoin d'accompagnement pour monter en maturité ;
- Manque de ressources ou d'expertise ;
- Besoin de service en 24x7 ;
- Réduction des coûts liés à la mutualisation ;
- Bénéficier d'un label PDIS pour une prestation qualifiée.

Les deux options ont leurs avantages et inconvénients. La discussion approfondie est reportée en Annexe : Externalisation du SOC.

V.4. Étape BUILD : mise en place du projet

Considérant le schéma qui suit, nous avons réalisé, à ce stade, la conception de l'infrastructure des services.

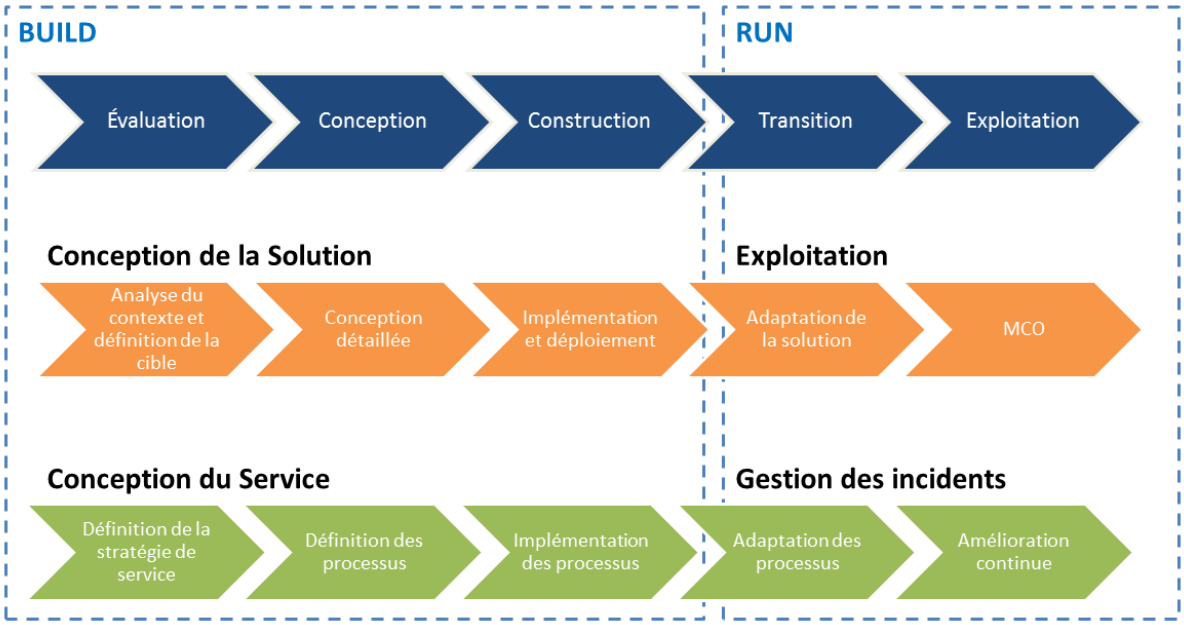


Figure 12 : Vue générale de la mise en place d'un SOC

Il n'y a pas une et une seule étape BUILD dans le déploiement d'un SOC. En effet, le périmètre du SOC peut être par la suite étendu, des nouveaux outils de sécurité peuvent être intégrés, il est possible d'étendre l'utilisation du SOC à la surveillance des applications après avoir traité de l'infrastructure. Chacune de ces extensions donnera lieu à une nouvelle étape de type BUILD.

V.4.1. Démarche pour la mise en place des moyens techniques

Le déploiement des moyens techniques du SOC tels que définis précédemment se déroule conformément au déploiement de tout projet informatique classique.

Notons qu'il ne faudra pas oublier les outils de supervision qui devront permettre de déterminer si les services techniques du SOC sont opérationnels et intègres à 100 %. Par exemple, il est important de savoir si les logs sont bien collectés et analysés chaque jour. Si certains logs ne sont pas collectés correctement, cela fausse les résultats du SOC.

Le déploiement des outils techniques est préalable à la mise en place des services de surveillance.

V.4.2. Démarche pour la mise en place de la surveillance des SI

L'équipe SOC est en place. L'architecture est déployée. Les ressources sont mobilisées et formées.

Il est temps de se focaliser sur les incidents de sécurité.

Pour être en mesure de mettre en place une détection pertinente des incidents de sécurité, il va falloir passer par les étapes suivantes :

- Analyser les risques des SI à surveiller ;
- Déterminer les alertes qui vont permettre de vérifier la couverture des risques ;
- Répertorier les équipements composant les SI à surveiller. Déterminer ceux qui vont produire des logs pertinents et inclus dans le périmètre choisi (par exemple, les applications peuvent être exclues du périmètre dans un premier temps). Se livrer à une première lecture des journaux d'événements afin de voir si les événements pertinents sont bien présents ;
- Revoir éventuellement la configuration des SI afin d'ajuster les logs ;
- Paramétrer les outils afin de délivrer les alertes pertinentes ;
- Puis tester, recetter et mettre en service.

V.4.2.a. L'analyse de risques

L'analyse de risques des SI qui font partie du périmètre du SOC existe déjà probablement et c'est justement parce qu'elle existe que l'on a décidé de commencer par ces SI. En tout état de cause, si elle n'existe pas, il est urgent de la faire.

Les méthodes d'analyse de risques ne sont pas l'objet du présent document et vous trouverez sur le site du Clusif, une documentation riche sur le sujet.

