SUPERVISION DE LA SECURITE DU SYSTEME D'INFORMATION DANS LES SECTEURS BANQUE ET ASSURANCE

Le **S**ecurity **O**peration **C**enter – SOC

Juin 2016

Une étude menée avec

Atos

Le Forum des compétences est une association composée de banques et de sociétés d'assurance qui échangent dans le domaine de la sécurité de l'information dans l'objectif d'élaborer des bonnes pratiques applicables dans leurs secteurs d'activités. Le résultat de ces échanges fait l'objet de publications sur son site web (www.forum-des-competences.org). L'organisation d'évènements est l'occasion de partager ces réflexions et d'échanger avec les acteurs de la place, notamment avec les régulateurs et les prestataires.

Table des matières

1 Introduction

Objet du groupe de travail

Le sujet de la supervision des Systèmes d'Information (S.I.) revient sur le devant de la scène notamment en raison de nouvelles réglementations auxquelles sont soumis certains domaines d'activité, mais également en raison des menaces accrues qui pèsent sur les S.I. et qui ont des impacts de plus en plus graves. Engagés dans une transition et transformation numériques, les S.I. se retrouvent pour la plupart au contact d'Internet, siège de la cybercriminalité et des « cyber-convoitises », l'exposition aux risques est certaine.

Dans le domaine de la supervision de la SSI, 3 difficultés majeures sont rencontrées :

1. la masse et la diversité des informations à traiter ;
2. l'identification des d'évènements précurseurs d'alertes de sécurité ;
3. l'appropriation du sujet et la réunion des compétences requises pour un projet d'envergure.

Sur les deux premiers points, des opportunités technologiques peuvent être mises à profit. Il s'agit de l'arrivée à maturité des outils d'analyse comportementale, de l'augmentation des capacités de traitement et de l'intégration des briques technologiques « big-data ».

Toutefois, s'il est certain que l'outillage est indispensable, le domaine de la supervision de sécurité des S.I., pour être efficace, doit être exigeant sur l'identification de la cible de sécurité, mais avant tout sur l'étendue des compétences des équipes qui servent le dispositif de supervision du S.I. Il est recommandé, et c'est généralement le cas, que la supervision SSI soit assurée par une entité spécialisée :

Le **C**entre **O**pérationnel de **S**écurité **COS** (COS en anglais devient le SOC pour Security Operation Center).

Ce document s'adresse à un public qui a déjà eu l'occasion d'aborder les questions de sécurité des systèmes d'information (SSI) et des enjeux qui s'y rapportent.

Le « Security Operation Center » (SOC)

Au-delà de la collecte pertinente des évènements de sécurité dans les journaux (i.e. les logs) et de la corrélation de ceux-ci, les attentes et les exigences grandissent ; de nombreuses questions émergent:

- Qu'est-ce qu'un SOC, quelles sont ses missions ?
- Comment s'intègre-t-il dans la stratégie de défense de l'Entreprise ?
- Comment s'organisent les interactions entre les missions d'un CSIRT et celles d'un SOC ?
- Quelles sont les fonctions d'un SOC ?
- Existe-t-il diverses générations de SOC ?
- Quels sont les modèles organisationnels applicables ?
- Quels sont les modèles économiques et technologiques (MSSP, SOC dédié, mutualisé, hybride) ?
- Quelles sont les spécificités d'une mise en œuvre en milieu banque-assurance ?
- Quid de la gestion de crise cyber ?

Les membres du groupe de travail

• **Arnaud GODET**	SCOR	agodet@scor.com
• **Yves JUSSOT**	ANSSI	yves.jussot@ssi.gouv.fr
• **Pierre HURET**	Crédit Agricole S.A	pierre.huret@credit-agricole-sa.fr
• **Xavier PANCHAUD**	BNP Paribas	xavier.panchaud@bnpparibas.com
• **Didier GRAS**	BNP Paribas	didier.gras@bnpparibas.com
• **Christian QUIVY**	Crédit Mutuel Arkéa	christian.quivy@arkea.com
• **Patrick BRUGUIER**	Banque de France	patrick.bruguier@banque-france.fr
• **Gérard LE COMTE**	Société Générale	gerard.le-comte@socgen.com
• **Dan NIZARD**	Atos	dan.nizard@atos.net
• **Jean-Baptiste VORON**	Atos	jean-baptiste.voron@atos.net
• **Wilfrid GHIDALIA**	Forum des Compétences	ghidalia@forum-des-competences.org

2 Contexte général

Une cybercriminalité omniprésente

Les cybermenaces entrent de façon pérenne dans la réalité quotidienne des entreprises. Les cyberattaques sont et seront de plus en plus fréquentes, multiples (c'est-à-dire mettant combinaison de plusieurs cyberattaques), discrètes et évoluées. Elles s'inscrivent dans la durée. Elles ne ciblent plus seulement les systèmes technologiques mais aussi directement les personnes (salariés, prestataires, partenaires, fournisseurs, clients), en leur dérobant des informations primordiales qui accroissent ensuite considérablement leur capacité de nuisance. L'écosystème complet de l'Entreprise s'en trouve directement menacé.

Les connaissances et compétences mises en œuvre dans le cade de ces attaques démontrent que les acteurs malveillants n'hésitent plus à investir dans des moyens techniques et humains importants pour atteindre leur objectifs.

L'actualité démontre que l'activité des entreprises attaquées est fortement perturbée, voire interrompue de façon durable. Les impacts financiers, organisationnels, juridiques et d'image peuvent être très importants, voire fatidiques lorsqu'ils font vaciller la confiance entre l'entreprise et ses clients, ses partenaires ou ses salariés dans le cas de vol ou divulgation de données personnelles, stratégiques ou critiques. Les dispositifs existants de gestion de crise et de continuité d'activité doivent être renforcés pour répondre aux risques associés.

Ces observations s'inscrivent dans une ère de transformation numérique de l'Entreprise sous-tendue par l'apparition de nouvelles technologies comme la mobilité, le cloud et l'ouverture des données de l'Entreprise à ses clients et partenaires via ses propres systèmes et/ou les réseaux sociaux. La multiplication et la diversification des systèmes techniques mis en œuvre induit une augmentation sans précédent du nombre de vulnérabilités. La surface d'attaque de l'Entreprise tend ainsi à croitre de façon très importante.

La cybercriminalité est désormais agile, industrialisée, structurée et professionnelle. Elle exploite toutes les vulnérabilités et failles techniques, organisationnelles et humaines. Quel que soit le secteur d'activité, plus aucune Entreprise n'est épargnée.

Législation, réglementation, conformité

En complément des aspects de société décrits dans le paragraphe précédent, les Entreprises, et plus particulièrement celles des domaines banque et assurances, sont contraintes et régies par un ensemble de règles et directives qui définissent et précisent les objectifs de sécurité à atteindre et qui se déclinent en organisations et moyens techniques. Parmi elles, on distingue :

- Contraintes réglementaires liées au domaine bancaire ;
- Contraintes réglementaires au domaine assurance ;
- Contraintes des réglementations internationales, européennes & nationales ;
- Obligation de localisation des données ;
- Obligation de notification d'incidents.

Pour les Entreprises reconnues (au moins en partie) en tant qu'Opérateur d'Intérêt Vital (OIV), s'appliquent en plus et en priorité :

- Les directives nationales de sécurité (DNS) ;
- Les conclusions du Le Livre blanc « défense et sécurité nationale » ;
- La loi de programmation militaire 2014-2019 (LPM) ;
- L'instruction générale interministérielle n°6600 du 07 janvier 2014 ;

Dans ce cadre, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) veille à l'application des règlements propres à la LPM, au contrôle de la mise en œuvre de systèmes qualifiés de détection d'événements malveillants et au contrôle de la notification de tout incident de sécurité par ces opérateurs.

La mise en œuvre d'un centre opérationnel de sécurité est elle-même soumise à un ensemble de règlements et de contraintes notamment liées à la gestion des événements et informations collectées sur le système d'information de l'Entreprise comme le stockage et archivage des informations et la collecte et l'utilisation de données à caractère personnel.

La responsabilité de la Direction de plus en plus engagée

Comme dans les autres domaines que la cybersécurité, il est *in fine*, de la responsabilité de la Direction de l'Entreprise de s'assurer du respect des exigences (légales, réglementaires et contractuelles) mentionnées dans le paragraphe précédent.

L'actualité nous montre régulièrement, qu'en cas d'attaques réussies, les impacts financiers et d'image peuvent être considérables. Par exemple, les directions de grandes entreprises comme *Sony Pictures* et le groupe de distribution *Target* ont été inquiétées par des actions collectives en justice (*data breach* américain pour Sony et vol géant de données bancaires de ses clients pour Target). Dans ce dernier cas,

les excuses du président de Target auprès de sa clientèle n'ont pas suffi et il a été contraint de quitter son poste.

Plus près de nous, en France, la CNIL a sanctionné Orange et Optical Center pour des défauts de sécurité des données clients. La direction de ces groupes a systématiquement été inquiétée.

3 Concepts et fondamentaux

Le "Security Operation Center" (SOC)

Un SOC est avant tout une équipe d'experts en sécurité chargée de surveiller, détecter, analyser et qualifier les évènements de sécurité. Cette équipe assure le pilotage des réactions appropriées aux incidents avérés de sécurité. Pour certaines organisations, cette équipe administre et contrôle au quotidien des dispositifs et dispositions de sécurité ; par exemple le « durcissement » de systèmes d'exploitation standards en vue de renforcer leur sécurité, ou bien la gestion d'accréditations (droits d'accès à des ressources) voire également la gestion du « patch management ».

En support direct du métier et en partenariat avec les services IT, un SOC a pour objectif de réduire à la fois la durée et l'impact des incidents de sécurité qui tirent profit, perturbent, empêchent, dégradent ou détruisent les systèmes dédiés aux opérations habituelles et standards. Cet objectif est atteint grâce à une surveillance efficace et à un suivi des incidents de bout en bout.

Le SOC a la responsabilité, d'une part, de déclarer qu'il y a effectivement un incident sur le SI, et, d'autre part, il est responsable de la conduite des opérations qui lui permettront de déclarer l'incident clos. Du point de vue opérationnel c'est le couple des entités SOC et CERT/C-SIRT qui assure la résolution[1] d'un incident.

Par ailleurs, selon les choix organisationnels, le SOC peut également assurer les missions suivantes :

- Suivi des vulnérabilités (de la détection à la correction)
- Veille en sécurité informatique
- Sensibilisation des utilisateurs en fonction des observations faites sur le SI
- Expertise et conseil auprès des équipes informatiques
- Pilotage de la mise en œuvre des correctifs de sécurité

Compte tenu de la variété des missions, des impacts technologiques ainsi que des impacts organisationnels majeurs, la mise en œuvre d'un SOC représente un réel investissement en temps et ressources pour l'Entreprise concernée; même avec l'aide d'un prestataire qualifié (type MSSP). C'est aussi pourquoi il est généralement nécessaire que l'Entreprise atteigne une taille critique avant de consacrer des ressources internes à l'opération de son propre SOC. Dans le cas des entreprises constituées de plusieurs entités, il est fréquent que le SOC soit porté par l'une d'entre elle de façon transverse pour les autres.

