Guide du modèle SOC

FONDAMENTAL Actualisé le 5 avril 2023, publié le 19 octobre 2021 - ID G00 754096 - 12 min de lecture

Par John Collins , Mitchell Schneider , **et 1 de plus**

Choisir le modèle de centre d'opérations de sécurité approprié est difficile, choisir le mauvais modèle de SOC peut entraîner une mauvaise posture de sécurité, un risque accru et des équipes de sécurité surmenées. Les responsables de la sécurité et de la gestion des risques doivent utiliser ce guide pour identifier le modèle qui correspond à leurs besoins.

Aperçu

Principales conclusions

- Les exigences du centre d'opérations de sécurité (SOC) sont souvent sous-étendues et mal alignées dans l'ensemble de l'organisation, ce qui entraîne une insatisfaction quant à la performance de la fonction SOC.
- Le fait de ne pas reconnaître les différences entre les différentes options de modèle SOC oblige les organisations à sélectionner une implémentation obsolète ou sur mesure qui ne répond pas aux objectifs de sécurité.
- L'exploitation d'un SOC de manière linéaire ou statique sans tenir compte des modifications des exigences organisationnelles et/ou du paysage des menaces entraîne une dégradation du SOC .

Recommandations

Les responsables de la sécurité et de la gestion des risques doivent s'assurer que leur processus de sélection du modèle de centre d'opérations de sécurité est en mesure de :

- Évaluez les feuilles de route de l'architecture informatique , la dotation en personnel, les processus et les priorités commerciales pour déterminer le bon modèle SOC.
- Utilisez le guide du modèle SOC Hybrid-Internal-Tiered (HIT) de Gartner pour identifier un modèle qui correspond le mieux aux exigences et aux besoins de l'organisation.
- Évaluez en permanence le modèle SOC pour permettre l'identification des ajustements nécessaires en fonction de l'évolution des besoins de l'entreprise, des cas d'utilisation, des ressources disponibles, des risques, des menaces et des facteurs environnementaux.

Hypothèses de planification stratégique

D'ici 2025, 90 % des SOC du G2000 utiliseront un modèle hybride en externalisant au moins 50 % de la charge de travail opérationnelle.

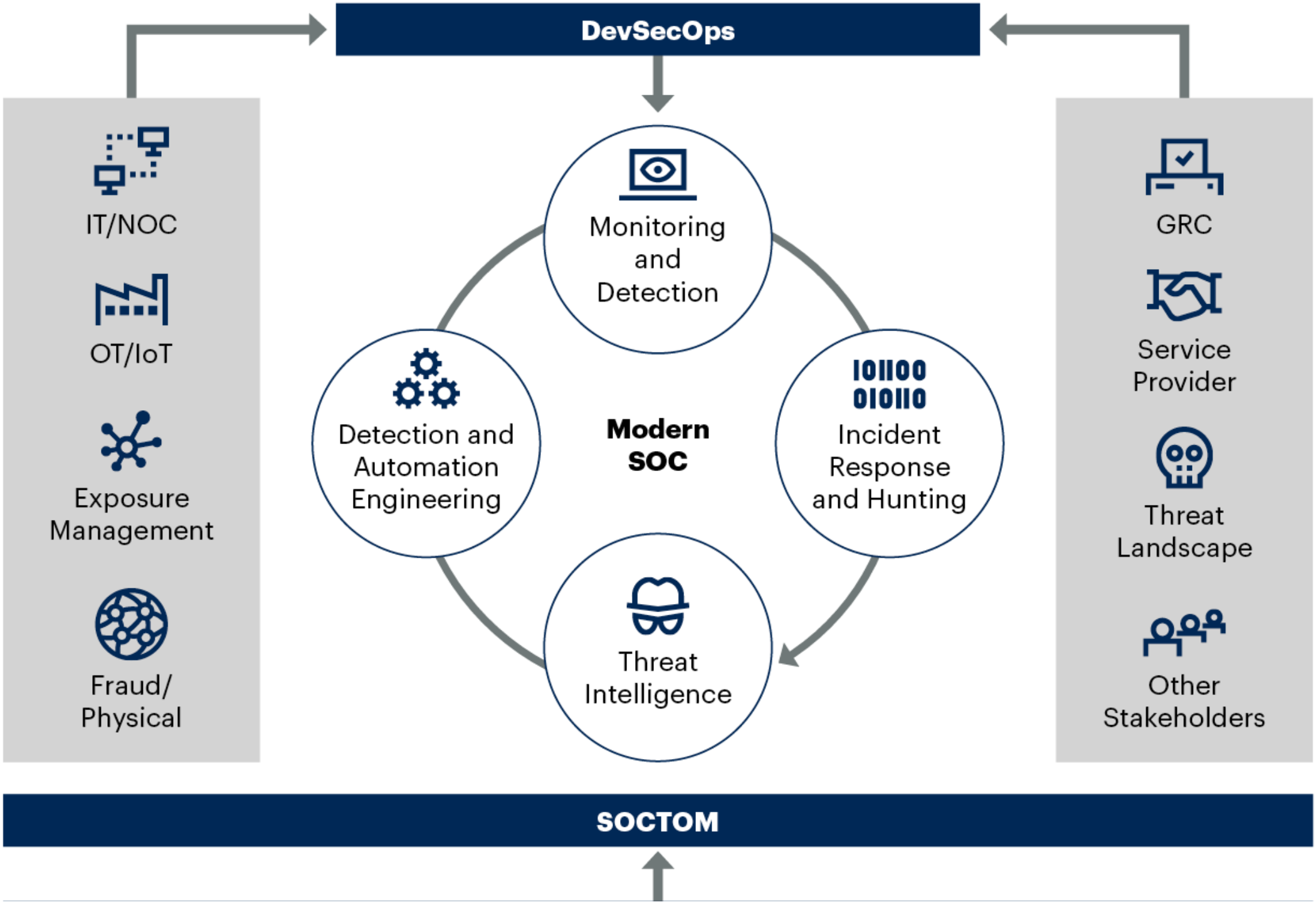
D'ici 2025, 33 % des organisations qui disposent actuellement de fonctions de sécurité internes tenteront en vain de créer un SOC interne efficace en raison de contraintes de ressources, telles que le manque de budget, d'expertise et de personnel.

