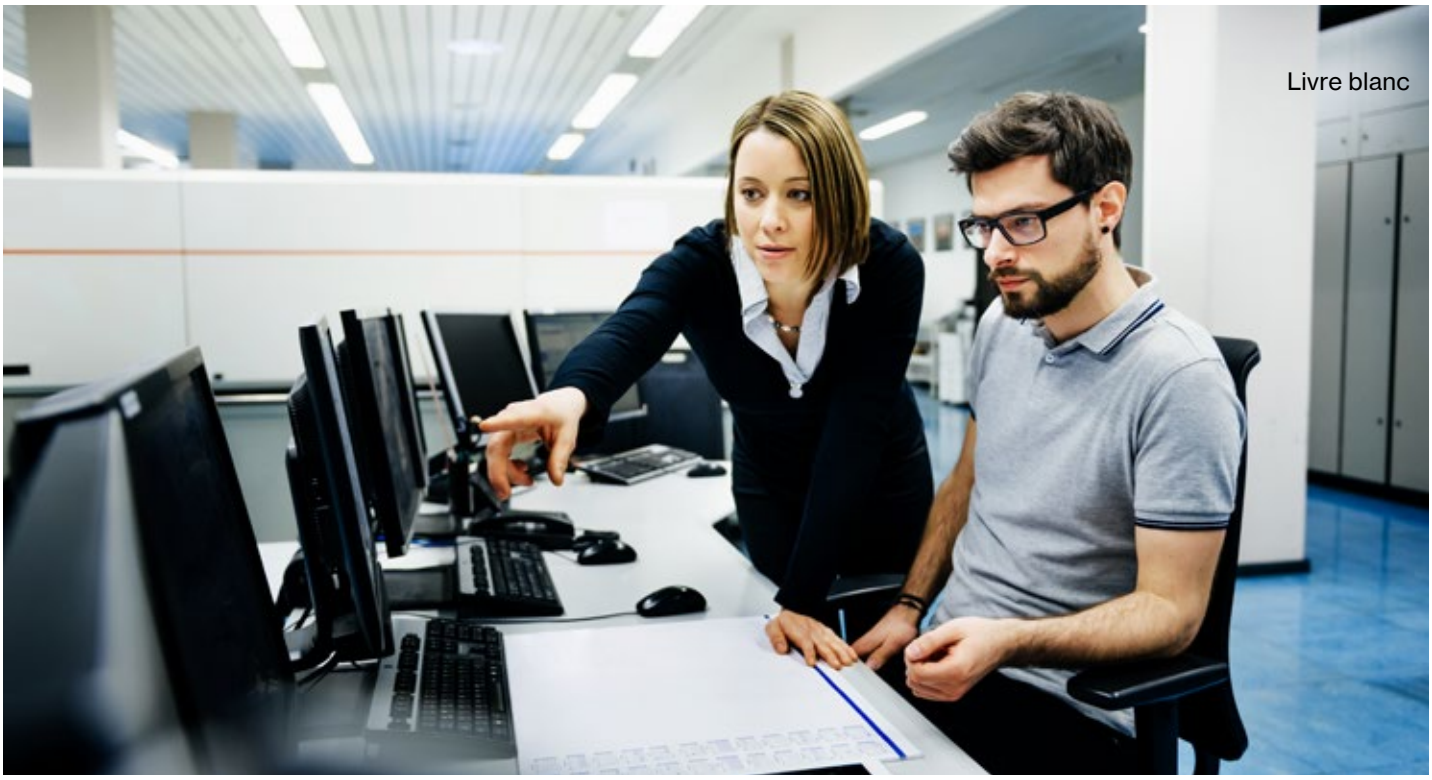
Livre blanc

Cap sur le SOC nouvelle génération

Trouver le juste équilibre entre risques, ressources et réalité

verizon business



À l'ère des cybermenaces incessantes, un centre des opérations de sécurité (SOC, *Security Operations Center*) constitue le poste de contrôle de la cybersécurité d'une entreprise. Sa mission : surveiller les alertes, détecter les incidents et répondre aux menaces en temps réel.

Dans cette optique, l'efficacité de votre cybersécurité passe par un bon équilibre entre d'une part votre tolérance au risque, et d'autre part l'expertise et les ressources disponibles. Interne, hybride ou externalisé, le SOC se décline en différents modèles. Avant d'opter pour telle ou telle approche, les entreprises doivent prendre en compte plusieurs critères : assets critiques, tolérance au risque, exigences réglementaires et enveloppe budgétaire.