[1] La phase de « résolution »comprend d'une part l'analyse et l'explication de l'incident et d'autre part les mesures à prendre en réaction à l'incident. Les mesures sont prises en accord avec les responsables métier impactés.

Principales différences entre le SOC et le CSIRT

Selon l'ENISA, un CSIRT est défini comme une équipe d'experts en sécurité informatique ayant pour mission principale de répondre aux incidents en proposant les services nécessaires au traitement des attaques et en aidant leurs parties prenantes à restaurer les systèmes qui en ont fait l'objet.

La limite entre SOC et CSIRT n'est pas toujours évidente à tracer. Seul un modèle de gouvernance et des responsabilités clairement établies permettent de partager détection, réaction et suivi des incidents. Les adhérences entre le modèle de sécurité de l'Entreprise et l'organisation de l'Entreprise peuvent constituer un frein supplémentaire au partage des tâches et responsabilités (il n'est pas rare que les fonctions/rôles des deux entités soient portés par les mêmes personnes).

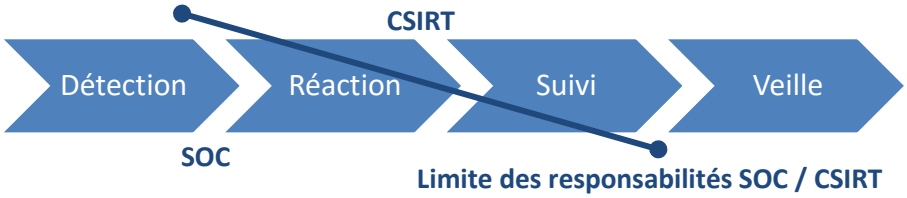


Figure 1 :4 grandes activités de la sécurité opérationnelle

Il est cependant communément admis que le SOC est responsable de la gestion des vulnérabilités, de la détection et de la qualification des incidents de sécurité alors que le CSIRT est responsable de la gestion de crise cyber (notion plus large que la réaction à un incident de sécurité) et de la veille autour des cybermenaces (y compris les analyses *forensics*).

Synergies entre SOC et CSIRT

Si la limite entre les deux entités n'est pas clairement définie, les adhérences et interfaces n'en sont que plus nombreuses. Ainsi, en considérant la chaîne plus détaillée présentée ci-dessous, le curseur du partage des missions est laissé à l'appréciation de l'organisation. **L'efficacité de la sécurité dépend de la complétude de la chaine et non de la répartition des missions**.

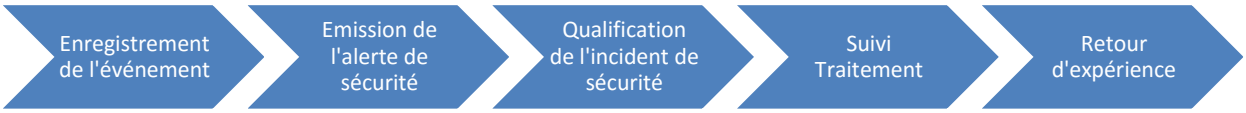


Figure 2 Chaîne de traitement d'un incident de sécurité

En complément, il primordial de bien organiser le ou les passages de témoins (*a minima* qualité et quantité de l'information transmise et moyen de transmission) entre les différents acteurs responsables des missions. Toutes les interactions entre les missions et activités doivent être prises en compte et pas seulement les grandes interfaces.

Si le traitement et la veille sont généralement confiés au CSIRT, il faut noter que l'objectif est que le SOC gagne en maturité et en efficacité au fur et à mesure du traitement des incidents. La façon la plus simple d'atteindre cet objectif est de constituer des fiches de retours d'expériences (REX ou REEX) à l'issue de

toute intervention du CSIRT. Ainsi, au fur et à mesure, si un incident est enregistré à propos de technologies, produits ou attaques connues, et que celui-ci fait l'objet d'une fiche ou procédure qui permet le traitement de l'incident, le SOC pourra dérouler la chaine sans avoir à solliciter l'entité CSIRT. Selon ce modèle de maturité, le CSIRT n'est alors sollicité (en escalade) qu'en cas de nouvelle attaque (inédite) nécessitant une expertise spécifique. Le CSIRT pilote alors la résolution le temps de pouvoir industrialiser la remédiation.

Le tableau ci-dessous propose une répartition typique des activités. Comme précisé dans les paragraphes ci-dessus, chaque organisation est libre d'adapter les missions des entités SOC et CSIRT du moment que la chaine de traitement est considérée de bout en bout.

	SOC	CSIRT
Gestion des vulnérabilités sur le périmètre	Responsable	Contribue (cf. Veille)
Collecte des événements sur le périmètre	Responsable	
Gestion des règles de corrélation d'évènements	Responsable	
Pondération des événements => émission d'alertes	Responsable	
Qualification de l'incident (instruction)	Responsable/Contribute	Responsable/Contributeur
Pilotage de la remédiation	Contribue	Responsable. Veille à l'industrialisation de la remédiation.
Remédiation technique	Acteur primaire (escalade N1 > N2 > N3)	Acteur sollicité sur escalade depuis N2 ou N3
Clôture de l'incident	Responsable	
Gestion de cybercrise	Contribue	Responsable
Veille technologique / Veille menaces		Responsable
Analyse post-mortem		Responsable
Communication avec les autres CERT[2]		Responsable

Figure 3 Répartition des activités SOC/CSIRT

Journaux, événements, alertes et incidents

Pour éviter toute confusion dans la suite de ce document, les définitions des termes « journaux / enregistrements », « événements », « alerte » et « incident » sont proposées ci-dessous :

Journaux / Enregistrements

Les « journaux » ou « enregistrements » constituent la matière première (généralement à l'état brut) que le SOC devra manipuler, analyser, corréler tout au long de la journée. Tout élément d'un système d'information produit désormais des enregistrements agrégés en journaux. C'est à partir de ces éléments que sont créés les premières métriques et rapports d'activités d'un SOC.

[2] Sous réserve de « certification CERT »

Constituant les logs d'un système actif, ces journaux sont généralement conservés à des fins d'exploitation ou d'investigation. Ils sont parfois les seuls éléments (à charge) qui peuvent être utilisés en cas de comportement anormal ou suspicieux d'un système. Ils sont donc généralement protégés voire séquestrés pour être utilisés en tant que preuve.

Etant donné que tous les systèmes, et leurs composants (et leurs sous-composants) génèrent des traces, des enregistrements et des journaux, le défi consiste à déterminer le bon compromis entre la granularité (aussi appelée verbosité) des éléments produits par rapport à l'utilisation qu'un SOC peut en faire.

Evénement

Selon la norme ITIL v3, un « événement » correspond à un changement d'état suffisamment important pour être notifié à un gestionnaire du service. Ainsi, il peut s'agir d'un changement d'état *normal* ou, au contraire, d'un changement pour un état anormal (ex. une défaillance). Un événement peut être transcrit par un ou plusieurs enregistrements dans un journal.

Dans le cadre de ce document, nous préférerons la définition de la norme ISO 27000 (2.20) qui précise qu'un événement de sécurité est une occurrence identifiée de l'état d'un service, d'un système ou d'un réseau indiquant une faille possible dans la politique de sécurité de l'information ou un échec des mesures de sécurité ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité.

Alerte

Une alerte correspond à un événement ou à un groupe d'événements pondéré. Cette pondération est particulièrement importante puisqu'elle permet de classer les événements et de ne retenir que ceux qui atteignent ou dépassent un seuil de vigilance. Tout comme pour les enregistrements et journaux, le défi consiste à fixer correctement le seuil (ou à le retenir auprès d'un organisme tiers) pour ne conserver que les événements qui nécessitent une attention particulière.

Parce que les mécanismes qui associent une pondération à l'événement peuvent être défaillants ou inadaptés, les alertes peuvent être classées en différentes catégories :

- *Faux positif* : la pondération a été positionnée de façon inadaptée, rendant un événement important à tort. Dans ce cas, le comportement du système est considéré défaillant à tort.
- *Vrai positif* : la détection a été correctement positionnée. Il s'agit d'une alerte qui correspond réellement à un événement redouté ou à comportement anormal du système.
- *Faux négatif* : le mécanisme de détection n'a pas correctement fonctionné et un événement qui aurait dû être identifié en tant qu'alerte n'a pas été repéré et classé. Le système est défaillant et aucune alerte n'appuie ce statut.
- *Vrai négatif* : le mécanisme de détection est adapté. Le comportement du système n'est pas défaillant et aucun événement n'est identifié en tant qu'alerte à tort.

Incident

Toujours selon la norme ITIL, un incident est une interruption non planifiée d'un service, une réduction de la qualité d'un service ou la défaillance d'un élément du système. Un incident est associé à un impact

négatif (perçu ou non) sur la qualité de service globalement perçue par les utilisateurs du système. Un incident est généralement (mais pas toujours) caractérisé par une série d'alertes. Il est généralement enregistré, analysé et traité sur la base des éléments d'information le constituant. Un incident appelle une réponse.

Dans le contexte de la sécurité des systèmes d'information, la norme ISO 27000 (2.21) définit un incident comme un ou plusieurs évènements liés à la sécurité de l'information indésirables ou inattendus présentant une probabilité forte de compromettre les activités de l'organisation et de menacer la sécurité de l'information.

La chronologie suivante peut être établie :

Les incidents peuvent être catégorisés par le SOC ou le CSIRT, selon des critères propres à l'organisation, pour permettre un reporting à plus haut niveau et, in fine, outiller le pilotage de la sécurité des S.I. La catégorisation permet également de favoriser les comparaisons entre pairs. La norme ISO 27014 et les documents de travail de l'ETSI[3] établissent à cet effet la catégorisation/taxonomie des indicateurs/catégories d'incidents de sécurité.

Le SIEM

Les SIEM (*Security Information and Event Management* – système de gestion des informations et des événements de sécurité) se sont imposés avec la démocratisation de la génération des journaux et des traces que produisent les différents systèmes et plus particulièrement ceux de sécurité. Il ne suffit plus, aujourd'hui, d'observer les traces produites par un composant de sécurité pour s'assurer du bienfondé du comportement du système complet. Il faut, à minima, considérer les traces des différentes briques essentielles du système.

