Security Operations Centers: enseignements et tendances pour 2026

Revue des thématiques, des tendances du marché et du niveau de maturité des SOC aujourd'hui pour se projeter vers l'avenir

WAVESTONE

Introduction

Commençons par explorer pourquoi ce rapport a été créé et **ce à quoi vous pouvez vous attendre…**

La **sécurité opérationnelle** connaît une transformation majeure: nous observons et accompagnons des clients qui repensent les approches traditionnelles du développement et des opérations. **Pourquoi ?** Les leaders de la sécurité voient désormais plus loin. Dans nos échanges avec des RSSI et des responsables SecOps, trois notions reviennent sans cesse : consolidation, vision long-terme et résilience.

La sécurité opérationnelle en 2025 dépasse largement la détection et la réponse. Il s'agit d'aligner la sécurité sur le risque business, d'intégrer la télémétrie IT/OT/Produit dans un cadre unifié de supervision, et de permettre des décisions plus rapides et plus intelligentes sur l'ensemble du workflow de détection et de réponse.

Parallèlement, la surface d'attaque a explosé avec le SaaS, les identités machine et désormais les outils GenAI. **Le résultat ?** Un paysage de menaces plus dynamique, plus flou et bien plus instable. Les campagnes de Scattered Spider et Shiny Hunters montrent que les cybercriminels exploitent pleinement cette situation. Et en 2025, une vague d'incidents majeurs, dopée par l'IA tant en ingénierie sociale qu'en découverte de vulnérabilités, confirme que les adversaires innovent aussi vite, voire plus vite, qu'en 2024.

Alors, qu'est-ce qui motive la création de cette édition ? C'est la prise de conscience que les capacités, les processus et les technologies sur lesquels nous comptions encore l'an dernier ne constituent plus un socle suffisant.

L'IA en est l'exemple paradigmatique. Elle n'accélère pas seulement les activités : elle impose de réécrire entièrement le modèle opérationnel.

L'objectif cette année est donc d'**explorer les tendances émergentes et transformatrices qui impactent la sécurité opérationnelle en 2025 au travers de six questions que nos clients nous posent fréquemment.**

Où en sommes-nous aujourd'hui, et qu'est-ce qui nous bloque ?

1. Naviguer dans la conformité réglementaire, que doivent savoir les équipes SecOps ?
2. Surmonter les défis des équipes SOC en 2025 : burnout, manque de compétences et voie d'avenir
3. Démontrer le retour sur investissement, comment créer un business case pour transformer le SOC ?

Quelles sont les prochaines étapes, et comment les atteindre ?

1. Le XDR est là, mais comment l'utiliser ? Pérenniser et moderniser les outils de détection et de réponse.
2. L'IA agentique dans les Security Operations : les analystes SOC sont-ils en voie de disparition ?
3. L'évolution du rôle de la donnée dans un SOC moderne : connecter les équipes sécurité et catalyser la valeur business

Nous espérons que vous prendrez autant de plaisir à parcourir ces analyses que nous en avons eu à les produire ! À l'année prochaine…

James Maidment
Consultant Senior
Equipe SecOps UK

Table des matières

01. Où en est la sécurité opérationnelle à la fin 2025 ?

Beaucoup de choses ont changé l'année dernière. Avant d'aborder les six défis de la sécurité opérationnelle, prenons du recul et évaluons les progrès réalisés depuis 2024.

Comment la sécurité opérationnelle a-t-elle mûri depuis 2024 ?

En sécurité opérationnelle, une semaine peut tout changer. Alors que dire de 52 ? **Cette première section offre un recul sur la situation en 2025.**

Défis Internes et externes

C'est la saison des rapports et des chiffres alarmants : la Revue annuelle du NCSC note 204 événements cybernétiques «d'importance nationale», soit 17 par mois. Simultanément, la première édition mondiale du rapport SOC-CMM note une croissance stagnante de la maturité, évoquant des défis persistants de rétention et de gouvernance. En résumé, les défis auxquels sont confrontés les dirigeants restent omniprésents, insaisissables et évolutifs.

Par conséquent, cette première section vise à clarifier le développement de la profession depuis 2024, ainsi que les perspectives plus larges du marché que nous pouvons tirer du Cyber Benchmark 2025 de Wavestone.