Il est à noter que les risques à retenir dans le cadre de ce document sont ceux qui sont pertinents dans le cadre de la mise en place d'un SOC. Il est évident que les risques dûs à l'environnement, par exemple, sont exclus de ce périmètre.

Les risques pertinents sont par exemple :

- Risque de pénétration sur un système sensible ;
- Risque d'utilisation hors contexte professionnel de ressources critiques ou sensibles ;
- Risque d'exfiltrations d'informations sensibles, confidentielles ou secrètes ;
- Risque de substitution d'identité (sur les différentes couches, depuis l'adresse IP jusqu'aux utilisateurs de l'application) ;
- Risque d'infiltration de code malveillant ;
- Risque de piégeage des utilisateurs ;
- Risque d'outrepasser le « droit d'en connaître ».

Cette liste n'est pas exhaustive.

V.4.2.b. Détermination des alertes

La détermination des alertes à mettre en place afin de détecter des incidents de sécurité en relation avec les risques cités ci-dessus reste du métier des experts en cyber sécurité qui doivent combiner les possibilités de plusieurs outils : sondes, SIEM, etc.

Il n'est pas possible de décrire cette analyse dans le présent document. À ce stade, nous pouvons citer des alertes qui peuvent être mise en place :

- Exfiltration de données sur les pare-feu ;
- Connexion non autorisée sur une passerelle réseau, sur un serveur, sur une base de données, … ;
- Virus détecté (non supprimé par l'antivirus) ;
- Suppression non autorisée d'un journal d'audit ;
- Elévation de privilèges.

Cette liste n'est pas exhaustive.

Les règles d'alerte représentent une modélisation des attaques et donc étant une modélisation, elle fait abstraction du comportement du système d'information. Il est donc nécessaire d'observer les règles afin de détecter les anomalies du système d'information (on ne parle pas d'attaque). Par exemple, une règle validant l'usage d'un compte traçant les adresses ip pourra être mise en défaut si un poste de travail, en mobilité, change d'ip à chaque nouvelle connexion filaire.

Certains risques peuvent être traités a priori (attaques déjà connues) ou a posteriori (attaques inconnues ou non détectables).

Les attaques connues peuvent faire l'objet d'une règle, par exemple pour éviter la fuite de données nocturnes, une règle sur la quantité de données envoyées de 21h à 6h doit être mise en place. Dans le cas d'un malware, on pourra penser à une règle IDS/IPS. Pour éviter des connexions vers des sites malveillants, on pourra définir une règle, après souscription à un service de catégorisation d'url, envoyant une alerte sur un trop grand nombre de connexion vers ce type de site.

Pour les attaques difficilement détectables (par exemple les fameux APT), le traitement du risque peut être réalisé via une vérification lors de la publication d'indice de compromission.

Le comité de gouvernance du SOC doit s'assurer que les alertes mises en place couvrent bien les risques des différents SI.

Notons que cette liste d'alertes fera l'objet d'une surveillance approfondie lors des comités projets et devra être mise à jour régulièrement.

V.4.2.c. Mise à niveau des SI surveillés

Concernant les SI inclus dans le périmètre de surveillance, il convient dans un premier temps d'obtenir la CMDB (Configuration Management DataBase) de ces SI ou bien si elle n'existe pas de la constituer. Celle-ci va permettre de connaître la liste des équipements pour lesquels il est possible d'obtenir les logs.

Cette liste sera affinée en tenant compte de la couverture désirée : infrastructure uniquement ou infrastructure et application.

Pour la surveillance d'un SI « classique », il est en général intéressant de collecter les événements des équipements suivants :

- *Pare-feu pour la vision des accès aux différentes zones du SI ;*
- *Passerelles VPN pour la surveillance des accès distants ;*
- *IDS et WAF qui remontent les alertes de sécurité réseau ;*
- *Sandbox utilisée dans la protection des accès Web et de la messagerie pour les alertes de sécurité d'intrusion et de malwares ;*
- *Proxy pour la surveillance accès aux sites identifiés malveillants et pour surveiller les exfiltrations ;*
- *Antivirus sur la détection des malwares connus et leur propagation ;*
- *Messagerie pour la surveillance des exfiltrations ;*
- *Active Directory qui est la cible de la majorité des attaques ;*
- *Annuaire LDAP et équipements d'authentification pour avoir une référence comportementale des utilisateurs ;*
- *Serveurs DNS pour identifier les attaques de type « Tunneling DNS ».*

Il convient ensuite de s'assurer que le SIEM est en mesure d'analyser les logs des équipements choisis. Deux possibilités existent à ce stade : soit le parser de l'équipement est disponible, soit il faut le créer, auquel cas l'équipe SIEM devra travailler sur le sujet.

Plus il y a de parsers à développer, plus le projet BUILD est long et couteux. C'est pourquoi, il est nécessaire de procéder à un examen des logs délivrés par les équipements pour déterminer :

- S'ils sont redondants avec ceux d'autres équipements auquel cas il n'est pas nécessaire de les traiter ;
- S'ils permettent bien d'obtenir les événements définis dans les alertes et si ce n'est pas le cas de reconfigurer l'équipement pour qu'il délivre les événements pertinents. S'il n'est pas possible d'obtenir certains événements, il faudra revoir sa stratégie d'alertes.

Exemple : les logs des routeurs ne présentent généralement pas d'intérêt et font double usage par rapport aux logs des pare-feu. D'autre part, un serveur ne peut journaliser que les connexions réussies alors que les connexions refusées présentent un intérêt pour le SOC.