Ces opérations d'observation et de recoupements, longues et fastidieuses, ont fait l'objet de plusieurs techniques et solutions de concentration et d'agrégation de traces. Ces systèmes de collecte et d'agrégation ont progressivement été enrichis de fonctionnalité de tri, de filtre et de statistiques produisant ainsi des rapports de journalisation sur tous les systèmes connectés. Par des mécanismes d'analyse statique des enregistrements, les SIEM sont désormais capables de détecter les enregistrements potentiellement générateurs d'événements voire même de qualifier certains d'entre eux en alertes.

Selon le système considéré, les traces, événements et alertes peuvent être rapprochés les uns des autres (géographiquement ou temporellement) pour permettre à un tiers (humain ou automatique) d'enregistrer/déclarer un incident.

[3] European Telecommunications Standards Institute : *ETSI GS ISI 001-1 V1.1.2*

Les SIEM sont généralement complétés d'une solution de gestion de traces (dotée des fonctionnalités d'archivage, de stockage, de protection et d'indexation).

Les SOC s'appuient systématiquement sur un ou plusieurs SIEM. Ce sont eux qui fournissent les éléments de base du travail de tout analyste. Leur prétraitement permet aux analystes de se débarrasser de la fastidieuse tâche de collecte et d'inventaire des événements sur tous les périmètres concernés.

Quid des événements métiers et applicatifs ?

Depuis quelques années, et compte tenu de la sophistication croissante des attaques, la seule observation des traces produites par les équipements techniques disséminés dans le système d'information de l'Entreprise ne suffit plus. Les comportements des applications et des systèmes métiers de l'Entreprise doivent également être observés.

Les mêmes mécanismes de collecte, de tri, de qualification et de remédiation s'appliquent. Cependant, les compétences humaines et techniques nécessaires à la compréhension de la situation et à son traitement sont très particulières.

Alors que le lien de cause (vulnérabilité dans un socle technique) à effet (vol d'information ou fraude) relevait jusqu'à présent du domaine d'experts en sécurité des infrastructures, les nouvelles attaques, qui ciblent directement les applicatifs, raccourcissent le chemin entre vulnérabilité du processus métier (ou applicatif) et l'impact business.

Il est donc primordial d'adjoindre la collecte des événements métiers à la collecte des événements technique en prenant soin :

- de séparer le traitement des deux sources
- de multiplier les croisements/comparaison/corrélation entre ces deux sources

Enfin, il faut noter que les développeurs d'applications portent désormais une responsabilité majeure dans l'efficacité des dispositifs de supervision de la sécurité (dont le SOC)[4]. En effet, il est de leur ressort de produire (ou de prévoir la production) les événements pertinents et détaillés de façon à alimenter les dispositifs de supervision.

4 Le SOC dans la stratégie SSI

La sécurisation d'un système d'information doit être abordée selon les 4 volets suivants :

1. **Gouvernance** : Définition et mise en place de la gouvernance, c'est-à-dire identifier les acteurs, les rôles, les règles et les processus qui régissent la sécurité du système d'information. Détermination de la cible de sécurité que l'entreprise se choisit.

[4] L'obligation pour tout développeur de prévoir la production des traces et les directives pour la production de traces de qualité (i.e. utiles dans le cadre de la supervision de la sécurité d'un système) figurent malheureusement encore trop peu souvent dans les PSSI des entreprises

2. **Protection**: Sélection puis mise en place des mesures de protection organisationnelles et techniques nécessaires pour mitiger les risques afin que la sécurité du SI ainsi implémentée soit conforme à la cible de sécurité que l'entreprise s'est choisie et aux multiples exigences réglementaires auxquelles elle est soumise.
3. **Détection/Réaction**: Sélection puis mise en place des mesures de sécurité relatives à la surveillance des incidents de sécurité et à leur traitement.
4. **Remédiation/Reconstruction** : Reconstruction de tout ou partie du SI après une attaque réussie.

Les mesures de protections ne peuvent pas être 100% durablement efficaces. En effet, pour des acteurs malveillants, les mesures de sécurité mises en œuvre ne sont que des obstacles retardant leurs progressions. Il est généralement admis que la probabilité de réussite d'une attaque dépend directement de la volonté de l'attaquant, des moyens et du temps dont il dispose.

C'est dans l'objectif de se prémunir des attaques que les mesures de protection n'ont pas été capable de bloquer (signal faible ou fort, inscrite dans le temps ou instantanées, exploitant des vulnérabilités publiquement connues ou inconnues à ce jour) que les SIEM et SOC sont mis en place par un nombre croissant d'organisations.

Historiquement les budgets sécurité étaient principalement affectés à la protection. Il est prévisible qu'une part de plus en plus importante des budgets soit affectée aux dispositifs de détection/réaction, voire même affectée pour partie, à la remédiation / reconstruction

L'indispensable *sponsorship*

Dans le cadre de la mise en œuvre d'un SOC, le sponsoring est nécessaire à « tous les étages » :

- **Raison #1** : La mise en œuvre d'un SOC est une opération d'envergure transverse à l'organisation de l'Entreprise et qui aura des impacts opérationnels. Il faut prévenir les résistances et faciliter/flécher les arbitrages.
- **Raison #2** : La mise en œuvre d'un SOC nécessite un accord explicite de la direction pour sanctuariser les dépenses récurrentes induites par une telle organisation.
- **Raison #3** : En situation de cyber-crise, il peut arriver de devoir prendre des décisions délicates comme la fermeture d'une application critique, d'un serveur ou d'un site web. Seul un soutien fort de la direction permet d'interrompre ainsi le « business ».

5 Les missions d'un SOC

Selon les standards des Systèmes de Management de la Sécurité des S.I. (SMSI), la Politique de Sécurité des SI (PSSI) définit les objectifs SSI de l'Entreprise. Ces objectifs sont généralement justifiés ou adossés à des risques portés par l'Entreprise et à son activité. Le SOC, qui est une mesure de sécurité pour réduire un ou plusieurs de ces risques, contribue à l'atteinte de ces objectifs mais n'est généralement pas décrit dans ce document fondateur. Autrement dit, la mise en œuvre d'un SOC ne nécessite pas la réécriture ou la modification de la PSSI Entreprise.

Cependant, quelle que soit l'organisation retenue, pour être légitime et efficace, le SOC doit avoir une liste de responsabilités correctement définie, attribuée et documentée. Ces responsabilités sont inscrites et documentées dans les procédures de sécurité (directement dérivées de la PSSI). La légitimité des activités du SOC vis-à-vis des autres entités de l'Entreprise est portée par la lettre de mission du SOC signée par le comité exécutif de l'Entreprise (COMEX). Cette lettre précise notamment que le SOC a pour mission de surveiller les événements de sécurité et réagir aux incidents de sécurité du système d'information.

Ces documents (procédure et lettre de mission) peuvent également définir les « partenariats » entre le SOC et d'autres entités capables de soutenir les efforts du SOC (si celui-ci n'est pas omnipotent). Par exemple, il peut être opportun d'indiquer que l'entité en charge de l'exploitation des réseaux peut être sollicitée pour permettre l'intervention sur des équipements filtrants. Les documents de politique indiquent alors les niveaux de priorité des interventions et le cadre des conventions de services entre entités ou équipes.

Le SOC travaille généralement en étroite relation avec les équipes de production pour ses capacités de réaction. Dans d'autres situations, le SOC dispose des moyens d'intervenir sur les équipements de production. Le SOC peut avoir des missions étendues (gestion des identités, habilitations, …).

Si les objectifs de sécurité sont définis au niveau de l'organisation, le consensus en termes de priorités et d'implication est plus facile à atteindre. Documenter clairement les responsabilités de chacun permet également de définir les besoins et les services rendus par un SOC et de communiquer au sein de l'organisation.

Activités d'un SOC

La mission principale d'un SOC consiste à surveiller, détecter, analyser et qualifier les évènements de sécurité. Elle se décline en 3 activités majeures pouvant être gérées indépendamment :

1. **Activité #1** Supervision/Qualification/Alerting ;
2. **Activité #2** Pilotage des incidents de bout en bout ;
3. **Activité #3** (optionnelle) Traitement standardisé d'un incident.

En complément de cette mission principale, le SOC à la charge de conserver les journaux d'activité (ou logs) qui lui sont remontés pour la durée qui a été définie. Cette mission est essentielle pour permettre des analyses inforensiques *à postériori* ainsi que la production de rapports et statistiques à valeur ajoutée.

Le SOC peut également se voir confier des missions additionnelles en fonction des organisations, telles que :

- L'investigation sur incident également appelée inforensique ou forensic ;
- La fourniture d'expertise ponctuelle sur la gestion de crise ;
- La gestion des vulnérabilités ;
- Un rôle de sécurité opérationnelle, au travers du :
    - Paramétrage des équipements de sécurité ;

    - Gestion des identités et habilitations ;
- Le traitement en profondeur des causes racines de l'incident ;
- La sensibilisation des utilisateurs et la communication de la sécurité.

Définition des missions d'un SOC

La définition des missions d'un SOC constitue le socle de tout SOC et doit être portée par le plus haut niveau du management de l'Entreprise. Elle est généralement explicitée par un document fondateur constitué d'une page portant le message du sponsor du projet et d'une seconde page expliquant dans les grandes lignes ses missions.

La définition de ses missions est la pierre angulaire qui permet d'assoir sa légitimité et d'entamer l'amélioration continue en termes de qualité et d'efficacité. Une fois le socle des missions défini, la monté en maturité permettant les transitions d'un modèle de SIEM SOC v1 vers un SOC v2. Ces gains de maturité sont soutenues par :

- L'accompagnement de spécialistes ;
- Le respect de normes ou de modèles IT.

Il convient de régulièrement revoir ces missions au regard de l'amélioration continue du SOC tant au niveau de son efficience que de sa maturité, ainsi que de son adhérence avec le système de gestion de la sécurité (ou SMSI). Cette revue doit obligatoirement tenir compte la gestion et de l'évolution des risques portés par l'Entreprise et doit intégrer la réduction de ces derniers dans ses missions.

Positionnement du SOC dans l'organisation

Il n'existe malheureusement pas de positionnement établi pour un SOC au sein d'une organisation. Il dépend avant tout de celle-ci et de son historique. Néanmoins il convient de prendre en considérations les facteurs suivants pour lui permettre d'effectuer sereinement ses missions :

- Positionnement pour un fort niveau d'autorité lui permettant de faire agir rapidement les différentes parties prenantes ;
- Lien fonctionnel étroit avec le RSSI, pour s'assurer du bon alignement de ses missions avec les objectifs de sécurité de l'Entreprise ;
- Positionnement pour garantir l'indépendance budgétaire pour une préservation des moyens du SOC. Il n'est pas inconcevable d'envisager un rattachement en fonction du détenteur budget.

Autorité d'un SOC

Afin de pouvoir répondre à la question : « Quels sont les pouvoirs nécessaires au SOC pour la réalisation de ses missions ? », il convient de conférer une certaine « autorité » au SOC. Cette « autorité » de fait doit être connue et définie de sorte que, lorsque le SOC besoin de quelque chose, il l'obtienne ou, le cas échéant, il puisse le faire.