Introduction

La perception prédominante d'un modèle SOC implique un emplacement physique avec des opérations centralisées guidées par un large cadre accepté par l'industrie pour la façon dont un SOC est censé fonctionner. Cette image est obsolète et n'est plus applicable dans le SOC moderne (voir Comment construire et exploiter un centre d'opérations de sécurité moderne), en particulier dans un monde post-COVID-19. Les responsables de la sécurité et de la gestion des risques (SRM) ont réalisé, via une fonction de forçage, qu'ils pouvaient fournir des opérations de sécurité (SecOps) et des fonctions SOC sans emplacement physique et avec des méthodes et des processus non standard. L'industrie de la sécurité doit également se rendre compte qu'il n'y a pas de bon modèle SOC pour exploiter ou fournir des fonctions SOC modernes. Les SOC varient en fonction de leur mission et de leurs objectifs, qui sont influencés par des caractéristiques telles que leur tolérance au risque, la verticale dans laquelle ils opèrent, le niveau de maturité, les compétences et l'expertise, les processus et les procédures, les outils utilisés et la manière dont les services de sécurité sont exploités - ce dernier si besoin. Un modèle SOC moderne (voir Figure 1) est tout ce dont un client a besoin, dans diverses permutations,priorités . Le paysage des menaces a constamment évolué plus vite que les défenseurs ne peuvent suivre le rythme, et les changements rapides provoqués par la transformation numérique ont augmenté le retard de manière exponentielle. Un SOC moderne ne réussira pas avec des étiquettes de modèles rigides qui dictent qu'un SOC ne peut être qu'une fonction à temps partiel, hybride avec un fournisseur, interne uniquement ou à plusieurs niveaux. Un modèle SOC moderne offre la flexibilité nécessaire pour couvrir toute permutation de ces modèles SOC et permettre aux responsables SRM et à l'entreprise de changer selon les besoins.

Figure 1. Exemple de modèle SOC moderne

Modern SOC Model Example



Source: Gartner
754096_C

gèrent d'autres domaines tels que la sécurité physique et la fraude. Les SOC ne possèdent pas tous les éléments des processus de sécurité, mais sont responsables de l'identification des problèmes et des incidents de sécurité et de la coordination entre plusieurs départements organisationnels pour gérer les réponses de sécurité, enregistrer et mesurer ces processus et informer une politique de sécurité efficace.