Une fois que l'on a déterminé exactement les composants des SI qui entrent dans le périmètre de surveillance et que les événements pertinents sont bien remontés dans les logs, il est temps de mettre en place la collecte des logs et le traitement de ces logs par le SIEM.

V.4.2.d. Test, recette et VABF

Les étapes de tests et recette sont identiques à celle d'un projet informatique classique. Les différents tests mettent en jeu des scénarios qui demandent de provoquer des incidents sur les SI surveillés.

Il convient de rédiger un cahier de recette avec des cas passants et non passants et de le dérouler complétement pour décider si la partie détection d'incident du SOC peut être mise en service.

La mise en service passe par une phase de VABF pendant laquelle seront ajustés les différents paramètres et qui permettra d'éliminer la plupart des faux positifs qui viennent polluer les statistiques.

V.4.3. Démarche pour la mise en place des services de réaction aux incidents

Le service de réaction aux incidents doit se mettre en place dès l'étape BUILD mais il est de nature différente.

Il convient de disposer d'une équipe mobilisable à tout moment qui en cas d'incident avéré et critique est en mesure d'effectuer le pilotage des activités techniques nécessaires au traitement des incidents, d'effectuer les analyses système, réseau et les analyses de codes malveillants qui ont dû être collectés par les équipes de surveillance.

Le but ici est d'être en mesure d'identifier le périmètre de compromission et le mode opératoire de l'attaquant puis déterminer les méthodes de remédiation pour limiter la compromission et enrayer l'attaque.

Cette équipe doit donc comporter des compétences pointues sur les systèmes, les réseaux et les codes malveillants et disposer d'une veille technologique importante.

Il est fort possible que cette équipe ne soit pas disponible au sein de l'entreprise auquel cas il faudra faire appel à un prestataire spécialisé dans cette activité. Ceci est l'objet de la certification PRIS mise en place par l'ANSSI destinée aux OIV mais pouvant être utilisée par d'autres entreprises.

Il est important de déterminer si l'entreprise est en mesure de mettre en place une équipe pour la réaction aux incidents. Pour certains types d'incidents comme les APT, il peut être nécessaire de faire appel à une prestation externe avec des experts en cyber sécurité. Il convient d'identifier rapidement les entreprises en mesure de répondre à ce besoin, voire de contractualiser à l'avance les possibilités d'intervention.

V.4.4. Démarche pour la mise en place du service de reporting

Le service de reporting fait appel à des outils intégrés dans le SIEM ou dans la supervision des SI du SOC, éventuellement à des outils complémentaires permettant de récupérer les informations et les mettre en forme convenablement. Par ailleurs, il existe des outils type SIRP qui peuvent être plus pertinents pour un reporting d'incident qualifié.

Les rapports produits par le SOC doivent être examinés par les différents comités et améliorés en permanence afin de répondre aux attentes du pilote et des clients du SOC.

V.4.5. Qu'en est-il de la prévention des incidents ?

La prévention des incidents est assurée par des équipements ou logiciels de sécurité tels que les IPS. Ces outils doivent être choisis avec soin suivant les besoins de l'entreprise et ils peuvent être déployés avant, pendant ou après le déploiement du SOC.

Notons ici que le SOC permet d'affiner la configuration de ces outils afin de leur assurer des performances optimales.

De plus, les outils de prévention peuvent eux aussi alimenter le SOC en remontant des informations non détectées en amont.

V.4.6. Coûts

La partie BUILD suit les mêmes règles que tous les projets informatiques classiques en matière de budget.

Il faudra donc intégrer les coûts suivants :

- Maîtrise d'œuvre et pilotage projet ;
- Gestion de projets ;
- Mise en place et intégration des différents outils cités ci-dessus ;

- Coûts des licences associées ;
- Développement des parsers pour le SIEM ;
- Tests et recette ;
- Paramétrage du SI surveillé, déploiement des agents de collecte des logs
- Formation des collaborateurs ;
- Formalisation des processus.

Les coûts engendrés dépendent de la taille de l'entreprise, du nombre de SI surveillés et de la couverture du SOC en termes de services managés.

V.5. Étape RUN : Opérer le service à long terme

L'étape RUN ne démarre qu'après validation de la VABF et finalisation d'une VSR réussie. À ce stade, les principaux problèmes techniques sont résolus et il est alors possible de se concentrer sur la détection et le traitement des incidents. Toutes les briques humaines et techniques opèrent de façon cohérente sous la baguette du Chef d'orchestre qu'est le pilote du SOC.

V.5.1. Opération du SOC

V.5.1.a. Les différents niveaux de support

Ces niveaux sont répartis en trois équipes :

- Le niveau 1 assure la fonction de supervision des alertes remontées par la plateforme SIEM et réalise les traitements procédurés en adéquation avec les alertes remontées. Si les procédures ne permettent pas de traiter l'alerte sécurité, elle est escaladée au Niveau 2 associé pour une analyse plus approfondie.

Il peut être intéressant de disposer de deux équipes niveau 1 complémentaires : une équipe qui remonte les alertes de sécurité à partir des traitements du SIEM, et une équipe métier qui traite l'alerte et détermine s'il s'agit d'un vrai incident ou bien un manque dans la CMDB (liste blanche pas à jour par exemple). Cette organisation naturelle lorsqu'on externalise le SOC peut être payante en interne. En particulier, l'équipe métier traite l'incident et le ferme dans l'outil ce qui permet de gérer un indicateur sur le taux de fermeture des tickets.