Les SOC/CSIRT ne sont pas idéalement placés pour juger des impacts d'une réponse à incidents lorsqu'il s'agit d'une intervention en production. Il est très important que les modèles de réaction impliquent les

métiers. La sécurité dans ces modèles prend une place de « conseil ». D'autres modèles de réaction privilégient la protection du Groupe au regard de la protection d'un métier. L'entité sécurité transverse peut alors prendre l'autorité de réagir en cas d'incident (avec consultation du métier). À l'inverse la sécurité peut, à l'aide de sa connaissance de la menace, relativiser l'incident et éviter la sur-réaction.

Les principes de gestion de risque de l'Entreprise doivent permettre de déterminer l'autorité « limite » attribuée au SOC/CSIRT (le compromis entre la capacité à répondre et les impacts de la réponse).

En plus de sa capacité d'intervention, et en accord avec son périmètre fondateur, le SOC a besoin d'avoir une visibilité sur autant d'activités que possible afin de protéger l'Entreprise sur la plus grande *surface* possible. Notons que cela ne signifie pas que le SOC doit recueillir tout type de journal ou trace à partir de tous les systèmes, mais plutôt qu'il nécessite les journaux des systèmes essentiels (au cœur du SI).

6 La mise en œuvre d'un SOC

[DESIGN] La phase de conception d'un SOC

La plupart des SOC sont construits en réponse à un contexte réglementaire, une contrainte légale ou suite à une prise de conscience du contexte d'insécurité et de menaces ambiant (parfois même en écho à un sinistre passé qui aurait pu être prévenu par un dispositif SOC). Dans ces cas-là, il existe une notion de « temps de réponse » à la menace. Une réponse rapide (*i.e.* la mise en œuvre du SOC) est attendue pour éviter toute compromission de grande ampleur, toute perte de données non maitrisée ou la survenue de tout sinistre majeur sur le S.I.

Comme décrit dans les paragraphes précédents, la mise en place d'un SOC est un projet d'envergure (donc généralement visible et suivi par les instances de direction) sur lequel viennent donc s'ajouter des contraintes de planning relativement fortes. Le SOC doit être mis en place, rendu opérationnel et efficace dès que possible pour pouvoir justifier les investissements (CAPEX/OPEX) et les changements d'organisation.

Ces contraintes de planning rendent difficile l'adoption d'une méthodologie réfléchie et partagée en termes de conception, de choix des outils, de recrutement des compétences *ad-hoc* pour construire et exécuter les services de SOC.

Quelle que soit la méthodologie retenue, la phase de conception/design doit, a minima, traiter les sujets suivants :

- Définition du périmètre technique
    - Outils déjà mis en œuvre et périmètre déjà couvert
    - Procédures techniques existantes (infrastructures, applicatifs, sécurité ou non)
    - Processus organisationnels (gestion de crise, astreintes, escalades, …)
- Définition du périmètre organisationnel
- Définition de l'organisation cible

- Identification des transformations nécessaires dans les équipes ?
- Quelles adhérences avec les activités des équipes IT actuelles ?
- Quelle conduite du changement pour les personnels impactés ?
- Faut-il mettre en œuvre une stratégie d'externalisation ?

Si l'étude de cadrage est le point de départ de tous les travaux, ces réflexions préliminaires sont néanmoins particulièrement importantes et permettent de fédérer les acteurs principaux autours du projet.

L'étude de cadrage

En fonction du périmètre considéré et des activités/organisation de l'entreprise, une première phase de cadrage/opportunité peut être organisée. Les aspects stratégiques tels que l'externalisation peuvent être décidés lors de cette phase.

Tous ces éléments peuvent être discutés préalablement dans des groupes de travail internes déjà existant et relatifs à la SSI. Cependant, l'organisation d'un tel projet (pour une Entreprise, par définition, novice dans le domaine) se révèle généralement complexe et chronophage. La recommandation est alors de ne pas hésiter à se faire accompagner par une assistance à maitrise d'ouvrage pour cadrer les débats et préconiser les solutions techniques et organisationnelles pour faire avancer le projet.

La première étape est d'exprimer le besoin de mise en œuvre du SOC et de fixer ses objectifs :

- Pourquoi un SOC pour l'Entreprise ?
- Faut-il un unique SOC ou plusieurs SOC (un dans chaque branche/domaine/entité) ?
- Tout le périmètre doit-il être couvert ? Faut-il se concentrer sur certains périmètres sensibles ?
- Quelles sont les activités opérationnelles en plus de la supervision confiées au SOC ?
- Quelles sont les technologies utilisées et pressentie pour outiller le SOC ?
- Faut-il externaliser le service SOC ou l'internaliser ?
- Faut-il conduire un POC ou construire le SOC ex-nihilo ?

L'étude de cadrage est également l'occasion de répondre et de contrôler les prérequis :

- Existence d'une ou plusieurs PSSI accompagnée de directives de sécurité.
- L'identification des principaux risques et des menaces associées
- La mise en œuvre des mesures de sécurité de base (hygiène SSI).

La seconde étape de l'étude de cadrage se concentre sur les besoins SSI couverts par le SOC :

- Liste des « *use cases* » standards portés par le SOC
- Construction des scénarios de menaces métiers à couvrir
- Etude Spire ou autres analyses de risques
- Quel temps de rétention des différentes traces collectées ?

Une fois les besoins évalués, l'étude de cadrage se focalise sur la compatibilité technique et organisationnelle du S.I. existant avec la mise en œuvre d'un SOC. Les éléments suivants viennent donc compléter l'étude de cadrage :

- Revue de l'architecture sécurisée existante
- Existence et disposition des serveurs de temps
- Gestion des journaux d'événements et périmètre de collecte
- Volumétrie des journaux actuellement collectés / Durée de rétention.
- Vérification de la politique des logs (verbosité, chiffrement, signature)

D'un point de vue organisationnel, cette dernière partie de l'étude de cadrage se concentre sur :

- L'organisation du projet (RACI)
- La définition du périmètre métier adressé et couvert par le SOC (cf. première étape)
- Définition du socle de base des équipements supervisés :
    - Passerelles internet et de messagerie
    - Système de détection/prévention d'intrusions (IDS/IPS) de flux et de postes
    - Active Directory (et annuaires d'entreprises)
    - Anti-virus de flux et de poste

En plus de la discussion de tous ces éléments, l'étude de cadrage peut conclure sur l'identification d'actions prioritaires et rapides à mettre en œuvre ou de petits périmètres prioritaires (« *quick-wins* ») pour que les premiers jalons puissent être identifiés et suivis par les sponsors du projet. L'objectif est de construire sur le périmètre de l'Entreprise la « *success story* » décrite dans le paragraphe 4.

Qualification et certifications d'un SOC

La qualification et la certification d'un SOC vis-à-vis des différents standards en vigueur est un chantier particulièrement chronophage et très complexe à mettre en œuvre dès l'initiation du chantier. L'ajout des contraintes propres à ces référentiels dès la conception du SOC peut alourdir exagérément le cahier des charges et mettre en péril le projet.

Comme dans tout projet, la certification n'est pas un objectif en soi mais une cible, un gage de maturité et de savoir-faire. La certification/qualification ne protège pas mais « (r)assure » en fournissant un moyen à l'Entreprise porteuse du SOC de se « retourner » vers l'entité de qualification/certification en cas de problème.

Sauf cas particulier (cf. ci-dessous), nous recommandons dans un premier temps une approche plus agile, permettant un gain en maturité de toute l'équipe et de l'organisation complète. A noter que la démarche est cependant obligatoire pour les OIV souhaitant héberger leur SOC en interne et traitant des journaux générés par les sondes qualifiées ANSSI. (cf. LPM / PDIS).

Périmètre organisationnel

Les aspects organisationnels traités pendant la phase de conception concernent à la fois l'organisation de l'équipe de construction et d'exécution mais aussi les autres entités qui doivent être mobilisées pour la conduite du projet (pendant la phase de construction mais aussi pendant la phase d'exécution).

Le « noyau » de l'équipe du SOC et les principaux interlocuteurs du service doivent être identifiés fonctionnellement et nominativement. Généralement, ces acteurs sont :

- Le/les DSI
- Le/les RSSI
- Le/les responsables des risques & de l'audit
- Le/les architectes réseaux/système
- Le/les responsable du SOC
- Le/les responsables d'équipe opérationnelle
- Les analystes

En plus de l'identification précise des acteurs concernés par le projet, la conception doit proposer au moins **une trajectoire** de mise en place d'un SOC :

- périmètre technique et métier couvert,
- volumétrie collectée et traitée,
- agilité dans la supervision et la réaction,
- montée en efficacité.

Cette trajectoire, doit notamment permettre de convaincre et de justifier les investissements tout en fournissant une feuille de route pour les prochains mois/années d'activités du service.

La phase de conception est également le moment le plus indiqué pour communiquer auprès des équipes techniques et métier.

- Pour les personnels de l'IT, il faut communiquer sur l'évolution de l'organisation induite par la mise en œuvre d'un tel service. L'idée principale de cette communication est que : la mise en œuvre d'un SOC ne doit pas être vécue par les personnels de l'IT comme une perte de contrôle ou une observation à charge des opérations des équipes IT mais comme un complément et une aide.
- Pour les personnels métiers, et en fonction des RACI discutés pendant les ateliers de conception, il faut communiquer sur l'arrivée de ce nouvel acteur et sur les nouveaux circuits de communication (ou sur les modifications à venir). Là encore, le SOC ne doit pas être perçu comme un observateur à charge mais bien comme une aide complémentaire dans la supervision des activités.

Un projet de SOC de par sa nature de « transformation des activités » génère des frictions et des adhérences fortes avec les activités courantes. La communication est le remède et le catalyseur qui limite ces frictions.

Périmètre technique

La conception technique du SOC doit se concentrer sur le choix des outils et/ou du contrat en fonction des équipements à surveiller. La collecte et les opérations de supervision doivent être considérées dans cette étude de conception.

Pour la collecte, la base du travail de conception est d'identifier et de localiser les outils déjà mis en œuvre sur le S.I. : IDS/IPS, pare-feu, détection de fuite de données, boitiers de chiffrement, antivirus, anti-spam, contrôles d'accès et d'identité… Chaque outil doit être associé à son/ses responsables et aux objectifs de sécurité poursuivis.

En fonction de l'existant, les travaux de conception doivent identifier les outils manquants en qualité ou en quantité pour couvrir le périmètre. Conformément à la trajectoire discutée dans la conception organisationnelle (cf. paragraphe précédent), ces outils peuvent être inscrits sur une feuille de route pour les futures évolutions du service.