Le Cyber Benchmark 2025 de Wavestone

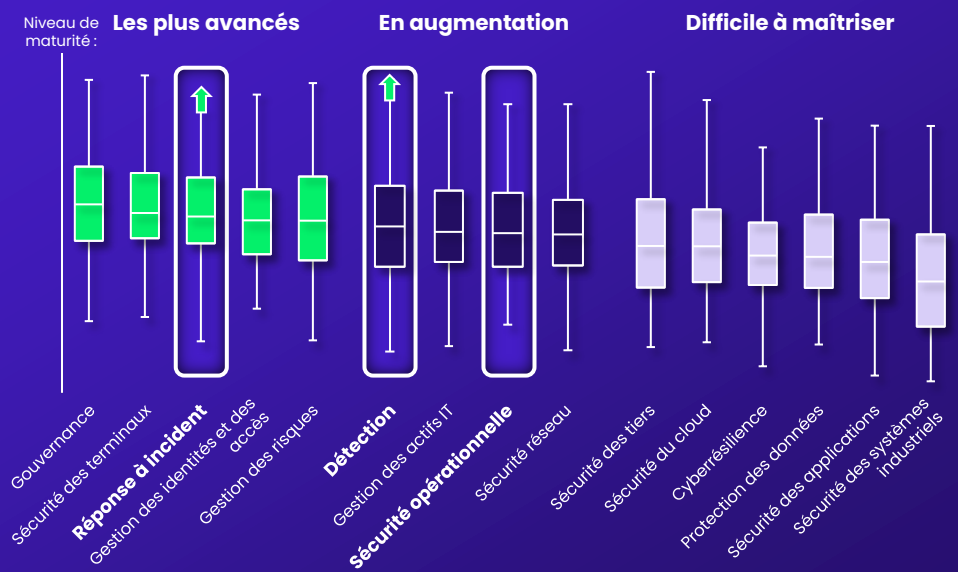
Organisé chaque année depuis 2019, ce benchmark a sondé plus de 150 clients Wavestone, représentant plus de 7 millions d'employés. Il est basé à la fois sur le NIST CSF et sur l'ISO 27001/2. Le benchmark lui-même se compose d'environ 200 questions réparties sur 16 sujets (mis en évidence ci-dessous).

Chaque année, nous rassemblons les résultats et présentons des résultats au public. La tendance cette année ? «Des progrès mesurés, des défis persistants ». Les entreprises ont progressé d'un point de pourcentage, jusqu'à 54 %. Le graphique ci-dessous et les pages suivantes mettent en lumière les principales conclusions spécifiquement pour la sécurité opérationnelle.

La sécurité opérationnelle dans son contexte

Vue en boîte des scores de maturité pour chaque sujet : minimum / 1er quartile / médiane / 3e quartile / maximum.

↑ *>3 % d'augmentation d'un an*



Source : *Wavestone Cyber Benchmark 2025*

Que dit le Benchmark de notre maturité ?

La réponse à incidents est routinière et bien maîtrisée

Les capacités de réponse aux incidents ont montré une nette amélioration depuis 2024 (+3 %), principalement grâce à l'amélioration de la coordination entre les unités commerciales avant les crises, et au renforcement des procédures de gestion de crise.

C'est une conséquence utile des récentes initiatives de conformité réglementaire, mais cela démontre également qu'une réponse efficace aux incidents est un facteur clé pour réduire l'impact réputationnel et opérationnel des incidents critiques en particulier.

La détection progresse, tout comme les menaces.

Les capacités de détection ont également continué de s'améliorer (+4 %), démontrant une efficacité accrue, notamment au sein des grandes organisations capables de mettre en place des pipelines de *detection-as-code*. Des progrès significatifs ont également été observés dans la surveillance des périmètres critiques ainsi que dans la couverture des logs dans les environnements cloud.

Cependant, ces progrès restent fragiles face à la réduction du temps d'exploitation des vulnérabilités, à des acteurs de menace plus avancés et à une surface d'attaque élargie par les identités non humaines.

La sécurité opérationnelle progresse au rythme de la cybersécurité.

Bien que les avancées technologiques depuis 2024 ne soient pas à sous-estimer, le Cyber Benchmark de cette année nous montre que **les avancées en gestion des ressources humaines restent limitées. D'importantes divergences entre secteurs subsistent** dans le ratio entre les ETP sécurité et les ETP métier, indiquant que les pressions budgétaires restent un problème cette année.

La sécurité opérationnelle semble suivre la tendance de la consolidation. Cela se voit plus directement lorsque l'on regarde les tendances sectorielles.

Détection : un défi en constante évolution

La détection est un cadre utile pour donner vie aux thèmes du Benchmark. En particulier, parmi les grandes organisations interrogées (environ 100 entreprises) qui ont mis en place des capacités de détection, on constate …

Des progrès mesurés & Des défis persistants

86 % Ont mis en place **des alertes** en cas d'**activité anormale**

77 % Surveillent et analysent régulièrement **les configurations IDP**

De bonnes performances en ITDR et en surveillance AD/Entra ID montrent une vigilance continue sur les indicateurs clés de ransomware, pour prévenir les incidents les plus critiques.

Plus largement, cela reflète un dépassement des IOC atomiques vers une détection basée sur le comportement.

48 % **Collectent** et **analysent** les journaux d'applications **métier**

22 % Créent **des cas d'usage personnalisés** pour identifier les APT

Les incidents très médiatisés (par exemple sur Salesforce, SAP ou SharePoint) montrent la nécessité de renforcer la surveillance des applications métier. De même, les campagnes récentes (par exemple Volt, Salt, Flax Typhoon) soulignent l'urgence d'implémenter des détections APT personnalisées.

Source : *Wavestone Cyber Benchmark 2025*

Que révèle le Benchmark sur les secteurs clés ?