- Le niveau 2 réalise principalement des enquêtes/investigations et des analyses complémentaires d'alertes/incidents en provenance du Niveau 1. En particulier, l'équipe métier directement en relation avec les services opérationnels de l'entreprise peut demander une analyse détaillée d'un incident.

- Le niveau 3 peut être considéré comme le service en charge de la réponse aux incidents mobilisable en cas d'attaque importante nécessitant des moyens et compétences exceptionnelles.

V.5.1.b. Les experts SOC

Les experts SOC sont constitués d'une équipe de « SOC Spécialistes » qui a pour mission de faire évoluer la plateforme SIEM ainsi que l'ensemble des outils mis en place tant sur les aspects performance que sur l'amélioration des règles et de la corrélation.

V.5.1.c. L'amélioration continue de la détection

La mission de cette équipe est multiple et doit permettre d'améliorer la valeur métier produite ou à produire et en décliner des propositions d'actions. Elle assure notamment les prestations suivantes :

- L'activité de veille, la relation avec les services CSIRT et la communication relative à cette veille (bulletin d'alerte, newsletter…) ;
- L'amélioration continue des moyens de détection.

Exemple de ses actions :

- Analyser au sens métier les alertes et les incidents produits ;
- Proposer des améliorations continues pour réduire les faux positifs ;
- Proposer des pistes d'amélioration métier sur le périmètre, reporting de la valeur métier produite ;
- Identifier les axes d'amélioration, et contribuer à la définition des chantiers de transformation ;
- Réaliser la veille sécurité.

V.5.1.d. La surveillance de l'activité du SOC

Il est nécessaire de surveiller à tout moment le bon fonctionnement du SOC et particulièrement la qualité de service et le respect des SLA.

Il faut donc mettre en place un suivi du pilotage opérationnel des processus ainsi que de leur adaptation dans le cadre d'une démarche d'amélioration continue.

Cette activité demande donc de faire travailler ensemble toutes les équipes citées ci-dessus.

V.5.1.e. Les comités

Les différents comités ont été décrits ci-dessus Les comités.

Ils jouent un rôle essentiel durant cette phase permettant de faire la synthèse des informations délivrées par les équipes opérationnelles et de prendre les décisions concernant l'évolution et l'amélioration continue du SOC.

V.5.2. Coûts

Les coûts du RUN doivent être ramenés en coûts d'ETP travaillant sur le sujet.

Il faut y rajouter les coûts d'outillage (licence et maintenance), et de souscription à des services de veille ou de threat intelligence ou autres.

Ceci dépend donc de la taille de l'entreprise, du nombre de SI surveillés et du nombre d'alertes retenues. Le fonctionnement en 24x7 a aussi un impact sur les coûts.

V.6. Premier bilan, retour d'expérience

Plusieurs éléments permettent d'effectuer le premier retour d'expérience de l'activité du SOC et de son efficacité :

- D'une part, les indicateurs de suivi de l'activité du SOC ainsi que les tableaux de bord d'activité ;
- D'autre part, des exercices réguliers ou audits qui permettent de simuler des incidents non encore détectés pour voir si le SOC les détecte bien et pour voir si l'organisation de la réaction aux incidents est opérationnelle.

V.6.1. Indicateurs et tableaux de bord

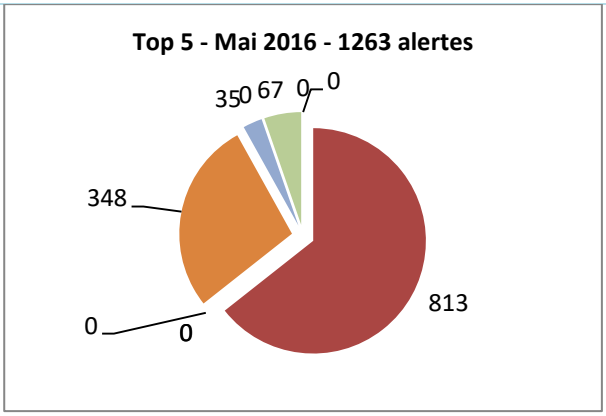
Nous donnons ici une liste d'indicateurs et de leur utilité. Cette liste est donnée à titre d'exemple.

Indicateurs d'activité du SOC		
Indicateur	**Type d'indicateur**	**Commentaire**
Nombre d'équipements surveillés **Nombre d'événements collectés**	Activité du SOC	Base de référence pour les taux qui suivent
Nombre d'alertes déclenchées **Nombre de faux positifs** **Nombre d'incidents de sécurité**	Efficacité du SOC suivant le paramétrage des outils	Si les ratios sont trop élevés, le SOC est mal ajusté. Il faut revoir le paramétrage des outils.
Indicateurs des risques du SOC		
Indicateur	**Type d'indicateur**	**Commentaire**

Nombre de risques identifiés	Ex : Risque de non déclenchement d'alertes sensibles Pic d'alertes sur certaines vulnérabilités	Proposition d'amélioration du SOC
Indicateurs d'efficacité du SOC		
Indicateur	**Type d'indicateur**	**Commentaire**
Détection d'incidents de sécurité	Efficacité de la détection des incidents de sécurité par le SOC sur son périmètre de surveillance	Rapport des incidents détectés par le SOC sur le total des incidents de sécu.
Taux de clôture des incidents sur le mois	Capacité de l'équipe SOC à traiter les incidents	Nombre d'incidents traités sur le total d'incidents déclarés
Indicateurs de surveillance du SOC		
Indicateur	**Type d'indicateur**	**Commentaire**
Surveillance	Pourcentage des alertes récurrentes sur une durée définie, identifiées comme faux positif.	Qualité de la détection
Demandes d'investigation	Respect du délai de fourniture du rapport d'investigation	Mesure des engagements de délais
Incidents	Taux d'incidents mal qualifiés	Nombre d'incidents mal qualifiés / total des incidents de sécurité
Changements	Tenue des délais de changement et amélioration continue	Tenue des délais
Gouvernance	Reporting sécurité	Livré dans les délais