Pour chacun des outils identifiés, la granularité des événements journalisés doit être adaptée à la capacité de détection. L'écueil à éviter à tout prix est de noyer les opérateurs dans un volume d'événements trop important et non pertinent compte tenu des cas d'utilisation et des objectifs du SOC.

Dans les cas où les scénarios de menaces justifient l'enregistrement d'une grande quantité d'événements, les outils propres aux opérations de supervision (cf. ci-dessous) doivent alors être choisis en pleine connaissance de cause.

Pour les opérations de supervision, l'étude de conception doit permettre de choisir l'outil majeur et les outils satellites permettant de recevoir, trier, qualifier/prioriser, suivre et traiter les incidents de sécurité. Ces outils doivent être adaptables et paramétrable par rapport aux contraintes de l'Entreprise. Sont notamment à prendre en compte :

- Compatibilité avec le ou les SIEM mis en œuvre ;
- Capacité à prioriser les incidents en rapport avec les échelles gravité/impact de l'Entreprise ;
- Adaptabilité des circuits d'escalade et de communication ;
- Echange et interactions avec d'autres SOC (entités de sécurité de l'Entreprise)

Pour faciliter les opérations de supervision, la liste des actifs critiques de l'Entreprise (serveurs, bases de données, annuaires, …) peut être constituée si elle n'existe pas déjà. Cette identification peut être pilotée/validée par les métiers en fonction de leur propre gestion des risques.

L'organisation interne du SOC pour la gestion d'incidents

En complément des aspects organisationnels et techniques décrits dans les paragraphes précédents, la phase de conception permet également de structurer les moyens humains mis à disposition en différents niveaux et de préciser les flux de traitement :

L'attaque est connue

Une règle de corrélation est déjà implantée dans le SIEM.

- Niveau 1 (alerté par les outils de détection) : L'équipe acquitte et qualifie l'alarme selon une procédure déterminée. L'équipe traite les alarmes connues et escalade tous les sujets non documentés (ou documentés comme devant être escaladés).

- Niveau 2 (sollicité par le niveau 1) : L'équipe traite l'incident escaladé par le niveau 1 et rédige des procédures de traitement pour le niveau 1 (objectif : transfert de ses activités au niveau 1 en les industrialisant). L'équipe participe à l'amélioration et à l'enrichissement des règles de corrélation.

- Niveau 3 (sollicité par le niveau 2) : L'équipe fournit une très forte expertise au niveau 2. Selon l'organisation de l'Entreprise cette mission peut être prise en charge par un CSIRT.

L'attaque n'est pas connue

- Les niveaux 1 et 2 ne sont pas alertés par les outils de détection du SOC
- Niveau 3 : L'équipe réalise une veille active sur les menaces et vulnérabilités en relation avec le CERT. Elle recherche les événements anormaux et/ou atypiques dans les entrepôts de logs. Ils ont une approche proactive (ils partent du postulat que le SI de l'Entreprise est cours de compromission).

  Ils chassent et traquent les indices de comportements anormaux et les signaux faibles (i.e. comportements atypiques). Ils utilisent de plus en plus des outils de type BigData pour faire de l'analyse prédictive. En outre, ils disposent d'un outillage spécialisé (ex. sandboxing pour l'analyse de malware), varié (réseau, système, middleware, applicatifs, …) et parfois développé en interne.

  Le niveau 3 est la principale source d'enrichissement des règles du SIEM. A défaut, un retour d'expérience sur l'évènement est attendu de leur part.

Ces différents niveaux sont encadrés par le responsable du SOC qui a pour principales missions :

- Organiser et piloter la charge des équipes (niveau 1, 2 et 3) en cohérence avec les missions du SOC dont le responsable du SOC est garant.
- Veiller aux engagements de service du SOC : détection, traitement de bout en bout, …
- Rapporter aux instances de pilotage qui veillent à l'adéquation des moyens et des résultats par rapport à ses missions.

Les différents modèles de SOC

Il existe principalement deux grandes familles de SOC :

1. Les SOC opérés en interne
2. Les SOC externalisés

Même s'il existe des modèles hybrides, le choix d'un type de SOC est capital lors des études de conception car cela conditionne la nature des travaux et du pilotage pendant la phase de construction. Les paragraphes suivants décrivent les avantages et les inconvénients de chacun des types de service.

L'évolution d'un modèle de SOC à un autre est naturellement envisageable mais nécessite une préparation et une anticipation importante pour éviter de devoir reconduire tous les travaux de conception et de construction lors de la bascule de l'un à l'autre des modèles. Ce changement de nature peut être justifié par l'atteinte d'un certain niveau de maturité par l'Entreprise et/ou l'évolution des objectifs de sécurité ou bien encore un changement de stratégie au niveau de la DSI ou de l'Entreprise.

SOC dédiés / internalisés

Avantages	Inconvénients
• Les SOC dédiés disposent de ressources humaines dédiées, organisées et en capacité de traiter toutes les alarmes reçues par les outils de collecte • Les équipes du service connaissent mieux les infrastructures et les applications supervisées et sont donc à même de qualifier plus efficacement les alarmes remontées. • Les solutions/outils dédiées sont plus flexibles et plus facilement paramétrables. Les scénarios de menaces et les objectifs de sécurité sont considérés de façon précise. • La communication (investigation) et l'escalade sont plus rapides (puisque utilisant les outils de communication de l'Entreprise) • Les journaux d'événements et tous les éléments de suivi des alarmes et incidents sont tous stockés en interne.	• L'investissement financier initial est très important (pour mettre en œuvre l'outillage, recruter et former les ressources, conduire les études et exécuter la réalisation). • De fait, la pression pour être en capacité de montrer le ROI d'un tel service est également très importante. • Le recrutement d'analyste SOC et d'expert en sécurité est un véritable défi et peut prendre un certain temps. • Le maintien en compétence et la gestion de carrière doivent être soigneusement considéré pour ne pas perdre rapidement toutes ses compétences internes. • Le risque d'entente entre des acteurs malveillants et des opérateurs du service SOC est plus important que dans le cas d'un service externalisé. • Les attaques large échelle, ciblant ou ayant ciblées, plusieurs autres Entreprises ne seront sans doute pas perçues par un SOC focalisé sur la supervision d'un périmètre interne

Fournisseur de services de sécurité (MSSP)

Avantages	Inconvénients
• L'investissement initial est plus raisonnable tant sur le plan technique qu'humain. • Le service est généralement proposé à	• Les opérateurs distants ne connaitront jamais aussi bien les infrastructures et applicatifs que des opérateurs agissant au sein de l'Entreprise. • L'externalisation d'un service de sécurité

plusieurs acteurs du même domaine. Ceux-ci bénéficient de fait de l'expertise des analystes pour le secteur d'activité concerné. • La mutualisation des couts opérés par les acteurs MSSP leur permet de proposer des modèles de SOC moins chers que les versions internalisées. • L'entente entre un acteur malveillant et un opérateur du SOC est moins probable car ces derniers sont moins exposés. • Il n'y a pas de limite à la croissance forte et soutenue du modèle (sous réserve de capacité du MSSP). • Le MSSP met tout en œuvre pour se doter des expertises les plus pointues sur les outils de collecte et de traitement.	essentiel comme le SOC peut avoir un impact négatif sur le « moral » des personnels IT de l'Entreprise • Sans contrat spécifique, les ressources du MSSP peuvent être mutualisées avec d'autres acteurs parfois concurrents • Les données internes de l'Entreprise sont envoyés à l'extérieur sans contrôle possible a priori. Une erreur de manipulation est tout à fait probable. • Toutes les données ne sont pas systématiquement archivées (sauf cadre contractuel particulier) • Le service fourni par un MSSP est plus difficilement paramétrable et ajustable aux réels besoins de sécurité et aux scénarios de menaces. Les approches sont généralement standard (tout en étant précise et efficace). • La clause de réversibilité doit être étudiée avec soin pour permettre de changer d'acteurs/opérateur en cours ou en fin de contrat.

SOC hybrides

Dans certains cas, les deux modèles peuvent être intégrés l'un à l'autre pour produire un SOC hybride. Le partage entre les deux modèles est réalisé selon :

- Le périmètre de collecte : certains périmètre sensibles/confidentiels sont traités en interne pendant que tous les autres périmètres sont laissés à la charge du MSSP. Dans le cas de Groupes qui opèrent plusieurs entités quasi-autonomes sur un territoire géographique important, certaines d'entre elles peuvent avoir fait le choix de faire appel à un MSSP alors que d'autres continuent d'opérer le service SOC en interne.
- Le niveau de traitement : la qualification et le traitement des alarmes les plus mineures peuvent être déléguées à un MSSP tout en gardant les escalades de niveau 3 et l'investigation sous la responsabilité d'une équipe interne.

Lors du choix d'un modèle de SOC, la pérennité du modèle pour l'Entreprise doit être étudiée et largement commentée. En termes d'investissement, la mise en œuvre d'un SOC est un projet d'envergure qui s'inscrit sur plusieurs années. Même si l'Entreprise choisi de faire appel à un MSSP, elle se retrouve généralement engagée sur de longues périodes rendant ainsi compliquée toute bascule vers un modèle internalisé.

De l'intérêt de conduire un POC

Quelle que soit l'approche organisationnelle et technique retenue, la conduite d'un « Proof of Concept » (PoC) sur un sous-périmètre représentatif permet de confirmer les hypothèses construites lors de la phase de cadrage et de conception et de préparer les différents acteurs opérationnels à mieux comprendre les conséquences de la présence d'un SOC au quotidien.

Comme tout démonstrateur, la finalité (objectifs et résultats attendus) du POC doit être clairement définie en amont de tout travail d'implémentation. L'objectif du POC est de travailler sur des cas d'utilisation concrets et simples (ex. « Sait-on gérer une alerte du SOC indiquant que 25% des collaborateurs ont activé un malware rendant inopérant le poste de travail ? »). Le POC n'est ni le lieu, ni le bon moment pour essayer de détecter des cas d'utilisation complexes et/ou à la marge (bien que mettant en danger l'intégrité du S.I. de l'Entreprise).

Le POC doit permettre de :

- valider les prérequis techniques :
    - collecte des traces,
    - horodatages des événements,
    - circulation de l'information
- valider les prérequis organisationnels :
    - circuit d'escalade
    - astreintes techniques/métiers
    - application des procédures/processus de gestion d'incidents et de crise
- valider les outils choisis pour l'opération du SOC en interne ;
- valider la capacité de l'Entreprise à traiter à une alerte de sécurité.

Dans le cas d'une organisation déléguée à un MSSP, les objectifs du POC peuvent être :

- juger de la capacité du MSSP à s'intégrer/prendre en compte le périmètre de l'Entreprise ;
- juger de la capacité du MSSP à réagir (valider les aspects organisationnels inter-entités) ;
- juger de la capacité de l'Entreprise à réagir face aux alertes remontées par le SOC.

