SOC Advisory

Le SOC : première ligne de défense contre les Cyber menaces

La difficulté croissante de la détection des incidents

La capacité à exercer une surveillance proactive des réseaux, des systèmes et des applications est un facteur clé pour défendre l'entreprise contre les menaces cyber, qu'elles soient d'origine externe ou interne.

Dans un environnement technologique en mutation constante (interconnexion des services personnels et professionnels, systématisation du recours au cloud, aux terminaux mobiles, au BYOD, développement du shadow IT, prolifération des objets connectés, nouvelles initiatives métier portées par la technologie), maintenir l'efficacité des moyens de détection et d'intervention sur incident constitue un défi de tous les instants pour les responsables cyber sécurité. Les SOC sont contraints de s'adapter rapidement pour continuer à identifier efficacement les événements anormaux au sein d'une masse croissante d'informations.

Parallèlement, la montée des obligations réglementaires (e.g., LPM, GDPR) introduit de nouvelles exigences et de nouvelles contraintes (parfois contradictoires) pour les SOC.

Choisir une stratégie de surveillance adaptée

La fonction Cybersécurité fait face à différents choix au moment de définir le modèle opérationnel du SOC : SOC dédié ou mutualisé, SOC interne, externe ou hybride, choix du niveau de service (24/24 ou horaires ouvrés, incluant ou non l'intervention sur incident), estimation des volumétries d'événements, etc.

Les réponses à ces questions dépendent de facteurs tels que la taille de l'entreprise, la nature et la sensibilité de son activité, son appétence au risque ou, dans certains cas, des obligations réglementaires ou contractuelles.

Savoir s'adapter aux changements

Face à des Cyber menaces en perpétuelle évolution, la capacité d'adaptation des défenses est un enjeu majeur. La flexibilité du SOC, son aptitude à évoluer rapidement pour prendre en compte des situations nouvelles et à s'améliorer en permanence, est une exigence qui doit être prise en considération en amont, dès la phase d'implémentation du projet de SOC.

Le SOC doit donc se donner les moyens de suivre et anticiper l'évolution incessante des menaces et techniques d'attaque, gagner en efficacité et mettre à profit les technologies émergentes (e.g., IA, sandboxing, threat intelligence).

Il doit aussi être impliqué dès l'origine dans tous les projets de modification des processus métier et des SI de l'entreprise afin d'en anticiper les conséquences en terme de surveillance de sécurité.

Mesurer l'efficacité du SOC

Que le SOC soit interne ou externalisé, les mêmes questions s'imposent au management qui s'interroge sur l'efficacité des mesures en place :

- *Quelles sont les menaces que nous détectons et celles que nous ne détectons pas ?*
- *A quelle vitesse savons-nous détecter une attaque ? Avec quelle rapidité sommes-nous en capacité de réagir ?*
- *Le SOC nous permet-il vraiment de réduire nos risques métiers ?*
- *Comment réduire le nombre de faux-positifs liés à la détection ?*
- *Répondons-nous aux exigences des réglementations actuelles et à venir ?*
- *Pouvons-nous réduire nos coûts ? Payons-nous le juste prix ?*

Nos services

SOC Strategy

- Cadrage de projets SOC : identification des besoins, définition du périmètre et de la mission du SOC
- Développement d'une stratégie autour de 4 axes : gouvernance, équipes, processus et technologie
- Choix du modèle organisationnel (interne, externe ou hybride, dédié ou mutualisé), scenarii et modélisation budgétaire
- Prise en compte de la réglementation en vigueur relative au(x) secteur(s) d'activité (LPM, GDPR, PDIS)

SOC Testing

- Evaluation de la performance : capacités et vitesse de détection, d'analyse et de réaction, taille du périmètre de détection, qualité de service
- Analyse de maturité : modèle organisationnel, mix de compétences, gestion de la connaissance, qualification des incidents de sécurité et réduction des faux-positifs, capacités d'évaluation des menaces
- Mise à l'épreuve : conduite de tests Redteam et Purpleteam

