Chapitre 3
Les équipes du SOC

1. Introduction générale

1.1 Pourquoi la technologie seule ne suffit pas

Le SOC est souvent perçu, à tort, comme un ensemble d'outils technologiques sophistiqués capables de détecter, corréler, et neutraliser des menaces informatiques. SIEM, EDR, SOAR, sondes, sandbox, TIP (*Threat Intelligence Platform*)… ces acronymes prennent une place prépondérante dans les représentations mentales des responsables sécurité, des RSSI et même du grand public informé. Pourtant, au cœur de toute cette architecture numérique, réside un facteur essentiel, souvent sous-estimé : l'humain.

1.1.1 Les machines ne remplacent pas la prise de décision

Même les outils de sécurité les plus avancés nécessitent un pilotage stratégique et tactique. Les décisions critiques (escalade d'un incident, acceptation d'un risque, déclenchement d'une réponse automatique ou investigation plus poussée) ne peuvent être prises que par des humains, formés, compétents, capables d'interpréter des signaux faibles dans un contexte métier.

L'intelligence artificielle, aussi performante soit-elle dans certaines tâches, reste dépendante de l'humain pour la supervision, la validation, le paramétrage, l'ajustement et la compréhension des dynamiques d'attaque complexes. Un analyste chevronné remarquera parfois en quelques minutes un détail qu'aucun moteur d'analyse automatisée n'aurait su corréler, tout simplement parce que ce détail sort du cadre des règles établies.

1.1.2 L'humain, moteur d'adaptation face à l'imprévu

Les attaques informatiques évoluent sans cesse. De nouvelles vulnérabilités apparaissent chaque semaine, des campagnes malveillantes émergent sans prévenir, et des techniques d'évasion toujours plus sophistiquées sont déployées par les groupes APT (*Advanced Persistent Threats*). Dans ce contexte, l'humain reste le seul capable de s'adapter à des situations inédites, de créer des contournements tactiques, d'explorer des pistes non conventionnelles.

Un SOC peut disposer de tous les outils du monde : si les équipes ne sont pas formées, motivées, coordonnées, il sera inefficace. C'est un peu comme posséder une armée de tanks sans pilotes ni commandement : la puissance est là, mais elle ne peut être activée sans compétence humaine.

1.1.3 Des outils pensés pour et par des humains

Un autre point essentiel est que les outils ne sont jamais neutres : ils sont conçus, configurés et exploités par des personnes. Le choix des sources de logs à intégrer, la rédaction des règles de corrélation, la gestion des exceptions, la pertinence des playbooks… tout cela repose sur la connaissance métier, la culture de la menace, l'expérience et l'intuition des opérateurs.

De plus, le ressenti des utilisateurs finaux, qu'il s'agisse d'analystes L1 ou d'experts CSIRT, permet d'affiner l'ergonomie, l'organisation des dashboards, les niveaux de criticité des alertes, et d'éviter le phénomène d'Alert Fatigue. Un outil mal configuré, mal compris, mal utilisé, peut produire plus de bruit que de valeur. Il est donc primordial d'intégrer les considérations humaines dans la chaîne de valeur technologique.

1.1.4 L'humain au centre de la remédiation

Si la détection peut être en grande partie automatisée, la remédiation, elle, reste encore très souvent le domaine de l'humain. Il ne s'agit pas seulement de bloquer une IP ou de désactiver un compte.

Il faut parfois contacter un utilisateur, comprendre un contexte métier, évaluer les conséquences d'une action de remédiation sur une chaîne de production, discuter avec les équipes IT, les métiers ou la direction… Toutes ces interactions sont humaines, politiques, organisationnelles.

Le SOC est donc à la croisée des chemins entre la technique et la stratégie, et ce pont ne peut être maintenu que par les personnes qui le traversent au quotidien.

1.2 SOC : combinaison de personnes, de processus et de technologies

Il est tentant, dans une logique d'industrialisation et d'efficacité, de penser le SOC comme une simple chaîne de production sécuritaire : un flux de logs entrants, des outils qui analysent, et des alertes qui en ressortent. Mais cette vision, bien qu'utile à certains égards, occulte la richesse réelle d'un SOC : sa structure tripartite.

1.2.1 Les personnes

Nous l'avons déjà évoqué : ce sont eux qui font vivre le SOC. Mais il est important d'aller plus loin : un SOC ne se limite pas à quelques analystes. Il regroupe une diversité de profils : des experts techniques, des chefs de projet, des spécialistes métier, des gestionnaires de crise, des intégrateurs, des architectes, des veilleurs, des coordinateurs, des communicateurs… Ce sont ces individus qui, ensemble, construisent la chaîne de valeur de la cybersécurité.

Chaque personne a un rôle spécifique, un savoir-faire, une capacité d'analyse. Certains sont brillants dans le traitement technique d'un incident, d'autres dans la gestion de l'information auprès de la direction. D'autres encore sont des facilitateurs, qui fluidifient la coopération entre les équipes. Cette diversité est une force, à condition qu'elle soit orchestrée.

