WAVESTONE

FUSION CENTER : LE FUTUR DU SOC

La sécurité opérationnelle est gérée chez nos clients par deux principales structures : le SOC, en charge de la détection, de la qualification et de la gestion des incidents ; et le CSIRT, responsable de la gestion de crise, de l'investigation numérique, de la veille et de la Threat Intelligence.

Quels sont les principaux leviers d'optimisation et les pistes prometteuses pour le futur de cette organisation bipolaire ? Le *Fusion Center* apporte des éléments de réponse.

Les rôles du SOC et du CSIRT ne sont parfaitement tranchés, et certaines tâches se retrouvent à la croisée des responsabilités : quelle contribution le SOC a-t-il dans la gestion des crises ? Comment le CSIRT peut-il aider à la détection ?

Par ailleurs, la création d'équipes dédiées à de nouveaux besoins spécifiques (cellules anti-fraude et SOC métiers par exemple), complexifie davantage l'organisation de la sécurité opérationnelle.

Au-delà de cette complexité, le bilan de la sécurité opérationnelle est mitigé et des problèmes récurrents restent sans réponse : pénurie de ressources cybersécurité, fort taux de faux positifs entrainant une sursollicitation des analystes, référentiels inexistants ou de mauvaise qualité et difficultés à répondre aux besoins métiers selon le planning souhaité.

AUTEURS

BENOIT MARION
benoit.marion@wavestone.com

JÉRÉMY PAGEAUX
jérémy.pageaux@wavestone.com

Cette publication a été réalisée avec la contribution de Amaury COULOMBAN, consultant en cybersecurité et confiance numérique.

AUTOMATISER POUR GAGNER EN EFFICACITÉ

Force est de constater que les analystes perdent aujourd'hui un temps précieux à réaliser de nombreux gestes manuels sur un grand nombre d'outils : recopie d'informations (copié-collé entre le SIEM, la multitude de référentiels et les différents outils de *ticketing*) et connexion aux ressources et aux outils de sécurité pour la remédiation notamment. Au-delà de la perte de temps, ces tâches répétitives et souvent sans valeur ajoutée génèrent une frustration et une lassitude au sein des effectifs.

Automatiser le processus de management des incidents

Les SOAR (*Security Orchestration, Automation & Response*) sont des outils d'aide et d'automatisation de la réaction aux incidents de sécurité qui visent notamment à pallier ces irritants.

Ces plateformes sont destinées à être l'unique outil de tous les intervenants de la gestion d'incidents. Elles permettent la définition de processus d'analyse et de réaction adaptés à chaque événement de sécurité. Une fois un processus défini, certaines tâches peuvent être automatisées grâce à des interactions API avec les solutions IT et de sécurité de l'environnement.

Lors de la phase d'analyse, l'outil peut automatiquement enrichir l'événement de sécurité en allant récupérer des informations de contexte sur le SI ou auprès de services de *Threat Intelligence*. Certaines solutions s'approchent même de l'automatisation complète d'un N1 en proposant l'utilisation de *chatbots*, par exemple pour vérifier auprès d'un administrateur — authentification multi-facteurs à l'appui — qu'il a bien effectué une action.

Ces informations peuvent être utilisées pour clôturer automatiquement certaines alertes, prioriser celles à traiter par des analystes et faciliter leur travail de qualification.

Mais l'automatisation ne s'arrête pas là. Bien que limitée à quelques cas bien maîtrisés (les plus simples étant le blocage d'URL avérées malveillantes sur le proxy, ou la suppression de mails de *phishing*), l'automatisation de la réaction représente un gain en charge important pour les équipes sécurité.

Automatiser la création de règles basées sur des menaces avérées

Même si le processus d'analyse et de réaction peut être industrialisé, la création de règles de détection nécessite actuellement beaucoup de travail manuel, unique pour chaque contexte : adaptation aux technologies de l'environnement, à ses particularités (seuils)... De plus, ces règles reposent sur des signatures d'attaque souvent standards, parfois connues et évitées par les attaquants les plus avancés.

Bien utilisée, la *Threat Intelligence* peut aider les équipes de surveillance à adresser ces problèmes. Les plateformes de *Threat Intelligence* transmettent au SOC, dans un format exploitable (IOC récupérables par des API), des informations contextualisées sur les menaces actuelles. En les interfaçant avec le SIEM, ces plateformes peuvent l'abreuver automatiquement et en temps réel avec les dernières signatures d'attaques à détecter. Ce mode de fonctionnement fait ses preuves : les MSSP utilisent déjà cette approche et indiquent que la majorité de leurs alertes avérées proviennent de scénarios basés sur des *feeds* de *Threat Intelligence*.