SOC Design

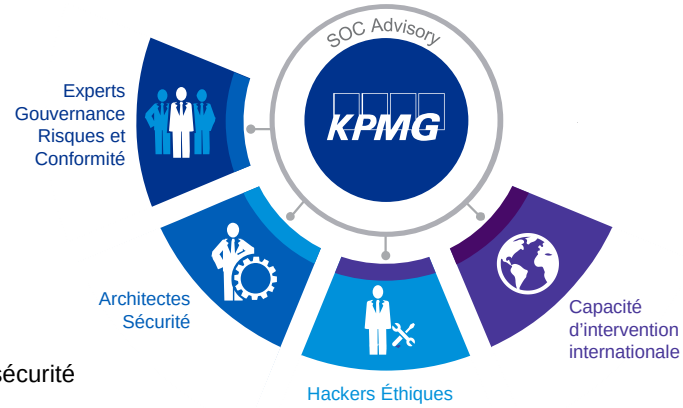
- Assistance à la conception du SOC selon la stratégie choisie
- Accompagnement au pilotage des appels d'offres et projets
- Intégration des nouvelles technologies de détection (sandboxing, IA, analyse comportementale, threat intelligence)
- Élaboration de la roadmap de mise en œuvre
- Mise en place d'une stratégie d'amélioration continue : processus de communication, veille technologique, base de connaissances, définition des cibles d'analyse
- Gestion des compétences et formation des personnels

Nos atouts

Pour délivrer ses services, KPMG s'appuie sur une **équipe pluridisciplinaire** combinant d'une part des compétences en Cybersécurité et d'autre part une expertise dans le domaine de la protection des données personnelles.

KPMG dispose d'un **réseau mondial** d'experts en Cybersécurité capables d'intervenir dans toutes les parties du globe pour nos clients multinationaux.

KPMG a été reconnu **leader mondial** en matière de Cybersécurité par Forrester en 2016 et 2017.



Exemples de prestations

- Tests d'intrusion sur infrastructure en scénario Redteam et Purpleteam pour tester la maturité et la réactivité du SOC
- Tests unitaires des fonctions de détection
- Revue des processus internes : détection, analyse, réaction, retour d'expérience et amélioration
- Simulation d'APT

Contacts

Vincent Maret
Associé, responsable de l'offre Cybersécurité et Protection des données personnelles

Tel : +33 1 55 68 26 64
Mob : +33 6 17 12 22 13
Email : vmaret@kpmg.fr

L'étendue et la nature des services détaillés dans ce document sont soumis aux règles déontologiques de la profession, selon que nous sommes commissaires aux comptes ou non de votre entité ou de votre groupe. Les informations contenues dans ce document sont d'ordre général et ne sont pas destinées à traiter les particularités d'une personne ou d'une entité. Bien que nous fassions tout notre possible pour fournir des informations exactes et appropriées, nous ne pouvons garantir que ces informations seront toujours exactes à une date ultérieure. Elles ne peuvent ni ne doivent servir de support à des décisions sans validation par les professionnels ad hoc. KPMG S.A. est le membre français du réseau KPMG International constitué de cabinets indépendants adhérents de KPMG International Cooperative, une entité de droit suisse (« KPMG International »). KPMG International ne propose pas de services aux clients. Aucun cabinet membre n'a le droit d'engager KPMG International ou les autres cabinets membres vis-à-vis des tiers. KPMG International n'a le droit d'engager aucun cabinet membre.

© 2020 KPMG S.A., société anonyme d'expertise comptable et de commissariat aux comptes, membre français du réseau KPMG constitué de cabinets indépendants adhérents de KPMG International Cooperative, une entité de droit suisse. Tous droits réservés. Le nom KPMG et le logo sont des marques déposées ou des marques de KPMG International