Les tableaux de bord suivant peuvent être générés pour chaque comité de suivi mensuel :

Activité globale du SOC	Synthétise toutes les activités Build et Run du mois : • Nouveaux livrables : nouvelles alertes, nouveaux équipements à surveiller, nouveaux rapports mis en place, … • RUN : incidents de production, SLA respectés (ou non)

	• Incidents N1 : nombre, en cours et clôturés, comparaison par rapport au mois précédent • Incidents N2 : nombre, en cours et clôturés, comparaison par rapport au mois précédent • N3 : nombre d'investigations demandées. • Nombre de propositions d'améliorations • Crise • Nombre d'avis CERT
Volumétrie des alertes et incidents	Chart des alertes et incidents sur les 12 derniers mois
Répartition des alertes par mois suivant leur type	
Analyse des faux positifs	Répartis par type d'alertes
Activité des alertes et incidents par type	Permet de voir l'évolution du nombre d'incidents détectés par type d'alerte et de déterminer si une alerte est inutile ou s'il faut rajouter des alertes.

V.6.2. Exercices et audits

Le fait qu'une alerte ne se déclenche jamais n'est pas le signe de sa non-pertinence.

Il convient donc d'imaginer des scénarios d'attaques exceptionnels et de les soumettre au SOC pour évaluer sa réaction.

Il est souhaitable que ces scénarios ne soient pas imaginés par l'équipe SOC. Il faut donc faire appel à une équipe autre (une red team) ou alors à un prestataire externe spécialisé dans ce type de scénario.

Il est d'ailleurs aussi souhaitable de ne pas prévenir les équipes du SOC tout en prenant les précautions nécessaires pour que cette attaque simulée ne dégénère pas.

V.7. Améliorer et étoffer le projet

Le SOC est opérationnel et donne satisfaction globalement à l'entreprise. Sa maturité va évoluer au fur et à mesure du temps et de son activité.

Il est alors possible d'aller de l'avant en étendant le périmètre du SOC à de nouveaux SI par exemple et/ou prendre en compte de nouveaux agents comme les applications.

Il est aussi possible de définir de nouvelles alertes, de modifier les rapports, en fait de réajuster tout ce qui ne convient pas dans le périmètre initial. Plus généralement, il convient de mettre en place un référentiel de maturité et d'évaluer et de mesurer les axes d'amélioration par rapport à ce référentiel.

On voit alors se superposer une nouvelle étape de BUILD pendant que le RUN continue. C'est pourquoi, il est nécessaire dans les tableaux récapitulatifs de bien lister les deux actions.

En cas de contractualisation avec un ou des partenaires, il est utile de définir tout ce qui peut changer dans le projet et les impacts sur les coûts du projet, afin de ne pas avoir de mauvaises surprises.

Annexe 1. Les aspects juridiques de la mise en œuvre d'un SOC

Lorsqu'une entreprise souhaite mettre en place un SOC, de nombreux enjeux juridiques doivent être anticipés, qu'ils soient internalisés ou externalisés.

a) Les enjeux juridiques du SOC externalisé et internalisé

Il est possible que les prérogatives du SOC entrent en conflit avec les normes internes à l'entreprise. Ainsi, certains changements internes devront être effectués afin de permettre la mise en œuvre des missions de sécurité du SOC (règlement intérieur, charte informatique, etc.).

Cependant, de tels changements peuvent nécessiter l'information et/ou la consultation du comité d'entreprise/des délégués du personnel.

Cette procédure pourrait aussi être mise en œuvre lorsque la mise en œuvre du SOC est susceptible d'entrainer un contrôle de l'activité du salarié.

b) Les enjeux juridiques de l'externalisation du SOC

Quels sont les enjeux soulevés par l'externalisation d'un SOC ? De prime abord, l'externalisation d'un service suppose une contractualisation entre l'entreprise et le prestataire. Sont exposés ci-dessous les principaux enjeux contractuels.

En premier lieu, il est nécessaire de prévoir le périmètre des prestations relatives à la mise en place du SOC, puis à l'exécution du contrat. Le prestataire devra-t-il seulement détecter les incidents ? Devra-t-il prendre le contrôle du système d'information pour faire face à ces incidents ? Quels acteurs le SOC devra-t-il alerter dans l'hypothèse d'une violation de données à caractère personnel ? Ce périmètre doit impérativement être intégré au contrat, afin d'éviter tout problème d'ingérence durant les situations de crise.

Il conviendra également de préciser les modalités d'accès au système d'information par le prestataire. L'entreprise devra ainsi délimiter les éléments à externaliser, afin de minimiser l'ouverture des données tout en garantissant l'efficacité de la prestation.

Pour sécuriser la confidentialité des données contenues dans le système d'information ou dans les données transférées en général, il est préférable d'inclure dans le contrat une clause de confidentialité vis-à-vis du prestataire.