Si un SOC interne offre un contrôle complet sur les opérations et les mesures de sécurité, il nécessite toutefois un investissement initial conséquent. À cela s'ajoutent les coûts technologiques et humains pour assurer une protection optimale et réduire les risques.

À l'inverse, un SOC managé met à votre disposition des analystes chevronnés qui possèdent une perspective mondiale sur les menaces et gardent l'œil sur vos opérations 24 h/7 j. Capacités, technologies, expertise, scalabilité… les entreprises n'ont qu'à puiser dans ces ressources déjà en place, sans avoir à investir du temps, des budgets et des efforts dans la mise en place d'un SOC interne.

Nombre de structures optent pour une approche hybride. Elles décident de confier à un partenaire les opérations quotidiennes pour laisser leurs propres équipes se recentrer sur les missions et décisions plus stratégiques.

Équipes, technologies, processus : les trois piliers d'un SOC interne

La technologie constitue un rouage essentiel de toute stratégie de cyberdéfense. Gestion des événements et des informations de sécurité (SIEM), automatisation et réponse aux incidents de sécurité (SOAR), détection et réponse sur les terminaux (EDR)… tous ces outils de sécurité essentiels fonctionnent en synergie pour identifier, investiguer et neutraliser les menaces.

Face à l'omniprésence des services cloud dans la majorité des écosystèmes technologiques, le SOC doit débusquer les erreurs de configuration, les vulnérabilités des interfaces de programmation d'applications (API) et les accès non autorisés dans des environnements hybrides et dynamiques. D'où la nécessité d'une approche Zero Trust qui implique de vérifier en permanence chaque utilisateur, appareil et application. Le but : réduire le risque d'accès malveillant aux systèmes et données sensibles. En clair, le SOC nouvelle génération a pour objectif de détecter les anomalies en temps réel et d'automatiser la neutralisation des menaces avant qu'elles ne se transforment en compromissions majeures.

Aujourd'hui, les cybercriminels misent toujours plus sur l'intelligence artificielle (IA) pour automatiser les attaques et accélérer la détection des vulnérabilités, la personnalisation des campagnes de phishing et l'obfuscation des malwares à grande échelle. Cependant, les attaquants n'ont pas le monopole de cette technologie. Côté défense, le SOC peut actionner le tandem IA/ML pour repérer plus rapidement les comportements anormaux, automatiser le tri et effectuer des analyses prédictives. Ces outils filtrent les faux positifs et permettent aux analystes de se recentrer sur les menaces prioritaires.

Les nouvelles menaces dépassent largement le champ des malwares traditionnels. Entre deep fakes et usurpation vocale, le phishing dopé à l'IA complique la détection des tactiques d'ingénierie sociale. Le SOC doit donc s'adapter et ériger la surveillance continue en véritable rempart.

Flux CTI complets, analytique pilotée par IA, suivi des comportements en temps réel… ces outils permettent au SOC d'identifier les nouvelles tactiques des attaquants en amont pour garder un coup d'avance sur eux.

L'importance du facteur humain

Sur la ligne de front, les analystes SOC et les threat hunters sont les premiers à intervenir pour trier les alertes et les faux positifs. Les cas les plus complexes font l'objet d'un processus d'escalade pour une analyse approfondie, un endiguement de la menace et une réponse coordonnée.

Étude des méthodes d'attaque, détection des anomalies, identification des tactiques susceptibles d'échapper aux contrôles de sécurité traditionnels... telles sont en substance les trois grandes missions des analystes SOC.

Des compétences très recherchées qui exigent de maîtriser la réponse à incident en temps réel, les méthodologies d'attaque et la Threat Intelligence.

Face à la pénurie chronique de professionnels de la cybersécurité, nombre d'entreprises misent sur la montée en compétences de leurs équipes IT. Le problème, c'est que ce processus de longue haleine expose l'entreprise aux cyberattaques pendant la phase transitoire.