A l'issue de ce POC, une conclusion potentielle peut être de retarder la mise en œuvre d'un SOC en se concentrant dans un premier temps sur la mise en place des fondamentaux de la sécurité dans l'Entreprise (cf. Guide ANSSI). Une autre conclusion peut être de se concentrer sur la satisfaction de prérequis techniques.

Création d'un SOC ex-nihilo

Si, à l'issue de l'étude de cadrage, la décision est de procéder à la construction d'un SOC de toute part sans passer par l'étape du démonstrateur, nous recommandons à minima de s'appuyer sur des compétences en MOA expertes dans le domaine.

Les prérequis indispensables à la mise en œuvre d'un SOC restent :

- L'étude de cadrage ;
- La capacité (technique, réglementaire et contractuelle) de collecter, de stocker et d'interpréter les logs collectés sur le périmètre concerné ;
- La garantie de la bonne intégration du SOC avec les processus IT de l'Entreprise

La construction du SOC peut être lotie et suivre l'une des deux stratégies suivantes :

- 1ère possibilité : Faire appel à un SOC externe (MSSP) pour monter rapidement en maturité ;
- 2ème possibilité : Opérer un SOC interne sur un petit périmètre critique métier.

[BUILD] La phase de construction d'un SOC

La phase de construction ne marque pas la fin des communications avec les instances dirigeantes. Il est nécessaire de poursuivre les ateliers de sensibilisation et de continuer à convaincre de l'utilité et de la pertinence du SOC. En conséquence, il faut se doter de la bonne personne pour piloter la construction et poursuivre les « négociations » avec les parties prenantes. La construction n'est pas uniquement technique.

La construction se concentre dans un premier temps sur la collecte et le traitement des événements existant. Il s'agit du socle primaire. Sa construction est séquentielle :

- Collecte des journaux d'événements (déjà concentré une première fois par le SIEM)
- Construction des scénarios de corrélation et implémentation dans le SIEM
- Alimentation du SOC en événements et résultats des corrélations.

En complément de ce socle, la construction considère :

- L'identification des profils des opérateurs/acteurs du SOC
- Les moyens de réaction
- Elaboration de scénarios de menaces et des priorités de traitement
- Pilotage du niveau de sensibilité (pour améliorer la qualité de l'alerte)

Dans le cadre de mise en œuvre de SOC dans un contexte multi-entités, des activités complémentaires propres aux échanges d'informations et processus de collaboration peuvent être nécessaires. Encore une fois, ces activités s'inscrivent après la construction du socle primaire. Dans ces cas-là, il convient également de déterminer :

- la localisation du stockage des événements,
- l'entité qui porte les consoles de gestion des alarmes,
- et, plus globalement, de distribuer les rôles et les responsabilités.

Collecte

La construction du système de collecte est une activité très dépendante de la technologie (des éléments collectés et des solutions de collecte elles-mêmes). Des prérequis techniques parfois complexes à

mettre en œuvre (tels que l'horodatage synchronisé de tous les événements) doivent avoir été vus et discutés en phase de conception technique.

Dans le cadre de la mise en œuvre d'un SOC, la collecte des données doit être réalisée dans l'objectif d'alimenter le service de supervision. Les événements doivent ainsi être formatés pour être exploitables – il faut donc généralement les adapter pour les rendre compatibles avec les objectifs de sécurité du SOC (notez que le SIEM est généralement déployé bien avant les études ou la mise en œuvre d'un SOC dans l'Entreprise).

Dans un premier temps, la collecte concerne :

- les équipements de sécurité
- les applications
- les équipements réseaux

Déployer la collecte sur un périmètre complet est un projet ambitieux.

Compte tenu de la difficulté de la mission, la gestion de projet doit éviter à tout prix l' « effet tunnel » en privilégiant les « mini-succès ». Ce lotissement peut s'appuyer sur les besoins de détection exprimé dans le cadrage du SOC (identification des scénarios de menace, identification des sources concernées par les scénarios d'attaque, collecte des événements permettant la détection du scénario).

En complément de la collecte, le projet doit veiller à :

- la normalisation des événements collectés pour permettre leur exploitation ;
- le stockage des événements collectés (dans le respect des contraintes réglementaires) ;
    - en tenant compte de la localisation du stockage
- l'archivage des événements collectés.
    - en tenant compte des obligations de non-répudiation et d'intégrité des données

Traitement

Le traitement a pour objectif de s'attacher à la détection des risques les plus redoutés par la structure. Ceux-ci sont généralement connus via les analyses de risques cyber dont va découler la priorité d'analyse. Le traitement des événements de sécurité est conditionné par les scénarios d'infrastructures et métiers.

Les scénarios d'infrastructures visent à définir les règles de bases liées aux événements produits par les systèmes d'infrastructure et plus particulièrement par les équipements de sécurité. Ces règles sont dites « events driven securtiy » ce qui implique que les équipements d'infrastructure produisent des événements de sécurité. Ces règles sont indispensables pour le traitement mais produisent un nombre de faux positif important et nécessitent un travail de qualification important.

Pour compléter l'efficacité du SOC et réduire le nombre de faux positifs, il est nécessaire de créer des scénarios métiers qui s'appuient sur des règles de corrélation issues des applications métiers et des règles d'infrastructure. Les scénarios métiers sont conçus spécifiquement pour le secteur d'activité dont le SOC est en charge. La détection d'événements métier est appelée « data driven security », l'objectif

est d'analyser les informations issues des applications et pas simplement de l'infrastructure. L'objectif des personnes malveillantes n'est pas de passer les systèmes de sécurité liés à l'infrastructure mais les données qui elles sont hébergées sur les applications. Les scénarios métiers ne produisent qu'un nombre très faible de faux positif, qui augmente l'efficacité globale du SOC tout en augmentant l'implication des métiers dans le système de défense global.

La conception des règles de corrélations d'infrastructures et métiers et un poste central du dispositif du SOC. Suivant la taille de la structure, une « usine à corrélation » est mise en place. Celle-ci est composée d'un poste pour la conception des règles d'infrastructure en masse et un poste pour la conception des règles métiers qui va être alimenté par les règles d'infrastructure, les informations sur les métiers, les analyses inforensiques et le « *threat intelligence* ».

Cependant il est primordial de mettre en place un processus de gestion des règles qui permet de s'assurer du suivi de l'efficacité de la détection.

Ce processus aborde les points suivants :

- Identifications du besoin de détection
- Conception de la règle
- Test, validation et mise en production de la règle
- Vérification hebdomadaire de l'efficacité de la règle
- Ajustement et enrichissement de la règle
- Identification des axes d'amélioration de la règle
- Modification de la règle

Le traitement des règles se doit d'être un processus industriel afin de s'assurer qu'aucune menace ne soit oubliée. Le processus de traitement est basé sur la norme ISO 27035 (gestion des incidents de sécurité d'un SOC) et sur les indicateurs ETSI GS ISI pour la définition qualifications et la définition des KPSI.

La structure de traitement est décomposée en niveaux 1/2/3. L'intérêt de ces niveaux est de s'assurer que tous les incidents sont traités par les personnes les plus compétentes sur le sujet. Ainsi le niveau 1 va traiter les incidents les plus simples et déclencher le N2 sur les incidents plus compliqués. Le N3 intervient sur les incidents complexes. Le passage d'un niveau à l'autre est appelé processus de triage.

Le processus de triage est basée sur le temps de traitement d'un incident, de sa complexité ainsi que de sa criticité. L'objectif du triage est d'adresser les incidents aux personnes les plus compétentes pour les gérer et cela dans les meilleurs délais.

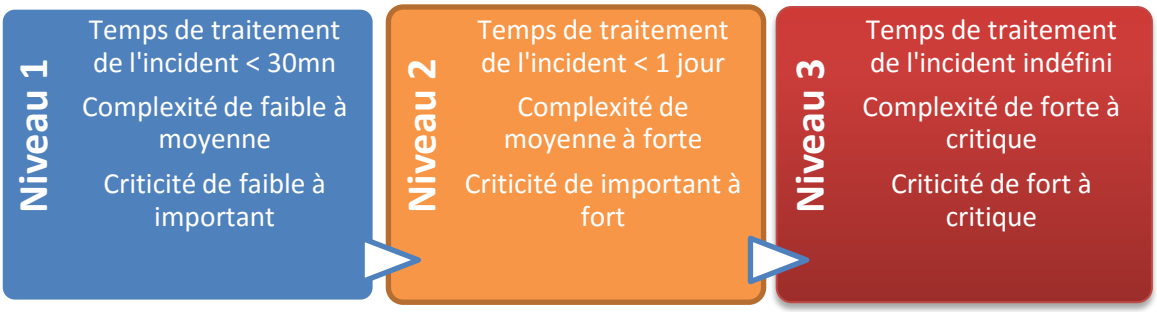


Figure 4 Indicateurs de triage

Le SOC apporte une protection inégale suivant les types de menaces. En ce qui concerne la fuite d'informations, la compromission de systèmes, la protection contre les malwares, les APT et les menaces ciblées, le SOC reste la meilleure des solutions pour la cyber-protection. Cependant les attaques de type DDOS sont détectées mais leur arrêt est dépendant d'élément actif d'infrastructure au niveau des opérateurs et des équipements d'infrastructures périphériques. Dans ce cas le SOC peut fournir des statistiques, des tendances et des analyses d'impacts pour affiner les besoins en moyen de protection anti-DDOS.

Au niveau de la détection, le SOC est efficace en fonction des moyens qui sont mis à sa disposition.

Le niveau de traitement est le suivant :

- Recherche par mot clé
  - Nécessaire pour l'investigation de problème en cas de dysfonctionnement (*root cause analysis)*
  - Peux efficace sur la détection des incidents de sécurité
  - Beaucoup de faux positif
- Règles d'infrastructure
  - Nécessaire pour la détection des incidents d'infrastructure (signaux forts)
  - Détection en temps réel
  - Basé sur les logs
  - Protection de l'infrastructure
  - Beaucoup de faux positifs
  - Pas de traitement des règles métiers (signaux faibles)
  - Principales menaces détectées : Virus, malwares, DDOS, phishing
  - Event driven security (Evénements de sécurité, IOC)
- Règles métiers
  - Nécessaire pour la détection des incidents métiers
  - Détection en temps réel et en temps différés
  - Peu de faux positifs
  - Basé sur les logs, les paquets, les analyses comportementales et prédictives
  - Principales menaces détectées : APT, fuite d'information, attaques ciblées, fraude et attaques internes.

- Data driven security (analytics)

Communications

Objectif des communications du SOC (reporting global/local) :

- Garder l'intérêt et le sponsorship de la direction
- Préserver le budget voire augmenter le budget de la SSI
- Suivre l'évolution de l'état de la menace
- Proposer des évolutions des dispositifs et processus de sécurité

S'appuyer sur des *Success stories* : Communication à la direction sur les attaques détectées et qui auraient pu porter préjudice majeur à l'Entreprise. Consolider ces détections dans un rapport d'activité du SOC.