En outre, il est conseillé d'insérer dans le contrat des mesures d'évaluation de la prestation, permettant éventuellement de le résilier en cas de non-respect de la part du prestataire. Il s'agira notamment de préciser les délais d'intervention (de réaction aux incidents, par exemple) tel qu'indiqué dans la *section V.3.5. Les SLA, indicateurs et reporting*. Des pénalités de retard peuvent être appliquées à certaines de ces clauses.

Toute entreprise choisissant d'externaliser un SOC devrait également songer à mettre en œuvre des procédures de contrôle. Pour cela, l'insertion d'une clause d'audit dans le contrat est fortement conseillée. Ceci permet de fixer concrètement le cadre du service et les prestations attendues.

Une attention particulière doit être portée à la clause relative à la responsabilité du prestataire (dommages couverts, plafond de responsabilité, etc.). Le contrat pourra également comporter une clause d'assurance, par exemple, garantissant la réparation des dommages le cas échéant.

Il faudra veiller à définir précisément dans le contrat les aspects liés aux durées de conservation des données chez le prestataire.

En dernier lieu, il convient de prévoir l'après contrat, notamment en vue d'assurer la continuité du service.

c) La protection des données personnelles dans le cadre d'un SOC

Dans le cadre d'un SOC, la conformité à la législation relative à la protection des données personnelles doit être assurée.

En effet, la loi Informatique et Libertés du 6 janvier 1978 et le règlement européen 2016/679 (entré en vigueur le 24 mai 2016 et applicable à partir du 25 mai 2018), fixent un cadre juridique de protection des données à caractère personnel.

Dans l'hypothèse où l'entreprise faisant appel aux services d'un SOC collecte des données à caractère personnel, elle sera caractérisée, a priori, comme « *responsable de traitement* ». À ce titre, le Règlement Général de Protection des Données impose au responsable de traitement de prendre des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation et le chiffrement des données.

Si le SOC est externalisé, le prestataire en charge de la sécurité du système d'information, sera susceptible de traiter ces données afin de mener à bien sa mission. Dès lors, il sera a priori caractérisé comme un « *sous-traitant* », au sens des dispositions législatives. Le Règlement Général de Protection des Données prévoit une évolution sur ce point puisque le sous-traitant pourra faire l'objet de sanctions en cas de non-respect des obligations qui lui sont imposées quant à la protection des données personnelles qu'il traite.

L'article 34 de la loi Informatique et Libertés dispose que « *Le responsable de traitement est tenu de prendre toutes les précautions utiles (…) pour préserver la sécurité des données* ». De plus, l'article 35 de la loi Informatique et Libertés dispose que « *les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant (…) que sur instruction du responsable de traitement* ». Il est donc bon de s'assurer que le SOC ne traite pas les données à caractère personnel en dehors des missions qui lui sont confiées. Pour rappel, en l'état actuel de la réglementation, seul le responsable de traitement peut être sanctionné par la CNIL.

Se pose en outre la question de la localisation du SOC extérieur à l'entreprise. En effet, le transfert de données à caractère personnel hors de l'Union européenne est strictement encadré.

Il faut alors que cet État soit considéré comme assurant un niveau de protection suffisant, ou qu'il soit inséré dans les contrats entre l'entreprise et le prestataire des clauses type dictées par la Commission européenne, assurant une protection adéquate des données.

d) Les textes à anticiper dans la mise en œuvre d'un SOC

Après trois ans de négociations, le Parlement européen et le Conseil de l'Union européenne ont adopté le 6 juillet 2016 la directive concernant les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, ou plus simplement « directive NIS » (Network and Information Security).

S'agissant d'une directive et non d'un règlement, sa transposition dans les droits nationaux de chaque État membre devra intervenir avant le 9 mai 2018.

La directive NIS se propose de renforcer la cyber-sécurité des États membres et leur coopération en matière de sécurité informatique. Les SOC sont concernés, en tant qu'acteurs de premier plan pour ce qui est de la cyber-sécurité.

Annexe 2. Politique de log

Les logs ou traces (aussi appelés événements de sécurité) sont la matière première pour la surveillance de la sécurité d'un SI. Que ce soit les postes de travail, les serveurs, les applications, les équipements de sécurité tels que les pare-feu ou les IDS (liste non exhaustive), tous génèrent des traces dans le but d'être exploitées ou d'identifier les comportements à risque. Toutefois, par défaut les systèmes génèrent peu ou pas de traces et souvent les informations nécessaires pour la supervision de la sécurité d'un SI sont manquantes. Il est donc important dans un premier temps de réviser la politique de logs par défaut des différents systèmes (serveurs, applications, équipements réseaux,…) afin de s'assurer que les scénarios d'attaque préalablement retenus seront correctement détectés. Il faudra le cas échéant procéder par itérations des scénarios d'attaque et affiner les politiques de logs en conséquence pour s'assurer de l'exhaustivité de la détection

La politique de logs doit prendre en compte :

- Les besoins de conformités réglementaires
- Les informations nécessaires pour l'investigation en cas d'incident de sécurité
- Les informations nécessaires aux équipes IT ou métiers suivant l'usage prévue de la solution de collecte et de centralisation des logs.
- Les capacités de traçage des équipements.
- La volumétrie et la capacité de traitement de la solution de collecte et de centralisation des logs.

En fonction du périmètre de supervision et de l'importance de l'équipement ou des assets de la zone, un type d'équipement peut avoir une politique de log différente. Par exemple, un pare-feu de bordure Internet ne trace pas toutes les connexions rejetées de l'Internet vers le réseau interne car il est souvent attaqué et cela générerait trop de logs inutiles. Par contre un pare-feu protégeant des actifs critiques doit tracer toute les connexions ou tentatives de connexions pour les besoins d'investigation en cas d'incident.