Les plateformes de *Threat Intelligence* permettent donc de compléter de manière automatique la création de règles de détection. En complément, elles participent aussi à l'industrialisation de l'analyse des évènements, en fournissant en temps réel (au SOAR) des éléments permettant de juger de la véracité d'une alerte.

Détecter de manière avancée avec le *Machine Learning*

Outre leur complexité de déploiement, les règles classiques présentent un autre défaut : elles se basent sur des analyses statiques, génératrices de nombreux faux positifs (sauf effort important de maintenance). De plus, cette approche par signature ne détecte que des attaques connues et n'est pas adaptée pour détecter des attaques sophistiquées.

Aux antipodes de l'approche par signatures d'attaques connues, le *Machine Learning* permet de réaliser de l'analyse comportementale et de la détection d'anomalies. Ces outils sont donc capables de détecter des attaques pour lesquelles la définition de signatures est impossible : nombre de cas à couvrir trop important ou niveau de corrélation nécessaire trop élevé. Ils sont donc mieux adaptés aux besoins des métiers, complexes à adresser avec les SIEM et leur vision technique : surveillance applicative (utilisant des formats de log spécifiques aux produits utilisés) et protection contre la fraude (se basant sur des sources très variées).

En complément d'une approche par signature, le *Machine Learning* aide à réduire le taux de faux positifs en adaptant automatiquement les seuils au contexte (volumétrie réseau, nombre d'utilisateurs...).

Adapter l'organisation à cette automatisation

Bon nombre de ces évolutions nécessitent d'adapter les effectifs du SOC. Autour du SOAR, on voit graviter les équipes de détection et de réaction, qui travaillent finalement dans un but commun de sécurisation : le *Fusion Center* propose donc l'unification du SOC et du CSIRT. Pour gérer les outils de *Machine Learning* décrits, des *data scientists* sont également requis au sein du *Fusion Center*.

Ces évolutions sont bénéfiques, pour la supervision sécurité comme pour les équipes : la réduction de la charge liée aux taches récurrentes et la variété accrue de postes à forte valeur ajoutée permettront aux effectifs du *Fusion Center* d'adopter différents rôles, aidant grandement à limiter le *turn-over* des équipes.

AJOUTER UNE TOUCHE D'AGILITÉ DANS LE SOC ET SES ACTIVITÉS

La transformation vers les *Fusion Centers* ne concerne pas que l'outillage. Les modes de fonctionnement, plus agiles, doivent aussi être revus, pour améliorer l'efficacité des équipes de sécurité opérationnelle.

Dans les SOC actuels, les règles de détection sont essentiellement créées en *top-down* en déclinant une analyse de risques globale en scénarios de supervision.

Des bonnes pratiques systématiques pour la création des règles de détection

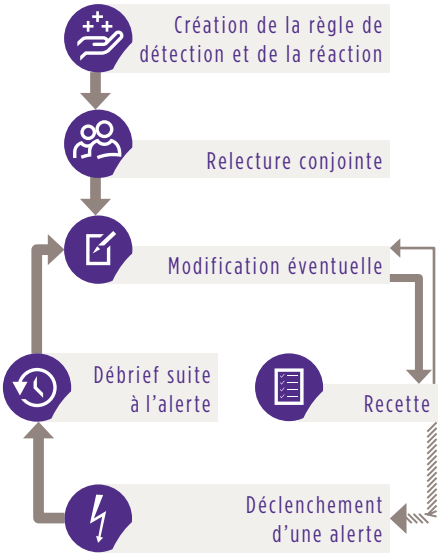
Cette méthodologie vertueuse ne permet pas de couvrir 100% des risques identifiés initialement, et bien souvent, le processus à suivre en cas d'alerte n'est pas défini. Les scénarios restent figés dans leur état initial, fréquemment générateurs de faux positifs ou inefficaces dans la durée. Quelques bonnes pratiques peuvent être appliquées pour limiter ces problèmes.

De trop nombreux scénarios, recettés d'un point de vue technique, s'avèrent non fonctionnels en situation réelle, que ce soit à cause d'un problème sur la chaine de logs, d'un changement du format attendu, ou de seuils mal définis. Chaque scénario doit donc faire l'objet d'une recette de bout en bout, afin de s'assurer que l'alerte associée est bien levée au bon moment.

