

Cybersécurité PME

Les processus essentiels à structurer pour piloter cette activité au quotidien.

12 processus à parcourir

01 Définir et piloter le cap de l'activité

Chaque trimestre

- ☐ Choisir les priorités de croissance : audits ciblés, remédiation, supervision, sensibilisation et contrats récurrents de sécurité
- ☐ Fixer des objectifs de chiffre d'affaires, marge, récurrence, capacité et qualité de service
- ☐ Comparer chaque mois objectifs, signé, livré, facturé, charge et capacité disponible
- ☐ Ne pas lancer une offre sans cible, résultat, prérequis, coût de support et preuve de demande

02 Qualifier le besoin technique

À chaque opportunité

- ☐ Créer une trame de découverte technique reliée au problème métier
- ☐ Qualifier techniquement avec : actifs critiques, exposition, identités, sauvegardes, incidents, obligations, périmètre et autorisations
- ☐ Recueillir les preuves disponibles sans demander d'accès inutile ou non autorisé
- ☐ Ne pas chiffrer définitivement tant que les inconnues critiques et leurs hypothèses ne sont pas écrites

03 Qualifier, proposer et conclure une prestation ou un abonnement

À chaque opportunité

- ☐ Décrire précisément dans l'offre : actifs couverts, règles d'engagement, profondeur des tests, livrables, remédiation, SLA et exclusions
- ☐ Décrire responsabilités client-prestataire, critères d'acceptation et procédure de changement
- ☐ Relier chaque prix aux volumes, licences, charge, astreinte, risque et niveau de service
- ☐ Ne jamais promettre délai ou disponibilité dépendant d'un prérequis client non sécurisé

04 Déployer, paramétrer ou intervenir

À chaque intervention

- ☐ Standardiser l'exécution : autorisation écrite, précontrôles, collecte horodatée, limitation d'impact, validation et remédiation
 - ☐ Enregistrer version, configuration, équipement, intervenant, heure et preuve avant changement
 - ☐ Exécuter dans la fenêtre autorisée puis tester le résultat avec le critère prévu
 - ☐ Faire valider la mise en service et documenter anomalie, correction ou retour arrière
-

05 Planifier et régler les échéances

Chaque semaine

- ☐ Créer un calendrier des licences, matériels, cloud, fournisseurs, taxes et renouvellements
 - ☐ Valider chaque facture avec commande, service rendu, compte client et conditions convenues
 - ☐ Classer facture, justificatif, validation, période et paiement dans le dossier prévu
 - ☐ Prévoir chaque mois les sorties et renouvellements des huit semaines suivantes
-

06 Suivre la marge projet ou récurrente

Chaque mois

- ☐ Créer un budget avec prix, temps, licences, matériel, cloud, sous-traitance et marge cible
 - ☐ Tracer particulièrement les risques de marge : périmètre découvert tardivement, actifs non inventoriés, preuves dispersées, urgence et remédiation non cadrée
 - ☐ Comparer vendu, consommé, reste à faire, facturé et encaissé par dossier ou compte
 - ☐ Traiter toute dérive avant de la compenser par du temps gratuit ou une baisse de qualité
-

07 Organiser l'équipe et les astreintes

Chaque semaine

- ☐ Planifier selon les compétences nécessaires : analyse de vulnérabilité, réponse à incident, systèmes, réseau, identité, cloud et conformité
 - ☐ Affecter une personne seulement si compétence, capacité, accès et relais sont disponibles
 - ☐ Ne pas masquer une surcharge par des délais irréalistes ou des interventions non tracées
 - ☐ Comparer chaque semaine charge prévue, tickets entrants, urgences, reste à faire et couverture
-

08 Transmettre un dossier en cas d'absence

À chaque transmission

- ☐ Transmettre obligatoirement : chronologie, périmètre, indicateurs, preuves, mesures prises, secrets révoqués, risques et contacts d'urgence
 - ☐ Partager tickets, changements, versions, décisions, contacts et échéances à jour
 - ☐ Faire reformuler au remplaçant le risque principal et la prochaine action sûre
 - ☐ Tester chaque trimestre la reprise d'un dossier critique sans son titulaire
-

09 Arbitrer et valider la production sans blocage

Chaque mois

- ☐ Déléguer explicitement : qualification d'alerte, mesure conservatoire, isolement autorisé, collecte de preuve et escalade
 - ☐ Classer chaque arbitrage selon impact client, sécurité, disponibilité, délai et marge
 - ☐ Escalader immédiatement tout risque majeur de sécurité, données, continuité ou engagement contractuel
 - ☐ Revoir chaque mois les décisions inutilement remontées et les limites devenues inadaptées
-

10 Centraliser et sécuriser les accès essentiels

Chaque mois

- ☐ Sécuriser les accès suivants : coffre de secrets, consoles EDR, SIEM, annuaire, pare-feu, sauvegardes et comptes privilégiés
 - ☐ Attribuer des accès nominatifs et minimaux puis les retirer dès la fin du besoin
 - ☐ Contrôler chaque mois comptes partagés, droits privilégiés, comptes dormants et secrets anciens
-

11 Sécuriser contrats, données et continuité

À chaque dossier

- ☐ Sécuriser en priorité : règles d'engagement, habilitation, chaîne de preuve, données personnelles, notification, rétention et continuité
 - ☐ Faire signer les autorisations et engagements nécessaires avant tout accès sensible
 - ☐ Ne collecter, utiliser, partager ou conserver que les données nécessaires et autorisées
 - ☐ Tester sauvegarde, restauration, contacts d'urgence, révocation et preuves selon la criticité
-

12 Cadrer un parc, un projet ou une intervention

À chaque dossier

- ☐ Cadrer précisément : inventaire des actifs, fenêtres de test, adresses autorisées, contacts d'urgence, preuves et arrêt immédiat
 - ☐ Nommer décideur, référent technique, utilisateurs concernés, valideur et contact d'urgence
 - ☐ Confirmer accès, données, sauvegardes, fenêtre, test, retour arrière et communication
 - ☐ Aucun changement hors périmètre sans impact délai, coût, sécurité et responsabilité accepté
-