Évaluer les feuilles de route de l'architecture informatique, la dotation en personnel, les processus et les priorités commerciales pour déterminer le bon modèle SOC

La permutation des besoins en matière d'opérations de sécurité est vaste, ce qui signifie que ce qui fonctionne pour une entité a peu de chances d'être la meilleure réponse pour une autre. Des facteurs tels que le temps de maturité, le budget et les compétences disponibles auront une incidence sur la décision sur le modèle nécessaire. Utilisez les conseils trouvés dans la réponse rapide : interne, hybride ou externalisée ? Trouvez la meilleure approche de centre d'opérations de sécurité pour vous aider à répondre aux besoins en matière de calendrier, aux exigences de niveau de compétence et à l'alignement du budget.

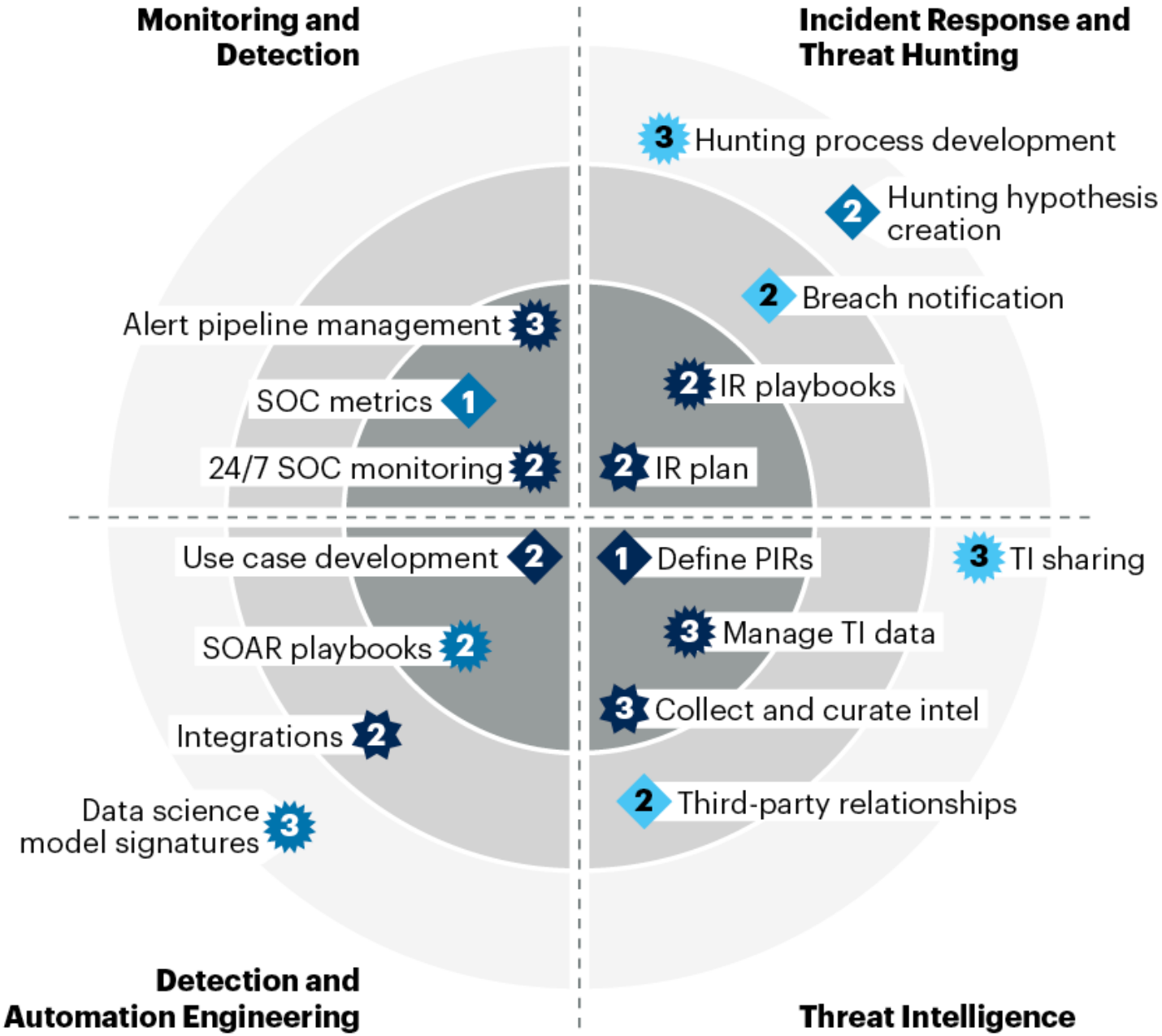
> **Chaque organisation a besoin d'une confrontation avec la réalité qui l'oblige à se demander : "Combien de fonctions de sécurité sommes-nous vraiment capables de réaliser efficacement en interne ?"**