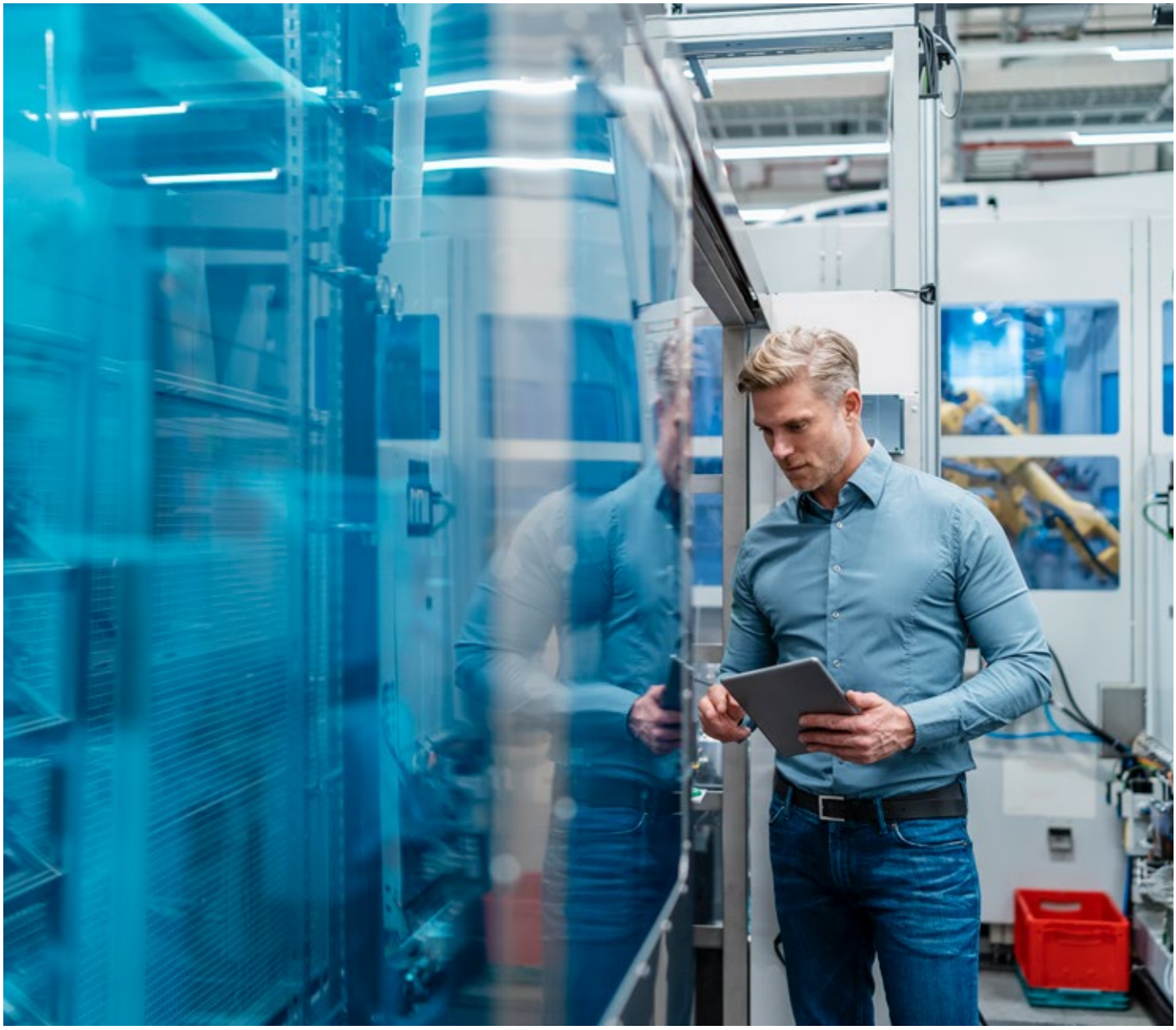
Autre impératif, disposer des talents et ressources nécessaires pour assurer une surveillance de la sécurité et une réponse à incident performantes H 24.

Processus : ITOps, détection des menaces et playbooks

Véritable ciment de l'entreprise, les processus ont pour vocation d'unifier les technologies et les équipes. Ainsi, les processus des opérations IT (ITOps) définissent des niveaux de risque acceptables en fixant des workflows et des limites. Ils contribuent également à déterminer les responsabilités et à imposer aux équipes de sécurité d'effectuer les mises à niveau, d'installer les correctifs et d'escalader les alertes conformément aux politiques définies.

En matière de détection des menaces, les processus doivent être dynamiques et constamment affinés pour anticiper les nouveaux dangers. Sans maintenance et évaluation régulières, la visibilité des équipes sur les risques connus et potentiels s'amoindrira au fil du temps.