1.2.2 Les processus

Un SOC ne peut pas fonctionner efficacement sans processus. Ces processus garantissent la cohérence des actions, la traçabilité, la conformité aux normes (ISO 27001, NIS2, etc.), et permettent d'éviter les décisions à chaud trop risquées. Ils peuvent concerner :

– le traitement des alertes : tri, priorisation, escalade ;

– la réponse à incident : analyse, remédiation, communication ;

– la gestion des accès et des habilitations ;

– le maintien en condition opérationnelle des outils ;

– le cycle de vie des règles de détection ou des playbooks.

Ces processus ne doivent pas être vus comme des contraintes, mais comme des repères. Ils permettent de garder le cap, même dans le tumulte d'une crise cyber. Et là encore, ils sont conçus, éprouvés et ajustés… par des humains.

1.2.3 La technologie

Enfin, évidemment, la technologie reste incontournable. C'est elle qui donne de la puissance, de la rapidité, de la profondeur. Les outils permettent de traiter des volumes impossibles à gérer manuellement. Ils donnent de la visibilité, du contexte, de la corrélation, du suivi.

Mais ces technologies doivent être choisies avec discernement, adaptées aux besoins réels, correctement intégrées, et bien exploitées. Un bon outil mal utilisé est une fausse sécurité. Il peut donner une illusion de maîtrise alors que des attaques passent sous le radar. La technologie, dans un SOC, est un levier. Mais c'est l'humain qui appuie dessus.

1.2.4 L'équilibre entre les trois

Le vrai défi d'un SOC n'est pas d'exceller sur une seule de ces structures. C'est d'assurer un équilibre durable entre les trois. Trop de technologie sans humains compétents conduit à l'inefficacité. Trop d'humains sans outil conduit à l'épuisement. Trop de processus sans agilité humaine bloquent l'innovation.

Un SOC mature est donc un écosystème vivant, où l'humain donne du sens, le processus donne une structure, et la technologie donne une force.

1.2.5 Exemple d'interdépendance dans un cas d'incident

Pour bien comprendre comment les personnes, les processus et les technologies s'articulent concrètement dans un SOC, prenons un exemple réaliste. Imaginons un incident de type compromission d'un poste utilisateur via une macro malveillante dans un fichier bureautique.

– Technologie : un EDR détecte un comportement suspect, tel qu'un powershell.exe lancé via un autre exécutable.
– Processus : l'alerte est automatiquement envoyée dans le SIEM, puis un ticket est généré selon un playbook défini.
– Humain : un analyste L1 vérifie l'alerte, cherche des indices de compromission supplémentaires, et escalade à un L2.
– Processus : l'analyste L2 suit une procédure standardisée de réponse à incident, isole la machine via l'EDR, et informe le CSIRT.
– Humain : un expert CSIRT analyse le payload, identifie le groupe de menace potentielle, documente l'incident, et alerte le RSSI.

Dans cet exemple :

– Sans technologie, l'alerte ne serait jamais apparue.
– Sans processus, elle n'aurait pas été correctement traitée ni remontée.
– Sans humain, elle n'aurait pas été comprise ni résolue.

Ces trois éléments fonctionnent comme un moteur : si l'un d'entre eux tombe en panne, tout le système ralentit, voire s'arrête.

1.2.6 Le facteur humain comme catalyseur d'évolution

Les SOC modernes doivent sans cesse s'adapter à la menace, aux exigences réglementaires, aux attentes des clients internes, aux nouvelles architectures IT. Or, cette adaptation passe rarement par l'achat d'un nouveau produit : elle passe d'abord par la montée en compétence des équipes, leur capacité à innover, à proposer de nouveaux indicateurs, à construire des règles plus fines, à créer des tableaux de bord adaptés aux besoins des métiers.

Dans cette optique, l'humain n'est pas simplement un opérateur : il est acteur de la transformation continue. Un bon SOC, c'est une équipe capable de remettre en cause ses propres pratiques, d'expérimenter, de prototyper de nouveaux processus, de tester des outils open source, de documenter, de former, de mentorer. C'est dans cet esprit que naissent les SOC les plus résilients.

1.2.7 Des profils variés, une culture commune

Ce qui rend un SOC à la fois complexe et passionnant, c'est la variété des profils impliqués. Un analyste junior fraîchement formé aux fondamentaux techniques côtoiera peut-être un expert ayant une expérience terrain de la réponse à incident. Un administrateur système reconverti en spécialiste SOAR croisera un consultant gouvernance habitué aux référentiels ISO.

Pour fonctionner, cette diversité doit s'accompagner d'une culture commune de la cybersécurité : vocabulaire partagé, vision commune des objectifs, compréhension mutuelle des contraintes métiers et techniques. Cela se travaille, via la documentation, la formation interne, les rituels d'équipe, les War Rooms, les rétrospectives, les simulations de crise.