Construire et exploiter un SOC est un parcours sans état final, ce qui signifie que les besoins de l'organisation évolueront inévitablement avec le temps. Les changements d'orientation de l'entreprise, les initiatives de transformation numérique, les fournisseurs de cloud, le leadership en matière de sécurité et/ou leur stratégie, ainsi que le paysage des menaces auront un impact direct sur la mission du SOC et sur la manière dont elle est accomplie. Un SOC complexe ou pleinement mature est un objectif, pas quelque chose de viable au début du processus. Il n'est pas conseillé de construire ou d'externaliser immédiatement un SOC complexe sans expérience préalable d'une telle opération, et certainementpas si les processus SOC fondamentaux ne sont pas établis. Par exemple, la mise en place d'une pratique de chasse aux menaces est absurde si l'organisation n'a pas mis en place de manuels de réponse aux incidents ou ne peut pas effectuer de base de détection et de corrélation des menaces.

Les responsables de la sécurité doivent travailler avec l'entreprise et les parties prenantes pour répertorier les capacités, les compétences, les processus et les outils actuels des opérations de sécurité et déterminer où se situent les lacunes. Lisez Créer un modèle d'exploitation cible SOC pour favoriser le succès ou tirez parti de la matrice SOC illustrée à la figure 2 pour aider à cartographier les capacités SOC actuelles, quel est l'état souhaité ou futur et ce qui est absolument hors de propos.

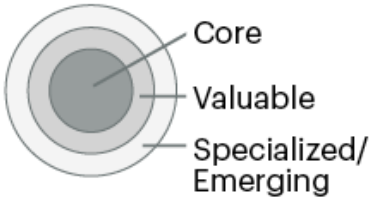
Figure 2. Matrice des capacités du SOC

SOC Capabilities Matrix



Legend

Relevance



Positive Impact on Development

Learning Curve

Impedance to Apply

Source: Gartner

754096_C

Il est important de construire un SOC basé sur les besoins de l'entreprise pour s'assurer que toutes les parties prenantes tirent profit de l'effort. La définition des priorités de l'entreprise et la compréhension des limites permettront de clarifier la sélection du modèle approprié à l'étape suivante.