Enfin, les entreprises doivent pouvoir compter sur des playbooks clairs pour investiguer et gérer correctement les alertes de sécurité. L'amélioration des processus exige donc des ressources dédiées, garantissant leur efficacité et leur pertinence face à l'évolution des menaces et des vulnérabilités.



Deuxième approche : l'externalisation

Confier les fonctions SOC à un partenaire permet de faire des économies, de scalabiliser les opérations de sécurité et de bénéficier d'une expertise de pointe. Au lieu de gérer une équipe interne à 100 %, les entreprises accèdent à une surveillance, une automatisation, une Threat Intelligence et des conseils d'experts 24/7. Le partenaire ne se contente pas d'offrir des services : il opère comme une équipe de sécurité intégrée. Cette approche peut directement réduire les coûts et répercussions d'une cyberattaque pour l'entreprise et ses clients.

Seulement voilà, tous les prestataires SOC ne se valent pas. Leurs prestations varient. Ainsi, les fournisseurs de services de sécurité managés (MSSP) mettent l'accent sur la surveillance des journaux, la détection des vulnérabilités et la conformité. S'ils produisent les rapports et assurent le suivi indispensables au respect des exigences réglementaires, le threat hunting et la réponse active ne figurent pas en tête de leurs priorités.

Pour les entreprises dépourvues d'une équipe IR interne, les services managés de détection et de réponse (MDR) permettent de combler ces lacunes.

Le SOC hybride, la troisième voie

La co-gestion du SOC permet aux entreprises de garder le contrôle sur les fonctions de sécurité critiques tout en externalisant la surveillance 24/7, l'automatisation et la Threat Intelligence. Non seulement l'équipe interne gagne en flexibilité et conserve la main sur les opérations à haut risque, mais elle bénéficie aussi du renfort de spécialistes IR et de la détection des menaces.

De nombreux critères interviennent dans le choix d'un partenaire SOC : connaissance du secteur, temps de réponse, maîtrise des enjeux de conformité, Threat Intelligence pilotée par IA, etc. Tous ces facteurs méritent un examen minutieux. Votre partenaire doit répondre à vos exigences de sécurité, s'intégrer efficacement à vos équipes internes et apporter la couverture nécessaire pour détecter les menaces et répondre aux incidents en temps réel.

L'efficacité et l'adaptabilité d'un SOC hybride exigent du fournisseur une intégration flexible et transparente des processus et des technologies. Ne négligez pas ces aspects.

Coût, risque et expertise : 3 points essentiels

Indéniablement, une entreprise qui crée un SOC interne pour répondre à toutes ses spécificités (exigences stratégiques et opérationnelles, exposition aux risques, obligations réglementaires, etc.) bénéficie d'un plus grand contrôle sur ses données et ses SecOps.

En contrepartie, ce dispositif sur mesure requiert d'investir constamment dans les technologies et les compétences en cybersécurité. Entre la modernisation de leurs outils de sécurité et le recrutement, la formation et la fidélisation des talents dans un marché du travail ultra-compétitif, les entreprises doivent être présentes sur tous les fronts.