Groupes Industriels

L'intégration de l'OT dans un cadre SOC unifié reste la tendance clé. Alors que les clients ressentent les avantages d'un modèle décentralisé (latence réduite et contexte accru), ils peinent à maintenir le même niveau de contrôle de base à travers les zones géographiques dans un marché actuellement volatil.

Par conséquent, les clients mettent en place une gouvernance évolutive et des indicateurs robustes (par exemple, évaluation continue du score d'exposition des zones OT) pour soutenir la consolidation des capacités et des performances.

Services financiers

Après un cycle de transformation axé sur la conformité et la défense fondée sur la CTI, les acteurs financiers se tournent désormais vers l'optimisation de la performance et l'amélioration des workflows de détection et de réponse grâce aux outils d'IA.

Ce changement est en partie dû à la fin des programmes et aux contraintes budgétaires, mais traduit aussi le besoin de renforcer les fondamentaux et de moderniser l'écosystème technologique face à un paysage de menaces en accélération.

Fabricants automobiles

Les fabricants automobiles font face au défi de la convergence directe, travaillant à intégrer des analyses de big data capables de gérer la télémétrie produit, de se corréler avec les sources traditionnelles de logs IT et OT, et de répondre à des exigences strictes de conformité (par exemple UNECE WP.29).

Pour y parvenir, ils déploient des solutions innovantes : visualisation du cycle de vie des mises à jour OTA pour repérer les anomalies, et règles de corrélation avec la télémétrie CAN bus pour détecter plus tôt les impacts sur les performances du véhicule.

Les tendances pour 2025 sont convergence et consolidation

Dans tous les secteurs, deux tendances majeures émergent: la convergence et la consolidation des opérations de sécurité sur les périmètres IT, OT et produits. Quels impacts concrets ont-elles ? Quatre effets majeurs, en particulier, ont retenu l'attention de nos clients :

Extension des fusion centers	Les fusion centers sont les derniers représentants du modèle de consolidation et de convergence. Les organisations qui adoptent ce modèle tentent désormais d'y intégrer la supervision des tiers, en réponse à une pression réglementaire croissante.
Test automatique des règles de détection	Les équipes SOC adoptent de plus en plus de solutions de validation automatisées afin de tester en continu leurs détections face aux TTP observés. L'objectif : améliorer l'efficacité opérationnelle et suivre le rythme des attaquants
Collaboration avec l'IA pour les activités N1	L'IA agentique apporte la capacité nécessaire pour absorber la surcharge d'alertes qui pèse sur les équipes SOC. Elle est désormais largement utilisée pour enrichir, filtrer et trier les alertes de niveau 1.
Transformation organisationnelle	Les entreprises les plus matures préparent déjà leur prochaine phase de transformation, notamment en renforçant leurs capacités de détection et de réponse. Les approches diffèrent, mais toutes reposent sur l'automatisation pour recentrer les analystes sur les tâches à forte valeur.

Comment continuer à améliorer les activités de la sécurité opérationnelles ?
C'est le thème central de cet article, dont la première section explorera l'évolution du paysage réglementaire...

02. Quels sont les enjeux majeurs en 2025 ?

Passant du stratégique au pratique, cette section se concentre sur trois défis majeurs auxquels les clients sont confrontés en 2025, et sur la manière de les surmonter.

Respect des réglementations en vigueur en 2025

Historiquement focalisée sur la supervision, la détection et la réponse, la sécurité opérationnelle doit désormais s'intégrer pleinement à la stratégie de l'entreprise et aux enjeux de conformité. Les régulateurs renforcent leurs attentes : preuve de conformité, traçabilité complète, remontée des incidents dans les délais et résilience.

Leur champ de contrôle s'étend aussi à la classification et à l'escalade des incidents, ainsi qu'à la qualité des registres et des preuves. Les équipes SecOps doivent donc prouver que leurs processus sont à la fois performants et conformes aux exigences légales et réglementaires.

Quelles sont les exigences clés auxquelles les équipes de sécurité opérationnelles doivent se plier ?

Les régulateurs ont donné la priorité à des exigences spécifiques, orientant les équipes SecOps dans différentes directions...

Prioriser la résilience opérationnelle

UE

NIS2 (*Secteurs critiques*)
Impose une détection 24h/24 et 7j/7, un signalement rapide des incidents (dans les 24 heures) et **la supervision de la *supply-chain*.**

DORA (*Services* financiers)
Exige une preuve de résilience opérationnelle, incluant la classification des incidents, **les tests de récupération** et un rapport unifié

Veiller à ce que les données clients soient protégées

Royaume - Uni

Réglementations NIS au Royaume-Uni (*secteurs critiques*)
En adéquation avec le NIS2 : impose des capacités de détection, de réponse aux incidents et **de partage de renseignements sur les menaces**

Directives RGPD / ICO au Royaume-Uni (*Toutes les org. traitant les PII*)
Nécessite **l'identification et le signalement des compromissions de données** dans un délai de 72 heures, étayés par des journaux et des preuves

Minimiser les impacts des incidents cyber

États-Unis

Règles de cybersécurité de la SEC (*Sociétés cotées en bourse*)
Exige **la divulgation des incidents cybernétiques importants** dans les 4 jours – ce qui pousse à une détection et une escalade rapides.

