

FICHE PRATIQUE

Le SOC managé en 5 questions

Ce qu'il fait, ce qu'il ne fait pas, et comment juger de sa qualité

Le terme SOC recouvre des réalités très différentes selon les prestataires. Cette fiche donne les cinq questions qui permettent de comparer deux offres sur le fond plutôt que sur la plaquette.

1. Qu'est-ce qu'un SOC managé, concrètement

C'est une équipe et une plateforme qui collectent en continu les traces de votre système d'information — postes, serveurs, messagerie, pare-feu, cloud —, les corrélent pour faire ressortir ce qui sort de l'ordinaire, qualifient ce qui remonte, et déclenchent une réponse quand c'est justifié.

Les trois verbes comptent autant l'un que l'autre. Collecter sans corréler produit un entrepôt de journaux que personne ne lit. Corréler sans qualifier produit un flot d'alertes qui finit par être ignoré. Qualifier sans pouvoir agir produit un constat d'impuissance documenté.

2. En quoi cela diffère d'un antivirus ou d'un EDR

Un EDR protège un poste et voit ce qui se passe sur ce poste. Un SOC voit l'ensemble et détecte ce qui n'est anormal qu'à l'échelle du système : une connexion réussie depuis un pays inhabituel suivie d'une création de règle de transfert dans la messagerie, puis d'un accès inhabituel à un partage de fichiers. Pris isolément, chacun de ces événements est banal. Enchaînés, ils décrivent une compromission de compte en cours.

L'EDR et le SOC ne sont pas concurrents : l'EDR est l'un des capteurs du SOC, et souvent son bras armé pour isoler une machine.

3. Ce qu'on attend de vous

Un SOC ne fonctionne pas en autonomie complète, et se méfier des offres qui le laissent entendre. Trois contributions sont indispensables côté client.

- Un accès aux sources de journaux, et l'autorisation de les collecter
- Un interlocuteur joignable pour valider une action intrusive, comme l'isolement d'un poste de direction
- Une connaissance du contexte métier : quelles applications sont critiques, quelles opérations sont normales chez vous

Cette dernière contribution est celle qui fait la différence entre un SOC qui vous alerte utilement et un SOC qui vous noie. Un transfert massif de fichiers un vendredi soir est une alerte dans une collectivité, une routine dans une industrie qui clôture sa semaine de production.

4. Comment juger de la qualité d'une offre

Cinq questions à poser, dont les réponses sont vérifiables.

01 Que couvrez-vous exactement

Postes, serveurs, messagerie, cloud, applications métier : la liste des sources réellement collectées, pas celle des sources supportées.

02 Qui répond la nuit

Une astreinte n'est pas une supervision continue. Demandez qui traite une alerte à trois heures du matin, et sous quel délai.

03 Que se passe-t-il après l'alerte

Un SOC qui notifie et s'arrête vous laisse le travail. Demandez quelles actions de confinement sont incluses, et lesquelles nécessitent votre feu vert.

04 Comment mesurez-vous votre efficacité

Délai de détection, délai de qualification, délai de confinement, taux de faux positifs. Un prestataire qui ne mesure pas ne progresse pas.

05 Que devient ma donnée

Où sont hébergés les journaux, combien de temps, sous quelle juridiction. Question déterminante pour un établissement de santé ou une collectivité.

5. À partir de quelle taille est-ce pertinent

La question n'est pas la taille mais l'exposition et la dépendance. Une structure de quarante personnes dont l'activité s'arrête si le système d'information tombe, ou qui traite des données de santé, a davantage besoin de supervision qu'une entreprise de trois cents personnes dont l'outil principal reste utilisable hors ligne.

Le bon critère de décision : combien de temps pouvez-vous fonctionner sans votre système d'information, et combien de temps s'écoulerait aujourd'hui entre une intrusion et le moment où vous la remarqueriez. Si le second délai dépasse le premier, la supervision n'est plus une option de confort.

Ce document a une vocation informative et ne constitue pas un conseil juridique. Pour situer votre exposition réelle et vos priorités, échangez avec un expert ASEVIO : www.asevio.com/contact