Utiliser le modèle Gartner SOC HIT

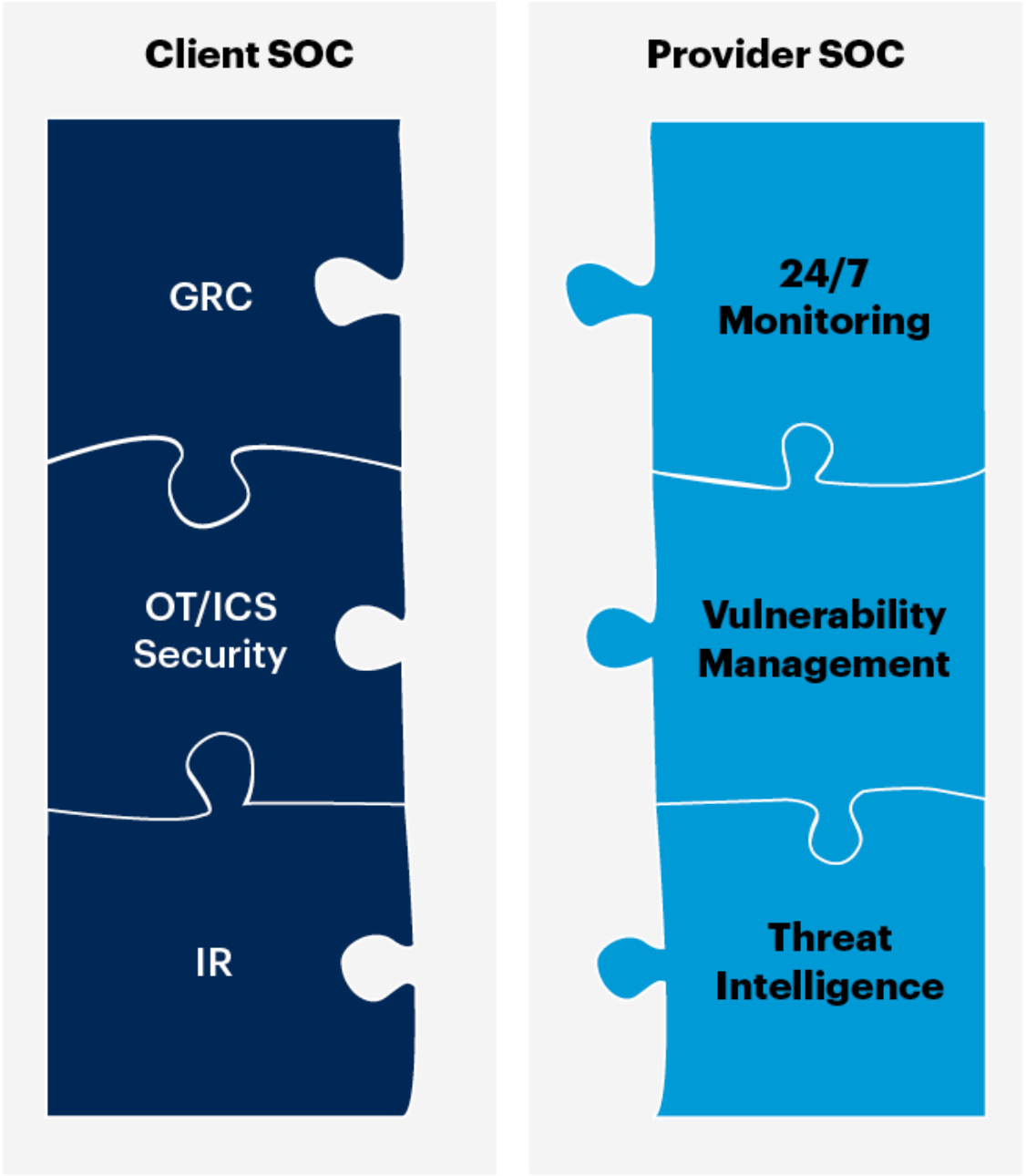
Le modèle Gartner SOC Hybrid-Internal-Tiered (HIT) fournit un guide de base aux organisations pour déterminer un modèle SOC pertinent qui s'aligne sur les besoins et les exigences discutés précédemment. Il n'est pas nécessaire de faire des modèles SOC un sujet complexe, ni qu'ils aient une multitude de facteurs de forme. Toute version d'un modèle SOC peut être alignée sur l'un des trois types de base.

Hybride

Il s'agit du plus diversifié des trois modèles SOC de base, et c'est sans doute le plus largement mis en œuvre par des organisations dans différentes régions du monde. Un SOC hybride est une combinaison de ressources internes et externes qui offre une fonction SOC combinée pour répondre aux besoins organisationnels. Il n'y a pas de cadre pour un modèle hybride, ni de « bonne » ou de « mauvaise » façon de le mettre en œuvre en raison de sa flexibilité. La figure 3 est un exemple de modèle SOC hybride qui sous-traite certaines fonctions à un fournisseur tout en conservant ce que l'exemple d'organisation a estimé pouvoir gérer en interne.

Figure 3. Exemple de SOC hybride

Hybrid SOC Example



Source: Gartner

754096_C

Un modèle hybride utilise généralement un service de sécurité géré (MSS), une détection et une réponse gérées (MDR) ou un fournisseur SIEM géré/co-géré (COMSIEM). Un nombre considérable de clients de Gartner externalisent les opérations de renseignement sur les menaces et de chasse aux menaces à des fournisseurs tiers en raison des exigences et des compétences uniques requises pour réussir. Ce modèle peut également inclure un centre d'exploitation de réseau hybride (NOC) et une fonction SOC (parfois appelée SOC multifonction) avec des exigences et des opérations uniques, détaillées dans Quand un SOC doit-il inclure des fonctions et des responsabilités NOC ? Dans certains cas, les organisations peuvent le faire, tout en tirant parti des fournisseurs de services, que ce soit en utilisant le même fournisseur pour les services de réseau gérés (MNS) et les services de sécurité, ou en utilisant des fournisseurs distincts.