GLBA / FFIEC (*Services financiers*)
Applique les exigences de détection des menaces, **de procédures de réponse** et d'efficacité des contrôles.

Et promouvoir la souveraineté des données

Chine

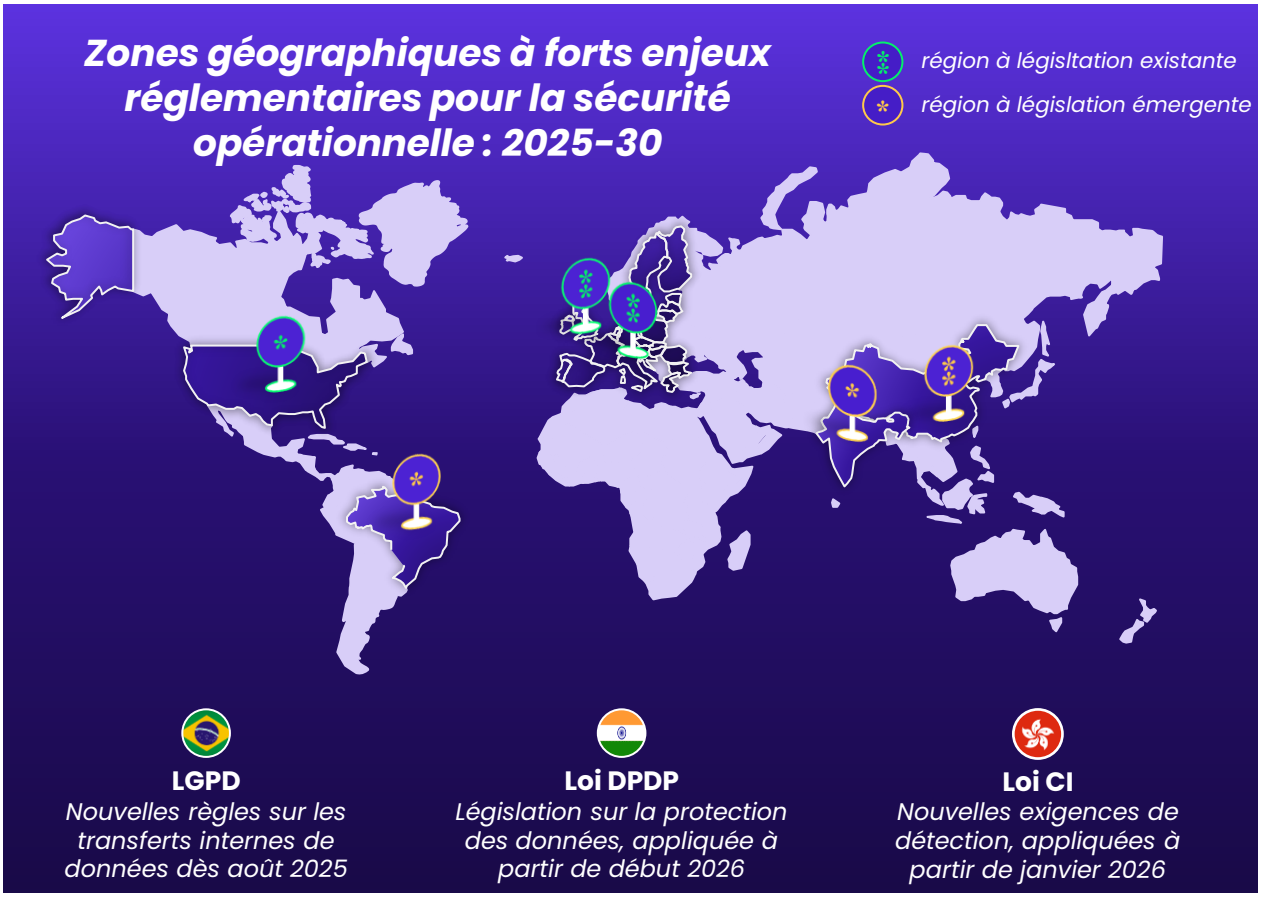
Cybersécurité, sécurité des données, lois sur la protection des informations personnelles (*tous les opérateurs réseau, CIIO, entités traitant les PII*)
Localisation des données, surveillance en temps réel, signalement d'incidents dans un délai de 1 à 4 heures, évaluations **de la sécurité des transferts** transfrontaliers.

Naviguer dans la conformité réglementaire cyber post-2025

Quelles nouvelles exigences faut-il surveiller ?

Malgré les différences régionales, des attentes communes émergent : documentation des procédures de réponse aux incidents, preuves de sauvegarde et de capacité de restauration des données, journalisation complète et visibilité sur les risques liés aux tiers.

La remontée des incidents en temps réel à destination des parties prenantes internes et externes devient une exigence standard dans toutes les juridictions.