La politique de logs d'un équipement doit prendre en compte à minima les catégories suivantes :

- Authentification ;
- Gestion des utilisateurs ;
- Gestions des groupes d'utilisateurs ou rôles ou profils ;
- Changements de configuration ;
- Erreurs de fonctionnement ;
- Alertes de sécurité ;
- Actions métiers essentielles.

Il convient également de limiter la redondance d'information. En particulier dans le cas de logs réseau il est possible de trouver la même communication sur plusieurs équipements surveillés. La politique devra définir en fonction des traces à obtenir quel est l'équipement le plus judicieux pour produire les logs.

Annexe 3. Externalisation du SOC

Nous présentons ici nombre de considérations, mais il appartiendra à chacun de faire les bons choix, en fonction de la situation particulière de chacun.

L'arbitrage Make or Buy est inhérent à chaque projet et la question se pose pour chaque service composant le SOC. Le choix de cet arbitrage relève de considérations propres aux entreprises (stratégie, politique RH, contexte économique, contraintes planning….).

Si les plus grandes organisations peuvent envisager de mettre en œuvre les ressources nécessaires pour construire un SOC interne, d'autres peuvent faire face à de très fortes difficultés dans la construction d'une telle fonction interne non directement liée à leur métier.

Les coûts de construction et de maintien d'un SOC interne peuvent être très importants et non envisageables pour des organisations qui ont pourtant un besoin essentiel d'une sécurité opérationnelle forte.

Comme tout chantier d'externalisation, il est structurant de définir sa stratégie et de bien cadrer ses attentes avant de se lancer dans un processus de recherche et d'achats, car cela influera non seulement sur les coûts des services, mais aussi sur l'organisation interne à mettre en place, la sélection des prestataires en capacité de répondre et les engagements de services à obtenir.

Certaines réglementations pourront influer sur la recherche d'un prestataire externe (exemple avec la Loi de Programmation Militaire pour les OIV qui demande des opérateurs qualifiés PDIS pour la surveillance des SI dits d'importance vitale).

Les éléments suivants sont proposés comme aide dans l'analyse d'un besoin d'externalisation.

Facteur	**Intérêts**	**Limites**
Mutualisation des informations	Un SOC externe peut faire bénéficier d'une vision plus globale des menaces, non exclusivement limitée au périmètre de l'organisation. Un incident chez un client du prestataire peut ainsi aboutir à une évolution des règles de détection pour tous les clients éventuellement avec une approche par secteur d'activité. Les règles de détection peuvent ainsi être plus ajustées et le prestataire peut apporter une vision préventive intéressante.	Dans les faits, ce facteur peut être limité par l'organisation et les performances du prestataire d'une part (croiser les informations représente du temps) et la spécificité du contexte (hors contexte, une information sur une menace reste très limitée). Il conviendra en cas de souhait d'externaliser de challenger le prestataire sur ce sujet. Par ailleurs, il peut exister d'autres moyens pour les organisations de réaliser une veille similaire par le biais de

		clubs ou regroupements d'entreprises, avec potentiellement une vision plus précise car sectorisée (ex : banque...). Une telle veille peut permettre des échanges d'indicateurs de compromission (IoC) utiles dans la mise à jour des règles de détection.
Évolutivité	Un SOC interne sera obligatoirement limité par ses ressources, qu'elles soient technologiques (logiciels, matériels...) ou humaines (compétences, personnes). Un SOC externe pourra potentiellement évoluer plus facilement en fonction des besoins et du contexte, par ajout de services supplémentaires et par le biais d'avenants et commandes complémentaires.	L'ajout d'un service constituera un coût à prendre en compte, et cela dès la phase de choix du prestataire. La contractualisation initiale d'un service évolutif n'est en effet pas facile : il faut prévoir avant le démarrage les cas possibles d'évolution afin de les maîtriser et d'évite un effet d'inflation permanente et/ou de perte de maîtrise du service. La même remarque peut d'ailleurs être appliquée à l'analyse du modèle d'évolution des coûts selon les volumes (en fonction des sources, des EPS, du périmètre). Enfin, il faudra s'aligner par rapport au catalogue du prestataire pour na pas avoir à demander des services sur mesures, qui peuvent être très onéreux, voire contractuellement impossibles. Selon ce catalogue, des limitations s'appliqueront donc.
Gestion des ressources et des compétences	Un prestataire spécialisé aura plus de grandes facilités que beaucoup d'organisations dans la gestion des ressources et des compétences. Parce que c'est son métier, il peut recruter et assurer la formation et la gestion de carrières de tous les	L'intérêt peut être limité par 2 facteurs : 1) L'organisation elle-même peut ne pas être en capacité de gérer une forte réactivité en réaction, ce qui rend peu pertinent un service externe en 24x7 et limite *de facto* la capacité d'analyse y