Cependant, les éléments importants à prendre en compte avant de faire converger les fonctions SOC et NOC sont :

1. Les avantages l'emporteraient-ils sur les coûts?

2. Cela aiderait-il à créer des synergies plus étroites dans l'ensemble de l'organisation ?

Le modèle SOC hybride peut réduire le coût des opérations 24h/24 et 7j/7. Par conséquent, il est bien adapté non seulement aux petites et moyennes entreprises, qui dans la plupart des cas travaillent beaucoup avec des tiers (voir Contexte du marché intermédiaire : « Sélectionner le bon modèle SOC pour votre organisation »), mais également aux grandes organisations et aux SOC matures. qui peuvent externaliser sélectivement certains services de sécurité. L'adoption de ce modèle est motivée par une pénurie et un manque de disponibilité des compétences, de l'expertise et du personnel, des contraintes budgétaires générales et le coût considérable des opérations de sécurité 24h/24 et 7j/7.

Interne

L'attribut déterminant d'un SOC interne est d'avoir une fonction centralisée de détection et de réponse aux menaces 24 heures sur 24, 7 jours sur 7, avec une équipe dédiée et des processus et flux de travail robustes. Il est autonome et possède toutes les ressources nécessaires aux opérations de sécurité quotidiennes continues. Certaines fonctions spécialisées peuvent parfois être externalisées – comme les tests techniques (test d'intrusion/équipe rouge), la rétro-ingénierie des logiciels malveillants ou l'utilisation de sources externes de renseignements sur les menaces – mais les fonctions principales du SOC et les opérations quotidiennes sont assurées exclusivement par une équipe interne.

Les SOC internes conviennent généralement aux organisations bien financées qui peuvent se permettre au moins 10 à 12 employés pour une couverture 24 heures sur 24, 7 jours sur 7, et qui disposent d'un large éventail de licences d'outils de sécurité et d'une bibliothèque de processus et de manuels complets. Des facteurs supplémentaires peuvent inclure des environnements sensibles, des cas d'utilisation complexes et des exigences à haut risque ou de haute sécurité.

Les organisations choisissent de créer, de mettre en œuvre et d'exécuter leurs propres SOC lorsque :

- Les lois, les réglementations ou les problèmes de gouvernance empêchent l'option d'externalisation.
- Il y a des inquiétudes concernant une menace spécifique/ciblée.
- L'expertise et les connaissances spécialisées sur l'entreprise ne peuvent être externalisées.
- La pile technologique de l'organisation n'est pas prise en charge par les services de sécurité tiers.

à plusieurs niveaux

Un modèle SOC à plusieurs niveaux comporte plusieurs SOC exploités indépendamment au sein de la même organisation qui sont synchronisés par un SOC de niveau supérieur (commande ou parent), pour fournir une détection et une réponse unifiées des menaces.

Les organisations très grandes et/ou distribuées (celles qui ont des bureaux régionaux avec une indépendance opérationnelle), les fournisseurs de services offrant des MSS et ceux qui fournissent des services partagés (par exemple, les agences gouvernementales) peuvent avoir plus d'un SOC sous leur responsabilité. Lorsque ces SOC doivent fonctionner de manière autonome, ils fonctionneront comme des SOC centralisés ou distribués. Dans certains cas, les SOC fonctionneront ensemble, mais doivent être gérés de manière hiérarchique. Dans ces cas, un SOC doit être désigné comme SOC parent ou de commande.

Le SOC de niveau supérieur est responsable de :

- Diriger et coordonner les opérations de renseignement sur les menaces et les rapports.
- Responsabilités du commandant d'intervention.
- Définir la procédure opérationnelle standard pour le processus SOC et les playbooks.
- Établir des normes technologiques dans tous les SOC (par exemple, SIEM, EDR et NDR).