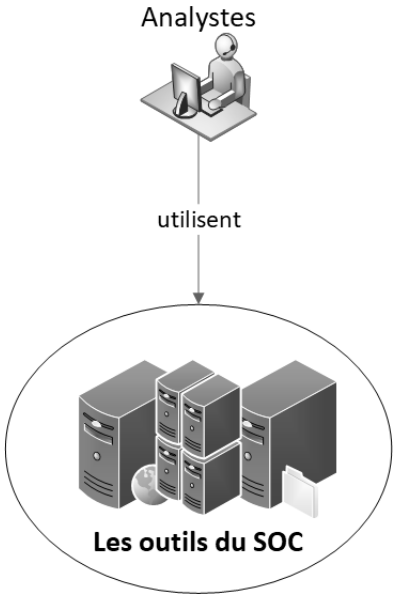
Un SOC doit être un espace d'apprentissage collectif, où chacun comprend l'importance de son rôle et celui des autres.

1.2.8 Conclusion de la section

L'introduction de ce chapitre avait pour but de poser un socle : le SOC n'est pas un simple empilement d'outils. C'est une organisation hybride, multidimensionnelle, où les ressources humaines sont centrales. Sans elles, les processus ne sont pas appliqués, et la technologie reste aveugle.

En préparant les sections suivantes sur les rôles des analystes, les équipes spécialisées, le management, les interactions, il est essentiel de garder cette idée en tête : le SOC est avant tout un centre de compétences. Un endroit où la technique rencontre l'intelligence humaine. Un lieu où la rigueur cohabite avec la créativité. Un environnement où des équipes engagées surveillent constamment les menaces et agissent sans relâche pour garantir la sécurité numérique du périmètre supervisé.

2. Les analystes SOC : L1, L2, L3



Le fonctionnement opérationnel quotidien d'un SOC repose avant tout sur le travail des analystes de sécurité. Ces professionnels constituent la première ligne de défense face aux menaces informatiques. Leur rôle ne se limite pas à traiter des alertes : ils analysent, décident, escaladent, documentent, et peuvent jouer un rôle pédagogique auprès des métiers ou d'autres équipes internes.

Traditionnellement, les analystes SOC sont organisés selon une logique de niveau – L1, L2, L3 (du terme anglais « *Level* » 1, 2, 3, parfois traduits en français par N1, N2, N3 pour « Niveau ») – reflétant la montée en expertise et en responsabilité. Toutefois, cette hiérarchie n'est pas une vérité universelle : certaines structures ont volontairement fait le choix d'un modèle plat, sans segmentation explicite. Nous explorerons dans cette section ces différents modèles, leurs avantages et leurs défis, tout en mettant en lumière les tâches et les parcours de ces analystes qui font vivre la supervision au quotidien.

2.1 Définition des rôles, tâches quotidiennes, périmètre

Le découpage L1, L2, L3 est inspiré de l'organisation en niveaux d'escalade que l'on retrouve aussi dans les centres de support informatique. Appliqué au SOC, il permet une répartition des tâches selon la complexité, l'urgence et la spécialisation requise.

2.1.1 Analyste L1 – la première ligne de supervision

L'analyste de niveau 1 est le guetteur en permanence sur les lignes du front. Il surveille les alertes générées par les outils de sécurité (SIEM, EDR, IDS, etc.), filtre le bruit et identifie les signaux pertinents.

Ses principales missions incluent :

– la surveillance en temps réel des flux d'alertes ;
– le tri initial des événements : faux positifs vs alertes légitimes ou potentielles ;
– l'ouverture de tickets d'incident lorsque nécessaire ;
– le renseignement initial de l'incident dans les outils de ticketing ;
– l'escalade vers le niveau 2 en cas de doute ou d'alerte avérée.

Le L1 ne dispose pas toujours des droits d'intervention technique : son rôle est surtout analytique, réactif et bien documenté. Il suit généralement des processus définis à l'avance, ce qui garantit une uniformité de traitement mais peut aussi limiter son autonomie. Il peut être amené à travailler en horaires décalés pour des structures assurant un service 24/7.

2.1.2 Analyste L2 – l'investigateur confirmé

Le niveau 2 est en quelque sorte le « médecin généraliste » du SOC. Lorsqu'un L1 remonte une alerte, le L2 prend le relais pour enrichir, comprendre, qualifier et contextualiser l'incident.

Ses missions vont bien au-delà de la lecture de logs :

– corréler les événements entre plusieurs sources (SIEM, EDR, proxies, AD, etc.) ;
– utiliser des outils d'enrichissement (Threat Intelligence, requêtes LDAP, etc.) ;
– communiquer avec les utilisateurs ou les équipes IT pour confirmer certains événements ;
– appliquer ou recommander des mesures de remédiation immédiates ;
– documenter en détail les investigations menées.

Le L2 est souvent celui qui "raconte l'histoire" derrière une alerte : d'où vient-elle, pourquoi s'est-elle produite, est-ce le signe d'une attaque plus large ? Il travaille étroitement avec les L1 et les L3, parfois avec les équipes d'exploitation ou d'architecture. Il est attendu qu'il fasse preuve de recul, de curiosité et de capacité à relier les points.