Préparation à l'audit réglementaire

Les équipes de sécurité opérationnelle doivent évaluer leur niveau de préparation face aux nouvelles exigences opérationnelles. Cela implique de revoir les procédures de réponse aux incidents, de s'assurer que la journalisation garantit une traçabilité suffisante et de vérifier que les procédures d'escalade respectent les délais imposés par la réglementation.

L'intégration avec les fonctions de gouvernance et de gestion des risques (GRC) est essentielle pour aligner opérations techniques et obligations légales.

Les organisations doivent aussi analyser leur résilience, notamment leur capacité de reprise après incident et le maintien de la continuité. La gestion des risques liés aux tiers doit également être intégrée à la sécurité opérationnelle, avec une visibilité claire sur les contrôles fournisseurs et les obligations contractuelles.

Surmonter le défi de la main-d'œuvre SOC

Quel est le problème?

Dans un paysage de menaces toujours plus complexe, les SOC font face à une pression croissante pour garder une longueur d'avance. Ces contraintes, ajoutées aux pressions internes, les poussent à rester proactifs et efficaces.

Malgré l'augmentation du nombre de diplômés en cybersécurité, les entreprises manquent de compétences techniques avancées, telles que le test d'intrusion, ce qui limite la proactivité des SOC. Par ailleurs, la forte charge de travail accroît stress et turnover, réduisant encore leur efficacité.

Quelle sont les solutions ?

1. Tirer parti des opportunités technologiques

Les avancées en automatisation et l'apparition d'outils basés sur l'IA transforment la sécurité opérationnelle et offrent de nouvelles possibilités pour les SOC modernes. En filtrant le bruit, en réduisant les faux positifs et en simplifiant le triage, ces technologies permettent aux analystes de se concentrer sur les menaces critiques plutôt que sur les alertes routinières. L'automatisation accélère la réponse à incident et ouvre la voie au développement de compétences avancées comme le threat-hunting, l'investigation forensique et le développement de stratégies de défense proactive.

2. Renforcer la formation et le soutien

Des parcours de formation clairs et le développement de plans de progression de carrière sont essentiels pour construire un SOC proactifs et résilient face à un paysage de menaces de plus en plus complexe.

30%

des entreprises signalent un manque de compétences techniques avancées *(UK Government, 2025)*

4.8 M

postes vacants dans le monde *(ICS2, 2024)*

70%

des analystes SOC déclarent être soumis à un stress élevé *(Cassetto, 2025)*

3. Maximiser les bénéfices de l'équipe conjointe

Les analystes doivent maîtriser l'interprétation des données générées par l'IA et savoir quand intervenir. Cela nécessite une formation solide et un mentorat des cadres ou des experts, ainsi qu'un environnement collaboratif favorisant le partage des connaissances. Enfin, un cadre de travail bienveillant, avec soutien en santé mentale et flexibilité, est indispensable pour maintenir des équipes résilientes et motivées.

Pour quels résultats ?

Suivre ces résolutions permet de construire un SOC plus efficace et résilient, où les charges de travail sont équilibrées, les délais de traitement réduits et les risques d'épuisement limités. Toutefois, les SOC doivent veiller à une bonne configuration de ces outils et former les analystes pour en garantir une utilisation optimale.

Faire de la transformation du SOC un objectif rentable

À mesure que le cadre réglementaire se précise, les organisations doivent être en mesure de justifier les investissements dans les SOC auprès de leur direction.

Estimation du coût vs valeur : La prévention des incidents

L'investissement dans un SOC comporte des coûts initiaux et récurrents (technologies, personnel, processus), tandis que sa valeur réside dans la réduction des impacts financiers liés aux cyber-incidents. Une détection rapide peut permettre d'éviter des pertes majeures liées aux fuites de données, ransomwares ou interruptions de service, offrant ainsi un retour sur investissement mesurable. Un SOC améliore aussi l'efficacité opérationnelle grâce à l'automatisation, à la priorisation des menaces et à une centralisation de la supervision. L'optimisation du SOC permet ainsi de couvrir plus de risques avec moins de ressources.

Aligner les objectifs du SOC et du conseil d'administration

Pour obtenir le soutien du conseil d'administration, les avantages du SOC doivent être présentés en termes de résilience, de conformité et de réputation. Une détection plus rapide des menaces favorise la continuité des activités. Une surveillance centralisée simplifie la préparation des audits et la production de rapports réglementaires. Une défense proactive réduit le risque d'incidents portant atteinte à la réputation de l'entreprise..

Des indicateurs comme le temps de détection et de réponse, la baisse des temps d'arrêt et les amendes évitées peuvent permettre de convertir les performances techniques du SOC en valeur business.

Dériver la valeur commerciale à partir des données du SOC

Les SOC modernes produisent des données utiles à une gestion des risques étendue. Les Fusion Center, qui regroupent cybersécurité, fraude, menace interne et sécurité physique, offrent une meilleure contextualisation et une réponse plus rapide. Les données du SOC permettent aussi d'identifier des tendances pour faciliter les décisions stratégiques.

