Procom

L'équipe qui assure le rendement.

CONSTITUER UNE MAIN-D'ŒUVRE RÉACTIVE EN CYBERSÉCURITÉ

PERSPECTIVES SUR LA SPÉCIALISATION

www.procomservices.com

Un guide pratique pour la constitution d'une main-d'œuvre spécialisée en cybersécurité qui adhère à la stratégie de défense de votre organisation et qui est prête à atténuer les menaces émergentes.

TABLE DES MATIÈRES

Comprendre **le nouveau paysage des menaces**

La surface d'attaque des menaces de cybersécurité s'est étendue, ce qui nécessite un renforcement de la main-d'œuvre spécialisée en cybersécurité pour protéger les données et les infrastructures sensibles.

Par ailleurs, le secteur de la cybersécurité est confronté à une grave pénurie de compétences en raison de l'augmentation des menaces, des avancées technologiques et du manque de programmes de formation complets.

« LE CYBERESPACE EST UNE PORTE GRANDE OUVERTE – N'IMPORTE QUI PEUT LA FRANCHIR, ET NOMBREUX SONT CEUX QUI LE FONT. LES DANGERS D'UNE TECHNOLOGIE NUMÉRIQUE UTILISÉE À DES FINS MALVEILLANTES SONT DE PLUS EN PLUS GRANDS ET PRÉSENTENT DE NOUVELLES VULNÉRABILITÉS POUR LES PERSONNES, POUR LES INSTITUTIONS ET POUR LES PAYS. »

– ANTÓNIO GUTERRES, SECRÉTAIRE GÉNÉRAL DES NATIONS UNIES

Les menaces critiques et émergentes suivantes en matière de cybersécurité requièrent une attention immédiate et proactive de la part des organisations du monde entier :

- **ATTAQUES INFONUAGIQUES**
- **MENACES LIÉES À L'IDENTITÉ**
- **EXPLOITS DES APPLICATIONS**
- **PUBLIQUES – RANÇONGICIELS**
- **VULNÉRABILITÉS DE TYPE « JOUR ZÉRO »**

10,5 $
BILLIONS

Les coûts liés aux dommages causés par la cybercriminalité dans le monde devraient atteindre 10,5 billions de dollars par année d'ici 2025, une croissance de 15 % par année, ce qui témoigne de l'urgence pour les organisations d'investir dans des talents spécialisés en cybersécurité.

(SOCRadar Cyber Intelligence Inc.)

N’avoir confiance en rien, **tout vérifier**

Les modèles traditionnels de cybersécurité ne suffisent plus à protéger les organisations contre les nouvelles menaces. Le modèle « confiance zéro », qui repose sur l’approche « Ne jamais faire confiance, toujours vérifier », s’est imposé comme le pilier des stratégies modernes en matière de cybersécurité. La confiance zéro ne se réduit pas à une technologie ou à un ensemble d’outils. Il s’agit d’un changement d’état d’esprit qui modifie la façon dont les organisations abordent la sécurité.

Les organisations qui entendent s’imposer en cybersécurité doivent non seulement adopter les principes de la confiance zéro, mais aussi développer une main-d’œuvre qui adhère à cette stratégie. La constitution d’une équipe qui maîtrise les méthodes de confiance zéro permet d’intégrer la sécurité à tous les niveaux de l’organisation, depuis le développement d’applications sécurisées jusqu’à la gestion des données sensibles.

L’IMPORTANCE DE LA CONFIANCE ZÉRO :

Un paysage de menaces sans précédent : Les cyberattaques devenant de plus en plus sophistiquées, il est nécessaire de mieux gérer les risques. La confiance zéro permet d’atténuer les risques en partant du principe que chaque interaction, qu’elle soit interne ou externe, peut constituer une menace.

Transformation de la main-d’œuvre : Alors que les organisations adoptent le télétravail, l’infonuagique et la collaboration numérique, la confiance zéro devient essentielle pour s’assurer que l’accès aux ressources est strictement contrôlé et sans cesse vérifié.

Conformité réglementaire : En raison de l’augmentation de la surveillance réglementaire, l’adoption d’une architecture de confiance zéro peut aider les organisations à répondre à des exigences de conformité strictes tout en protégeant les données sensibles.