Transition BUILD > RUN

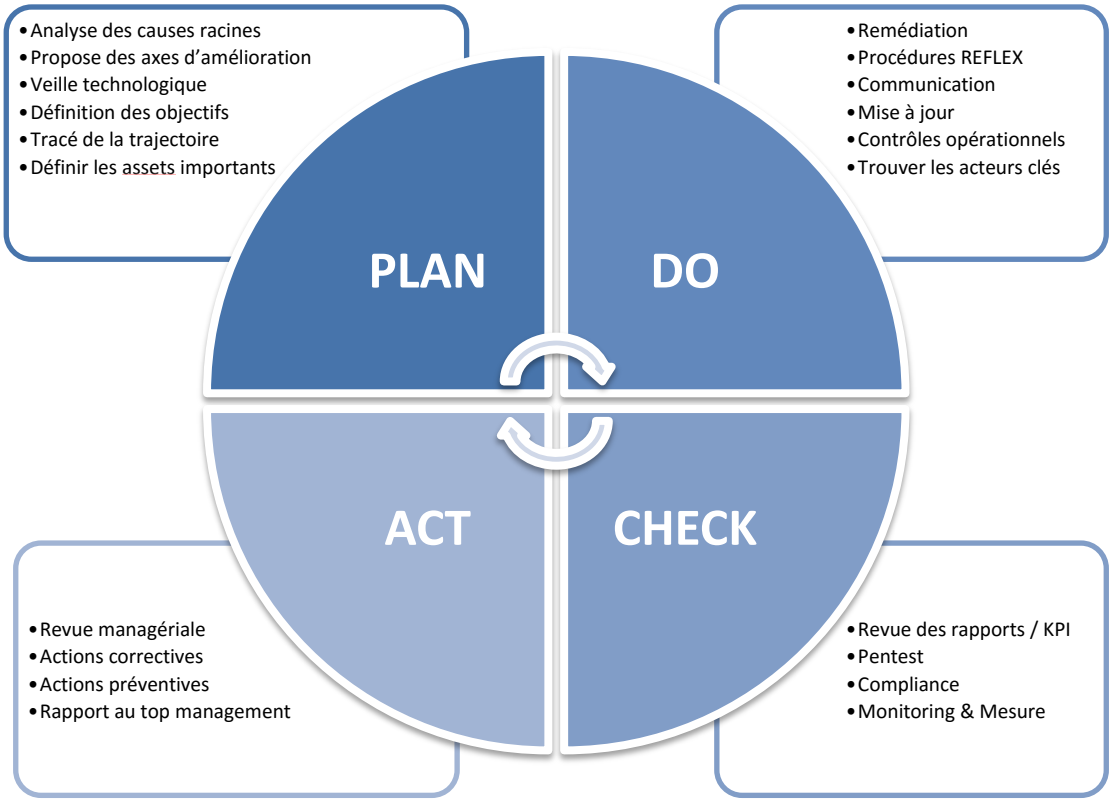
1ère idée : Industrialisation des processus et des techniques (phase de transition à proprement parler). Y compris du passage de compétences.

2ème idée : Accès aux référentiels de l'entreprise (en agrégeant tout ou partie des référentiels de l'entreprise CMDB + bases de vulnérabilités + référentiel RH = concept de datawarehouse au niveau du SOC). Objectif : la priorisation du traitement des incidents sur les assets critiques.

[RUN] La phase de fonctionnement nominal pérenne d'un SOC

Un SOC, comme tout outil de sécurité, doit s'inscrire dans la roue vertueuse de Deming (ou PDCA : Plan Do Check Act). Pour ce faire il convient de prendre en compte le processus métier de gestion des incidents de sécurité. En effet la frontière entre le SOC et le CSIRT étant fortement poreuse et dépendante des organisations, l'exercice d'entreprendre deux roues de Deming indépendantes s'avère fort périlleux de par le risque de conflit dans les cibles à atteindre.

Le schéma ci-dessous illustre une roue de Deming prenant en compte ces différents aspects.



Bien que la mission première du processus d'amélioration continue reste le maintien en conditions opérationnelles du SOC par rapport aux objectifs de sécurité qu'il remplit, il doit également veiller à maintenir sa capacité à :

- Établir sa gouvernance propre en étant capable de s'autoévaluer et d'être une force de proposition quant à l'élargissement de son périmètre. Le dernier point est un élément clé de la viabilité de ce dernier, d'autant plus que pour des raisons pratiques son périmètre est souvent minimal au début ;
- S'assurer de la bonne correction des vulnérabilités détectées pour que la réponse aux incidents demeure pérenne. En effet le SOC est malheureusement souvent utilisé comme un moyen de détection en aval et plus rarement comme un moyen de prévention en amont, ce qui a pour effet de provoquer la lassitude des équipes et accrois le risque de faux négatifs (attaque réelle qui n'aurait pas été détectée) ;
- Revoir la priorisation des incidents de sécurité qu'il remonte, notamment au travers de sa connaissance du système d'information et de ses assets sensibles ;
- Maintenir sa basse de connaissance propre à jour en lien avec la gestion des ressources ;
- Susciter « l'appétit » du top management et de son sponsor pour sanctuariser les dépenses budgétaires de son organisation.

Le maintien en conditions opérationnelles s'effectue quant à lui, par le contrôle de la qualité des informations qui lui sont remontées et celui de celles qu'il transmet. Pour ce faire, il convient à minima de :

- Maintenir à jour et effectuer les montés de versions des équipements remontant des informations au SOC. Ces opérations sur les équipements doivent garantir le maintien de la qualité des événements versés dans les journaux transmis ;
- S'assurer de l'implication continue du métier dans la définition et la mise à jour des procédures de réaction. Le métier est un élément nécessaire dans la qualification de l'intervention à effectuer, et son implication continue permet également de mieux le sensibiliser aux problématiques de la réponse à incident ;
- Être informé des changements majeurs opéré sur le système d'information, au risque de voir un changement non répertorié provoquer un accroissement des incidents et une saturation des équipes ;
- Trouver et maintenir le bon équilibre entre les différents niveaux de support du SOC. Cette tâche avec la suivante (le maintien des compétences) sont les plus difficiles et demeurent extrêmes liées. Un mauvais équilibre entre le support de Niveau 1 et de Niveau 2 peut soit entrainer une surcharge du Niveau 2, qui impliquera une saturation de ce dernier et fort risque de lassitude du Niveau 1 et entrainer une fuite des ressources compétentes, soit une saturation du Niveau 1 qui le rendra inefficace à terme. Malheureusement il n'existe pas de recette miracle pour maintenir un tel équilibre, notons néanmoins quelques initiatives visant à fluidifier les échanges inter-niveaux :
    - Revoir régulièrement les rôles de chaque niveau et les fiches de postes associées pour les valoriser ;
    - Mixer régulièrement les équipes. Une société n'hésite pas à demander à ses supports de Niveau 2 et 3 d'effectuer une journée par semaine de support de Niveau 1. Cette initiative, certes couteuse, offre l'avantage intéressant d'illustrer aux différents supports les problèmes quotidiens du Niveau 1 et de permettre d'améliorer leurs procédures opérationnelles ;
- Maintenir la compétence humaine qui est le fondement de tout SOC. Cette tâche, comme la précédente, n'est pas aisée et ne dispose malheureusement pas de règles établies. Il existe néanmoins plusieurs initiatives dont celles qui suivent :
    - Trouver un leader de SOC charismatique qui soit à la fois un bon manager et « geek » ;
    - Permettre aux équipes de travailler sur des projets une journée par semaine ou quelques semaines réparties dans l'année ;
    - Gérer finement les carrières et les profils, notamment pour les SOCs opérants en 24/7, pour offrir des perspectives d'évolution aux différentes équipes ;
- Surveiller le taux d'alertes pour éviter une saturation du SOC et la constitution d'un reste à faire trop important (backlog). Pour ce faire un SOC doit rester agile et capable de modifier, en en mesurant les impacts sur les objectifs de sécurité, les seuils déclencheurs des alertes ;

- Favoriser l'industrialisation des processus (automatisation des taches à faible valeur ajoutée), pour permettre aux équipes de se concentrer sur l'analyse des alertes et la remonté d'informations pertinentes ;
- Maintenir en place l'outil de gestion des tickets d'incident de sécurité qui contrairement à son homologue sur les incidents de production, doit avoir des accès restreints. Par ailleurs, les bonnes pratiques actuelles conseillent fortement de maintenir ces deux outils séparés.

En supplément de son maintien en conditions opérationnelles et de son amélioration continue, le SOC est en passe de devenir hyper-communiquant au sein et à l'extérieur de nos organisations. En effet, il doit :

- Échanger en interne avec les autres entités sécurité (RSSI, CERT, Soc Manager, …) ;
- Faire de la veille technologique et rester à niveau sur l'état de l'art de la menace, notamment en participant à des colloques d'échanges ;
- Partager la menace au travers des échanges inter CERT et s'enrichir des retours.

Maintenir le fonctionnement nominal d'un SOC et le pérenniser est une tâche complexe et importante qu'il faut prendre en compte dès la conception du SOC. Elle doit être portée par une volonté managériale forte sous l'exécution d'un manager fort et proche de ses équipes pour pouvoir être réalisée dans des conditions optimales.

7 L' « humain » au centre du SOC

Culture et compétences

Les sujets et données traités par les intervenants d'un SOC sont par définition sensibles. Encore plus que tout administrateur de systèmes, les analystes sont au contact des malveillances internes comme externes, comportements anormaux et faiblesses du SI de l'Entreprise. Il est attendu de la part de ces acteurs un **sens éthique** appuyé. En complément d'un circuit de recrutement adapté (contrôles pré-embauches et clauses spécifiques insérées dans le contrat de travail), il pourra être demandé de signer une charte d'engagement éthique.

Maintenir les compétences d'un SOC constitue un vrai challenge. Comment conserver les ressources ? Comment valoriser et promouvoir ses métiers ? Quels plans de carrière pour ces profils ?

Gestion des compétences

Dans le but de retenir les compétences dans l'équipe SOC, il est essentiel de pouvoir offrir des perspectives d'évolution de carrière dès leur embauche.

Par exemple, plutôt que de recruter des analystes de niveau 2, il est préférable de faire jouer les montées en compétence. Il peut être offert des perspectives d'évolution d'analyste niveau 1, vers les niveaux 2 et 3, puis vers le poste de responsable d'équipe SOC

Une autre approche plus radicale celle-là, consiste à faire appel à un prestataire MSSP pour s'affranchir de ces aspects RH.

Profils

Analystes (niveaux 1 et 2)

L'état d'esprit des analystes est souvent comparé à celui de chasseurs qui trouvent une grande part de leurs motivations dans la traque des attaquants et dans l'investigation.