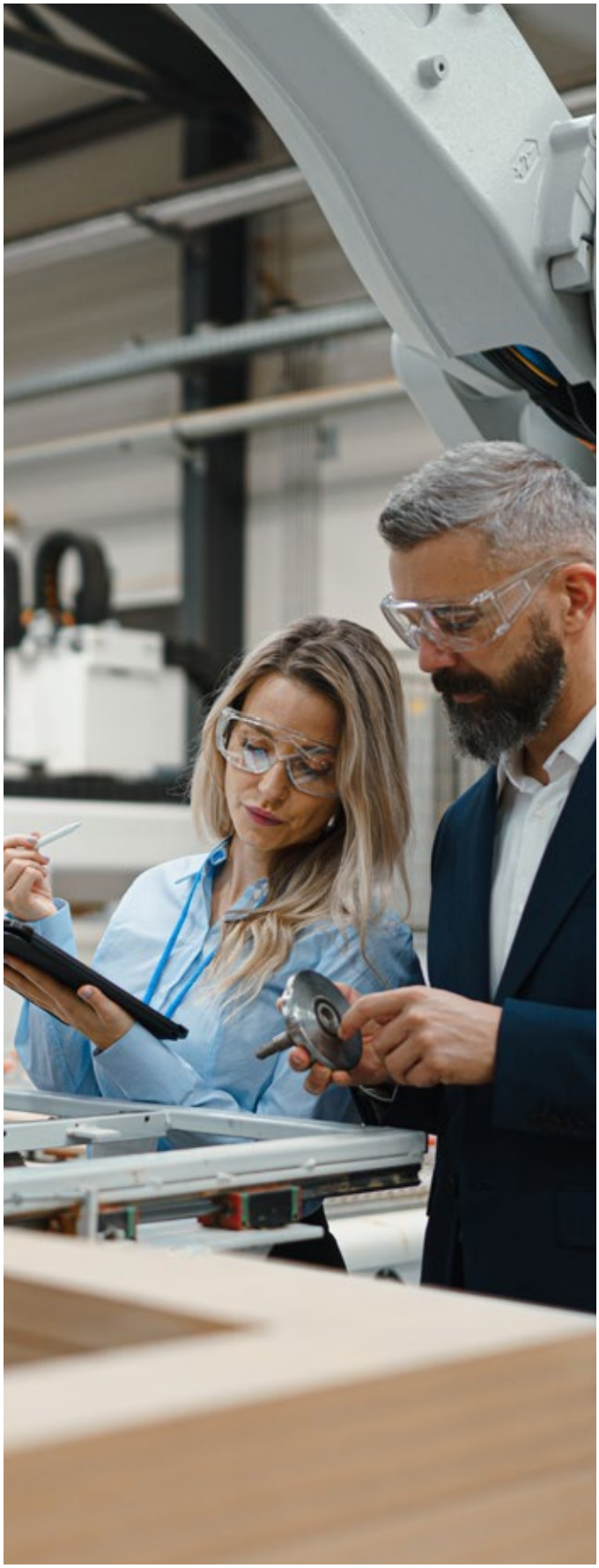
L'alternative au SOC interne consiste à faire appel à un partenaire qui propose un éventail de services réactifs et personnalisables de gestion des incidents. Il est possible d'intégrer ce prestataire aux capacités IT et de sécurité de l'entreprise par la création d'une équipe dédiée qui se coulera parfaitement dans l'infrastructure et la culture de l'entreprise. Cette approche garantit la présence d'une cellule de sécurité sur mesure et disponible H24.

Chaque modèle de SOC présente des avantages et des inconvénients. Si les équipes internes maîtrisent l'environnement, les risques et les objectifs de l'entreprise dans ses moindres détails, l'acquisition et le maintien de ces savoirs et compétences coûtent cher et prennent du temps. Développer et fidéliser les talents n'a rien d'une formalité. En outre, la phase de mise en place peut engendrer une augmentation des cyber-risques. À l'inverse, le recours à un SOC externe apporte une scalabilité et une expertise immédiates. Revers de la médaille, ce prestataire ne dispose pas de la même maîtrise de l'environnement ni de la présence sur site qu'une équipe maison. Interne, hybride, externalisé… quel que soit le type de SOC que vous choisissez, plusieurs critères rentrent en ligne de compte : compatibilité des cultures d'entreprise, maîtrise des solutions de sécurité existantes, conformité réglementaire et appétence pour plus de flexibilité opérationnelle.

Dans tous les cas, votre SOC doit se conformer aux exigences réglementaires et sectorielles en matière de sécurité. Les réglementations imposent aux entreprises de mener une surveillance, des audits et une gouvernance proactive de la sécurité pour garantir la conformité.

Loin d'être un projet ponctuel et définitif, la création d'un SOC relève d'un processus évolutif qui implique une surveillance, une maintenance et une adaptation de tous les instants. Cette nécessité de s'adapter s'explique non seulement par l'évolution et la sophistication constantes des menaces en présence, mais aussi par un changement des besoins métiers exigeant toujours plus de réactivité et de rentabilité.

Force est de constater que sans un investissement soutenu dans les nouvelles technologies, les compétences et les stratégies de sécurité, même le SOC le plus en pointe peut vite perdre en efficacité et devenir obsolète.



En savoir plus

Pour faire les bons choix et trouver une approche SOC à la hauteur de vos exigences, contactez votre responsable de compte Verizon Business, par e-mail à info@verizonenterprise.com ou rendez-vous sur verizon.com/business/fr-fr/contact-us/.