	niveaux de personnels requis par le SOC. Parce qu'il peut mutualiser entre plusieurs clients, il peut organiser un fonctionnement en 24x7 si besoin sur plusieurs sites et mettre en place des astreintes sur des profils "rares" (forensics, gestion de crise...). Pour une organisation, recruter plusieurs personnes pour un SOC (sans parler de 24x7 pour lequel il faudra au minimum 7 ETP pour une personne en continu), assurer la disponibilité de toutes les compétences (techniques, technologiques, métiers...) et gérer les carrières de ces profils très spécifiques peut représenter un challenge très important.	compris en heures ouvrées. Il faut rappeler qu'un SOC externalisé est obligatoirement limité dans sa capacité de qualification d'une alerte. Il fait gagner du temps à une organisation mais ne remplace pas des équipes internes. Il est possible de donner à un SOC externe des capacités de réaction (comme fermer des flux ou des services), mais cela demande un travail important de préparation compte tenu des impacts métiers potentiels. 2) Si une supervision continue est demandée, il convient de vérifier lors du choix d'un prestataire la manière exacte dont la gestion d'événement se fait en heures non ouvrées. Beaucoup de prestataires n'offriront en heures non ouvrées qu'un service limité à la prise en compte d'alertes critiques, avec une capacité réduite d'analyse.
Gestion des budgets et des contrats	Un SOC externe peut permettre d'avoir une souplesse dans la gestion des budgets notamment pour des organisations ayant des capacités d'investissement limité. De manière temporaire ou plus longue, le SOC externe peut également apporter ses propres outils en mode "location", évitant l'acquisition et le MCO de solutions technologiques souvent coûteuses et pas toujours aussi matures qu'on ne le croit.	Il est essentiel de prendre en compte les coûts "cachés" habituels en cas d'externalisation, notamment : 1) Le processus d'achat qui peut être complexe à gérer compte tenu de la complexité du sujet 2) Le pilotage des services externalisés qu'il convient d'assurer de manière fine et qui peut devenir très conséquente en cas de périmètre mal défini ou de mauvais choix initiaux. 3) Le maintien de la compétence interne, qui reste fondamental car un SOC externe pourra détecter des incidents mais ne les résoudra pas. Un projet

		d'externalisation devra identifier très clairement des charges internes à conserver pour alimenter le SOC, assurer une qualification précise et réagir aux incidents. 4) La réversibilité, qui dans le cadre d'un SOC, peut être une vraie complexité notamment en cas de solution propriétaire du prestataire. Même avec des solutions du marché, l'interopérabilité reste limitée et la reprise de compétences sur les règles de détection et les procédures en place peut être complexe.

Dans un certain nombre de cas, il peut également être utile de faire appel **ponctuellement** à des ressources externes. Ces cas incluent :

- Les temps de crise (nombre très important d'alertes prioritaires, attaque avérée, etc.) ;
- Des lacunes en termes de veille sur la cyber sécurité ;
- Des lacunes en termes d'analyse approfondie de certains incidents (compétences techniques particulières pour l'analyse d'un malware par exemple) ;
- Le manque de compétence pour intégrer ou configurer une solution de sécurité nouvelle pour le SOC.

Ainsi, il est possible d'acheter des services externalisés en accompagnement du SOC :

- Veille de sécurité dont l'objet est la description des nouvelles techniques d'attaque et des moyens disponibles pour les détecter dans des traces (ensemble de règles) ;
- Assistance à l'amélioration de la supervision d'un périmètre technique ;
- Prestations de niveau 3 de support ou de type forensics en cas d'attaque
- Audit du SOC.

Effet secondaire de la mutualisation, le recours à l'externalisation pour des services aux horaires étendus voire 24x7, ou pour des expertises très pointues ou précises, peut être un levier important sur les coûts.

L'externalisation du service peut paraître à moindre coût qu'un service équivalent rendu en interne mais il faut intégrer les coûts indirects de gestion et de réversibilité. En effet, il est nécessaire de suivre un processus d'achat (par exemple rédaction des appels d'offres). De plus lorsque le contrat expire et si le prestataire en place n'est pas remplacé, toute opération à effectuer et non spécifiée dans le contrat pourra être bloquée. Enfin lorsqu'un nouveau

prestataire sera en place, une perte d'efficacité pourra être notée le temps qu'il monte en compétence.

Quel que le soit le type d'externalisation choisi, il faut souligner l'importance de l'interface à créer avec le ou les prestataires. Le choix d'externaliser implique la création d'un pilote du prestataire interne à l'organisation, et la mobilisation d'opérationnels internes capables de gérer les sollicitations (ex : alertes levées) du prestataire.

En forçant le trait, un MSSP peut être vu comme un générateur d'incidents, qu'il faut être capable de traiter ! (les incidents se sont produits mais n'ont pas été détectés…)

Annexe 4. Présentation du document du MITRE

Le MITRE est une organisation américaine à but non lucratif qui gère des centres de recherche et développement financés par le Gouvernement fédéral.

Le MITRE publie sur son site Internet un document rédigé par Zimmerman sur les 10 stratégies à suivre pour mettre en place un centre opérationnel de sécurité de classe mondiale que nous résumons ici.

Stratégie 1 : Consolider le SOC sous une même organisation

Stratégie 2 : Trouver un équilibre entre la taille et l'agilité

Stratégie 4 : Faites peu de choses, faîtes les bien

Stratégie 5: Préférez la qualité du personnel à sa quantité

Stratégie 6: Maximiser la valeur des technologies acquises

Stratégie 7: Exercez de la discrimination dans les données collectées

Stratégie 8: Protéger les missions du SOC

Stratégie 9: Être un acteur consommateur et producteur sur l'intelligence en matière de Cyber menaces

Stratégie 10: Stop, Réfléchir, Répondre …. dans le calme

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11 rue de Mogador
75009 Paris
France
✆ +33 1 53 25 08 80
clusif@clusif.fr

Téléchargez toutes les productions du CLUSIF sur
www.clusif.fr