Un business-case solide pour moderniser le SOC doit refléter le profil de risque, les obligations réglementaires et les objectifs stratégiques de l'organisation. Il doit illustrer comment le SOC réduit les risques, soutient la mise en conformité et génère une valeur mesurable. Le coût de l'investissement doit être comparé au coût de l'inaction, souvent bien plus élevé face aux menaces actuelles.

« Pour obtenir le soutien du conseil d'administration, les avantages du SOC doivent être présentés en termes de résilience, de conformité et de réputation. »

Saaid Mohamoud
Consultant Senior

03. Quelles sont les prochaines étapes pour la sécurité opérationnelle ?

Cette dernière section aborde les tendances émergentes qui indiquent comment le rôle des équipes de sécurité opérationnelle continuera d'évoluer dans le futur.

XDR : stratégie pour une mise en œuvre durable

Depuis 2018, les outils d'*Extended Detection and Response* (XDR) ont gagné en popularité dans le paysage de la sécurité opérationnelle, soutenus par des promesses convaincantes : détection proactive et capacités de sécurité unifiées (deux défis majeurs déjà mis en avant dans notre Livre blanc 2024).

Cependant, les perceptions de ce que sont les XDR varient. La définition est souvent informelle, mélant aspects techniques et jargon commercial.

Au fond, **XDR est un modèle architectural conçu pour briser les silos** et relier des outils de sécurité auparavant isolés.

En pratique, cette approche renforce la sécurité opérationnelle: le XDR centralise, corrèle et enrichit les données issues de multiples sources, détecte les menaces et automatise les réponses, tout en réduisant le nombre de portails, de plateformes et de licences à gérer.

Gartner définit deux types ...

Le XDR ouvert (open XDR) propose des connecteurs vers plusieurs solutions de fournisseurs, adoptant pleinement la philosophie XDR en brisant les silos.

Le XDR fermé (closed XDR) propose une plateforme unique regroupant tous les outils de sécurité, assurant une intégration fluide et simplifiant les processus métiers, mais au risque d'entraîner un verrouillage durable auprès d'un fournisseur.

Les plateformes XDR peuvent être très utiles pour atteindre une haute maturité de sécurité et réduire fortement les temps de détection et de réponse dans un environnement en constante évolution.

Cependant, déterminer si un XDR est nécessaire à votre organisation et, le cas échéant, lequel choisir reste complexe. Voici un résumé des principaux points à considérer.

Les questions clés pour définir sa stratégie XDR

Votre socle de sécurité est-il adapté ?	Quelle stratégie de changement adopter ?	Ce changement est-il nécessaire ?
Bien que les plateformes XDR représentent une opportunité de simplifier et d'augmenter l'efficacité opérationnelle, elles nécessitent que les capacités sous-jacentes soient déjà matures pour être efficaces. La maturité de la gestion des données, de la Threat intelligence, et de l'intégration des outils entre eux a un impact significatif sur l'efficacité opérationnelle d'une plateforme XDR.	À long terme, les plateformes XDR ouvertes offrent de nombreux avantages sans exiger une refonte complète de votre stack technologique, mais leur adoption implique une gestion opérationnelle plus complexe. À l'inverse, les plateformes XDR fermées nécessitent un changement initial important (avec plusieurs migrations d'outils en parallèle), mais permettent d'obtenir plus rapidement simplification et valeur.	Quel que soit le type choisi, une analyse approfondie, une planification rigoureuse et un long travail de transformation technique et opérationnelle sont inévitables. Lors du choix des outils, les aspects métiers et financiers doivent être croisés avec les objectifs du SOC, en s'appuyant sur des indicateurs de performance, de risque et de conformité clairement définis, avec leurs cibles associées.

IA agentique et sécurité opérationnelle : les enjeux

Avec l'IA « Big Sleep » de Google qui corrige désormais autonomement les vulnérabilités avant les humains, **l'urgence d'équilibrer la précision machine et la supervision humaine dans les opérations de sécurité a atteint un point d'inflexion** critique.

Dans ce qui suit, nous chercherons à prouver que, bien que l'automatisation progresse rapidement dans les opérations de sécurité, la supervision humaine reste vitale.

Les analystes apportent un jugement contextuel que l'IA ne possède pas, mais auquel elle peut apporter son support. En conséquence, les experts universitaires et en cybersécurité soutiennent une approche d'« autonomie calibrée », qui ajuste le niveau de contrôle de la machine en fonction du degré de confiance et de la sensibilité de la tâche.

L'IA ne remplacera pas les analysts, mais les assistera

L'IA peut aider à réduire l'épuisement des analystes SOC, non pas comme un outil strictement déterministe, mais comme un "partenaire d'apprentissage" permettant d'ouvrir la voie à des fonctions plus adaptatives et contextualisées. Les chercheurs parlent d'un paradigme de "co-teaming" visant à guider les décisions des analystes sans les remplacer.

Dans ce modèle, les agents IA renforcent les workflows du SOC en intégrant et en transmettant des connaissances, ce qui soutient une prise de décision plus dynamique et surtout proactive. Par exemple, l'attaque contre Sony, attribuée à la Corée du Nord, a commencé par une campagne de phishing. Albanese et al. (P. 16, 2025) estiment que le "co-teaming" aurait permis d'intégrer les signaux géopolitiques, d'harmoniser des données disparates et d'exploiter les modèles LLM pour une analyse contextuelle en temps réel, fournissant aux analystes des renseignements exploitables bien avant que l'attaque n'atteigne les seuils de détection avancée propres à un SOC automatisé.

