MY TRUST PARTNER

Cybersecurite - Conformite - IA

Choisir son SOC manage

Criteres, SLA, questions RFP et comparatif interne vs externalise

LIVRE BLANC MTP 2026

www.mytrustpartner.fr - contact@mytrustpartner.fr - +33 1 84 16 05 27

Sommaire

1. Comprendre les differents niveaux de services

MDR, XDR, EDR : le vocabulaire

EDR (Endpoint Detection and Response) : outil de detection sur les postes. XDR (Extended Detection and Response) : corrIe les signaux de plusieurs sources (endpoints, reseau, cloud, identites). MDR (Managed Detection and Response) : service qui opere un EDR/XDR a votre place avec analystes humains 24/7. SOC managed = couverture complete (MDR + ingestion logs + threat hunting + reponse a incident).

Les piliers d'un SOC

Collecte de logs (SIEM), detection (EDR/XDR, regles de correlation, IA), analyse humaine (analystes niveau 1, 2, 3), reponse a incident, threat intelligence, threat hunting proactif, reporting client. Un SOC sans analystes humains n'est pas un SOC.

2. Les criteres de choix essentiels

Couverture horaire et delai de reaction

24/7/365 est la norme pour un SOC managed. Le delai de prise en charge d'une alerte critique doit etre contractuel (typiquement 15 minutes). Le delai de confinement d'un incident avere doit etre aussi formalise (1 a 4 heures selon criticite).

Souverainete et conformite

Donnees logs et incidents stockees en France ou UE. Conformite RGPD, HDS si secteur sante, ISO 27001 du prestataire. Verifiez la localisation des analystes (France ou offshore). Pour NIS2, privilegier un prestataire qualifie PDIS par l'ANSSI.

Technologie et integrations

Compatibilite avec votre stack existant (AD, M365/Workspace, pare-feu, cloud). Nombre de sources d'ingestion supportees. Capacite a integrer vos applications metiers. Evitez les solutions proprietaires qui vous enferment.

Equipe et certifications

Nombre d'analystes, niveau d'experience moyen, certifications (GIAC, OSCP, CISSP). Analyste dedie ou pool. Taux de rotation de l'equipe (indicateur de satisfaction). Formation continue sur les nouvelles menaces.

3. Les SLA critiques a negocier

Temps moyen de detection (MTTD)

Objectif raisonnable : moins de 15 minutes pour les alertes critiques. Moins de 1 heure pour les alertes hautes. A tracer dans un tableau de bord mensuel.

Temps moyen de qualification

De l'alerte brute a la decision (faux positif ou incident reel) : moins de 30 minutes pour les alertes critiques. L'objectif est d'eviter que les alertes s'accumulent et de ne pas submerger le client.

Temps moyen de remediation (MTTR)

Variable selon le type d'incident. Confinement sous 1 heure pour un ransomware detecte en phase initiale. Eradication complete sous 48 heures pour la plupart des incidents majeurs.

Penalites et credits service

Formaliser les consequences d'un depassement de SLA : credits de service, resiliation sans frais. Un prestataire qui refuse tout SLA chiffre est un drapeau rouge.

4. Les 20 questions a poser en RFP

Organisation et equipe

1) Combien d'analystes dans l'equipe ? 2) Quelle experience moyenne ? 3) Ou sont-ils localises ? 4) Quelles certifications ? 5) Comment geres-vous la nuit et les weekends ? 6) Quelle disponibilite garantie ?

Technologies

7) Quelles sont les solutions EDR/XDR utilisees ? 8) Comment ingestez-vous mes logs ? 9) Supportez-vous AWS/Azure/GCP ? 10) Quels sont les delais d'integration ?

Processus

11) Avez-vous un runbook public pour les principaux scenarios ? 12) Comment communiquez-vous en cas d'incident ? 13) Faites-vous des exercices de crise ? 14) Comment validez-vous un faux positif ?

Reporting et contrat

15) Frequence et contenu des rapports ? 16) Acces au SIEM pour consultation ? 17) Quels sont les SLA et penalites ? 18) Duree et reversibilite du contrat ? 19) Quelle prime liee a la performance ? 20) Qui est mon interlocuteur unique ?

5. Comparatif interne vs managed

Cout total sur 3 ans

SOC interne : 1,5 a 2,5 millions d'euros (equipe 24/7 minimum 8 ETP, licences SIEM/EDR, outillage, formation, locaux). SOC managed : 200 a 600 mille euros (selon perimetre et volume). Rupture de seuil autour de 500 postes : au-dela, l'internalisation devient plus pertinente.

Avantages du managed

Deploiement rapide (semaines vs mois), expertise mutualisee sur plusieurs clients (vision menaces plus large), flexibilite contractuelle, pas de probleme de recrutement, montee en charge facile.

Avantages de l'interne

Connaissance metier profonde, reactivite absolue, controle total des donnees, developpement de competences internes, integration poussee avec les equipes IT.

L'hybride : une option serieuse

Niveau 1 managed + niveau 2/3 interne, ou inversement. Utile pour garder l'expertise strategique tout en externalisant l'exploitation 24/7.

6. Nos services SOC

L'offre My Trust Partner

SOC managed 24/7 localise en France, analystes certifies, SLA contractuels chiffres, ingestion illimitee, threat hunting mensuel, reporting temps reel. Prestations complementaires : CISO as a Service, reponse a incident, audit NIS2. Consultation sans engagement : contact@mytrustpartner.fr, 01 84 16 05 27.

My Trust Partner

Cybersecurite - Conformite - IA

Labellise SecNumEdu-FC par l'ANSSI sur l'ensemble de notre catalogue formation.

Contact

www.mytrustpartner.fr
contact@mytrustpartner.fr
+33 1 84 16 05 27