Les analystes interprètent les événements de sécurité, écoutent le « bruit de fond » et traitent les alertes et les incidents. Selon la taille du SOC, les analystes sont organisés en niveaux à l'image d'un centre de support. Ainsi les analystes de niveau 1 dégrossissent et pré-qualifient les alertes, appels, tickets. Leur première tâche consiste à formaliser et enregistrer le contexte de l'incident. Les activités sont majoritairement cadrées par des procédures et tout écart donne systématiquement lieu à une escalade vers le niveau 2. Leurs principales activités peuvent être classées en 3 parties :

1. **Analyse et interprétation des différentes remontées des alertes issues du centre de supervision**
    - Analyse de logs de sécurité issus du SIEM
    - Analyse flux réseaux issus du SIEM
    - Mise en place de règles de corrélation pour la détection
    - Gestion d'incidents de sécurité
2. **Veille**
    - Menaces
    - Vulnérabilités
    - Rédaction de bulletins d'alertes
3. **Reporting et documentation**
    - Participation à la rédaction de rapports de suivis d'activités
    - Participation au fond documentaire du SOC

Les analystes de niveau 2 sont, quant à eux, chargés de traiter les incidents ne relevant pas de cas standards.

Ingénieur Sécurité (niveau 3)

Les Ingénieurs Sécurité niveau 3, possèdent en plus de l'expertise sur les méthodes d'attaques.

Ils sont à même de mener des investigations à partir de « signaux faibles » et de faire de la recherche exploratoire sur l'ensemble des événements. Ils ont la capacité à faire du « reverse » dans un mode industrialisé.

En plus d'un excellent niveau techniques, des qualités rédactionnelles et de synthèse sont également indispensables.

Responsable SOC

Il s'agit du poste de chef de l'équipe SOC qui allie des qualités managériales et techniques. Le responsable du SOC fédère l'équipe et assure une bonne communication entre le SOC et les autres entités de l'entreprise.

Ses principales activités sont :

- Management de l'équipe opérationnelle du SOC
- Respect des « *Service Level Agreements* » (SLA) du SOC
- Garant de la bonne l'application des processus :
  - Gestion des incidents,
  - Optimisations des traitements
  - Suivi des demandes de changements
- Garant de la cohérence et de la stratégie technique du SOC
- Animations des revues hebdomadaires, mensuelles.
- Définition et suivi des indicateurs de performance du SOC et mise en place des tableaux de bord
- Gestion des escalades et crises : coordination, plans d'actions, reporting, organisation des opérations d'urgence
- Rédaction des rapports d'activités (tendances et statistiques opérationnelles des menaces)
- Gestion de la communication du SOC vers les autres entités de l'entreprise
- Rédaction de messages pré-formatés d'alerte
- Réalisation des opérations de niveau 2 et 3

Les missions de récupération/investigation (saisie de preuve, copie des informations, …) sur les systèmes en réaction à un incident peuvent être portées par le SOC, le CERT ou les équipes locales pour leur proximité avec les actifs. A définir en fonction de l'organisation de l'entreprise (objectif : efficacité)

8 Evaluation de l'efficacité des SOC

La mesure de performance d'un SOC doit être faite en fonction des missions et de l'engagement du SOC. Ce dernier peut en effet avoir :

- Un engagement de résultats portant sur la détection et la réaction à des scénarios prédéterminés validés et testés (avec un engagement complémentaire d'amélioration continue). En complément, le SOC doit mettre à disposition les meilleurs efforts à la détection de nouveaux scénarios d'attaque. Cet engagement est le plus fréquemment mis en œuvre car il est facilement mesurable et induit l'obtention d'un niveau minimum de sécurité ;

- Un engagement de moyen portant sur la mise à disposition de ressources et de capacités d'analyse. Ce modèle est très rarement mis en œuvre bien que plus efficace dans la détection d'APTs car il repose avant tout sur la gestion et l'encadrement d'équipe, offrant ainsi peu d'éléments factuels de mesure de performance hormis les tests d'intrusion.

Quelle que soit l'engagement choisi pour son modèle, un SOC doit pour démontrer son efficacité répondre à la question : « Comment garantir que l'Entreprise est mieux protégée ? ». Il dispose pour ce faire de plusieurs axes de réponse :

1. Démontrer sa conformité au contrat : Test des scénarios d'attaque convenus et dont la détection et le traitement ont été implémentés au niveau du SOC. Cette recette des scénarios prédéterminés se concentre sur le comportement adopté par le SOC face à la situation, depuis la collecte/détection jusqu'à la remédiation ;
2. Démontrer sa capacité opérationnelle de gestion d'incident au travers de simulations : Tests internes/externes sur les scénarios de menaces (contractuels et de l'état de l'art). Cette démonstration est effectuée en observant les réactions du SOC face aux stimuli non annoncés (pertinence de la détection, temps de détection et de traitement de bout en bout, envergure de la réaction, …) ;
3. Mettre en avant les retours d'expérience internes : Partage des conclusions des attaques déjouées ou subies ;
4. Se comparer avec les autres établissements sur les indicateurs de type R2GS.

L'évaluation par la conduite de test d'intrusion sur les scénarios de menaces couvert par le SOC est désormais une bonne pratique courante qui offre l'avantage d'alimenter le SOC en nouveaux scénarios d'attaque au plus proche de la réalité. Cette approche en plus de s'inscrire dans la méthodologie ISO d'amélioration continue fournie des retours d'expérience en conditions quasi réelles permettant ainsi au SOC de s'évaluer de manière indépendante. Il ne faut néanmoins pas oublier que ce type de tests bien qu'au plus proche de la réalité, ne remplace pas une attaque réelle qui est souvent par nature complexe et qui implique parfois des contre-feux pour occuper le SOC.

Indicateurs de performance

Il est fortement conseillé d'utiliser des indicateurs standards de place (tels que ceux du R2GS) qui en plus d'avoir été conçu par une communauté d'experts, permettent de comparer l'efficacité et l'efficience de son SOC par rapport au marché. De plus dans le cas d'un SOC info-géré, la capacité du prestataire à produire et traiter facilement ces indicateurs est un bon critère d'évaluation de maturité.

Les indicateurs de performances doivent être revus à minima mensuellement par le responsable en charge du SOC (ou SOC leader) pour lui permettre d'avoir une vision factuelle et objective du service fourni. Il doit ensuite restituer les plus pertinents avec son analyse dans les différents comités de pilotage.

Le tableau de bord qu'il produit est généralement constitué d'un transparent avec les indicateurs clés suivi d'un ou plusieurs transparents où sont mis en avant des indicateurs particuliers avec leur analyse. Les indicateurs clés de performance doivent permettre d'évaluer synthétiquement les capacités du SOC et leurs évolutions potentielles.

En plus des indicateurs standards de performances basés sur des métriques, il est intéressant de mesurer qualitativement :

- La qualité des alertes reçues par le SOC ;
- La qualité des alarmes émises par le SOC
- La qualité de la résolution d'incident ;
- La qualité de la passation entre le Niveau 1 et le Niveau 2.

Vulnérabilités

Un SOC ne doit pas être un moyen aval de ne pas régler un problème de sécurité amont. Pour ce faire il doit participer autant que faire ce peut à la correction des vulnérabilités et des faiblesses du SI. Cette participation doit se faire à minima dans le pilotage de l'analyse des causes racines (ou « Root Cause Analysis ») des incidents majeurs ou des incidents répétitifs.

Il peut donc ainsi être également évalué par rapport au nombre de vulnérabilités qui sont corrigées au sein du SI, même si cette correction ne dépend pas directement de ses attributions.

Tickets

Un ticket d'incident peut se résumer comme étant une fiche de suivi de l'incident qui permet de lui attribuer un responsable de sa résolution et d'assurer sa résolution. Il est le livrable métier du SOC, et doit donc en ce sens être évalué.

L'évaluation de la qualité des tickets doit comprendre plusieurs critères pour rester la plus objective possible :

- La qualification au bon niveau de criticité d'incidentologie à la clôture de ce dernier ;
- La surveillance des seuils d'escalade entre les différents niveaux. Cet indicateur mettra en lumière les risques de saturation ainsi que les problèmes intrinsèques d'efficience ;
- L'analyse de la raison de la clôture par le CERT du ticket.

En plus de cette analyse systémique, il est conseillé de procéder à la revue par échantillonnage du contenu des tickets émis.

Incidents

L'une des missions principales du SOC est d'assurer le pilotage de la résolution des incidents de sécurité. À ce titre, il est indispensable de s'assurer que l'ensemble des tickets d'incident ont été clôturés avec les informations nécessaires pour comprendre les raisons de cette clôture. Ce suivi s'effectue au travers de l'indicateur du reste à faire (ou « backlog ») et par échantillonnage sur les tickets fermés.

Notons également que dans certes circonstances l'entreprise à l'obligation de déclarer ses incidents de sécurité. Dans ce cadre il peut être intéressant de disposer d'indicateurs permettant de connaitre le nombre d'incidents communiqué aux différentes autorités ainsi que le temps nécessaire pour faire ces déclarations. En effet certaines législations imposent des contraintes de délai dans la déclaration des incidents. Parmi les législations en vigueur imposant la déclaration d'incident de sécurité, nous retiendrons les suivantes qui sont les plus susceptibles de toucher notre secteur :

- France : Obligation de notification des incidents de sécurité informatique pour les OIV (Opérateur d'Importance Vitale) ;
- USA : Obligation de déclaration en cas de fuite de données contenant des informations personnelles ;
- Singapour : Obligation de notification auprès des clients ainsi que de l'autorité de régulation locale (le MAS : Monetary Authority Of Singapore) ainsi qu'à la police en cas de piratage et d'intrusion informatique.

9 Conclusion

Un SOC est avant tout une équipe d'experts en sécurité. Le succès de son intégration et de son maintien en conditions opérationnelles dépendra certes des moyens techniques mis en œuvre mais avant tout du maintien de la compétence humaine mobilisée.

Le SOC doit s'inscrire dans la stratégie globale de sécurité du SI et disposer de missions claires et établies pour pouvoir être dans un premier temps évalué et pour établir ses limites. Il ne doit pas seulement être un être un moyen de contrôle aval mais aussi un moyen de prévention positionné en amont.

In fine pour pouvoir être en mesure d'effectuer sa mission de résolution des incidents de sécurité informatique, il doit s'assurer du sponsoring du top management et réussir à maintenir son intérêt. Cet élément est la clé de voute indispensable pour donner au SOC la place nécessaire pour pouvoir faire agir les différentes parties prenantes, incluant les métiers, en cas d'incident et de maintenir sa capacité à évoluer pour s'adapter aux nouvelles menaces.

10 Annexes

Document MITRE

https://www.mitre.org/publications/all/ten-strategies-of-a-world-class-cybersecurity-operations-center