Évaluer en continu le modèle SOC adopté

L'histoire montre que les fonctions et la portée d'un SOC évolueront et/ou s'étendront également, compte tenu des changements inévitables du paysage des menaces et des besoins, des ressources disponibles, des cas d'utilisation et des exigences d'une organisation. Par exemple, en raison de la pandémie de COVID-19, de nombreuses organisations ont dû adopter de nouvelles technologies et de nouveaux processus de sécurité, acquérir et/ou développer des talents pour prendre en charge les opérations de sécurité à distance et/ou embaucher des prestataires de services externes pour aider à combler les lacunes (voir Embrace opérations de sécurité à distance) . Le modèle SOC adopté doit être continuellement évalué et évalué pour s'assurer qu'il s'aligne sur les buts et les objectifs de l'organisation et qu'il est maintenu à un niveau de fonctionnement efficace et réussi. Le tableau 1 fournit des exemples de questions et d'actions à entreprendre pour évaluer le modèle et l'efficacité du SOC.

Évaluez fréquemment les capacités du SOC (personnel, processus et technologie) pour déterminer s'il fonctionne conformément à la charte du SOC et au modèle opérationnel cible du SOC pour lequel il a été conçu.

Ces tests incluent, mais ne sont pas limités à :

- Tests d'intrusion (identifient et exploitent les vulnérabilités et les erreurs de configuration, et sont bruyants).
- Exercices de l'équipe rouge (évalue et teste furtivement les défenses de l'organisation, y compris la prévention, la détection et la réponse).
- Exercices de l'équipe violette (une forme d'équipe rouge, mais effectuant les tests de sécurité dans un modèle plus collaboratif, facilitant la communication et les leçons apprises en temps réel).
- Solutions de simulation de violation et d'attaque (exécute des simulations d'attaque pour identifier les failles de sécurité et valider que les contrôles de sécurité actuellement déployés fonctionnent efficacement).
- Capacité à atténuer les risques et les menaces identifiés par l'entreprise.
- Évaluations continues des menaces pour s'assurer que l'accent est mis sur les bonnes solutions, compétences et processus pour atténuer les risques .

Consultez Utilisation des tests d'intrusion et des équipes rouges pour évaluer et améliorer la sécurité et Réponse rapide : Quels sont les principaux cas d'utilisation de la technologie de simulation de violation et d'attaque ? pour plus d'informations sur les options de test de sécurité.

Les tests permettent au SOC d'être tenu à jour, garantissent la capacité de prévenir, de détecter et de répondre aux menaces modernes et émergentes, et effectuent les ajustements nécessaires afin de s'aligner sur les ressources existantes, les tolérances aux risques et les technologies de sécurité disponibles et les besoins en services. .