Wavestone observe déjà comment les LLM complètent (plutôt que remplacent) les opérations de sécurité, notamment via le déploiement d'agents Copilot pour mobiliser documentations internes et retours d'expérience afin d'adopter une posture de défense dynamique.

Ainsi, les modèles de "co-teaming" offrent une voie pragmatique pour les organisations cherchant à intégrer l'IA sans recourir à une approche tout ou rien. Elles pourraient tirer parti de l'IA en entraînant itérativement les agents à partir de renseignements internes sur les menaces et de données historiques d'incidents, afin de soutenir la décision contextuelle et renforcer la confiance par une valeur démontrable.

Le fait est que **les analystes humains restent essentiels pour mettre en œuvre une stratégie de défense « proactive »**, à savoir prendre des décisions plus larges, fondées sur des preuves et nuancées. Sous cet angle, le "co-teaming" en IA représente un facilitateur stratégique pour une défense proactive, et pas seulement un triage réactif, qui peut aider les organisations à aligner les initiatives IA sur leur stratégie de résilience et de risque.

Comment parvenir à une autonomie calibrée, capable d'ajuster le contrôle automatisé selon la confiance envers l'IA et la sensibilité de la tâche ?

Les données de sécurité, un levier stratégique

Puisque la donnée reste une ressource précieuse, les équipes SecOps exploitent leurs propres ressources pour en tirer information et valeur.

L'usage de modèles de données massifs et d'architectures de collecte toujours plus complexes reste une tendance forte chez nos clients. On met souvent l'accent sur ce que cela impose aux équipes sécurité: devoir héberger et traiter d'immenses volumes de données pour suivre des activités comme les outils GenAI, la robotique industrielle ou les produits connectés, mais on passe à côté d'une évidence :

Le SOC est souvent le plus datalake de l'entreprise.

Mais, que font les équipes SecOps de toutes ces données ?

1. Saisir l'opportunité de consolider des services de surveillance disparates dans un SOC global conjoint (JSOC) : De plus en plus d'organisations regroupent sous un même périmètre la sécurité physique, la fraude ou l'OT. Cette convergence permet de mutualiser l'infrastructure data, d'ouvrir de nouvelles capacités d'analyse et de réduire les coûts. Elle favorise aussi un travail plus étroit entre équipes, créant des opportunités de corrélation, d'enrichissement et d'investigation plus complètes. Bien menée, cette convergence dépasse la simple efficacité opérationnelle pour devenir un véritable atout de sécurité.

2. Exploiter cet actif de données unique pour créer de la valeur métier:
Avec une telle richesse de données issues des systèmes techniques comme des systèmes métiers, l'application de véritables méthodes de data science peut révéler de nouvelles informations stratégiques. Elle permettrait notamment:

- D'Identifier les tendances commerciales pour les produits, ou des tendances clients pour améliorer les services.
- De gagner en efficacité dans les processus métier et opérationnels
- D'automatiser pour les contrôles de sécurité et de performance de l'entreprise

Les bénéfices n'arrivent pas en un jour, les problèmes si

Alors, quels sont les points clés ?

- **Qualité des données et cohérence à travers toutes les sources** :
  Les résultats ne valent que par la qualité des données en entrée.
- **Forte collaboration entre équipes**
  Le contexte est essentiel et nécessite une intégration entre le SOC et les métiers qui manipulent la donnée au quotidien.
- **Correspondance des compétences**
  S'assurer que vos équipes sont bien formées pour soutenir de tels processus complexes est essentiel.

L'avenir appartient aux organisations qui voient les données de sécurité opérationnelle non comme un coffre-fort réservé à la sécurité, mais comme un prisme révélant risques et opportunités.

Henry James
Consultant SecOps

Réflexions finales

Pour conclure, revenons à la trajectoire du marché à long terme et aux éléments à anticiper au-delà de l'horizon aujourd'hui perceptible.

L'avenir de la sécurité opérationnelle

Nous présentons ici trois tendances émergentes et les priorités des entreprises les plus matures.

1. Gestion dynamique des risques

Une évolution vers des capacités de détection et de réponse agentiques

En 2024, nous annoncions l'essor de la détection as code ; elle est désormais bien intégrée.

La nouveauté, c'est l'essor de la détection agentique : la GenAI peut désormais générer la logique de détection à partir de la threat-intelligence, tandis que des agents IA s'intègrent aux outils BAS pour les tester et déployer ensuite des règles de façon autonome.

Associé avec une approche GRC, nos clients peuvent aller plus loin : les scores de risque pourraient s'ajuster dynamiquement selon la télémétrie, les alertes et les actions pour adapter les contrôles en temps réel.

2. Préparation au Q-Day

Développement d'un SOC prêt pour le quantique

Avec l'arrivée prochaine de l'ordinateur quantique, les clients les plus matures évaluent leur exposition à la menace quantique.