Harmoniser avec les cadres de cybersécurité établis

Établir des fondements solides en matière de cybersécurité pour votre organisation

01

LA TRIADE CIA

Un modèle fondationnel de cybersécurité qui assure la confidentialité, l'intégrité et l'accessibilité (CIA) des données, en les protégeant contre les accès non autorisés et les modifications, et en veillant à ce qu'elles soient accessibles en cas de besoin.

02

CADRE DU NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

Un guide complet pour les organisations, structuré autour des fonctions d'identification, de protection, de détection, de réponse et de récupération, qui aide à gérer et à réduire efficacement les risques liés à la cybersécurité.

03

ISO/IEC 27001

AUne norme reconnue à l'échelle internationale pour la gestion de la sécurité de l'information, qui fournit une approche systématique de la sécurisation des données sensibles et de la conformité aux réglementations mondiales.

04

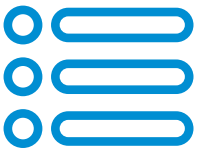
CADRE NICE

Un cadre détaillé axé sur la définition et le développement d'une main-d'œuvre compétente en cybersécurité, décrivant les fonctions, les compétences et la formation nécessaires pour se défendre contre l'évolution des cybermenaces. Nous nous concentrerons principalement sur ce cadre.

Intégration du cadre de cybersécurité NICE

Élargir votre main-d'œuvre spécialisée en cybersécurité : Fonctions dans les domaines émergents

L'évolution des cybermenaces s'accompagne d'une évolution des fonctions et des compétences de la main-d'œuvre spécialisée en cybersécurité. Le cadre NICE pour la main-d'œuvre spécialisée en cybersécurité propose une approche structurée pour déterminer les fonctions et les compétences nécessaires pour traiter les domaines nouveaux et émergents de la cybersécurité. Le cadre peut être décomposé en cinq éléments distincts, mais chacun d'entre eux comporte d'autres sous-éléments. Les catégories, par exemple, peuvent être décomposées comme suit : Supervision et gouvernance, Conception et développement, Mise en œuvre et exploitation, Protection et défense, Enquête, Renseignement sur le cyberespace et Effets sur le cyberespace. La consultation du cadre NICE aidera votre organisation à définir une fonction hautement spécialisée en cybersécurité.



Catégories

Les grands domaines fonctionnels qui organisent le travail de cybersécurité en sept catégories distinctes, comme Protection et défense, orientent la structure générale des fonctions de cybersécurité.

Spécialités

Des sous-divisions dans les catégories axées sur des types particuliers de tâches de cybersécurité, qui fournissent des classifications détaillées des différentes fonctions de cybersécurité.

Postes

Des définitions de postes figurant dans le cadre, qui précisent les tâches, les connaissances, les compétences et les aptitudes nécessaires pour des emplois précis dans le secteur de la cybersécurité.

Tâches

Activités particulières associées à chaque rôle professionnel, détaillant les responsabilités et les actions quotidiennes nécessaires à l'exécution du travail.

CCA

Connaissances, compétences et aptitudes (CCA). Les compétences essentielles requises pour chaque poste, qui orientent à la fois l'embauche et le perfectionnement professionnel en cybersécurité.

Faire face aux menaces grâce à des postes spécialisés

1

Analystes en cyberdéfense

Détection, analyse et atténuation des cybermenaces en temps réel.

2

Répondant·es aux incidents

Gestion et coordination des réponses aux incidents de cybersécurité.

3

Analystes en évaluation des vulnérabilités

Détermination et atténuation des vulnérabilités des systèmes avant qu'elles ne puissent être exploitées.

4

Évaluateur·trices de logiciels sécurisés

Évaluation de la sécurité des logiciels tout au long du cycle de vie du développement.