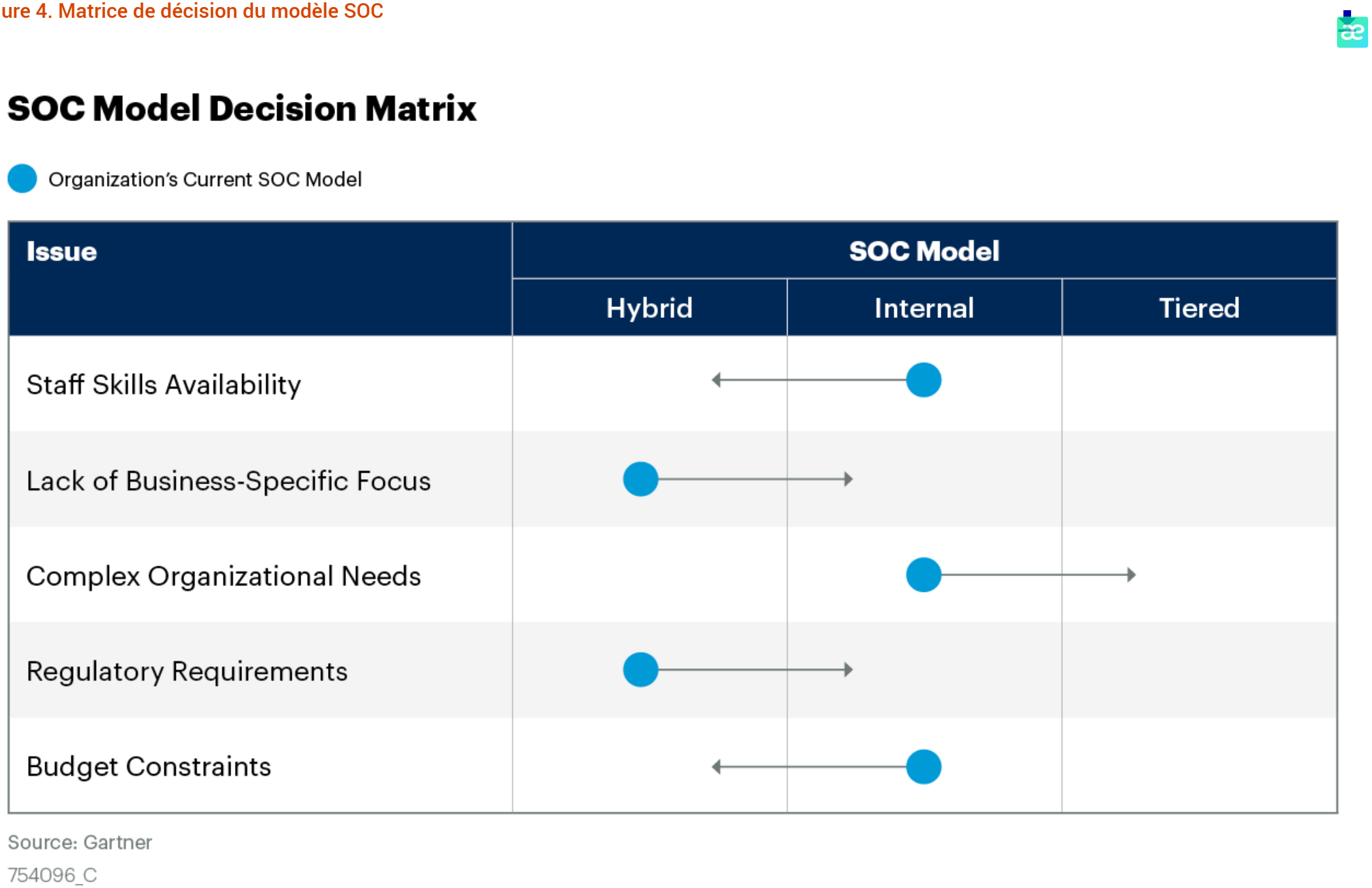
Tableau 1 : Exemples de questions et d'actions à poser lors de l'évaluation du modèle et de l'efficacité du SOC

Question à poser	*Comment répondre*
La mission du SOC est-elle toujours alignée sur le risque commercial ?	Maintenir une relation et une communication avec les chefs d'entreprise et les responsables des risques pour que le SOC reste aligné sur tout changement dans les menaces et les risques perçus pour l'entreprise.
Comment savoir si nos outils sont capables de détecter les dernières tactiques, techniques et procédures ?	Utilisez les technologies de simulation d'attaques par brèche pour tester en continu les outils existants et continuez à tirer parti des engagements de tests techniques dirigés par l'homme, tels que les équipes rouges, les tests de pénétration et les tests de l'équipe violette.
Le SOC s'attaque-t-il au paysage actuel des menaces ?	Effectuez des évaluations continues des menaces pour l'organisation et tirez parti des informations sur les menaces pour maintenir la visibilité et la compréhension du quoi, du pourquoi, du comment, du quand et peut-être du qui.
Comment mesurons-nous l'efficacité du SOC ?	Maintenez le cap pour atteindre les objectifs du SOCTOM et mesurez la capacité du SOC à améliorer l'investigation et la réponse à la détection des menaces au fil du temps.

Source : Gartner (octobre 2021)

Il peut être utile d'utiliser une matrice de décision pour faciliter le suivi et la gestion des évaluations régulières du modèle SOC et apporter les ajustements nécessaires à votre modèle opérationnel au fur et à mesure des besoins. Identifiez le problème ou les défis auxquels l'organisation est confrontée ou les ambitions de l'équipe de sécurité d'augmenter ou d'externaliser les capacités (voir l'exemple de la Figure 4). Utiliser les positions des problèmes clés pour décider du modèle SOC le plus efficace pour votre organisation à ce moment. Exécutez régulièrement l'exercice en présentant les problèmes nouvellement identifiés pour vous assurer que vous disposez toujours du modèle le plus efficace, ou si vous envisagez de passer à un modèle plus approprié pour montrer que vos besoins organisationnels ont évolué .

Figure 4. Matrice de décision du modèle SOC



Preuve

Cette recherche est basée sur l'enquête des clients et les recherches Gartner existantes