La recette permettant de s'assurer de l'efficacité des scénarios de supervision, il convient aussi de s'assurer que la procédure de réaction est bien définie, en collaboration avec l'équipe projet métier (client, demandeur et concepteur de la règle).

Une fois ces règles de détection et de réaction en place, il est nécessaire de les faire vivre pour qu'elles restent optimisées. Le moyen le plus efficace pour améliorer continuellement la qualité des règles est la mise en place d'une boucle de *feedback* systématique. Pour chaque alerte levée, les acteurs (analyse, réaction) débriefent le *Fusion Center*, ayant implémenté la règle. Si l'alerte est erronée, la règle (ou l'analyse automatique du SOAR) doit être modifiée pour supprimer ces faux positifs. Dans tous les cas, le *feedback* peut servir à automatiser des actions effectuées : ajout d'une source d'information, automatisation d'une remédiation…

En complément, la relecture conjointe de plusieurs analystes — *peer review* — lors de la création de chaque scénario permet d'améliorer la qualité des règles, et donc de faciliter le partage des connaissances et le maintien dans le temps.



La chasse aux menaces, un moyen efficace de compléter les scénarios de supervision

Une autre manière d'améliorer la qualité de la détection est de compléter les scénarios de supervision (plutôt *top-down*) par une approche *bottom-up* grâce au *Threat Hunting*.

Des analystes se voient attribuer une charge régulière (une journée hebdomadaire par exemple) pour partir à la « chasse » aux événements suspects. Ces traces peuvent être récoltées en externe (informations confidentielles trouvées sur le *Darkweb*…) ; ou en interne, sur des ressources de production ou des outils de sécurité (et notamment les logs du SIEM). L'objectif est alors d'identifier des événements ou des comportements suspects, à investiguer pour lever éventuellement des alertes. Ce faisant le *Threat Hunter* est amené à améliorer des règles de détection existantes ou en créer de nouvelles. En complément, cette méthode permet aux analystes d'améliorer leur connaissance de leur environnement, et pousse à la recherche de traces et à la proposition de nouvelles alertes à valeur ajoutée, plutôt qu'à la simple réponse aux alertes du SIEM selon les SLA définis.

Plus d'agilité dans les relations avec les projets métiers

Toutes ces tâches sont complexes et mobilisent les efforts du SOC, qui a donc des difficultés à adresser les nouveaux besoins. Les équipes métiers et la lutte anti-fraude ont ainsi tendance à créer leurs équipes dédiées. Mais la création d'entités séparées limite les possibilités de corrélations globales et génère une redondance d'efforts, ce qui est d'autant plus dommage que les sources d'informations sont souvent très similaires (logs d'infrastructure, logs applicatifs, logs d'accès utilisateurs…).

Pour remettre le *Fusion Center* au centre de la supervision, y compris pour les métiers, il s'agit de faciliter les échanges avec les équipes projets métiers. En traduisant quelques concepts de l'Agile, le *Fusion Center* vise à impliquer davantage les équipes projets métiers dans la supervision, à la fois dans la phase de conception, et dans la phase de traitement des alertes. Pour ce faire, de nouvelles ressources (des « champions de la supervision ») sont à intégrer dans les équipes projets métiers agiles. Ces équipes sont alors capables d'exprimer un besoin de supervision directement implémentable par le *Fusion Center,* et de le mettre à jour à mesure de l'évolution du projet métier.

En retour, lors de la détection d'une alerte, le *Fusion Center* procède (automatiquement si possible !) à l'analyse et à l'enrichissement, puis communique l'alerte à l'équipe projet métier, qui est la mieux placée pour qualifier — et potentiellement remédier — une alerte sur son périmètre. Le *feedback* permet enfin d'améliorer le processus et les alertes en continu.

LE FUSION CENTER, UN SOC AMÉLIORÉ… QUI DÉMONTRE SON EFFICACITÉ !

Le *Fusion Center,* grâce à l'automatisation, au *Machine Learning*, et à son organisation et son fonctionnement plus agile, va gagner en efficacité sur les SOC et CSIRT actuels.