5

Spécialistes en sécurité infonuagique

Sécurisation des données et de l'infrastructure dans les environnements infonuagiques

Constituer une main-d'œuvre résiliente en cybersécurité

Aujourd'hui, le paysage des menaces est complexe et les auteurs de menaces ciblent les organisations à l'échelle mondiale. La constitution d'une main-d'œuvre résiliente en cybersécurité suppose non seulement la capacité de se défendre contre les menaces actuelles, mais aussi d'anticiper, de s'adapter et de répondre aux nouveaux défis à mesure qu'ils émergent. Pour y parvenir, les organisations doivent donner la priorité au développement continu des compétences techniques, favoriser une approche multidisciplinaire et mettre en œuvre des pratiques stratégiques de recrutement et de maintien en poste qui s'harmonisent avec le cadre NICE pour la main-d'œuvre spécialisée en cybersécurité.

ACCORDER LA PRIORITÉ AU DÉVELOPPEMENT CONTINU DES COMPÉTENCES DANS UN CONTEXTE D'ÉVOLUTION DES MENACES

Objet : La formation continue est essentielle, car 62 % des entreprises indiquent que le manque de personnel compétent en cybersécurité est un problème important dans la gestion de leur posture de sécurité.

Mise en œuvre : Alors que les cybermenaces évoluent, il est essentiel de maintenir les compétences de votre équipe à jour. Investissez dans des formations régulières et des certifications comme celles du CISSP et de l'OSCP, qui sont cruciales pour les fonctions nécessitant une expertise technique approfondie dans des domaines comme les tests de pénétration, la réponse aux incidents et le renseignement sur les menaces. L'apprentissage continu est nécessaire pour lutter contre les menaces avancées comme les rançongiciels, dont le nombre d'attaques a augmenté de 105 % à l'échelle mondiale rien qu'en 2021.

TIRER PARTI D'UN RECRUTEMENT FONDÉ SUR LES DONNÉES POUR RÉDUIRE LA PÉNURIE DE MAIN-D'ŒUVRE

Objet : Tirer parti des stratégies de recrutement qui ciblent les compétences les plus demandées, comme celles liées à la sécurité infonuagique et à l'analyse des menaces.

Mise en œuvre : Alors que LinkedIn fait état d'une augmentation de 30 % de la demande de professionnels spécialisés en cybersécurité en glissement annuel, il est essentiel d'utiliser des outils de recrutement fondés sur les données. Concentrez-vous sur l'embauche pour les postes définis par le cadre NICE, comme les analystes en cyberdéfense et les ingénieurs en sécurité infonuagique, afin de vous assurer que votre organisation est en mesure de faire face aux cybermenaces modernes. Les bonnes stratégies de recrutement sont essentielles pour remédier à la pénurie mondiale de talents spécialisés en cybersécurité.

FAVORISER L'EXPERTISE INTERFONCTIONNELLE POUR ATTÉNUER LES RISQUES

Objet : Les organisations dotées d'équipes de cybersécurité interfonctionnelles ont 2,5 fois plus de chances de disposer d'une posture de sécurité solide.

Mise en œuvre : Intégrez des professionnels spécialisés en cybersécurité aux équipes chargées des questions juridiques, de la conformité et des opérations commerciales. Cette collaboration garantit que les stratégies de cybersécurité sont harmonisées avec les objectifs plus larges de l'entreprise et les exigences réglementaires. Par exemple, les équipes peuvent travailler ensemble pour relever les défis réglementaires croissants posés par des cadres comme le GDPR et le CCPA, dont les amendes pour non-conformité ont atteint plus d'un milliard de dollars en Europe rien qu'en 2021.

DES RESSOURCES EXTERNES PEUVENT COMPLÉTER LES ÉQUIPES INTERNES

Objet : Le manque de compétences en cybersécurité pousse les entreprises à faire de plus en plus appel à des ressources externes pour répondre à leurs besoins en matière de sécurité.

Mise en œuvre : Établissez des relations avec un fournisseur spécialisé en ressources externes pour combler les lacunes critiques de votre équipe de cybersécurité. Cette approche vous permet d'accéder aux meilleurs talents selon les besoins, en particulier pour les tâches hautement spécialisées comme 'analyse médicolégale, la recherche de menaces avancées ou la réponse aux incidents. Selon une enquête de Deloitte, 41 % des organisations font désormais appel à des travailleur·euses occasionnel·les pour des fonctions essentielles en cybersécurité, ce qui leur permet de rester agiles et réactives face à l'évolution des menaces.

