DÉVELOPPEMENT DES EFFECTIFS

IDENTIFIER LES BESOINS

- Identifiez vos exigences en matière de personnel.
  - Évaluez la complexité de vos opérations et la rapidité à laquelle les actions doivent être exécutées.
  - Envisagez les besoins de capacité de mobilisation et si des technologies avancées peuvent permettre de réduire la surface d'attaque.
- Identifiez vos besoins de personnel.
  - Envisagez la compétence, la flexibilité et l'agilité de l'équipe chargée de la cyber-sécurité dans votre organisation.
  - Identifiez des structures de signalement idéales et précisez pour lesquelles une polyvalence serait préférable.
- Définissez les connaissances, aptitudes, capacités et compétences requises de vos employés en fonction des postes qu'ils occupent et des fonctions métiers qu'ils prennent en charge.
- Identifiez les écarts critiques au sein de l'équipe chargée de la cyber-sécurité en place dans votre organisation.
  - Utilisez des outils existants tels que le cadre NICE pour orienter les évaluations internes des postes et des responsabilités.

FAVORISER LA FORMATION ET LE DÉVELOPPEMENT EN INTERNE

- Développez des fiches de carrière qui soulignent les parcours de progression de votre équipe chargée de la cyber-sécurité
- Identifiez des parcours dans votre organisation pour requalifier et repositionner des employés talentueux à des postes chargés de la cyber-sécurité.
  - Envisagez la possibilité de points d'entrée non conventionnels dans la cyber-sécurité basés sur l'intérêt et la capacité.
  - Développez des programmes de mise à niveau des compétences et de requalification et encouragez les transitions au sein de votre organisation.
- Encouragez la formation en interne et l'apprentissage autonome.
  - Offrez des opportunités de formation continue et de validation des compétences.
- Effectuez le suivi des données sur la fidélisation du personnel.
  - Évaluez périodiquement les données de fidélisation afin de déterminer si la programmation de formations et du développement répond aux besoins des employés.

AMÉLIORER LE RECRUTEMENT EXTERNE

- Améliorez les offres d'emploi en rédigeant des fiches de postes claires et cohérentes en interne.
  - Utilisez des outils existants tels que le cadre NICE pour mettre en avant des compétences pertinentes.
- Collectez des données sur le recrutement par le biais d'une procédure de candidature, en capturant des types de candidats et des expériences professionnelles antérieures.
  - Systématisez la collecte et le partage des données au sein de l'entreprise afin d'éviter la formation d'un silo et d'appuyer le repérage et le développement des talents.
  - Évaluez périodiquement les données de recrutement pour identifier les écarts de portée.
- Fiez-vous à plusieurs indicateurs pour évaluer le potentiel des candidats.
  - Envisagez la mise en œuvre d'évaluations d'embauche systématiques.
  - Évaluez des diplômes, certifications et expériences professionnelles pertinents.
  - Ne vous fiez pas qu'à une seule métrique spécifique (par ex., un diplôme équivalent à un master en ingénierie) lors de vos prises de décisions en matière de recrutement.

Approches fondamentales

Envisagez les approches stratégiques suivantes lors du développement d'une équipe chargée de la cyber-sécurité.

1. **Développez le pipeline des approvisionnements** produisant les nouveaux talents.
   - Avez-vous des relations avec des universités et des collèges d'enseignement professionnels ?
   - Proposez-vous des stages ou des formations en apprentissage dans le domaine de la cyber-sécurité ?
2. **Identifiez et faites correspondre les approvisionnements existants** avec les opportunités de talents.
   - Votre service des ressources humaines convertit-il efficacement les compétences requises dans les publications des fiches de postes ?
3. **Reformez** le **personnel existant** pour qu'il intègre l'équipe chargée de la cyber-sécurité.
   - Votre organisation utilise-t-elle les talents existants en transférant des ressources dans son équipe chargée de la cyber-sécurité ?
4. **Réduisez les demandes** sur votre équipe chargée de la cyber-sécurité grâce à l'**innovation technologique**.
   - Avez-vous passé des accords avec des prestataires de services tiers pour créer une capacité de mobilisation pendant les périodes critiques ?
5. **Améliorez le maintien** des effectifs actuels.
   - Votre organisation investit-elle dans des membres d'équipe talentueux ?
   - Votre organisation permet-elle à des individus intéressés d'explorer des carrières dans la cyber-sécurité ?

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE
INTERNATIONAL MONETARY FUND
THE WORLD BANK IBRD • IDA | WORLD BANK GROUP
SWIFT
SWIFT INSTITUTE
FS-ISAC
Standard Chartered
CYBER READINESS INSTITUTE
GLOBAL CYBER ALLIANCE
ICBA INDEPENDENT COMMUNITY BANKERS of AMERICA®