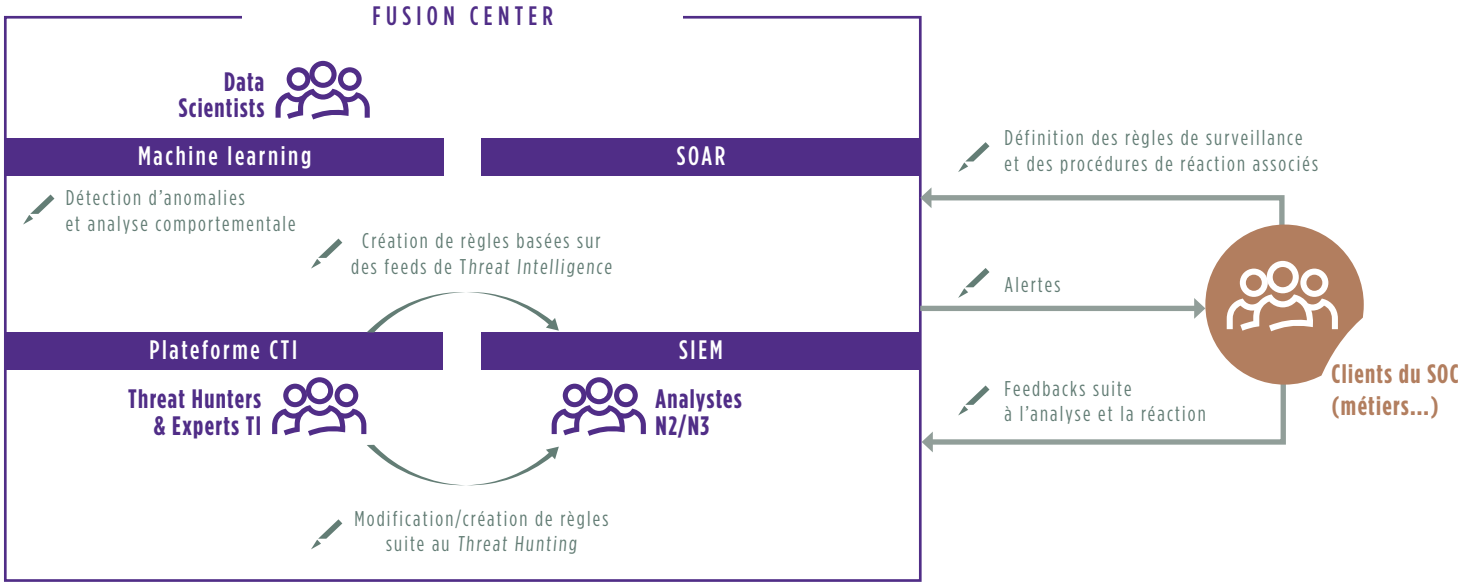
Pour rendre tangible cette amélioration — reproche parfois fait aux SOC —, il est nécessaire de se doter de moyens de mesure de sa maturité. Les bénéfices sont multiples : démontrer les résultats et justifier les investissements souvent lourds de ces organisations, ou apporter la conformité par rapport à un cadre réglementaire.

Les référentiels, limités jusque-là, se sont multipliés ces dernières années. Nous en retenons deux : le référentiel PDIS[1] de l'ANSSI, très exigeant et complet, peut donner une vision de l'état de l'art et mesurer un écart ; et le référentiel SOC-CMM[2] — en accès libre — couvre tous les sujets et permet aux SOC de s'auto-évaluer à partir d'un ensemble de questions précises.

De toutes les bonnes pratiques partagées sur les *Fusion Centers* de demain, celle à démarrer dès aujourd'hui est certainement la mesure régulière de la maturité grâce à ces référentiels !

1 - https://www.ssi.gouv.fr/uploads/2014/12/pdis_referentiel_v2.0.pdf
2 - https://soc-cmm.com/

Résumé des nouveaux effectifs, outils et modes de fonctionnement du Fusion Center



WAVESTONE

www.wavestone.com

Dans un monde où savoir se transformer est la clé du succès, Wavestone s'est donné pour mission d'éclairer et guider les grandes entreprises et organisations dans leurs transformations les plus critiques avec l'ambition de les rendre positives pour toutes les parties prenantes. C'est ce que nous appelons « The Positive Way ».

Wavestone rassemble 2 800 collaborateurs dans 8 pays. Il figure parmi les leaders indépendants du conseil en Europe, et constitue le 1er cabinet de conseil indépendant en France.

Wavestone est coté sur Euronext à Paris et labellisé Great Place To Work®.