Renforcer la posture et l'état de préparation en matière de sécurité

Posture de sécurité proactive : la clé des économies de coûts

Une approche proactive de la cybersécurité est essentielle. Les organisations qui se concentrent sur des mesures proactives, comme la surveillance continue et le renseignement sur les menaces en temps réel, voient leurs coûts de reprise après une violation diminuer. L'utilisation d'outils comme les systèmes de gestion des informations et des événements de sécurité, que 80 % des grandes entreprises ont mis en place, permet de détecter et d'atténuer les menaces avant qu'elles ne s'aggravent.

L'importance des évaluations régulières de la sécurité

Des contrôles de sécurité et des tests de pénétration réguliers sont essentiels pour repérer les vulnérabilités et y remédier. Une étude de Deloitte montre que les entreprises qui procèdent à ces évaluations tous les trimestres courent 40 % moins de risques de subir des violations importantes. Les tests de pénétration simulent des attaques réelles et fournissent des renseignements précieux qui permettent aux entreprises de renforcer leurs défenses de manière proactive.

Planification stratégique de la réponse aux incidents

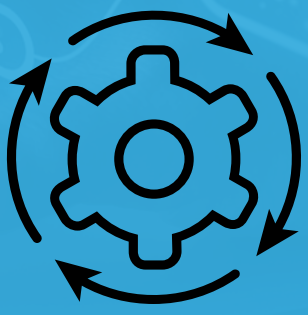
Un plan d'intervention en cas d'incident complet est essentiel pour réduire au minimum l'incidence des cyberincidents. Les recherches d'IBM indiquent qu'un plan d'intervention en cas d'incident bien préparé peut réduire les coûts d'une violation de 2,66 millions de dollars en moyenne. La tenue régulière de formations et de simulations permet à votre équipe de réagir avec rapidité et efficacité en cas d'incident.

Favoriser une culture de sensibilisation à la cybersécurité

Selon le Rapport des enquêtes sur les violations de données de Verizon, l'erreur humaine demeure l'une des principales causes des violations de données, puisqu'elle est à l'origine de 85 % des incidents. Les organisations qui investissent dans des simulations régulières d'hameçonnage et dans des formations à la cybersécurité réduisent de 70 % la probabilité de réussite des attaques par hameçonnage. Pour protéger les actifs de votre organisation, il est indispensable d'instaurer une culture dans laquelle chaque employé est au courant des meilleures pratiques en matière de cybersécurité.

Des programmes de formation réguliers et attrayants

Participation et engagement des dirigeants



Intégration de la cybersécurité dans les activités quotidiennes

Procom

L'équipe qui assure le rendement.

Procom peut vous aider à trouver des talents spécialisés en cybersécurité.

1	**PROCESSUS DE RECRUTEMENT RIGHTFIT™ :** Chaque candidat·e informatique spécialisé·e en cybersécurité que nous vous soumettons a été soumis à notre processus éprouvé en cinq étapes, certifié ISO, pour garantir qu'il·elle possède les compétences nécessaires et qu'il·elle correspond bien aux besoins de votre organisation et de votre projet.
2	**RENSEIGNEMENTS SUR LES TAUX DU MARCHÉ :** En sa qualité de l'une des plus importantes entreprises de dotation en personnel informatique d'Amérique du Nord, Procom dispose de plus de 28 000 points de données par mois sur les tarifs en vigueur dans tous les secteurs verticaux et les secteurs d'activité d'Amérique du Nord.
3	**PORTAIL CLIENTÈLE DÉDIÉ :** Accédez à vos talents Procom et gérez-les depuis un seul et même tableau de bord. Gagnez en visibilité sur le cycle de vie du recrutement de vos candidat·es. Collaborez et communiquez plus facilement pour prendre plus rapidement de meilleures décisions d'embauche.
4	**EXPÉRIENCE AVÉRÉE :** Les spécialistes en recrutement de talents informatiques spécialisés en Salesforce de Procom comptent plus de 45 années d'expérience dans le secteur de la cybersécurité.
5	**VILLES DESSERVIES :** Comptant plus de 20 succursales en Amérique du Nord, Procom est l'une des plus importantes entreprises nord-américaines de dotation en personnel informatique et de gestion des ressources externes.