La sécurité opérationnelle jouera un rôle clé dans cette transition : elle devra surveiller les activités d'exfiltration liées au modèle "collect now, decrypt later", tout en protégeant l'architecture et le pipeline de données du SOC contre les menaces émergentes.

Les clients se préparent déjà à la cryptographie post-quantique lors du déploiement du ZTNA, et modélisent les menaces pour identifier les scénarios qu'ils pourraient rencontrer à l'avenir.

3. SecOps ou cyber-résilience ?

Les RSSI envisagent la convergence de SecOps, OpRes et GRC

Alors que les silos organisationnels entre ces équipes s'effacent, les organisations matures commencent à envisager comment elles pourraient consolider et/ou faire converger ces fonctions dans des équipes de résilience cyber unifiées.

Tout d'abord, les clients intègrent des ingénieurs GRC dans leurs équipes SecOps.

Les organisations les plus avancées mettent en place des centres de compétences partagés, soutenus par des plateformes unifiées, des modèles de données communs et des taxonomies d'incidents harmonisées, permettant une prise de décision plus rapide et une exécution plus cohérente sur l'ensemble du cycle de vie de la sécurité.

Conclusion

Alors, où va le marché ?

Il est clair que la détection et la réponse resteront des sujets majeurs à l'horizon 2030. Comme évoqué tout au long de ce document, nous pensons être actuellement dans une *Sattelzeit* (une période charnière) où nous gérons la transition d'un cycle de transformation vers le suivant.

Cela se reflète dans notre premier thème clé: la consolidation. Elle s'observe aussi bien au sein des équipes SecOps qu'à travers les dynamiques plus larges de fusions-acquisitions (comme les rachats de Trustwave puis de Stroz Friedberg par LevelBlue). Cette phase est loin d'être terminée et continuera d'influencer les tendances à moyen terme, surtout dans un contexte de volatilité économique, commerciale et réglementaire.

Ce changement dans les tendances du marché indique une évolution plus large des attitudes parmi les entreprises de toutes tailles. Beaucoup envisagent désormais de manière proactive les implications des nouvelles offres technologiques et de l'investissement croissant dans l'IA agentique et générative en particulier, afin de revoir leurs modèles d'exploitation et stack technologiques, afin de suivre la sophistication croissante des cyberattaques et de ne pas devenir la prochaine victime.

Au-delà de cela, la question naturelle est : ***à quoi ressemblera cette transformation ?***

Le mot d'ordre des cinq prochaines années est la rapidité. Tout s'accélère: interactions commerciales, développement technologique, et acteurs malveillants...

S'appuyant sur leurs bases solides et leur succès, les équipes SecOps devront suivre ce rythme et ce dynamisme. Par conséquent, nous sommes convaincus qu'il sera nécessaire de se transformer pour adopter une approche plus résiliente.

Les objectifs stratégiques de simplification, d'évolution et de démonstration du ROI en sont le moteur ; l'impératif commercial de centralisation sur le client poussera à briser davantage les silos et obligera le SOC à dépasser la simple logique de triage pour ne plus être perçu comme un centre de coûts.

Le moment est venu de passer à des capacités SecOps réellement dynamiques. La question est désormais : comment allez-vous vous y prendre ?

Francesca Kempster
Senior Manager
Responsable SecOps au Royaume-Uni

Nous entrons dans une période riche en opportunités passionnantes pour la sécurité opérationnelle. Plus que jamais, nous disposons des outils nécessaires pour la transformer en profondeur.
Profitons de cette dynamique pour initier une évolution stratégique majeure.

Benoît Marion
Senior Manager
Expert SOC - France

Rédacteurs en chef

Francesca Kempster

Senior Manager

James Maidment

Consultant Senior

Remerciements

Chacun des sujets abordés ici est apparu à l'origine sous forme de publications LinkedIn individuelles rédigées par l'équipe SecOps au Royaume-Uni.

Nous adressons un remerciement particulier aux rédacteurs cités ci-dessous, dont les contributions ont largement nourri cet article.

Fatima Azim

Consultant

Henry James

Consultant

Matthew Hood

Consultant

Euan Fairweather

Consultant

Saaid Mohamoud

Consultant Senior

Martin Grégoire

Analyst

Traduction

Antoine d'Estalenx

Consultant Senior

Ayoub El Moutaouakkil

Consultant

À propos de Wavestone

Wavestone est un cabinet de conseil qui a pour mission d'accompagner les entreprises et organisations dans leurs transformations stratégiques. Présents à l'échelle internationale, nous sommes aux côtés de nos clients dans toutes les régions du monde pour relever les défis d'un marché très concurrentiel et en constante évolution.

En s'appuyant sur plus de 5 500 collaborateurs à travers l'Europe, l'Amérique du Nord et l'Asie, le cabinet dispose d'expertises sectorielles de premier plan complétées par un portefeuille de savoir-faire cross-sectoriels permettant d'adresser à 360° les grands programmes de transformation.

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

www.wavestone.com